IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

Received February 26, 2017, accepted April 8, 2017, date of publication April 13, 2017, date of current version May 17, 2017.

Digital Object Identifier 10.1109/ACCESS.2017.2694050

The Fall of One, the Rise of Many: A Survey on Multi-Biometric Fusion Methods

LAVINIA MIHAELA DINCA AND GERHARD PETRUS HANCKE, (Senior Member, IEEE)
Department of Computer Science, City University of Hong Kong, Hong Kong

Corresponding author: Lavinia Mihaela Dinca (lavinia.dinca@gmail.com)

This work was supported by the City University of Hong Kong under Project 7004473.

ABSTRACT Increasing operational and security demands changed biometrics by shifting the focus from single to multi-biometrics. Multi-biometrics are mandatory in the current context of large international biometric databases and to accommodate new emerging security demands. Our paper is a comprehensive survey on multi-biometrics, covering two important topics related to the multi-biometric field: fusion methods and security. Fusion is a core requirement in multi-biometric systems, being the method used to combine multiple biometric methods into a single system. The fusion section surveys recent multi-biometric schemes categorized from the perspective of fusion method. The security section is a comprehensive review of current issues, such as sensor spoofing, template security, and biometric encryption. New research trends and open challenges are discussed, such as soft, adaptive contextual-based biometrics. Finally, an implementation blueprint for a multi-biometric system is presented in the form of a list of questions to be answered when designing the system.

INDEX TERMS Biometric sensor, multi-biometrics, multi-biometric fusion, template protection, biometric cryptosystems, biometric key derivation.

I. INTRODUCTION

Biometrics are found in a number of fields [1], including medical applications, e.g. body dimensions and blood type, natural science studies, e.g. changes in the evolution of the human species, and social sciences, e.g. changes in anthropology of the human species, but is probably most widely known for its use in crime forensics and information security services ranging from authentication to key derivation. Today the use of biometrics in security applications are part and parcel of our everyday lives.

The spread of biometrics was triggered by two factors: technical advancements and need for security. The need for special sensors to obtain biometrics was long considered a disadvantage, especially if multi-biometrics was considered. Today reliable biometric data can be obtained more easily with everyday devices being interconnected and having the ability to gather sensor data [2], [3], with advances in sensor hardware [4], [5]. For example, a smartphone has a multitude of potential biometric sensors, some for this very purpose, like a fingerprint scanner, and others that can capture biometrics as a secondary function such as a high resolution camera, for face recognition, iris and retina scans, a microphone for voice recording, and inertial sensors for gait. Of course, these same devices could also be misused to gather personal data, requiring further consideration about system security [6], [7]. Security concerns is the second factor for the adoption of multi-biometrics. Although there are many acceptable ways to authenticate people biometrics provide the strongest evidence that the person in question is actually involved, e.g. a password could be given to someone else. Most countries have implemented eIDs, which include biometric elements on passports and IDs, but some have also created a unique digital ID for the subject in the form of a digital certificate/private key, such as project Stork [8], for important online transactions like tax filings. Biometrics also offer several additional security advantages such good entropy when used to derive encryption keys, non-repudiation and negative recognition. Negative recognition is useful in cases where a user should be prevented from denying being already enrolled in the biometric system, hence detecting attempts at double enrollment using an alias.

As biometric systems evolve new methods are found for gathering and processing biometric information. The reminder of this paper is organised as follows: Section II introduces the field of biometric in general and details the difference between uni and multi-biometrics. In Section III

we make a comprehensive survey of multi-biometric systems from the fusion perspective. We focus on recent work (2011-2015), but in some cases also mention research prior to this point if particularly relevant to the discussion or because it remains a core example of specific approach. Section IV discusses some of the security issues related to multi-biometrics, like template security, biometric spoofing (bypassing biometric sensors), biometric cryptosystems, key derivation and PKI. Section V briefly discusses some emerging trends and open problems in the multi-biometric field. Section VI represents our main contribution in a form of a list to be used when designing a multi-biometric system. This list helps determine the need of a multi-biometric system, which types of sensors to be used, sensor architecture, fusion and processing type etc. This study provides extensive classifications of recent biometric systems based on features used and fusion method. This focus on fusion method should provide and reference for and help designers, especially those of embedded devices capable of sensing biometric data. The discussion on security should assist the secure integration of biometrics in currently emerging computing paradigms, such as Internet-of-Things.

II. BASIC BACKGROUND

When considering biometrics as a way for identifying and authentication human users we generally use two classifications [9]:

- **Physical biometrics.** These are features inherent to the physical body of a person that could be considered unique, e.g, face, fingerprint, hand biometrics (hand geometry, palmprint, hand vein) and ocular biometrics (iris, retina, periocular).
- **Behavioural biometrics.** These are features of a person's actions that could uniquely distinguish a person, e.g. written signatures, keystroke patterns, gait and voice. Some biometrics could be considered a mixture of physical and behavioural biometrics, e.g. as we speak our voice has unique frequency characteristics, which is physical, while the way we speak could be behavioural.

A basic biometric system is shown in Figure 1. The first process is **enrollment**, which acquires the biometric data using a sensor, extracts features and store it in a biometric template. Usually enrollment takes place once, but in special cases, it can be specifically updated, if that biometric trait changed significantly. In subsequent day to day usage, a user presents his biometric to the sensor and feature extraction is performed. The matcher module will compare the sample with the stored template and make a decision of accept or reject. The biometric features variations of the same biometric trait from the same user is called **intra-class variation**, as opposed to **inter-class** variation which relates to different users. A useful biometric template has small intra-class variation and large inter-class variations [10]. When two biometric samples for the same trait are matched they are given a match score, which must exceed a certain threshold

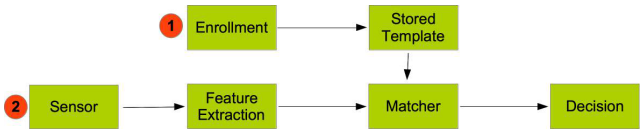

FIGURE 1. Biometric process depicted by [11] and modified by us.

to be considered authentic. Depending on the origin of the samples this score can be: genuine score if the biometric samples are from the same user or impostor score otherwise.

A biometric system can function in verification or identification mode. Verification mode confirms the user's identity, by comparing the input with a stored template of that user. Identification mode tries to find out who user is by comparing the input sample against the entire template database.

Given the variability involved with the capture of any biometric the matching function always allows for some threshold of difference between the input and the stored template. Given that it is not feasible to consistently achieve a 100% match and that there is an error threshold the system could make an incorrect decision. As such, regardless of the type of biometric system used, single or multiple, the systems performance is usually evaluated in terms of accepted quality metrics. These metrics are well known [10] so we mention them only briefly: False Match Rate (FMR), False Acceptance Rate (FAR), False Reject Rate (FRR), Genuine Acceptance Rate (GAR), Equal Error Rate (EER), Failure To Enroll (FTE), Failure to Capure (FTC), system matching and enrollment speed and upper bound. The last metric calculates the maximum number of patterns the biometric system is able to recognise. The difference between FMR and FAR is FMR doesn't include previously rejected samples due to image quality or FTC, and this is the reason some authors agree that FMR is a better metric. Jain *et al.* [12] determine the upper bound to be dependent on:

- *Information limitation* based on a specific biometric trait the number of distinguishable patterns differ, for example the number of different palmprint patterns are lower than fingerprint patterns.
- *Representation limitation* the algorithms used in the biometric features extraction limit the information stored by the system, which can't store all the discriminatory information into the template.
- *Invariance limitation* the storing template should be capable to model inter-class variations, but in practice it's not so easy. Trying to authenticate a user who presents a slightly different face pose might prove difficult, if the stored template is made on a straight face pose.

A biometric system which makes a decision based on evidence from multiple biometric sources is called a multi-biometric system. Multi-biometric systems can be based on multiple traits or multiple representations of the same trait. Under the first approach, *multi-modal* systems use multiple different biometric traits to make a decision. For the latter

approach, *multi-sensor* systems use at least two different sensors for acquiring the same biometric trait, *multi-algorithm* systems use different algorithms for processing the same biometric sample, *multi-instance* systems use at least two instances from the same biometric source for the same person, and *multi-sample* systems uses multiple samples of the same biometric trait to account for variations.

TABLE 1. Problems with single biometric systems.

Name	Description
Noise in sensed data	Data is compromised at enrollment due to acquisition environment or the user's biometric feature is altered or non existent.
Non-universality	Data from a certain biometric trait can't be acquired because of clinical and other conditions like: iris scan failure due to long eyelashes, drooping eyelids, or fingerprints worn down due to manual labour.
Upper bound on identification accuracy	Any biometric system has a maximum number of distinguishable patterns it can recognise, which becomes a problem for large databases.
Spoof attacks	Some physical and behavioural traits are vulnerable to spoof attacks, such as voice, signatures and even fingerprints. Successful presentation of a spoofed biometric would obviously lead to authentication compromise.

Multi-biometric systems are increasingly considered more suitable because of weaknesses of single biometric systems [13] with regards to reliability, e.g. having a back-up biometric in case one fails, security, e.g. having more than one way to verify a user in case one approach is compromised, and upper bound, e.g. maintaining unique identification for very large populations, as depicted in Table 1. Multi-biometric systems offer the following advantages [10]:

- *Improved matching accuracy* - because multiple sources of evidence are used the matching accuracy of a multi-biometric system is better then traditional uni-modal system, FAR and FRR of a multi-biometric system are reduced.
- *Universality and large population coverage* - unlike uni-modal systems, where a certain biometric feature might not be available, multi-biometric systems allow users to use another biometric trait. Using multiple evidences a multi-biometric system pertains to large populations, because it not longer has the upper bound of a uni-modal system.
- *Resistance to spoofing* - it's considered unrealistic that an attacker will be able to produce more then two adequate spoofed biometrics. Further more a multi-biometric system can randomly request certain biometric traits for every authentication or identification. This assumption was proven to be false by later research, which we will detail in the biometric security section IV.
- *Reduced noisy data* - uni-modal systems can become unusable due to the noisy environment of the sample. If a user has to use voice identification in a noisy environment, authentication might not be possible, because the sample data is ''corrupted'' by noise. A multi-biometric system can adapt itself to environment conditions and request another biometric evidence that is not affected by that particular environmental problem.
- *Continuous monitoring* - multi-biometric systems offer better continuous monitoring than one single form can, which might be circumvented or obstructed. Face recognition can be hindered by sun glasses, hood and gazing down, but faking gait at the same time becomes increasingly difficult.
- *Fault tolerance* - multi-biometric systems continue to work when a single biometric trait is compromised due to theft, sensor malfunction or deliberate user manipulation.

Multi-biometric systems do, however, add some complexity in terms of how the different sample input and stored templates will be used to reach one single verification or identification decision. There is numerous approaches to achieving this fusion of different biometric features, and this is the core topic discussed in Section III. Multi-biometric systems also presents some security challenges discussed in Section IV.

III. MULTI-BIOMETRIC FUSION

Data fusion is the integration of multiple information and knowledge about the same object in order to obtain a more accurate description. The goal of data fusion is to improve data quality of that object, which can be achieved if the information is stored separately [14], obtaining synergy. Synergy can be defined as: the representation of a whole is better then the representation of the individual components. Data fusion should have the following results [15]:

- **Gain in representation:** the data obtained after the fusion process should contain better abstract level or granularity than the same data presented separately;
- **Gain in certainty:** considering U a set of data to fuse and $p(U)$ the data probability before fusion, then $p(U^{'}) > p(U)$;
- **Gain in accuracy:** data is more accurate after the fusion process and noise and errors are less then the individual representation;
- **Gain in completeness:** the data represented by fusion is complete or less redundant and greater accuracy is observed.

Multi-biometrics is classified by fusion type. Sanderson and Paliwal [16] defined two major fusion groups: prior to matching and after matching, as shown in Figure 2. Other experts classified biometric fusion in three levels: feature extraction level, matching score level and decision level [17]. Later it was agreed that there is a need to classify biometric fusion based on when the matching takes place, because once the matching is done the information available is reduced significantly [18]. Fusion before matching fuses all the biometric samples, then compares them with the

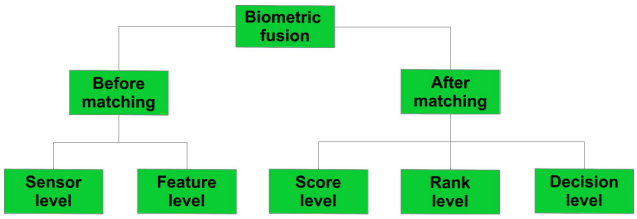

FIGURE 2. Biometric fusion levels, as depicted by [18].

stored template. The other type of fusion means that every sample is matched against it's template and only the decisions are compared. The second type of fusion reduces the data compared, because only the top ranking results are compared with the rest of the biometric traits. The next subsection details the various types of fusion. Every subsection contains a summarising table of the schemes mentioned in text. The tables contain information about the scheme, methods used, the results, metrics, databases used, and biometric type. The scope of these tables is to offer a picture of the methods/algorithm used by the schemes detailed in text.

A. SENSOR LEVEL FUSION

This type of fusion combines biometric traits from multiple sensors prior to feature extraction. In image processing this type of fusion is called pixel level or phase level for audio / video. Sensor level fusion is useful in multi-sample systems. A sensor can capture two or more samples of the same trait and create a more accurate description for that trait. Most modern systems include pixel level fusion, but they don't specifically mention it. Because of this fact we will only detail schemes where pixel level fusion is evident. Table 2 represents a summary of the papers depicted in this section.

A very good example of sensor level fusion is used in a process called mosaicking. Fingerprinting mosaicking was proposed by various authors [19]–[24]. This type of fusion is embedded in many fingerprint systems because it creates a more accurate fingerprint image by combining information captured using two or more impressions from the same fingerprint. Enrolling a fingerprint image poses some difficulties. A fingerprint image has distortions caused by the fingerprint being pressed on the sensor which affects the data quality.

Another problem is the presence of dirt on the sensor or cuts and bruises on the fingerprint, which can cause noise in the image. For these reasons multiple images are mandatory when registering a fingerprint. Fingerprint mosaicking can fix this issues by using a modified version of the Iterative Closest Point (ICP) [20] algorithm, which reconstructs 2D or 3D scanned surfaces, by adding information from multiple scans. This way only one single ''complete'' image is retained. Mosaicking is very useful in the new generation touchless fingerprint systems. Some have explored acquiring 3-D touchless fingerprint scan by incorporating images from multiple cameras [25]. Fatehpuria *et al.* [35] used a 3D touchless setting with multiple cameras and SLI (Structured Light illumination) to obtain the 3D fingerprint shape and 2D fingerprint images.

These technologies, using multiple cameras, are very expensive, so Choi *et al.* [26] proposed a system using a single camera and two mirrors, which reflect the finger side views. This system captures three images and creates a composite mosaicking image using the thin plate spline model, depicted by [27].

Ghouti and Bahjat [28] proposed a new iris fusion algorithm. The system uses two iris images fused into a single normalised iris image. The fusion is done using two methods known as: wavelet-based iris texture retrieval and Generalised Gaussian Distribution (GGD). The system constructs a normalised iris image based on image fusion, then performs iris features extraction and matching. This system gains an overall 5.73% better accuracy for FAR.

Kusuma and Chua [29] proposed a multi-sample 2D and 3D facial recognition system by image recombination using the Principal Component Analysis (PCA) method. Two recombined images are obtained which can be fused together at pixel fusion. This system can function based solely on pixel fusion or combined in hybrid mode, using the two recombined images and applying score level fusion. The best recognition results are obtained in the hybrid mode.

Jaisakthi and Aravindan [30] proposed two different methods for face recognition: one based on data fusion and the other based on sensor fusion. The presented methods produced an accuracy of 99.75% for data fusion and 99.8% for sensor fusion, and a FRR of 0%. Usually sensor level fusion is used for the same trait, but the following are examples of sensor level fusion for different traits:

- Jing *et al.* [31] depicts a multi-modal biometric system for combining face images and palmprint. The Gabor transform is used on the images prior to pixel level fusion. The scheme is very efficient for the small sample scenario.
- Wang *et al.* [32] proposed a system for sensor level fusion for palmprint and palm vein. A near IR camera is used to capture both palmprint and vein images simultaneously. The images have to go through a process called image registration, which creates an optimal image transformation, then they are fused together at pixel level.
- Froba *et al.* [33] proposed a person recognition system based on sensor fusion. The authors describe an audio-visual recognition system based on voice, lip motion and still image. In essence the system is multi-modal, but it uses sensor level fusion for processing. A person is video-audio recorded speaking a code word, then the information from independent sensors is processed, classified, and sensor fusion is made which aids in decision making. The authors argument that using multiple sensors to measure biometric cues independently leads to fewer errors and better classification, than single sensor.

TABLE 2. Sensor level fusion summary.

Paper	Algorithm/system	Result	Dataset	Biometrics
[19]	Rolled fingerprint images from live-scan	The extraction algorithm is evaluated in terms of: Image Area, Quality of minutia extracted.	12 fingerprints were acquired by rolling the fingerprint over the sensor	Fingerprint
[20]	ICP	Input image extracted 22 minutiae, Composite image extracted 30 minutiae.	300x300 fingerprint images from 160 different subjects.	Fingerprint
[21]	Rolled fingerprint images from live-scan	Area is 96% and 80 minutiae extracted. Other methods: minimum, naive, foreground extracted 203, 55, 143 minutiae respectively.	50 pre-captured rolled fingerprints	Fingerprint
[22]	Fingerprint images captured sequentially by rolling and sliding	Mosaicking success rate 88% and 42 minutiae extracted, compared to 143 minutiae for rolled method (this method generates false minutiae).	100 different fingers using 4 different enrollment schemes. The ACCO 1394 sensor was used, image size is 600x600, 500 dpi	Fingerprint
[23]	TPS	Improves alignment of minutiae points between template and sample. Matching score improved from 0.300 (affine model) to 0.408 (average deformation).	1600 finger images of 50 different users, using Identix sensor (256x255, 380 dpi), collected over a period of 2 weeks	Fingerprint
[24]	Swipe fingerprint sensor, used in smartphones, by performing measuring the overlap between sequenced fingerprint images using the MAE algorithm	Scheme is suitable for real time applications, and can capture 40 high quality frames per second.	FPC1031B sensor, 152x32 pixels. Tests were performed on 6 captured fingerprints.	Fingerprint
[25]	Unwrapping algorithm	This algorithm makes the scanned fingerprints compatible with ink fingerprints	38 different fingers consisting of ink rolled fingerprints and touchless print, using new line sensor 1000 ppi.	Fingerprint
[27]	Touchless fingerprint system using a camera and 2 mirrors	29% more true minutiae and 28% larger quality	112 different fingers from different subjects, capturing front, left and right view images.	Fingerprint
[28]	2D TSP	The average number of minutiae increased from 36 to 45 after mosaicing. GAR 97% for EER 0.97, compared with EER 4.02 and EER of 1.54 for individual matchers.	FVC2002DB1 database which has eight fingerprint impressions from 110 people	Fingerprint
[29]	Daugman Algorithm for iris verification, wavelet-based iris and Generalised Gaussian Distribution (GGD) image fusion	5.73% overall recognition improvement.	MIRLIN database, for 400 people	Iris
[30]	PCA (2D and 3D) face samples	EER of 6.3% for NTU-CSP dataset and 7.1% based on Bosphorus dataset	NTU-CSP and Bosphorus databases	Face
[31]	Different feature extraction using PCA, LM, ZM, GFD	99.75% accuracy for data fusion and 99.8% for sensor fusion method, and a FRR of 0%.	300 images from ORL database and 200 non-faces images	Face
[32]	Gabor transform on face and palmprint image and combination at pixel level	Multi-modal recognition rate is 99.81% as opposed to 67.32% for face and 60.88% for palmprint.	AR and FERET face database and HK-PolyU Palmprint database	Face and palmprint
[33]	Color palmprint and vein image are fused, and Laplacianpalm method is used for palm representation	GAR of 99.7% for fused images, compared to GAR of 99.1% and 99.0% for palm vein and palmprint, respectively.	120 subjects having three: palmprint images, palm-vein images and fused images, sensor resolution of 768x576 pixel	Palmprint and palm vein
[34]	Synergetic computer method for face recognition, optical flow analysis for mimic processing and text dependent approach for speech recognition	EER 2.4% for three sensors, compare to 5.8%, 5.9%, 9.5% for audio, flow and face respectively.	170 persons with a total of 6315 samples, each consisting of an audio recording and a video recording of a person pronouncing a code word.	Voice, lip motion and still image
[35]	PCA fusion and DWT image fusion	Different FAR and FRR based on fusion types and classifiers. The system achieves better performance then individual biometrics.	Fingerprint and FKP Hong Kong PolyU database	FKP and fingerprint

Table finished

- Meraoumia *et al.* [34] proposed a fingerprint and Finger Knuckle Print (FKP) multi-modal biometric system which can perform fusion at both image level and score level. The authors use a matching module based on correlation filtering using MACE and UMACE filtering. Fusion is performed at image fusion and score level fusion. The authors experimented with PCA and DWT image level fusion and five score fusion techniques of which MAX rule offered the best results.

B. FEATURE LEVEL FUSION

Feature level fusion consolidates information from two feature sets, extracted from the same individual, 1.

$$X = x_1, x_2, \ldots, x_m; \quad Y = y_1, y_2, \ldots, y_m \tag{1}$$

Feature level fusion has to deal with large dimensionality and variance of feature sets, especially when different traits are used. In order to reach common ground and create a concatenated feature vector algorithms like: normalization, transformation or reduction [36] are used. Feature level creates correlations between features extracted with different algorithms, managing to create a set of most important features which improves recognition accuracy [37]. Sometimes feature level fusion needs a lot of training data to work, that's why the amount of training data needed might be a metric of system performance. If the feature sets come from the same biometric trait, they can be used for template update or improvement. Rattani *et al.* [38] made a comprehensive survey on methods of template update, and categorise them into supervised and semi-supervised methods. Next we give examples of papers using feature level fusion. Some of the papers are summarised in Table 3, we only included papers with relevant data.

Finger Knuckle Print (FKP) is used extensively in biometric recognition. Guru *et al.* [39] proposed a system of multi-instance level fusion using Zernike Moments (ZM) to identify the finger knuckle instances. ZM are polynomial functions used extensively in image processing, because they can represent an image without no redundancy or information overlap. ZM are dependant on image scaling and rotation and used to extract shape characteristics of an object. This method is used extensively in the medical field, like classifying benign and malignant breast tumours [40], [41]. The same principle applies to biometrics, where the ZM from the knuckle samples are extracted and stored in the database. The experiments prove that the proposed feature extraction methodology, ZM, provides better accuracy then classic methods like: PCA [42], LPP [43], (2D)2PCA [44], (2D)2LPP [45]. Long *et al.* [46] use ZM to extract fingerprint and face features and RBF neural networks (RBFNN) for classification. The system is better then the uni-modal ones and the ZM feature extraction is very reliable.

Another multi-algorithm FKP verification scheme is proposed by [51], which uses four algorithms, LG (Log-Gabour) filters [70], LPQ (Local Phase Quantisation) [71], PCA, and LPP to extract FKP features. For feature normalisation four different methods were used: Min-Max, Z-Score, Median and Median Absolute Deviation (MAD), Tangent-Estimator. The experiments showed that fusing two algorithms produced improved performance than a single algorithm, but fusing three algorithms doesn't improve significantly than two algorithm fusion. In the case of a two or three algorithm combination the single most important factor is the chosen fusion method. Huang *et al.* [62] proposed a multimodal biometric authentication system based on palmprint and FKP. This scheme uses Monogenic Binary Coding (MBC) to extract palmprint features.

MBC was proposed by [72] for face recognition and consists of decomposing an image into three components: amplitude, orientation and phase, encoded using monogenic variation at local region and pixel level. For Knuckle feature extraction Bhaskar and Veluchamy used two separate algorithms: Finite Ridgelet Transform (FRIT) and Scale Invariant Feature Transform - (SIFT), existing methodologies for extracting knuckle features. The scheme performs better than their uni-modal counterparts and some multibiometric modalities using the same biometric traits.

Some authors solve the problem of large feature vector dimensionality by applying a Particle Swarm Optimisation (**PSO**) algorithm on the feature vectors. Examples are: [73] and [74] applied on face and palmprints, [75] for irises, palmprints, and fingerprints, and [48] a multi-sensor system for face recognition, using visible and IR images. The PSO algorithm is described in Section V.

Multi-modal systems including **face** recognition. Kim *et al.* [76] proposed an acquisition system using time-of-flight (ToF) depth camera and near infra red (NIR) camera simultaneously to capture touchless information about the face and hand vein. Huang *et al.* [57] proposed a multimodal face and hand geometry recognition system, which uses DCT to extract the face features and distance identification between the hand geometry features, using SVM as a classifier. This demonstrates that SVM is a good choice as a classifier.

Face and ear multi-modal systems are also considered, mostly because the ear is one of the most unchangeable feature of the human traits. If the face is affected by ageing, the human ear is not. Yang and Zhang [59] developed a robust recognition system using PCA to extract the features and Sparse Representation (SR) method for feature level fusion. Experiments show that the proposed scheme outperforms their uni-modal counterparts and offers the same performance as the uni-modal systems when one of the traits sample is corrupted. Islam *et al.* [77] propose a recognition system based on extraction of local 3D features called (L3DF) for ear and frontal face images. This system works both at feature and score level and achieves a recognition accuracy of 99.0% and 99.4% with a FAR of 0.001.

Multi-modal authentication systems for **face and palmprint** were proposed. AlMahafzah *et al.* [47] also used K-medoids clustering and isomorphic graph for the face and palmprint. The algorithm extracts SIFT feature points [78]

TABLE 3. Feature level fusion summary.

Paper	Algorithm/system	Result	Dataset	Biometrics
[39]	Zernike moments using different space reduction algorithms: PCA, LPP, $(2D)^2PCA$, $(2D)^2LPP$	Identification accuracy: 86.76% (PCA), 88% (LPP), 88.24% $(2D)^2(PCA)$, 88.85% $(2D)^2LPP$	Hong Kong PolyU FKP database collected from 165 users	Finger Knuckle Print
[51]	K-medoids clustering algorithm and isomorphic graph	98.75% recognition accuracy with 0% FAR for IIT Kanpur; 99.5% recognition accuracy with 0% FAR for chimeric	Chimeric database consisting of: ORL face and palmprint database form Hong Hong PolyU; IIT Kanpur database containing 800 faces and palmprints	Face and palmprint
[52]	PSO used to select an optimal subset of features and calculate weighted coeficients. Feature fusion is performed using Weighted Euclidean distance	EER 1.15 for S2P1 protocol, EER 2.42 for S2PA protocol (S2P1 and S2PA represent a image selection protocol from the existing database)	IRVI database consisting of videos of 60 persons acquired in 2 different sessions, in an office environment	Visible and IR Face images
[53]	Own palm capture system enclosed in a black box	EER of 0.538%, 0.6141%, 0.5482% for feature fusion, sum rule score fusion, product rule score fusion, respectively.	55 users and 440 images of palm and fingerprints images, using a Sony DSCW-35 Cyber Shot camera with 72 dpi	Palm and fingerprint
[54]	Simple PCA feature extraction and PCA-LDA for processing for low resolution video surveillance systems using different classifiers: Bayesian linear and bayesian quadratic, 1-NN (nearest neighbor)	PCA: 65% accuracy for bayesian linear classifier, 60% accuracy for Bayesian quadratic classifier, 55% accuracy 1-NN classifier. PCA-LDA: 100% accuracy for all 3 classifiers	100 video sequences for 25 people, of which 19 male and 9 female	Face and gait
[46]	Zernike Moment (ZM) and Radial Basis Function (RBF) Neural Network	FAR 4.95% and FRR 1.12% for fusion, compared to face (FAR 11.52%, FRR 13.47%) and fingerprint (FAR 7.108%, FRR 7.151%)	Public domain DB4 FVC2004 fingerprint and ORL face databases	Fingerprint and face
[47]	LG, LPQ, PCA, and LPP for FKP feature extraction with four different normalization techniques: Min-Max, Z-Score, Median Absolute Derivation (MAD) Tanh-Estimator	Different scores for different extraction algorithms and tehniques	DZhang FKP database from 165 subjects	Finger Knuckle Print
[55]	Gabor texture for feature extraction	Recognition accuracy of 92% and FRR of 1.6 compared with other fusion methods which have a recognition accuracy between $[79.79, 98.82]\%$	Hong Kong PolyU palmprint database and IITK iris database of 125 users	Palmprint and iris
[56]	Eigen-face and Eigen-palm methods based on PCA for features extraction and Min-Max normalization method	GAR of 95% for fusion compared to 81.48% for palmprint and 88.88% for face.	The test images were acquired using Canon- Power Shot SX 120 IS, 10 mega pixels	Face and palmprint
[57]	Patch distribution compatible semi-supervised dimension reduction for dimension reduction	Average recognition accuracy for different test data and samples 84.99% for unseen test data and 87.41% and 88.60% for unlabeled training data.	CMU PIE, FERET, and AR face databases and USF HumanID gait database	Face and gait
[58]	Active Lines among Face Landmark Points (ALFLP) for face representation and Active Horizontal Levels (AHL) for gait.	Authors propose 6 different classifiers from which IBK yields best results: 96.3% recognition accuracy.	CASIA database	Face and gait
[59]	Gabor filter framework for features extraction, novel supervised local-preserving canonical correlation analysis method (SLPCCAM) for feature vector generation,	Average increase in accuracy of 1.14% in comparison with score level fusion.	Two database containing 640 fingerprint and finger-vein images	Finger and finger-vein
[60]	Discrete Cosine Transform (DCT) for face features extraction and SVM for classification	99.75% identification accuracy, FAR of 0.007% and FRR of 0.02%	A database of 40 subjects each having 10 hand and images	Face and hand geometry

Continued on next page

TABLE 3. *Continued.* **Feature level fusion summary.**

Paper	Algorithm/system	Result	Dataset	Biometrics
[61]	Haar wavelet-based technique for feature extraction, and Support Vector Machine (SVM) classifier for training and testing	RBF Kernel performs better with GAR 93% and FAR 0%, compared with fingerprint (GAR 87%, FAR 4%) and iris (GAR 88%, FAR 2%).	CASIA database	Iris and fingerprint
[62]	Sparse Coding Error Ratio (SCER) used to determine the weight scheme, Sparse Representation based Classification (SRC) and Robust Sparse Coding (RSC) classification	Authors develop multiple recognition methods which can provide different accuracy rates when both samples are 100% corrupted	Extended Yale B, AR face database and USTB ear database III	Face and ear
[63]	1D Log-Gabor dual iris codes is used to fuse them into a vector, Complex Gabor Jet Descriptor (CGJD) for visible and thermal face representations, and Aczel-Alsina triangular norm (AA t-norm) fusion	EER 2.89×10^{-4}. Other methods obtained an ERR between $[2.95, 13.4] \times 10^{-4}$.	CASIA-Iris-Thousand and NVIE face database	Dual iris, visible and thermal Face
[64]	Robust linear programming method to fuse the multi-biometric data	ROC curves shows improvement for the proposed method compared with the single biometrics	CASIA-Iris-Distance	Eye and face
[50]	Monogenic Binary Coding (MBC) palmprint feature extraction, inner knuckle print recognition two algorithms Ridgelet Transform and Scale Invariant Feature Transform (SIFT), SVM for classification	Recognition rate of 98.1% for (MBC-Ridgelet) and 98.5% for (MBC-SIFT)	IIT Delhi database	Palmprint and Finger Knuckle Print
[65]	Minutiae extraction is done on a preprocessed thinned image, Hough Transformation for ridge extraction	FAR 1.2%, FRR 1.6%, Accuracy 96.66%	FVC2004 database	Fingerprint minutia and ridge
[66]	Intel RealSense 3D camera used for contactless hand geometry feature extraction	EER 2.83%, FRR 9.43% (for FAR 0.5%) FRR 4.72% (for FAR 1%)	10 instances of hand scans of 100 subjects, using Intel RealSense camera	Contactless hand geometry
[67]	SurfaceCode 3-D palm-print representation, CompCode for 2-D palm-print representation, includes pose correction	EER of 0.72% for 2D+3D palmprint EER of 0.71% for 2D+3D palmprint + hand geometry Dynamic fusion 0.28%	PolyU Hand database of 114 subjects, each subject presenting 10 different poses (1140 total images).	Contactless hand geometry
[68]	Non-stationary feature fusion, a matrix structure constructed from features traits	Recognition accuracy of 99.7% of ORL DB and 97% for FERET DB	ORL and FERET Hong Kong PolyU databases	Face and palmprint
[69].	Viola and Jones method for face extraction, background subtraction for silhouette	Recognition rate of 97.4% for fusion, compared with 97.7% for face and 89.25% for gait.	27 persons database	Face and gait
[70]	The entire palm is considered a Region of Interest (ROI) which allows sufficient features to be extracted	EER 0.16% for CASIA and 0.73% Lab database	CASIA Palm vein Image Database and Lab database consisting of images of right and left hands of 105 users, using ulti-spectral Camera (AD-080GE), resolution 1024x768 and 940 nm active infrared illumination	Palm-vein
[71]	Uses four levels of fusion: multi-algorithm, data fusion, feature fusion and score fusion	Accuracy of 100% and ERR of 1.31%.	ITK database consisting of 4120 images from 1030 subjects	Palm-dorsa vein pattern
				Table finished

and divides them into clusters using the PAM algorithm [79], and an isomorphic graph is created. The two resulting graphs (one for face and one for palmprint) are later fused into one graph and then matching is made. Mohi-ud Din *et al.* [53] use PCA for both feature extraction and Min Max method for score normalisation. The experimental results showed a GAR of 95% for the multi-modal system, above the uni-modal counter parts, where the GAR is 81.48% for the palmprint

and 88.88% for the face. Svoboda *et al.* [66] defined a new approach using a matrix interleaved concatenation method. The face and palmprint features are extracted using the DCT method, but they are concatenated in an interleaved matrix capable of estimating the parameters of the concatenation features and illustrate their statistical distribution. The main advantage for this method is that it allows usage of large data points, as opposed to "classic" methods. The authors compared their method with 5 other schemes, 2 at feature level, one at score, decision and rank level, and showed that the proposed system provides a 99.7% recognition accuracy, better then other methods.

