IEEE Access
Multidisciplinary ⋮ Rapid Review ⋮ Open Access Journal

Received 7 March 2024, accepted 25 April 2024, date of publication 30 April 2024, date of current version 13 May 2024.

Digital Object Identifier 10.1109/ACCESS.2024.3395417

TOPICAL REVIEW

A Comprehensive Review of Unimodal and Multimodal Fingerprint Biometric Authentication Systems: Fusion, Attacks, and Template Protection

U. SUMALATHA[1], K. KRISHNA PRAKASHA[1], (Senior Member, IEEE), SRIKANTH PRABHU[2], (Senior Member, IEEE), AND VINOD C. NAYAK[3]

[1]Department of Information and Communication Technology, Manipal Institute of Technology (MIT), Manipal Academy of Higher Education (MAHE), Manipal, Karnataka 576104, India
[2]Department of Computer Science and Engineering, Manipal Institute of Technology (MIT), Manipal Academy of Higher Education (MAHE), Manipal, Karnataka 576104, India
[3]Department of Forensic Medicine, Kasturba Medical College (KMC), Manipal Academy of Higher Education (MAHE), Manipal, Karnataka 576104, India

Corresponding authors: K. Krishna Prakasha (kkp.prakash@manipal.edu) and Srikanth Prabhu (srikanth.prabhu@manipal.edu)

ABSTRACT In the contemporary technological landscape, biometrics, encompassing the analysis of biological data, have gained significance. Biometrics is a methodology that utilize unique behavioral, physical, or morphological traits—such as speech, facial features, iris, fingerprint, retina, and signature for individual identification. Biometric technology has been successfully used in forensic science, security, and authorization systems. This review highlights understanding the classification, types of biometric traits and their comparisons, fingerprint recognition stands out as a reliable and widely adopted method due to its simplicity and cost-effectiveness, accuracy and robustness compared to others. Unimodal fingerprint biometric systems safeguard authentication information through the analysis of characteristic sequences and, face challenges such as vulnerability to spoof attacks, inter-class similarity, intra-class variation, non-universality, and noisy data. These challenges are addressed by multimodal fingerprint biometric systems, in which various biometric sources compensate for each other's limitations. The review focuses on the overview of unimodal and multimodal fingerprint biometric systems and the importance of fusion, advancements in data acquisition, preprocessing, feature extraction, matching algorithms, performance metrics, indexing, template protection, and addressing attacks in enhancing system security and reliability. The review paper sheds light on the intricate relationship between these elements, offering valuable insights into the current state and potential evolution of the field. The review paper highlights current challenges and suggests future research directions, emphasizing the necessity for continual advancements in fusion techniques, template protection methods, and novel defense mechanisms to effectively mitigate emerging threats in unimodal and multimodal fingerprint biometric systems.

INDEX TERMS Fingerprint, biometric authentication, biometric fusion, multimodal biometrics, attacks, template protection, biometric robustness.

I. INTRODUCTION

Biometrics is the study of measuring and analyzing specific physical or behavioral traits that are employed to identify a person. Because each person's biometric traits are distinct,

The associate editor coordinating the review of this manuscript and approving it for publication was Larbi Boubchir.

it is challenging for an outsider to sneak them successfully. Many traits that are suitable for automatic recognition have been researched, such as the iris, voice, fingerprint, and face. A biometric modality refers to a category within a biometric system, determined by the specific type of human trait it utilizes as input. Each modality corresponds to a distinct biometric trait. A biometric trait, the type of sensor, and the algorithms used to extract and analyze the digital representations of the trait are combined to produce a biometric modality. The term ''different modalities'' refers to the fact that any two or more of these three components are different among systems. For instance, iris and infrared facial recognition are distinct modalities even when the same camera is utilized because of differences in methods and traits [1]. Biometric-based descriptors are frequently used owing to their uniqueness and robustness. Biometric-based authentication systems have been successfully employed for three decades at the University of Georgia and for over a decade at the airports in San Francisco and Walt Disney World, with tens of thousands of daily users. The use of biometric technologies in many security applications has grown globally as a result of its major benefits with regard to authentication rate, universality, and security. As technology develops, more people are beginning to doubt the security of their secret password. One may find the bank login credentials online. Therefore, a system that uses physical or behavioral traits as passwords must be created. Consequently, a security system was developed that uses various biometric traits as system passwords. These extremely secure systems are used by many governmental and private applications that require the automatic control of access to physical or virtual places. Systems for security and surveillance, ATMs, banking transactions, border inspections and computer and network security, etc. are some examples [2].

A. A TYPICAL BIOMETRIC CHARACTERISTICS

Any individual physiological or behavioral trait must meet criteria which are stated as follows:

1) Universality: Anyone must be able to use the application using biometric features.
2) Uniqueness: Everybody has a different biometric feature.
3) Permanence: In the long run, the biometric feature must not alter.
4) Measurability: Sensors should be capable of acquiring and digitizing the biometric attributes of each person.
5) Performance: The overall accuracy should be high, with low False Acceptance Rate (FAR) and False Rejection Rate (FRR).
6) Acceptability: refers to how well individuals accept the need for a certain biometric system as well as their willingness to provide biometric data.
7) Circumvention: This demonstrates how easily the system can be tricked using a fake biometric trait [3].

The comparison of biometrics traits with respect to acceptability, performance, distinctiveness, universality, permanence, circumvention and measurability are shown in Table 1.

B. APPLICATIONS OF BIOMETRICS

The field of biometrics is developing rapidly and has applications in mug shots, forensics, and post-event analysis in the criminal justice system. It offers protection against unwanted access to ATMs, mobile devices, email ID verification on multimedia workstations, computer networks, medical record management, personal digital assistants, and distance learning [5]. Voice biometrics find applications in various domains, including telephone, internet, commerce, and banking transactions. This technology was employed to verify and authenticate individuals based on their unique voice characteristics [6]. On the other hand, retinal patterns offer valuable medical insights, revealing information about conditions such as high blood pressure or diabetes. The utilization of these biometric modalities underscores their versatility in both security-related and healthcare contexts [7]. In cars, fingerprint systems replace keys with keyless entry devices [8]. Applications involving smart cards use facial biometrics [9]. Face recognition is used in forensic applications, including the identification of terrorists and dead bodies, crime detection, surveillance, and access control management [10]. Social security, National ID cards, border control, and passport control are other biometric applications which often utilize biometric traits such as fingerprint, iris, or facial for identity verification and authentication [5].

C. OUTLINE OF THE ARTICLE

Addressing the challenges inherent in unimodal biometric systems, including intra-class dissimilarity, inter-class similarity, noisy data, spoofing, and non-universality, this study emphasizes the need for a comprehensive examination of these issues. This focus extends to both unimodal and multimodal fingerprint biometric identification systems, highlighting the limitations associated with relying solely on a single biometric mode. By doing so, this article aims to underscore the importance of exploring and implementing multimodal approaches to mitigate these challenges, ultimately contributing to improved security and reliability in biometric identification systems. Over 350 articles from Springer, Science Direct, IEEE Xplore, and Google Scholar were reviewed for this study, the majority of which were published between 2017 and 2024. The research article is divided into the following sections as mentioned: The classification of biometric traits is provided in Section II. The types of biometric systems used are discussed in Section III. Section IV delves into fingerprint biometric system, fingerprint acquisition, detailing the procedure of capturing high-resolution fingerprint images using dedicated scanners or sensors. A survey of the literature on unimodal fingerprint biometric systems is presented in Section V. Section VI examines vulnerabilities in fingerprint recognition

TABLE 1. Analyzing biometric traits used in biometric systems based on the existing literature review [4].

Biometric Identifier	Universality	Uniqueness	Permanence	Measurability	Performance	Acceptability	Circumvention
Face	3	1	2	3	1	3	3
Fingerprint	2	3	3	2	3	2	2
Ear	3	2	3	2	2	3	2
Gait	2	1	1	3	1	3	2
Hand Geometry	2	2	2	3	2	2	2
Hand Vein	2	2	2	2	2	2	1
Iris	3	3	3	2	2	1	1
Retina	3	3	2	1	3	1	1
Voice	2	1	1	2	1	3	3
DNA	3	3	3	1	1	1	1
Signature	1	1	1	3	1	3	3
Keystroke	1	1	1	2	1	2	2

3: Highest rating, 2: Intermediate rating, 1: Lowest rating

systems, Section VII discusses the protection of fingerprint biometric templates, and Section VIII highlights the different fusion methods applied to multimodal fingerprint biometric systems. A survey of the literature on multimodal fingerprint biometric systems is presented in Section IX. To determine future research directions, Section X discusses limitations and solutions related to fingerprint unimodal and multimodal biometric systems, and Section XI concludes the paper.

II. CLASSIFICATION OF BIOMETRIC TRAITS

Two types of biometric traits are identified based on their behavioral or physiological characteristics. Figure 1 shows illustrations of physiological and behavioral biometric traits that are incorporated into a biometric identification system.

A. PHYSIOLOGICAL TRAITS

Physical characteristics include features such as face, fingerprint, ear, iris, palm, and knuckleprint.

Faciale recognition, relying on faciale images captured at specific distances, undergoes initial stages of detection and feature extraction to ensure integrity and originality [12]. Meanwhile, fingerprint authentication, a long-standing method, relies on ridge and valley patterns, categorized into loops, arches, and whorls, with minutiae points serving as distinctive features [13]. Ear biometrics, characterized by line-based elements and robustness, are segmented from raw faciale profiles for identification purposes [14].

The iris, another widely recognized trait, features distinct textures like furrows, ridges, and crypts, captured under high-resolution near-infrared light (NIR) illumination due to its sensitivity to light [15]. Similarly, palmprints boast reliability and distinctiveness through ridge patterns, principal lines, minutiae details, delta points, and complex textures [16], while knuckleprints offer discriminating features captured by various sensors [17]. These traits collectively contribute to the diverse landscape of biometric authentication, each with its unique strengths and applications. The description of physiological biometric traits is given in Table 2.

B. BEHAVIORAL TRAITS

Behavioral attributes include gait, voice, signature, EEG, and electrocardiography (ECG).

Gait analysis utilizes video streams and locomotive light displays to capture essential data points like pressure and stride patterns, revealing distinctive walking patterns [48]. Signatures, both offline and online, provide static features like breakpoints and writing angles, as well as dynamic characteristics such as pen speed and pressure [56], [76]. Voice identification systems leverage the unique tonal quality and texture of a person's voice, but are susceptible to spoofing and impersonation [62].

Hand geometry, known for its universality and long-term invariance, is widely used in various applications [43], [77]. Brain activity is recorded electrically via EEG, which shows voltage changes caused by ionic current flows in brain neurons. Electrodes applied to the scalp covering the brain allow for non-invasive recording of EEG signals. The EEG waves have a frequency of 0.5 - 40 Hz and an amplitude that varies from 10 to 200V. The five distinct frequency bands that constitute an EEG waveform are the delta, gamma, beta, and theta bands [67], [78]. ECG, with its highly personalized signals, is particularly intriguing to the biometrics community due to its difficulty to counterfeit [71], [79]. The description of behavioral biometric traits is given in Table 3.

III. TYPES OF BIOMETRIC SYSTEMS

Biometric systems are available in two different types:

A. UNIMODAL BIOMETRIC SYSTEM (UBS)

A unimodal biometric authentication system relies on a single biometric trait to identify and authenticate users. This system captures and analyzes data from a specific biological or behavioral characteristic unique to an individual. Despite offering a high degree of security for identity recognition, unimodal systems have limitations that might compromise their dependability, security, scalability, efficacy, accuracy, and privacy. Here are the specifics:

1) Accuracy: Any conventional biometric system should be able to accurately identify an individual. Several factors influence the accuracy of biometric systems that function based on a single attribute:
   Noise in the gathered data: A variety of factors, including environmental, and physical damage might affect the biometric data collection process. The

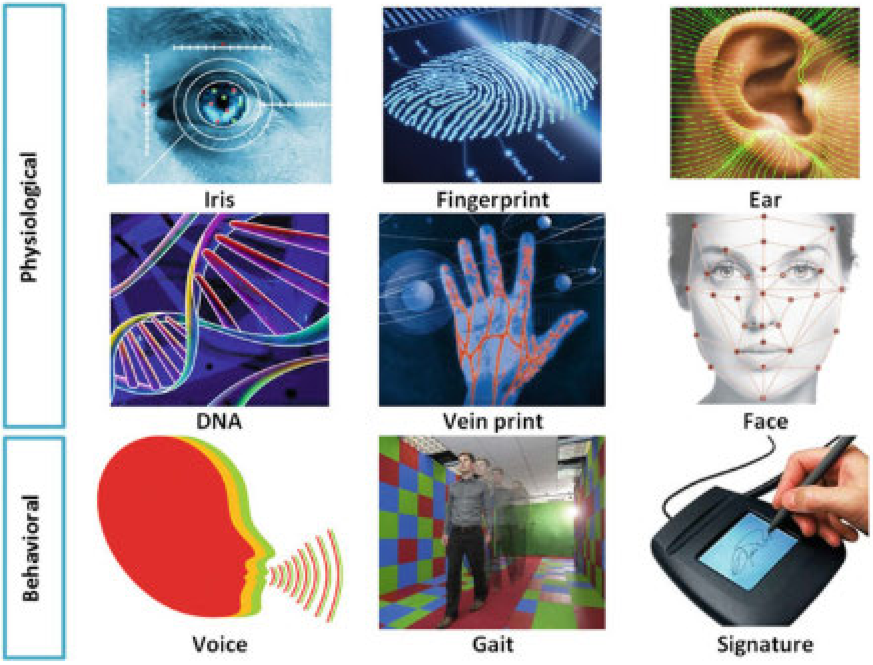


FIGURE 1. Physiological and behavioral biometric traits (source: Bouchrika et al. [11]).

accuracy of fingerprint characteristics accuracy can be compromised, by contamination on the surface of the fingerprint scanner. The system's overall accuracy declines because of poor biometric input [80].

2) Non-universality: A segment of the population may be unable or unwilling to give the requisite biometric feature precisely, resulting in an increased failure to enroll rate (FER). When a person has a cut or wound, wear gloves, or when their fingerprints are smudged with oil or debris. Fingerprint sensors are ineffective at identifying them, which may affect and restrict the operation of a biometric system. Therefore people working in the manufacturing, construction, and mining industries do not prefer fingerprints in attendance systems. Along with technical, physical and medical challenges, cultural or religious considerations may also restrict a group or individual's ability to enroll in an authentication system [5].
3) Intra-class variations: This refers to the differences in samples obtained from individuals during the enrollment and recognition stages. These variances could be caused by reader malfunction (e.g., translation, pressure variation, or rotation on the fingerprint sensor), scars, or bruising of the fingerprint. This leads to an increase in the FAR [5].
4) Scalability: As the number of enrolled users grow [81], the computational complexity of matching queries against the expanding database also increased, resulting in longer identification times [82]. The query needs to match the templates of N enrolled users stored in the database. This database expansion may contribute to a higher frequency of false matches or mismatches, potentially stemming from fingerprint resemblances or fluctuations in image quality [83].
5) Security and Privacy: Physical and behavioral features can be targeted for spoofing attacks. In biometric systems, the privacy of all individual templates maintained in the system's database is a critical concern. Various strategies for dealing with biometric spoofing difficulties include a liveness-detection mechanism [84] for physical traits and a challenge-response technique for both behavioral and physical traits [17], [85].

B. MULTIMODAL BIOMETRIC SYSTEM (MBS)

Multimodal biometric systems are gaining increasing popularity in real-world applications. A multimodal biometric system utilizes multiple biometric traits to enhance accuracy and security. Scalability challenges may also impact multimodal biometric systems, despite their utilization of multiple modalities for accuracy and reliability improvements. Managing data from various modalities, ensuring interoperability among different components, and sustaining performance under increased workload can contribute to scalability concerns. Therefore, addressing scalability is crucial for effective operation in large-scale deployment scenarios. However, scalability issues may not be exclusive to unimodal systems, as multimodal systems could also exhibit similar characteristics. The following is a list of some benefits of multibiometric systems over unimodal biometric systems.

1) The precision and accuracy of recognition systems are improved by significantly reducing the influence of noise and low quality in the biometric features that

TABLE 2. Description of physiological biometric traits.

Biometric Trait	Features	Feature Extraction Methods	Applications	Advantages	Disadvantages
Face [12]	Faciale landmarks, texture, color	Deep learning [18], Geometric Pattern Analysis [19] Eigenfaces, Fisherfaces [20], LBP [21], LDN [22], Deep Feature Fusion [23], Faciale Landmarks based [24]	Access control, surveillance, biometric authentication	Simple capture, universal acceptance	Sensitive to lighting, pose variation, occlusion, aging
Iris [15]	Unique iris patterns, crypts, furrows	Texture-based [25] Daugman's algorithm [26], Gabor filters [27], Deep learning [28]	High-security applications, border control, National ID cards, Google data center access	Unique texture, fast processing, accurate, stable over time	Sensitive to occlusion, contact lens, off-angle recognition, expensive equipment
Ear [14]	Ear shape, contours, ridges	LBP [29], gradient directional pattern [30], deep learning [31], Fourier descriptors, wavelet transform [32]	Forensic investigations, personal authentication	Less affected by aging, difficult to spoof, non-intrusive collection, sturdy shape	Illumination, occlusions, variations, limited availability of databases
Palmprint [16]	Palm texture, wrinkles, ridges	Deep Learning [33], LBP [34], gradient-based approaches [35], and multiscale texture analysis [35]	Access control, forensic analysis	Fast acquisition, Low-cost sensors, stable features	Low resolution, rotation, lighting, occlusion, susceptible to damage
Knuckleprint [36]	Knuckle creases, shape, geometry	LBP [37], HOG [38], PCA [39]	Access control, forensic applications	Unique, difficult to alter, inexpensive sensors	Less studied, cuts, rotation, lighting, limited research
Fingerprint [13]	Ridge patterns, minutiae points	Graph convolutional networks [40], Minutiae extraction, ridge orientation [41], deep learning [42],	Law enforcement, biometric authentication	Widely used, cost-effective, simple collection, distinct fingerprints	Spoofing, quality, injured fingers, degradation over time
Hand Geometry [43]	Hand size, finger length	3D scanners, Geometric Measurements [2], PCA [44], Procrustes Analysis [45], Fourier Descriptors [46], CSS [47]	Access control, time attendance	Fast enrollment, low-cost, user-friendly, precise	Limited distinctiveness for robust identification

LBP: Local Binary Patterns, LDN: Local Directional Number Patterns, HOG: Histogram of Oriented Gradients, PCA: Principal Component Analysis, CSS: Curvature Scale Space

were gathered. The incorporation of multiple biometric sources into a multibiometric system enhances its effectiveness and resilience. This approach acknowledges the potential limitations or variability associated with individual biometric traits. If one trait, such as a user's speech attribute, proves challenging for identification owing to factors such as environmental noise or health conditions, another trait, such as a fingerprint, can be used as an alternative [86].

2) With the help of multibiometric systems, enrollment phase problems such as non-universality are resolved, allowing for adequate population coverage. As a result, even if a user cannot provide one biometric trait, they can still enroll and be recognized by providing a different biometric trait. For instance, despite having poor fingerprint quality, a manual laborer can nonetheless enlist and be recognized using features such as their face, voice, iris, etc. Therefore, FER decreases as population coverage increases [12].

3) By combining biometric qualities and using a fusion approach, a multibiometric system can significantly reduce the overlap between the image features of different people (inter-class similarities). The feature vector will become more dimensional as a result of collecting data from several sources; however, the overall accuracy of the biometric system will increase. For instance, even if two family members share a voice characteristic, they do not have the same fingerprint or iris attributes.

4) Multibiometric systems have the potential to enhance accuracy and resist unauthorized access more effectively than unimodal biometric systems. This increased security is attributed to the heightened difficulty of counterfeiting or spoofing multiple biometric features simultaneously for an authorized user. The use of a multibiometric system can also be combined with another method, such as asking the user to reveal one of their biometric traits at random during the acquisition

TABLE 3. Description of behavioral biometric traits.

Trait	Key Features	Feature Extraction Methods	Uses	Advantages	Disadvantages
Gait [48]	Dynamic patterns of walking	GEI [49], DTW [50], Fourier Transform [51], PCA [52], Wavelet Transform [53], CNN [54], HOG [55]	Security access, health monitoring	Non-intrusive, continuous authentication	Affected by walking conditions
Signature [56]	Writing style, stroke order	DTW [57], HOG [58], Wavelet Transform [59], PCA [60], Directional Feature Extraction [61]	Document authentication, financial transactions	Widely accepted, convenient	Forgery potential, Variability due to aging, writing surface, and emotion
Voice [62]	Pitch, tone, speech patterns	MFCCs [63], LPC [64], PLP [65], Pitch Detection [66]	Voice authentication, telephone banking	Non-invasive, can be combined with other modalities	Vulnerable to imitation, Voice degradation due to aging, mood, environmental factors
EEG [67]	Brainwave patterns	Deep Learning [68], Wavelet Transform [69], Entropy [70]	Security, medical, wearable, consumer electronics	Universality, versatility, potential for authentication in various states	Limited accuracy, stability over time, requires specialized equipment
ECG [71]	Heartbeat patterns	Statistical Features [72], Wavelet Transform [73], Frequency Domain Analysis [74], HRV Analysis [75]	Health monitoring, authentication	Accurate, unique, universal, permanent, liveness verification	Limited to specific use cases, absence of comprehensive ECG databases

GEI: Gait Energy Image, DTW: Dynamic Time Warping, MFCCs: Mel-Frequency Cepstral Coefficients, LPC: Linear Predictive Coding, PLP: Perceptual Linear Prediction, HRV: Heart Rate Variability

process (for instance, a fingerprint, followed by a face attribute and a voice characteristic) to confirm that they are the real users of the system. For this, the terms "Challenge-Response Mechanism" or "Liveness Detection Mechanism" are employed.

5) By utilizing a multibiometric system, the throughput of a biometric system is greatly boosted, especially when performing an identification operation that requires a one-to-many comparison. To achieve this, start by utilizing the biometric traits that are the less accurate (such as the face trait) condense the size of the database to a reasonable level, and then apply the most accurate biometric data (such as the fingerprint, iris) to the remaining database to draw a conclusion.
6) Additionally, a multibiometric system offers the user a great deal of flexibility during the recognition phase. Consider a system that employs three biometric traits. Depending on the type of application and its convenience, the user can then decide whether to give all of their biometric features during the recognition phase [87].

IV. THE FINGERPRINT BIOMETRIC AUTHENTICATION SYSTEM

The fingerprint trait of a person is recorded using a biometric authentication system, which is a categorization and recognition tool. It does this by comparing a number of unique features from the trait evidence with a template of fingerprint data stored in the database maintained by the system. The results of the comparison are considered when making the final yes/no decisions. Figure 2 illustrates the four basic modules that constitute the overall architecture of a traditional fingerprint biometric system, together with the order in which they take place.

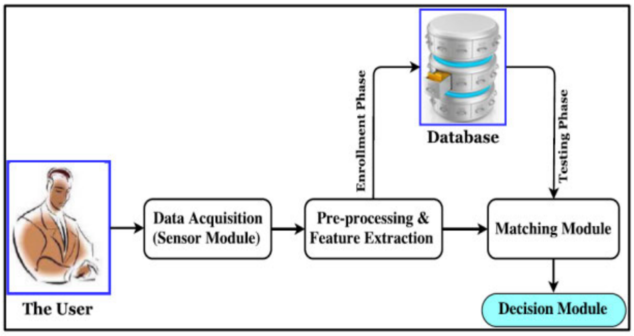


FIGURE 2. A fingerpirnt biometric authentication system (source: Jain et al. [2]).

1) Sensor Module: Users interact with the system through a sensor or reader, capturing fingerprint properties and converting them into digital signals. This initial step is crucial for subsequent processing [88].
2) Preprocessing and Feature Extraction Module: This phase refines and optimizes captured fingerprint data to enhance accuracy. It involves evaluating characteristics, segmenting the fingerprint area of interest, enhancing image quality, and deriving discriminating features for matching [86], [89], [90], [91].