Other systems consisting of **hand recognition** (palm, fingerprint, veins etc) are detailed now. A dual recognition system using iris and fingerprint is shown in [58]. The Haar wavelet-based technique is used to extract both feature vectors, the Mahalanobis distance method is used to fuse the features, and the SVM method is used for system training. The system has a very low FRR, less then 7%, compared to 8 to 10% for the other existing approaches. Iris scans and fingerprints are used on a large scale by the India UID project. The same author [80] proposed an iris and fingerprint recognition system which is both multi-modal and multi-algorithm. It uses Haar wavelet and block sum techniques to extract iris features and minutiae and wavelet transforms for fingerprints. The four feature vectors are fused at feature level, which offers better accuracy then their uni-modal counterparts.

A palm and fingerprint multi-modal system at both feature level and score level is proposed by [49]. Specific to this system is the acquisition system, consisting of a black box using a Sony DSC W-35 Cyber Shot camera having resolution of 72 dpi for contactless palmprint acquisition. The experiments were run on a database of 440 palm and fingerprints of 55 people. The conclusion is that feature level fusion performs better then score level fusion.

A palmprint and iris multimodal feature level system is proposed in [52]. The feature vectors are obtained by extracting Gabor texture from preprocessed palmprint and iris images, using wavelet-based fusion techniques to obtain a common feature vector. Matching is done using the KNN classifier. This system is tested on a database of 125 users and has a recognition accuracy of 99.2% with FRR of 1.6%.

Miao *et al.* [64] proposed a contactless multi-sensor system for hand geometry recognition using an Intel RealSense 3D camera. This camera is the first mass produced 3D camera. The system captures the hand image from the camera, and uses foreground segmentation to identify the hand silhouette and contour. Once the hand contour has been defined the fingertips and valleys are detected and the wrist line is computed. After the necessary extractions two features vectors are created: $X2D$ containing: finger length, width, and wrist valley distances and $Y3D$ containing finger widths calculated by traversing the overall hand surface and median axis to surface distances. The proposed system had the lowest error FAR (1.61%), FRR (1.61%), EER (1.61%) then other hand recognition systems such as in [65] and [81]–[83].

Wang *et al.* [63] proposed a system for fusing fingerprint minutia and ridges at feature level. The scheme obtains a higher accuracy then other minutia or ridge systems. The fingerprint recognition system uses the FVC2004 database and consists of 5 steps: the gray scale fingerprint image is binarised, the image is thinned and the ridges thickness is reduced to 1 pixel, minutia extraction is performed on the thinned image resulting in a feature vector called M, ridge extraction is performed using Hough Transformation resulting in a feature vector called R. According to the authors the proposed system has an accuracy level of 96.66%, which is better then 93.5% for minutiae based or 94.6% for ridge based systems.

Veins, the blood vessels under the skin, can be used for identification because they are unique to a person including twins, they don't change with age, and are harder to forge. Bokade and Sapkal [56] presented a finger and finger-vein system. The feature extraction system uses the Gabor filter and Supervised Local-Preserving Canonical Correlation Analysis (SLPCCAM) for feature fusion. This fusion rate achieves an FAR of 1.35% and FRR of 0%. Ahmad *et al.* [68] proposed a contactless multi-sample palm-vein recognition which solved the low resolution images with a bad contrast problem encountered in most similar systems. To address this issue the entire palm is used when features are extracted. The experiments show that the recognition performance is superior for posture changes compared to other systems.

Human identification at a distance has become an area of interest, especially for automatic access control systems in buildings. These systems use facial recognition, but due to low resolution cameras or improper lighting conditions because of the area where the camera is positioned, such as hallways, the recognition is far from accurate. Research showed that combining gait with face recognition can improve the recognition accuracy. Various systems are presented: a system using PCA-LDA algorithms for feature extraction which works both at score level and feature level fusion [50], a recognition system with a new dimension reduction algorithm called PDC-SSDR [54], a feature level system using Active Lines among Face Landmark Points (ALFLP) for face feature extraction and Active Horizontal Levels (AHL) for gait features representation [55], a gait feature coupling used in conjunction with low resolution face images [84].

Another face and gait distance recognition was proposed by Xing *et al.* [85]. This scheme differs from traditional face and gait recognition by combining the features without normalisation using coupled projections. The authors prove by experiments that their system achieves a recognition rate as high as 98.71% in the context of access control systems such as the one proposed by [67], who implemented a practical one camera automatic access control system based on frontal face and gait recognition, with a recognition rate of 97.4%.

Gawande *et al.* [61] proposed a novel approach in multi-biometrics, using robust linear programming (RLP), useful in identification at a distance. This system obtains good results

in noisy environments and with small training data. RLP uses uncertain constraints and was modelled in the context of biometrics by concatenating all the heterogeneous features from different biometric modalities $A = [A^1, A^2, .., A^M] \in R^{nxD}$, where M represents the biometric modalities, (n) training samples, (D) features. Weight variables are introduced for each biometric modality and represent the contribution degree for the fusion. The higher the weight the more relevant that biometric feature is. The proposed method was tested on the CASIA-Iris-Distance database containing two eye and one partial frontal face region pictures. The method produces high accuracy for noisy environments, thus should be considered for further research in recognition from a distance where noise is a significant factor.

C. SCORE LEVEL FUSION

According to researchers score level fusion is more effective and produces better matching then other fusion methods [10]. The first step in score level fusion is score normalisation, because features extracted from different modalities have different domains. Lets assume that biometric modality 1 produces a feature vector $V_1 \in [1, 100]$ and biometric modality two $V_2 \in [1, 2000]$. In order to fuse the vectors a common domain must be defined, so score normalisation techniques are used. The most common are minimum maximum (MM), hyperbolic tangent (HT), and z-score (ZS). In the literature authors present multiple techniques [86], but one of the most promising ones is Likelihood Ratios (LR), which can obtain the highest GAR for a predetermined FAR [87], [88].

The last step in score fusion is to fuse the two normalised vectors. This operation is done either by classification or by combination. Classification divides the result into impostor and genuine and has the disadvantage of needing a large amount and high quality data. Combination fuses scores generated by different comparators and generates a single decision. Next we review some of the proposed schemes, summarised in Table 4.

Jain *et al.* showed that the best results are obtained by applying MM, HT and ZS normalisation schemes and adding the scores [89]. Indovina *et al.* [90] made an assessment of COTS software for fingerprint and face recognition using different algorithms for score level fusion. The tests were preformed on a database with 972 subjects, and showed that COTS multi-modal fingerprint and face recognition achieve better results then their uni-modal counterparts. MM and Simple Sum algorithms work best on large populations.

Dempster-Shafer theory (D-ST) supports data variation by introducing uncertainty in fusion [117], [118]. D-ST is used as a generalization of probability theory and assigns degrees of belief to hypothesis as a whole as opposed to single events. Different multi-biometric systems have been proposed based on this theory such as a multi-fingerprint system [119], multi-modal face recognition using 3D modality containing face ridge lines, and 2D modality containing feature facial points [120], face and voice [93], face and ear [91], face recognition based score level fusion of global and local (part of the face) features [92], signature and hand shape [121]. Vishi and Yayilgan [110] used D-ST on a biosecure DS2 database containing 17 data channels like three face, six optical and six thermal fingerprint, and two irises. The framework incorporated a quality fusion which has better performance then other systems.

There are some multi-biometric verification and authentication schemes using **fuzzy logic**, a mathematical approach based on degrees of truth. Conti *et al.* [122] proposed the concept of fuzzy fusion using a multi-modal fingerprint authentication system comprised of two parallel mono-modal fingerprint systems and a fusion module.The system is very scalable and additional mono-modal fingerprint systems can be added. The authentication system, named AFAS, contains two submodules, AFAS1 and AFAS2, which will generate matching scores in the independent fingerprint authentication systems. AFAS1 uses the index fingerprint for authentication and AFAS2 the middle fingerprint. The fuzzy vault containing 16 fuzzy rules will perform fusion at score level or decision level. The system has a better recognition then the mono-modal one, and the score level fusion is better then the decision level. Fakhar *et al.* [123] described a multimodal biometric system using fuzzy fusion on face and iris. This system used the output of each matching system (the face and the iris) and transforms it into a fuzzy set of rules. The fuzzy fusion estimates the reliability of the data supplied by the individuals matchers and performs score level fusion. The experiments done of a multimodal database containing 108 subjects show better accuracy then the respective unimodal systems and existing score level fusion schemes. The authors extended their work by proposing another multibiometric system based on fuzzy fusion at score level, with Choquet integral [111]. The Choquet integral is applied in decision theory to measure the utility of an uncertain event. The values of each biometric matcher are represented in a fuzzy set using a score matrix. A score equal to 0 makes the user an impostor and a score equal to 1 shows a genuine user. Then the fuzzy densities are calculated and used to compute the Choquet integral. This method was tested on a database containing two face and fingerprint scores of 517 subjects, and showed improved accuracy compared to the individual systems.

Perez *et al.* [124], proposed a multi-biometric recognition system using **Local Phase Array (LPA)**, which was proven to be reliable for face, palmprint and knuckle recognition. Another biometric recognition system using LPA was presented in [103]. The multi-modal proposal uses the LPA score level on iris, face, palmprint and knuckle. The features are extracted from multi-scale image pyramids with 3 layers. First reference points for the image are set, then hierarchical image generation is generated by shrinking the initial image using the following formula: $I^l(n_1, n_2)$, where l is the layer number, and n_1, n_2 are $1/2^l$ of initial image sizes. Reference points are calculated for this layer image. The last step is phase feature extraction, calculated using the 2D DFT (Discrete Fourier Transform).

TABLE 4. Score level fusion summary.

Paper	Algorithm/system	Result	Dataset	Biometrics
[52]	PSO used to select an optimal subset of features and calculate weighted coefficients. NIR-KDDA/VI-KDDA For score fusion	EER 1.02 for S2P1 protocol, EER 2.07 for S2PA protocol (S2P1 and S2PA represent an image selection protocol from the existing database)	IRVI database consisting of videos of 60 persons acquired in 2 different sessions in an office environment.	Visible and IR face images
[53]	Own palm capture system enclosed in a black box	EER of 0.6141% for sum rule EER of 0.5482% for product rule	55 users and 440 images of palm and fingerprints images, using a Sony DSCW-35 Cyber Shot camera with 72 dpi	Palm and fingerprint
[54]	Simple PCA feature extraction and PCA transformed in LDA space for processing low resolution video surveillance systems and different classifiers: Bayesian linear and bayesian quadratic, 1-NN (nearest neighbor)	90% accuracy for Bayesian linear classifier 95% accuracy for Bayesian quadratic classifier 85% accuracy 1-NN classifier	100 video sequences for 25 people, of which 19 male and 9 female.	Face and gait
[71]	Uses four levels of fusion: multi-algorithm, data fusion, feature fusion and score fusion	Accuracy of 100% and ERR of 1.31%.	ITK database consisting of 4120 images from 1030 subjects	Palm-dorsa vein pattern
[96]	Gaussian Mixture Model (GMM) and Dempster-Shafer decision theory for fusion	FRR 5.55%, FAR 3.40%, EER 4.47%, recognition rate 95.53%	IIT Kanpur for 420 subjects	Face and ear
[97]	SIFT features related to independent face areas for both global and part of the face and Dempster-Shafer decision theory for fusion	98.93% recognition accuracy for ORL and 96.29% for IITK	ORL and the IITK face databases	Global and local (part of the face) features
[95]	Fusion of face and voice using Dempster-Shafer	Half Total Error Rate (HTER) varies from 0.030% to 2.056%.	Scores of XM2VTS Benchmark database	Face and voice
[100]	Palmprint features are extracted using VARiance measures (VAR) and compressed using PCA, Hidden Markov Model (HMM) for vector modeling	Rank one identification between 99.45% and 85%	PolyU 2D-3D palmprint database of 250 users	Palmprint
[101]	Phase-Correlation Function (PCF) matching algorithm	EER = 0.003% for threshold of 0.876	Hong Kong PolyU palmprint and FKP database	Palmprint and Finger Knuckle Print
[102]	Introduces the use of T-norms for combining scores from different modalities.	For FAR=0.01% the GAR varies between 99.5% and 100% for all t-norms types.	ITD and PolyU database	Palmprint, hand vein and hand geometry
[103]	Simple Average and Weighting Average fusion algorithm	EER varies between 0.0035% to 1.29% for different normalization techniques	TJU hand vein database, CASIA iris and fingerprint database	Hand vein, iris and fingerprint
[104]	RIBG (Robust Imputation Based on Group method of data handling) used for missing data	Recognition rate of 94.32% for rank 1, when the missing data is 25%	NIST multimodal database	Fingerprint and face
[105]	1D Log-Gabor feature extraction, normalized matching distance for matching, normalized Hamming distance for matching	EER of 0.222% at a threshold of 0.392.	Hong Kong PolyU palmprint and FKP database	Palmprint and FKP
[106]	DCT is used to extract face features and PSO to optimize the vector	Total error rate varies between 0.0440 and 0.0650 for different fusion methods.	Olivetti Research Laboratory face database and CASIA iris database	Face and iris
[35]	PCA fusion and DWT image fusion	Different FAR and FRR based on fusion types and classifiers. The system achieves better performance then individual biometrics.	Fingerprint and FKP Hong Kong PolyU database	FKP and fingerprint
[107]	ICA reduction technique used for feature extraction	FAR 0.02% and FRR 0.35%	500 subjects with 6 dorsal and 6 palmar veins each, using CMOS digital camera, infrared filters and LEDs	Dorsal and palmar vein
[108]	Multi-normalization based fusion	Improved FRR and FAR, results varies among the normalization methods	FVC2002 fingerprint database and ELSDSR voice database	Fingerprint and voice

Continued on next page

TABLE 4. *Continued.* **Score level fusion summary.**

Paper	Algorithm/system	Result	Dataset	Biometrics
[109]	Phase information using 2D Discrete Fourier Transform (DFT)	EER of 0.278% and computation time of 40-60 ms (extraction) and 70-90 ms (matching)	FERET face and iris database, PolyU and CASIA Palmprint database, PolyU FKP database	Iris, face, palmprint, knuckle
[110]	Uses three normalization techniques (Min-Max, Z-Score, Hyperbolic Tangent) and four score fusion Methods (Minimum Score, Maximum Score Simple Sum and User Weighting)	EER = 0.00010%, the system increases performance with 55% than unimodal counterparts	Machine Learning and Applications (MLA) fingeprint and iris database and CASIA-Iris-Lamp database	Fingerprint and iris
[111]	PIUS system. Uses ZS (Zhang-Suen) trithinning for thumb mathcing. Ear processing uses 5 features out of 9 (Helix Rim, Lobule, Triangular Fossa, Concha, and Tragus)	GAR 13.33% and FAR 3.33% for fusion, compared to face (GAR 12.66%, FAR 4) and eye (GAR 11.66%, FAR 5%)	PUIS database	Left thumb and left ear
[112]	Weight optimization scheme to determine the right weight in different noise conditions.	The overall system offers better FAR and FRR than unimodal counterparts and maintained accuracy under noise conditions.	FVC2002 fingerprint database and ELSDSR voice database	Fingerprint and voice
[113]	The system uses a quantitative measure of shared information between sequent video frames	The system is tested using different score rules, but Sin-Rule 2 yields best results with an EER ranging from 0.019% to 0.179%	132 videos, of 720x480, 30 fps	Face
[114]	Features extraction uses DWT and PCA and classification Euclidean distance. Fusion uses simple sum rule with equal weights	EER = 0.072676%, better then the best fvc2004 competitors which obtained an EER of 0.2205 and 1.9025	Lab fingerprint database for 20 subjects with 8 fingerprint and iris images, CASIA v4 iris database	Fingerprint and iris
[115]	SugenoWeber (SW) T-norm fusion	Sum rule,W-Sum rule,Yg and SW t-norms based-methods perform better for fusion than other methods	Hong Kong PolyU finger image Database v1 (for veins and shape), FVC2002 Database Db1 set A for fingerprints and PolyU FKP database	Finger vein, finger shape, FKP and fingerprint
[99]	DempsterShafer theory fusion with uncertainty	EER of almost 1%	Biosecure DS2 database	Face, fingerprint (optical and thermal)
[116]	Fusion at score level using the Choquet integral	First rank accuracy of 99.94%	NIST-Multimodal databas	Face (two scores) and fingerprint
[117]	Sign Local Gradient (SLG)	Recognition accuracy of 100% and EER of 0.01%.	CASIA and PolyU palmprint databases, and PolyU FKP database	FKP and palmprint
[118]	2D Discrete Fourier Transform (DFT)	FRR of 82.67% and FAR of 17.33%.	FRAV3D database	Face texture and depth
[119]	ACO algorithm for selection of decision threshold and fusion rule	The authors evaluate the algorithm in comparison with PSO, demonstrating that ACO is better.	IITD palmprint and iris database, XM2VTS speech and face database, and the NIST BSSR1 faces and fingerprint database	Palmprint and iris, speech and face, face and fingerprint
[120]	Transformation-based score fusion algorithm.	Accuracy 99.22% and FAR 0.71%	Extended Yale Face Database, NIST FERET databases, ELSDSR voice database	Face and voice
[121]	Order-Preserving Tree (OTP)	GAR of 99% for FAR of 0.01%	NIST-multimodal, NIST-face, NIST-fingerprint, XM2VTS	Face and fingerprint
				Table finished

Mahoor and Abdel-Mottaleb [94] performed multiple fusion scenarios on 2D and 3D palmprints using the following rules: sum-score, min-score, max-score, mul-score and weighting-score, in a multi-sensor palmprint recognition system. This system uses the PCA method for transforming the acquired 2D and 3D palmprint features into vectors and Hidden Markov Model (HMM) for feature vector representation. The experiments done on the PolyU palmprint database

consisting of 250 subjects, clearly showed that the multi-biometric system is more efficient then the uni-modal ones. The use of multiple fusion techniques yield interesting results such as: the max-score rule gives the best EER in an open set identification system and weight score performs better in a closed set identification system, with an accuracy of 99.45%.

Meraoumia *et al.* [125] proposed another multi-modal biometric system for a palmprint using 2D and 3D images. The system uses PCA to reduce the dimensionality of the feature vector. Features are extracted for each trait using multiple modalities: on the original data (ORG), on rotation invariant texture (VAR) and multi-scale wavelet decomposition (DWT). The Hidden Markov Model (HMM) is used to model the feature vectors. The system can perform fusion at both feature or score level. Tests are performed for different feature extraction and fusion types. Best results are obtained using ''2D-3D-ORG-DWT'' [125]. Derbel *et al.* [69] described a hybrid multi-modal system. First a palm-dorsa image is acquired and the vein pattern extracted. When the user is enrolling in the system two palm-dorsa images and three vein patters are extracted, which are fused at data fusion level. Feature level fusion is performed on shape and minutiae vein patterns, and finally score level fusion is performed on the matching scores.

A multimodal palmprint and FKP system described by Mezai *et al.* [95] uses **Phase-Correlation Function (PCF)**. The novelty of the system consists in using the PCF function for matching of both biometric modalities and then performing fusion at score level. Phase-correlation is applied in imaging processing for image registration using the frequency domain to estimate the offset between similar images. The system was tested on a database consisting of 156 subjects and showed fusion improves both verification and identification results.

Kisku *et al.* [96] proposed the use of **triangular norms (t-norms)** in multi-biometrics. A t-norm is a binary function which satisfies the following properties: commutativity, monotonicity, associativity and the number 1 is the identity element. The associative property of the function allows fusion to be performed in any order. The authors implemented several t-norms for their test like: Einstein product, Hamacher, Yager, Schweizer & Sklar, Frank. The proposed fusion methods are tested using palmprint, hand vein and hand geometry. The features were obtained using Gabor wavelets from the first two modalities and Independent Component Analysis (ICA) for the latter. Results show that for a FAR of 0.01% SchweizerSklar and Hamacher t-norms can achieve a GAR of 100%. Another system using t-norms for fusion is proposed by Aoyama *et al.* [109]. The system fuses evidence from finger vein, finger shape, FKP, and fingerprint taken from a single human finger. Different methods are used for feature extraction for every trait such as gabor wavelets and local binary patterns for vein feature, hybrid descriptor method for fingerprint, Fourier descriptor and PCA for finger shape, and log-Gabor filters for FKP. The system out-performs the uni-biometric counterparts and other multi-modal score level systems, using classic methods like Max, Min, Sum, Weighted Sum, etc.

Anzar and Sathidevi [112] proposed a multi-modal authentication system using finger knuckleprint and palmprint. The authors use the **Sign Local Gradient (SLG)** method to transform the Regions of Interest (ROIs) from both features in vcode and hcode. These image representations are more stable then gray-scale images and provide better feature representations, which allows for better feature extraction. The SLG transformation computes the *sign code* (*SC*) for every pixel in the image using 8 neighbouring pixels. In the end the SC will be represented as a binary number defined by the following formula:

$$SC_i = \begin{cases} 1 & \text{if } (Neigh_i > 0) \quad \text{where } Neigh_i \in [1, 2, 3 \ldots, 8] \\ 0 & \text{otherwise} \end{cases} \tag{2}$$

After the feature extraction the sum score fusion rule is used. The experiments are run on publicly available databases: CASIA and PolyU palmprint databases, and PolyU knuckleprint database. The system achieved a recognition accuracy of 100% and EER of 0.01%.

Fakhar *et al.* [116] try to improve recognition accuracy with a new order preserving probabilistic algorithm called **Order-Preserving Tree (OTP)**. Because OTP is non-parametric it doesn't need fine tuning during the training phase, making the training procedure faster and more efficient. OTP doesn't use density probability estimation, but estimates the posterior probabilities. This algorithm is applied on two public multi-biometric face and fingerprint databases. Results show that the OPT algorithm outperforms many well known score level algorithms achieving a GAR of 99% for FAR of 0.01%.

Research showed that when applying score level fusion weighting the influence of a modality in the overall matching score is desirable. This principle was applied to the next level by incorporating **AI algorithms** in determining the optimal weights to be used based on particular multi-biometric system. Such a proposal is made by Alford *et al.* [126] which introduce Genetic and Evolutionary Computation (GEC) to optimise the weights for face and periocular biometrics authentication. Eigenface method is used to extract the face features and Local Binary Patterns (LBP) for periocular. The experiments show that when the two traits are weighted evenly the recognition accuracy is 90.77% as opposed to 95.24% when GEC is applied. Meraoumia *et al.* [100] proposes a multimodal system for face and iris using PSO for both feature extraction and SVM for score level fusion.

A similar concept is proposed by Sim *et al.* [127] for iris and face recognition in non-ideal conditions such as: reflections, blurred image, wrong angles and poses. The authors propose a new algorithm for iris segmentation in off-angle scenario named DLSEFGC. DLSEFGC combines geometric calibration which is first used to minimize the pupil distortion and restore it to the circular shape and ellipse fitting to fit the

ellipse around the iris. In off-angle images the iris circular shape of the iris can't be distinguished, so additional methods need to be used. Significant iris features are extracted using a combination of Haar Wavelet and Neural Network, called NeuWave Network. This method transforms the segmented iris into wavelet coefficients. The higher the coefficient the more representative the data is, small coefficients represent noise. The weighted scores for the fusion are set after the normalised score of each individual matcher. The results show that compared with other score level fusion techniques, the proposed system achieves better FAR and FRR.

Poh and Kittler [128] proposed a unified framework with **quality measures**. Quality dependant fusion is a fairly new research direction aiming to combine quality measures in the fusion process. This will allow the system to detect and automatically assign better weights to traits that present a better quality. Such a framework must incorporate a method to detect quality measures and a special fusion mechanism which can incorporate quality measures and match scores from the modalities fused. Quality measures have several meanings in literature and ranges from the degree of accuracy of the biometric trait to quality of the specific biometric sample. The authors managed to incorporate in the proposed framework both approaches, feature-based and cluster-based, which can be created using generative or discriminative classifiers. The study concluded that a discriminative classifier is preferred because it needs to estimate less parameters, and cluster-based models should be chosen because they can implement more quality measures, which might be very important when combining multiple biometric traits where quality measures can differ from one trait to another. Fierrez-Aguilar [129], [130] proposes a quality based multi-algorithm for fingerprint verification. The method uses the average sum rule for two different matchers based on ridges and minutia. The basic approach for the use of this rule is the significant drop in matching accuracy for one of the matchers under poor image quality. Experiments have demonstrated that ridge fingerprint verification performs better using low quality fingerprint images than the minutiae approach.

Hanmandlu *et al.* [102] showed that **multi-normalisation** can be applied to achieve better score fusion results. Normally a multi-biometric system uses a single type of normalisation, which is applied to all traits. The authors proposed different normalisation techniques to be applied to each trait or even on the same trait. The system is tested on fingerprint and voice for different noise environments. With regards to the score normalisation methods, Kisku *et al.* [97] performed a mathematical and practical analysis for different normalisation techniques applied to hand vein, iris and fingerprint, and demonstrated that the theoretical and the practical results coincide.

Score level fusion under a condition of **missing data** can't be performed. Applying reduction algorithms to delete the incomplete vectors can't be used at this level, because fusion can't be performed at all. For this problem Kisku *et al.* [98] proposed a recognition scheme designed to function with missing data. The scheme uses the Robust Imputation Based Group (RIBG) method for filling in the missing data. RIBG algorithm fills in the vector with estimates by calculating a simple mean imputation. Then the initial estimates are updated using the Group Method of Data Handling (GMDH) method. The process is repeated until the missing score estimates are below a predefined threshold. The proposed scheme uses Bees Algorithm to automatically assign the best weights for the Weighted Sum method. Experiments were run on databases containing left and right index fingerprints and two face scores (obtained using different algorithms). The recognition rate is 100% when missing data is 5%, 10% or 15% and 99.61% for 20% and 25%.

We have grouped multi-biometric systems by certain algorithms used or interesting features. In what follows we will group them by traits. We'll start with schemes containing **thumbs**. Meraoumia *et al.* [105]proposed PUIS, a multi-modal left thumb and left ear biometric system. The main system characteristics are the preprocessing steps for enhancing the thumb image acquisition, before feature extraction. A Gaussian smoothing function is applied to the thumb image for enhancement and ZS (Zhang-Suen) thinning algorithm, which proved to yield the best results. Ear processing uses 5 out of 9 features. The system can work at score/rank level, and proved a 80% reliability, which can be increased to 100% if the additional 4 ear features are included.

Xu *et al.* [131] proposed a new method of multi-modal biometrics, by combining the left and right palmprint at score level. Three different matching scores are fused: the left plamprint, right palmprint and a cross matching of a sample left palmprint, and a stored right palmprint. The method demonstrated that there is a correlation between the left palmprint and right palmprint of the same subject, which can be used as a match score, and for better matching accuracy. It's proven by testing that left and right palmprint can be cross-matched for better identity identification.

Anzar and Sathidevi [108] proposed a **fingerprint and iris** system using discrete wavelet transformation (DWT), which generates 4 fingerprint subsamples, and PCA (Principal Techniques Analysis) for feature extraction. The sample feature vector is matched with the template database using Euclidean Distance (ED). The iris matching uses the same algorithms for feature extraction and matching. The fusion of these two modules is done at score level using the sum of score technique. The experiments were conducted on a database of 20 subjects and prove that the proposed method has a GAR of 98% as opposed to 58% for a uni-modal fingerprint and 75% for a uni-modal iris. Also, the EER is as low as 0.35 for multi-modal system, compared to 0.40 and 0.35 for uni-modal fingerprint and iris respectively.

Another fingerprint and iris authentication system was proposed by Tran *et al.* [104], combining multiple techniques: three score normalisation (the most common ones: MM, HT, and ZS) and four score fusion techniques (Minimum Score, Maximum Score, Simple Sum, and User Weighting). The experiments were conducted on two separate databases with

different image quality. Four scenarios were proposed by the authors: Best fingerprint - best iris, best fingerprint - worst iris, worst fingerprint - best iris, worst fingerprint - worst iris. As expected the best results were obtained by the first scenario utilising the best of the databases, and the worst result by the last scenario, which uses the worst databases.

Schemes including **face** recognition are detailed next. A multi-modal distance recognition system using face and gait was proposed by Hofmann *et al.* [132] using a foreground segmentation technique based on alpha-matting. This technique improves the feature extraction for gait features and when fused with face it provides better recognition accuracy. The same features were combined by Guan *et al.* [133] who proposed this multi-modal approach to account for intra-class recognition problems in uni-modal gait recognition systems using the Random Subspace Method (RSM).

El-Alfy and BinMakhashen [60] proposed a dual iris, and visible and thermal face recognition system. 1D Log-Gabor feature level fusion was performed on two iris codes and Complex Gabor Jet Descriptor (CGJD) on visible and thermal face sample. Score level fusion was applied for the final decision.

Some multi-modal systems are susceptible to noise, especially those using one of the following traits: voice, face, signature. Liau and Isa [106] optimised a score level fusion multi-modal scheme, by introducing a weighted sum rule. The idea was to assign different weights to account for the traits with noisy data. The method was tested on a multi-modal system using fingerprint and voice. The weight factor was determined in the training/validation phase using the Leave-One-Out Cross Validation (LOOCV) technique. LOOCV divides the data samples into subsets and uses a single observation as validation data and the rest as training data.

Heenaye and Khan [107] proposed a multi-sample face recognition system useful for video surveillance. The system compares information from multiple frames from a video frames to a stored template. The approach accounts for the information diversity found in consecutive video frames, unlike traditional score fusion methods. The information between consecutive frames is captured and used to enhance fusion score performance. In practice if two video frames have similar content only the best of them will be considered for fusion. The experiments showed that the proposed frame quality method provides better performance then classic methods.

Satheesan *et al.* [113] proposed a multi-modal 3D face recognition system fusing texture and depth features. The recognition is made only by 3D facial scan from the user and no other additional information. Results show that recognition is better then each trait separately with a FRR of 82.67% and FAR of 17.33%.

Peng *et al.* [115] proposed a transformation based fusion algorithm for face and voice, based on ensemble classifier. Two separate voice and face modules generate compatible matching scores which are sent and processed by the fusion module. The scores are fused using the weighted sum score method. The algorithm has a FAR of 0.71% and might not be suitable for applications where FAR must be 0%.

Peng *et al.* [101] proposed a multi-biometric authentication based on **dorsal and palmar vein**. The authors used a CMOS digital camera using infra-red and LEDs to capture the vein images. In total 500 individuals from different ethnic groups participate in the study and 6 dorsal and palmar images were captured. Each trait is represented using the ICA method, the Min-Max normalisation scheme is applied and then sum rule fusion is applied. Experimental results clearly show that the multi-modal approach yields better recognition results with a FAR of 0.02% and FRR of 0.35% as opposed to uni-biometric counterparts.

D. RANK LEVEL FUSION

Rank level fusion is performed by ranking the potential matches between the sample and the database, and creating a list between all possible matches in the database. The first choice is the match. Ranks should offer accuracy and consistency when different matchers are used, and doesn't require normalisation like score level fusion. A rank level fusion will create a matrix $R = r_{i,j}$, where r is the rank of the I_i identity and j matcher. Then the matrix is reordered so the highest rank (from all the matchers) is assigned to the identity with lowest r.

The methods for rank consolidation to make a final decision are discussed by [134]. The ones used extensively in biometrics are highest rank, Borda count, logistic regression, and the Bayesian approach.

The highest rank method is useful for fusing results from individual matchers. The final decision or consensus ranking (CR) is obtained by sorting the identities by their highest rank obtained from individual matchers, using the following formula:

$$CR = \min_{i=1}^{m} R_i, \quad \text{where } m \text{ is the number of classifiers.} \tag{3}$$

This method uses the strength of the individual matchers, but it can cause problems when multiple matchers are used because some classifiers can have the same rankings.

Borda count is the most frequently used method for rank fusion. It sums up the assigned rank by individual matchers. The consensus rank is obtained by using the following equation:

$$CR = \sum_{i=1}^{m} R_i \quad \text{where CR is sorted in ascending order.} \tag{4}$$

This method is very easy to implement, but has a practical disadvantage: it assumes that all matchers perform equally, which can't be true in a real life scenario.

The logistic regression method, a variation of the Borda count method, introduces weights to calculate the ranks,

using the following formula:

$$CR = \sum_{i=1}^{m} W_i R_i \tag{5}$$

Logistic regression should be used when the matchers perform differently and their ''importance'' in final decision should be weighted.

The Bayesian approach introduces the concept of rank distribution modelled as the probability that the matcher will assign a true identity. CR is given by the formula:

$$CR = \prod_{i=1}^{m} P_i(Ri) \tag{6}$$

where $P_i(Ri)$ is the probability that rank R_i is assigned to a genuine identity. This method can be negatively impacted by missing data, a false identity can be mistakenly assigned a true identity. In this scenario, at the very least the same probability should be assigned to all users [135], or use another ranking method.

Kumar and Shekhar [136] studied the implication of using different combination of methods in rank level fusion for palmprint identification, using multiple palmprint representations. The authors tried to aggregate the results obtained by different matchers, using a new method called Nonlinear Weighted Ranks (NWR), which combines the ranks returned by individual ranking methods and weights and combines them. Combining different methods gives better results and is, in author's opinion, very useful for COTS devices which combine information from different sensors or combining different touchless biometric systems. Kumar *et al.* [137] proposed a hybrid system based on ear and iris. Each individual trait produces an individual match score, which is then ranked. The system performs a fused rank level fusion. The fused rank is compared with every individual score threshold and a decision is made. The optimal thresholds are estimated using PSO. The experimental results show a FAR of 0.09% and FRR of 1.5%.

Rank level fusion may be deficient with low quality data due to noisy environments. Abaza and Ross [138] presented a method to work with low quality fingerprints. They use a derivation of the Borda count method, which includes image quality. This method is similar to the logical regression method, but instead of weights image quality is used because it doesn't require a training phase like the logical regression method. Marasco *et al.* [139] tried to assess the real impact of low quality images in rank level fusion. Their experiment proved that rank level fusion is stable when the degradation of the image is not significant.

The ranking methods might pose a problem for large databases, where not all outputs are calculated and only few ranks are assigned, so Monwar and Gavrilova [140] introduced the Markov chain approach for rank level fusion. Markov chain is a stochastic series of events, where the next event depends on the present or preceding state. A Markov chain can be formally modelled by a series of graphs where the edges describe the transition from time n to $n+1$. First the ranks for each classifier corresponding to a biometric identity are created. If the classifiers are only outputting partial data, such as the first 3 ranking results, the lists can be completed by adding randomly inserted elements or by examining the partial list. The transition matrix T is created and the stationary distribution of the Markov chain is computed, using the equation:

$$\pi = \pi T, \text{ please refer to [141] for details on Marcov chains} \tag{7}$$

The identities will be ranked according to the highest score of the stationary distribution. The authors tested the fusion technique using a multi-modal biometric system using face, ear, and iris. The system obtained a EER of 1.71% compared to the following multi-biometric systems: [142] EER of 1.88% using signature and voice at match score level, [143] EER of 3.20% using palmprint (texture, line, appearance), and [144] EER of 3.39% using fingerprint (minutia and texture). Another approach to solving the problem of different matchers ranks was proposed by [145]. The multi-modal system uses three matchers (face, ear, and signature), but fusion is performed only on the identities outputted by at least two matchers.

In Table 5 we included a small summary of the most relevant rank level schemes:

E. DECISION LEVEL FUSION

Decision level fusion combines either the decisions of separate algorithms, or decisions made separately on different evidence. Many COTS products have implemented this type of fusion. There are several ''classic'' rules used in decision fusion, which are detailed next. ''AND'' and ''OR'' rules [146] is the simplest and easiest to implement. The ''AND'' rule will output genuine if all the matchers outputs are in agreement the sample are genuine. The ''OR'' rule will output genuine if at least one matcher decides the sample is genuine. ''AND'' rule might be considered reliable which is validated by a low FAR, but the downside is the FRR extremely high, higher then the ones of individual matchers. The same principle applies in reverse for the ''OR'' rule: FAR is higher then individual matchers and FRR is low. This rule is rarely used in practice, though Tao and Veldhuis [147] proposed a optimised threshold method using the ''AND'' and ''OR'' rule. In order to work the thresholds of the classifiers are modified and optimised in the training phase.

Majority voting proposed by [148] is another decision fusion method, and the most common approach. The final decision is the one that the majority of matchers agree on. Majority voting assumes that all the matchers perform at the same level. If this is not the case weighted majority voting must be used [149]. This method assigns higher weights to better performing matchers.

Prabhakar and Jain [150] proposed a multi-algorithm decision level fusion for fingerprints. The system combines

TABLE 5. Rank level fusion summary.

Paper	Algorithm/system	Result	Dataset	Biometrics
[137]	Incorporates both rank and decision fusion by using PSO	FAR is 0.09% and FRR is 1.5%	IIT Delhi, 100 users with 5 year samples, CASIA V2 lamp iris database	Ear and iris
[138]	Quality based rank level fusion	Including image quality in the ranking increases the Borda count by 40%	WVU multibiometric database, public database from the National Institute of Standards and Technology (NIST)	Face and 4 fingers (index and thumb of the right and left hands)
[145]	PCA and Fishers linear discriminant	EER 1.12%	Olivetti Research Lab Database face database, two public domain ear databases, University of Rajshahi signature databaseRUSign	Face, ear, and signature
[136]	Multiple rank level fusion approaches: Borda count, logistic regression, weighted Borda count, highest rank method, and Bucklin method	Best performance is achieved by Weighed Borda Count	NIST BSSR1 multimodal database	Palmprint
[140]	Markov chain model	EER 1.71%	CASIA Iris Image Database, USTB ear database, FERET face database	Face, ear, and iris

four different fingerprint matching algorithms, two minutia based (Hough transform, String distance, 2D dynamic programming) and one texture based. The scheme design emphasises classifier selection prior to applying decision fusion. The proposed scheme improves the fingerprint verification system by 3%.

Decision fusion depends on the threshold of each classifier, that minimum score which determine if the sample is genuine (above threshold) or an impostor (below). Some of the biometric systems assumed that the classifiers are independent of one another, but there are others which assume that the classifiers must be dependent, at least in a multi-biometric system. Veeramachaneni *et al.* [151] proposed a verification system based on two fusion strategies for correlated threshold classifiers: Likelihood Ratio Test (LRT), which experiments show to still be dependent on the threshold of the individual classifiers, and Particle Swarm Optimisation (PSO) decision strategy, which is proven more effective. The PSO strategy offers better accuracy then score level fusion algorithms (using sum-rule or z-norm). PSO is used by [152] for decision level fusion of palmprint and hand geometry and automatically selects the sensor points which are optimal and one of the 16 fusion rules. The authors used the same work for score level fusion [153] and demonstrated that this system achieves better performance at score level then decision level. Veeramachaneni *et al.* [154] proposed a multi-modal biometric management (AMBM) which performs real time sensor management using PSO, by searching in real time the optimal sensor configuration and optimal decision rule. Kumar *et al.* [155] presented another scheme for palmprint and hand vein based on a similar concept, Ant Colony Optimization (ACO), an algorithm which models the optimal path finding by ants in a colony, where all the possible solutions are proven to be slightly better then PSO. A continuation of this work was made by Rajbhoj and Mane [114], where the ACO algorithm was tested on multiple multi-modal databases such as palmprint and iris, speech and face, face and fingerprint. The system was tested on both score level fusion and decision fusion, from which score level fusion yields better results.

Paul *et al.* [156] proposed the first paper to use Social Network Analysis (SNA) in biometric recognition. The multimodal system based on three features (face, ear, signature), combines multi-modal fusion with SNA, thus reducing the error rate and increasing security. The feature extraction uses the FLDA method commonly known as Fisherimage feature extraction, which is a combination of PCA and LDA. Afterwards the extraction of a SN (social network) is constructed for both testing and classification, and the SN map is constructed. The following metrics can be used to increase classifier confidence: betweenness, Eigenvector and degree centrality. The system obtained a 100% GAR with 5% FAR.

Fuzzy vault can be used for authentication and verification systems. We have presented such systems in Section III-C. Some systems operate both at decision level and score level, such as [122]. Lau *et al.* [157] presented a multimodal biometric system which operates at the decision level, for speaker and fingerprint verification combined with face authentication. The system operates under strenuous conditions and can verify and authenticate subjects in adverse conditions like finger misplacement, different fingerprint pressure and sweat, difficult lighting or turned head for face recognition. Authors obtained a relative improvement of 52% above similar systems.

Abdolahi *et al.* [158] proposed a multi-modal fingerprint and iris system at the decision level. The novelty is implementation of weights in the fusion, which can improve the accuracy of the system because some biometric traits are stronger and more reliable then others. Benaliouche and Touahria [159] proposed a multi-modal multi-algorithm biometric system based on iris and fingerprint using fuzzy logic matching scheme at decision level. This system implements three distinct matching algorithms: the first two algorithms use fusion of the iris and fingerprint by the sum rule and weighted rule, then the final decision is made by the fuzzy system using if then rules. The authors

TABLE 6. Decision level fusion summary.

Paper	Algorithm/system	Result	Dataset	Biometrics
[163]	PCA, LDA, LBPH, Sub-pattern PCA, and Modular PCA extraction algorithms. Uses multiple fusion levels	Recognition accuracy 98.75%	ORL face and CASIA iris database	Face and iris
[119]	ACO algorithm for selection of decision threshold and fusion rule	The authors evaluate the algorithm in comparison with PSO, demonstrating that ACO is better	IITD palmprint and iris database, XM2VTS speech and face database, and the NIST BSSR1 faces and fingerprint database	Palmprint and iris, speech and face, face and fingerprint
[155]	ACO algorithm for selection between 16 fusion rules and decision thresholds	Recognition rate 99%	150 users, using a Canon A630 digital camera with 8.5 mega pixel, and a ring shaped fluorescent lighting source, have been used to acquire the images	Palmprint and hand vein
[137]	Incorporates both rank and decision fusion by using PSO	FAR is 0.09% and FRR is1.5%	IIT Delhi, 100 users with 5 year samples, CASIA V2 lamp iris database	Ear and iris
[158]	Fuzzy logic is used for decision fusion	FAR is 2%, FRR 2% and accuracy 98.3%	CASIA standard database	Fingerprint and iris
[159]	Comparative performance study of classical sum rule, weighted sum rule, and fuzzy logic method for decision level	Fuzzy logic is best for decision level	CASIA-Iris databases V1 and V2 and the FVC 2004 fingerprint database	Iris and fingerprint
[156]	FLDA for feature extraction and SNA for classification	100% GAR with 5% FAR	Face: FERET, VidTIMIT, Olivetti Research Lab Database; Ear: the University of Science and Technology Beijing (USTB) Image Database I and Database II; Signature: University of Rajshahi signature database: RUSign	Face, ear and signature

proposed an implementation of their system and show that the proposed system is better then other schemes, having a FRR = 0.05% and match time = 0.174 sec, as opposed to FRR over 2% for similar schemes. The system is compared with similar multi-modal fingerprint and iris schemes like [160] at decision level fusion and two at feature level fusion: [161], [162]. A hybrid scheme is proposed by Azom *et al.* [163]. This scheme uses five different feature extraction algorithms: Principal component analysis (PCA), Linear discriminant analysis (LDA), Local binary pattern histogram (LBPH), Sub-pattern principal component analysis, and Modular principal component analysis for each trait: face and iris. Feature level fusion is performed for each modality, obtaining two classifiers. Weighted score level fusion is performed for the LDA face extraction algorithm and LBPH for iris creating the third classifier. The resulting three classifiers are fused using decision level fusion.

In Table 6 we provide a small summary of the most relevant decision level schemes.

F. FUSION SUMMARY

We can't tell for sure which fusion method is better, because it depends on the biometric traits being fused and other conditions such as data noise and missing data. Marasco and Sansone [164] made experimental comparison between different methods of combining biometric systems. They consider multiple fusion levels: score level (for min, max, media, weighted sum, and weighted product), rank level (for Highest rank, Borda count, Logistic regression schemes), decision level (for pure majority voting) and Hybrid rank-score fusion (for predictor-based majority voting, predictor-based sequential and predictor-based borda count). The experiments were conducted on face and fingerprint. The main conclusion is that adding biometric traits to the fusion does not necessary increase the performance, not for all the methods. The score sum method increases performance for different modalities. The best results are obtained by hybrid score-rank fusion.

Table 10, located in Appendix A, summarises of relevant fusion schemes. This Table aims to be a easy to follow and an overview of the schemes. We have opted to divide the multi-biometric types into multi-modal, hybrid and other. If the scheme is included in the other category we mention to which category it belongs. The schemes are sorted by publication year. All the schemes in this table are included in the individual fusion tables, but the general overview helps researchers identify schemes based on a certain trait. If as an example we are interested in multi-biometric schemes in which fingerprint feature was used, table 10 can be very useful. After identifying all the schemes using the desired

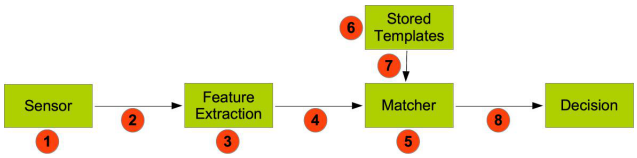

FIGURE 3. Biometric attack places, as depicted by [165].

feature the researcher can go to the appropriate fusion section and check the table there and receive additional information regarding methods and algorithms used.

IV. MULTI-BIOMETRIC SECURITY

Using biometrics (single or multiple) poses the following security and privacy issues: [11]:

- Biometrics are not secret - nowadays user biometric data can be acquired very easily without user knowledge by: voice recording, video recording from a distance, which manages to register user gait, face etc.
- Biometrics can't be revoked or cancelled, and once compromised that biometric trait should be considered unusable. Biometric data is permanent, it's impossible to "issue" new fingerprints, and if disclosed that data is still linked to the user. A biometric feature can be compromised by two means: data hacking and user accident resulting in trait compromise, like fingertips burning.
- Permanent tracking record - biometric data can be successfully used to track the user.

According to Ratha *et al.* [165] a generic biometric system is vulnerable to attacks in 8 places depicted in Figure 3. The numbers in Figure 3 are detailed below:

- **1 Fake biometrics** - an attacker presents fake biometrics to the sensor with the scope of fooling the system. This type of attacks are quite successful.
- **2 Resubmitting stored signals** - a recorded signal is presented to the system, like a face photo or a recorded audio signal.
- **3 Overriding the feature extraction process** - the feature extraction module is attacked directly and the intruder replaces the feature set with the desired one.
- **4 Tampering with biometric representation** - the features extracted by the extraction module are replaced with a different set.
- **5 Corrupting the matcher** - the attacker gains control over the matcher and obtains desired match scores.
- **6 Tampering with stored templates** - the templates are stored in a database, so a possible attacker might try to modify the stored templates or use the templates to generate fake biometrics.
- **7 Communication interception** - intercepting the communication between the matcher and database and sending other information.
- **8 Overriding the final decision** - will make the matcher give the decision desired by the attacker.

All items detailed above, with the exception of 1, 2 and 6, imply gaining access to the biometric system itself and some methods might work only on some biometric systems. Meanwhile compromising items 1, 2 (fake biometrics) and 6 (tampering with the stored template) will yield results on all types of biometric systems. Tampering with the stored template has two aspects: the first one is compromising the database and editing or deleting records, and the second using the stored template to recreate the original biometrics and obtain fake biometrics. Creating fake biometrics can be achieved by recreating them from the stored template or acquiring from the subject itself without his knowledge. In the end, in relation with biometric security, the most important things are: faking biometric data and template protection. In the reminder of this chapter we'll focus on these two aspects.

A. FAKING BIOMETRIC DATA

Can biometrics be faked easily? We are going to answer this question by surveying some of the most relevant papers on this subject.

Matsumoto *et al.* [166] demonstrated that using artificial fingers fingerprints sensors can be fooled. Different authors [167]–[170], showed that many fingerprint verification systems can be susceptible to artificial fingerprints attacks, that's why there are multiple proposals on how to stop the use of fake fingerprints like: odor analysis [171], fingerprints pores [172], and liveness detection [173]. Like fingerprints, iris scans are vulnerable to fake iris attacks as shown by [174] and various detection mechanisms are proposed by [175]–[180] to mention a few. Another biometric very susceptible to spoofing attacks is face authentication by using pictures. There are a lot of techniques proposed to detect this issue: [181]–[189]. Zhang *et al.* [190] proposed the first face spoofing database to be used as an evaluation framework. Hands geometry can also be spoofed by creating fake hands. This concept was introduced by [191] and [192], but it was Chen *et al.* [193] who proposed a practical model using plaster to create fake hands. The authors demonstrate that the fake hands can be created without the user knowledge from hand templates stored into the database. Other soft biometrics can be easily spoofed: voice can be easily recorded or spoofed artificially [194], gait can be spoofed using a video camera from a distance to capture the user motion [195].

Multi-modal biometrics are believed to be more secure, because it is very unlikely that an attacker can gain access to all sources of biometric data and spoof them all. This claim however hasn't been proven and research demonstrates the contrary [196]. Rodrigues *et al.* [196] ran 4 different experiments on a face and fingerprint multi-modal system. The 4 scenarios were: no trait was spoofed, only fingerprint spoofed, only face spoofed, and both traits spoofed. Three different multi-modal fusion schemes were tested and the results contradict popular believe that a multi-modal biometric system is more secure. The experiments showed that it is enough to spoof only one trait while the other one is a random impostor one. The same conclusion was independently verified in [197], [198], and [199], who used spoofed samples and different attacks scenarios. The authors also confirmed that

the FAR increases under spoofed conditions and the attacker might be wrongly authenticated by spoofing only one trait. Gomez-Barrero *et al.* [200] details a software attack on a multi-biometric system and achieve the same conclusion as previous studies: the multi-biometric system didn't present more security then the uni-modal counterparts.

Marasco *et al.* [201] proposed a system that incorporates a spoofing detection algorithm (liveness) in the fusion scheme. The multi-modal system using face and fingerprint includes a liveness detection for fingerprint. The results show the system is resistant to attacks when only the fingerprint is spoofed. Other spoofing detection methods incorporated in the fusion are proposed in [202] and [203]. Marfella *et al.* [202] tested the liveness integration for score and decision fusion and concluded that incorporating liveness at fusion level makes the system more secure against spoofing attacks.

Recently Cornett [204] argued that including a liveness sensor might not be as easy as it sounds especially for mobile devices. Most smartphone vendors have a fingerprint sensor embedded into the home button, which can be used to unlock the phone. The sensors for smarphones were designed to provide a good balance between easiness of use and security. If the sensor is very accurate, but the FRR high, a user might be annoyed because he has to try multiple times to authenticate himself. Introducing a liveness detection in the sensor might have opposing effects and will most certainly reject a genuine user more times then it should. In this case the smartphone user will choose to disable the feature.

1) ACQUIRING BIOMETRIC DATA THROUGH IoT

We believe that some IoT devices represent the most danger to multi-biometrics, because they can be used to acquire biometric data with or without user knowledge. This data might be used to fake biometrics. A recent attack on U.S. government Office of Personnel Management (OPM) resulting in 5.6 million fingerprint stolen, is a clear indication that poor data security can have devastating consequences. The most troubling news is not the attack itself, but the entity in question: the OPM unit of the U.S. military. OPM stores the identities and biometrics of federal contractors, some of them working on classified military technology. One might assume that this data would be guarded against attacks. What happens with the biometric data stored by private companies, which don't have as much security as the U.S. government? Google now, Apple's Siri, Microsoft Cortana record everything the user says and sends the information to companies servers over the Internet [205], Samsung TV's automatically records conversations the user have and uses them for automatic speech recognition [206], most wearable devices record vital information about behavioural biometrics. In the context of IoT and smart devices the most dangerous of them all is our smartphone, because it can be used to acquire direct multi-biometric data from it's user. We are demonstrating our claim in the next paragraphs.

Nowadays smartphones are a privacy nightmare, because they can be used very easily to record information and to acquire user multi-biometric data. If companies like Google, Apple, Microsoft might be considered safe, from the perspective of data security and selling acquired biometric, the same cannot be said about third party applications installed on smartphones. We are not arguing that third party applications use the data for malicious purposes, but most of the vendors of free applications ask for more permissions then needed because they sell the data to advertisers. This is the business model and how they make money, because it is more lucrative to sell user data then earning money through in-app advertising. Even if the application vendor doesn't sell the data, the biometric data might be in danger. We don't know how this data is stored and it's safe to assume that if military computers were penetrated, a smartphone application vendor might not be much of a challenge.

When an application is installed on a smartphone it requires permissions, defining what the application can access from that device. The most misused permission is camera and microphone [207]. This permission can be used to capture images for face recognition, retina scan, voice recording. Sometimes applications request root enabling them access to every device sensor such as fingerprint, heart monitoring and gait, key logging for getting behavioural information about keystrokes and screen shots, very useful to gather user passwords.

When a smartphone application is published in the respective application store, it has to be checked for compliance to store policy. In 2013 Han *et al.* [208] published a research paper demonstrating how they circumvented Apple's permission system. The researchers created free applications, which used special crafted functions concealing their access to not granted permissions. When a user installed one of the free applications, they saw no permissions requests. As a result the authors managed to get user passwords, unlock the phone in almost 40 seconds (for phones using birth-date as PIN) and less than 10 minutes for other PINs, block calls, snapshot-taking, secret filming, tweet-posting, SMS sending, Email-sending. It took Apple one year to solve the problems with the permissions in the application store, meanwhile other malicious entities could have used them to gain valuable data including user multi-biometric data.

Zcaler's labs stated that over 40% of mobile applications communicate data to third parties [209], majority of smart-phone users don't understand or check the permissions requests when installing a new application and root exploits can bypass the entire permissions system [210]. Fiebig *et al.* [211] show how a smart-phone's high resolution camera can be used to acquire fingerprints using the rear back camera, just by taking a finger image. The high resolution camera makes it easy to distinguish the fingerprint.

Meng et. al [212] made a comprehensive survey of biometrics authentication by smarphone. A smartphone can successfully perform 11 biometric authentication types, of which 5 are physiological and 6 behavioural. The physiological ones are fingerprints, face, iris, retina, hand and palmprint, and the behavioural ones voice, signature, gait,

behaviour profiling, keystroke dynamics and touch dynamics. The authors surveyed successful attacks on mobile phones, which claim to have circumvented authentication on mobile phones. Zhang *et al.* [213] presented a successful attack, implemented on touch devices, which is used to guess passwords. The device is first dusted, resulting in revealing on screen fingerprints. The device is photographed and using image processing software, fingerprints are enhanced and run through special algorithms used to guess passwords. Face recognition on mobile phones is very easy to circumvent since the devices don't check for liveness, as such, a simple picture can trick them [214]. Anyone can get someone's picture without his knowledge and social networks makes this easier, because the attackers can use images posted on social networks to circumvent users facial recognition. According to Li *et al.* [215] more then 93% of mobile device users are susceptible to this type of attacks. The same type of attacks work for retina/iris authentication, printing a fake iris image fooled more then 40% iris sensors [174]. Behavioural biometrics are even easier to mimic like voice recording, signature, keystroke and touch dynamics are very easy to spoof.

The proposals for securing smartphone authentication schemes, and authentication in general, are: use of multi-modal biometrics, check for liveness, combining with other authentication techniques (dual factor authentication) and use cancelable biometrics to store the templates. These proposals are useless if the user installs malware or a free application including a root kit that bypasses the permission system and captures biometric data from the user as he uses the smartphone.

We made a simple experiment, to backup our claims. We have used a OnePlus two smartphone running Android 5.1 and searched for the word ''flashlight'' in the application store. This type of application should only require ''camera'' or ''camera and microphone'' permission, depending on the Android version, because the application needs to use the camera flash to create the Flashlight. Table 7 shows the first 10 search results. Over 4 applications, downloaded by more the 56 million users, require more permissions then they should, 2 of which ask for permissions like: location, Photos/Media/Files, WiFi connection, Device and call information, depicted in Figure 4.

There are many problems with smartphone permission systems on different platforms like iOS, Android, etc. There are experts who proposed some improvements, but in the end it doesn't matter, because everything has a single point of failure: the user. As long as the user installs applications from unknown sources, without checking the vendor name (fake applications impersonating well known ones), and/or without reading the permissions, all other security measures are useless. The minute a user grants a certain permission to an application it will give access to certain device features and implicitly data: biometric or otherwise. Even if the application manufacturers are not selling the data to third parties, they might be penetrated by a malicious attacker who might use the data.