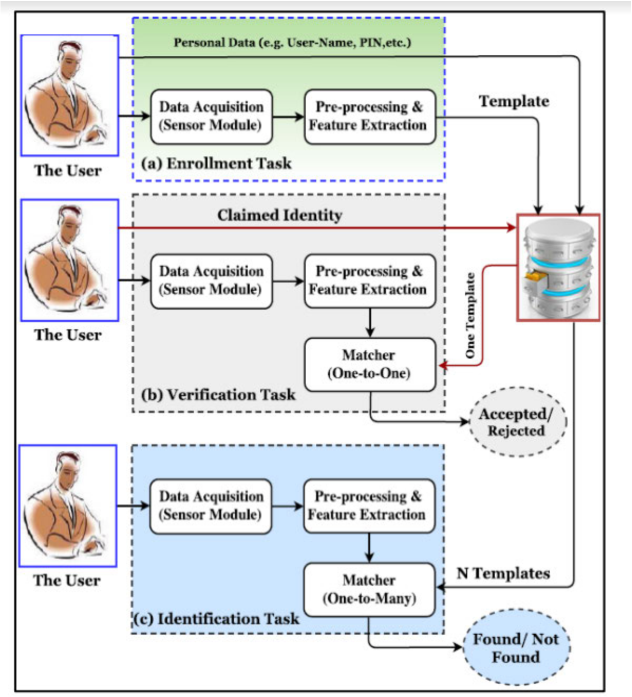

Personal Data (e.g. User-Name, PIN,etc.)
The User
Data Acquisition (Sensor Module)
Pre-processing & Feature Extraction
Template
(a) Enrollment Task
Claimed Identity
The User
Data Acquisition (Sensor Module)
Pre-processing & Feature Extraction
One Template
Matcher (One-to-One)
(b) Verification Task
Accepted/ Rejected
The User
Data Acquisition (Sensor Module)
Pre-processing & Feature Extraction
Matcher (One-to-Many)
N Templates
(c) Identification Task
Found/ Not Found

FIGURE 3. Functionalities of a fingerprint biometric system (source: Jain et al. [2]).

3) Matching Module: Extracted feature vectors are compared with templates in the system's database to determine matching scores.
4) Decision Module: Based on matching scores, the system determines whether the person's stated identity is accepted or rejected [2].

Three tasks are accomplished using a fingerprint biometric system, depending on the application situation: enrollment, verification, and identification. "Recognition" refers to the last two functionalities [2]:

1) Enrollment: A sensor is used to collect fingerprint information from an individual, convert it into a digitized format, and store templates in a database. This process, referred to as enrollment or training, is depicted in Figure 3 and contains certain biographic information (such as their profile, PIN number, and address) to help identify them.The template is encrypted to ensure its security.
2) Verification: Fingerprint verification through template matching entails the generation of a distinctive template based on an individual's fingerprint characteristics. During the verification process, a user fingerprint is acquired, relevant features are extracted, and a similarity score is determined by comparing these features with the stored template. Access is granted if the score surpasses a predefined threshold. Otherwise, it is rejected. The effectiveness of this method depends on the inherent uniqueness of the fingerprint patterns, ensuring secure and reliable authentication. As shown in Figure 3, decides whether to approve or reject the submitted verification claim, by performing a one-to-one comparison between the query template and retrieved reference template. Typical examples of this type of scenario are fingerprint-based access control and large scale civil verification systems (such as Aadhaar), in which users authenticate themselves with a fingerprint impression and a unique ID (such as an employee's RFID card or an Aadhaar 12-digit unique ID).
3) Identification: This takes longer and requires more effort than verification. The system requests a fingerprint from the user, as shown in Figure 3, and compares every template kept in the database with the data gathered in a one-to-many manner. Identification is the act of establishing a person's identity by comparing their registered fingerprint template with a database of known fingerprint templates. This comparison generates a similarity score, quantifying the degree of resemblance between the captured fingerprint and the stored fingerprints in the database. The identity is validated if the similarity score is greater than a predetermined threshold, signifying a sufficiently close match. This threshold-based method guarantees precise and dependable identification in applications such as forensic investigations, access control, and law enforcement [92].

A. PERFORMANCE METRICS FOR FINGERPRINT BIOMETRIC RECOGNITION SYSTEM

1) False Acceptance/Match Rate (FAR)/(FMR):
is a statistical metric utilized to determine the probability that the fingerprint biometric system incorrectly accepts an impostor as an authorized user. Fake fingers, or presentation attacks, contribute to FAR by introducing unauthorized biometric samples that are incorrectly accepted by the system, thus increasing the probability of false acceptances. FAR measures the rate at which unauthorized individuals are incorrectly identified as genuine users, given by (1). A lower FAR indicates a higher level of security in the system [5].

$$FAR(\%) = \frac{No.ofFalseAcceptances * 100}{No.ofAttemptsbyImpostors} \tag{1}$$

2) False Reject/NonMatch Rate (FRR)/(FNMR):
is a statistical metric utilized to determine the probability that the fingerprint biometric system fails to recognize a genuine user. FRR typically focuses on genuine matches, fake fingers (presentation attacks) indirectly impact FRR by potentially causing genuine users to be incorrectly rejected if the system fails to distinguish between genuine and fake biometric samples. FRR measures the rate at which valid inputs are incorrectly rejected, given by (2). A lower FRR indicates a higher level of accuracy in recognizing

genuine users [5].

$$FRR(\%) = \frac{No.ofFalseRejections * 100}{No.ofAttemptsbyLegitimateusers} \tag{2}$$

3) Equal Error Rate (EER): EER is the point on a ROC or detection error tradeoff (DET) curve at which the FAR and FRR are equal. EER represents the threshold at which the system makes an equal number of false acceptance and false rejection errors. Lower EER values indicate better overall performance [5].
4) True/Genuine Acceptance Rate (TAR)/(GAR): The degree to which the system is able to correctly match the fingerprint information from the same person.
5) True/Genuine Rejection Rate (TRR)/(GRR): The degree to which the system is able to correctly deny fingerprint information from an imposter [88].
6) The performance of fingerprint indexing techniques is assessed using metrics, such as the hit rate, penetration rate, error rate, and pre-selection error rate. The number of true matches found at the top t matches out of all the queries is known as the hit rate. The penetration rate is the percentage of the database that returns as a list of potential retrievals that are successful. Suppose N, ni, CI, and X represent the total number of queries performed during identification, the total number of images successfully retrieved for the i^{th} inquiry, the number of accurately recognized query samples, and the total number of images in the database, hit, penatration, and error rate are given by 3,4, and 5

$$HitRate(\%) = CI * N * 100 \tag{3}$$

$$PenetrationRate(\%) = \frac{1}{N} * \sum_{i=1}^{N} ni * \frac{1}{X} * 100 \tag{4}$$

$$ErrorRate(\%) = \frac{[N] - [CI]}{N} * 100 \tag{5}$$

7) ROC (Receiver Operating Characteristic) Curve: The ROC curve demonstrates the balance between the true positive rate (sensitivity) and the false positive rate (1)-specificity) as the threshold varies. It offers insight into the system's ability to differentiate between genuine matches and impostor attempts.
8) CMC (Cumulative Match Characteristic) Curve: The CMC curve depicts the likelihood of accurately identifying an individual within the top N matches. It evaluates how effectively the system prioritizes true matches over impostors across different possible match ranks.
9) AUC (Area Under the Curve): AUC, representing the area under the ROC curve, provides a single numerical measure summarizing the overall performance of a biometric system. Higher AUC values indicate superior discrimination ability between genuine and impostor matches, with an AUC of 1 signifying flawless performance.

B. DIFFERENT MODALITIES OF FINGERPRINT DATA ACQUISITION

A widely utilized biometric sensing method is fingerprint sensing, which is categorized based on user interaction into touch, contactless, partial, slap, and other modalities. These sensors employ sensing technologies to identify the ridge-valley structure of a finger. Fingerprint sensors are classified according to the fundamental technologies they use, including (i) optical, (ii) capacitive, (iii) thermal, (iv) pressure, and (v) ultrasonic technologies. Figure 4 illustrates the variations in both standard contact and contactless fingerprints.

The most widely used method for capturing images, which is currently used in numerous applications, is physical contact. Capacitive sensors, optical sensors with charge-coupled device (CCD), and digital scanners have been utilized to acquire images through contact. High-resolution fingerprint recognition is often facilitated using optical sensors.

Fingerprint sensor output is classified as (i) rolled (ii) latent prints (iii) plain (iv) partial fingerprints Imaging techniques are evolving along with sensor variations. Significant physical finger placements on the sensor surface can result in significant issues for each acquisition mode, necessitating the need for alternate solutions.

1) Rolled fingerprints: These are generated by applying pressure to the finger and inspecting the fingertip in a sweeping motion.
2) Plain fingerprints: are recorded without rotating the fingertip.
3) Latent fingerprints: In Latent prints are utilized in forensic and law enforcement applications. The methods for obtaining these prints involve contamination of the fingerprints with chemicals.
4) Partial prints: Images are acquired with an optical sensor from diverse fingerprint skin conditions.
5) 2D Contactless fingerprints: This refer to images that represent the 3D surface structure of a finger without direct physical contact. These images are typically obtained using digital cameras, and the setups often utilize sensors based on LED colors and white light to capture fingerprint information in an optical manner.
6) 3D Contactless fingerprints: In the realm of 3D contactless fingerprint capturing, researchers have explored various prototypes within laboratory settings. These prototypes employ multiple strategies and methods, including:
   a) Photometric Stereo Techniques: This involves using a high-speed camera was used to capture numerous 2D images from a fixed viewpoint under different illumination conditions.
   b) Non-Invasive Optical Coherence tomography: This technique provides a non-destructive, high-resolution method for capturing 3D fingerprint images.

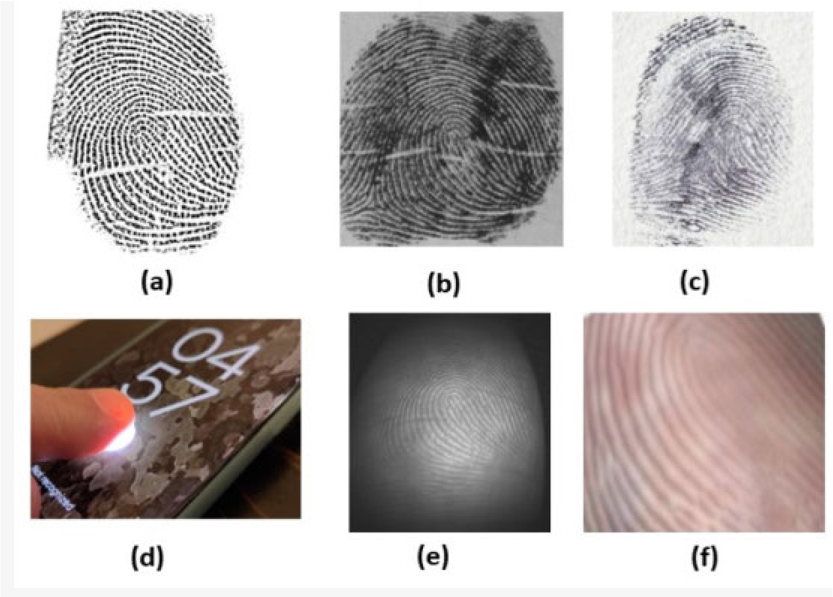


FIGURE 4. Variations of the standard contact as well as contactless fingerprints. (a) plain, (b) rolled, (c) latent, (d) partial print, (e) contactless 2D, (f) contactless 3D (source: Cader et al. [93]).

c) Structured Light Scanning: In approach, a multi-camera setup with a projector is used to capture 3D images.

d) Stereo Vision: Images are captured using multiple cameras positioned at various angles to create a stereo effect.

e) Ultrasonic Sensing: Utilizing acoustic pulses, this method involves the transmission of sound waves from a transmitter to the fingerprint and the reception of echoed waves by a receiver.

These techniques collectively contribute to the advancement of 3D fingerprint capturing capabilities in a contactless manner [94], [95], [96]. The fingerprint image acquisition modes are listed in Table 4.

C. THERMAL IMAGING OF FINGERPRINT

Thermal cameras are increasingly used in surveillance for their affordability, improved features, and expanded applications like video surveillance, self-driving cars, airport screening, and medical diagnostics. They capture thermograms using the long-wave portion of the electromagnetic band, allowing recording in adverse weather, at night, and over long distances. Thermal imaging detects heat emitted by fingerprint ridges and valleys, unaffected by surface conditions, making advantageous for capturing fingerprints in challenging environments. This method detects latent fingerprints and is suitable for biometric authentication, undergoing analysis for feature extraction and matching similar to traditional fingerprint images.

Zhang et al. [97] developed a system employing deep ultraviolet photo-synapses and a memristor array for latent fingerprint recognition using photoelectronic reservoir computing (RC) with a Ga-rich design, achieving 90% accuracy on the FVC2002 dataset. Hu et al. [98] investigated the use of polarimetric thermal imaging to capture latent fingerprints on nonporous surfaces without traditional dusting, presenting an innovative approach to latent print acquisition.

V. LITERATURE REVIEW ON UNIMODAL FINGERPRINT BIOMETRIC SYSTEMS

Based on research conducted by the National Institute of Standards and Technology (NIST) in 2021, fingerprinting has an accuracy more than 99% [99]. Each individual is recognized by its distinctive fingerprints, which are used to access lock identifying ones. Biometric technology, has been the most actively researched. It has been, and remains highly popular because of the availability of numerous sources for data collection, including the ten fingers, because it is inherently simple to obtain, and its established application and gathering by immigration and law enforcement [100], [101].

Table 5 provides an overview of some fingerprint datasets that are commonly used in both unimodal and multimodal biometric systems.

A. FINGERPRINT PREPROCESSING TECHNIQUES

Fingerprint thinning is a crucial step in fingerprint classification and serves as a vital preprocessing stage. Thinning involves extracting the image skeleton and eliminating the redundant pixels to create a refined image. The resulting skeleton, often represented as a one-pixel thickened line, effectively reveals the image's topology.

Jaya Lakshmi et al. [103] used B-Splines and presented a method that is both quicker and more effective at eliminating impulsive noise while maintaining the image's edges. The

TABLE 4. Modes of fingerprint data acquisition.

Acquisition Mode	Issues
Contact Acquisition	Contact with a surface causes the 3D fingerprint ridge structure to disappear. The ridge surface may be affected by inadequate or excessive pressure.
Acquisition of flat fingerprints	The surface of the finger is flattened against the sensor's surface. Distortion could happen during the capture.
Acquisition of rolled fingerprints	Rolling the finger creates a 2D plane from the 3D finger structure.
Acquisition of inked fingerprints	Ridge surface friction is represented by the print that is impressed onto the card. A digital image which depicts a second-order ridge structure is generated by the card's inked impression. Errors may occur when optical scanning is used to convert the inked impression to digital format.
Contactless Acquisition	To optically display an illuminated finger surface, a 3D structure is transformed into a 2D plane.

TABLE 5. Fingerprint datasets overview.

Dataset Name	Description	No. of Images	URL
FVC2000	Benchmark dataset for fingerprint verification. Used in the FVC2000 competition.	3800	http://bias.csr.unibo.it/fvc2000/
FVC2002	Dataset for fingerprint verification, employed in the FVC2002 competition.	3200	http://bias.csr.unibo.it/fvc2002/
FVC2004	Fingerprint dataset utilized in the FVC2004 competition, focusing on verification tasks.	2560	http://bias.csr.unibo.it/fvc2004/
FVC2006	Fingerprint dataset utilized in the FVC2006 competition, focusing on verification tasks.	1800	http://bias.csr.unibo.it/fvc2006/
IIIT-D Latent	IIIT-Delhi's dataset containing latent fingerprints, suitable for evaluating latent print recognition.	1046	https://iab-rubric.org/index.php/mslfd
IIIT-D MOLF	Dataset from IIIT-Delhi featuring both optical and latent fingerprint images for multi-sensor evaluation.	19,200	https://iab-rubric.org/old1/resources/molf.html
IIIT-D MSLFD	IIIT-Delhi's latent fingerprint dataset designed with a multi-surface approach.	551	https://iab-rubric.org/index.php/mslfd
PolyU HRF	High-resolution fingerprint dataset from PolyU, valuable for assessing recognition algorithms at finer levels.	1560	https://www4.comp.polyu.edu.hk/~csajaykr/3Dfingerprint.htm
NIST D4	Fingerprint dataset provided by NIST, utilized for benchmarking fingerprint recognition systems.	4000	https://www.nist.gov/itl/iad/image-group/nist-special-database-4-fingerprint (database withdrawn)
BIOMET	Multimodal-audio, hand, face, fingerprint, and signature images	130 subjects	[102]

results are substantially better for forensic image edge preservation and noise removal than the linear and nonlinear filter approaches. Tertychnyi et al. [80] focused on extremely blurry fingerprint images that exhibited a variety of well-known aberrations, including dryness, wetness, dot presence, physical damage, and blurriness. The VGG16-based deep learning model was used to classify fingerprints and dry fingerprints with accuracies of 84% and 93% respectively. Taee and Abdulsamad [104] proposed the BRISK technique to extract important data from corner spots in the fingerprints. When compared to minutiae details, BRISK can pick up a lot more information because it is insensitive to changes in scale, illumination, and direction. An average EER of 0.004 and accuracy of 99.98% were obtained.

Khan et al. proposed a false patch removal strategy, which makes use of ''majority of neighbours'' to eliminate isolated and incorrectly classified patches. The Covolution Neural Network (CNN) model was trained to categorize image patches into fingerprint and non-fingerprint classes using Stochastic Gradient Descent (SGD). Following the false patch removal strategy, a Region of Interest (ROI) was constructed using the final set of patches. This process is employed to differentiate between the background and foreground of the latent fingerprint data. When compared to other methods in their literature analysis, the experimental results show gains in overall accuracy for the model when using the IIIT-D fingerprint database [105].

Nguyen et al. proposed the use of computer vision techniques in the image preparation stage which enhances the input image quality and quickly and accurately classifies the input photos in automatic fingerprint identification systems with huge databases, yet increases the computation time. This combination of improvements reduces the number of comparisons in these systems. The Random Forest (RF) model attained the highest accuracy of 96.75% when compared to SVM classifiers on the FVC 2000, 2002, and 2004 databases [106].

Kumar et al. introduced Image Enhancement Techniques (IETs) to enhance fingerprint images, thereby providing a matching process with more accurate feature extraction data. This overview encompasses a discussion of various IETs employed in Fingerprint Recognition (FPR) system. It details the types, uses, and roles of these enhancement techniques, offering valuable insights for researchers aiming to improve the accuracy and reliability of feature extraction in fingerprint biometric systems [107]. Chen et al. proposed an advanced image quality classification approach that can reject invalid input for the system's preprocessing stage to reduce response time, particularly for fingerprint-on-display (FoD) applications. A self-assembled dataset of 50,130 fingerprint images from FoD sensing was used to test the approach, which showed that it could achieve 95.83% [108].

The Table 6 provides an analysis of the performance of recent unimodal fingerprint biometric systems.

B. TECHNIQUES FOR FEATURE EXTRACTION AND CLASSIFICATION BASED ON FINGERPRINT PATTERNS

The performance of modern automated fingerprint recognition systems is significantly affected by feature extraction algorithm. Fingerprint patterns can be categorized into three feature extraction levels.

At Level 1, the focus is on global fingerprint patterns, encompassing the overall ridge flow. This level includes five categories: the left loop, right loop, whorl, arch, and tented arch. It captures detailed information regarding the friction ridge direction, pattern type, and singular points. Global ridge flow pattern are extracted even in cases of poor image quality.

At Level 2, features are associated with minutiae information, including ridge bifurcations and endings, making each fingerprint a unique pattern. Ridge endings, such as bifurcations, play a key role in defining Level-2 features.

At Level 3, features encompass ridge dimensional attributes like ridge path deviation, width, shape, sweat pore locations, geometric details of the ridges, and edge contours. This level also includes additional details like scars and incipient ridges, etc. Microscopes are typically used at this level, making them particularly relevant for forensic examiners. The Table 7 and Table 8 describes fingerprint feature extraction traditional and deep learning methods.

Fingerprint classification has evolved since the inception the of computer technology. Henry's classification method stands out as the most widely employed approach in fingerprint classification. Over time, this method has progressed to the automated fingerprint identification system (AFIS). The Table 9 presents the fingerprint matching methods.

Darlow et al. developed a minutiae extraction network, (MENet), a deep neural network that addresses the minutiae extraction using a machine learning challenge. MENet was trained with data-driven representations of minutiae points. A voting system is utilized to create training data, which is trained automatically on a large dataset for portability and robustness, and does away with tiresome human data labelling. A postprocessing method that uses MENet's output to locate the positions of the minutia is used. A minutiae misrate of 14.2% has been achieved on FVC datasets [89]. Hassanat et al. presented the task of feature extraction from low-quality images. The probability density functions for the features are used to represent them when evaluating the approach with other classifiers. Using in house databases, the highest identification accuracy obtained in several experiments was 95.11% [86].

Refoa et al. proposed an algorithm that assigns a unique value to each piece of information, speeding up person searches. The algorithm divides the fingerprint image into four distinct sections, systematically computing the attributes of every minutia within each section, and subsequently archives this information in a dedicated database tailored for this task. Rather than searching for a collection of 200 fingerprints for the latent, there will be a search of the 47 fingers database, which has 7731 minutiae [134]. Borra et al. proposed a novel method for classifying whether a fingerprint is genuine or false utilizing hybrid neural networks. The Bat algorithm and neural network were combined to optimize the weight factor [135].

Liu et al. intricately designed CNN models for the purpose of training a deep feature known as DeepPoreID for each individual pore. The similarity between these DeepPoreIDs is subsequently evaluated using Euclidean Proximity, which provides a measure of their resemblance. This innovative strategy enhances recognition accuracy. The proposed approach effectively addresses the challenges of imperfect fingerprint matching [136]. The fingerprint templates were created using the rotation and translation invariant properties of the minutiae found in the Delaunay triangulation by Surajkanta et al. Local ridge information derived from discrete curvature and, digital straightness was added to the features extracted from the Delaunay triangulation. FVC2000 experiments demonstrate that the proposed technique performs better in comparison [137], [138].

Soler et al. outlined a Fisher Vector approach that combines global and local data from a variety of local descriptors of features to improve the generalization abilities of PAD. Using unidentified scenarios with LivDet 2011 to LivDet 2017, experimental results shows a decrease in overall classification error rates approximately fourfold, with an accuracy of 96.17% [139]. CNN models such as Darknet, Alexnet, Resnet, Deep Belief Network, and VGG16 were utilized to develop the Henry Classification System as discussed by Souza et al. When tests were conducted using grayscale and previously processed images as input, the best accuracy of 95.1% on NIST database 4 is achieved when the Gabor filter and morphological thinning operation were combined [140].

Nahar et al. developed a CNN-based finger impression affirmation approach, without image preprocessing. The frame combines the coordination and extraction steps. Different filters with various parameter sets are used to realise feature elicitation; the matching junction connects the features that were extracted and generates the associated score. A total of 99.1% of samples are correctly categorized from the FVC2004 database [141].

C. FINGERPRINT INDEXING TECHNIQUES

In essence, searching the complete database is required at the identification step whenever a new fingerprint is submitted

TABLE 6. Analysis of the performance of recent unimodal fingerprint biometric systems.

Year	Author	Methodologies	Utilized Dataset	Performance	Resistant to attacks	Advantages	Drawbacks
2018	Pandya et al. [109]	Deep Histogram equalization, Gabor enhancement, fingerprint thinning, Deep CNN	Composed	Accuracy -98.21%	No	Model generalization	Performance on large database is not checked
2018	Lin et al. [110]	FCN, Siamese networks	Contactless 3D, Multi-view contactless	EER-0.64% on A database, 2.84% on B database	No	Performance improvement in partial 3D fingerprint identification, low storage	Partial 3D fingerprint imaging degrades matching accuracy
2018	Ajay et al. [111]	3D minutiae tetrahedron, Hierarchical tetrahedron	Composed	EER-1.41% for protocol A, EER-1.25% for protocol B, accuracy-99.27%	No	Recovered 2D minutiae to improve matching	Require structured lighting with scanners, multiple cameras, high cost, slow matching
2019	Minaee et al. [112]	CNN, visualization	PolyU	Accuarcy-95.7%	No	Useful in scenarios with limited labeled images per class	Not discussed other performance variables
2020	Anand et al. [113]	DeepResPore, PoreNet, Euclidean distance-based	PolyU HRF, IITI-HRF	2.27% and 0.24% EERs on partial and complete fingerprints	No	High-resolution fingerprint images considered	Robustness not discussed
2021	González-Soler et al. [114]	PHOW, BoW, FV, VLAD, SVM	LivDet 2011-2019	Overall accuracy -96.17%	Presentation	Low BPCERs ,detects known, unknown attack	Computational cost-FV encodings
2022	Chhabra et al. [115]	Stacked convolutional autoencoder, CNN	IIIT-D	Segmentation accuracy-98.45%	No	Reduction of irrelevant information	Not dealing noisy images
2022	Li et al. [116]	IndexMinMax, partial hadamard	FVC2002, FVC2004	EER-3.90%	Brute force ARM False Accept	Security all aspects covered	Scalability, reliability not mentioned, quality of the images decrease accuracy
2023	Chhabra et al. [115]	Autoencoder with CNN	IIIT-D	Segmentation accuracy-98.45% , MDR-1%, FDR-1%	No	Patch-based approach decreased the misclassification rate and false classification rate	Reliability not discussed
2023	Rai et al. [117]	MobileNet, SVC	LivDet 2011-2019	Overall accuracy -98.64%, 99.50%, 97.23%, 95.06%, 95.20%	Presentation	Model works for cross-material, cross-sensor	Training time is more

PHOW: Pyramid Histogram of Visual Words, BoW: Bag-of-Words,FV: Fisher Vector, VLAD: Vector Locally Aggregated Descriptors-encoding methods,SVM: Linear Support Vector Machine,BPCER: Bona Fide Presentation Classification Error Rate, SVC: Support Vector Classifier, FCN: Fully Convolutional Network, MDR: Missed fingerprint Detection Rate, FDR: False fingerprint Detection Rate

and the goal is to locate the fingerprint from the huge database that is most similar as shown in Figure 5. For large databases, identification is computationally intensive. Cost-effective identification results from reducing the search space from the whole database to a limited size list. These systems are divided into four main categories: deep learning based, hybrid, minutiae-based, and texture-based. These schemes involve deep features, texture, and Levels 1 and 2.