TABLE 7. First 10 application results.

No	Permissions	No of downloads
1	Device and app history Camera	**50,000**
2	Camera	100,000,000
3	Camera	100,000,000
4	Camera	5,000,000
5	Location Photos/Media/Files Camera WiFi Connection Info Device ID & call info	**50,000,000**
6	Camera	10,000,000
7	Camera	10,000,000
8	Camera	10,000,000
9	In app purchases Location Photos/Media/Files Camera Microphone WiFi Connection Info	**5,000,000**
10	Camera WiFi Connection Info Location	**1,000,000**

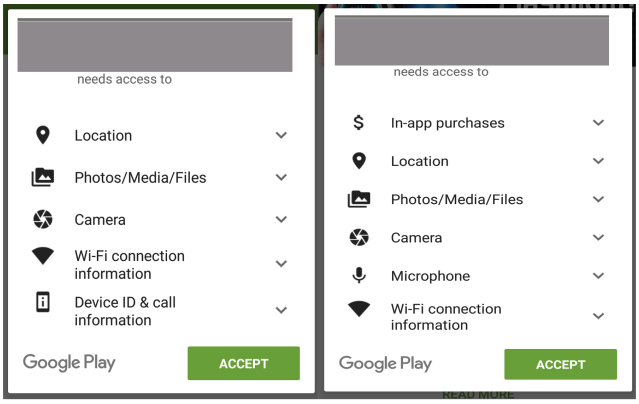

FIGURE 4. Flashlight applications permissions.

B. TEMPLATE SECURITY

For some time experts believed that the original biometric data can't be reconstructed from a stored template, but [216], [217] to name a few, proved otherwise. To protect against template compromise, encryption was proposed, but it was proven that biometric recognition can't be performed in the encrypted domain [217]. Storage on tamper resistant devices, like smart cards [218], might be feasible for a single template for verification but cannot secure larger template databases. Even though cancelable biometrics [11] or private templates [219], were proposed a long time ago, most of the biometric systems still store insecure templates in the database. When this happens, the security of the multi-biometric system resumes to database security, and the argument that multi-modal biometric systems are more secure, doesn't stand. Actually, in the case of multi-modal biometrics, a database breach is even more dangerous, because multiple biometric traits are compromised.

Ratha *et al.* [11] introduced the concept of cancelable biometrics which can be a solution to the problems presented above. Later, template protection schemes were divided into two main groups: cancelable transformations and biometric cryptosystems, depicted in Figure 5.

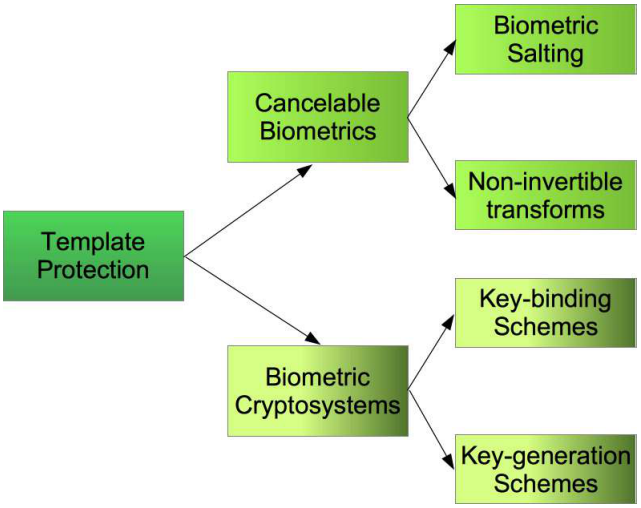

FIGURE 5. Biometric template protection, depicted by [11].

A template protection scheme must tackle the following issues [220]:

- **Diversity**: the protected template has to be different from one database to another, so an attacker can't perform cross matching and determine which user is enrolled in both databases.
- **Revocability**: if the user's biometric template is compromised, the system should be able to generate a new template based on the same biometric data.
- **Security**: an attacker shouldn't be able to obtain the original biometric data from the template.
- **Performance**: the biometric system should not impact the biometric system performance in terms of FAR and FRR.

Jain *et al.* [217] describes the advantages and disadvantages of each template protection type, synthesized in Table 8. There is extensive literature on cancelable uni-biometric schemes and cryptosystems thoroughly surveyed by Rathgeb and Uhl [221]. We chose not to give any examples of single biometric systems, because it's not in the scope of this paper, but we detail relevant systems for multi-biometrics in next sections of this chapter.

1) BIOMETRIC SALTING

This uses the concept of password salting from cryptography, which adds random bits (the salt) to the secret key. Before storing a hashed H password in the database a pseudo random string S is added to the password and it's hash, $H(P + S)$, is stored. This operation adds biometric template entropy, increases security, and makes the template cancelable.

TABLE 8. Summary of cancelable biometrics advantages and disadvantages.

Name	Advantages	Disadvantages
Biometric salting	• Multiple templates generation • Templates revocation • Low FAR • Large upper bound	• Useless if password is known • Degraded recognition
Non-invertible transform	• Biometric data cannot be recovered • Templates revocation	• Less similarity of the feature set
Key-binding cryptosystems	• Template security	• Error correcting code is needed • Cannot be revoked
Key generation cryptosystems	• Template protection • Multiple key generation for the same user	• Low key entropy and key stability.

Advantages:

- Multiple templates can be generated for the same user by simply changing the password. In the end multiple keys will be created, which can be used in different applications.
- Templates can be revoked and reissued. If the template is compromised the same biometric data can be used, with a different password.
- The authentication schemes have a low FAR, because of the password component.
- Extends the upper bound of the biometric system, making it possible to increase the number of patterns the system can recognise.

Disadvantages:

- The biometric template might by compromised if the password is known and matching accuracy might be impacted. This problem resides from the salting process, which is invertible, meaning if an attacker has access to both the user password and the stored template, the biometric data is no longer secure and can be recovered. There could be major implications of this weakness in the form of key management. Let's imagine a scenario where a user has three stored keys in the database, each key is created with a different password. If one of the keys gets compromised, because the user forgot the password, it should be completely deleted from the database because it now represents a template weakness.

- The recognition might be degraded because it takes place in the transformed domain, which might be affected by large inter-user variations.

Canuto *et al.* [222] proposed a multi-biometric fusion framework for voice and iris. The cancelation techniques used are: BioHashing, interpolation, BioConvolving, and four different types of fusion techniques, i.e. uni-algorithm uni-modal, uni-algorithm multi-modal, multi-algorithm uni-modal, and multi-algorithm multi-modal. Multi-algorithms for cancelable biometrics are more efficient and the best results, in terms of accuracy and security of the biometric system, are obtained when using multi-algorithm and multi-modal fusion.

2) NON-INVERTIBLE TRANSFORM

The biometric data is transformed using a non-invertible function and then it is stored into the database. A non-invertible transform can be defined as function F, easy to calculate, but hard to invert. The biometric key presented at authentication represents a parameter for the non-invertible transform. This cancelable biometrics is considered more secure then salting, because it's very hard to determine the biometric template even if an attacker possesses both the key and the stored biometric template.

Advantages:

- The biometric data should be impossible to recover, even by brute force attack, if the stored template is compromised.
- Templates can be revoked using different transformations specific to the user or application, security level, etc.

Disadvantages:

- The non-invertible transform might create less similarity of the feature set. In the transform domain the features similarity should be the same as the normal domain, which is not possible for a very good non-invertible transform. The better the non-invertible transformation, the most secure the scheme is and an attacker can't determine the original biometric data, but this comes at the expense of features similarity which can't remain the same as in the normal domain.

Non-invertible transforms have been applied a lot in uni-biometrics. In 2013 Rathgeb *et al.* [223] introduced the concept of alignment-free cancelable iris templates using bloom filters. This concept aims to solve the template alignment problem identified as an issue for template protection in [224]. The same authors applied this concept in [225] for binary iris codes (left and right), [226] for face and iris. The biometric traits are represented using the bloom filters irreversible transformation. The EER of the system is the same like the score level fusion of the unprotected multi-biometric system 0.4%, but the system excels in security and storage space. An attacker would have to run 2^{268} sequences to recover both biometric traits. The storage space of the protected template is reduced with 63% compared with the original ones. Hermans *et al.* [227] made a security analysis for the system proposed by Rathgeb *et al.* [223] and demonstrated the scheme doesn't produce unlinkability by implementing an attack with succeed rate in a worst case scenario of 90%. Bringer *et al.* [228] extended this study to existing schemes to be vulnerable to cross matching attacks. Recently [229] solved the problem of cross matching attacks by proposing a framework for the evaluation of unlinkability in biometric template protection schemes.

3) KEY-BINDING SYSTEMS

The biometric template is bind by the encryption key and both are stored as a single entity. According to Uludag *et al.* [230] this type of system needs to solve three important issues: issuing new biometric templates if one is compromised, design different biometric templates for different applications, and the biometric key generation and transmission must be secure and easy to use.

Advantages:

- The template is secure because it is hard to decrypt, by brute force, the key or the biometric template without knowledge of users' data.

Disadvantages:

- Biometric matching cannot be made without using error correcting codes, which limit the available matchers that can be used.
- It does not provide diversity (generation of multiple keys using the same biometric data), and as a result they are not revocable.

Fuzzy vault is one of the most used key-binding template protection schemes. Nandakumar [231], [232] proposed a fuzzy vault, transforming the input from two different biometric sources into one template. The author implemented the fuzzy vault (cancelable biometrics) as elements in the Galois Field GF(2^{16}). The author proposed an algorithm of transforming the elements from two different biometric sources (fingerprint minutia encoding and iris features) into GF(2^{16}) elements. Three variations of implementation are proposed, based on different biometric sources: multiple impressions of the same finger, multiple instances of the same biometrics (left and right hand index fingers), and two different biometric sources: fingerprint right index and iris. The last scenario is the most successful one, because it provides the best rates: $FTCR = 0$ (Failure to Capture Rate), $FAR = 0.02$ (False Acceptance Rate), $GAR = 98.2$ (Genuine Acceptance Rate). The system offers high performance and security with a key entropy of 49 bits, which is higher if the templates were stored separately (27 bits for fingerprints and 40 bits for the iris template).

Another hardened multi-biometric fuzzy vault (FV) is proposed in [233]. The features of iris and fingerprint minutia are extracted and each feature vector template is transformed using a random user password, obtaining two transformed vectors. These vectors are encoded in the multi-modal fuzzy vault. The authors conclude that the system contains two levels of security: the password and the biometric system. Even if an attacker gains access to the password the vault

is still protected by the biometric features. The vault can be compromised only if the attacker gains access to both biometric traits and password.

The fuzzy commitment scheme (FCS) is a common biometric key binding system. FCS is proposed for multi-biometric purposes in [234] for 3D face templates obtained by different extraction algorithms and [235] which combines fingerprint and face templates. Both systems use a simple concatenation of binary biometric templates, but Rathgeb *et al.* [236] proposes a reliability-balanced feature level fusion for the FCS, by fusing two iris templates obtained from multi-algorithms into one single template.

Nagar *et al.* [237] implemented a multi-biometric cryptosystem for fingerprint, iris and face using a secure sketch to store a single template. The embedding algorithm extracts of the features for each of the biometric traits and stores them in different vectors z, then the fusion module creates a fused vector Z. The last module, the biometric cryptosystem, generates a secure sketch using the fused feature vector and a key. Depending on the representation of the z vector, two different implementations are used: fuzzy commitment for binary string or fuzzy vault for point set. The experiments show that the proposed system improves both matching accuracy and template security in the context of multi-biometric cryptosystems.

Merkle *et al.* [238] introduced the concept of hash-level fusion. This level can be compared with decision level fusion contained at using only the AND rule for fusion. Hash level fusion is not as flexible as decision level fusion, but offers flexibility for error correcting codes. This new hash level fusion could in theory achieve more privacy and easier implementation. A multi-modal dual fingerprint fuzzy vault system is presented in [239]. The system fuses the central feature points extracted from both hand thumbs, then encrypts the users key. The system achieves a success rate of 85.5%, with FAR 0%. A practical implementation of a multi-biometric system, using the fuzzy vault is proposed by [240]. The multi-modal system fuses face, iris, password and fingerprints, using feature level fusion to store the data in a fuzzy vault. A new binary template fusion is proposed in [241], aiming to provide higher template entropy and discriminability for the fused template. The authors reported that the proposed template can be used as input for popular biometric cryptosystems based on fuzzy extractors or fuzzy commitments.

There are novel template protection schemes based on watermarking. Steganography is the science of covert communication, and digital watermarking is a branch of steganography. Watermarking inserts a recognition mark into a cover medium. In the digital era watermarking is associated with insertion of copyrighted information in multi-media files. There are two types of watermarks: visible with the naked eye (logo) or invisible (library id on a borrowed library book). The role of an invisible watermark is to retain the information even if the cover media file is tampered with. To accomplish this, watermarking methods spread the same mark throughout the file. The goal of invisible watermarking is to have at least one unaltered mark after the cover file has been tampered with. The watermarking process consists in a cover file which will have the mark applied. The same process is used in multi-biometrics. The multi-biometric features are extracted, fused and then applied as a mark in a cover file. The new file will be stored in the database, thus assuring template protection. A fingerprint and iris using DCT watermarking protection are proposed by [242]. The iris and fingerprint features are extracted and decision fusion using a conjunction rule is applied. The system is tested on FVC2004 and CASIA databases. The authors tested the proposed system under different attack conditions obtaining different ERR. The security of the watermarking was tested against two other methods, using different attack scenarios: JPEG compression, median filtering, Gaussian filtering, and salt and pepper noise. The tests showed the system performs better under attack then the two other compared with. The overall performance of the biometric system doesn't degrade significantly. A similar system was proposed by Nair and Aruna [243] for fingerprint, iris and palmprint traits, using PSO as watermarking technique. A new approach in using watermarking for multi-modal template protection was proposed by Nafea *et al.* [244]. The finger print features are watermarked into the face image using the SWT-DVD technique. Then the watermarked face is encrypted using shuffling, Hadamard and the chaotic map. The system is highly resistant to attacks and the overall performance isn't degraded because of the encryption. Using robust watermarking to secure a template shouldn't be the only security measure taken for template protection, as proven by Hammerle-Uh *et al.* [245], who describe an attack against a robust watermarking multi-biometric system. The authors suggest using fragile or semi-fragile embedding techniques for the watermark and classic cryptography to secure the transmission channel between smart card and biometric matching module.

A novel template security regards fingerprints and manages to secure the templates without using a key. Ross and Othman [246] introduce the concept of visual cryptography, where a fingerprint image is decomposed into two images (named sheets) and stored in two separate databases. The two sheets are overlaid when authentication is needed. This way the fingerprint image is never stored in complete form. Other schemes propose the protection of fingerprints by combining two different fingerprints from two fingers [247]–[250]. This technique is useful in creating virtual identities to be used for research, or to create a secure template by hiding the biometric information, and also create a cancelable template. Storing a fingerprint in this manner in the database makes it impossible for an attacker to distinguish between the fingerprints and normal matching techniques can be used. Li and Kot [251] proposes another fingerprint combination technique which extracts the minutiae from the first images and embeds the orientations from the second image. The authors claim this technique is better then the previous ones, because it is not creating many false minutiae.

4) KEY-GENERATION CRYPTOSYSTEMS

The key is derived from the biometric template and stored in the database.

Advantages:

- Template protection is built in because the key is generated from the biometric template.
- Multiple key generation for the same user, which can be used for different applications or revoked if compromised.

Disadvantages:

- Low key entropy and key stability. Direct key derivation cannot offer high key entropy and key stability. Key entropy is the number of keys that the system can generate for different biometric data, and key stability the number of repeatable keys for the same biometric data. These metrics are in direct correlation, if the key entropy is high the key stability is low and vice versa.

Kanade *et al.* [252] proposed a cryptographic regeneration system multi-biometric system using left and right iris code. A random string K is generated and encoded using Reed-Solomon(RS) codes and then the output is further encoded using Hadamard error correcting codes and a pseudo code string S is obtained. The features extracted from the left and right iris create two feature vectors I_L and I_R, which are fused in one single vector, I_{ref}, using feature level fusion combined with error correction. *XOR* is performed on the fused vector I_{ref} and pseudo code S, thus the encoded template is obtained. The system succeeds in generating 147 bit keys with FAR 0% and FRR 0.18%. The authors concluded that this scheme can be combined with other biometric modalities. The authors proposed an improvement of their work in [253] using two different biometric modalities: iris and face. The system works the same, the only difference is the type of fusion used, i.e. weighted feature level fusion. The change in fusion type is a necessity due to the different representation and error correction needed for the two different biometric modalities. Because multi-biometric fusion is used, the key entropy is bigger and 183 bits key can be generated. In [254] multiple multi-biometric systems based on the same fusion method are discussed.

Prasanalakshmi *et al.* [255] detailed a unique approach to a biometric cryptosystem. The biometric traits for face, fingerprint and palm vein are acquired and the fingerprint template created and normalised to a 256 bit template. A secret key is generated from the palm vein, which is used to encrypt the fingerprint template. The encrypted template is transformed into a 2D vector, and later embedded into the face image. The system was implemented in MATLAB and achieved an FRR of 0.01% and FAR of 0.00008%.

C. BIOMETRICS USED AS KEY FOR ENCRYPTION AND PKI

A biometric PKI system works exactly like a normal PKI key, using a set of two keys: public and private. There are two specific differences: private key generation (called enrolment process) and signing. During the enrolment process the user presents his biometric traits for the master template to be created and the private key derived. During the signing process the user will provide the biometric data used for the private key generation. The same principle applies for symmetric biometric encryption.

The concept of biometric signature was first proposed by Janbandhu and Siyal [256] who mentioned that biometrics can't be directly used as an encryption decryption key because some are unstable on the course of a person's life and have a high EER. Pawan and Siyallls proposed a signature system based iris scan which is stable in time and has a low EER one in 1.2 million [257]. The authors presented a method of using iris scan biometrics in RSA and DSA. Feng and Wah [258] implemented a hand written signature which performs a shape matching for eliminating poor quality signatures and extracts values of predefined signature features. The obtained values (strings) can be used to generate the private key for DSA algorithm. The EER rate is 8% with a FAR of 1.2%. Lan and Hang [259] used a specialised technique to extract the finger minutiae points and to generate a Biometric Encryption Key (BEK), which is used for private key encryption and certificate creation. A biometrics key generation function was used by Jo *et al.* [260] to generate the required RSA keys, and the user fingerprint input is captured as a biometric template. The RSA keys were generated using a hash function on a user biometric template and a secret key, thus allowing the algorithm to be cancelable and the keys revoked.

Gong *et al.* [261] created a feature based generation scheme for PKI. They extract features from iris codes, which are tested agaist the Rabin-Miller algorithm to determine if the number is prime. In the end two large prime numbers will be obtained from the left and right iris. These numbers represent the input values for the RSA algorithm for key generation.

Mohammadi and Abedi [262] proposed an ECC algorithm which has advantages over the RSA biometric signature. The main benefits of the suggested approach are: security - ECC security is based on the elliptic curve discrete logarithm problem (ECDLP), which is harder then the Discrete Logarithm (DL) on which RSA is based. This means that ECC biometrics can use shorter keys and still offer the same level of protection as other algorithms with shorter keys. In [263] Ramya *et al.* implemented a multi-biometric system for obtaining the private key for AES encryption. This system extracts the iris and fingerprint features and performs feature level fusion. The fused vector is used to generate the 128 bits secret key used for encryption.

Hiep *et al.* [264] made an attempt of BioPKI using multiple biometrics. The authors presented the same system as the current one using public and private keys, the private key being stored on a token. The biometric data is to be used for extracting the private key from the token. The authors used 2 different finger print templates, stored separately in the fuzzy vault. The token containing the private key is secured with biometrics instead of a password. When the user needs to sign, he'll have to provide the required biometrics to unlock

the token and access the private key. This method is very easy to implement and doesn't require changes in the current PKI infrastructure.

The security of a cryptosystem is dependant on the security of the key. Nowadays a system is considered secure if the key is at least 1024 bit, though 2048 bit is better. The security of a biometric key can be determined by key entropy - which won't allow an attacker to guess the key. The efficiency of a biometric system can be measured by FRR and FAR rates. When assessing the security of a biometric system all three elements must be taken into consideration; those elements are FRR, FAR and entropy. If a system is designed with high key entropy and high FRR, ultimately that system is unusable, because legitimate users cannot use it. Buhan *et al.* [265] demonstrated that the larger the key the larger the error rates and the FRR and FAR rate increase. According to [266] three factors should be considered when evaluating a biometric cryptokey: accuracy, key size, and effective entropy of the biometric features used to derive the key.

Ballard *et al.* [267] show that the common techniques used to generate biometric keys are not secure. The authors propose three requirements that a biometric key generator has to fulfil in order to be considered secure:

- **key randomness** - the biometric keys appear random to an adversary even if he has access to auxiliary information.
- **weak biometric privacy** - no information can be deduced given auxiliary information and the biometric template.
- **strong biometric privacy** - no information can be deducted given auxiliary information, the biometric template and the key itself.

Because of increasing demands on biometrics PKI Balakumar and Venkatesan [268] suggested that multi-modal biometrics should be used for generation keys, that means multiple inputs from different biometric devices. This will certainty increase security over convenience since the user will have to provide multiple biometric inputs when signing. Related to this Rathgeb and Uhl [221] identified a potential problem, i.e. the inability to decide which biometric characteristics should be used for which type of application. This should be decided based on the application type and the security needed for the application.

D. SECURITY SUMMARY

There is no generic framework that can accommodate all the protection templates and when designing a multi-biometric biometric system the need for template protection should be considered, because it will impact the choice of type of fusion and the type of protection template used [269]. Tyagi *et al.* [270] concluded that the main benefits of biometrics implementation on a large scale are fraud detection and deterrence, increased user accountability (and implicit non-repudiation), increased overall security and convenience. The last one is very important because usually security implies stricter rules which become inconvenient for the user. Because multi-biometrics systems are very sensitive, when implemented in practice they should be compliant with recognised industry standards like: ISO/IEC 2382:2015 Harmonized Biometric Vocabulary (HBV) [271], ISO/IEC TR 24722:2015 Multimodal and other multibiometric fusion [272], ISO/IEC 24745:2011 Biometric Information protection [273], ISO/IEC 19792:2009 Security evaluation of biometrics [274], ISO/IEC TR 30125:2016 Biometrics used with mobile devices [275] etc. There are many biometric standards and one should choose the ones relevant to their application and country where the system will be implemented. This document [276] represents a good introduction into biometric standards and issuing organisation and should be consulted before implementing any biometric system.

V. EMERGING RESEARCH AREAS AND OPEN CHALLENGES

To conclude our paper we include a brief discussion on emerging trends in biometrics, such as adaptive, soft and context-based biometrics. This section concentrates more on discussing the general concepts and challenges, and less on detailed descriptions of specific schemes. We cover topics like: adaptive multi-biometrics with details on quality based methods, soft biometrics, context biometrics (which includes continuous authentication).

A. ADAPTIVE MULTI-BIOMETRICS

With the implementation of large, long-term multi-biometric systems problems might occur due to time lapse and operational conditions. **Time lapse** issues include ageing, diseases and accidents which have resulted in a permanent loss of or altered biometric. For example, one would think that face recognition is likely to be affected by this process, but it is not the only one. Fingerprints and palmprints could be affected by wrinkles, cuts, skin conditions and smoothing of the skin as result of manual labour. Retina, speech, heart-beat biometrics could be affected by a contracted medical condition altering biometric features, like glaucoma, dysphonia and arrhythmia. There are not many studies reflecting the effects of ageing in biometrics, but the ones conducted showed that templates and biometrics change over time. The studies were performed on: face [277], on-line signature [278], iris [279], [280]. Fairhurst *et al.* [281] present an extensive study on effects of ageing in biometrics, and even try to emphasis the positive side of ageing by offering applications where incorporating ageing information helps the biometric process, such as limiting the search in a database based on subject's age. **Operational problems** category refers to factors specific to the multi-biometric system such as: environment, lack of biometric data or data deficiency, biometric type and it's weight in fusion.

Adaptive biometrics try to address the issue of biometric change over time. Adaptive biometric systems are defined as automatic updates to the intra-class variation by introducing operational data [282]. An adaptive biometric system has a new module for adaptation that is responsible for updating the

template using operational data. Adaptive biometric systems can be classified by their key attributes [283]:

- *Supervised, semi-supervised or unsupervised:* In a supervised adaptive biometrics system a human supervisor has to manually label the input data, as opposed to unsupervised methods where this process is done by the biometric system. Semi-supervised techniques are a type of supervised methods, which use a small set of labeled data and a large amount of unlabeled data. The best performing systems are the supervised ones, where a human supervisor labels the data [283].
- *Static or video based:* Type of data used in the multi-biometric system makes a difference. For example we could consider a single image (static) as opposed to an entire video sequence. A video sequence represents a series of consecutive pair images of the same subject. The biometric system can establish identity constancy [284], [285] only from the video sample sequence, by analysing consecutive frames of the video, thus obtaining many samples of the same subject. The same identity verification can't be done using a single image. A single image is easier to spoof then a video sequence, and provides only one perspective of the user.
- *Level of adaptation:* The adaptive process can extend to the fusion level. So besides using the adaptive process only for updating templates, it is used actively in the matching system at a certain fusion level. Most matchers today can make a decision on how much a certain biometric should be weighed based on biometric type reliability or the environment the sample was taken in. There are several examples of implementing adaptation at different levels: adaptive score weighting ([115], [127]), score normalization [286], adaptive feature weighting ([59], [287], [288]).
- *Self or co-training:* Self and co-training are methods used by semi-supervised methods, which use operational data to deduce the label. These methods are inspired by machine learning systems. Self-training methods use highly classified input samples to infer and update the model, as opposed to co-training methods, which use two biometrics to adapt the reference. Didaci *et al.* [289] analyses the difference between semi-supervised methods and shows that co-training methods are more proficient then self-training ones.
- *On-line or off-line adaptation:* The system can update itself as soon as a new sample is received and processed (on-line) or after the samples have been processed (off-line) [290], [291]. Memory is the constraint when choosing the adaptation type. Memory becomes an issue for behavioural biometrics, such as signature, keystroke dynamics, which might require a large amount of input data or more time to process. If such is the case, all the processing and data storage may be done off-line, and the system can be updated at a later time. In case signature biometric systems on-line systems incorporate keystroke dynamics as opposed to off-line ones who don't [292]. Off-line signature systems are harder to implement and use static images for signature verification [293].
- *Quality or non-quality:* Input data quality has a massive impact on multi-biometric system. Quality measures can be defined as a set of quality standards for biometric samples and other criteria known to influence a biometric system [283]. Sometimes bad input quality can result in missing data, which can result in an inability to perform biometric fusion. This is why many multi-fusion algorithms have a prediction module to infer the missing data based on stored samples, or known behaviour [98], [135], [294]. Bad quality samples might be the direct result of someone trying to use spoofed biometrics to attack a system, this is why image quality assessment must be introduced as a countermeasure into a biometric system [295]. Many fusion techniques include quality based fusion. A bad quality sample can undermine the biometric system. In case of multi-biometric fusion weighting is done based on: sample quality, biometric characteristics type (soft biometrics receives a lower weight then hard biometrics), and both criteria. There are many examples for this type of fusion, many of which were mentioned throughout the paper, but we're mentioning some schemes in this section not grouped by fusion type. Support Vector Machines (SVM) methods are commonly used in quality based multi-biometric systems [296], [297] to analyse and classify data based on previously training data. Multivariate polynomials regression is used by [298] for fingerprint and voice authentication. This method gives better results then optimal weighting methods. One of the mostly used techniques is the Bayesian belief network [299]–[304] for biometric fusion. The Bayesian belief is a statistical model that allows to make decisions with incomplete information, and most importantly re-evaluate decisions based on new information [305]. In [130] propose an adaptive automatic quality estimation with different weighting of two matchers ridge and minutia based matchers for fingerprints. Another automatic weighting system is proposed by [306] for fingerprint and iris using likelihood ratio-based fusion. Latest techniques in estimating weights in quality fusion use computational intelligence techniques such as: neural networks and other advanced AI algorithms. Fuzzy logic was used extensively in computer science in understanding of natural language [307], which can't be interpreted as 1 or 0. Fuzzy logic advances the idea of degrees of truth. Fuzzy logic is also applied to in multi-biometric systems to determine the reliability and quality of the samples provided based on biometric type or adverse context conditions such as: finger misplacement, noisy environments. These factors are used to automatically weight the importance of a biometric feature [123], [158], [159]. Prasad *et al.* [308] proposes a theoretical usage of fuzzy logic to determine the automatic

thresholds for every matcher used in multi-biometric fusion. Cancellable biometrics is the field where fuzzy vault or fuzzy commitment scheme (FCS) are being used increasingly. Most of the schemes presented in the template protection Section IV-B are based on these methods and are discussed in more detail there.

Particle Swarm Optimisation (PSO) is and advanced artificial intelligence technique evolved from the social study of birds and their flying patterns. PSO [309] can determine the location of each bird in the swarm, location being characterised by position and velocity. The birds in the swarm are in constant communication and can update their location information in real time, based on the position of the best located bird. The same principle can be applied to a multi-dimensional space, where a particle can constantly update it's position in that space, depending on the best position (named local best position p_ak), global position (p_gk), velocity vector (v) and acceleration (a). For biometrics the binary version is used to create the position vector, where it can have only two values 1 or 0. PSO is used in feature level fusion to solve the feature dimensionality problem [73]–[75] or to update the score weights or thresholds [48], [100], [137], [151]. Ant Colony Optimization (ACO) is another AI algorithm used in multi-biometrics. ACO models the optimal path finding by ants in a colony, and has proven to provide better results then PSO when implemented in a multi-biometric system [114].

Methods for adaptive template update are very promising but they still have some open problems that need to be addressed before being widely adopted [284].

- *Vulnerability to attacks*: Template updates allow impostor introduction and introduction of multiple samples which can lead to a genuine person loosing identity [283]. Introducing impostors when updating a template is impossible to avoid completely, even by using stringent updating procedures [310]. A comprehensive study must be made to see if the use of adaptive biometric systems outweighs the impostor problem they pose. Creating a threshold scenario that stops the introduction of impostors it's still an open problem [284]. Poh textitet al. [311] reports that classification errors in an adaptive system lead to lower system performance with higher error rates. Poh *et al.* [285] made a study on face and speech and conclude that adaptive biometric systems should be subject specific, resulting in less impostors.
- *Reduced sample size*: adaptive biometric systems can capture a limited amount of available samples [38], because of stringent thresholds. If lax thresholds are used impostors might be added to the database. The practice of stringent thresholds is safe from the impostor perspective, but it has a major drawback: large amount of unexplored samples, which might provide invaluable information.
- *No sample distinction*: the adaptive system can't distinguish between informative, redundant or noisy samples [38].

B. SOFT BIOMETRICS

Our paper mostly detailed schemes involving hard biometrics, i.e. traits that can provide strong certainty as to the uniqueness of the user based on mathematical matching. However, soft biometrics are also receiving attention as a research direction. The idea behind soft biometrics is that the user match could be made in a way more akin to the way humans recognise each other, through the recognition of a combination of potentially non-unique features. Soft biometrics are classified into: physical (skin colour, hair colour, eye colour, height and weight, beard or moustache), behavioural (gait, keystroke, mouse stroke), adhered human characteristics (clothes colour, accessories, tattoos) [312].

Soft biometrics could be built into multi-biometric systems in a number of ways:

- *Mixed authentication:* soft biometrics are used in conjuncture with hard biometrics for authentication. Human identification at a distance is one of the most prolific usage of such techniques, e.g. [55], [67], [84] and [85]. These schemes are discussed in more detail in Section III Zhang *et al.* [313] defines a multi-modal adaptive framework with emphasis on weaker traits. The authors propose semi-supervised learning techniques to straighten the weaker features.
- *Soft authentication:* soft biometrics are solely used for authentication. Bailey *et al.* [314] proposes such a system using only soft biometrics: keyboard, mouse and GUI interactions.

Gavrilova and Monwar [315] also introduces the concept of social connections as a ''soft biometrics''. Social connections can be defined as: ''Whom the person knows''. The authors propose a multi-biometric system based on gait and social information to increase system security. The experiments demonstrated that the system doesn't provide any improvement when user behaviour is erratic, but it can be used in a predictable environment. A later paper formally defines the concept of Social Behavioural Biometrics (SBB) [316]. SBB is defined as identification of an author (real person or avatar) based on the social interactions [316]. Social interactions are divided into two groups: on-line in social networks, websites, forums, blogs, chats, etc. and off-line interactions, like face-to-face meetings, and behaviour in different environments, such as work place, family, school, etc. The authors define the following future applications for SBB, in the context of user authentication and verification: *automatic generation of security questions*, based on known facts about the user; *on-line continuous authentication*, when the user authenticates to a site his behaviour will be constantly monitored and if the system detects significant behaviour changes it can stop access to certain application features; *combination of SBB with other biometrics* soft or hard to increase system security.

A study [317] shows the large amount of private personal data biometrics can reveal. Privacy is disappearing at an alarming rate and new questions arise regarding privacy and ethics in biometrics. Some of the on-going privacy trends are: privacy of facial biometrics - how to suppress certain features, but still have user identity [318], privacy regarding airport whole body scanners and mostly how to limit the visualisation of naked body picture, identification of medical conditions [319] and information regarding gender, which doesn't not coincide with travel documents (transgender people) [320]. Wickins [321] foresees a possible social exclusion for certain groups of people due to increase usage of biometrics for authentication.

C. CONTEXT-BASED BIOMETRICS

Biometric traits could be complemented by the context of the user. The context could shape the nature or the number of traits measured and evaluated. This has to potential to achieve acceptable security levels but allow flexibility to provide more user friendly systems. One related area that is receiving attention is **continuous authentication**.

Continuous authentication aims to continuously monitor the user behaviour and use it to re-authenticate the user continuously through potentially a less onerous process than used to setup the initial session. It could use hard biometrics, but as was touched upon in the previous section continuous authentication also relies on soft biometrics, e.g. user's movement before sitting down at his PC, which would not be able to uniquely distinguish a person but in a chosen context the user's behaviour could verify his identity. Alternatively, eye movement could be used to check whether the same user is still present [322], possibly after a stronger measure was used to login initially. There are four closely related areas where continuous authentication systems could potentially be useful [323]:

- *Intrusion detection:* The goal is to determine whether the system is currently communicating with a legitimate user or an attacker. To achieve this goal the system has to concentrate on abnormal or intrusive events, rather then the normal. An important task is to define what is considered normal and abnormal user behaviour. There are two important factors in such systems: *accuracy vs convenience* and *live vs bulk reporting*. An accurate system will have a low FAR, but will likely generate many false positives translated into high FRR, as opposed to a convenient one which will generate less false positives (low FRR) and more likely have higher FAR. Both scenarios are undesirable, because it will result in the system losing credibility. A balance has to be achieved, and according to [323] a FRR between (0-1%) and FAR (5-15%) could be considered acceptable. *Live vs bulk reporting* refers to live intrusion reporting or bulk reporting at a predefined time. Live reporting makes a system more accurate and implies the presence of a human operator to constantly monitor the intrusion. Bulk reporting is more convenient, but is prone to mistakes and late reaction. If at the end of the day 100 events are reported, chances are that they won't be thoroughly reviewed. Late reaction is a direct result of bulk reporting, a possible intrusion might be detected too late. Examples of multi-modal biometric systems used for intrusion detection are: keystroke and mouse dynamics [314], [324], [325], keystroke and voice recognition for mobile systems [326], [327], gait and voice [328], face images and keystroke dynamics [329] text based multi-modal approach linguistic analysis, keystroke dynamics and behavioural profiling [330], [331]. In [332] the authors conclude that more emphasis should be on using multi-biometrics for continuous authentication, since most systems use a single one.
- *Session security:* This goal is related to the form and is aiming to prevent a user session from being hijacked, by detecting that the behaviour of the user has changed. Session hijacking can be accomplished by an attacker accessing an unlocked computer when the user is away, stealing a device, or man in the middle attack (MTM) an attacker inserts himself between the user and the server after the authentication. Ceccarelli *et al.* [333] proposes a multi-modal biometrics of session management without the user interaction. The system contains a distributed architecture consisting of: authentication server, computational servers and user database templates. Different devices can be used in the system, which will adapt and use the available biometrics it is capable of collecting.
- *Insider detection:* Is a special case of intrusion detection system which focuses on system misuse by authorised users. An authorised user gain lawful access to the system and tries to escalate his privileges or access a restricted area. A high security place installation might use hard biometrics for authentication (at the door) and behavioural biometrics (such as: gait) to constantly monitor users in a secure area.
- *Network forensics:* Forensics deals with what happens after an attack has been detected. According to Ahmed and Traore [334] *attack attribution* depends on identifying the persons responsible for the attack is an important aspect of forensics task. The authors identify a possible usage of multi-biometrics of users to verify the user involved in a transactions or session, which might be used to attribute the attack to a specific user.

The challenges for continuous authentication systems are: massive amount of data created, processed and stored. Existing systems must limit the amount of data because of practical constraints, which limits the efficacy of the system, especially in network forensics. Another challenge for continuous monitoring system is the ability to deal with different architectures and OS. An enterprise continuous monitoring systems has to track users on their desktops, company servers, mobile phones.

VI. IMPLEMENTATION BLUEPRINT

This chapter is an implementation blueprint intended to help design a multi-biometric system. This section includes a list of questions to be answered when designing a multi-biometric system. We have included examples of which techniques should be used and in what context. The list should be used recursively, because all questions are intricate and dependent on each other. A first pass should be made by answering all the questions, then all the answers should be revised based on the overall picture. Only a recursive approach will lead to a good system design. We will detail each question (Q) in the following paragraphs:

- **Q1: What's the system purpose?** The system purpose might raise a constraint for multi-modal biometrics. If the system is used for smartphone authentication, then a simple face recognition (uni-biometrics) is enough. For sensitive access control systems, like military installations, multi-biometrics is desiderable if not required.
- **Q2: How many people are expected to use the system?** When the number of users is small, uni-biometrics may suffice. Biometric systems have an upper bound, described as the maximum number of patterns a certain biometric feature can recognise. The upper bound for large massive systems will call for the use of multi-modal biometrics. When answering this question keep in mind the table 1 and multi-biometric system advantages both found at the end of section II.
- **Q3: Are all the traits used at once?** This type of access might have to be implemented when a company has hundreds of employees of which only very few have security clearances. Asking for two or more biometric features from every employee, when entering the building, might certainly create a queue. The building authentication system should use a mixture: users are authenticated by one biometric when they enter the building. As the user progresses through the building, to higher security zones, additional biometrics should be required, as described in [335].
- **Q4: What environment is the system going to be used?** The noisiness of the environment has to be considered, because it might automatically eliminate some biometric traits, such as using voice recognition on a construction site. The environment is a factor to consider when choosing sensor types. If the system has to perform face authentication at night or under peculiar light conditions, which might affect the image quality, then a thermal sensor might be needed. The type of sensor used has direct implications in the enrollment process, discussed in Q9.
- **Q5: Are there any special constraints?** Special constraints might have something to do with special legislation, constraints of the group of population etc.
- **Q6: What is the system budget?** System budget is a factor which will impact many decisions and should be answered as early as possible. For example: if the budget is not too high less expensive sensors might be used. A sensor that includes liveness detection is very expensive, where as software liveness detection might be very efficient and considerably less expensive.
- **Q7: Type of biometric security?** Security covers two aspects: **template security and anti-spoofing (liveness)**. The answer to question 1 might be the answer to what type of template protection does the system need (IV-B). We might choose certain traits because they offer security (see table 9), different schemes for protecting the template or schemes that include spoofing protection. Biometric salting IV-B1 and non-invertible transforms IV-B2 offer security, and matching can be done in the transformed domain, which makes the matching faster. Key-binding systems IV-B3 and key-generation systems IV-B4 offer better template security, since the template is encrypted with a key derived from the biometric itself, but the matching can't be done in the encrypted domain. The additional decrypting time might be an issue for large systems in terms of system response. Using liveness detection and resistance to spoofing (refer section IV-A) might be mandatory in sensitive systems, but the budget question will decide which type of detection can be implemented. Liveness detection can be hardware, very expensive because it's included at biometric sensor level, and software less expensive. Sensitive systems might require some form of continuous authentication (refer sectionV-C). The most obvious form is gait through building video cameras, but there are other forms of like key stroke movement (refer section V-B).
- **Q8: Which biometric traits to use?** The answer to previous questions has to be taken into consideration when answering this question. Not every biometric is equal as shown in table 9. We can't say one is better then the other, it depends on what we are looking for and the environment they are going to be used. For sensitive systems, hard biometrics are desirable since they are the most resistant to spoofing and offer better security. A reliable biometric key can be extracted from hard biometrics, which can be used to encrypt the biometric template offering better protection. Continuous authentication by monitoring gait, mouse movements, or key stroke, can help detect intruders in a building or a computer system, but it's not recommended as a sole authentication measure. For sensitive security systems we recommend using two hard biometrics such as: fingerprint and iris for authentication, and continuous authentication throughout the building.
- **Q9: Which is the enrollment procedure?** Enrollment procedure must be thought of since some users might not be available. Plus the FTE of the system has to be taken into consideration. Will the users be allowed to enroll by themselves or is this procedure only done in the presence of a supervisor? Sensors types are very important too. A biometric system might be extended

with the addition of new sensors for the same biometric. Problems might arise at authentication when the samples are taken with another type of sensor then the one that created the template.

- **Q10: What FAR and FRR are acceptable?** The FAR, FRR and GAR of the proposed multi-biometric system has to be calculated to see if the results are fall into acceptable rates. A good comparison of FAR and GAR for existing databases, mostly for face and ear biometrics, is made in [336] and [337].
- **Q11: What additional information is stored by the system?** The design should include the ancillary information to be stored by the system such as: user name, social security number, id etc. This information can enhance the authentication accuracy, if used together with the primary biometric traits [338], and can also be used to filter information from very large databases. The system can automatically determine if the subject is a ''White Female'', for example, and perform matches only on the identities with this attribute.
- **Q12: What is the sensor array configuration?** This question includes the answer to: **number of sensors, placement, and acquisition sequence**. Acquisition sequence can be at the same time or sequentially. The first type is very convenient and decreases overall system enrolment time significantly, especially for systems storing millions of identities. The examples below are meant to see differences between acquisition types. Kim *et al.* [76] proposed an acquisition system using time-of-flight (ToF) depth camera and near infra red (NIR) camera to simultaneously capture information about hand vein or face. Yoo and Kang [339] described a simultaneous dual-sensor acquisition system for face and iris. The vast majority of multimodal biometric systems use sequential acquisition of biometric features. The BioSecure Multimodal Database (BSMD) was created by 11 European Institutions which collected three types of data sets (DS) using various collection methods [340]. DS1 was acquired via the internet without supervision and consisted of users providing: 2 frontal images, audio and video files of various scenarios: 4 digits pin codes from a set of 100 codes spoken in English, 4 digits pin codes from a list of 10 codes spoken in national language, digits from 0..9 in English, 2 different sentences in both English and national language. DS2 acquired data in an office under the supervision of an acquisition responsible, who verified the biometric samples and also provided user training in handling the biometric equipment. The following biometric data was acquired: voice, face, signature, fingerprint, face and iris. DS3 used mobile devices to capture biometric data like: face, voice, fingerprint and signature. This DS was also supervised by a human responsible, and the voice samples were acquired in two different environments: indoor and outdoor.

TABLE 9. Comparison of biometric traits as depicted by [230] and adjusted by us, based on current situation. We have used the following notation: H (high), M (medium), L (low).

Biometric characteristics	Face	Fingerprint	Hand geometry	Iris	Keystroke	Signature	Voice
Universality	H	M	M	H	L	L	M
Distinctiveness	L	H	M	H	L	L	L
Permanence	M	H	M	H	L	L	L
Collectability	H	M	H	M	M	H	M
Performance	L	H	M	H	L	L	L
Acceptability	H	M	M	H	L	H	H
Circumvention	H	M	M	L	M	H	H

- **Q13: What is the processing sequence?** Processing sequence or operational mode is strictly related to acquisition sequence. A multi-biometric system can operate: sequentially, parallel or hierarchical mode. Sequential mode is very useful to filter through identities before the next modality is used [341], and a decision might be possible before matching all traits, which reduces the recognition time. In this mode multiple traits don't have to be acquired at the same time. In parallel mode of operation the information from all the sensors/traits is used simultaneously. Hierarchical mode combines the previous modes with some traits processed in parallel and others in sequence.
- **Q14: Which fusion methodology is going to be used?** Fusion methodology to be used, based on constraints identified until now. This is by far the most difficult decision because of the multitude of methods available. Sensor level fusion is usually performed in order to acquire a better biometric representation such as: acquiring the face using multiple cameras and create a better template. Feature level fusion can be done for multiple modalities, if the features are compatible. Features obtained from the different fingerprints using the same extraction algorithm can be easily fused into a single vector. Some feature extraction algorithms from different traits are incompatible with each other and feature level fusion might not be possible. On the other hand, feature level fusion offers better matching accuracy, because lot of information is lost after the matching is done [18]. According to [89] decision level fusion should be used when every individual matcher decides on the best match judging by the input, rank level fusion is used when each matcher creates a list representing the degree of confidence, and score level fusion should be used when the matcher outputs a set of possible matches with the quality of each match. Sore level fusion is considered the most robust type of fusion because it can include different types of biometrics and algorithms. Most quality measures schemes perform matching at score level.

TABLE 10. Multibiometric schemes summary.

No	Year	Author	Decision level					Type			Traits
			Sensor	Feature	Score	Rank	Decision	Multi-modal	Hybrid	Other	
1	1998	Ratha et al. [19]	x							Multi-sample	Fingerprint
2	2000	Froba et al. [34]	x					x			Voce, lip motion, still image
3	2002	Jain and Ross [20]	x							Multi-sample	Fingerprint
4	2002	He et al. [21]	x							Multi-sample	Fingerprint
5	2005	Choi et al. [22]	x							Multi-sample	Fingerprint
6	2005	Ross et al. [23]	x							Multi-sample	Fingerprint
7	2005	Zhang et al. [24]	x							Multi-sample	Fingerprint
8	2005	Shah et al. [28]	x							Multi-sample	Fingerprint
9	2006	Chen et al. [25]	x							Multi-sample	Fingerprint
10	2007	Jing et al. [32]	x					x			Face images and palm print
11	2008	Wang et al. [33]	x					x			Palm print and vein
12	2009	Abaza and Ross [138]				x				Multi-instance	Face and 4 fingers (index and thumb of the right and left hands)
13	2009	Monwar and Gavrilova [145]				x		x			Face, ear, and signature
14	2009	Kisku et al. [160]	x	x				x			Face and palmprint
15	2009	Ren et al. [93]			x					Multi-instance	Fingerprint
16	2009	Kisku et al. [96]			x			x			Face and ear
17	2009	Kisku et al. [97]			x					Multi-instance	Global and local (part of the face) features
18	2009	Ghouti and Bahjat [29]	x							Multi-sample	Iris
19	2010	Kumar et al. [155]					x				Palmprint and hand vein
20	2010	Kumar et al. [153]			x			x			Iris and palmprint; Face and speech; fingerprint and hand geometry
21	2010	Guru et al. [39]		x						Multi-instance	Finger Knuckle Print
22	2010	Choi et al. [27]	x							Multi-sample	Finger print and finger shape
23	2011	Kumar et al. [137]				x	x		x		Ear and iris
24	2011	Kumar and Shekhar [136]				x				Multi-sample	Palmprint
25	2011	Monwar and Gavrilova [140]				x		x			Face, ear, and iris
26	2011	Raghavendra et al. [52]		x	x					Multi-sensor	Visible and IR Face images
27	2011	Mohi-ud-din et al. [53]		x	x			x			Palm and fingerprint
28	2011	Hossain and Chetty [54]		x	x			x			Face and gait
29	2011	Kusuma and Chua [30]	x		x				x	Multi-sample	Face (the system can function in pixel level fusion or hybrid using both pixel level and score level)
30	2011	Mezai et al. [95]			x			x			Face and voice
31	2011	Meraoumia et al. [100]			x					Multi-sensor	Palmprint
32	2011	Meraoumia et al. [101]			x			x			Palmprint and Finger Knuckle Print
33	2011	Hanmandlu et al [102]			x			x			Palmprint, hand vein and hand geometry
34	2011	Xiuyan et al. [103]			x			x			Hand vein, iris and fingerprint
35	2011	Tran et al. [104]			x			x		Multi-algorithm	Fingerprint and face
36	2011	Meraoumia et al. [105]			x			x			Palmprint and FKP
37	2011	Liau and Isa [106]			x			x			Face and iris
38	2011	Kim et al [76]		x				x			Face and hand vein
39	2011	Kisku et al. [51]		x				x			Face and palmprint
40	2011	Jaisakthi and Aravindan [31]	x							Multi-algorithm	Face recognition
41	2012	Meraoumia et al. [35]	x		x			x			Fingerprint and FKP
42	2012	Hofmann et al. [132]			x			x			Face and gait
43	2012	Heenaye and Khan [107]			x					Multi-algorithm	Dorsal and palmar vein
44	2012	Poh et al. [128]			x			x			Face and fingerprint
45	2012	Anzar and Sathidevi [108]			x			x			Fingerprint and voice

Continued on next page

TABLE 10. *Continued.* **Multibiometric schemes summary.**

No	Year	Author	Decision level					Type			Traits
			Sensor	Feature	Score	Rank	Decision	Multi-modal	Hybrid	Other	
46	2012	Long et al. [46]		x				x			Fingerprint and face
47	2012	Almahafzah et al.[47]		x						Multi-algorithm	Finger Knuckle Print
48	2012	Kankrale and Sapkal [161]		x				x			Iris and fingerprint
49	2012	Gawande et al. [162].		x				x			Iris and fingerprint
50	2012	Gayathri and Ramamoorthy [55]		x				x			Palmprint and iris
51	2012	Bokade and Sapkal [56]		x				x			Face and palmprint
52	2012	Huang et al. [57]		x				x			Face and gait
53	2012	Almohammad et al. [58]		x				x			Face and gait
54	2012	Ben et al. [84]		x				x			Face and gait
55	2012	Yang and Zhang [59]		x				x			Finger and Finger-vein
56	2012	El-Alfy and BinMakhashen [60]		x				x			Face and hand geometry
57	2012	Fakhar et al. [123]									Face and iris
58	2013	Abdolahi et al. [158]					x	x			Fingerprint and iris
59	2013	Meraoumia et al. [125]		x	x					Multi-algorithm	2D and 3D palmprint
60	2013	Wang et al. [63]		x	x						Dual iris, visible and thermal Face
61	2013	Aoyama et al. [109]			x			x			Iris, face, palmprint, knuckle
62	2013	Vishi and Yayilgan [110]			x			x			Fingerprint and iris
63	2013	Indi and Raut [111]			x			x			Left thumb and left ear
64	2013	Anzar and Sathidevi [112]			x			x			Fingerprint and voice
65	2013	Satheesan et al. [113]			x					Multi-sample	Face
66	2013	Guan et al. [133]		x				x			Face and gait
67	2013	Gawande et al. [61]		x				x			Iris and fingerprint
68	2013	Gawande et al. [80]		x				x		Multi-algorithm	Iris and fingerprint (use two different extraction algorithms for both features)
69	2013	Huang et al. [62]		x				x			Face and ear
70	2014	Benaliouche and Touahria [159]					x	x		Multi-algorithm	Iris and fingerprint
71	2014	Rajbhoj and Mane [114]			x			x			Fingerprint and iris
72	2014	Peng et al [115]			x					Multi-algorithm	Finger vein, finger shape, FKP and fingerprint
73	2014	Sim et al. [127]			x			x			Face and periocular
74	2014	Miao et al. [64]		x				x			Eye and face
75	2014	Bhaskar and Veluchamy [50]		x				x			Palmprint and Finger Knuckle Print
76	2014	Paul et al. [156]					x	x			Face, ear, signature
77	2015	Azom et al. [163]		x	x		x			Multi-algorithm	Face and iris
78	2015	Kumar and Kumar [119]			x		x	x			Palmprint and iris,speech and face, face and fingerprint
79	2015	Gupta and Gupta [71]		x	x					Multi-algorithm	Palm-dorsa vein pattern
80	2015	Xu et al. [131]			x					Multi-instance	Left and right palmprint
81	2015	Perez et al [124]			x			x			Face, iris, palmprint and knuckle
82	2015	Nguyen et al. [99]			x			x		Multi-instance	Face, fingerprint (optical and thermal)
83	2015	Fakhar et al. [116]			x			x		Multi-instance	Face (two scores) and finger-print
84	2015	Nigam and Gupa [117]			x			x			FKP and palmprint
85	2015	Naveen and Moni [118]			x						Face texture and depth
86	2015	Assaad and Serpen [120]			x			x			Face and voice
87	2015	Gudavalli et al. [65]		x						Multi-algorithm	Fingerprint minutia and ridge
88	2015	Svoboda et al. [66]		x						Multi-algorithm	Contactless hand geometry
89	2015	Kanhangard et al. [67]		x						Multi-algorithm	Contactless hand geometry
90	2015	Ahmad et al. [68]		x				x			Face and palmprint
91	2015	Xing et al. [85]		x				x			Face and gait
92	2015	Derbel et al [69].		x				x			Face and gait
93	2015	Yan et al. [70]		x						Multi-sample	Palm-vein
94	2016	Liang et al [121]			x			x			Face and fingerprint

Table finished

- **Q15: What hardware and software is needed?** System operational requirements should be taken into consideration such as: the amount of hardware needed and configuration, storage capacity, processing necessities, software needed, backup and recovery, system operational hours etc. All of these have a huge impact on system cost.

VII. CONCLUSIONS

Due to advances in technology and the needs for more secure systems, multi-biometrics systems are becoming widely used. This paper gives an extensive overview on methods used for the fusion of multiple-biometric traits into a single authentication or identification decision. This is a useful reference for designers implementing new systems, especially in systems with resource constraints, such as embedded and mobile devices. We also discuss the security challenges of multi-biometric systems, including biometric spoofing, template security and use of biometrics for key generation. We highlight the ease with which biometric data could be obtained, sometimes in an unauthorised manner, using simple smartphone as sensor device. Finally, we briefly discuss some emerging areas in biometrics.

Our last section represents our proposal of an implementation blueprint, for a multi-biometric system. What questions should be answered when designing a biometric system, and where to find the information - we have included references to chapters from this extensive study.

APPENDIX A
SUMMARISING TABLE MULTI-BIOMETRIC FUSION

See Table 10.

REFERENCES

[1] D. E. Mordini, *Handbook of Global Bioethics*. Dordrecht, The Netherlands: Springer, 2014, pp. 505–526, doi: 10.1007/978-94-007-2512-6_101.

[2] C. H. Potter, G. P. Hancke, and B. J. Silva, "Machine-to-machine: Possible applications in industrial networks," in *Proc. IEEE Int. Conf. Ind. Technol. (ICIT)*, Feb. 2013, pp. 1321–1326.

[3] C. A. Opperman and G. P. Hancke, "Using NFC-enabled phones for remote data acquisition and digital control," in *Proc. AFRICON*, Sep. 2011, pp. 1–6.

[4] R. Serra, D. Knittel, P. Di Croce, and R. Peres, "Activity recognition with smart polymer floor sensor: Application to human footstep recognition," *IEEE Sensors J.*, vol. 16, no. 14, pp. 5757–5775, Jul. 2016.

[5] H. Ma *et al.*, "On-display transparent half-diamond pattern capacitive fingerprint sensor compatible with AMOLED display," *IEEE Sensors J.*, vol. 16, no. 22, pp. 8124–8131, Nov. 2016.

[6] L. Francis, G. Hancke, K. Mayes, and K. Markantonakis, "Potential misuse of NFC enabled mobile phones with embedded security elements as contactless attack platforms," in *Proc. Int. Conf. Internet Technol. Secured Trans. (ICITST)*, Nov. 2009, pp. 1–8.

[7] G. P. Hancke, K. Markantonakis, and K. Mayes, "Security challenges for user-oriented RFID applications within the 'Internet of Things,'" *J. Internet Technol.*, vol. 11, no. 3, pp. 307–313, 2010.

[8] EU. (2012). *Stork—What Is It?* [Online]. Available: https://www.eid-stork.eu/

[9] H. AlMahafzah and M. Z. AlRwashdeh. (2012). "A survey of multibiometric systems." [Online]. Available: https://arxiv.org/abs/1210.0829

[10] A. A. Ross, K. Nandakumar, and A. K. Jain, *Handbook of Multibiometrics* (International Series on Biometrics), vol. 6. Boston, MA, USA: Kluwer, 2006. [Online]. Available: http://link.springer.com/10.1007/0-387-33123-9

[11] N. K. Ratha, S. Chikkerur, J. H. Connell, and R. M. Bolle, "Generating cancelable fingerprint templates," *IEEE Trans. Pattern Anal. Mach. Intell.*, vol. 29, no. 4, pp. 561–572, Apr. 2007.

[12] A. Jain, S. Pankanti, S. Prabhakar, L. Hong, and A. Ross, "Biometrics: A grand challenge," in *Proc. 17th Int. Conf. Pattern Recognit. (ICPR)*, vol. 2. Aug. 2004, pp. 935–942.

[13] A. Ross and N. Poh, "Multibiometric systems: Overview, case studies, and open issues," in *Handbook of Remote Biometrics* (Advances in Pattern Recognition), M. Tistarelli, S. Z. Li, and R. Chellappa, Eds. London, U.K.: Springer, 2009, pp. 273–292.

[14] H. B. Mitchell, *Data Fusion: Concepts and Ideas*. Berlin, Germany: Springer, 2012. [Online]. Available: http://link.springer.com/10.1007/978-3-642-27222-6

[15] D. Bellot, A. Boyer, and F. Charpillet, "A new definition of qualified gain in a data fusion process: Application to telemedicine," in *Proc. 5th Int. Conf. Inf. Fusion*, vol. 2. Jul. 2002, pp. 865–872.

[16] C. Sanderson and K. K. Paliwal, "Information fusion and person verification using speech & face information," IDIAP Res. Inst., Martigny, Switzerland, Tech. Rep. Idiap-RR-33-2002, 2002.

[17] A. Ross and A. Jain, "Information fusion in biometrics," *Pattern Recognit. Lett.*, vol. 24, no. 13, pp. 2115–2125, 2003. [Online]. Available: http://www.sciencedirect.com/science/article/pii/S0167865503000795

[18] A. Ross, K. Nandakumar, and A. K. Jain, "Introduction to multibiometrics," in *Handbook of Biometrics*, A. K. Jain, P. Flynn, and A. Ross, Eds. New York, NY, USA: Springer, 2008, pp. 271–292.

[19] N. K. Ratha, J. H. Connell, and R. M. Bolle, "Image mosaicing for rolled fingerprint construction," in *Proc. 14th Int. Conf. Pattern Recognit.*, vol. 2. Aug. 1998, pp. 1651–1653.

[20] A. Jain and A. Ross, "Fingerprint mosaicking," in *Proc. IEEE Int. Conf. Acoust., Speech, Signal Process. (ICASSP)*, vol. 4. May 2002, pp. IV-4064–IV-4067.

[21] D. He, G. Rong, and J. Zhou, "Image mosaicing algorithm for rolled fingerprint construction," *Tsinghua Sci. Technol.*, vol. 7, no. 3, pp. 317–321, Jun. 2002.

[22] K. Choi, H.-S. Choi, and J. Kim, "Fingerprint mosaicking by rolling and sliding," in *Audio- and Video-Based Biometric Person Authentication*. Berlin, Germany: Springer, 2005, pp. 260–269.

[23] A. Ross, S. Dass, and A. Jain, "A deformable model for fingerprint matching," *Pattern Recognit.*, vol. 38, no. 1, pp. 95–103, 2005.

[24] Y.-L. Zhang, J. Yang, and H.-T. Wu, "A hybrid swipe fingerprint mosaicing scheme," in *Audio- and Video-Based Biometric Person Authentication*. Berlin, Germany: Springer, 2005, pp. 131–140.