1) Fingerprint Indexing using Texture:
The ridge flow structure, ridge frequency field, ridge pattern types, ridge orientation field, and core and delta points that comply with the fingerprint database index are global features used in these indexing techniques [143], [144].

2) Fingerprint Indexing using Minutiae:
These methods create feature vectors using minutiae. These can be further divided into minutiae cylinder-code based techniques, minutiae k-plet, minutiae doubles, minutiae triplets, minutiae quadruplets, and minutiae quadruplets. It has been noted that details contain more unique information than the number and direction of ridges [145].

3) Hybrid Fingerprint Indexing:
To achieve greater accuracy, they leverage both minutiae, and non-minutiae features, by combining global and local features [142].

4) Fingerprint Indexing employing a Deep Neural Network:

TABLE 7. Fingerprint feature extraction traditional methods.

Year	Author	Method	Description	Advantages	Disadvantages
2013	Kumar et al. [118]	Directional Filters	Emphasizes directional information.	Robust in ridge structure analysis	Limited in handling complex patterns
2015	Park et al. [119]	Fourier Transform	Represents patterns in the frequency domain.	Effective for global structure analysis	Sensitive to noise, complex computation
2016	Maltoni et al. [83]	Singular Points	Identifies core and delta points.	Robust in pattern recognition	Limited in capturing local details
2016	Yuan et al. [120]	PCA	Reduces dimensionality.	Feature reduction, data visualization	Loss of local details
2017	Daugman et al. [121]	Gabor Filtering	Captures texture and frequency information.	Good for texture analysis, robust	Computationally intensive
2017	Smith et al. [122]	Minutiae-based	Extracts minutiae points from fingerprint ridges.	High accuracy, well-established	Sensitive to image quality, prone to noise
2018	Johnson et al. [123]	Ridge Counting	Counts ridge features.	Simple, fast computation	Sensitivity to image variations
2019	Miller et al. [124]	Phase-based Features	Focuses on phase information.	Enhancement of fingerprint patterns	Sensitive to noise, less robust
2021	Mua et al. [125]	local binary pattern (LBP)	Describes local patterns using binary codes.	Simple, effective for texture analysis	Sensitivity to noise, less discriminative

TABLE 8. Fingerprint feature extraction deep learning methods.

Year	Author	Method	Description	Advantages	Disadvantages
2016	Dey et al. [126]	Autoencoders	Unsupervised learning of efficient data codings	Unsupervised learning, dimensionality reduction	May require substantial computational resources
2017	Li et al. [127]	Siamese Networks	Learn similarity between two inputs	Effective for verification tasks, handles varying image qualities	Requires paired training data
2017	Shazeer et al. [128]	Attention Mechanisms	Allows the model to focus on specific image regions.	Enhanced feature extraction, interpretability	Increased model complexity
2018	Minaee et al. [129]	GANs	a generative model framework for fingerprint image synthesis	Generates realistic fingerprint images with high variability	Training stability issues, sensitive to hyperparameters
2021	Singh et al. [130]	Capsule Networks	Overcome limitations of traditional neural networks	Improved generalization, resistance to adversarial attacks	Limited research compared to traditional CNNs

A feature vector with a fixed length is created by applying a deep neural network that can extract the fingerprint's pattern [76]

Cappelli et al. proposed employing ridge-line orientation and frequency-based scalar and vector feature indexing methods. The evaluation of this technique involved six databases: NIST, FVC2000 DB2, FVC2002 DB3, and FVC2002 DB1. This study revealed that the average search time for locating a fingerprint in the NIST DB4 database was 1.6 milliseconds. However, the authors suggested that the technique could be further enhanced by decreasing the number of score computations through the utilization of spatial data structures and ad-hoc clustering methods [143].

Cao et al. a Convolutional Neural Network (ConvNet) was used to construct a fingerprint indexing system. ConvNet is then trained using a sizable longitudinal fingerprint database, where each finger has been captured many times over time. Experimental findings on the NIST SD4 and NIST SD14 datasets demonstrate that the proposed approach outperforms the most recent fingerprint indexing techniques described in the academic literature [100]. Perez et al. considered impressions from diverse databases, transforming them into sets of interconnected tiny cylinder codes to construct indices using k-means++ clustering. Through this method, the search space is significantly reduced by four orders of magnitude, particularly when dealing with background databases containing over one million impressions [146].

To provide an indexing method for pore-based features in high-resolution fingerprints, a dynamic pore filtering technique was created by Anand et al. and utilized to obtain pores from high-resolution fingerprint images. A pore descriptor was used as an indexing feature vector. Next, a cluster-based retrieval approach was used to efficiently and rapidly extract the candidate list. In their literature review, DBI and IITI-HRFP's partial fingerprints that contain fingerprints showed that the method outperforms minutiae-based fingerprint indexing methods [147].

Bai et al. introduced a novel approach known as the deep compact binary minutiae cylinder code (DCBMCC), which offers a practical and distinctive representation of features

TABLE 9. Fingerprint matching methods.

Year	Author	Method	Description	Advantages	Disadvantages
2017	Peralta et al. [131]	Minutiae-based	Matches fingerprint templates based on extracted minutiae points.	Well-established, widely used, provides high accuracy	Sensitivity to noisy input, Limited feature representation
2019	Castillo et al. [132]	Ridge-based	Utilizes ridge patterns for matching fingerprints	Robust against some distortions, suitable for low-quality images	Limited effectiveness in complex patterns, Less discriminative than minutiae-based methods
2020	Liu et al. [133]	Deep Learning-based	Employs deep neural networks for feature learning and matching	Capture complex patterns, less dependency on handcrafted features	Requires large amounts of labeled data, computationally intensive training

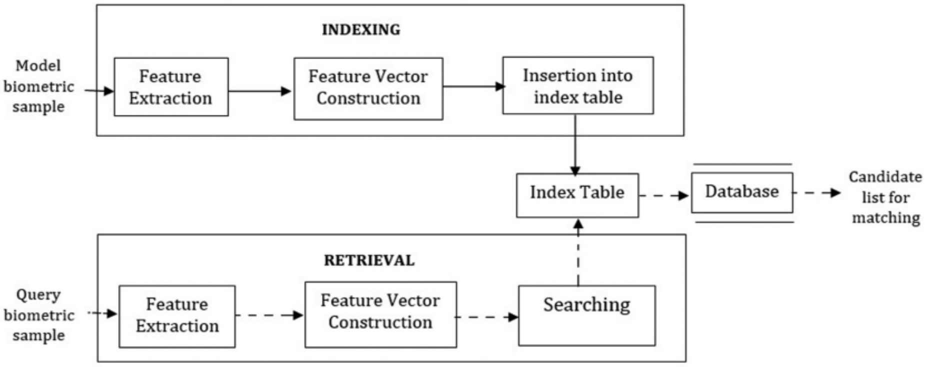


FIGURE 5. A fingerint biometric system's indexing and retrieval process (source: Gupta et al. [142]).

for fingerprint indexing. Their proposed fingerprint indexing strategy, leverages multi-index hashing and, accelerates precise scans within the Hamming space by creating multiple hashing tables using binary code substrings. According to the authors, this method demonstrated a low penetration rate and minimal error rate [148].

D. FINGERPRINT BIOMETRIC SYSTEM LIVENESS DETECTION TECHNIQUES

Yuan and Sun [85] developed a novel software-based method utilizing the rotation-invariant local binary pattern (RILBP) and multiscale wavelet transform to assess the liveness of a fingerprint. Jiang and Liu [149] introduced an original software-based liveness detection approach that, incorporates a spatial pyramid and uniform local binary pattern (ULBP) to discern the authenticity of a fingerprint. Yuan and Sun proposed the creation of novel software designed to enhance the classification accuracy and counteract spoofing attacks across various fingerprint sensors. Their innovative software-based liveness detection approach utilizes a multiscale wavelet transform and rotation-invariant local binary pattern (RILBP). Experimental results, based on the LivDet 2011 dataset, indicate that this method exhibits improved classification performance in detecting fingerprint liveness compared to existing fingerprint liveness detection (FLD) methods [85].

Xia et al. proposed a feature extraction technique to address the FLD (Fingerprint Liveness Detection) problem. Utilizing the Weber Local Binary Pattern (WLBP) and Circularly Symmetric Gabor Feature (CSGF), the features analyze fingerprint images in both the spatial and frequency domains. The final features are derived based on the likelihood of occurrence of the two components. These features were employed to train classifiers using SVM separately on two databases for the FLD Competitions in 2011 and 2013 [150]. Mehboob et al. implemented Shepard magnitude and orientation for real-time fingerprint recognition via separate quantization of both global and local features retrieved from the space and frequency domains. In accordance with these findings, the average error rate for LivDet 2011–2015 were reduced to 5.8, 5.3, and 2.2 respectively [151].

Zhang et al. proposed Slim-ResCNN, which is a slim yet powerful network topology composed of stacks of enhanced residual blocks. The primary purpose of the improved residual blocks is to reduce processing time and prevent overfitting when determining whether a fingerprint is alive. With an overall accuracy of 95.25%, the fingerprint liveness recognition accuracy based on the LivDet2013 and 2015 datasets significantly increased. Slim-ResCNN won the 2017 FLD competition's top prize [152]. Yuan et al. developed an enhanced Deep Convolutional Neural Network (DCNN) incorporating picture scale equalization and a Fingerprint Liveness Detection (FLD) method to maintain image resolution and texture information. Notably, their study introduces the use of the confusion matrix as a performance measure in the evaluation of FLD for the first time. Experimental results, based on the LivDet 2011 and LivDet 2013 databases, further support the method's superior performance in terms of detection accuracy [153].

Yuan et al. introduced an autoencoder designed to automatically identify rich hierarchical semantic features in the samples. Specifically, a stacked autoencoder is employed for real-time fingerprint liveness detection (RFLD). The model comprises two components: Fingerprint Liveness Detection (FLD) utilizing supervised learning and parameter pre-training established through unsupervised learning. The testing outcomes confirm the robust performance of both detection and RFLD, as demonstrated on the LivDet 2011 and 2013 datasets, validating the efficacy of the proposed approach [154].

Chitra et al. designed a fuzzy vault system with a key-binding technique and the ability to account for data variance among classes. The minutiae of the fingerprint image were utilized to perform the approach. The fuzzy vault scheme is a polynomial function-encoding cryptography technique [155]. Hernandez et al. suggested a template-protection strategy utilizing a fuzzy vault system. Helper data are gathered in a key-binding crypto scheme by fusing biometric information with the key [156].

Chauhan et al. developed a better fuzzy commitment method. The error-correcting codes (ECC) decoder, encoder, data base, feature extraction, and comparator modules are the five components of the technique. The encoding process is managed by an error-corrective encoding module. The comparator module assesses whether the verification is successful by comparing the hash value acquired by the key to the stored hash value [157]. Soliman et al. developed a comb filter-based cancellable iris recognition system. Gabor filter was used as a local band-pass filter. The Gabor filter localizes the frequencies in an image with ideal joint localization, in contrast to the Fourier transform, which simply identifies the spatial frequencies in an image. Coarse-to-fine segmentation was used to construct iris code [158].

Abikoye et al. proposed a steganography and cryptography-based template generation technique using the Twofish algorithm to produce a cipher image. To address the issue of exploiting and hacking biometric templates, this study combines steganographic and cryptography techniques known as the least significant bits [159]. Panchal et al. proposed a method that utilizes finger biometrics to generate cryptographic keys. This technique involves extracting minute, core, and delta points from the fingerprint image. Subsequently, straight line features are established by breaking the image into smaller blocks, and the points on each block are related to those on the adjacent blocks. These components were then integrated to generate a bio-crypto key [160].

E. FINGERPRINT BIOMETRIC SYSTEM PERFORMANCE IMPROVEMENT TECHNIQUES

Yang et al. proposed a fingerprint authentication method that enhances authentication performance without requiring additional sensor data by using 3D Delaunay triangulation. Each block of a three-dimensional Delaunay triangulation, a Delaunay tetrahedron, may provide better discrimination over a Delaunay triangle [138]. Thejaswini et al. presented an reference algorithm, which is a method of adaptive auto-correction. The system modifies the user's reference biometric templates to increase identification rate based on the collected fingerprint template and daily similarity score. A total of 250 fingerprint templates from 10 individuals were gathered at 25°C to 0°C for analysis. The trial results showed that applying the auto-correcting technique increased the rate of identification by 40% [161].

Oh et al. discussed a method to capture finger images from smartphones and preprocess them so that they can quickly compare them to images from optical sensors also techniques for recording and enhancing finger images, extracting fingerprint patterns, finding core points, and aligning image. EER ranging from 6% to 15%, which falls within the allowable bounds [162]. Noor et al. contributed MATLAB classifiers aimed to improve the performance of fingerprint recognition systems. The classifiers encompassed a Fine K-Nearest Neighbor, Linear Discriminant Analysis, Decision Tree, Medium Gaussian Support Vector Machine (MG-SVM), and Bagged Tree Ensemble. Among these classifiers, the MG-SVM by achieve the highest verification rate of 98.90% among all the classifiers employed [163].

"Associative memory in alter multi-connect architecture," a novel technique Almajmaie proposed, has pattern recognition processing period of about thirty seconds for the FVC2004 database, the internal database, as well as International NIST database 4, with an average rate of accuracy of 99.56% [164]. A rapid rate of recognition was achieved when numerous fingerprint features, such as ridges ends and ridge bifurcations, were combined by Vidyasree et al. Numerous spoofing attacks are addressed by autoencoder (AE), which also achieves revocability. A minimal cost matcher (MCM) was utilized to maximize the accuracy of the multi-representation system [165]. Li et al. proposed an innovative method for modifying fixed-length bit strings called the "minutia vicinity combination feature" (MVCF), which enables reasonable bit-string conversion speed and accuracy makes use of spectral clustering and the recently established discriminative biometric representation. The performance assessment, which uses the benchmark data collections FVC2002 DB1, DB2, DB3, and FVC2004 DB1, DB2, and DB3 which are available to the general public, confirms the superiority of the offered solution [166].

Rojas et al. devised a fingerprint identification methodology utilizing an Ensemble Subspace Discriminant Classifier, Wavelet transform, and multiple domain feature extraction. The proposed strategy demonstrated the highest accuracy 97.5% among the FVC2000-2004 databases [167]. Mo et al. developed a person recognition method using Wi-Fi channel state data based on deep learning. Performance analysis showed that the convolutional long-and short-term memory (CLSTM) model is appropriate for the application, with an accuracy of 92% and can recognize up to eight subjects [168].

F. HIGH CAPACITY FINGERPRINT BIOMETRIC SYSTEMS

High capacity fingerprint biometric systems are used to efficiently manage large volumes of fingerprint data, facilitating the processing of extensive user databases or transaction volumes.

Chundi et al. introduced a method that leverages pre-stored patterns to estimate the capacity while employing a Hopfield neural network for learning. To mitigate the risk of network overflow and potential replacement of recorded traces, the model systematically updates the crosstalk associated with the stored patterns. Experimental results using the NIST database 10 demonstrate that the system exhibits 2.7 to 8 times greater memory capacity than baseline systems utilizing static capacity estimations [169].

Moga et al. described a Siamese network that compares two input images using two metrics, each of which has a threshold that has been defined through experimentation. When comparing the accuracy rates from the CASIA and SOCOFing datasets, the findings obtained using VGG-16 demonstrate that the test data accuracy rates close to the mean accuracy rate of 87% [170].

G. CONTACTLESS FINGERPRINT IDENTIFICATION

Innovations in fingerprint recognition technology have enabled identification without the need for physical contact, providing both convenience and hygiene advantages.

Yin et al. introduced a non-contact fingerprint identification method that utilize loose genetic algorithms and global minutia topology. To enhance the accuracy of minutiae correspondence, a robust approach for boosting minutiae pairs is employed, addressing the issue of inaccurate minutiae alignment commonly observed in traditional transformation-based methods. The effectiveness of the proposed technique was assessed using contactless fingerprint benchmark databases DB1 and DB1-A [171].

Yin et al. proposed a novel characteristic known as 3D Topology Polymer (TTP). This characteristic involves projecting 3D minutiae onto multiple 2D planes, utilizing the TTP properties to effectively represent the three-dimensional architecture of the minutiae distribution [172]. Labati et al. investigated fingerprint biometric techniques specifically tailored to smartphones. This study primarily emphasizes 2D contactless fingerprint identification systems, covering aspects such as image collection, preprocessing, template extraction, and comparison [173]. Veena et al. considered the polynomial curve coefficients of a 3D fingerprint image as a template. The curve was calculated by measuring the separation between the minute details and singular points [174].

VI. FINGERPRINT BIOMETRIC AUTHENTICATION VULNERABILITIES

In this section, we describe and classify several potential attack weak spots of fingerprint biometric authentication [2].

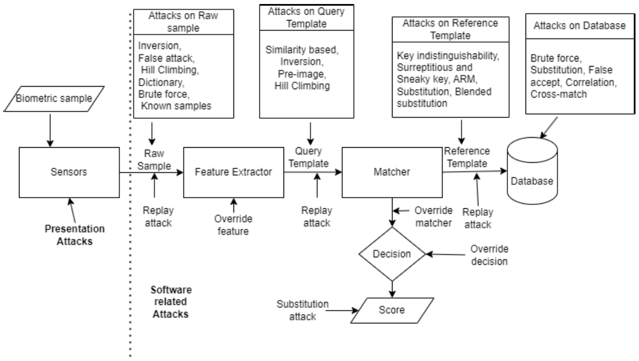

Attacks on Raw sample
Inversion, False attack, Hill Climbing, Dictionary, Brute force, Known samples
Attacks on Query Template
Similarity based, Inversion, Pre-image, Hill Climbing
Attacks on Reference Template
Key indistinguishability, Surreptitious and Sneaky key, ARM, Substitution, Blended substitution
Attacks on Database
Brute force, Substitution, False accept, Correlation, Cross-match
Biometric sample
Sensors
Raw Sample
Feature Extractor
Query Template
Matcher
Reference Template
Database
Presentation Attacks
Replay attack
Override feature
Replay attack
Override matcher
Replay attack
Decision
Override decision
Software related Attacks
Substitution attack
Score

FIGURE 6. Fingerprint biometric system vulnerabilities.

1) Faking the sensor: Attackers use synthetic fingers, photos, or voice recordings to deceive the biometric sensor, substituting genuine features with fabricated ones.
2) Resubmitting biometric signals: Attackers replay recorded signals, obtained through network eavesdropping, to bypass the sensor during subsequent authentication attempts.
3) Common server network attacks: Attackers exploit vulnerabilities like SQL injection to access the server, gaining unauthorized access to sensitive data, including biometric information.
4) Override the matcher: Attackers compromise the matcher to manipulate match scores in their favor.
5) Changing templates: Attackers alter templates to associate legitimate identities with fraudulent ones.
6) Data modification over the channel: Attackers intercept and tamper with templates sent over the communication channel.
7) Changing the result: Attackers manipulate authentication outcomes to their advantage [175].

Fingerprint biometric systems are vulnerable to two types of attacks: software-related and presentation. Presentation attacks involve presenting fake material to the sensor to trick the system into granting unauthorized access. These attacks are common with iris, face, and fingerprint modalities. Software-related attacks exploit system weaknesses using advanced tools and hacking skills. The weak areas of a fingerprint biometric system is shown in Figure 6.

1) Brute-force attack: An attacker tries various password and key combinations to gain system access, resulting in significant computational complexity due to the need to examine every possible combination.
2) Record Multiplicity attack: The attacker aims to obtain the original template by correlating several encoded templates made using the same biometric.
3) Lost token attack: The attacker uses information about the victim, such as a token or password, to approximate the original template, requiring a computational complexity of 2^m for m features.

4) Dictionary-based attack: The attacker tries samples with the highest chance of success based on a predefined dictionary of likely passwords.
5) Spoofing attack: The attacker employs prosthetic fingers, recorded videos, or contact lenses to deceive the biometric sensor.
6) Database template theft: The hacker gains access to stored templates and attempts to create a physical copy using reverse engineering.
7) Cryptanalysis attack: The attacker tries to extract plaintext from encrypted text without knowledge of the encryption algorithms.
8) Stolen biometric feature attack: The attacker uses stolen biometric features to attempt logging into systems and applications with different key combinations.
9) Hill-climbing attack: Synthetic user biometric templates are repeatedly presented to the matcher until successful recognition, with data altered based on previous attempts.
10) Inverse attack: The number of changed features for each reference point is mapped back to the original arrays.
11) Pre-image attack: The attacker looks for samples with similar features to spoof a biometric system, employing a brute-force approach.
12) Cipher text only attack (COA): An intrusive attempt to recover plaintext from ciphertext in a symmetric key cryptosystem.
13) Known plaintext attack (KPA): The attacker has access to both plaintext and ciphertext to uncover hidden data, including cryptographic keys.
14) Chosen ciphertext attack (CCA): By decrypting selected ciphertexts, the attacker learns the transformation or secret key.
15) Equation attack: Various equations with parametric variables are used to create templates.

Fei et al. evaluated adversarial attack approaches and emphasized the importance of anti-adversarial protection in deep learning applications [176]. The RTK-PAD method achieved promising results in countering presentation attacks, with a true detection rate (TDR) of 91.19%, an average classification error (ACE) of 2.28%, and a false detection rate (FDR) of 1% [177]. Additionally, the OCPAD model and the OCT fingerprint PAD demonstrated efficient spoof detection capabilities using optical coherence technology, achieving a true positive rate (TPR) of 99.43% at a false positive rate (FPR) of 10% and an accuracy of 81.89% with a low error rate of 0.67%, respectively [178], [179].

Popli et al. proposed a hybrid fingerprint system for spoof detection and matching, achieving a TAR of 100%, a FAR of 0.1%, and an accuracy of 98.56% on the LiveDet 2015 dataset [180]. Husseis et al. designed a presentation attack instrument species evaluation mechanism compliant with ISO/IEC 30107 specifications, showing effective presentation attack recognition with low error rates [181].

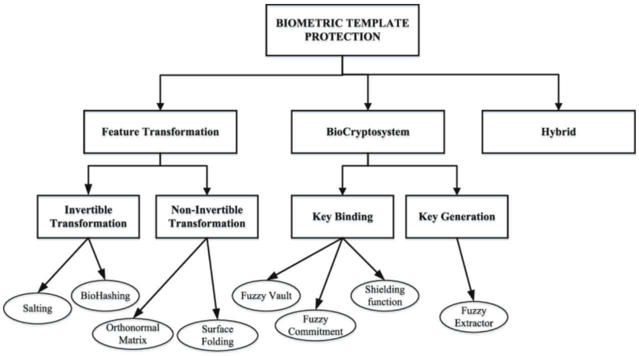


FIGURE 7. Fingerprint template protection categories (source: Garcia-Salicetti et al. [102]).

An overview of the attacks related to fingerprint and the necessary countermeasures is provided in Table 10.

A literature review of recent attacks on fingerprint recognition systems is presented in Table 11.

VII. PROTECTION OF FINGERPRINT BIOMETRIC TEMPLATES

Different categories of fingerprint biometric protection [102] are shown in Figure 7. Feature transformation and biometric encryption are the two categories under which biometric template protection techniques are categorized [226]. A summary of fingerprint biometric template protection methods is given in Table 12, an overview of the recent template protection methods against brute force attacks is given in Table 13, and an overview of recent fingerprint template-protection methods against inversion attacks is given in Table 14. An overview of recent fingerprint template-protection methods against other software attacks is provided in Table 15.

A. FEATURE TRANSFORMATION

Feature transformation and biometric encryption are the two categories under which biometric template protection techniques are categorized. Based on these categories, we investigated and discussed the available biometric template methodologies available in the literature.

Cancellable biometrics enable the replacement of compromised templates, addressing limitations of traditional authentication methods like passwords [227]. These schemes modify biometric data through transformations to maintain security and allow for the issuance of new templates if needed. Recent advancements in deep learning and error-correction coding enhance security in multi-biometric systems [228], with researchers exploring fusion architectures and integrating secure sketch cancelable blocks (SSTB) and cancelable template blocks (CTB) to bolster system resilience.