[25] Y. Chen, G. Parziale, E. Diaz-Santana, and A. K. Jain, "3D touchless fingerprints: Compatibility with legacy rolled images," in *Proc. Biometrics Symp., Special Session Res. Biometric Consortium Conf.*, 2006, pp. 1–6.

[26] H. Choi, K. Choi, and J. Kim, "Mosaicing touchless and mirror-reflected fingerprint images," *IEEE Trans. Inf. Forensics Security*, vol. 5, no. 1, pp. 52–61, Mar. 2010.

[27] S. Shah, A. Ross, J. Shah, and S. Crihalmeanu, "Fingerprint mosaicing using thin plate splines," in *Proc. Biometric Consortium Conf.*, 2005, pp. 1–2.

[28] L. Ghouti and A. A. Bahjat, "Iris fusion for multibiometric systems," in *Proc. IEEE Int. Symp. Signal Process. Inf. Technol. (ISSPIT)*, Dec. 2009, pp. 248–253.

[29] G. P. Kusuma and C.-S. Chua, "PCA-based image recombination for multimodal 2D + 3D face recognition," *Image Vis. Comput.*, vol. 29, no. 5, pp. 306–316, Apr. 2011. [Online]. Available: http://www.sciencedirect.com/science/article/pii/S0262885610001599

[30] S. M. Jaisakthi and C. Aravindan, "Face detection using data and sensor fusion techniques," in *Proc. Int. Conf. Soft Comput. Pattern Recognit. (SoCPaR)*, Oct. 2011, pp. 274–279.

[31] X.-Y. Jing, Y.-F. Yao, D. Zhang, J.-Y. Yang, and M. Li, "Face and palmprint pixel level fusion and kernel DCV-RBF classifier for small sample biometric recognition," *Pattern Recognit.*, vol. 40, no. 11, pp. 3209–3224, Nov. 2007. [Online]. Available: http://www.sciencedirect.com/science/article/pii/S0031320307001033

[32] J.-G. Wang, W.-Y. Yau, A. Suwandy, and E. Sung, "Person recognition by fusing palmprint and palm vein images based on 'Laplacianpalm' representation," *Pattern Recognit.*, vol. 41, no. 5, pp. 1514–1527, May 2008. [Online]. Available: http://www.sciencedirect.com/science/article/pii/S0031320307004682

[33] B. Froba, C. Rothe, and C. Kublbeck, "Evaluation of sensor calibration in a biometric person recognition framework based on sensor fusion," in *Proc. 4th IEEE Int. Conf. Autom. Face Gesture Recognit.*, Mar. 2000, pp. 512–517.

[34] A. Meraoumia, S. Chitroub, and A. Bouridane, "Multimodal biometric person recognition system based on fingerprint & finger-knuckle-print using correlation filter classifier," in *Proc. IEEE Int. Conf. Commun. (ICC)*, Jun. 2012, pp. 820–824.

[35] A. Fatehpuria, D. L. Lau, and L. G. Hassebrook, "Acquiring a 2D rolled equivalent fingerprint image from a non-contact 3D finger scan," *Proc. SPIE*, vol. 6202, p. 62020C, Apr. 2006.

[36] F. Deravi *et al.*, "Multibiometrics and data fusion standardization," in *Encyclopedia of Biometrics*, S. Z. Li and A. K. Jain, Eds. New York, NY, USA: Springer, 2015, pp. 1133–1142.

[37] A. Ross, "An introduction to multibiometrics," in *Proc. 15th Eur. Signal Process. Conf.*, Sep. 2007, pp. 20–24.

[38] A. Rattani, B. Freni, G. L. Marcialis, and F. Roli, "Template update methods in adaptive biometric systems: A critical review," in *Advances in Biometrics* (Lecture Notes in Computer Science), vol. 5558, M. Tistarelli and M. S. Nixon, Eds. Berlin, Germany: Springer, Jun. 2009, pp. 847–856, doi: 10.1007/978-3-642-01793-3_86.

[39] D. S. Guru, K. B. Nagasundara, and S. Manjunath, "Feature level fusion of multi-instance finger knuckle print for person identification," in *Proc. 1st Int. Conf. Intell. Interact. Technol. Multimedia (IITM)*, 2010, pp. 186–190. [Online]. Available: http://doi.acm.org/10.1145/1963564.1963595

[40] A. Tahmasbi, F. Saki, H. Aghapanah, and S. B. Shokouhi, "A novel breast mass diagnosis system based on Zernike moments as shape and density descriptors," in *Proc. 18th Iranian Conf. Biomed. Eng. (ICBME)*, Dec. 2011, pp. 100–104.

[41] A. Tahmasbi, F. Saki, and S. B. Shokouhi, "Classification of benign and malignant masses based on Zernike moments," *Comput. Biol. Med.*, vol. 41, no. 8, pp. 726–735, Aug. 2011. [Online]. Available: http://www.sciencedirect.com/science/article/pii/S0010482511001296

[42] R. O. Duda, P. E. Hart, and D. G. Stork, *Pattern Classification*. Hoboken, NJ, USA: Wiley, Nov. 2012.

[43] X. Niyogi, "Locality preserving projections," in *Advances in Neural Information Processing Systems*, vol. 16. Cambridge, MA, USA: MIT Press, 2004, p. 153.

[44] M. Safayani, M. T. M. Shalmani, and M. Khademi, "Extended two-dimensional PCA for efficient face representation and recognition," in *Proc. 4th Int. Conf. Intell. Comput. Commun. Process. (ICCP)*, Aug. 2008, pp. 295–298.

[45] L. R. Veerabhadrappa, L. Rangarajan, and B. Shekar, "(2D)2LPP: A new dimensionality reduction technique with application to face/object representation and recognition," *Int. J. Syst., Cybern. Inform.*, pp. 17–22, Apr. 2009.

[46] T. B. Long, L. H. Thai, and T. Hanh, "Multimodal biometric person authentication using fingerprint, face features," in *PRICAI 2012: Trends in Artificial Intelligenc* (Lecture Notes in Computer Science), vol. 7458, P. Anthony, M. Ishizuka, and D. Lukose, Eds. Berlin, Germany: Springer, Sep. 2012, pp. 613–624.

[47] D. R. Kisku, P. Gupta, and J. K. Sing, "Multibiometrics feature level fusion by graph clustering," *Int. J. Secur. Appl.*, vol. 5, no. 2, pp. 61–74, 2011.

[48] R. Raghavendra, B. Dorizzi, A. Rao, and G. H. Kumar, "Particle swarm optimization based fusion of near infrared and visible images for improved face verification," *Pattern Recognit.*, vol. 44, no. 2, pp. 401–411, 2011. [Online]. Available: http://www.sciencedirect.com/science/article/pii/S0031320310003924

[49] S.-U.-D. G. Mohi-ud-Din, A. B. Mansoor, H. Masood, and M. Mumtaz, "Personal identification using feature and score level fusion of palm- and fingerprints," *Signal, Image Video Process.*, vol. 5, no. 4, pp. 477–483, Aug. 2011. [Online]. Available: http://link.springer.com/article/10.1007/s11760-011-0251-7

[50] E. Hossain and G. Chetty, "Multimodal face-gait fusion for biometric person authentication," in *Proc. IFIP 9th Int. Conf. Embedded Ubiquitous Comput. (EUC)*, Oct. 2011, pp. 332–337.

[51] H. AlMahafzah, M. Imran, and H. S. Sheshadri, "Multi-algorithm feature level fusion using finger knuckle print biometric," in *Computer Applications for Communication, Networking, and Digital Contents* (Communications in Computer and Information Science), vol. 350, T.-H. Kim, D.-S. Ko, T. Vasilakos, A. Stoica, and J. Abawajy, Eds. Berlin, Germany: Springer, 2012, pp. 302–311.

[52] R. Gayathri and P. Ramamoorthy, "Feature level fusion of palmprint and iris," *IJCSI Int. J. Comput. Sci. Issues*, vol. 9, no. 4, pp. 194–203, 2012.

[53] G. U. Bokade and A. M. Sapkal, "Feature level fusion of palm and face for secure recognition," *Int. J. Comput. Elect. Eng.*, vol. 4, no. 2, p. 157, 2012.

[54] Y. Huang, D. Xu, and F. Nie, "Patch distribution compatible semisupervised dimension reduction for face and human gait recognition," *IEEE Trans. Circuits Syst. Video Technol.*, vol. 22, no. 3, pp. 479–488, Mar. 2012.

[55] M. S. Almohammad, G. I. Salama, and T. A. Mahmoud, "Human identification system based on feature level fusion using face and gait biometrics," in *Proc. Int. Conf. Eng. Technol. (ICET)*, Oct. 2012, pp. 1–5.

[56] J. Yang and X. Zhang, "Feature-level fusion of fingerprint and finger-vein for personal identification," *Pattern Recognit. Lett.*, vol. 33, no. 5, pp. 623–628, Apr. 2012. [Online]. Available: http://www.sciencedirect.com/science/article/pii/S0167865511003771

[57] E.-S. M. El-Alfy and G. M. BinMakhashen, "Improved personal identification using face and hand geometry fusion and support vector machines," in *Networked Digital Technologies* (Communications in Computer and Information Science), vol. 294, R. Benlamri, Ed. Berlin, Germany: Springer, Apr. 2012, pp. 253–261. [Online]. Available: http://link.springer.com/chapter/10.1007/978-3-642-30567-2_21

[58] U. Gawande, M. Zaveri, and A. Kapur, "A novel algorithm for feature level fusion using SVM classifier for multibiometrics-based person identification," *Appl. Comput. Intell. Soft Comput.*, vol. 2013, Jun. 2013, Art. no. 515918. [Online]. Available: http://dx.doi.org/10.1155/2013/515918

[59] Z. Huang, Y. Liu, C. Li, M. Yang, and L. Chen, "A robust face and ear based multimodal biometric system using sparse representation," *Pattern Recognit.*, vol. 46, no. 8, pp. 2156–2168, Aug. 2013. [Online]. Available: http://www.sciencedirect.com/science/article/pii/S0031320313000599

[60] N. Wang, Q. Li, A. A. A. El-Latif, X. Yan, and X. Niu, "A novel hybrid multibiometrics based on the fusion of dual iris, visible and thermal face images," in *Proc. Int. Symp. Biometrics Secur. Technol. (ISBAST)*, Jul. 2013, pp. 217–223.

[61] D. Miao, Z. Sun, and Y. Huang, "Fusion of multibiometrics based on a new robust linear programming," in *Proc. 22nd Int. Conf. Pattern Recognit. (ICPR)*, Aug. 2014, pp. 291–296.

[62] B. Bhaskar and S. Veluchamy, "Hand based multibiometric authentication using local feature extraction," in *Proc. Int. Conf. Recent Trends Inf. Technol. (ICRTIT)*, Apr. 2014, pp. 1–5.

[63] M. Gudavalli, D. S. Kumar, and S. V. Raju, "A multibiometric fingerprint recognition system based on the fusion of minutiae and ridges," in *Emerging ICT for Bridging the Future—Proceedings of the 49th Annual Convention of the Computer Society of India)* (Advances in Intelligent Systems and Computing), vol. 337, S. C. Satapathy, A. Govardhan, K. S. Raju, and J. K. Mandal, Eds. Springer, 2015, pp. 231–237.

[64] J. Svoboda, M. Bronstein, and M. Drahansky, "Contactless biometric hand geometry recognition using a low-cost 3D camera," in *Proc. Int. Conf. Biometrics (ICB)*, May 2015, pp. 452–457.

[65] V. Kanhangad, A. Kumar, and D. Zhang, "Contactless and pose invariant biometric identification using hand surface," *IEEE Trans. Image Process.*, vol. 20, no. 5, pp. 1415–1424, May 2011.

[66] M. I. Ahmad, W. L. Woo, and S. Dlay, "Non-stationary feature fusion of face and palmprint multimodal biometrics," *Neurocomputing*, vol. 177, pp. 49–61, Feb. 2016. [Online]. Available: http://www.sciencedirect.com/science/article/pii/S0925231215016343

[67] A. Derbel, D. Vivet, and B. Emile, "Access control based on gait analysis and face recognition," *Electron. Lett.*, vol. 51, no. 10, pp. 751–752, 2015.

[68] X. Yan, W. Kang, F. Deng, and Q. Wu, "Palm vein recognition based on multi-sampling and feature-level fusion," *Neurocomputing*, vol. 151, pp. 798–807, Mar. 2015. [Online]. Available: http://www.sciencedirect.com/science/article/pii/S0925231214013587

[69] P. Gupta and P. Gupta, "Multi-modal fusion of palm-dorsa vein pattern for accurate personal authentication," *Knowl.-Based Syst.*, vol. 81, pp. 117–130, Jun. 2015. [Online]. Available: http://www.sciencedirect.com/science/article/pii/S0950705115000994

[70] D. J. Field, "Relations between the statistics of natural images and the response properties of cortical cells," *J. Opt. Soc. Amer. A, Opt. Image Sci.*, vol. 4, no. 12, pp. 2379–2394, 1987.

[71] V. Ojansivu and J. Heikkilä, "Blur insensitive texture classification using local phase quantization," in *Image and Signal Processing*. Berlin, Germany: Springer, 2008, pp. 236–243.

[72] M. Yang, L. Zhang, S. C.-K. Shiu, and D. Zhang, "Monogenic binary coding: An efficient local feature extraction approach to face recognition," *IEEE Trans. Inf. Forensics Security*, vol. 7, no. 6, pp. 1738–1751, Dec. 2012.

[73] R. Raghavendra, B. Dorizzi, A. Rao, and G. Hemantha, "PSO versus AdaBoost for feature selection in multimodal biometrics," in *Proc. IEEE 3rd Int. Conf. Biometrics, Theory, Appl., Syst. (BTAS)*, Sep. 2009, pp. 1–7.

[74] R. Raghavendra, B. Dorizzi, A. Rao, and G. H. Kumar, "Designing efficient fusion schemes for multimodal biometric systems using face and palmprint," *Pattern Recognit.*, vol. 44, no. 5, pp. 1076–1088, May 2011. [Online]. Available: http://www.sciencedirect.com/science/article/pii/S0031320310005352

[75] K. Roy and M. S. Kamel, "Multibiometric system using distance regularized level set method and particle swarm optimization," in *Computer Vision and Graphics* (Lecture Notes in Computer Science), vol. 7594, L. Bolc, R. Tadeusiewicz, L. J. Chmielewski, and K. Wojciechowski, Eds. Berlin, Germany: Springer, Sep. 2012, pp. 590–599.

[76] T.-C. Kim, K.-M. Kyung, and K. Bae, "New biometrics-acquisition method using time-of-flight depth camera," in *Proc. IEEE Int. Conf. Consumer Electron. (ICCE)*, Jan. 2011, pp. 721–722.

[77] S. M. S. Islam, R. Davies, M. Bennamoun, R. A. Owens, and A. S. Mian, "Multibiometric human recognition using 3D ear and face features," *Pattern Recognit.*, vol. 46, no. 3, pp. 613–627, Mar. 2013. [Online]. Available: http://www.sciencedirect.com/science/article/pii/S0031320312004220

[78] D. G. Lowe, "Object recognition from local scale-invariant features," in *Proc. IEEE Int. Conf. Comput. Vis.*, vol. 2. Sep. 1999, pp. 1150–1157.

[79] L. Kaufman and P. J. Rousseeuw, "Partitioning around medoids (program PAM)," in *Finding Groups in Data: An Introduction to Cluster Analysis*. Hoboken, NJ, USA: Wiley, 1990, pp. 68–125. [Online]. Available: http://onlinelibrary.wiley.com/doi/10.1002/9780470316801.ch2/summary

[80] U. Gawande, M. Zaveri, and A. Kapur, "Bimodal biometric system: Feature level fusion of iris and fingerprint," *Biometric Technol. Today*, vol. 2013, no. 2, pp. 7–8, 2013. [Online]. Available: http://www.sciencedirect.com/science/article/pii/S0969476513700353

[81] W. Xiong, K.-A. Toh, W.-Y. Yau, and X. Jiang, "Model-guided deformable hand shape recognition without positioning aids," *Pattern Recognit.*, vol. 38, no. 10, pp. 1651–1664, Oct. 2005. [Online]. Available: http://dx.doi.org/10.1016/j.patcog.2004.07.008

[82] S. Malassiotis, N. Aifanti, and M. G. Strintzis, "Personal authentication using 3-D finger geometry," *IEEE Trans. Inf. Forensics Security*, vol. 1, no. 1, pp. 12–21, Mar. 2006.

[83] V. Kanhangad, A. Kumar, and D. Zhang, "Combining 2D and 3D hand geometry features for biometric verification," in *Proc. IEEE Comput. Soc. Conf. Comput. Vis. Pattern Recognit. Workshops (CVPR Workshops)*, Jun. 2009, pp. 39–44.

[84] X. Y. Ben, M. Y. Jiang, Y. J. Wu, and W. X. Meng, "Gait feature coupling for low-resolution face recognition," *Electron. Lett.*, vol. 48, no. 9, pp. 488–489, Apr. 2012.

[85] X. Xing, K. Wang, and Z. Lv, "Fusion of gait and facial features using coupled projections for people identification at a distance," *IEEE Signal Process. Lett.*, vol. 22, no. 12, pp. 2349–2353, Dec. 2015.

[86] A. F. Abate, M. Nappi, D. Riccio, and G. Sabatino, "2D and 3D face recognition: A survey," *Pattern Recognit. Lett.*, vol. 28, no. 14, pp. 1885–1906, Oct. 2007. [Online]. Available: http://www.sciencedirect.com/science/article/pii/S0167865507000189

[87] B. Ulery, A. Hicklin, C. I. Watson, W. Fellner, and P. Hallinan, "Studies of biometric fusion," U.S. Dept. Commerce, Nat. Inst. Standards Technol., Gaithersburg, MD, USA, Tech. Rep. NISTIR 7346, 2006.

[88] K. Nandakumar, Y. Chen, S. C. Dass, and A. K. Jain, "Likelihood ratio-based biometric score fusion," *IEEE Trans. Pattern Anal. Mach. Intell.*, vol. 30, no. 2, pp. 342–347, Feb. 2008.

[89] A. Jain, K. Nandakumar, and A. Ross, "Score normalization in multimodal biometric systems," *Pattern Recognit.*, vol. 38, no. 12, pp. 2270–2285, Dec. 2005.

[90] M. Indovina, U. Uludag, R. Snelick, A. Mink, and A. Jain, "Multimodal biometric authentication methods: A COTS approach," in *Proc. MMUA*, 2003, pp. 99–106.

[91] D. R. Kisku, J. K. Sing, and P. Gupta, "Multibiometrics belief fusion," in *Proc. 2nd Int. Conf. Mach. Vis. (ICMV)*, Dec. 2009, pp. 37–40.

[92] D. R. Kisku, M. Tistarelli, J. K. Sing, and P. Gupta, "Face recognition by fusion of local and global matching scores using DS theory: An evaluation with uni-classifier and multi-classifier paradigm," in *Proc. IEEE Comput. Soc. Conf. Comput. Vis. Pattern Recognit. Workshops (CVPR Workshops)*, Jun. 2009, pp. 60–65.

[93] L. Mezai, F. Hachouf, and M. Bengherabi, "Score fusion of face and voice using Dempster–Shafer theory for person authentication," in *Proc. 11th Int. Conf. Intell. Syst. Design Appl. (ISDA)*, Nov. 2011, pp. 894–899.

[94] A. Meraoumia, S. Chitroub, and A. Bouridane, "2D and 3D palmprint information and hidden Markov model for improved identification performance," in *Proc. 11th Int. Conf. Intell. Syst. Design Appl. (ISDA)*, Nov. 2011, pp. 648–653.

[95] A. Meraoumia, S. Chitroub, and A. Bouridane, "Fusion of finger-knuckle-print and palmprint for an efficient multi-biometric system of person recognition," in *Proc. IEEE Int. Conf. Commun. (ICC)*, Jun. 2011, pp. 1–5.

[96] M. Hanmandlu, J. Grover, A. Gureja, and H. M. Gupta, "Score level fusion of multimodal biometrics using triangular norms," *Pattern Recognit. Lett.*, vol. 32, no. 14, pp. 1843–1850, Oct. 2011. [Online]. Available: http://www.sciencedirect.com/science/article/pii/S0167865511002133

[97] X. Li, C. Miao, T. Liu, and C. Yuan, "Theoretical analysis and experimental study on multimodal biometric," in *Proc. Int. Conf. Control, Autom. Syst. Eng. (CASE)*, Jul. 2011, pp. 1–4.

[98] Q. D. Tran, P. Liatsis, B. Zhu, and C. He, "An approach for multimodal biometric fusion under the missing data scenario," in *Proc. Int. Conf. Uncertainty Reason. Knowl. Eng. (URKE)*, vol. 1. Aug. 2011, pp. 185–188.

[99] A. Meraoumia, S. Chitroub, and A. Bouridane, "Palmprint and finger-knuckle-print for efficient person recognition based on Log–Gabor filter response," *Analog Integr. Circuits Signal Process.*, vol. 69, no. 1, pp. 17–27, Mar. 2011. [Online]. Available: http://link.springer.com/article/10.1007/s10470-011-9632-7

[100] H. F. Liau and D. Isa, "Feature selection for support vector machine-based face-iris multimodal biometric system," *Expert Syst. Appl.*, vol. 38, no. 9, pp. 11105–11111, Sep. 2011. [Online]. Available: http://www.sciencedirect.com/science/article/pii/S0957417411003794

[101] M. Heenaye and M. Khan, "A multimodal hand vein biometric based on score level fusion," *Procedia Eng.*, vol. 41, pp. 897–903, 2012. [Online]. Available: http://www.sciencedirect.com/science/article/pii/S1877705812026604

[102] S. M. Anzar and P. S. Sathidevi, "Multi-normalization: A new method for improving biometric fusion," in *Proc. Int. Conf. Adv. Comput., Commun. Inform. (ICACCI)*, New York, NY, USA, 2012, pp. 931–937. [Online]. Available: http://doi.acm.org/10.1145/2345396.2345546

[103] S. Aoyama, K. Ito, and T. Aoki, "Similarity measure using local phase features and its application to biometric recognition," in *Proc. IEEE Conf. Comput. Vis. Pattern Recognit. Workshops (CVPRW)*, Jun. 2013, pp. 180–187.

[104] K. Vishi and S. Y. Yayilgan, "Multimodal biometric authentication using fingerprint and iris recognition in identity management," in *Proc. 9th Int. Conf. Intell. Inf. Hiding Multimedia Signal Process.*, Oct. 2013, pp. 334–341.

[105] T. S. Indi and S. D. Raut, "Person identification based on multi-biometric characteristics," in *Proc. Int. Conf. Emerg. Trends Comput., Commun. Nanotechnol. (ICE-CCN)*, Mar. 2013, pp. 45–52.

[106] S. M. Anzar and P. S. Sathidevi, "Optimization of integration weights for a multibiometric system with score level fusion," in *Advances in Computing and Information Technology* (Advances in Intelligent Systems and Computing), vol. 177, N. Meghanathan, D. Nagamalai, and N. Chaki, Eds. Heidelberg, Germany: Springer, 2013, pp. 833–842.

[107] S. P. Satheesan, S. Tulyakov, and V. Govindaraju, "A feature information based approach for enhancing score-level fusion in multi-sample biometric systems," in *Proc. 4th Nat. Conf. Comput. Vis., Pattern Recognit., Image Process. Graph. (NCVPRIPG)*, Dec. 2013, pp. 1–4.

[108] S. M. Rajbhoj and P. B. Mane, "Match score integration of iris and fingerprint in multibiometrics system," in *Proc. Int. Conf. Electron. Commun. Syst. (ICECS)*, 2014, pp. 1–5.

[109] J. Peng, A. A. A. El-Latif, Q. Li, and X. Niu, "Multimodal biometric authentication based on score level fusion of finger biometrics," *Optik-Int. J. Light Electron Opt.*, vol. 125, no. 23, pp. 6891–6897, Dec. 2014. [Online]. Available: http://www.sciencedirect.com/science/article/pii/S0030402614007682

[110] K. Nguyen, S. Denman, S. Sridharan, and C. Fookes, "Score-level multibiometric fusion based on Dempster–Shafer theory incorporating uncertainty factors," *IEEE Trans. Human-Mach. Syst.*, vol. 45, no. 1, pp. 132–140, Feb. 2015.

[111] K. Fakhar, M. El Aroussi, M. N. Saidi, and D. Aboutajdine, "Biometric score fusion in identification model using the Choquet integral," in *Proc. Int. Conf. Elect. Inf. Technol. (ICEIT)*, Mar. 2015, pp. 233–236.

[112] A. Nigam and P. Gupta, "Designing an accurate hand biometric based authentication system fusing finger knuckleprint and palmprint," *Neurocomputing*, vol. 151, pp. 1120–1132, Mar. 2015. [Online]. Available: http://www.sciencedirect.com/science/article/pii/S092523121401340X

[113] S. Naveen and R. S. Moni, "Multimodal face recognition system using spectral transformation of 2D texture feature and statistical processing of face range images," *Procedia Comput. Sci.*, vol. 46, pp. 1537–1545, 2015. [Online]. Available: http://www.sciencedirect.com/science/article/pii/S1877050915001428

[114] A. Kumar and A. Kumar, "Adaptive management of multimodal biometrics fusion using ant colony optimization," *Inf. Fusion*, vol. 32, pp. 49–63, Nov. 2015. [Online]. Available: http://www.sciencedirect.com/science/article/pii/S1566253515000858

[115] F. S. Assaad and G. Serpen, "Transformation based score fusion algorithm for multi-modal biometric user authentication through ensemble classification," *Procedia Comput. Sci.*, vol. 61, pp. 410–415, 2015. [Online]. Available: http://www.sciencedirect.com/science/article/pii/S1877050915030057

[116] Y. Liang, X. Ding, C. Liu, and J.-H. Xue, "Combining multiple biometric traits with an order-preserving score fusion algorithm," *Neurocomputing*, vol. 171, pp. 252–261, Jan. 2016. [Online]. Available: http://www.sciencedirect.com/science/article/pii/S0925231215008802

[117] G. Shafer, *A Mathematical Theory of Evidence*, vol. 1. Princeton, NJ, USA: Princeton Univ. Press, 1976.

[118] K. Sentz and S. Ferson, *Combination of Evidence in Dempster–Shafer Theory*, vol. 4015. 2002.

[119] X. Ren, J. Yang, H. Li, and R. Wu, "Multi-fingerprint information fusion for personal identification based on improved Dempster–Shafer evidence theory," in *Proc. Int. Conf. Electron. Comput. Technol.*, 2009, pp. 281–285.

[120] M. H. Mahoor and M. Abdel-Mottaleb, "A multimodal approach for face modeling and recognition," *IEEE Trans. Inf. Forensics Security*, vol. 3, no. 3, pp. 431–440, Sep. 2008.

[121] M. Arif, T. Brouard, and N. Vincent, "A fusion methodology based on Dempster–Shafer evidence theory for two biometric applications," in *Proc. 18th Int. Conf. Pattern Recognit. (ICPR)*, vol. 4. 2006, pp. 590–593.

[122] V. Conti, G. Milici, P. Ribino, F. Sorbello, and S. Vitabile, "Fuzzy fusion in multimodal biometric systems," in *Knowledge-Based Intelligent Information and Engineering Systems* (Lecture Notes in Computer Science), vol. 4692, B. Apolloni, R. J. Howlett, and L. Jain, Eds. Heidelberg, Germany: Springer, Sep. 2007, pp. 108–115.

[123] K. Fakhar, M. El Aroussi, M. N. Saidi, and D. Aboutajdine, "Score fusion in multibiometric identification based on fuzzy set theory," in *Image and Signal Processing* (Lecture Notes in Computer Science), vol. 7340, A. Elmoataz, D. Mammass, O. Lezoray, F. Nouboud, and D. Aboutajdine, Eds. Heidelberg, Germany: Springer, Jun. 2012, pp. 261–268.

[124] L. R. M. Pérez, S. Aoyama, K. Ito, and T. Aoki, "Score level fusion of multibiometrics using local phase array," in *Advances in Multimedia Information Processing—PCM* (Lecture Notes in Computer Science), vol. 9315, Y. S. Ho, J. Sang, Y. Ro, J. Kim, and F. Wu, Eds. Heidelberg, Germany: Springer, 2015, pp. 215–224.

[125] A. Meraoumia, S. Chitroub, and A. Bouridane, "2D and 3D palmprint information, PCA and HMM for an improved person recognition performance," *Integr. Comput.-Aided Eng.*, vol. 20, no. 3, pp. 303–319, Jul. 2013. [Online]. Available: http://dx.doi.org/10.3233/ICA-130431

[126] A. Alford *et al.*, "GEC-based multi-biometric fusion," in *Proc. IEEE Congr. Evol. Comput. (CEC)*, Jun. 2011, pp. 2071–2074.

[127] H. M. Sim, H. Asmuni, R. Hassan, and R. M. Othman, "Multimodal biometrics: Weighted score level fusion based on non-ideal iris and face images," *Expert Syst. Appl.*, vol. 41, no. 11, pp. 5390–5404, Sep. 2014. [Online]. Available: http://www.sciencedirect.com/science/article/pii/S0957417414001316

[128] N. Poh and J. Kittler, "A unified framework for biometric expert fusion incorporating quality measures," *IEEE Trans. Pattern Anal. Mach. Intell.*, vol. 34, no. 1, pp. 3–18, Jan. 2012.

[129] J. Fierrez-Aguilar, "Adapted fusion schemes for multimodal biometric authentication," Ph.D. dissertation, Techn. Univ. Madrid, Madrid, Spain, 2006.

[130] J. Fierrez-Aguilar, Y. Chen, J. Ortega-Garcia, and A. K. Jain, "Incorporating image quality in multi-algorithm fingerprint verification," in *Advances in Biometrics*. Heidelberg, Germany: Springer, 2006, pp. 213–220. [Online]. Available: http://link.springer.com/chapter/10.1007/11608288_29, doi: 10.1007/11608288_29.

[131] Y. Xu, L. Fei, and D. Zhang, "Combining left and right palmprint images for more accurate personal identification," *IEEE Trans. Image Process.*, vol. 24, no. 2, pp. 549–559, Feb. 2015.

[132] M. Hofmann, S. M. Schmidt, A. N. Rajagopalan, and G. Rigoll, "Combined face and gait recognition using alpha matte preprocessing," in *Proc. 5th IAPR Int. Conf. Biometrics (ICB)*, Mar. 2012, pp. 390–395.

[133] Y. Guan, X. Wei, C.-T. Li, G. L. Marcialis, F. Roli, and M. Tistarelli, "Combining gait and face for tackling the elapsed time challenges," in *Proc. IEEE 6th Int. Conf. Biometrics, Theory, Appl. Syst. (BTAS)*, Sep./Oct. 2013, pp. 1–8.

[134] T. K. Ho, J. J. Hull, and S. N. Srihari, "Decision combination in multiple classifier systems," *IEEE Trans. Pattern Anal. Mach. Intell.*, vol. 16, no. 1, pp. 66–75, Jan. 1994.

[135] K. Nandakumar, A. K. Jain, and A. Ross, "Fusion in multibiometric identification systems: What about the missing data?" in *Advances in Biometrics* (Lecture Notes in Computer Science), vol. 5558, M. Tistarelli and M. S. Nixon, Eds. Heidelberg, Germany: Springer, Jun. 2009, pp. 743–752, doi: 10.1007/978-3-642-01793-3_76.

[136] A. Kumar and S. Shekhar, "Personal identification using multibiometrics rank-level fusion," *IEEE Trans. Syst., Man, Cybern. C, Appl. Rev.*, vol. 41, no. 5, pp. 743–752, Sep. 2011.

[137] A. Kumar, M. Hanmandlu, V. Sharma, and H. M. Gupta, "Rank based hybrid multimodal fusion using PSO," in *Swarm, Evolutionary, and Memetic Computing* (Lecture Notes in Computer Science), vol. 7076, B. K. Panigrahi, P. N. Suganthan, S. Das, and S. C. Satapathy, Eds. Heidelberg, Germany: Springer, Dec. 2011, pp. 217–224. [Online]. Available: http://link.springer.com/chapter/10.1007/978-3-642-27172-4_27

[138] A. Abaza and A. Ross, "Quality based rank-level fusion in multibiometric systems," in *Proc. IEEE 3rd Int. Conf. Biometrics, Theory, Appl., Syst. (BTAS)*, Sep. 2009, pp. 1–6.

[139] E. Marasco, A. Abaza, L. Lugini, and B. Cukic, "Impact of biometric data quality on rank-level fusion schemes," in *Algorithms and Architectures for Parallel Processing* (Lecture Notes in Computer Science), vol. 8286, R. Aversa, J. Kołodziej, J. Zhang, F. Amato, and G. Fortino, Eds. Heidelberg, Germany: Springer, Dec. 2013, pp. 209–216.

[140] M. M. Monwar and M. Gavrilova, "Markov chain model for multimodal biometric rank fusion," *Signal, Image Video Process.*, vol. 7, no. 1, pp. 137–149, Apr. 2011. [Online]. Available: http://link.springer.com/article/10.1007/s11760-011-0226-8

[141] K. Sigman. (2009). "Lecture notes on stochastic modeling I, introduction to discrete-time Markov chains I," Dept. Ind. Eng. Oper. Res., School Eng. Appl. Sci. Columbia Univ., New York, NY, USA, Tech. Rep. [Online]. Available: http://www.columbia.edu/~ks20/stochastic-I/stochastic-I-MCI.pdf

[142] S. Garcia-Salicetti, M. A. Mellakh, L. Allano, and B. Dorizzi, "Multimodal biometric score fusion: The mean rule vs. support vector classifiers," in *Proc. 13th Eur. Signal Process. Conf.*, Sep. 2005, pp. 1–4.

[143] A. Kumar and D. Zhang, "Palmprint authentication using multiple classifiers," *Proc. SPIE*, vol. 5404, pp. 20–29, Aug. 2004. [Online]. Available: http://dx.doi.org/10.1117/12.542764

[144] K. Nandakumar, A. Ross, and A. K. Jain, "Incorporating ancillary information in multibiometric systems," in *Handbook of Biometrics*. Springer, 2008, pp. 335–355. [Online]. Available: http://www.springer.com/gp/book/9780387710402#otherversion=9781441943750

[145] M. M. Monwar and M. L. Gavrilova, "Multimodal biometric system using rank-level fusion approach," *IEEE Trans. Syst., Man, Cybern. B, Cybern.*, vol. 39, no. 4, pp. 867–878, Aug. 2009.

[146] J. Daugman, "Combining multiple biometrics," Comput. Lab., Univ. Cambridge, Cambridge, U.K., Tech. Rep., 2000.

[147] Q. Tao and R. Veldhuis, "Threshold-optimized decision-level fusion and its application to biometrics," *Pattern Recognit.*, vol. 42, no. 5, pp. 823–836, May 2009.

[148] L. Lam and C. Y. Suen, "Application of majority voting to pattern recognition: An analysis of its behavior and performance," *IEEE Trans. Syst., Man, Cybern. A, Syst., Humans*, vol. 27, no. 5, pp. 553–568, Sep. 1997. [Online]. Available: http://www.sciencedirect.com/science/article/pii/S0031320301001030
[149] L. I. Kuncheva, *Combining Pattern Classifiers: Methods and Algorithms*. Hoboken, NJ, USA: Wiley, 2004.
[150] S. Prabhakar and A. K. Jain, "Decision-level fusion in fingerprint verification," *Pattern Recognit.*, vol. 35, no. 4, pp. 861–874, 2002.
[151] K. Veeramachaneni, L. Osadciw, A. Ross, and N. Srinivas, "Decision-level fusion strategies for correlated biometric classifiers," in *Proc. IEEE Comput. Soc. Conf. Comput. Vis. Pattern Recognit. Workshops (CVPRW)*, Jun. 2008, pp. 1–6.
[152] M. Hanmandlu, A. Kumar, V. K. Madasu, and P. Yarlagadda, "Fusion of hand based biometrics using particle swarm optimization," in *Proc. 5th Int. Conf. Inf. Technol., New Generat. (ITNG)*, Apr. 2008, pp. 783–788.
[153] A. Kumar, V. Kanhangad, and D. Zhang, "A new framework for adaptive multimodal biometrics management," *IEEE Trans. Inf. Forensics Security*, vol. 5, no. 1, pp. 92–102, Mar. 2010.
[154] K. Veeramachaneni, L. A. Osadciw, and P. K. Varshney, "An adaptive multimodal biometric management algorithm," *IEEE Trans. Syst., Man, Cybern. C, Appl. Rev.*, vol. 35, no. 3, pp. 344–356, Aug. 2005.
[155] A. Kumar, M. Hanmandlu, H. Sanghvi, and H. M. Gupta, "Decision level biometric fusion using ant colony optimization," in *Proc. 17th IEEE Int. Conf. Image Process. (ICIP)*, Sep. 2010, pp. 3105–3108.
[156] P. P. Paul, M. L. Gavrilova, and R. Alhajj, "Decision fusion for multimodal biometrics using social network analysis," *IEEE Trans. Syst., Man, Cybern., Syst.*, vol. 44, no. 11, pp. 1522–1533, Nov. 2014.
[157] C. W. Lau, B. Ma, H. M. Meng, Y. S. Moon, and Y. Yam, "Fuzzy logic decision fusion in a multimodal biometric system," in *Proc. INTERSPEECH*, 2004, pp. 1–4.
[158] M. Abdolahi, M. Mohamadi, and M. Jafari, "Multimodal biometric system fusion using fingerprint and iris with fuzzy logic," *Int. J. Soft Comput. Eng.*, vol. 2, no. 6, pp. 504–510, 2013.
[159] H. Benaliouche and M. Touahria, "Comparative study of multimodal biometric recognition by fusion of iris and fingerprint," *Sci. World J.*, vol. 2014, Jan. 2014, Art. no. 829369. [Online]. Available: http://www.hindawi.com/journals/tswj/2014/829369/abs/ and http://www.hindawi.com/journals/tswj/2014/829369/abs/
[160] D. R. Kisku, J. K. Sing, M. Tistarelli, and P. Gupta, "Multisensor biometric evidence fusion for person authentication using wavelet decomposition and monotonic-decreasing graph," in *Proc. 7th Int. Conf. Adv. Pattern Recognit. (ICAPR)*, 2009, pp. 205–208.
[161] R. N. Kankrale and S. D. Sapkal, "Template level concatenation of iris and fingerprint in multimodal biometric identification systems," *Int. J. Electron., Commun. Soft Comput. Sci. Eng.*, pp. 29–36, May 2012.
[162] U. Gawande, S. R. Nair, H. Balani, N. Pawar, and M. Kotpalliwar, "A high speed frequency based multimodal biometric system using iris and fingerprint," *Int. J. Adv. Comput. Eng. Commun. Technol.*, vol. 1, no. 2, pp. 66–73, 2012.
[163] V. Azom, A. Adewumi, and J.-R. Tapamo, "Face and iris biometrics person identification using hybrid fusion at feature and score-level," in *Proc. Pattern Recognit. Assoc. South Africa Robot. Mechatronics Int. Conf. (PRASA-RobMech)*, Nov. 2015, pp. 207–212.
[164] E. Marasco and C. Sansone, "An experimental comparison of different methods for combining biometric identification systems," in *Image Analysis and Processing—ICIAP* (Lecture Notes in Computer Science), vol. 6979, G. Maino and G. L. Foresti, Eds. Heidelberg, Germany: Springer, Sep. 2011, pp. 255–264. [Online]. Available: http://link.springer.com/chapter/10.1007/978-3-642-24088-1_27
[165] N. K. Ratha, J. H. Connell, and R. M. Bolle, "Enhancing security and privacy in biometrics-based authentication systems," *IBM Syst. J.*, vol. 40, no. 3, pp. 614–634, Apr. 2001.
[166] T. Matsumoto, H. Matsumoto, K. Yamada, and S. Hoshino, "Impact of artificial 'gummy' fingers on fingerprint systems," *Proc. SPIE*, vol. 4677, pp. 275–289, Apr. 2002. [Online]. Available: http://dx.doi.org/10.1117/12.462719
[167] M. Espinoza, C. Champod, and P. Margot, "Vulnerabilities of fingerprint reader to fake fingerprints attacks," *Forensic Sci. Int.*, vol. 204, nos. 1–3, pp. 41–49, Jan. 2011. [Online]. Available: http://www.sciencedirect.com/science/article/pii/S0379073810002331
[168] J. Galbally *et al.*, "An evaluation of direct attacks using fake fingers generated from ISO templates," *Pattern Recognit. Lett.*, vol. 31, no. 8, pp. 725–732, Jun. 2010. [Online]. Available: http://www.sciencedirect.com/science/article/pii/S0167865509002669
[169] R. Cappelli, D. Maio, A. Lumini, and D. Maltoni, "Fingerprint image reconstruction from standard templates," *IEEE Trans. Pattern Anal. Mach. Intell.*, vol. 29, no. 9, pp. 1489–1503, Sep. 2007.
[170] J. Galbally-Herrero, J. Fierrez-Aguilar, J. D. Rodriguez-Gonzalez, F. Alonso-Fernandez, J. Ortega-Garcia, and M. Tapiador, "On the vulnerability of fingerprint verification systems to fake fingerprints attacks," in *Proc. 40th Annu. IEEE Int. Carnahan Conf. Secur. Technol.*, Oct. 2006, pp. 130–136.
[171] D. Baldisserra, A. Franco, D. Maio, and D. Maltoni, "Fake fingerprint detection by odor analysis," in *Advances in Biometrics* (Lecture Notes in Computer Science), vol. 3832, D. Zhang and A. K. Jain, Eds. Berlin, Germany: Springer, Jan. 2006, pp. 265–272, [Online]. Available: http://link.springer.com/chapter/10.1007/11608288_36
[172] G. Marcialis, F. Roli, and A. Tidu, "Analysis of fingerprint pores for vitality detection," in *Proc. 20th Int. Conf. Pattern Recognit. (ICPR)*, Aug. 2010, pp. 1289–1292.
[173] G. L. Marcialis *et al.*, "First international fingerprint liveness detection competition—LivDet 2009," in *Image Analysis and Processing—ICIAP 2009* (Lecture Notes in Computer Science), vol. 5716, P. Foggia, C. Sansone, and M. Vento, Eds. Berlin, Germany: Springer, Sep. 2009, pp. 12–23. [Online]. http://link.springer.com/chapter/10.1007/978-3-642-04146-4_4
[174] V. Ruiz-Albacete, P. Tome-Gonzalez, F. Alonso-Fernandez, J. Galbally, J. Fierrez, and J. Ortega-Garcia, "Direct attacks using fake images in iris verification," in *Biometrics Identity Management* (Lecture Notes in Computer Science), vol. 5372, B. Schouten, N. C. Juul, A. Drygajlo, and M. Tistarelli, Eds. Berlin, Germany: Springer, May 2008, pp. 181–190. [Online]. Available: http://link.springer.com/chapter/10.1007/978-3-540-89991-4_19, doi: 10.1007/978-3-540-89991-4_19.
[175] R. Bodade and S. Talbar, "Dynamic iris localisation: A novel approach suitable for fake iris detection," in *Proc. Int. Conf. Ultra Modern Telecommun. Workshops (ICUMT)*, Oct. 2009, pp. 1–5.
[176] Z. Wei, X. Qiu, Z. Sun, and T. Tan, "Counterfeit iris detection based on texture analysis," in *Proc. 19th Int. Conf. Pattern Recognit. (ICPR)*, Dec. 2008, pp. 1–4.
[177] X. He, Y. Lu, and P. Shi, "A fake iris detection method based on FFT and quality assessment," in *Proc. Chin. Conf. Pattern Recognit. (CCPR)*, Oct. 2008, pp. 1–4.
[178] M. Kanematsu, H. Takano, and K. Nakamura, "Highly reliable liveness detection method for iris recognition," in *Proc. Ann. Conf. (SICE)*, Sep. 2007, pp. 361–364.
[179] E. C. Lee, K. R. Park, and J. Kim, "Fake iris detection by using purkinje image," in *Advances in Biometrics* (Lecture Notes in Computer Science), vol. 3832, D. Zhang and A. K. Jain, Eds. Berlin, Germany: Springer, Jan. 2006, pp. 397–403. [Online]. Available: http://link.springer.com/chapter/10.1007/11608288_53, doi: 10.1007/11608288_53.
[180] I. Rigas and O. V. Komogortsev, "Eye movement-driven defense against iris print-attacks," *Pattern Recognit. Lett.*, vol. 68, pp. 316–326, Dec. 2015. [Online]. Available: http://www.sciencedirect.com/science/article/pii/S0167865515001737
[181] T. D. F. Pereira *et al.*, "Face liveness detection using dynamic texture," *EURASIP J. Image Video Process.*, vol. 2014, no. 1, pp. 1–15, Jan. 2014. [Online]. Available: http://link.springer.com/article/10.1186/1687-5281-2014-2
[182] J. Komulainen, A. Hadid, M. Pietikainen, A. Anjos, and S. Marcel, "Complementary countermeasures for detecting scenic face spoofing attacks," in *Proc. Int. Conf. Biometrics (ICB)*, Jun. 2013, pp. 1–7.
[183] J. Komulainen, A. Hadid, and M. Pietikäinen, "Face spoofing detection using dynamic texture," in *Computer Vision - ACCV 2012 Workshops* (Lecture Notes in Computer Science), vol. 7728, J.-I. Park and J. Kim, Eds. Berlin, Germany: Springer, Nov. 2012, pp. 146–157. [Online]. Available: http://link.springer.com/chapter/10.1007/978-3-642-37410-4_13, doi: 10.1007/978-3-642-37410-4_13.
[184] J. Yan, Z. Zhang, Z. Lei, D. Yi, and S. Li, "Face liveness detection by exploring multiple scenic clues," in *Proc. 12th Int. Conf. Control Autom. Robot. Vis. (ICARCV)*, Dec. 2012, pp. 188–193.
[185] G. Kim, S. Eum, J. K. Suhr, D. I. Kim, K. R. Park, and J. Kim, "Face liveness detection based on texture and frequency analyses," in *Proc. 5th Int. Conf. Biometrics (ICB)*, Mar. 2012, pp. 67–72.

[186] Y. Kim, J.-H. Yoo, and K. Choi, "A motion and similarity-based fake detection method for biometric face recognition systems," *IEEE Trans. Consum. Electron.*, vol. 57, no. 2, pp. 756–762, May 2011.

[187] J. Maatta, A. Hadid, and M. Pietikainen, "Face spoofing detection from single images using micro-texture analysis," in *Proc. Int. Joint Conf. Biometrics (IJCB)*, Oct. 2011, pp. 1–7.

[188] H.-K. Jee, S.-U. Jung, and J.-H. Yoo, "Liveness detection for embedded face recognition system," *Int. J. Biol. Med. Sci.*, vol. 1, no. 4, pp. 235–238, 2006.

[189] J. Li, Y. Wang, T. Tan, and A. K. Jain, "Live face detection based on the analysis of Fourier spectra," *Proc. SPIE*, vol. 5404, pp. 296–303, Aug. 2004. [Online]. Available: http://dx.doi.org/10.1117/12.541955

[190] Z. Zhang, J. Yan, S. Liu, Z. Lei, D. Yi, and S. Li, "A face antispoofing database with diverse attacks," in *Proc. 5th Int. Conf. Biometrics (IAPR)*, Mar. 2012, pp. 26–31.

[191] B. Miller, "Vital signs of identity [biometrics]," *IEEE Spectr.*, vol. 31, no. 2, pp. 22–30, Feb. 1994.

[192] D. Sims, "Biometric recognition: Our hands, eyes, and faces give us away," *IEEE Comput. Graph. Appl.*, vol. 14, no. 5, pp. 14–15, Sep. 1994.

[193] H. Chen, H. Valizadegan, C. Jackson, S. Soltysiak, and A. K. Jain, "Fake hands: Spoofing hand geometry systems," *Biometric Consortium*, Washington, DC, USA, 2005. [Online]. Available: https://pdfs.semanticscholar.org/d86f/4a1fec35901a0017e7517cb43f584fdb7c0b.pdf

[194] F. Alegre, R. Vipperla, N. Evans, and B. Fauve, "On the vulnerability of automatic speaker recognition to spoofing attacks with artificial signals," in *Proc. 20th Eur. Signal Process. Conf. (EUSIPCO)*, Aug. 2012, pp. 36–40.

[195] D. Gafurov, E. Snekkenes, and P. Bours, "Spoof attacks on gait authentication system," *IEEE Trans. Inf. Forensics Security*, vol. 2, no. 3, pp. 491–502, Sep. 2007.

[196] R. N. Rodrigues, N. Kamat, and V. Govindaraju, "Evaluation of biometric spoofing in a multimodal system," in *Proc. 4th IEEE Int. Conf. Biometrics Theory Appl. Syst. (BTAS)*, Sep. 2010, pp. 1–5.

[197] Z. Akhtar and N. Alfarid, "Robustness of serial and parallel biometric fusion against spoof attacks," in *Computer Networks and Intelligent Computing* (Communications in Computer and Information Science), vol. 157, K. R. Venugopal and L. M. Patnaik, Eds. Berlin, Germany: Springer, 2011, pp. 217–225. [Online]. Available: http://link.springer.com/chapter/10.1007/978-3-642-22786-8_27

[198] Z. Akhtar and S. Kale, "Security analysis of multimodal biometric systems against spoof attacks," in *Advances in Computing and Communications* (Communications in Computer and Information Science), vol. 191, A. Abraham, J. L. Mauri, J. F. Buford, J. Suzuki, and S. M. Thampi, Eds. Berlin, Germany: Springer, Jul. 2011 pp. 604–611. [Online]. Available: http://link.springer.com/chapter/10.1007/978-3-642-22714-1_62

[199] Z. Akhtar, S. Kale, and N. Alfarid, "Spoof attacks on multimodal biometric systems," in *Proc. Int. Conf. Inf. Netw. Technol. (IPCSIT)*, vol. 4. 2011, pp. 46–51.

[200] M. Gomez-Barrero, J. Galbally, and J. Fierrez, "Efficient software attack to multimodal biometric systems and its application to face and iris fusion," *Pattern Recognit. Lett.*, vol. 36, pp. 243–253, Jan. 2014. [Online]. Available: http://www.sciencedirect.com/science/article/pii/S0167865513001876

[201] E. Marasco, P. Johnson, C. Sansone, and S. Schuckers, "Increase the security of multibiometric systems by incorporating a spoofing detection algorithm in the fusion mechanism," in *Multiple Classifier Systems* (Lecture Notes in Computer Science), vol. 6713, C. Sansone, J. Kittler, and F. Roli, Eds. Berlin, Germany: Springer, Jun. 2011, pp. 309–318. [Online]. Available: http://link.springer.com/chapter/10.1007/978-3-642-21557-5_33

[202] L. Marfella, E. Marasco, and C. Sansone, "Liveness-based fusion approaches in multibiometrics," in *Proc. IEEE Workshop Biometric Meas. Syst. Secur. Med. Appl. (BIOMS)*, Sep. 2012, pp. 1–7.

[203] P. Wild, P. Radu, L. Chen, and J. Ferryman, "Robust multimodal face and fingerprint fusion in the presence of spoofing attacks," *Pattern Recognit.*, vol. 50, pp. 17–25, Sep. 2016. [Online]. Available: http://www.sciencedirect.com/science/article/pii/S0031320315002952

[204] M. Cornett, "Can liveness detection defeat the m-commerce hackers?" *Biometric Technol. Today*, vol. 2015, no. 10, pp. 9–11, Oct. 2015. [Online]. Available: http://www.sciencedirect.com/science/article/pii/S0969476515301570

[205] M. Sparkes. (2015). *Why Your Smartphone Records Everything You Say to it*. [Online]. Available: http://www.telegraph.co.uk/technology/news/11434754/Why-your-smartphone%-records-everything-you-say-to-it.html

[206] C. Matyszczyk. (2015). *Samsung's Warning: Our Smart TVs Record Your Living Room Chatter*. [Online]. Availabel: http://www.cnet.com/news/samsungs-warning-our-smart-tvs-record-your-liv%ing-room-chatter/

[207] A. P. Felt, E. Chin, S. Hanna, D. Song, and D. Wagner, "Android permissions demystified," in *Proc. 18th ACM Conf. Comput. Commun. Secur.*, New York, NY, USA: 2011, pp. 627–638. [Online]. Available: http://doi.acm.org/10.1145/2046707.2046779

[208] J. Han *et al.*, "Launching generic attacks on ios with approved third-party applications," in *Applied Cryptography and Network Security* (Lecture Notes in Computer Science), vol. 7954, M. Jacobson, M. Locasto, P. Mohassel, and R. Safavi-Naini, Eds. Berlin, Germany: Springer, Jun. 2013, pp. 272–289, [Online]. Available: http://link.springer.com/chapter/10.1007/978-3-642-38980-1_17, doi: 10.1007/978-3-642-38980-1_17.

[209] Z. Labs. (2012). *10% of Mobile Apps Leak Passwords, 40% Communicate With Third Parties | Cloud Security Solutions | Zscaler*. [Online]. Available: https://www.zscaler.com/press/10-mobile-apps-leak-passwords-40-communic%ate-third-parties

[210] Y. Zhou and X. Jiang, "Dissecting android malware: Characterization and evolution," in *Proc. IEEE Symp. Secur. Privacy (SP)*, May 2012, pp. 95–109.

[211] T. Fiebig, J. Krissler, and R. Hänsch, "Security impact of high resolution smartphone cameras," in *Proc. 8th USENIX Conf. Offensive Technol.*, Berkeley, CA, USA, 2014, p. 15. [Online]. Available: http://dl.acm.org/citation.cfm?id=2671293.2671308

[212] W. Meng, D. Wong, S. Furnell, and J. Zhou, "Surveying the development of biometric user authentication on mobile phones," *IEEE Commun. Surveys Tuts.*, vol. 17, no. 3, pp. 1268–1293, 3rd Quart., 2015.

[213] Y. Zhang, P. Xia, J. Luo, Z. Ling, B. Liu, and X. Fu, "Fingerprint attack against touch-enabled devices," in *Proc. 2nd ACM Workshop Secur. Privacy Smartphones Mobile Devices*, New York, NY, USA, 2012, pp. 57–68. [Online]. Available: http://doi.acm.org/10.1145/2381934.2381947

[214] N. Duc and B. Minh, "Your face is NOT your password," in *Proc. Black Hat Conf.*, vol. 1. 2009, pp. 1–40.

[215] Y. Li, K. Xu, Q. Yan, Y. Li, and R. H. Deng, "Understanding OSN-based facial disclosure against face authentication systems," in *Proc. 9th ACM Symp. Inf. Comput. Commun. Secur.*, New York, NY, USA, 2014, pp. 413–424. [Online]. Available: http://doi.acm.org/10.1145/2590296.2590315

[216] A. Ross, J. Shah, and A. K. Jain, "From template to image: Reconstructing fingerprints from minutiae points," *IEEE Trans. Pattern Anal. Mach. Intell.*, vol. 29, no. 4, pp. 544–560, Apr. 2007.

[217] A. K. Jain, K. Nandakumar, and A. Nagar, "Biometric template security," *EURASIP J. Adv. Signal Process.*, vol. 2008, p. 113, Apr. 2008.

[218] K. Markantonakis, M. Tunstall, G. Hancke, I. Askoxylakis, and K. Mayes, "Attacking smart card systems: Theory and practice," *Inf. Secur. Tech. Rep.*, vol. 14, no. 2, pp. 46–56, 2009. [Online]. Available: http://www.sciencedirect.com/science/article/pii/S136341270900017X

[219] G. I. Davida, Y. Frankel, and B. Matt, "On enabling secure applications through off-line biometric identification," in *Proc. IEEE Symp. Secur. Privacy*, May 1998, pp. 148–157.

[220] D. Maltoni, D. Maio, A. K. Jain, and S. Prabhakar, *Handbook of Fingerprint Recognition | Davide Maltoni |*. London, U.K.: Springer, 2003. [Online]. Available: http://www.springer.com/gp/book/9781848822535

[221] C. Rathgeb and A. Uhl, "A survey on biometric cryptosystems and cancelable biometrics," *EURASIP J. Inf. Secur.*, vol. 2011, no. 1, pp. 1–25, 2011.

[222] A. M. P. Canuto, F. Pintro, and J. C. Xavier-Junior, "Investigating fusion approaches in multi-biometric cancellable recognition," *Expert Syst. Appl.*, vol. 40, no. 6, pp. 1971–1980, May 2013. [Online]. Available: http://www.sciencedirect.com/science/article/pii/S0957417412011165

[223] C. Rathgeb, F. Breitinger, and C. Busch, "Alignment-free cancelable iris biometric templates based on adaptive bloom filters," in *Proc. Int. Conf. Biometrics (ICB)*, Jun. 2013, pp. 1–8.

[224] C. Rathgeb and C. Busch, *Multi-Biometric Template Protection: Issues and Challenges*. Rijeka, Croatia: INTECH Open Access Publisher, 2012.

[225] C. Rathgeb and C. Busch, "Cancelable multi-biometrics: Mixing iris-codes based on adaptive bloom filters," *Comput. Secur.*, vol. 42, pp. 1–12, May 2014. [Online]. Available: http://www.sciencedirect.com/science/article/pii/S0167404814000029

[226] C. Rathgeb, M. Gomez-Barrero, C. Busch, J. Galbally, and J. Fierrez, "Towards cancelable multi-biometrics based on bloom filters: A case study on feature level fusion of face and iris," in *Proc. Int. Workshop Biometrics Forensics (IWBF)*, Mar. 2015, pp. 1–6.

[227] J. Hermans, B. Mennink, and R. Peeters, "When a Bloom filter is a Doom filter: Security assessment of a novel iris biometric template protection system," in *Proc. Int. Conf. Biometrics Special Interest Group (BIOSIG)*, Sep. 2014, pp. 1–6.

[228] J. Bringer, C. Morel, and C. Rathgeb, "Security analysis and improvement of some biometric protected templates based on Bloom filters," *Image Vis. Comput.*, vol. 58, pp. 239–253, 2015. [Online]. Available: http://www.sciencedirect.com/science/article/pii/S0262885616301263

[229] M. Gomez-Barrero, C. Rathgeb, J. Galbally, C. Busch, and J. Fierrez, "Unlinkable and irreversible biometric template protection based on bloom filters," *Inf. Sci.*, vols. 370–371, pp. 18–32, Nov. 2016. [Online]. Available: http://www.sciencedirect.com/science/article/pii/S0020025516304753

[230] U. Uludag, S. Pankanti, S. Prabhakar, and A. Jain, "Biometric cryptosystems: Issues and challenges," *Proc. IEEE*, vol. 92, no. 6, pp. 948–960, Jun. 2004.

[231] K. Nandakumar and A. K. Jain, "Multibiometric template security using fuzzy vault," in *Proc. 2nd IEEE Int. Conf. Biometrics Theory Appl. Syst. (BTAS)*, Sep. 2008, pp. 1–6.

[232] K. Nandakumar, *Multibiometric Systems: Fusion Strategies and Template Security*. Ann Arbor, MI, USA: ProQuest, 2008.

[233] V. S. Meenakshi and G. Padmavathi, "Secure and revocable multi-biometric templates using fuzzy vault for fingerprint and iris," in *Information and Communication Technologies* (Communications in Computer and Information Science), vol. 101, V. V. Das and R. Vijaykumar, Eds. Berlin, Springer, Sep. 2010, pp. 206–214. [Online]. Available: http://link.springer.com/chapter/10.1007/978-3-642-15766-0_30

[234] E. J. C. Kelkboom, X. Zhou, J. Breebaart, R. N. S. Veldhuis, and C. Busch, "Multi-algorithm fusion with template protection," in *Proc. 3rd IEEE Int. Conf. Biometrics Theory Appl. Syst.*, Piscataway, NJ, USA, 2009, pp. 222–229. [Online]. Available: http://dl.acm.org/citation.cfm?id=1736406.1736442

[235] Y. Sutcu, Q. Li, and N. Memon, "Secure biometric templates from fingerprint-face features," in *Proc. IEEE Conf. Comput. Vis. Pattern Recognit. (CVPR)*, Jun. 2007, pp. 1–6.

[236] C. Rathgeb, A. Uhl, and P. Wild, "Reliability-balanced feature level fusion for fuzzy commitment scheme," in *Proc. Int. Joint Conf. Biometrics (IJCB)*, Oct. 2011, pp. 1–7.