Bio-hashing, a method for protecting biometric templates, utilizes a transformation function controlled by a user-specific password or secret key to modify features from an existing template [229]. While it enhances template entropy,

TABLE 10. An overview of the fingerprint attacks with the necessary countermeasures.

Attack point module level	Countermeasures
Attack at sensor module	Liveness detection
Attacks at the point where two modules interface	Challenge-response strategies or usage of time-stamps
Attacks at the software module	Specialized hardware capable of ensuring software is executed securely
Attacks at biometric template database	Biometrics template protection strategies

TABLE 11. A literature review of recent attacks in fingerprint recognition systems.

Year	Author	Dataset	Attack/s	Module Level	Method for detecting attacks	Results
2017	Wang et al. [182]	FVC2002 FVC 2004	ARM	Matcher-decision	Partial discrete Fourier transformation with zoned minutiae pairs	EER-0.19,1,4.29% on FVC2002-DB1,2,3 -EER-9.01%-FVC2004-DB1
2019	kim et al. [183]	LivDet 2011, 2013,2015	Presentation	Sensor	2 GAN model to produce a fingerprint, master minutia set, One half million parameters	Average detection error rate of 1.57%
2019	Hussein et al. [184]	Customized (778 images)	Presentation	Sensor	CNN classification not discussed model parameters	APCER, BPCE fusion score-0 fusion achieves an AUC-1.0
2019	Roy et al. [185]	FingerPass FVC 2002 DB1 DB1-A,AES3400	Dictionary	Matcher-decision	CMA-ES DE,PSO	FMR of 0.1% attacked 47% users-FingerPass DB7,84% users-FVC
2020	Abdullahi et al. [186]	FVC 2002 FVC 2004	ARM, false accept, brute force	Matcher-decision	Mellin transform Fractal coding	0.364%, 0.538%, 2.395% on FVC2002-DB1,2,3 EER-2.348%,5.925%, 2.365% on FVC2004-DB1,2,3
2020	Raj et al. [187]	FVC 2002 ATVS CASIA	Hill-climbing	Sensor	Nonlinear optimization partial discrete	Average matching score-111.2, 97.17,111.07
2021	Lai et al. [188]	FVC 2002 LFW	False Accept	Sensor	Sample	EER-1.38%
2021	Donget al. [189]	LFW	Pre-image/ similarity-based	Matcher-decision	Genetic Algorithm facilitated similarity-based attack framework (GASAF)	FAR-14.19%
2021	Shahzad et al. [190]	FVC 2002 FVC 2004	ARM Masquerade	Matcher-decision, Sensor	Window-shift XOR, Partial discrete wavelet transform	EER-1.57%, 1.50%, 4.93% on FVC2002-DB1,2,3 EER-10.49%, 8.62% on FVC2004-DB1,2
2021	Lee et al. [191]	FVC 2002 LFW FVC 2004	ARM, reverse, birthday, false accept, brute force	Matcher-decision, database	Partial discrete wavelet transform, Window-shift XOR	EER-0.31±0.14 on FVC2002-DB1+LFW EER-0.46±0.17%on FVC2004-DB2+LFW EER-0.53±0.16% on FVC2004-DB1+LFW
2021	Tran and Hu [192]	FVC 2002 FVC 2004	Pre-image, hill climbing, ARM	Matcher-decision	Multifilter framework-EMCC, KNN	EER-0.23%, 0.08%, 1.46% on FVC2002-DB1,2,3 EER-3.25%-FVC2004-DB2
2022	Park et al. [193]	LivDet 2015	Presentation	Sensor	NN + CNN models-combined via weighted voting technique not discussed model parameters.	99% classification accuracy
2022	Sun et al. [194], [195]	NIST SD4	Inversion	Sensor	Mapping function	TAR of about 98.3%, FAR of 0.01%

APCER: Attack Presentation Classification Error Rate, BPCER: Bonafide Presentation Classification Error Rate, EMCC: EnhancedMinutia Cylinder Code,LFW ,CMA-ES: Covariance Matrix Adaptation Evolution Strategy, DE: Differential Evolution, PSO: Particle Swarm Optimization

it may exhibit reduced performance compared to cancellable biometrics when adversaries present legitimate tokens. For instance, Hakan et al. applied bio-hashing with a fixed-length template generated through spectral minutiae representation, achieving an EER of 0% in FVC2002 databases, with the lowest EER in the stolen token scenario recorded at 14.77% in the FVC DB1 database [230]. Another variation, "Index-of-Max" (IoM) hashing, developed by Jin et al. [208], converts real-value biometric feature vectors into discrete indexed hashed codes, yielding an EER of 4.10% in the stolen token scenario. Additionally, Ghammam et al. [218] introduced a transformation function effective against specific attacks, embedding biometric data into an orthogonalized pseudo-random numeric matrix created using a secret key or token and nonlinear operations, with an EER of 0.4% at a GAR of 99%.

B. BIOMETRIC CRYPTOSYSTEMS

Simple dictionary attacks have always compromised identity authentication techniques that rely on short passwords, Cryp-

TABLE 12. A summary of fingerprint biometric template protection methods.

Year	Author	Method	Methodology	Advantages	Disadvantages
2016	Sadhya et al. [196]	Key-binding Biometric Cryptosystem	Production of cryptographic keys are derived from the biometric characteristics	Beneficial for cryptographic applications	Challenging to attain key stability with entropy
2019	Lutsenko et al. [197]	Key-generating Biometric Cryptosystem	The key and the biometric template are both embedded in the helper data	Error-correcting is used to control intra-user variability	Decreased accuracy in matching as a matcher with specialized error-correcting capabilities is needed,diversity and revocability not provided
2019	Alloghani et al. [198]	Homomorphic encryption	Homomorphic encryption is employed to biometric encryption data using a public key	Protection method without the verification accuracy	Slow process, limiting applications
2019	Vijay et al. [199]	Hybrid	Integrate different template security methods including their strengths	Improved security with improved accuracy	Sometimes suffer discriminability loss
2019	Kumar et al. [200]	Steganographic	Data-concealing techniques within another biometric	Safe for sending raw biometric data via insecure channels	Attacks could occur while raw biometric data is being transmitted
2020	Manisha et al. [201]	Cancelable Biometrics	Non-invertible transformation function	Keyless transformation,difficult to get the original template	The function should meet both noninvertibility and discriminability
2020	Kant et al. [202]	Watermarking	Hide a biometric template into another	Challenging to determine whether a watermark is present in an authenticated work without the key, forging the saved biometric is difficult	Challenging to provide restriction to access the key, time complexity is high
2021	Tarek et al. [203]	Salting	Transformed function defined by K,unique to each person	Low FAR, produce several templates from the same user using different key	Impossible to manage significant intra-user variances

tographic secret keys and passwords have been suggested to overcome these restrictions. Biometric cryptosystems fall into two categories: key generation and binding.

1) Key Generation: Biometric cryptosystems generate keys directly from biometric data, offering secure sketching and fuzzy extractors for this purpose.
2) Key Binding: In key binding, a secret key is securely bound with a biometric template, preventing decryption without knowledge of the user's biometric data. Key binding-based cryptography includes fuzzy commitment and fuzzy vault techniques.
   Fuzzy Vault: A cryptographic architecture utilizing fuzzy vaults securely encrypts and decrypts sensitive data. However, it faces drawbacks such as susceptibility to biometric template cross-matching, vulnerability to statistical analysis attacks, and the potential for attackers to replace biometric features or steal the original template if made public.
   Fuzzy Commitment: This technique protects biometric features stored in binary vectors, ensuring secure representation using uniformly randomized keys and appropriate error-correcting codes [227].

Other biometric template protection techniques have been employed, such as watermarking schemes, elliptic curve cryptography (ECC), homomorphic encryption, and Rivest, Shamir and Adleman (RSA) [198].

Elmouhtadi et al. proposed a technique based on the alteration of fingerprint features to safeguard the fingerprint template data. It uses a minutiae triplet-based indexing method and transformation. The results show that the suggested defense mechanism is tolerated by the altered attack [231]. Trivedi et al. produced a non-invertible fingerprint template that contained only relative geometric information about small spots. The suggested template can withstand the reconstruction process, deformation, rotation, and translation. The suggested method performed better in testing using the traditional FVC2000 database with regard to EER and FMR [232].

Wang et al. produced partial Hadamard fingerprint templates that can be cancelled. satisfying the demands of performance, variety, non-invertibility, and revocability. The EER for the suggested method in the case of a lost token is 1% for FVC2002 DB1, 2% for DB2, and 5.2% for DB3In the event if a token is lost, the recommended method's EER is 1%, 2%, 5.2% for FVC2002-DB1, 2 and 3 respectively [212]. Mahto et al. proposed Elliptic Curve Cryptography (ECC) plus a fingerprint biometric one-time password authentication method. Customers produce their ECC secret keys using their fingerprints [233]. Haddada et al. proposed a hybrid watermarking technique that was confirmed on fingerprint and face images at two levels to safeguard biometric data. The two watermarking methods preserve the watermarked image while enhancing the integrity of the watermark and the host image. In the initial stage, the face acts as the host image, and small particles are employed as the watermark. The fingerprint acts as a host image in the next stage, with the previously watermarked face acting as a watermark [234].

Ali et al. provided a safe approach that uses the location information from the minutia points to construct a user-specific template. Each minutia point is given a securely adjusted position using the minutiae of its neighbors and a key set. Using the FVC2002 DB1, DB2, and DB3 fingerprint databases, they obtained an EER of 0.00% under the same key situation. They considered two user key sets for every

TABLE 13. An overview of the recent fingerprint template protection methods against brute force attack.

Year	Author	Methodology	Attack/s	Dataset	Results	Drawbacks
2018	Kim et al. [204]	Custom locality-sensitive hashing method with Indexing First Order hashing orthogonalized pseudo-random numerical matrix using nonlinear operations	Brute force, COA, KPA, false accept, CCA	FVC2002 FVC2004	EER-0.30% FAR-0.30% system threshold value-0.86	Performance could be improved using point based representation for fingerprint minutia
2019	Kim et al. [205]	Sparse Combined Index-of-Maximum (SC-IoM) hashing	Brute force Inversion false accept	FVC2002 FVC2004	EER-0.43%,0.32% ,2.02% on FVC2002 1.92%,4.97,% 1.86% on FVC2004	No visible trade off between performance and security
2019	Djebli et al. [206]	User-specific random projections are applied to Scale Invariant Feature Transformation(SIFT) followed by quantization	Brute force	FVC2002 -DB1-3	EER-1.78%	Decrease in DB3 distorted image performance
2019	Kho et al. [207]	A new, alignment-free minutiae descriptor with a partially local structure	Brute force, false accept, ARM, inversion	FVC2002-DB1-3 FVC2004-DB4,DB2	EER-0%,0%,2%,6%,4%	Lack of performance-security tradeoff
2019	Jin et al. [208]	Partial Local Structure (PLS) descriptor Randomized Non-Negative Least Square (R-NNLS)	Inversion, ARM, brute force, false accept	FVC2002 FVC2004	EER-0.01%,0.06,% 3.61%-DB1-3 - FVC2002, 5%,4.51%-DB2, DB4-FVC2004 at threshold 20	Trade-off between performance and security
2020	Li et al. [209]	New Minimum Hash Signature (NMHS),Secure Extended Feature Vector(SEFV)	Brute force, birthday, false accept	FVC2002 FVC2004	EER-0.55%,0.93% ,5.81%,6.85% for FVC2002-DB1,2, FVC2002-DB1,2	Accuracy is better in unprotected instance
2020	Abdullahi et al. [186]	The domain fingerprint's minutiae blocks are combined with the Fourier-Mellin transform to provide feature alignment	ARM, false accept, brute force	FVC2002 FVC2004	0.36,0.54, 2.4%-DB1,2, 3-FVC2002 2.35%,5.93%, 2.37%-DB1-3 -FVC2004	Performance needs to be improved
2021	Baghel et al. [210]	Using the fuzzy vault approach separate the real vault points among an accumulation of chaff and real points	Brute force, inversion	FVC2002 DB1,2 FVC2004 DB1	GAR/FAR at threshold 14 & 10 93 / 3.39 97 / 3.11	Not discussed unlinkability
2023	Dang et al. [211]	Transform function Absolute Value Equations Transform (AVET) that non linearly projects features into another domain	Brute force, false accept, ARM	FVC2002-DB1-3	EER-0.05+-0.17%, 0.39+-.18%, 1.55+-0.37%	EER for DB1 dataset is comparable before and after protection

TABLE 14. An overview of the recent fingerprint template protection methods against inversion attack.

Year	Author	Methodology	Attack/s	Dataset	Results	Drawbacks
2017	Wang et al. [212]	Partial Hadamard transformation	Inversion	FVC2002 FVC2004	EER-1%,2%,5.2% -DB1,2,3-FVC2002 EER-13.3%-DB2 -FVC2004.	Performance decreased for low quality binary biometric representations
2017	Jin et al. [208]	Using Index-of-Max for Hashing (IoM)	Inversion, birthday	FVC2002 FVC2004	EER-0.22%,0.47%, 3.07%- DB1,2, 3-2002 4.74%, 4.10%, 3.99%, -DB1,2, 3-2004	Doesn't support variable-sized minutiae representation of a fingerprint.
2020	Trivedi et al. [213]	The Delaunay triangulation method for the minutiae point	Inversion	FVC2002	EER -1.2%,2.1% -DB1,2	Not discussed unlinkability
2021	Bedari et al. [214]	Fingerprint templates with MCC based on Dyno-key concept	Inversion, revoked template, masquerade	FVC2002 FVC2004 FVC2006	EER-1.38%, 1.35%, 4.21%-DB1,2, 3-FVC2002 8.89%, 7.63%%, 1.14% DB1, 2, 3-FVC2004 1.14%, 7.06%-DB2, 3-FVC2006.	Matching performance could be improved
2022	Wijewardena [195]	DeepPrint, deep learning method for representing fingerprints	Inversion	NIST SD4	TAR-85.95%, FAR of 0.01%	Boost the performance by enhancing Level-2 features in the biometric images reconstructed through embeddings of deep templates

TABLE 15. An overview of the recent fingerprint template protection methods against other software attacks.

Year	Author	Methodology	Attack/s	Dataset	Results	Drawbacks
2016	Jagadiswary et al. [215]	Key generation (using RSA) and feature extraction	Not mentioned	Customised	GAR-95.3% FAR-0.01%.	Not discussed ISO standards and attacks
2016	Nafea et al. [216]	Watermarking, shuffling and Hadamard matrix processes	JPEG brightness, contrast, brightness, additive white Gaussian noise geometric	FVC2002 -DB1	EER-0% at threshold 0.4109	Performance reduced when the shuffled key and Hadamard code are compromised, presence of noise
2017	Barrero et al. [217]	Protection of multibiometric templates via homomorphic encryption	Hill-climbing inverse	BiosecurID	EER-0.12%	Renewability must be attained
2018	Ghammam et al. [218]	Enhanced Bio-hashing method	Stolen token	FVC2002 DB1	EER-0.4% FAR- 99%	When raw features are used, the EER value is more than 22%
2018	Kim et al. [204]	Transformation function using Enhancement of BioHashing orthogonalized pseudo-random numerical matrix using nonlinear operations	Stolen token	PolyHK	EER-0.4% GAR-99%	Further analysis is required about template invertibility
2018	Stanko et al. [219]	Spectral representations of minutia pairs	Stolen key	MCYT, FVC2000-DB2, FVC2002-DB2	EER -1% for MYCT	Performance reduced for low quality images
2019	Atighehchi et al. [220]	GREYC-Hashing: Integrating secret information with biometrics Vector(SEFV)	Reversibility linkability false accept	FVC2002-DB1 FVC2004-DB1,2	EER-3.72,% 5.81%,6.85%	Performance could be increased by creating the projection matrix using the secret and the first biometric modality
2020	Mehmood et al. [221]	Fuzzy Vault in a modified form	Stolen key	FVC2002-DB1,2, 3,4	FAR,FRR,GAR -92%, 90%, 85%	FAR decreased as the polynomial degree increased
2021	Ali et al. [222]	alignment-free template protection	Plain key, stolen key	FVC2002-DB1,2	EER-0%	Not discussed unlinkability
2021	Donget al. [189]	Bio-Hashing, Bloom-filter	Pre-image	LFW	FAR-42.88% for 3 templates	Susceptible to an inversion brute-force attack
2022	Patil et al. [223]	The transformation procedure makes use of Lagrange's interpolation as well as the discrete cosine transform	Not mentioned	Customised	GAR-95.42%, FRR-4.57%	Time complexity is high
2022	Mohsin et al. [224]	Enhanced Bio-hashing method with enhancement of BioHashing	Stolen token	FVC2002	EER- 2.7,% FRR=0.8%	Difficulty in representing the minutiae into fixed-length feature vector,decrease in performance FRR increase by 4% for distorted images
2023	Ali et al. [225]	Secure fingerprint templates that are quantized, non-invertible, alignment free and single point independent.	Stolen key	FVC2002 -DB1,2,3 FVC2004-DB1,2	EER-0.99%,1.76%, 2.42%%,3.15%,3.43%	Not discussed other attacks

database and created two distinct systems with two different key sets. To determine the pseudo-genuine score, every fingerprint template belonging to the same person in System1 is compared with fingerprint templates belonging to the same person in System2. They proved that their system was resistant to cross-matching attack [235]. Harikrishnan et al. proposed a revolutionary paradigm that generates a secure one-time finger codes for each user's authentication. To build this, minuscule vectors obtained using a circular tesselation technique are combined with timestamps, finger codes, and pseudo-random number generators. These were generated across each user transaction session. Unauthorized users find it challenging to decode the finger code utilized in a specific authentication session [236].

Ali et al. proposed a Fingerprint Shell technique that creates a 2-dimensional spiral curve that serves as a secure user template by utilizing a single intra-subject invariant feature: the distances between tiny points and a particular point. The proposed approach is rotation and translation invariant. It has been tested on IIT Kanpur's fingerprint databases and the FVC 2000, 02, 04 utilizing 1-vs-1 and FVC protocols. The EER of the suggested technique was found to be 0.00% [237]. Kim et al. created a fully operational fingerprint authentication system by utilizing Fully Homomorphic Encryption on Torus (TFHE) toolkit with a fingerprint database of 4,000 samples. The process of matching fingerprints was completed by the system at an average of 166 s [238]. Rachapalli and Kalluri [239] devised a texture-only fingerprint recognition technique that uses a QR pattern to generate a cancellable fingerprint template with a lower likelihood of error without impairing the system's performance.

Liu et al. discussed the utilization of optical coherence tomography (OCT), which records depth data regarding the layers of skin, for the accurate and high-security recognition of fingerprints. The EER and FMR are 0.42 and 0.36 respectively, according to analyses of OCT-based fingerprints. The EER and FMR values determined from traditional 2D surface fingerprints were 8.05% and 18.18% [240]. Yang et al. used the homomorphic encryption approach to encrypt the template, making it more challenging for hackers to obtain raw biometric templates with no private key by allowing the encrypted domain to be used whenever biometric data are matched. Furthermore, the compromise between the speed of computation and authentication accuracy was upheld utilizing the FVC2002 DB2 fingerprint database [241]. Li et al. developed a compact 128-byte, cancellable method for generating a fingerprint binary code that allows for great security and exact and efficient comparison. A partial Hadamard transform was employed to further highlight the irreversibility of the system. When combined with security analysis, experimental results on six benchmark datasets (FVC2002 and FVC2004) show that the method performs better than other state-of-the-art techniques [242].

VIII. MULTIMODAL FINGERPRINT BIOMETRIC SYSTEMS: FUSION LEVELS

Figure 8 illustrates different biometric fusion levels.: rank, decision, sensor, score, and feature level [243]. Table 16 provides a comprehensive literature review of the recent fingerprint biometric fusion approaches.

A. FUSION AT THE SENSOR LEVEL

This type of fusion emphasizes the integration of raw sensor data. This can be achieved by using many suitable sensors to acquire the same biometric features or by using the same sensor to make multiple acquisitions. For instance, fingerprint scanners may combine a number of small images into a single large image, or 3D face scans can be created by combining raw data from various cameras. Processing was then performed on these biometric traits. Three classes of sensor-level fusion were distinguished:

1) Single sensor-multiple instances, in which several instances derived from only one sensor are combined to obtain the data in a reliable and descriptive manner.
2) Intra-class multiple sensors: These combine numerous data points from different sensors to indicate the position of a similar sensor or range of distinct sensors.
3) Inter-class multiple sensors: Few studies have been conducted on the inter-class multiple sensor fusion mode [252].

B. FUSION AT THE FEATURE LEVEL

Signals from various biometric traits were evaluated at the feature level to generate unique feature vectors, independently extracted from each trait. These vectors undergo feature-level fusion to combine signals from different channels. Fusion algorithms were then applied to create composite feature vectors, with feature reduction techniques used to select relevant features. Feature-level fusion offers improved recognition accuracy by leveraging more biometric information compared to matching score approaches, especially with multiple biometric aspects involved [253].

Poonguzhali and Ezhilarasan [254] improved a unibiometric fingerprint recognition system by integrating feature levels at Levels 1 and 2, finding concatenated feature sets more effective than discrete ones, particularly with their Fingerprint Feature Vector approach leveraging richer gray level data and analyzing poor-quality images. Ahsan et al. [255] developed an automatic fingerprint verification system combining CNN features with those from Gabor filtering, followed by PCA for overfitting reduction and accuracy enhancement, achieving a 99.87% accuracy.

C. MATCHING SCORE LEVEL FUSION

Biometric systems process feature vectors separately, calculating a composite match score by combining individual matching levels. Various classification methods like mean fuse, highest rank, or logistic regression are applied for this purpose, enabling score normalization through techniques such as piecewise linear, min-max, and z-score normalization. The matching score level of fusion is favored for its simplicity compared to other fusion levels [246].

D. DECISION LEVEL FUSION

This can be seen as an example of score-level fusion in which the scores are first converted to a binary (match/non-match) using a majority vote or other fusion rules. Because of the limited quantity of data provided at the fusion stage, this strategy has the lowest complexity and the greatest interoperability across various biometric features and is less effective than score-level fusion [256].

Data transmission from sensor to decision unit is increasingly compressed. Sensor level fusion encounters compatibility issues among data from different sensors, making it rare in multimodal biometrics. Feature-level fusion is expected to enhance recognition performance more effectively due to richer, more meaningful information in features, but incompatible feature sets from different biometric modalities limit its research. Decision-level fusion, involving less data, is also seldom used in multimodal recognition systems [257].

IX. LITERATURE REVIEW ON MULTIMODAL FINGERPRINT BIOMETRIC SYSTEMS

The Table 17 provides an analysis of the performance of recent multimodal fingerprint biometric systems.

Tran et al. provided a verification methodology based on palm print, face, fingerprint, and hand form. The Zernike Moment (ZM) is used in the proposed approach to extract multimodal information. Subsequently, a ratio test was used to combine the similarity scores. Authentic and impostor distributions of the similarity scores were estimated using a finite GMM. Utilizing databases that are open to the public, including FVC2004, PolyU, ORL, and IIT Delhi, the highest verification rates were obtained- FAR of 0.01%, GAR of 99.4% are attained [269].

Fatt et al. devised a multimodal biometric identification system that combined face and fingerprint features through score level fusion. The features of the fingerprint trait were generated using minutiae points in the ridge region, while the features of the face were constructed using Local Binary Patterns (LBP). The system achieves a recognition accuracy

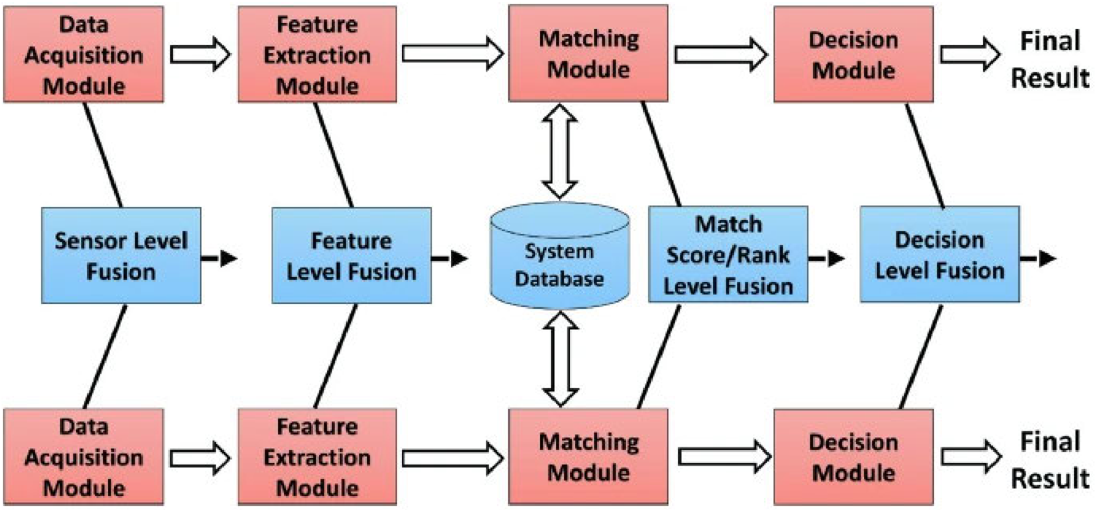


FIGURE 8. Multibiometric fingerprint system fusion levels (source: gavrilova et al [244]).

TABLE 16. A literature review of recent fingerprint biometric fusion studies.

Year	Author	Biometric traits	Level of fusion	Dataset	Notes
2019	Ahmad et al. [245]	Multimodal:face, fingerprint	Rank	BSSR1, BSS4	Accuracy -99.42%, 91.63%
2020	Herbadji et al. et al. [246]	Multimodal:fingerprint, Palmprint	Score	POLYU, IIT-Delhi	GAR-100.0%, EER-0.00%
2020	Zhang et al. [247]	Unimodal:fingerprint	Score	LivDet2015,2019	Accuracy-96.88%
2020	El_Rahman et al. [248]	Multimodal:fingerprint, ECG	Score, decision	FVC2004, MIT-BIH	AUC up to 0.985 for sequential multimodal system, up to 0.956 for parallel multimodal system
2022	Aizi et al. [249]	Multimodal:iris, fingerprint	Score	CASIA-IrisV4, CASIA-FingerprintV5	Accuracy-95%
2022	Hammouche et al. [250]	Multimodal:minor, major dorsal finger, knuckle	Score	POLYU	EER below 0.60%
2022	Srivastava et al. [251]	Multimodal:finger, knuckle, iris	Score	POLYU, CASIA	Accuracy 98%

of 98.1%, surpassing that of standalone systems [270]. Shams et al. introduced a biometric modality retrieval system employing Adaptive Deep Learning Vector Quantization (ADLVQ) based on both face and fingerprint data, including multi-sample and multi-instances of faces and fingerprints. Input characteristics are extracted using Local Gradient Pattern using variance (LGPV), which is then quantized using the k-means technique based on previous learning vector quantization (LVQ) expertise. Experiments conducted on SDUMLA-HMT and CASIA-V5 datasets yielded an accuracy of 95% [271].

Gawande et al. utilized textural data from fingerprints and the iris, employing the block sum and minutiae techniques, respectively. The effectiveness of these methods was tested on the YCCE Biometric database and CASIA 3.0 iris. Through feature-level fusion, the recommended methods achieved a recognition rate of 96% and a 0% False Acceptance Rate (FAR) [272]. Bhardwaj et al. introduced a multiple instance fingerprint acquisition method within a multimodal system by, incorporating both fingerprints and associated time dynamics. Experiments involving user verification and spoof resistance assessments were conducted on synthetic multimodal databases created by merging the fingerprint dynamics databases of ATVS and LivDet-13. Fusion at the match score level was performed using sum and weighted sum rules. The results indicated a relative average increase in Equal Error Rate (EER) of 90.64% over unimodal systems [273].

Algashaam et al. introduced a Multi-model Concise Multi-linear Pool, utilizing an efficient outer product computation of features extracted in a low-dimensional space generated by the counters sketch projection. The incorporation of elliptical higher-order-spectral characteristics demonstrated the development of a comprehensive multispectral periocular biometric system through feature-level fusion. The system achieved an accuracy of 93% using a custom periocular and IIIT periocular dataset [274]. Sultana et al. devised a novel person recognition system that leverages the knowledge

TABLE 17. Analysis of the performance of recent multimodal fingerprint biometric systems.

Year	Author	Methodologies	Utilized Dataset	Performance	Resistant to attacks	Advantages	Drawbacks
2018	Xin et al. [258]	Point mode, DCT feature level fusion- face, fingerprint, finger vein	Composed	Accuracy -93.3%	Camouflage, forgery	Anti-forgery	Recognition rate decreases with the increase in the no. of users
2018	Arteaga-Falconi et al. [117]	SVM decision level fusion-, ecg, fingerprint	FVC2006-DB1, Physionet	EER-0.46%, FAR-2.96%, TAR-100%	Spoofing	Added security	Not discussed security of data storage
2019	Hameed et al. [259]	fuzzy logic, decision fusion- 3 different fingerprints	FVC2000-DB2	EER-13.61%	No	NA	Low performance
2020	El_rahman et al. [248]	SOM-NN, LDA, fuzzy logic, fusion-ECG, fingerprint, score level for parallel, decision level for sequential	MIT-BIH, FVC2004	AUC up to 0.985 for sequential, AUC up to 0.956 for parallel	Spoofing	Recognition performance is comparable	Use of virtual database
2020	Gavisiddappa et al. [260]	LBP, HOG, GLCM, MSVM, feature level fusion-Face, iris,fingerprint	CASIA	Accuracy -97.09%	Spoofing	Use of iris makes forge difficult	High computation time
2020	El mehdi Cherrat et al. [261]	Gabor filter, HOG, CNN, LBP, SVM, decision level fusion-fingerprint, fingervein, face	FVC2004, VERA, AR	Accuracy -99.43%	No	System is flexible in absence of biometric trait	Security aspects not mentioned
2020	Mustafa et al. [262]	GLCM, KNN, decision level fusion-iris, fingerprint	CASIA-V1,V2, FVC 2004	Accuracy -95%-making decision	No	Final decision making accuracy good on 20 test users	Preprocessing enhancements feasible
2021	Kamlaskar et al. [263]	CCA, feature level fusion-iris, fingerprint	SDUMLA-HMT	EER-0.8474%	No	Verification performance	Performance enhancement required
2022	Rajasekar et al. [264]	Fuzzy genetic algorithm, score-level fusion-iris, fingerprint	Accuracy -99.88%, EER-0.18%	CASIA V3, FVC2006	No	Comparable FAR, FRR, precision, recall, accuracy	Security aspects not discussed
2022	Safavipour et al. [265]	kernel-based, Hough Transform, Daugman algorithm, feature level fusion-2 fingerprints, 2 irises,face	ORL, FERET, Shahed University, CASIA	Accuracy -100%	Spoofing	Reliable	High computation time
2022	Ren et al. [266]	FPV-Net, NAS, feature fusion-fingerprint, finger vein	NUPT-FPV	Accuracy -88.05%	No	New large dataset produced	Accuracy to be improved
2023	Omara et al. [267]	HVicT, WFF -iris, fingerprint, palmprint, DWAM	CASIA	Accuracy-99.02%, specificity-98.94%, F1 score-98.63%	Predator	Noise reduction, original image preservation	Higher FRR, computation time
2023	Kazi et al. [268]	PCA, SVD, DWT, DCT, Fusion-Score Level and Decision Level-face, fingerprint,signature	YALE,BioID, FVC2002, FVC2000, KVKR	Accuracy -99%	No	Reduced computation cost by resizing data	System reliability not mentioned

HVicT: Hybrid vision capsule transformer model, WFF: Weighted Feature Fusion, DWAM: Dense Pelican Channel block weighted autoencoder model, GLCM: Gray-Level Co-occurrence Matrix, KNN: K-nearest neighbor, MSVM: Multi-Support Vector Machine, DCT: Discrete Cosine Transform, CCA: Canonical Correlation Analysis, SOM-NN: self-organizing feature map-neural network, LDA: Linear Discriminant Analysis, PCA: Principal Component Analysis,SVD: Singular Vector Decomposition,DWT: Discrete Wavelet Transform, DNN: Deep Neural Networks, MLP: Multilayer Perceptron,NAS: neural architecture search, NA: Not applicable of individuals' social behavior. Traditional face and ear biometrics were combined with social behavioral data collected from an online network. Face and ear fusion yielded a rank-1 identification rate of 91%, wheras combining Social Behavioral Biometric (SBB) profiles with low-quality face and ear biometrics achieved a 100% rank-1 recognition rate [275].

Elhoseny et al. developed a cascade multimodal biometric system incorporate fingerprint and iris recognition. The system employs a log-Gabor filter for iris recognition, and minutiae extraction for fingerprint authentication. The accuracy of the system was reported as 99.86%, with a FAR of 0% and a FRR of 0.057% [257]. Tarif et al. introduced a highly secure encryption/hiding technique and multimodal biometric authentication system that guarantees secure biometric data transmission. The concealed fingerprint and iris vectors are sparsely calculated using an advanced recursive hard thresholding technique and are embedded in the host Slantlet-SVD domain of the face picture. Experimental results demonstrate that even when the medium carrying the image is substantially damaged, hidden biometric data can still be recovered with high fidelity [276].

NS et al. observed that while the accuracy rate of an electrocardiogram (ECG) is comparatively lower than that of traditional biometrics, such as fingerprints significantly more challenging to deceive the system. Their fingerprint and ECG-based system achieved 98% accuracy rate, 2% FAR, and practically no FRR [277]. Siddiqui et al. proposed a system that utilize both iris and fingerprint modalities for individual identification. A minutiae matcher, employing similarity and distance methods, is utilized for fingerprint recognition, whereas iris images are extracted using the wavelet algorithm. The system was assessed on the KVK and an internal datasets, achieving an accuracy of 99.2% with a FAR of 0.02% and a FRR of 0.1% [278].

Kabir et al. implemented a multibiometric system by integrating fingerprint, palm, and earprint data using a Matcher Performance-based (MPb) method to enhance overall recognition accuracy. MPb employs score level and feature level data fusion, with an additional option being the overlap extrema-variation-based anchoring min-max (OEVBAMM) normalization strategy. The system achieved a 100% GAR at a low FAR for FVC2002-DB1, COEP, and AMI earprint databases [279]. Hammad et al. proposed a multimodal biometric system that combines Convolutional Neural Network (CNN) and Q-Gaussian Multiple Support Vector Machines (QG-MSVM) with feature and decision level fusion. The testing results demonstrated an average accuracy of 98.94% for PTB, CYBHi, LivDet2015, and FVC 2004 [280].

Li et al. conducted feature fusion of fingerprints, finger veins, and finger knuckle prints using the unique localized coding-based feature expressions method. A correction technique was employed to address the pose variation among the trimodal finger images. Oriented Gabor filters were utilized to enhance the velocity features in finger photographs, and a Generalized Symmetric Local Graph Structure (GSLGS) was employed to fully define the orientation and position interactions between neighboring pixels [281].

A multimodal system template security analysis was created by Sujitha et al.using both fingerprint and palmprint data. The fingerprint and palmprint templates were also protected using the fuzzy vault method. To create a database in the vault, the extracted features were concatenated and coupled with a secret key. For key recovery during authentication, query images are supplied as input along with a template that has been previously stored. According to experimental findings, the suggested multibiometric system offers improved GAR and defends against correlation and brute-force assaults [282]. Xin et al. developed a matching technique that uses face, finger vein, and fingerprint biometric modalities as well as the secondary computation of the Fisher vector. After the modalities were combined, the feature-level fusion was completed. The system uses DCT to determine if an image is real or false before eliminating the fake ones to improve system robustness and reduce the impact on the accuracy rate [258].

Arteaga-Falconi et al. proposed a bimodal biometric system with an ECG and a fingerprint. An SVM classifier is employed for the ECG method, whereas the matcher and minutiae extractor using NBIS are used for the fingerprint methodology. At the decision level, they combined the fingerprint and ECG authentication findings to discriminate between real users and fraudsters [283]. Kim et al. developed multimodal biometrics combining finger-vein and finger shapes using a deep neural network and an NIR light camera sensor. The SDUMLA-HMT and KPU were used in the experiments, and the findings showed that the method in the study had a higher performance [284].

Shivakumar developed a feature-level, fusion-based multimodal biometric system (FFI-FLF-MM-BS), that utilize the biological characteristics of the face, fingerprint, and iris. The fingerprint was extracted from the minutiae after the face and iris traits were retrieved using the bi-directional empirical mode decomposition algorithm. It uses MC-SVM as a classifier with 95.71% accuracy [285]. Cheniti et al. designed a framework for score-level fusion using symmetric sums (S-sums). Triangular norms were used to construct these S-sums. The system was tested using the NIST-BSSR1 database with GAR of 92.8% and an FAR of 0.01% [286].

Damer et al. utilized information from both the iris and fingerprints and devised, a joint multibiometric retrieval method. Using eight different candidate list fusion algorithms with varying degrees of difficulty, this strategy was evaluated on a dataset of ten thousand reference and probing records for fingerprint and iris pictures. Reduced the miss rate (or 1-hit rate) at the 0.1% penetration rate by 93% and 88%, compared to iris and fingerprint indexing [287].

Hammad et al. introduced a multimodal biometric system that combined fingerprint and electrocardiogram (ECG) data using a CNN for feature extraction. The authentication performance was enhanced using a Q-Gaussian multi support vector machine (QG-MSVM). The system, evaluated on PTB and LivDet2015 datasets, achieved a remarkable accuracy rate of 99.99% [288]. Walia et al. developed an integrated biometric system incorporating fingerprints, finger veins, and iris modalities. The system employed a backtracking search optimization technique and proportional conflict redistribution principles (PCR-6) to improve performance. Evaluation with chimeric multimodal datasets demonstrated an accuracy of 98.43% and Equal Error Rate (EER) of 1.57% [289].

Siddiqui et al. proposed a multimodal biometric recognition system based on fingerprints and the iris. The minutiae matcher approach and wavelet were utilized for feature extraction, resulting in an accuracy of 99.2% on the KVK dataset, with a low FAR of 0.02% and FRR of 0.1 Karthi et al. presented a multimodal biometric technology integrating the distance approach and template-based feature extraction for enhanced security. The system achieved accuracy, universality, and usability, with a focus on the distance approach for fingerprint centers and ridge points. The proposed system showed a comprehensive approach with promising results [290].

Kabir et al. utilized the Matcher Performance-based (MPb) strategy, implementing palmprint, fingerprint, and earprint data to enhanced the identification accuracy. Fusion was executed at the score and feature levels, considering the accuracy of individual matchers for effective feature-level fusion. The system demonstrated improved overall identification accuracy, with promising results [279]. Zhang et al. addressed the challenges of three trimodal features in an individual's finger: fingerprints, finger-veins, and finger-knuckle prints. A graph-based technique successfully extracted features, overcoming the feature space incompatibilities. The algorithm achieved a notable 99.9% accuracy rate with over-generated databases [291].

Sistla et al. developed a two-phase multimodal framework incorporating facial, finger, and speech modalities. By leveraging Gabor wavelets, semi-supervised kernel discriminant analysis, and dynamic time warping, the system achieved a high True Acceptance Rate (TAR). The utilization of the Dempster-Shafer theory and fingerprint trait features further contributed to achieving a high TAR [292]. Sajjad et al. introduced a system to verify a user's identity through face, palm vein, and fingerprint recognition at Tier I, with CNN-based models used at Tier II to identify spoofing attempts. The system demonstrated 100% accuracy and, effectively prevent malicious users from unauthorized access [293].

El et al. proposed a multimodal biometric system based on cascade advancement and decision-level fusion, combining fingerprints, finger veins, and face data. The cascade decision-making strategy achieved an accuracy of 99.43%, demonstrating the effectiveness of combining different biometric types [261].

Abdul et al. developed a generic feature extraction method based on key images, utilizing face, fingerprint, and iris data to reduce the feature dimensions and achieve revocability. The system achieved robustness against presentation and replay attacks, with an EER of 0.2% [294].

Cherrat et al. proposed a hybrid system combining CNN, Softmax, and RF classifiers for multibiometric fingerprints, finger-veins, and face identification. The system demonstrated an accuracy of 99.49% on the SDUMLA-HMT dataset, utilizing a GPU-based implementation [295]. Sahar et al. created a multibiometric system utilizing fingerprints and ECG, achieving high AUC values in both sequential and parallel multimodal systems compared to unimodal systems [248].

Abdul et al. presented a fingerprint and face multimodal template protection system using fusion at the score level. The system achieved an EER of 3.87%, providing enhanced security for the biometric templates [296]. Kamlaskar and Abhyankar [263] implemented fusion of the same person's fingerprint and iris feature sets using canonical correlation analysis, achieving an EER of 0.1050%.

Tantubay et al. proposed an effective multimodal key-binding biocrypto-System (MKBB) utilizing a feature-level fusion technique based on statistically irreversible data. The system achieved high accuracy, GAR, and low FMR, thereby demonstrating its effectiveness [297]. Tran et al. developed a two-layer authentication system with multi-filter fingerprint matching to address poor-quality fingerprint images more effectively. The system demonstrated robustness against various attacks on public datasets FVC2002-4 [192].

Kumar et al. developed an Improved Biometric Fusion System (IBFS), that combine face and fingerprint modalities. By leveraging the whale optimization algorithm, minutiae features, and Maximally Stable External Regions (MSER), the system achieved a high TPR and accuracy [298]. Leghari et al. [299] proposed a CNN-based model for the feature-level fusion of online signatures and fingerprints, achieving high accuracy rates through early and late fusion techniques.

Atilla et al. developed a system with a fixed-size descriptor, transmission timestamp integration, and a unique system identification number for fingerprints and face templates. The system achieved a recognition rate of 99.41% and incorporated privacy protection and anti-replay features [300]. Tomar et al. proposed a hybrid approach that combines fingerprints and facial images in a multimodal biometric framework. Using cascaded and fusion-based techniques, the system achieves high accuracy rates at different fusion levels [301].

Shende and Dandawate [302] developed a face, fingerprint, and palm vein verification system based on a CNN, achieving a high accuracy for each modality. Lee et al. [191] introduced Multimodal Extended Feature Vector Hashing for tokenless cancellable biometric, achieving a GAR of 90%. Brindha and Meenakshi [303] proposed a multimodal biometric approach for detecting Sybil attacks in MANETs, outperforming other methods in terms of its effectiveness.

X. DISCUSSION

Our comprehensive analysis identifies unresolved issues in the area of biometric authentication that require thorough research.

Research gap 1: Enhancing the fingerprint biometric systems' accuracy and speed in challenging data scenarios is necessary. Innovative performance metrics are essential to accurately gauge identification and verification in such contexts.

Limitations:

1) Noisy Data: Real-world fingerprint images often contain noise, impacting accuracy.
2) Partial Fingerprints: Incomplete fingerprints pose challenges for identification.
3) Variability: Fingerprints vary in quality, clarity, and distinctiveness.
4) Adverse Conditions: Environmental factors affect fingerprint quality.
5) Limited Data: Scarcity of labeled data hampers model training.

Solutions:

1) Noise Reduction: Develop algorithms to filter noise from fingerprint images.
2) Partial Fingerprint Recognition: Explore methods to identify individuals from partial prints.
3) Robust Feature Extraction: Develop feature extraction techniques resilient to variability.
4) Environmental Compensation: Algorithms to mitigate adverse environmental effects.
5) Data Augmentation: Use synthetic data to augment limited training datasets.
6) New Metrics: Define metrics focusing on noise robustness and partial print matching. Like robustness score, adversarial robustness index, template update frequency, latency reduction ratio multi-modality fusion rate.
7) Ensemble Learning: Combine models to improve overall performance and robustness.

Research gap 2: Achieving an optimal balance between security, system performance, and usability remains a crucial aspect in the realm of fingerprint biometrics.

Limitations:

1) Complexity: Balancing security, performance, and usability is complex.
2) Trade-offs: Improving one aspect often compromises another.
3) User Acceptance: Stricter security may reduce user acceptance.
4) Technological Constraints: Current technology limits optimal balance.

Solutions:

1) Adaptive Systems: Systems adjusting security based on context.
2) Multi-Factor Authentication: Combining biometrics with other methods.
3) Continuous Improvement: Refining algorithms for better performance.
4) User-Centric Design: Prioritizing user experience in design.
5) Education and Training: Educating users on security importance.
6) Technological Advancements: Advancing technology for better systems.

Research gap 3: The effectiveness of current strategies to ensure the privacy of fingerprint biometric authentication is uncertain, emphasizing the requirement for thorough assessment and the development of more resilient solutions.

Limitations:

1) Privacy Vulnerabilities: Fingerprint biometric systems face privacy risks.
2) Data Security: Protecting fingerprint data from unauthorized access is crucial.
3) Biometric Template Protection: Ensuring the security of stored biometric templates is essential.
4) Legal and Ethical Compliance: Meeting privacy regulations and ethical standards poses challenges.

Solutions:

1) Encryption: Use robust encryption for secure data transmission and storage.
2) Biometric Template Protection: Implement secure methods for managing biometric templates.
3) Access Control: Employ strict access controls to prevent unauthorized data access.
4) Privacy-Preserving Protocols: Adopt protocols like secure multi-party computation to enhance privacy.
5) Legal Compliance: Ensure adherence to privacy laws through transparent practices.
6) Ethical Frameworks: Establish ethical guidelines for biometric data handling to protect user privacy.

Research gap 4: There is a need for comprehensive datasets containing multiple biometric traits to facilitate more rigorous evaluations and comparisons of these systems.

Limitations:

1) Limited Benchmark Datasets: Scarcity of datasets containing multiple biometric traits restricts comprehensive evaluations.
2) Assumption of Statistical Independence: Difficulty in assuming independence between biometric traits due to insufficient real-world data.
3) Reliance on Virtual Databases: Virtual databases may not accurately represent real scenarios, introducing biases.

Solutions:

1) Development of Comprehensive Datasets: Creating standardized datasets with various biometric traits can enhance evaluations.
2) Collaboration and Data Sharing: Sharing datasets among researchers can alleviate data access limitations.
3) Advancement of Simulation Techniques: Improving simulation methods can generate more realistic data, reducing reliance on virtual databases.

Research gap 5:Limited exploration in optimizing multimodal fingerprint biometric systems hampers effective integration and synchronization of multiple sensor modalities, requiring focused efforts for robust advancements.

Limitations:

1) Integration Complexity: Harmonizing multiple sensor modalities in multimodal fingerprint biometric systems is technically challenging.
2) Synchronization Accuracy: Ensuring precise data synchronization from various sensors is essential for reliable authentication.
3) Data Fusion: Developing efficient algorithms to merge and interpret data from diverse sensors remains a challenge.
4) Standardization: Lack of standardized protocols hinders seamless integration and interoperability of multimodal systems.

Solutions:

1) Advanced Integration Techniques: Implementing sophisticated methods for integrating multiple sensor modalities seamlessly.
2) Synchronization Algorithms: Developing accurate algorithms to synchronize data from different sensors with precision.
3) Fusion Algorithm Development: Designing robust algorithms for effectively merging and interpreting data from diverse sensor sources.
4) Standardized Protocols: Establishing protocols to facilitate interoperability and seamless integration of multimodal fingerprint biometric systems.

Research gap 6: The dearth of recent research on fingerprint thermal imaging in biometric system.

Challenges:

1) Limited Data Availability: Recent research on fingerprint thermal imaging lacks sufficient datasets and benchmarks crucial for evaluating thermal-based fingerprint recognition algorithms.
2) Technological Constraints: The specialized hardware and software needed for fingerprint thermal imaging are often expensive and not easily accessible, slowing down research progress.
3) Integration Complexity: Integrating thermal imaging into existing biometric systems poses technical challenges, including compatibility issues and complexities in calibration and data fusion.

Solutions:

1) Collaborative Research: Encouraging collaboration among researchers, industry partners, and governmental bodies can foster data sharing and resource pooling to address the scarcity of research in fingerprint thermal imaging.
2) Technology Investment: Increased investment in thermal imaging technology research can drive advancements in hardware and algorithms, making thermal-based biometric solutions more attainable.
3) Standardization and Evaluation: Establishing standardized protocols, metrics, and benchmark datasets specific to fingerprint thermal imaging can facilitate evaluation and further research.
4) Training and Education: Providing training opportunities for researchers and practitioners in thermal imaging and biometrics can improve expertise and knowledge dissemination, easing integration complexities.
5) Advocacy and Awareness: Raising awareness about the benefits of fingerprint thermal imaging in biometric systems and advocating for its inclusion in research agendas can stimulate interest and investment in this technology.

XI. CONCLUSION

We discussed the benefits and drawbacks of fingerprint recognition systems by performing a performance analysis of each type of system. This review focuses on and studies the considerable advancements in fingerprint biometrics, both unimodal and multimodal. As the benefits of fingerprint biometric systems are being discussed, several application scenarios illustrating the algorithms used to construct fingerprint biometric systems are emphasized. We found that although some devices that use dynamic biometrics need to improve their verification accuracy, most of the current solutions have privacy and security flaws. When data from multiple sources are combined, the accuracy of biometric authentication systems can be significantly improved. Of all the levels of data fusion, score level fusion continues to be the most beneficial because it is simple to identify and merge the matching scores. Additionally, it was found that using multimodal biometric frameworks over unimodal biometrics eliminates constraints. Multimodal biometric systems are to be improved by incorporating additional sensors, improving matching algorithms, handling noise errors, and analyzing data. However, to create reliable, compatible, safe, privacy-preserving, and user-friendly systems, an enormous amount of works need to be done.

REFERENCES

[1] *Biometric Recognition: Challenges and Opportunities*, Nat. Res. Council Whither Biometrics, 2010.