[237] A. Nagar, K. Nandakumar, and A. Jain, "Multibiometric cryptosystems based on feature-level fusion," *IEEE Trans. Inf. Forensics Security*, vol. 7, no. 1, pp. 255–268, Jan. 2012.

[238] J. Merkle, T. Kevenaar, and U. Korte, "Multi-modal and multi-instance fusion for biometric cryptosystems," in *Proc. Int. Conf. Biometrics Special Interest Group (BIOSIG)*, Sep. 2012, pp. 1–6.

[239] X. Li and D. Sun, "A dual-mode fingerprint fusion encryption method based on fuzzy vault," in *Proc. Int. Conf. Cyber-Enabled Distributed Comput. Knowl. Discovery (CyberC)*, Oct. 2012, pp. 208–215.

[240] A. Razaque, P. S. Sreeramoju, F. H. Amsaad, C. K. Nerella, M. Abdulgader, and H. Saranu, "Multi-biometric system using fuzzy vault," in *Proc. IEEE Int. Conf. Electro Inf. Technol. (EIT)*, May 2016, pp. 122–126.

[241] G. Mai, M. H. Lim, and P. C. Yuen, "Fusing binary templates for multi-biometric cryptosystems," in *Proc. IEEE 7th Int. Conf. Biometrics Theory Appl. Syst. (BTAS)*, Sep. 2015, pp. 1–8.

[242] M. Paunwala and S. Patnaik, "Biometric template protection with DCT-based watermarking," *Mach. Vis. Appl.*, vol. 25, no. 1, pp. 263–275, Jul. 2013. [Online]. Available: http://link.springer.com/article/10.1007/s00138-013-0533-x

[243] H. Nair, S. Anu, and P. Aruna, "PSO watermarking model for multimodal biometric system," *Int. J. Comput. Appl.*, vol. 100, no. 16, Apr. 2014.

[244] O. Nafea, S. Ghouzali, W. Abdul, and E.-U.-H. Qazi, "Hybrid multi-biometric template protection using watermarking," *Comput. J.*, vol. 59, no. 9, p. 107, Dec. 2015. [Online]. Available: http://comjnl.oxfordjournals.org/content/early/2015/12/10/comjnl.bxv107

[245] J. Hämmerle-Uhl, K. Raab, and A. Uhl, "Attack against robust watermarking-based multimodal biometric recognition systems," in *SpringerLink*. Berlin, Germany: Springer, 2011, pp. 25–36, [Online]. Available: http://link.springer.com/chapter/10.1007/978-3-642-19530-3_3, doi: 10.1007/978-3-642-19530-3_3.

[246] A. Ross and A. Othman, "Visual cryptography for biometric privacy," *IEEE Trans. Inf. Forensics Security*, vol. 6, no. 1, pp. 70–81, Jan. 2011.

[247] B. Yanikoglu and A. Kholmatov, "Combining multiple biometrics to protect privacy," in *Proc. ICPR-BCTP Workshop*, Sep. 2004, pp. 43–46.

[248] A. Ross and A. Othman, "Mixing fingerprints for template security and privacy," in *Proc. 19th Eur. Signal Process. Conf.*, 2011, pp. 554–558.

[249] A. Othman and A. Ross, "Mixing fingerprints for generating virtual identities," in *Proc. IEEE Int. Workshop Inf. Forensics Security*, Sep. 2011, pp. 1–6.

[250] A. Othman and A. Ross, "On mixing fingerprints," *IEEE Trans. Inf. Forensics Security*, vol. 8, no. 1, pp. 260–267, Jan. 2013.

[251] S. Li and A. C. Kot, "Fingerprint combination for privacy protection," *IEEE Trans. Inf. Forensics Security*, vol. 8, no. 2, pp. 350–360, Feb. 2013.

[252] S. Kanade, D. Petrovska-Delacrétaz, and B. Dorizzi, "Multi-biometrics based cryptographic key regeneration scheme," in *Proc. IEEE 3rd Int. Conf. Biometrics Theory Appl. Syst. (BTAS)*, Sep. 2009, pp. 1–7.

[253] S. Kanade, D. Petrovska-Delacrétaz, and B. Dorizzi, "Obtaining cryptographic keys using feature level fusion of iris and face biometrics for secure user authentication," in *Proc. IEEE Comput. Soc. Conf. Comput. Vis. Pattern Recognit. Workshops (CVPRW)*, Jun. 2010, pp. 138–145.

[254] S. Kanade, D. Petrovska-Delacrétaz, and B. Dorizzi, "Obtaining cryptographic keys using multi-biometrics," in *Security Privacy in Biometrics*, P. Campisi, Ed. London, U.K.: Springer, 2013, pp. 123–148, [Online]. Available: http://link.springer.com/chapter/10.1007/978-1-4471-5230-9_6, doi: 10.1007/978-1-4471-5230-9_6.

[255] B. Prasanalakshmi, A. Kannammal, B. Gomathi, K. Deepa, and R. Sridevi, "Biometric cryptosystem involving two traits and palm vein as key," *Procedia Eng.*, vol. 30, pp. 303–310, Sep. 2012. [Online]. Available: http://www.sciencedirect.com/science/article/pii/S1877705812008752

[256] P. K. Janbandhu and M. Y. Siyal, "Novel biometric digital signatures for Internet-based applications," *Inf. Manage. Comput. Secur.*, vol. 9, no. 5, pp. 205–212, 2001. [Online]. Available: http://dx.doi.org/10.1108/09685220110408022

[257] J. Daugman, "Biometric decision landscapes," Comput. Lab., Univ. Cambridge, Cambridge, U.K., Tech. Rep. 482, 2000.

[258] H. Feng and C. C. Wah, "Private key generation from on-line handwritten signatures," *Inf. Manage. Comput. Secur.*, vol. 10, no. 4, pp. 159–164, 2002.

[259] N. T. H. Lan and N. T. T. Hang, "An approach to protect private key using fingerprint biometric encryption key in BioPKI based security system," in *Proc. 10th Int. Conf. Control, Autom., Robot., Vis. (ICARCV)*, Dec. 2008, pp. 1595–1599.

[260] J.-G. Jo, J.-W. Seo, and H.-W. Lee, "Biometric digital signature key generation and cryptography communication based on fingerprint," in *Frontiers in Algorithmics*. Berlin, Germany: Springer, 2007, pp. 38–49.

[261] Y. Gong, K. Deng, and P. Shi, "PKI key generation based on iris features," in *Proc. Int. Conf. Comput. Sci. Softw. Eng.*, vol. 6. Dec. 2008, pp. 166–169.

[262] S. Mohammadi and S. Abedi, "ECC-based biometric signature: A new approach in electronic banking security," in *Proc. Int. Symp. Electron. Commerce Secur.*, Aug. 2008, pp. 763–766.

[263] M. Ramya, A. Muthukumar, and S. Kannan, "Multibiometric based authentication using feature level fusion," in *Proc. Int. Conf. Adv. Eng., Sci. Manage. (ICAESM)*, Mar. 2012, pp. 191–195.

[264] D. V. Hiep, T. Q. Duc, and N. T. H. Lan, "A multibiometric encryption key algorithm using fuzzy vault to protect private key in BioPKI based security system," in *Proc. IEEE RIVF Int. Conf. Comput. Commun. Technol., Res., Innov. Vis Future (RIVF)*, Nov. 2010, pp. 1–6.

[265] I. Buhan, J. Doumen, P. Hartel, and R. Veldhuis, "Constructing practical fuzzy extractors using QIM, centre for telematics and information technology," Univ. Twente, Enschede, The Netherlands, Tech. Rep. TR-CTIT-07-52, 2007.

[266] H. Al-Assam and S. Jassim, "Security evaluation of biometric keys," *Comput. Secur.*, vol. 31, no. 2, pp. 151–163, Mar. 2012. [Online]. Available: http://www.sciencedirect.com/science/article/pii/S0167404812000065

[267] L. Ballard, S. Kamara, and M. K. Reiter, "The practical subtleties of biometric key generation," in *Proc. 17th Conf. Secur. Symp.*, Berkeley, CA, USA, 2008, pp. 61–74. [Online]. Available: http://dl.acm.org/citation.cfm?id=1496711.1496716

[268] M. P. Balakumar and R. Venkatesan, "A survey on biometrics based cryptographic key generation schemes," *Int. J. Comput. Sci. Inf. Technol. Secur.*, vol. 2, no. 1, pp. 80–85, 2012.

[269] C.-A. Toli and B. Preneel, "A survey on multimodal biometrics and the protection of their templates," in *Privacy and Identity Management for the Future Internet in the Age of Globalisation* (IFIP Advances in Information and Communication Technology), J. Camenisch, S. Fischer-Hbner, and M. Hansen, Eds. Cham, Switzerland: Springer, Sep 2014, pp. 169–184. [Online]. Available: http://link.springer.com/chapter/10.1007/978-3-319-18621-4_12

[270] A. Tyagi, P. B. Singh, V. S. Yadav, S. K. Singh, and A. Tiwari, "Security role of biometrics in electronic transactions," in *Proc. IEEE Int. Conf. Comput. Intell. Comput. Res. (ICCIC)*, Dec. 2012, pp. 1–3.

[271] ISO/IEC. (2015). *ISO/IEC 2382:2015—Information Technology—Vocabulary*. [Online]. Available: http://www.iso.org/iso/home/store/catalogue_ics/cataloguedetail_ics.htm?csnumber=63598

[272] ISO/IEC. (2015). *ISO/IEC TR 24722:2015—Information Technology—Biometrics—Multimodal and Other Multibiometric Fusion*. [Online]. Available: http://www.iso.org/iso/home/store/catalogue_ics/catalogue_detail_ics.htm?csnumber=64061

[273] ISO/IEC. (2011). *ISO/IEC 24745:2011—Information Technology—Security Techniques—Biometric Information Protection*. [Online]. Available: http://www.iso.org/iso/iso_catalogue/xcatalogue_tc/catalogue_detail.htm?csnumber=52946

[274] ISO/IEC. (2009). *ISO/IEC 19792:2009—Information Technology—Security Techniques—Security Evaluation of Biometrics*. [Online]. Available: http://www.iso.org/iso/home/store/catalogue_tc/catalogue_detail.htm?csnumber=51521

[275] ISO/IEC. (2016). *ISO/IEC TR 30125:2016—Information Technology—Biometrics Used With Mobile Devices*. [Online]. Available: http://www.iso.org/iso/home/store/catalogue_tc/catalogue_detail.htm?csnumber=53245

[276] National Science and Technology Council (NSTC), "Biometric standards," Nat. Sci. Technol. Council (NSTC), Washington, DC, USA, 2006. [Online]. Available: https://www.hsdl.org/?view&did=463906

[277] N. Tsapatsoulis, T. F. Cootes, G. Panis, and A. Lanitis, "Overview of research on facial ageing using the FG-NET ageing database," *IET Intell. Transp. Syst.*, vol. 5, no. 2, pp. 37–46, Jun. 2016. [Online]. Available: http://digital-library.theiet.org/content/journals/10.1049/iet-bmt.2014.0053

[278] J. Galbally, M. Martinez-Diaz, and J. Fierrez, "Aging in biometrics: An experimental analysis on on-line signature," *PLoS ONE*, vol. 8, no. 7, p. e69897, Jul. 2013. [Online]. Available: http://journals.plos.org/plosone/article?id=10.1371/journal.pone.0069897

[279] S. P. Fenker and K. W. Bowyer, "Analysis of template aging in iris biometrics," in *Proc. IEEE Comput. Soc. Conf. Comput. Vis. Pattern Recognit. Workshops*, Jun. 2012, pp. 45–51.

[280] S. E. Baker, K. W. Bowyer, P. J. Flynn, and P. J. Phillips, "Template aging in iris biometrics," in *Handbook of Iris Recognition* (Advances in Computer Vision and Pattern Recognition), M. J. Burge and K. W. Bowyer, Eds. London, U.K.: Springer, 2013, pp. 205–218. [Online]. Available: http://link.springer.com/chapter/10.1007/978-1-4471-4402-1_11, doi: 10.1007/978-1-4471-4402-1_11.

[281] M. Fairhurst, M. Erbilek, and M. D. Costa-Abreu, "Selective review and analysis of aging effects in biometric system implementation," *IEEE Trans. Human-Mach. Syst.*, vol. 45, no. 3, pp. 294–303, Jun. 2015.

[282] A. Rattani, "Adaptive biometric system based on template update procedures," Dept. Electr. Electron. Eng., Ph.D. dissertation, Univ. Cagliari, Cagliari, Italy, 2010.

[283] A. Rattani, "Introduction to adaptive biometric systems," in *Adaptive Biometric Systems* (Advances in Computer Vision and Pattern Recognition), A. Rattani, F. Roli, and E. Granger, Eds. Cham, Switzerland: Springer, 2015, pp. 1–8. [Online]. Available: http://link.springer.com/chapter/10.1007/978-3-319-24865-3_1, doi: 10.1007/978-3-319-24865-3_1.

[284] A. Rattani, G. L. Marcialis, E. Granger, and F. Roli, "A dual-staged classification-selection approach for automated update of biometric templates," in *Proc. 21st Int. Conf. Pattern Recognit. (ICPR)*, Nov. 2012, pp. 2972–2975.

[285] N. Poh, J. Kittler, C.-H. Chan, and M. Pandit, "Algorithm to estimate biometric performance change over time," *IET Biometrics*, vol. 4, no. 4, pp. 236–245, 2015.

[286] A. B. Khalifa, S. Gazzah, and N. E. BenAmara, "Adaptive score normalization: A novel approach for multimodal biometric systems," *World Acad. Sci., Eng. Technol., Int. J. Comput., Elect., Autom., Control Inf. Eng.*, vol. 7, no. 3, pp. 376–384, 2013.

[287] Z. Huang, Y. Liu, X. Li, and J. Li, "An adaptive bimodal recognition framework using sparse coding for face and ear," *Pattern Recognit. Lett.*, vol. 53, pp. 69–76, Feb. 2015. [Online]. Available: http://www.sciencedirect.com/science/article/pii/S016786551400316X

[288] Y. Xu and Y. Lu, "Adaptive weighted fusion: A novel fusion approach for image classification," *Neurocomputing*, vol. 168, pp. 566–574, Nov. 2015. [Online]. Available: http://www.sciencedirect.com/science/article/pii/S0925231215007687

[289] L. Didaci, G. L. Marcialis, and F. Roli, "Analysis of unsupervised template update in biometric recognition systems," *Pattern Recognit. Lett.*, vol. 37, pp. 151–160, Feb. 2014. [Online]. Available: http://www.sciencedirect.com/science/article/pii/S0167865513002195

[290] S. Mohamed, "Product of likelihood ratio scores fusion of dynamic face and on-line signature based biometrics verification application systems," *Int. J. Database Theory Appl.*, vol. 8, no. 4, pp. 91–106, 2015.

[291] Y. Elmir, Z. Elberrichi, and R. Adjoudj, "Multimodal biometric using a hierarchical fusion of a person's face, voice, and online signature," *J. Inf. Process. Syst.*, vol. 10, no. 4, pp. 555–567, 2014.

[292] M. Soltane, "Face, Voice and signature multi-modal biometric verification fusion systems," *Ann. Faculty Eng. Hunedoara*, vol. 13, no. 4, pp. 139–150, Nov. 2015. [Online]. Available: http://search.proquest.com/docview/1734599995/abstract/80867FBDEAE9458BPQ/1

[293] R. A. Mohammed, R. M. Nabi, S. M.-R. Mahmood, and R. M. Nabi, "State-of-the-art in handwritten signature verification system," in *Proc. Int. Conf. Comput. Sci. Comput. Intell. (CSCI)*, Dec. 2015, pp. 519–525.

[294] X. Zhai, Y. Zhao, J. Wang, and Y. Li, "Adaptive SVM fusion for robust multi-biometrics verification with missing data," *Proc. SPIE*, vol. 8768, pp. 87682R-1–87682R–7, Mar. 2013. [Online]. Available: http://dx.doi.org/10.1117/12.2010895

[295] J. Galbally, S. Marcel, and J. Fierrez, "Image quality assessment for fake biometric detection: Application to iris, fingerprint, and face recognition," *IEEE Trans. Image Process.*, vol. 23, no. 2, pp. 710–724, Feb. 2014.

[296] J. Fierrez-Aguilar, J. Ortega-Garcia, J. Gonzalez-Rodriguez, and J. Bigun, "Kernel-based multimodal biometric verification using quality signals," *Proc. SPIE*, vol. 5404, pp. 544–554, Aug. 2004. [Online]. Available: http://dx.doi.org/10.1117/12.542800

[297] J. Fierrez-Aguilar, J. Ortega-Garcia, J. Gonzalez-Rodriguez, and J. Bigun, "Discriminative multimodal biometric authentication based on quality measures," *Pattern Recognit.*, vol. 38, no. 5, pp. 777–779, May 2005. [Online]. Available: http://www.sciencedirect.com/science/article/pii/S003132030400411X

[298] K.-A. Toh, W.-Y. Yau, E. Lim, L. Chen, and C.-H. Ng, "Fusion of auxiliary information for multi-modal biometrics authentication," in *Biometric Authentication*. Berlin, Germany: Springer, 2004, pp. 678–685. [Online]. Available: http://link.springer.com/chapter/10.1007/978-3-540-25948-0_92, doi: 10.1007/978-3-540-25948-0_92.

[299] E. S. Bigün, J. Bigün, B. Duc, and S. Fischer, "Expert conciliation for multi modal person authentication systems by Bayesian statistics," in *Audio-Video-Based Biometric Person Authentication*. Berlin, Germany: Springer, Mar. 1997, pp. 291–300. [Online]. Available: http://link.springer.com/chapter/10.1007/BFb0016008, doi: 10.1007/BFb0016008.

[300] D. E. Maurer and J. P. Baker, "Fusing multimodal biometrics with quality estimates via a Bayesian belief network," *Pattern Recogn.*, vol. 41, no. 3, pp. 821–832, Mar. 2008. [Online]. Available: http://dx.doi.org/10.1016/j.patcog.2007.08.008

[301] J. Bigun, J. Fierrez-Aguilar, J. Ortega-Garcia, and J. Gonzalez-Rodriguez, "Multimodal biometric authentication using quality signals in mobile communications," in *Proc. 12th Int. Conf. Image Anal. Process.*, Sep. 2003, pp. 2–11.

[302] J. Richiardi, P. Prodanov, and A. Drygajlo, "A probabilistic measure of modality reliability in speaker verification," in *Proc. IEEE Int. Conf. Acoust. Speech, Signal Process. (ICASSP)*, vol. 1. Mar. 2005, pp. 709–712.

[303] A. B. Teoh, S. A. Samad, and A. Hussain, "A face and speech biometric verification system using a simple Bayesian structure," *J. Inf. Sci. Eng.*, vol. 21, no. 6, pp. 1121–1137, 2005.

[304] K. Kryszczuk, J. Richiardi, P. Prodanov, and A. Drygajlo, "Error handling in multimodal biometric systems using reliability measures," in *Proc. 13th Eur. Signal Process. Conf.*, Sep. 2005, pp. 1–4.

[305] S. N. Yanushkevich, "Belief network design for biometric systems," in *Proc. IEEE Workshop Comput. Intell. Biometrics Identity Manage. (CIBIM)*, Apr. 2011, pp. 1–10.

[306] K. Nandakumar, Y. Chen, A. K. Jain, and S. C. Dass, "Quality-based score level fusion in multibiometric systems," in *Proc. 18th Int. Conf. Pattern Recognit. (ICPR)*, vol. 4. Aug. 2006, pp. 473–476.

[307] J. P. Carvalho, F. Batista, and L. Coheur, "A critical survey on the use of fuzzy sets in speech and natural language processing," in *Proc. IEEE Int. Conf. Fuzzy Syst.*, Jun. 2012, pp. 1–8.

[308] P. S. Prasad, P. G. N. Purohit, and D. S. Mukherjee, "Implementation of fuzzy logic in biometric system," *Imperial J. Interdiscipl. Res.*, vol. 2, no. 4, pp. 1054–1058, Mar. 2016. [Online]. Available: http://www.imperialjournals.com/index.php/IJIR/article/view/393

[309] J. Kennedy, J. F. Kennedy, R. C. Eberhart, and Y. Shi, *Swarm Intelligence*. San Mateo, CA, USA: Morgan Kaufmann, 2001.

[310] A. Rattani, G. L. Marcialis, and F. Roli, "Biometric system adaptation by self-update and graph-based techniques," *J. Vis. Lang. Comput.*, vol. 24, no. 1, pp. 1–9, 2013. [Online]. Available: http://www.sciencedirect.com/science/article/pii/S1045926X12000626

[311] N. Poh, A. Rattani, and F. Roli, "Critical analysis of adaptive biometric systems," *IET Biometrics*, vol. 1, no. 4, pp. 179–187, Dec. 2012.

[312] A. Dantcheva, C. Velardo, A. D'Angelo, and J.-L. Dugelay, "Bag of soft biometrics for person identification," *Multimedia Tools Appl.*, vol. 51, no. 2, pp. 739–777, Jan. 2011.

[313] Q. Zhang, Y. Yin, D.-C. Zhan, and J. Peng, "A novel serial multimodal biometrics framework based on semisupervised learning techniques," *IEEE Trans. Inf. Forensics Security*, vol. 9, no. 10, pp. 1681–1694, Oct. 2014.

[314] K. O. Bailey, J. S. Okolica, and G. L. Peterson, "User identification and authentication using multi-modal behavioral biometrics," *Comput. Secur.*, vol. 43, pp. 77–89, Jun. 2014. [Online]. Available: http://www.sciencedirect.com/science/article/pii/S0167404814000340

[315] M. L. Gavrilova and M. Monwar, *Multimodal Biometrics and Intelligent Image Processing for Security Systems, Information Science*. 2013.

[316] M. Sultana, P. P. Paul, and M. Gavrilova, "A concept of social behavioral biometrics: Motivation, current developments, and future trends," in *Proc. Int. Conf. Cyberworlds (CW)*, Oct. 2014, pp. 271–278.

[317] A. Dantcheva, P. Elia, and A. Ross, "What else does your biometric data reveal? A survey on soft biometrics," *IEEE Trans. Inf. Forensics Security*, vol. 11, no. 3, pp. 441–467, Mar. 2016.

[318] A. Othman and A. Ross, "Privacy of facial soft biometrics: Suppressing gender but retaining identity," in *Proc. Comput. Vis. Workshops (ECCV)*, Sep. 2014, pp. 682–696. [Online]. Available: http://link.springer.com/chapter/10.1007/978-3-319-16181-5_52, doi: 10.1007/978-3-319-16181-5_52.

[319] R. L. Finn, D. Wright, and M. Friedewald, "Seven types of privacy," in *European Data Protection: Coming of Age*, S. Gutwirth, R. Leenes, P. D. Hert, and Y. Poullet, Eds. Amsterdam, The Netherlands: Springer 2013, pp. 3–32. [Online]. Available: http://link.springer.com/chapter/10.1007/978-94-007-5170-5_1, doi: 10.1007/978-94-007-5170-5_1.

[320] P. Currah and T. Mulqueen, "Securitizing gender: Identity, biometrics, and transgender bodies at the airport," *Social Res.*, vol. 78, no. 2, pp. 557–582, 2011. [Online]. Available: http://www.jstor.org/stable/23347190

[321] J. Wickins, "The ethics of biometrics: The risk of social exclusion from the widespread use of electronic identification," *Sci. Eng. Ethics*, vol. 13, no. 1, pp. 45–54, Jan. 2007. [Online]. Available: http://link.springer.com/article/10.1007/s11948-007-9003-z

[322] S. Eberz, K. B. Rasmussen, V. Lenders, and I. Martinovic, "Looks like eve: Exposing insider threats using eye movement biometrics," *ACM Trans. Privacy Secur.*, vol. 19, no. 1, p. 1, Jun. 2016.

[323] I. Traore and A. A. E. Ahmed, Eds., *Continuous Authentication Using Biometrics: Data, Models, and Metrics*. Hershey, PA, USA: IGI Global, 2012. [Online]. Available: http://services.igi-global.com/resolvedoi/resolve.aspx?doi=10.4018/978-1-61350-129-0

[324] A. A. E. Ahmed and I. Traore, "Anomaly intrusion detection based on biometrics," in *Proc. 6th Annu. IEEE SMC Inf. Assurance Workshop*, Jun. 2005, pp. 452–453.

[325] M. Pusara, "An examination of user behavior for user re-authentication," Dept. Electr. Electron. Eng., Purdue Univ., West Lafayette, IN, USA, Ph.D. Dissertations, 2007, pp. 1–243. [Online]. Available: http://docs.lib.purdue.edu/dissertations/AAI3291194

[326] H. Crawford and K. Renaud, "Understanding user perceptions of transparent authentication on a mobile device," *J. Trust Manage.*, vol. 1, no. 1, p. 7, 2014. [Online]. Available: http://journaloftrustmanagement.springeropen.com/articles/10.1186/2196-064X-1-7

[327] H. Crawford, K. Renaud, and T. Storer, "A framework for continuous, transparent mobile device authentication," *Comput. Secur.*, vol. 39, pp. 127–136, Nov. 2013. [Online]. Available: http://www.sciencedirect.com/science/article/pii/S0167404813000886

[328] E. Vildjiounaite *et al.*, "Unobtrusive multimodal biometrics for ensuring privacy and information security with personal devices," in *Pervasive Computing* (Lecture Notes in Computer Science), K. P. Fishkin, B. Schiele, P. Nixon, and A. Quigley, Eds. Berlin, Germany: Springer, May 2006, no. 3968, pp. 187–201. [Online]. Available: http://link.springer.com/chapter/10.1007/11748625_12, doi: 10.1007/11748625_12.

[329] N. Damer, F. Maul, and C. Busch, "Multi-biometric continuous authentication: A trust model for an asynchronous system," in *Proc. 19th Int. Conf. Inf. Fusion (FUSION)*, Jul. 2016, pp. 2192–2199.

[330] H. Saevanee, N. Clarke, S. Furnell, and V. Biscione, "Continuous user authentication using multi-modal biometrics," *Comput. Secur.*, vol. 53, pp. 234–246, Sep. 2015. [Online]. Available: http://www.sciencedirect.com/science/article/pii/S0167404815000875

[331] J. Peng, K.-K. R. Choo, and H. Ashman, "User profiling in intrusion detection: A review," *J. Netw. Comput. Appl.*, vol. 72, pp. 14–27, Sep. 2016. [Online]. Available: http://www.sciencedirect.com/science/article/pii/S1084804516301412

[332] A. Al Abdulwahid, N. Clarke, I. Stengel, S. Furnell, and C. Reich, "Continuous and transparent multimodal authentication: Reviewing the state of the art," *Cluster Comput.*, vol. 19, no. 1, pp. 455–474, Mar. 2015. [Online]. Available: http://link.springer.com/article/10.1007/s10586-015-0510-4

[333] A. Ceccarelli, L. Montecchi, F. Brancati, P. Lollini, A. Marguglio, and A. Bondavalli, "Continuous and transparent user identity verification for secure internet services," *IEEE Trans. Depend. Sec. Comput.*, vol. 12, no. 3, pp. 270–283, May 2015.

[334] A. A. E. Ahmed and I. Traore, "Employee surveillance based on free text detection of keystroke dynamics," in *Handbook of Research on Social and Organizational Liabilities in Information Security*. Hershey, PA, USA: IGI Global, 2008.

[335] M. Beattie, B. V. K. V. Kumar, S. Lucey, and O. K. Tonguz, "Combining verification decisions in a multi-vendor environment," in *Audio-Video-Based Biometric Person Authentication* (Lecture Notes in Computer Science), vol. 3546, T. Kanade, A. Jain, and N. K. Ratha, Eds. Berlin, Germany: Springer, Jul. 2005, pp. 406–415, doi: 10.1007/11527923_42.

[336] G. Amirthalingam and G. Radhamani, "A multimodal approach for face and ear biometric system," *Int. J. Comput. Sci.*, vol. 10, no. 5, 2013. [Online]. Available: http://ijcsi.org/articles/A-multimodal-approach-for-face-and-ear-biometric-system.php

[337] A. Raju and V. Udayashankara, "Biometric person authentication: A review," in *Proc. Int. Conf. Contemp. Comput. Inform. (IC3I)*, Nov. 2014, pp. 575–580.

[338] A. K. Jain, K. Nandakumar, X. Lu, and U. Park, "Integrating Faces, Fingerprints, and Soft Biometric Traits for User Recognition," in *Biometric Authentication* (Lecture Notes in Computer Science), vol. 3087, D. Maltoni and A. K. Jain, Eds. Berlin, Germany: Springer, May 2004, pp. 259–269.

[339] J.-H. Yoo and B. J. Kang, "A simply integrated dual-sensor based non-intrusive iris image acquisition system," in *Proc. IEEE Conf. Comput. Vis. Pattern Recognit. Workshops (CVPRW)*, Jun. 2015, pp. 113–117.

[340] J. Ortega-Garcia *et al.*, "The multi-scenario multi-environment BioSecure multimodal database (BMDB)," *IEEE Trans. Pattern Anal. Mach. Intell.*, vol. 32, no. 6, pp. 1097–1111, Jun. 2010.

[341] M. Gudavalli, A. Babu, S. Raju, and D. Kumar, "Multimodal biometrics—Sources, architecture and fusion techniques: An overview," in *Proc. Int. Symp. Biometrics Secur. Technol. (ISBAST)*, Mar. 2012, pp. 27–34.

LAVINIA MIHAELA DINCA received the bachelor's degree in computer science from Romanian American University, the master's degree in computer networks from the University of Bucharest, and the MBA degree from the Academy of Economic Studies Bucharest. She is currently pursuing the Ph.D. degree with the City University of Hong Kong. She has vast experience in the software field with emphasis on security. Her main research interests are biometrics, encryption, computer security, and steganography.

GERHARD PETRUS HANCKE received the B.Eng. and M.Eng. degrees from the University of Pretoria, South Africa, in 2002 and 2003, respectively, and the Ph.D. degree in computer science with the Computer Laboratory, Security Group, University of Cambridge, in 2008. He is currently an Assistant Professor with the City University of Hong Kong, Hong Kong. His research interests are system security, embedded platforms, and distributed sensing applications.