[2] A. K. Jain, A. A. Ross, and K. Nandakumar, *Fingerprint Recognition*. Boston, MA, USA: Springer, 2011, pp. 51–96.

[3] S. Dargan and M. Kumar, "A comprehensive survey on the biometric recognition systems based on physiological and behavioral modalities," *Expert Syst. Appl.*, vol. 143, Apr. 2020, Art. no. 113114.

[4] A. K. Jain, A. Ross, and S. Prabhakar, "An introduction to biometric recognition," *IEEE Trans. Circuits Syst. Video Technol.*, vol. 14, no. 1, pp. 4–20, Jan. 2004.

[5] A. K. Jain, A. Ross, and K. Nandakumar, *Introduction to Biometrics*. Cham, Switzerland: Springer, 2016.

[6] K. El-Maleh and W. El-Hajj, "Voice biometrics: Security, forensics, and healthcare," *J. Med. Syst.*, vol. 43, no. 9, p. 306, 2019.

[7] K. Banerjee, J. P. Singh, and R. Kaur, "Human retinal identification: Review and future scope," *J. Comput. Sci. Technol.*, vol. 15, no. 1, pp. 10–15, 2014.

[8] A. Kumar and R. Vigneshwaran, "Fingerprint-based vehicle security system using microcontroller," *Proc. Comput. Sci.*, vol. 46, pp. 1625–1631, Jan. 2015.

[9] D. H. Kim, S. H. Park, and K. S. Yoon, "Face recognition for smart card security," *Int. J. Secur. Appl.*, vol. 11, no. 3, pp. 65–76, 2017.

[10] S. Z. Li and A. K. Jain, *Handbook of Face Recognition*. Cham, Switzerland: Springer, 2011.

[11] I. Bouchrika, "A survey of using biometrics for smart visual surveillance: Gait recognition," in *Surveillance in Action: Technologies for Civilian, Military and Cyber Surveillance*, 2018, pp. 3–23.

[12] V. Sivalenka, S. Aluvala, Y. Sneha, K. Mannan, S. Farheen, and E. Kumaraswamy, "An empirical study of various face recognition and face liveness detection techniques and algorithms," in *Proc. Int. Conf. Res. Sci., Eng. Technol.*, 2022, p. 20056.

[13] K. Okokpujie, E. Noma-Osaghae, O. Okesola, O. Omoruyi, C. Okereke, S. John, and I. P. Okokpujie, "Fingerprint biometric authentication based point of sale terminal," in *Proc. Int. Conf. Inf. Sci. Appl.* Cham, Switzerland: Springer, 2018, pp. 229–237.

[14] S. Tharewal, T. Malche, P. K. Tiwari, M. Y. Jabarulla, A. A. Alnuaim, A. M. Mostafa, and M. A. Ullah, "Score-level fusion of 3D face and 3D ear for multimodal biometric human recognition," *Comput. Intell. Neurosci.*, vol. 2022, pp. 1–9, Apr. 2022.

[15] A. S. Al-Waisy, R. Qahwaji, S. Ipson, S. Al-Fahdawi, and T. A. M. Nagem, "A multi-biometric iris recognition system based on a deep learning approach," *Pattern Anal. Appl.*, vol. 21, no. 3, pp. 783–802, Aug. 2018.

[16] G. Jaswal, A. Kaul, and R. Nath, "Multimodal biometric authentication system using hand shape, palm print, and hand geometry," in *Computational Intelligence: Theories, Applications and Future Directions*. Cham, Switzerland: Springer, 2019, pp. 557–570.

[17] C. Kant and S. Chaudhary, "A multimodal biometric system based on finger knuckle print, fingerprint, and palmprint traits," in *Innovations in Computational Intelligence and Computer Vision*, M. K. Sharma, V. S. Dhaka, T. Perumal, N. Dey, and J. M. R. S. Tavares, Eds. Singapore: Springer, 2021, pp. 182–192.

[18] J. Deng, J. Guo, and Y. Zhou, "Facial expression recognition based on multi-feature deep learning," *Multimedia Tools Appl.*, vol. 79, nos. 43–44, pp. 32873–32890, 2020.

[19] W. Xia, J. Cao, and X. Ding, "Facial expression recognition using geometric features and extreme learning machine," *Signal, Image Video Process.*, vol. 15, no. 5, pp. 999–1006, 2021.

[20] J. Wang, B. Li, W. Deng, and Y. Gao, "Fisherfaces revisited: Self-supervised learning for unsupervised face recognition," *IEEE Trans. Image Process.*, vol. 30, pp. 2574–2584, 2021.

[21] N. Mokhtari and R. Chellappa, "Face recognition using texture features from local binary patterns," in *Proc. IEEE Int. Conf. Identity, Secur. Behav. Anal. (ISBA)*, Jun. 2018, pp. 1–6.

[22] W. Zou, S. Zeng, J. Wang, and T. X. Han, "Local directional number pattern for face recognition," *IEEE Trans. Inf. Forensics Security*, vol. 15, pp. 945–957, 2020.

[23] X. Zhu, Z. Lei, J. Yan, D. Yi, and S. Z. Li, "High-performance face recognition via deep hybridized representations," *IEEE Trans. Pattern Anal. Mach. Intell.*, vol. 40, no. 11, pp. 2634–2647, Sep. 2017.

[24] Y. Zhang, Y. Song, Y. Song, and Q. Chen, "Face recognition with facial landmarks: A comprehensive review," *Pattern Recognit. Lett.*, vol. 145, pp. 120–128, 2021.

[25] R. Tiwari, P. Gupta, and P. Gupta, "Iris recognition using Daugman's algorithm with texture-based feature extraction," *Multimedia Tools Appl.*, vol. 80, no. 6, pp. 9725–9740, 2021.

[26] M. A. Siddique, M. A. Islam, and M. M. H. Rana, "Enhanced iris recognition using adaptive Gabor filter for blurred and noisy iris images," *IEEE Access*, vol. 9, pp. 30351–30362, 2021.

[27] S. S. Ali, M. Javaid, and Z. A. Khan, "An iris recognition system based on localized 2D Gabor filters," *IEEE Access*, vol. 9, pp. 34154–34165, 2021.

[28] H. Li, Y. Wang, and L. Li, "Deep learning for iris recognition: A comprehensive survey," *IEEE Access*, vol. 9, pp. 12785–12800, 2021.

[29] Y. Liu, Y. Lu, X. Zhu, and G. Zhang, "Ear recognition based on multi-scale feature fusion and graph convolutional networks," *IEEE Access*, vol. 9, pp. 108809–108818, 2021.

[30] J. Siddiqui, M. T. Abdullah, A. Khan, and M. Shafique, "Ear recognition based on gradient directional pattern and deep feature extraction," *IEEE Access*, vol. 9, pp. 117002–117013, 2021.

[31] H. Lin, J. Wang, J. Xie, and Z. Li, "Ear recognition using deep learning and fuzzy entropy," *IEEE Access*, vol. 9, pp. 70284–70293, 2021.

[32] H. Proença, S. Filipe, and L. A. Alexandre, "Ear biometrics: A comprehensive survey," *IEEE Trans. Inf. Forensics Security*, vol. 7, no. 6, pp. 1938–1954, 2012.

[33] Z. Hou, B. Yang, Y. Chen, and X. Lu, "Palmprint recognition using deep learning with texture feature extraction," *J. Vis. Commun. Image Represent.*, vol. 76, Feb. 2021, Art. no. 102836.

[34] J. Cui and H. Liu, "Palmprint recognition based on local binary pattern and ridge feature extraction," *Pattern Recognit. Lett.*, vol. 144, pp. 95–101, May 2021.

[35] Z. Wang, J. Zhang, Y. Liu, and Y. Wang, "Palmprint recognition based on multiscale gradient feature extraction," *Signal, Image Video Process.*, vol. 15, no. 6, pp. 1173–1182, 2021.

[36] S. Li, L. Fei, B. Zhang, X. Ning, and L. Wu, "Hand-based multi-modal biometric fusion: A review," *Inf. Fusion*, vol. 109, Sep. 2024, Art. no. 102418.

[37] B. M. Hasan, Z. J. Jaber, and A. A. Habeeb, "Digits recognition for Arabic handwritten through convolutional neural networks, local binary patterns, and histogram of oriented gradients," *Baghdad Sci. J.*, 2024.

[38] C. G. Dias, K. L. Rodrigues, N. C. Menegasse, W. A. L. Alves, and L. C. da Silva, "Histogram of oriented gradients for rotor speed estimation in three-phase induction motors," *IEEE Trans. Instrum. Meas.*, vol. 72, pp. 1–11, 2023.

[39] 63 J. Bharadiya and J. P. Bharadiya, "A tutorial on principal component analysis for dimensionality reduction in machine learning," *Int. J. Innov. Res. Sci. Eng. Technol.*, vol. 8, no. 5, pp. 2028–2032, 2023.

[40] Z. Liu, W. Liu, M. Liu, J. Liu, and S. Lian, "Robust palmprint recognition using sparse representation and graph convolutional networks," *Pattern Recognit. Lett.*, vol. 145, pp. 139–146, Jan. 2021.

[41] X. Zhang, J. Yang, J. Chen, and Y. Zhang, "A comprehensive survey on fingerprint recognition: From classical techniques to deep learning methods," *IEEE Access*, vol. 8, pp. 133315–133339, 2020.

[42] A. Kumar, D. Bhattacharjee, and M. Nasipuri, "Fingerprint recognition using multi-level feature extraction and deep learning," *Expert Syst. Appl.*, vol. 181, Jul. 2021, Art. no. 115213.

[43] W. A. Laghari, T. K. Gaik, A. Huong, Y. Y. Choy, and C. C. Chew, "Dorsal hand vein identification using transfer learning from AlexNet," *Int. J. Integr. Eng.*, vol. 14, no. 3, pp. 111–119, Jun. 2022.

[44] A. N. Rafferty and P. D. Kovesi, "A PCA-based approach to hand geometry recognition," in *Proc. IEEE Int. Conf. Image Process. (ICIP)*, Sep. 2016, pp. 3096–3100.

[45] R. Kumar and R. Bansal, "Hand geometry recognition using Procrustes analysis and local binary patterns," in *Proc. Int. Conf. Comput., Commun. Autom. (ICCCA)*, 2019, pp. 1–5.

[46] S. Abbasi and A. Sarif, "Hand geometry recognition using Fourier descriptors and fuzzy clustering," *J. Intell. Fuzzy Syst.*, vol. 38, no. 2, pp. 1289–1297, 2020.

[47] Y. Zhou, X. Wang, and J. Feng, "Hand geometry recognition based on curvature scale space and deep learning," *Pattern Recognit. Lett.*, vol. 105, pp. 69–75, Aug. 2018.

[48] J. Upadhyay, T. Gonsalves, R. Paranjpe, H. Purohit, and R. Joshi, "Biometric identification using gait analysis by deep learning," in *Proc. IEEE Int. Conf. Innov. Technol. (INOCON)*, Nov. 2020, pp. 1–4.

[49] Y. Han, S. Li, and Z. Zhang, "Gait feature extraction based on gait energy image," *J. Sensors*, vol. 2020, pp. 1–9, 2020.

[50] M. A. Khan, P. Kumar, and P. Gupta, "Dynamic time warping-based gait feature extraction for human identification," in *Proc. Int. Conf. Intell. Sustainable Syst. (ICISS)*, 2021, pp. 518–522.

[51] Z. Liu, X. Li, and H. Zhang, "Gait feature extraction and recognition based on improved Fourier transform," *J. Phys., Conf. Ser.*, vol. 1262, no. 1, 2019, Art. no. 012061.

[52] Y. Zhao, X. Yang, and Y. Jiang, "Gait feature extraction and recognition method based on principal component analysis and convolutional neural network," *Measurement*, vol. 184, 2021, Art. no. 109845.

[53] N. Abdullah, S. Yaacob, and H. Zamzuri, "Gait recognition using wavelet transform and support vector machine," *Indonesian J. Electr. Eng. Comput. Sci.*, vol. 17, no. 2, pp. 816–823, 2020.

[54] H. Wang, Y. Liu, and Y. Zhang, "Deep learning-based gait feature extraction and recognition for healthcare applications," *Sensors*, vol. 20, no. 14, p. 3883, 2020.

[55] A. Al-Rahayfeh, M. Al-Fayoumi, and A. Hudaib, "Gait recognition based on histogram of oriented gradients and convolutional neural networks," *Sensors*, vol. 21, no. 13, p. 4420, 2021.

[56] E. Sujatha and A. Chilambuchelvan, "Multimodal biometric authentication algorithm using iris, palm print, face and signature with encoded DWT," *Wireless Pers. Commun.*, vol. 99, no. 1, pp. 23–34, Mar. 2018.

[57] M. R. Karim, M. S. Alam, and M. Z. Abedin, "Offline signature verification based on dynamic time warping," *IEEE Access*, vol. 9, pp. 85339–85352, 2021.

[58] M. Gómez-Barrero, F. Maiorano, and J. Fierrez, "Online signature verification using convolutional neural networks with offline training," *Sensors*, vol. 21, no. 9, p. 3037, 2021.

[59] J. Guo, W. Zhang, and X. Shang, "Offline signature verification based on the wavelet transform and modified image enhancement," *J. Inf. Secur. Appl.*, vol. 56, 2020, Art. no. 102607.

[60] X. Zhang and L. Chen, "Offline handwritten signature verification based on improved principal component analysis and deep belief network," *Appl. Sci.*, vol. 11, no. 3, p. 1148, 2021.

[61] W. G. Al-Khatib, A. R. Ramli, and K. B. Ahmad, "Enhanced offline signature verification using combination of directional features and machine learning techniques," *Int. J. Adv. Comput. Sci. Appl.*, vol. 11, no. 9, pp. 68–74, 2020.

[62] K. Li, C. Baird, and D. Lin, "Defend data poisoning attacks on voice authentication," 2022, *arXiv:2209.04547*.

[63] S. Huda, M. A. Islam, and N. U. Siddique, "Comparative analysis of feature extraction techniques for speaker recognition," in *Proc. Int. Conf. Electr., Comput., Commun. Eng. (ECCE)*, 2022.

[64] H. Jiang, X. Zhou, and S. Li, "Voice feature extraction based on linear prediction and convolutional neural network," in *Proc. Int. Conf. Artif. Intell. Educ. Technol. (ICAIET)*, 2021.

[65] S. Barman, A. Das, and D. Bhattacharyya, "Comparative study on feature extraction techniques for speaker verification system," *Int. J. Emerg. Technol. Innov. Eng.*, vol. 7, no. 5, pp. 124–130, 2021.

[66] C. Huang, Y. Wang, and Y. Huang, "Speaker identification based on improved pitch detection algorithm," *J. Phys., Conf. Ser.*, vol. 1618, no. 4, 2020, Art. no. 042031.

[67] Z. He, Y. Chen, D. Zhang, W. Yin, and H. R. Karimi, "A new intelligent ECG recognition approach based on CNN and improved ALO-SVM," *Signal, Image Video Process.*, vol. 17, no. 4, pp. 965–972, Jun. 2023.

[68] P. Bashivan, I. Rish, M. Yeasin, and N. Codella, "Learning representations from EEG with deep recurrent-convolutional neural networks," 2015, *arXiv:1511.06448*.

[69] J. Rizkallah and M. S. Mabrouk, "Eeg signal classification based on multi-scale wavelet-based features and adaptive neuro-fuzzy inference system," *Cognit. Neurodyn.*, vol. 12, no. 4, pp. 353–362, 2018.

[70] L. N. Sharma et al., "EEG-based motor imagery classification using entropy-based features and machine learning techniques," *J. Healthcare Eng.*, vol. 2019, pp. 1–11, Jan. 2019.

[71] J. Pinto, J. Cardoso, A. Lourenço, and C. Carreiras, "Towards a continuous biometric system based on ECG signals acquired on the steering wheel," *Sensors*, vol. 17, no. 10, p. 2228, Sep. 2017.

[72] C. Sun, Q. Ma, and W. Jing, "Ecg signal feature extraction and classification based on variational mode decomposition and deep learning," *J. Ambient Intell. Humanized Comput.*, vol. 11, no. 10, pp. 4221–4231, 2020.

[73] V. Sharma, S. Sharma, and I. Kaur, "Feature extraction using discrete wavelet transform for ECG signal classification," in *Proc. 2nd Int. Conf. Inventive Syst. Control (ICISC)*, 2018, pp. 634–638.

[74] A. Jovic, N. Bogunovic, and D. Gajic, "Feature selection for ECG signal classification using mutual information," *Comput. Biol. Med.*, vol. 107, pp. 145–152, Jun. 2019.

[75] F. Shaffer and J. P. Ginsberg, "An overview of heart rate variability metrics and norms," *Frontiers Public Health*, vol. 5, p. 258, Sep. 2017.

[76] K. Prihodova and M. Hub, "Hand-based biometric system using convolutional neural networks," *Acta Inf. Pragensia*, vol. 9, no. 1, pp. 48–57, Jul. 2020.

[77] A. Kumar, D. C. M. Wong, H. C. Shen, and A. K. Jain, "Personal authentication using hand images," *Pattern Recognit. Lett.*, vol. 27, no. 13, pp. 1478–1486, Oct. 2006.

[78] M. Abo-Zahhad, S. M. Ahmed, and S. N. Abbas, "A new EEG acquisition protocol for biometric identification using eye blinking signals," *Int. J. Intell. Syst. Appl.*, vol. 7, no. 6, pp. 48–54, May 2015.

[79] H. J. Kim and J. S. Lim, "Study on a biometric authentication model based on ECG using a fuzzy neural network," *IOP Conf. Ser., Mater. Sci. Eng.*, vol. 317, Mar. 2018, Art. no. 012030.

[80] P. Tertychnyi, C. Ozcinar, and G. Anbarjafari, "Low-quality fingerprint classification using deep neural network," *IET Biometrics*, vol. 7, no. 6, pp. 550–556, Nov. 2018.

[81] R. Ryu, S. Yeom, S.-H. Kim, and D. Herbert, "Continuous multimodal biometric authentication schemes: A systematic review," *IEEE Access*, vol. 9, pp. 34541–34557, 2021.

[82] A. K. Jain, K. Nandakumar, and A. Ross, "50 years of biometric research: Accomplishments, challenges, and opportunities," *Pattern Recognit. Lett.*, vol. 79, pp. 80–105, Aug. 2016.

[83] D. Maltoni, D. Maio, A. K. Jain, and S. Prabhakar, *Handbook of Fingerprint Recognition*. Cham, Switzerland: Springer, 2016.

[84] M. Hammad, G. Luo, and K. Wang, "Cancelable biometric authentication system based on ECG," *Multimedia Tools Appl.*, vol. 78, no. 2, pp. 1857–1887, Jan. 2019.

[85] C. Yuan and X. Sun, "Fingerprint liveness detection adapted to different fingerprint sensors based on multiscale wavelet transform and rotation-invarient local binary pattern," *J. Internet Technol.*, vol. 19, no. 1, pp. 91–98, 2018.

[86] A. B. A. Hassanat, V. B. S. Prasath, M. Al-kasassbeh, A. S. Tarawneh, and A. J. Al-shamailh, "Magnetic energy-based feature extraction for low-quality fingerprint images," *Signal, Image Video Process.*, vol. 12, no. 8, pp. 1471–1478, Nov. 2018.

[87] A. Natarajan and N. Shanthi, "A survey on multimodal biometrics authentication and template protection," in *Proc. Int. Conf. Intell. Comput. Commun. Smart World (I2C2SW)*, Dec. 2018, pp. 64–71.

[88] T. Sabhanayagam, V. P. Venkatesan, and K. Senthamaraikannan, "A comprehensive survey on various biometric systems," *Int. J. Appl. Eng. Res.*, vol. 13, no. 5, pp. 2276–2297, 2018.

[89] L. N. Darlow and B. Rosman, "Fingerprint minutiae extraction using deep learning," in *Proc. IEEE Int. Joint Conf. Biometrics (IJCB)*, Oct. 2017, pp. 22–30.

[90] P. Aithal, "fingerprint image segmentation: A review of state of the art techniques," Tech. Rep., 2017.

[91] M. Sood and A. Girdhar, "A novel approach for low-quality fingerprint image enhancement using spatial and frequency domain filtering techniques," in *Cognitive Behavior and Human Computer Interaction Based on Machine Learning Algorithm*, 2021, pp. 265–299.

[92] D. Maltoni, D. Maio, A. K. Jain, and J. Feng, *Introduction*. Cham, Switzerland: Springer, 2022, pp. 1–62.

[93] A. J. Mohamed Abdul Cader, J. Banks, and V. Chandran, "Fingerprint systems: Sensors, image acquisition, interoperability and challenges," *Sensors*, vol. 23, no. 14, p. 6591, Jul. 2023.

[94] C. Lin and A. Kumar, "Matching contactless and contact-based conventional fingerprint images for biometrics identification," *IEEE Trans. Image Process.*, vol. 27, no. 4, pp. 2008–2021, Apr. 2018.

[95] J. Priesnitz, C. Rathgeb, N. Buchmann, C. Busch, and M. Margraf, "An overview of touchless 2D fingerprint recognition," *EURASIP J. Image Video Process.*, vol. 2021, no. 1, pp. 1–28, Dec. 2021.

[96] X. Yin, Y. Zhu, and J. Hu, "A survey on 2D and 3D contactless fingerprint biometrics: A taxonomy, review, and future directions," *IEEE Open J. Comput. Soc.*, vol. 2, pp. 370–381, 2021.

[97] Z. Zhang, X. Zhao, X. Zhang, X. Hou, X. Ma, S. Tang, Y. Zhang, G. Xu, Q. Liu, and S. Long, "In-sensor reservoir computing system for latent fingerprint recognition with deep ultraviolet photo-synapses and memristor array," *Nature Commun.*, vol. 13, no. 1, p. 6590, Nov. 2022.

[98] S. Hu, N. Short, K. Gurton, and B. Riggan, "Overview of polarimetric thermal imaging for biometrics," *Proc. SPIE*, vol. 10655, Jul. 2018, Art. no. 1065502.

[99] (Jan. 2023). [Online]. Available: https://www.nist.gov/news-events/news/2004/07/nist-study-shows-computerized-fingerprint-matching-highly-accurate

[100] K. Cao and A. K. Jain, "Fingerprint indexing and matching: An integrated approach," in *Proc. IEEE Int. Joint Conf. Biometrics (IJCB)*, Oct. 2017, pp. 437–445.

[101] D. Sero, I. Garachon, E. Hermens, R. V. Liere, and K. J. Batenburg, "The study of three-dimensional fingerprint recognition in cultural heritage: Trends and challenges," *J. Comput. Cultural Heritage*, vol. 14, no. 4, pp. 1–20, Dec. 2021.

[102] S. Garcia-Salicetti, C. Beumier, G. Chollet, B. Dorizzi, J. Jardins, J. Lunter, Y. Ni, and D. Petrovska-Delacrétaz, "BIOMET: A multimodal person authentication database including face, voice, fingerprint, hand and signature modalities," in *Proc. Int. Conf. Audio-Video-Based Biometric Person Authentication*, 2003, pp. 845–853.

[103] M. J. Lakshmi, K. S. Murthy, and S. N. Rao, "A novel algorithm for impulse noise removal using B-splines for finger print forensic images," *Int. J. Appl. Eng. Res.*, vol. 12, no. 1, pp. 127–131, 2017.

[104] E. J. Al Taee and Z. Abdulsamad, "A new approach for fingerprint authentication in biometric systems using BRISK algorithm," *Int. J. Adv. Sci., Eng. Inf. Technol.*, vol. 8, no. 5, pp. 1941–1947, Oct. 2018.

[105] A. I. Khan and M. A. Wani, "Patch-based segmentation of latent fingerprint images using convolutional neural network," *Appl. Artif. Intell.*, vol. 33, no. 1, pp. 87–100, Jan. 2019.

[106] H. T. Nguyen and L. T. Nguyen, "Fingerprints classification through image analysis and machine learning method," *Algorithms*, vol. 12, no. 11, p. 241, Nov. 2019.

[107] M. Kumar et al., "Various image enhancement and matching techniques used for fingerprint recognition system," *Int. J. Inf. Technol.*, vol. 11, no. 4, pp. 767–772, 2019.

[108] X.-Z. Chen, J.-L. Lin, and Y.-L. Chen, "FoD enroll image quality classification method for fingerprint authentication system," in *Proc. Int. Symp. Intell. Signal Process. Commun. Syst. (ISPACS)*, Nov. 2021, pp. 1–2.

[109] B. Pandya, G. Cosma, A. A. Alani, A. Taherkhani, V. Bharadi, and T. M. McGinnity, "Fingerprint classification using a deep convolutional neural network," in *Proc. 4th Int. Conf. Inf. Manage. (ICIM)*, May 2018, pp. 86–91.

[110] C. Lin and A. Kumar, "Contactless and partial 3D fingerprint recognition using multi-view deep representation," *Pattern Recognit.*, vol. 83, pp. 314–327, Nov. 2018.

[111] C. Lin and A. Kumar, "Tetrahedron based fast 3D fingerprint identification using colored LEDs illumination," *IEEE Trans. Pattern Anal. Mach. Intell.*, vol. 40, no. 12, pp. 3022–3033, Dec. 2018.

[112] S. Minaee, E. Azimi, and A. Abdolrashidi, "FingerNet: Pushing the limits of fingerprint recognition using convolutional neural network," 2019, *arXiv:1907.12956*.

[113] V. Anand and V. Kanhangad, "PoreNet: CNN-based pore descriptor for high-resolution fingerprint recognition," *IEEE Sensors J.*, vol. 20, no. 16, pp. 9305–9313, Aug. 2020.

[114] L. J. González-Soler, M. Gomez-Barrero, L. Chang, A. Pérez-Suárez, and C. Busch, "Fingerprint presentation attack detection based on local features encoding for unknown attacks," *IEEE Access*, vol. 9, pp. 5806–5820, 2021.

[115] M. Chhabra, K. K. Ravulakollu, M. Kumar, A. Sharma, and A. Nayyar, "Improving automated latent fingerprint detection and segmentation using deep convolutional neural network," *Neural Comput. Appl.*, vol. 35, no. 9, pp. 6471–6497, Mar. 2023.

[116] Y. Li, L. Pang, H. Zhao, Z. Cao, E. Liu, and J. Tian, "Indexing-min–max hashing: Relaxing the security–performance tradeoff for cancelable fingerprint templates," *IEEE Trans. Syst., Man, Cybern., Syst.*, vol. 52, no. 10, pp. 6314–6325, Oct. 2022.

[117] A. Rai, S. Dey, P. Patidar, and P. Rai, "MoSFPAD: An end-to-end ensemble of MobileNet and support vector classifier for fingerprint presentation attack detection," 2023, *arXiv:2303.01465*.

[118] R. Kumar, P. Chandra, and M. Hanmandlu, "Local directional pattern (LDP) based fingerprint matching using SLFNN," in *Proc. IEEE 2nd Int. Conf. Image Inf. Process.*, Dec. 2013, pp. 493–498.

[119] C. H. Park and H. Park, "Fingerprint classification using fast Fourier transform and nonlinear discriminant analysis," *Pattern Recognit.*, vol. 38, no. 4, pp. 495–503, Apr. 2005.

[120] C. Yuan, X. Sun, and R. Lv, "Fingerprint liveness detection based on multi-scale LPQ and PCA," *China Commun.*, vol. 13, no. 7, pp. 60–65, Jul. 2016.

[121] J. G. Daugman, "Gabor filtering for fingerprint image enhancement," *IEEE Trans. Image Process.*, vol. 26, no. 1, pp. 1–7, 2017.

[122] J. Smith, "Minutiae-based fingerprint feature extraction," *Int. J. Biometrics*, vol. 12, no. 3, pp. 123–135, 2017.

[123] M. Johnson, "Ridge counting in fingerprint feature extraction," *J. Pattern Recognit.*, vol. 25, no. 2, pp. 67–82, 2018.

[124] A. Miller, "Advancements in fingerprint recognition: A comprehensive review," *Pattern Recognit.*, vol. 93, pp. 238–258, Jan. 2019.

[125] M. Mua'ad, Z. A. Alqadi, and K. Aldebei, "Comparative analysis of fingerprint features extraction methods," *J. Hunan Univ. Natural Sci.*, vol. 48, no. 12, 2021.

[126] S. Dey, S. Dey, M. Maitra, M. Ghosh, K. Dey, and A. C. Bovik, "Fingerprint image quality analysis using convolutional neural network," in *Proc. IEEE Calcutta Conf. (CALCON)*, 2016, pp. 1–6.

[127] F. Li, C. Zhang, W. Du, J. Qiao, and B. Wen, "Siamese neural networks for one-shot image recognition," in *Proc. IEEE Conf. Comput. Vis. Pattern Recognit.*, 2017, pp. 945–953.

[128] A. Vaswani, N. Shazeer, N. Parmar, J. Uszkoreit, L. Jones, A. N. Gomez, L. Kaiser, and I. Polosukhin, "Attention is all you need," in *Proc. Adv. Neural Inf. Process. Syst.*, vol. 30, 2017.

[129] S. Minaee and A. Abdolrashidi, "Finger-GAN: Generating realistic fingerprint images using connectivity imposed GAN," 2018, *arXiv:1812.10482*.

[130] T. Singh, S. Bhisikar, and M. Kumar, "Fingerprint identification using modified capsule network," in *Proc. 12th Int. Conf. Comput. Commun. Netw. Technol. (ICCCNT)*, Jul. 2021, pp. 1–6.

[131] D. Peralta, S. García, J. M. Benitez, and F. Herrera, "Minutiae-based fingerprint matching decomposition: Methodology for big data frameworks," *Inf. Sci.*, vol. 408, pp. 198–212, Oct. 2017.

[132] K. Castillo-Rosado and J. Hernández-Palancar, "Latent fingerprint matching using distinctive ridge points," *Informatica*, vol. 30, no. 3, pp. 431–454, Jan. 2019.

[133] Y. Liu, B. Zhou, C. Han, T. Guo, and J. Qin, "A novel method based on deep learning for aligned fingerprints matching," *Appl. Intell.*, vol. 50, no. 2, pp. 397–416, Feb. 2020.

[134] A. Al-Refoa, M. Alshraideh, and A. Sharieh, "A new algorithm for locating and extracting minutiae from fingerprint images," *Pattern Recognit. Image Anal.*, vol. 29, no. 2, pp. 268–279, Apr. 2019.

[135] S. R. Borra, G. J. Reddy, and E. S. Reddy, "An efficient fingerprint identification using neural network and BAT algorithm," *Int. J. Electr. Comput. Eng.*, vol. 8, no. 2, p. 1194, Apr. 2018.

[136] F. Liu, Y. Zhao, G. Liu, and L. Shen, "Fingerprint pore matching using deep features," *Pattern Recognit.*, vol. 102, Jun. 2020, Art. no. 107208.

[137] Y. Surajkanta and S. Pal, "A digital geometry-based fingerprint matching technique," *Arabian J. Sci. Eng.*, vol. 46, no. 4, pp. 4073–4086, Apr. 2021.

[138] W. Yang, G. Zheng, A. Ibrahim, J. Chaudhry, S. Wang, J. Hu, and C. Valli, "Application of 3D Delaunay triangulation in fingerprint authentication system," in *Proc. Int. Conf. Mobile Netw. Manage.* Cham, Switzerland: Springer, 2017, pp. 291–298.

[139] L. J. González-Soler, M. Gomez-Barrero, J. Kolberg, L. Chang, A. Pérez-Suárez, and C. Busch, "Local feature encoding for unknown presentation attack detection: An analysis of different local feature descriptors," *IET Biometrics*, vol. 10, no. 4, pp. 374–391, Jul. 2021.

[140] J. W. Souza, A. G. Medeiros, G. B. Holanda, P. A. Rego, and P. P. Rebouças Filho, "Fingerprint classification based on the Henry system via ResNet," in *Proc. Int. Conf. Syst., Signals Image Process.* Cham, Switzerland: Springer, 2021, pp. 15–28.

[141] P. Nahar, N. S. Chaudhari, and S. K. Tanwani, "Fingerprint classification system using CNN," *Multimedia Tools Appl.*, vol. 81, no. 17, pp. 24515–24527, Jul. 2022.

[142] P. Gupta, K. Tiwari, and G. Arora, "Fingerprint indexing schemes—A survey," *Neurocomputing*, vol. 335, pp. 352–365, Mar. 2019.

[143] R. Cappelli, "Fast and accurate fingerprint indexing based on ridge orientation and frequency," *IEEE Trans. Syst., Man, Cybern., B, Cybern.*, vol. 41, no. 6, pp. 1511–1521, Dec. 2011.

[144] V. Anand and V. Kanhangad, "Pore based indexing for high-resolution fingerprints," in *Proc. IEEE Int. Conf. Identity, Secur. Behav. Anal. (ISBA)*, Feb. 2017, pp. 1–6.

[145] M. M. Rahman, T. I. Mishu, and M. A. A. Bhuiyan, "Performance analysis of a parameterized minutiae-based approach for securing fingerprint templates in biometric authentication systems," *J. Inf. Secur. Appl.*, vol. 67, Jun. 2022, Art. no. 103209.

[146] I. Pérez-Sánchez, B. Cervantes, M. A. Medina-Pérez, R. Monroy, O. Loyola-González, S. García, and F. Herrera, "An indexing algorithm based on clustering of minutia cylinder codes for fast latent fingerprint identification," *IEEE Access*, vol. 9, pp. 85488–85499, 2021.

[147] V. Anand and V. Kanhangad, "Pore-based indexing for fingerprints acquired using high-resolution sensors," *Pattern Anal. Appl.*, vol. 23, no. 1, pp. 429–441, Feb. 2020.

[148] C.-C. Bai, W.-Q. Wang, T. Zhao, R.-X. Wang, and M.-Q. Li, "Deep learning compact binary codes for fingerprint indexing," *Frontiers Inf. Technol. Electron. Eng.*, vol. 19, no. 9, pp. 1112–1123, Sep. 2018.

[149] Y. Jiang and X. Liu, "Uniform local binary pattern for fingerprint liveness detection in the Gaussian pyramid," *J. Electr. Comput. Eng.*, vol. 2018, pp. 1–9, Mar. 2018.

[150] Z. Xia, R. Lv, and X. Sun, "Rotation-invariant weber pattern and Gabor feature for fingerprint liveness detection," *Multimedia Tools Appl.*, vol. 77, no. 14, pp. 18187–18200, Jul. 2018.

[151] R. Mehboob, H. Dawood, H. Dawood, M. U. Ilyas, P. Guo, and A. Banjar, "Live fingerprint detection using magnitude of perceived spatial stimuli and local phase information," *J. Electron. Imag.*, vol. 27, no. 5, p. 1, Oct. 2018.

[152] Y. Zhang, D. Shi, X. Zhan, D. Cao, K. Zhu, and Z. Li, "Slim-ResCNN: A deep residual convolutional neural network for fingerprint liveness detection," *IEEE Access*, vol. 7, pp. 91476–91487, 2019.

[153] C. Yuan, Z. Xia, L. Jiang, Y. Cao, Q. M. Jonathan Wu, and X. Sun, "Fingerprint liveness detection using an improved CNN with image scale equalization," *IEEE Access*, vol. 7, pp. 26953–26966, 2019.

[154] C. Yuan, X. Chen, P. Yu, R. Meng, W. Cheng, Q. M. J. Wu, and X. Sun, "Semi-supervised stacked autoencoder-based deep hierarchical semantic feature for real-time fingerprint liveness detection," *J. Real-Time Image Process.*, vol. 17, no. 1, pp. 55–71, Feb. 2020.

[155] D. Chitra and V. Sujitha, "Security analysis of prealigned fingerprint template using fuzzy vault scheme," *Cluster Comput.*, vol. 22, no. S5, pp. 12817–12825, Sep. 2019.

[156] W. Ponce-Hernandez, R. Blanco-Gonzalo, R. Sanchez-Reillo, and J. Liu-Jimenez, "Template protection approaches: Fuzzy vault scheme," in *Proc. Int. Carnahan Conf. Secur. Technol. (ICCST)*, Oct. 2019, pp. 1–5.

[157] S. Chauhan and A. Sharma, "Improved fuzzy commitment scheme," *Int. J. Inf. Technol.*, vol. 14, no. 3, pp. 1321–1331, May 2022.

[158] R. F. Soliman, M. Amin, and F. E. Abd El-Samie, "Cancelable iris recognition system based on comb filter," *Multimedia Tools Appl.*, vol. 79, nos. 3–4, pp. 2521–2541, Jan. 2020.

[159] O. C. Abikoye, U. A. Ojo, J. B. Awotunde, and R. O. Ogundokun, "A safe and secured iris template using steganography and cryptography," *Multimedia Tools Appl.*, vol. 79, nos. 31–32, pp. 23483–23506, Aug. 2020.

[160] G. Panchal and D. Samanta, "A novel approach to fingerprint biometric-based cryptographic key generation and its applications to storage security," *Comput. Electr. Eng.*, vol. 69, pp. 461–478, Jul. 2018.

[161] P. Thejaswini, R. Srikantaswamy, and A. Manjunatha, "Novel adaptive auto-correction technique for enhanced fingerprint recognition," *Int. J. Adv. Comput. Sci. Appl.*, vol. 10, no. 8, 2019.

[162] S.-W. Oh, H. Park, and J.-B. Kim, "The fingerprint authentication model using smartphone camera," *J. Adv. Res. Dyn. Control Syst.*, vol. 11, no. 5, pp. 264–272, 2019.

[163] K. Noor, T. Jan, M. Basheri, A. Ali, R. A. Khalil, M. H. Zafar, M. Ashraf, M. I. Babar, and S. W. Shah, "Performances enhancement of fingerprint recognition system using classifiers," *IEEE Access*, vol. 7, pp. 5760–5768, 2019.

[164] L. Almajmaie, O. N. Ucan, and O. Bayat, "Fingerprint recognition system based on modified multi-connect architecture (MMCA)," *Cognit. Syst. Res.*, vol. 58, pp. 107–113, Dec. 2019.

[165] P. Vidyasree and S. ViswanadhaRaju, "Minimum cost fingerprint matching on fused features through deep learning techniques," in *Data Engineering and Communication Technology*. Cham, Switzerland: Springer, 2020, pp. 131–140.

[166] Y. Li, H. Zhao, Z. Cao, E. Liu, and L. Pang, "Ordered and fixed-length bit-string fingerprint representation with minutia vicinity combined feature and spectral clustering," *IET Image Process.*, vol. 14, no. 16, pp. 4220–4228, Dec. 2020.

[167] A. Rojas and G. J. Dolecek, "Fingerprint recognition based on wavelet transform and ensemble subspace classifier," in *Proc. IEEE URUCON*, Nov. 2021, pp. 508–511.

[168] H. Mo and S. Kim, "A deep learning-based human identification system with Wi-Fi CSI data augmentation," *IEEE Access*, vol. 9, pp. 91913–91920, 2021.

[169] P. K. Chundi, A. K. Sridhar, S. Sarup, and M. Seok, "High-capacity fingerprint recognition system based on a dynamic memory-capacity estimation technique," in *Proc. IEEE Biomed. Circuits Syst. Conf. (BioCAS)*, Oct. 2018, pp. 1–4.

[170] D. Moga and I. Filip, "Study on fingerprint authentication systems using convolutional neural networks," in *Proc. IEEE 15th Int. Symp. Appl. Comput. Intell. Informat. (SACI)*, May 2021, pp. 000015–000020.

[171] X. Yin, Y. Zhu, and J. Hu, "Contactless fingerprint recognition based on global minutia topology and loose genetic algorithm," *IEEE Trans. Inf. Forensics Security*, vol. 15, pp. 28–41, 2020.

[172] X. Yin, Y. Zhu, and J. Hu, "3D fingerprint recognition based on ridge-valley-guided 3D reconstruction and 3D topology polymer feature extraction," *IEEE Trans. Pattern Anal. Mach. Intell.*, vol. 43, no. 3, pp. 1085–1091, Mar. 2021.

[173] R. Donida Labati, A. Genovese, V. Piuri, and F. Scotti, "A scheme for fingerphoto recognition in smartphones," in *Selfie Biometrics*, 2019, pp. 49–66.

[174] M. B. Veena, "Analysis of polynomial co-efficient based authentication for 3D fingerprints," in *Proc. IEEE Int. Conf. Innov. Technol. (INOCON)*, Nov. 2020, pp. 1–6.

[175] S. Cimato, M. Gamassi, V. Piuri, D. Sana, R. Sassi, and F. Scotti, "Personal identification and verification using multimodal biometric data," in *Proc. IEEE Int. Conf. Comput. Intell. Homeland Secur. Pers. Saf.*, Oct. 2006, pp. 41–45.

[176] J. Fei, Z. Xia, P. Yu, and F. Xiao, "Adversarial attacks on fingerprint liveness detection," *EURASIP J. Image Video Process.*, vol. 2020, no. 1, pp. 1–11, Dec. 2020.

[177] H. Liu, W. Zhang, F. Liu, H. Wu, and L. Shen, "Fingerprint presentation attack detector using global-local model," *IEEE Trans. Cybern.*, vol. 52, no. 11, pp. 12315–12328, Nov. 2022.

[178] F. Liu, H. Liu, W. Zhang, G. Liu, and L. Shen, "One-class fingerprint presentation attack detection using auto-encoder network," *IEEE Trans. Image Process.*, vol. 30, pp. 2394–2407, 2021.

[179] W. Zhang, H. Liu, and F. Liu, "Fingerprint presentation attack detection by learning in frequency domain," in *Proc. IEEE 2nd Int. Conf. Pattern Recognit. Mach. Learn. (PRML)*, Jul. 2021, pp. 183–189.

[180] A. Popli, S. Tandon, J. J. Engelsma, N. Onoe, A. Okubo, and A. Namboodiri, "A unified model for fingerprint authentication and presentation attack detection," in *Proc. IEEE Int. Joint Conf. Biometrics (IJCB)*, Aug. 2021, pp. 1–8.

[181] A. Husseis, J. Liu-Jimenez, and R. Sanchez-Reillo, "The impact of pressure on the fingerprint impression: Presentation attack detection scheme," *Appl. Sci.*, vol. 11, no. 17, p. 7883, Aug. 2021.

[182] S. Wang, W. Yang, and J. Hu, "Design of alignment-free cancelable fingerprint templates with zoned minutia pairs," *Pattern Recognit.*, vol. 66, pp. 295–301, Jun. 2017.

[183] H. Kim, X. Cui, M.-G. Kim, and T. H. B. Nguyen, "Fingerprint generation and presentation attack detection using deep neural networks," in *Proc. IEEE Conf. Multimedia Inf. Process. Retr. (MIPR)*, Mar. 2019, pp. 375–378.

[184] M. E. Hussein, L. Spinoulas, F. Xiong, and W. Abd-Almageed, "Fingerprint presentation attack detection using a novel multi-spectral capture device and patch-based convolutional neural networks," in *Proc. IEEE Int. Workshop Inf. Forensics Secur. (WIFS)*, Dec. 2018, pp. 1–8.

[185] A. Roy, N. Memon, J. Togelius, and A. Ross, "Evolutionary methods for generating synthetic MasterPrint templates: Dictionary attack in fingerprint recognition," in *Proc. Int. Conf. Biometrics (ICB)*, Feb. 2018, pp. 39–46.

[186] S. M. Abdullahi, H. Wang, and T. Li, "Fractal coding-based robust and alignment-free fingerprint image hashing," *IEEE Trans. Inf. Forensics Security*, vol. 15, pp. 2587–2601, 2020.

[187] S. Raj, J. S. Pannu, S. L. Fernandes, A. Ramanathan, L. L. Pullum, and S. K. Jha, "Attacking NIST biometric image software using nonlinear optimization," *Pattern Recognit. Lett.*, vol. 131, pp. 79–84, Mar. 2020.

[188] Y. Lai, Z. Jin, K. Wong, and M. Tistarelli, "Efficient known-sample attack for distance-preserving hashing biometric template protection schemes," *IEEE Trans. Inf. Forensics Security*, vol. 16, pp. 3170–3185, 2021.

[189] X. Dong, Z. Jin, and A. T. B. Jin, "A genetic algorithm enabled similarity-based attack on cancellable biometrics," in *Proc. IEEE 10th Int. Conf. Biometrics Theory, Appl. Syst. (BTAS)*, Sep. 2019, pp. 1–8.

[190] M. Shahzad, S. Wang, G. Deng, and W. Yang, "Alignment-free cancelable fingerprint templates with dual protection," *Pattern Recognit.*, vol. 111, Mar. 2021, Art. no. 107735.

[191] M. J. Lee, A. B. J. Teoh, A. Uhl, S.-N. Liang, and Z. Jin, "A tokenless cancellable scheme for multimodal biometric systems," *Comput. Secur.*, vol. 108, Sep. 2021, Art. no. 102350.

[192] Q. N. Tran and J. Hu, "A multi-filter fingerprint matching framework for cancelable template design," *IEEE Trans. Inf. Forensics Security*, vol. 16, pp. 2926–2940, 2021.

[193] S. H. Park, M. Y. Lim, D. Kang, and Y. K. Lee, "Towards robust combination of neural networks for fingerprint presentation attack detection," in *Proc. 13th Int. Conf. Inf. Commun. Technol. Converg. (ICTC)*, Oct. 2022, pp. 1829–1834.

[194] Y. Sun, L. Leng, Z. Jin, and B.-G. Kim, "Reinforced palmprint reconstruction attacks in biometric systems," *Sensors*, vol. 22, no. 2, p. 591, Jan. 2022.

[195] K. P. Wijewardena, S. A. Grosz, K. Cao, and A. K. Jain, "Fingerprint template invertibility: Minutiae vs. deep templates," *IEEE Trans. Inf. Forensics Security*, vol. 18, pp. 744–757, 2023.

[196] D. Sadhya, S. K. Singh, and B. Chakraborty, "Review of key-binding-based biometric data protection schemes," *IET Biometrics*, vol. 5, no. 4, pp. 263–275, Dec. 2016.

[197] M. Lutsenko, A. Kuznetsov, A. Kiian, O. Smirnov, and T. Kuznetsova, "Biometric cryptosystems: Overview, state-of-the-art and perspective directions," in *Proc. Conf. Math. Control Theory*. Cham, Switzerland: Springer, 2019, pp. 66–84.

[198] M. Alloghani, M. M. Alani, D. Al-Jumeily, T. Baker, J. Mustafina, A. Hussain, and A. J. Aljaaf, "A systematic review on the status and progress of homomorphic encryption technologies," *J. Inf. Secur. Appl.*, vol. 48, Oct. 2019, Art. no. 102362.

[199] M. Vijay and G. Indumathi, "Deep belief network-based hybrid model for multimodal biometric system for futuristic security applications," *J. Inf. Secur. Appl.*, vol. 58, May 2021, Art. no. 102707.

[200] A. Kumar, R. Rani, and S. Singh, "A survey of recent advances in image steganography," *Secur. Privacy*, vol. 6, no. 3, p. e281, 2023.

[201] N. Kumar, "Cancelable biometrics: A comprehensive survey," *Artif. Intell. Rev.*, vol. 53, no. 5, pp. 3403–3446, Jun. 2020.

[202] C. Kant and S. Chaudhary, "A watermarking based approach for protection of templates in multimodal biometric system," *Proc. Comput. Sci.*, vol. 167, pp. 932–941, Jan. 2020.

[203] M. Tarek, E. Hamouda, and S. El-Metwally, "Unimodal-bio-GAN: Keyless biometric salting scheme based on generative adversarial network," *IET Biometrics*, vol. 10, no. 6, pp. 654–663, Nov. 2021.

[204] J. Kim and A. B. Jin Teoh, "One-factor cancellable biometrics based on indexing-first-order hashing for fingerprint authentication," in *Proc. 24th Int. Conf. Pattern Recognit. (ICPR)*, Aug. 2018, pp. 3108–3113.

[205] K. Jihyeon and A. B. J. Teoh, "Sparse combined index-of-max hashing for fingerprint template protection," in *Proc. 12th Int. Congr. Image Signal Process., Biomed. Eng. Informat. (CISP-BMEI)*, Oct. 2019, pp. 1–6.

[206] H. Djebli, S. Ait-Aoudia, and D. Michelucci, "Quantized random projections of SIFT features for cancelable fingerprints," *Multimedia Tools Appl.*, vol. 82, no. 5, pp. 7917–7937, Feb. 2023.

[207] J. B. Kho, J. Kim, I.-J. Kim, and A. B. J. Teoh, "Cancelable fingerprint template design with randomized non-negative least squares," *Pattern Recognit.*, vol. 91, pp. 245–260, Jul. 2019.

[208] Z. Jin, J. Y. Hwang, Y.-L. Lai, S. Kim, and A. B. J. Teoh, "Ranking-based locality sensitive hashing-enabled cancelable biometrics: Index-of-max hashing," *IEEE Trans. Inf. Forensics Security*, vol. 13, no. 2, pp. 393–407, Feb. 2018.

[209] H. Li and X. Wang, "One factor cancellable fingerprint scheme based on novel minimum hash signature and secure extended feature vector," *Multimedia Tools Appl.*, vol. 81, no. 9, pp. 13087–13113, Apr. 2022.

[210] V. S. Baghel, S. Prakash, and I. Agrawal, "An enhanced fuzzy vault to secure the fingerprint templates," *Multimedia Tools Appl.*, vol. 80, nos. 21–23, pp. 33055–33073, Sep. 2021.

[211] T. M. Dang, T. D. Nguyen, T. Hoang, H. Kim, A. B. J. Teoh, and D. Choi, "AVET: A novel transform function to improve cancellable biometrics security," *IEEE Trans. Inf. Forensics Security*, vol. 18, pp. 758–772, 2023.

[212] S. Wang, G. Deng, and J. Hu, "A partial Hadamard transform approach to the design of cancelable fingerprint templates containing binary biometric representations," *Pattern Recognit.*, vol. 61, pp. 447–458, Jan. 2017.

[213] A. K. Trivedi, D. M. Thounaojam, and S. Pal, "Non-invertible cancellable fingerprint template for fingerprint biometric," *Comput. Secur.*, vol. 90, Mar. 2020, Art. no. 101690.

[214] A. Bedari, S. Wang, and W. Yang, "Design of cancelable MCC-based fingerprint templates using dyno-key model," *Pattern Recognit.*, vol. 119, Nov. 2021, Art. no. 108074.

[215] D. Jagadiswary and D. Saraswady, "Biometric authentication using fused multimodal biometric," *Proc. Comput. Sci.*, vol. 85, pp. 109–116, Jan. 2016.

[216] O. Nafea, S. Ghouzali, W. Abdul, and E.-u.-H. Qazi, "Hybrid multi-biometric template protection using watermarking," *Comput. J.*, vol. 59, no. 9, pp. 1392–1407, Sep. 2016.

[217] M. Gomez-Barrero, E. Maiorana, J. Galbally, P. Campisi, and J. Fierrez, "Multi-biometric template protection based on homomorphic encryption," *Pattern Recognit.*, vol. 67, pp. 149–163, Jul. 2017.

[218] L. Ghammam, M. Barbier, and C. Rosenberger, "Enhancing the security of transformation based biometric template protection schemes," in *Proc. Int. Conf. Cyberworlds (CW)*, Oct. 2018, pp. 316–323.

[219] T. Stanko, B. Chen, and B. Skoric, "Fingerprint template protection using minutia-pair spectral representations," 2018, *arXiv:1804.01744*.

[220] K. Atighehchi, L. Ghammam, M. Barbier, and C. Rosenberger, "GREYC-hashing: Combining biometrics and secret for enhancing the security of protected templates," *Future Gener. Comput. Syst.*, vol. 101, pp. 819–830, Dec. 2019.

[221] R. Mehmood and A. Selwal, "Polynomial based fuzzy vault technique for template security in fingerprint biometrics," *Int. Arab J. Inf. Technol.*, vol. 17, no. 6, pp. 926–934, Nov. 2020.

[222] A. Ali, V. S. Baghel, and S. Prakash, "An alignment-free fingerprint template protection technique based on minutiae triplets," in *Proc. Int. Conf. Recent Trends Image Process. Pattern Recognit.* Cham, Switzerland: Springer, 2021, pp. 169–182.

[223] S. D. Patil, R. Raut, R. H. Jhaveri, T. A. Ahanger, P. V. Dhade, A. B. Kathole, and K. N. Vhatkar, "Robust authentication system with privacy preservation of biometrics," *Secur. Commun. Netw.*, vol. 2022, pp. 1–14, May 2022.

[224] M. Imteyaz Mohsin, J. Bharti, and R. K. Pateriya, "Improved bio-hashing fingerprint security using modified Arnold's cat map," in *Artificial Intelligence and Sustainable Computing*, M. Pandit, M. K. Gaur, P. S. Rana, and A. Tiwari, Eds. Singapore: Springer, 1007, pp. 159–173.

[225] A. Ali, V. S. Baghel, and S. Prakash, "A novel technique for fingerprint template security in biometric authentication systems," *Vis. Comput.*, vol. 39, no. 12, pp. 6249–6263, Dec. 2023.

[226] J. J. Engelsma, A. K. Jain, and V. N. Boddeti, "HERS: Homomorphically encrypted representation search," *IEEE Trans. Biometrics, Behav., Identity Sci.*, vol. 4, no. 3, pp. 349–360, Jul. 2022.

[227] T. Thomas, "Cancelable biometric scheme based on dynamic salting of random patches," *Multimedia Tools Appl.*, vol. 82, no. 10, pp. 14337–14366, Apr. 2023.

[228] V. Talreja, M. C. Valenti, and N. M. Nasrabadi, "Multibiometric secure system based on deep learning," in *Proc. IEEE Global Conf. Signal Inf. Process. (GlobalSIP)*, Nov. 2017, pp. 298–302.

[229] B. Abd El-Rahiem, F. E. Abd El Samie, and M. Amin, "Efficient cancellable multi-biometric recognition system based on deep learning and bio-hashing," *Appl. Intell.*, vol. 53, no. 2, pp. 1792–1806, Jan. 2023.

[230] B. Topcu, H. Erdogan, C. Karabat, and B. Yanikoglu, "Biohashing with fingerprint spectral minutiae," in *Proc. Int. Conf. BIOSIG Special Interest Group (BIOSIG)*, Sep. 2013, pp. 1–12.

[231] M. Elmouhtadi and M. Lafkih, "Biometric protection approach based on fingerprint hierarchical identification," *Int. J. Appl. Eng. Res.*, vol. 12, no. 21, pp. 11007–11014, 2017.

[232] A. K. Trivedi, D. M. Thounaojam, and S. Pal, "A robust and non-invertible fingerprint template for fingerprint matching system," *Forensic Sci. Int.*, vol. 288, pp. 256–265, Jul. 2018.

[233] D. Mahto and D. K. Yadav, "A secure one-time password authentication scheme using elliptic curve cryptography with fingerprint biometric," *J. Eng. Appl. Sci.*, 2017.

[234] L. Rzouga Haddada, B. Dorizzi, and N. Essoukri Ben Amara, "A combined watermarking approach for securing biometric data," *Signal Process., Image Commun.*, vol. 55, pp. 23–31, Jul. 2017.

[235] S. S. Ali, I. I. Ganapathi, and S. Prakash, "Robust technique for fingerprint template protection," *IET Biometrics*, vol. 7, no. 6, pp. 536–549, Nov. 2018.

[236] D. Harikrishnan, N. Sunil Kumar, S. Joseph, and K. K. Nair, "Towards a fast and secure fingerprint authentication system based on a novel encoding scheme," *Int. J. Electr. Eng. Educ.*, vol. 61, no. 1, pp. 100–112, Jan. 2024.

[237] S. S. Ali and S. Prakash, "3-dimensional secured fingerprint shell," *Pattern Recognit. Lett.*, vol. 126, pp. 68–77, Sep. 2019.

[238] T. Kim, Y. Oh, and H. Kim, "Efficient privacy-preserving fingerprint-based authentication system using fully homomorphic encryption," *Secur. Commun. Netw.*, vol. 2020, pp. 1–11, Feb. 2020.

[239] D. Rachapalli and H. Kalluri, "Color QR pattern-driven cancelable biometric fingerprint system," *Ingénierie Systèmes Inf.*, vol. 25, no. 2, pp. 245–251, May 2020.

[240] F. Liu, G. Liu, Q. Zhao, and L. Shen, "Robust and high-security fingerprint recognition system using optical coherence tomography," *Neurocomputing*, vol. 402, pp. 14–28, Aug. 2020.

[241] W. Yang, S. Wang, K. Yu, J. J. Kang, and M. N. Johnstone, "Secure fingerprint authentication with homomorphic encryption," in *Proc. Digit. Image Comput., Techn. Appl. (DICTA)*, Nov. 2020, pp. 1–6.

[242] Y. Li, H. Zhao, Z. Cao, E. Liu, and L. Pang, "Compact and cancelable fingerprint binary codes generation via one permutation hashing," *IEEE Signal Process. Lett.*, vol. 28, pp. 738–742, 2021.

[243] M. O. Oloyede and G. P. Hancke, "Unimodal and multimodal biometric sensing systems: A review," *IEEE Access*, vol. 4, pp. 7532–7555, 2016.

[244] M. Gavrilova, I. Luchak, T. Sudhakar, and S. N. Tumpa, "Artificial intelligence in biometrics: Uncovering intricacies of human body and mind," in *Advances in Selected Artificial Intelligence Areas: World Outstanding Women in Artificial Intelligence*. Cham, Switzerland: Springer, 2022, pp. 123–169.

[245] S. Ahmad, R. Pal, and A. Ganivada, "Rank level fusion of multimodal biometrics based on cross-entropy Monte Carlo method," in *Proc. International Symposium on Signal Processing and Intelligent Recognition Systems*. Cham, Switzerland: Springer, 2019, pp. 64–74.

[246] A. Herbadji, N. Guermat, L. Ziet, Z. Akhtar, M. Cheniti, and D. Herbadji, "Contactless multi-biometric system using fingerprint and palmprint selfies," *Traitement Signal*, vol. 37, no. 6, pp. 889–897, Dec. 2020.

[247] Y. Zhang, C. Gao, S. Pan, Z. Li, Y. Xu, and H. Qiu, "A score-level fusion of fingerprint matching with fingerprint liveness detection," *IEEE Access*, vol. 8, pp. 183391–183400, 2020.

[248] S. A. E. Rahman, "Multimodal biometric systems based on different fusion levels of ECG and fingerprint using different classifiers," *Soft Comput.*, vol. 24, no. 16, pp. 12599–12632, Aug. 2020.

[249] K. Aizi and M. Ouslim, "Score level fusion in multi-biometric identification based on zones of interest," *J. King Saud Univ.-Comput. Inf. Sci.*, vol. 34, no. 1, pp. 1498–1509, Jan. 2022.

[250] R. Hammouche, A. Attia, and S. Akhrouf, "Score level fusion of major and minor finger knuckle patterns based symmetric sum-based rules for person authentication," *Evolving Syst.*, vol. 13, no. 3, pp. 469–483, Jun. 2022.

[251] R. Srivastava, V. P. Bhardwaj, M. T. B. Othman, M. Pushkarna, A. Mangla, M. Bajaj, A. U. Rehman, M. Shafiq, and H. Hamam, "Match-level fusion of finger-knuckle print and iris for human identity validation using neuro-fuzzy classifier," *Sensors*, vol. 22, no. 10, p. 3620, May 2022.

[252] B. Aldjia and B. Leila, "Sensor level fusion for multi-modal biometric identification using deep learning," in *Proc. Int. Conf. Recent Adv. Math. Informat. (ICRAMI)*, Sep. 2021, pp. 1–5.

[253] P. Drozdowski, F. Stockhardt, C. Rathgeb, D. Osorio-Roig, and C. Busch, "Feature fusion methods for indexing and retrieval of biometric data: Application to face recognition with privacy protection," *IEEE Access*, vol. 9, pp. 139361–139378, 2021.

[254] N. Poonguzhali and M. Ezhilarasan, "A framework for level-1 and level-2 feature level fusion," in *Proc. ieee Int. Conf. Syst., Comput., Autom. Netw.*, Jul. 2018, pp. 1–6.

[255] M. Ahsan, M. A. Based, J. Haider, and M. Kowalski, "An intelligent system for automatic fingerprint identification using feature fusion by Gabor filter and deep learning," *Comput. Electr. Eng.*, vol. 95, Oct. 2021, Art. no. 107387.

[256] M. Ghosh, A. Dey, and S. Kahali, "Type-2 fuzzy blended improved D-S evidence theory based decision fusion for face recognition," *Appl. Soft Comput.*, vol. 125, Aug. 2022, Art. no. 109179.

[257] M. Elhoseny, A. Elkhateb, A. Sahlol, and A. E. Hassanien, "Multimodal biometric personal identification and verification," in *Advances in Soft Computing and Machine Learning in Image Processing*. Cham, Switzerland: Springer, 2018, pp. 249–276.

[258] Y. Xin, L. Kong, Z. Liu, C. Wang, H. Zhu, M. Gao, C. Zhao, and X. Xu, "Multimodal feature-level fusion for biometrics identification system on IoMT platform," *IEEE Access*, vol. 6, pp. 21418–21426, 2018.

[259] E. Majeed Hameed, N. Abbood, and A. A. Alani, "Fuzzy logic decision fusion in a fingerprints based multimodal biometric system," *J. Eng. Appl. Sci.*, vol. 14, no. 3, pp. 920–926, Dec. 2019.

[260] G. Gavisiddappa, S. Mahadevappa, and C. Patil, "Multimodal biometric authentication system using modified ReliefF feature selection and multi support vector machine," *Int. J. Intell. Eng. Syst.*, vol. 13, no. 1, pp. 1–12, Feb. 2020.

[261] E. M. Cherrat, R. Alaoui, and H. Bouzahir, "A multimodal biometric identification system based on cascade advanced of fingerprint, fingervein and face images," *Indonesian J. Electr. Eng. Comput. Sci.*, vol. 17, no. 3, p. 1562, Mar. 2020.

[262] A. S. Mustafa, A. J. Abdulelah, and A. K. Ahmed, "Multimodal biometric system iris and fingerprint recognition based on fusion technique," *Int. J. Adv. Sci. Technol.*, vol. 29, no. 3, pp. 7423–7432, 2020.

[263] C. Kamlaskar and A. Abhyankar, "Iris-fingerprint multimodal biometric system based on optimal feature level fusion model," *AIMS Electron. Electr. Eng.*, vol. 5, no. 4, pp. 229–250, 2021.

[264] V. Rajasekar, B. Predić, M. Saracevic, M. Elhoseny, D. Karabasevic, D. Stanujkic, and P. Jayapaul, "Enhanced multimodal biometric recognition approach for smart cities based on an optimized fuzzy genetic algorithm," *Sci. Rep.*, vol. 12, no. 1, p. 622, Jan. 2022.

[265] M. Doostari, M. Safavipour, and H. Sadjedi, "A hybrid approach to multimodal biometric recognition based on feature-level fusion of face, two irises, and both thumbprints," *J. Med. Signals Sensors*, vol. 12, no. 3, p. 177, 2022.

[266] H. Ren, L. Sun, J. Guo, and C. Han, "A dataset and benchmark for multimodal biometric recognition based on fingerprint and finger vein," *IEEE Trans. Inf. Forensics Security*, vol. 17, pp. 2030–2043, 2022.

[267] I. Omara, A. Hagag, S. Chaib, G. Ma, F. E. Abd El-Samie, and E. Song, "A hybrid model combining learning distance metric and DAG support vector machine for multimodal biometric recognition," *IEEE Access*, vol. 9, pp. 4784–4796, 2021.

[268] M. Kazi, K. Kale, R. S. Mehsen, A. Mane, V. Humbe, Y. Rode, S. Dabhade, N. Bansod, A. Razvi, and P. Deshmukh, "Face, fingerprint, and signature based multimodal biometric system using score level and decision level fusion approaches," *IETE J. Res.*, pp. 1–20, Jun. 2023.

[269] L. Binh Tran and T. H. Le, "Multimodal personal verification using likelihood ratio for the match score fusion," *Comput. Intell. Neurosci.*, vol. 2017, pp. 1–9, Jan. 2017.

[270] W. K. Fatt, A. Kushsairy, H. Nasir, S. I. Safie, and N. Noor, "Fingerprint and face recognition: Application to multimodal biometrics system," *J. Telecommun., Electron. Comput. Eng.*, vol. 9, nos. 2–2, pp. 81–85, 2017.

[271] M. Shams, S. Sarhan, and A. S. Tolba, "Adaptive deep learning vector quantisation for multimodal authentication," *J. Inf. Hiding Multim. Signal Process.*, vol. 8, no. 3, pp. 702–722, 2017.

[272] U. Gawande, K. Hajari, and Y. Golhar, "Efficient multimodal biometric feature fusion using block sum and minutiae techniques," in *Proc. Int. Conf. Comput. Vis. Image Process*. Cham, Switzerland: Springer, 2017, pp. 215–225.

[273] I. Bhardwaj, N. D. Londhe, and S. K. Kopparapu, "A spoof resistant multibiometric system based on the physiological and behavioral characteristics of fingerprint," *Pattern Recognit.*, vol. 62, pp. 214–224, Feb. 2017.

[274] F. M. Algashaam, K. Nguyen, M. Alkanhal, V. Chandran, W. Boles, and J. Banks, "Multispectral periocular classification with multimodal compact multi-linear pooling," *IEEE Access*, vol. 5, pp. 14572–14578, 2017.

[275] M. Sultana, P. P. Paul, and M. L. Gavrilova, "Social behavioral information fusion in multimodal biometrics," *IEEE Trans. Syst., Man, Cybern., Syst.*, vol. 48, no. 12, pp. 2176–2187, Dec. 2018.

[276] E. B. Tarif, S. Wibowo, S. Wasimi, and A. Tareef, "A hybrid encryption/hiding method for secure transmission of biometric data in multimodal authentication system," *Multimedia Tools Appl.*, vol. 77, no. 2, pp. 2485–2503, Jan. 2018.

[277] N. Maheswari, A. Samraj, and M. Vijayakumar, "An efficient score level multimodal biometric system using ecg and fingerprint," *J. Telecommun., Electron. Comput. Eng.*, vol. 10, no. 4, pp. 31–36, 2018.

[278] A. Siddiqui, R. L. Telgad, S. A. Lothe, and P. D. Deshmukh, "Development of secure multimodal biometric system for person identification using feature level fusion: Fingerprint and iris," in *Proc. Int. Conf. Recent Trends Image Process. Pattern Recognit.* Cham, Switzerland: Springer, 2018, pp. 406–432.

[279] W. Kabir, M. O. Ahmad, and M. N. S. Swamy, "A multi-biometric system based on feature and score level fusions," *IEEE Access*, vol. 7, pp. 59437–59450, 2019.

[280] M. Hammad, Y. Liu, and K. Wang, "Multimodal biometric authentication systems using convolution neural network based on different level fusion of ECG and fingerprint," *IEEE Access*, vol. 7, pp. 26527–26542, 2019.

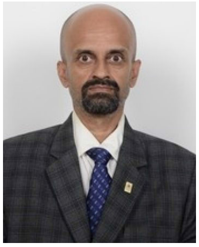
[281] S. Li, H. Zhang, Y. Shi, and J. Yang, "Novel local coding algorithm for finger multimodal feature description and recognition," *Sensors*, vol. 19, no. 9, p. 2213, May 2019.

[282] V. Sujitha and D. Chitra, "A novel technique for multi biometric cryptosystem using fuzzy vault," *J. Med. Syst.*, vol. 43, no. 5, pp. 1–9, May 2019.

[283] J. S. Arteaga-Falconi, H. Al Osman, and A. El Saddik, "ECG and fingerprint bimodal authentication," *Sustain. Cities Soc.*, vol. 40, pp. 274–283, Jul. 2018.
[284] W. Kim, J. M. Song, and K. R. Park, "Multimodal biometric recognition based on convolutional neural network by the fusion of finger-vein and finger shape using near-infrared (NIR) camera sensor," *Sensors*, vol. 18, no. 7, p. 2296, Jul. 2018.
[285] M. Shivakumar and C. M. Patil, "Face, finger print and iris biological characters using feature level fusion based multimodal biometric systems," *J. Comput. Theor. Nanoscience*, vol. 15, no. 9, pp. 2939–2948, Sep. 2018.
[286] M. Cheniti, N. Boukezzoula, and Z. Akhtar, "Symmetric sum-based biometric score fusion," *IET Biometrics*, vol. 7, no. 5, pp. 391–395, Sep. 2018.
[287] N. Damer, P. Terhörst, A. Braun, and A. Kuijper, "Fingerprint and iris multi-biometric data indexing and retrieval," in *Proc. 21st Int. Conf. Inf. Fusion (FUSION)*, Jul. 2018, pp. 2083–2090.
[288] M. Hammad and K. Wang, "Parallel score fusion of ECG and fingerprint for human authentication based on convolution neural network," *Comput. Secur.*, vol. 81, pp. 107–122, Mar. 2019.
[289] G. S. Walia, T. Singh, K. Singh, and N. Verma, "Robust multimodal biometric system based on optimal score level fusion model," *Expert Syst. Appl.*, vol. 116, pp. 364–376, Feb. 2019.
[290] G. Karthi and M. Ezhilarasan, "Multimodal biometrics authentication using multiple matching algorithm," in *Cognitive Informatics and Soft Computing*. Cham, Switzerland: Springer, 2019, pp. 361–369.
[291] H. Zhang, S. Li, Y. Shi, and J. Yang, "Graph fusion for finger multimodal biometrics," *IEEE Access*, vol. 7, pp. 28607–28615, 2019.
[292] V. P. K. Sistla, V. K. K. Kolli, and K. P. Valurouthu, "A novel adaptive two-phase multimodal biometric recognition system," *Int. Arab J. Inf. Technol.*, vol. 16, no. 5, pp. 936–946, 2019.
[293] M. Sajjad, S. Khan, T. Hussain, K. Muhammad, A. K. Sangaiah, A. Castiglione, C. Esposito, and S. W. Baik, "CNN-based anti-spoofing two-tier multi-factor authentication system," *Pattern Recognit. Lett.*, vol. 126, pp. 123–131, Sep. 2019.
[294] G. S. Walia, G. Jain, N. Bansal, and K. Singh, "Adaptive weighted graph approach to generate multimodal cancelable biometric templates," *IEEE Trans. Inf. Forensics Security*, vol. 15, pp. 1945–1958, 2020.
[295] E. M. Cherrat, R. Alaoui, and H. Bouzahir, "Convolutional neural networks approach for multimodal biometric identification system using the fusion of fingerprint, finger-vein and face images," *PeerJ Comput. Sci.*, vol. 6, p. e248, Jan. 2020.
[296] W. Abdul, O. Nafea, S. Ghouzali, and D. Tzovaras, "Combining watermarking and hyper-chaotic map to enhance the security of stored biometric templates," *Comput. J.*, vol. 63, no. 1, pp. 479–493, Jan. 2020.
[297] N. Tantubay, "Multimodal key-binding biocrypto-system using least-square polynomial curvefitting based new featurelevel fusion method," *Indian J. Comput. Sci. Eng.*, vol. 12, no. 1, pp. 10–20, Feb. 2021.
[298] T. Kumar, S. Bhushan, and S. Jangra, "An improved biometric fusion system of fingerprint and face using whale optimization," *Int. J. Adv. Comput. Sci. Appl.*, vol. 12, no. 1, 2021.
[299] M. Leghari, S. Memon, L. D. Dhomeja, A. H. Jalbani, and A. A. Chandio, "Deep feature fusion of fingerprint and online signature for multimodal biometrics," *Computers*, vol. 10, no. 2, p. 21, Feb. 2021.
[300] D. C. Atilla, R. S. H. Alzuhairi, and C. Aydin, "Producing secure multimodal biometric descriptors using artificial neural networks," *IET Biometrics*, vol. 10, no. 2, pp. 194–206, Mar. 2021.
[301] P. Tomar and R. C. Singh, "Cascade-based multimodal biometric recognition system with fingerprint and face," in *Proc. Macromolecular Symposia*. Hoboken, NJ, USA: Wiley, 2021, vol. 397, no. 1, p. 2000271.
[302] P. Shende and Y. Dandawate, "Convolutional neural network-based feature extraction using multimodal for high security application," *Evol. Intell.*, vol. 14, no. 2, pp. 1023–1033, Jun. 2021.
[303] N. V. Brindha and V. S. Meenakshi, "An RSSI-based Sybil attack detection system with continuous authentication using a novel lightweight multimodal biometrics," *Int. J. Intell. Unmanned Syst.*, vol. 10, no. 1, pp. 3–21, Jan. 2022.

U. SUMALATHA received the B.E. and M.Tech. degrees from Visvesvaraya Technological University, Belagavi. She is currently pursuing the Ph.D. degree with the Department of Information and Communication Technology, Manipal Institute of Technology, Karnataka, India. Her current research interests include deep learning, biometrics, multimodal biometric systems, biometric template security, privacy enhancing technologies, cryptographic protocols, and their applications.

K. KRISHNA PRAKASHA (Senior Member, IEEE) received the B.E. and M.Tech. degrees from Visvesvaraya Technological University, Belagavi, and the Ph.D. degree in network security from the Manipal Academy of Higher Education (MAHE), Manipal, India. He is currently working as an Associate Professor with the Department of Information and Communication Technology, Manipal Institute of Technology, MAHE. He has more than 30 publications in national and international conferences and journals. His current research interests include information security, network security, algorithms, real-time systems, and wireless sensor networks.



SRIKANTH PRABHU (Senior Member, IEEE) received the M.Sc., M.Tech., and Ph.D. degrees from IIT Kharagpur. He is currently working as a Professor with the Department of Computer Science and Engineering, Manipal Institute of Technology, MAHE, Manipal. He has more than 150 publications in national and international conferences and journals. His current research interests include pattern recognition, pattern classification, fuzzy logic, image processing, and parallel processing.

VINOD C. NAYAK received the M.B.B.S. degree from the Kasturba Medical College, Manipal, India, and the M.D. degree from the Kasturba Medical College, Manipal Academy of Higher Education (MAHE), Manipal. He is currently working as a Professor with the Department of Forensic Medicine, Kasturba Medical College, MAHE. His current research interests include public health, epidemiology, traffic medicine, suicidology, toxicology, medical ethics and laws about medicine, medical education, endocrinology, and forensic pathology.