

## TOPICAL REVIEW

# The Evolution of Biometric Authentication: A Deep Dive Into Multi-Modal Facial Recognition: A Review Case Study

MOHAMED ABDUL-AL<sup>1</sup>, GEORGE KUMI KYEREMEH<sup>1</sup>,

RAMI QAHWAJI<sup>1</sup>, (Senior Member, IEEE),

NAZAR T. ALI<sup>2</sup>, (Senior Member, IEEE),

AND RAED A. ABD-ALHAMEED<sup>1,3</sup>, (Senior Member, IEEE)

<sup>1</sup>Faculty of Engineering and Digital Technologies, University of Bradford, BD7 1DP Bradford, U.K.

<sup>2</sup>Department of Electrical Engineering and Computer Science, Khalifa University, Abu Dhabi, United Arab Emirates

<sup>3</sup>Al-Farqadein University College, Basrah 61004, Iraq

Corresponding authors: Mohamed Abdul-Al (m.abdul-al@bradford.ac.uk) and Raed A. Abd-Alhameed (r.a.a.abd@bradford.ac.uk)

This work was supported by European Union's Horizon-Marie Skłodowska-Curie Actions (MSCA)-RISE-2019-2023, Marie Skłodowska-Curie, Research, and Innovation Staff Exchange (RISE), titled: Secure and Wireless Multimodal Biometric Scanning Device for Passenger Verification Targeting Land and Sea Border Control.

**ABSTRACT** This survey provides an insightful overview of recent advancements in facial recognition technology, mainly focusing on multi-modal face recognition and its applications in security biometrics and identity verification. Central to this study is the Sejong Face Database, among other prominent datasets, which facilitates the exploration of intricate aspects of facial recognition, including hidden and heterogeneous face recognition, cross-modality analysis, and thermal-visible face recognition. This paper delves into the challenges of accurately identifying faces under various conditions and disguises, emphasising its significance in security systems and sensitive sectors like banking. The survey highlights novel contributions such as using Generative Adversarial Networks (GANs) to generate synthetic disguised faces, Convolutional Neural Networks (CNNs) for feature extractions, and Fuzzy Extractors to integrate biometric verification with cryptographic security. The paper also discusses the impact of quantum computing on encryption techniques and the potential of post-quantum cryptographic methods to secure biometric systems. This survey is a critical resource for understanding current research and prospects in biometric authentication, balancing technological advancements with ethical and privacy concerns in an increasingly digital society.

**INDEX TERMS** Facial recognition (FR), multi-modal face recognition, security biometrics, identity verification, Sejong face database, deep learning techniques, convolutional neural networks, cross-modality analysis, visible, infrared, thermal, thermal-visible face recognition, presentation attacks, facial disguises, biometric authentication, dataset analysis, algorithmic advancements, machine learning models.

## I. INTRODUCTION

Recent developments in facial recognition technology have driven multi-modal face recognition research using data types like visible light, infrared, and thermal imaging. This approach is especially relevant for security biometrics and

The associate editor coordinating the review of this manuscript and approving it for publication was Zhe Jin<sup>1</sup>.

identity verification. By leveraging the Sejong Face Database and other prominent datasets, researchers have explored complex aspects of facial recognition, including hidden and heterogeneous face recognition, cross-modality analysis, and thermal-visible face recognition. The Sejong Face Database, in particular, has played a significant role in enabling sophisticated approaches to facial recognition. Its comprehensive multi-modal disguise face dataset, encompassing images

captured in visible, infrared, thermal, and combined modalities, has been instrumental in addressing significant obstacles such as presentation attacks and facial disguises. This survey highlights the integration of advanced techniques like Generative Adversarial Networks (GANs) and Convolutional Neural Networks (CNNs) to enhance facial recognition systems. GANs generate synthetic datasets of disguised faces, improving system robustness against disguise attacks. CNNs are employed for deep feature extraction and classification, enhancing the accuracy of recognition systems.

Additionally, the survey explores the role of Fuzzy Extractors in combining biometric identification with cryptographic security, enabling the creation of reliable cryptographic keys from noisy biometric data and ensuring secure storage and transfer of biometric templates. The paper also considers the implications of quantum computing for standard encryption techniques. Quantum computing threatens traditional encryption methods, making them vulnerable to quantum attacks. Extensive research on post-quantum cryptography has been conducted to address this challenge. This includes exploring lattice-based and code-based methods to guarantee quantum-resistant security for biometric systems. The McEliece cryptosystem is identified as a promising option for safeguarding biometric systems in the quantum computing era. Ethical and privacy concerns are also a significant focus of this survey. The careful handling of privacy, consent, and data protection is crucial when storing, transmitting, and processing biometric data.

This paper underscores the importance of navigating these ethical and privacy considerations while ensuring robust security when developing and implementing biometric systems. This survey aims to compile a comprehensive inventory of the techniques and advancements used with the Sejong Face Database, focusing on the frontiers of facial recognition technology. By investigating new approaches and algorithms, this study demonstrates significant advancements in the accuracy and reliability of facial recognition systems. Using deep learning techniques, cross-modality discriminator networks, and unit-class loss represents substantial progress in developing safer and more efficient systems. Researchers' contributions significantly advance biometric authentication and its potential applications in our increasingly digitised society, navigating diverse face modifications and varying environmental conditions.

The paper is structured as follows: Section II provides an overview of the literature on utilising the SFD in various research publications. Section III presents a detailed compilation of databases used as authentication or verification systems in addition to the SFD. The methodology employed for the systematic review is explained in Section IV. The findings are examined and discussed in Section V. The conclusion and future directions are presented in Section VI.

## II. LITERATURE REVIEW

Facial recognition technology has seen substantial progress in recent years, particularly with the development of

multi-modal recognition systems that leverage diverse data types, such as visible, infrared (IR), and thermal imagery, as well as the significant advancements have been made in the field of facial recognition, particularly in the context of Disguised Face Recognition (DFR). This section categorises existing methods and provides detailed analyses of each to understand their contributions and limitations comprehensively.

Cheema et al. [1] proposed a Cross-Modality Discriminator Network (CMDN) to address challenges in high-frequency recognition (HFR) by effectively bridging the gap between visible and thermal modalities. Historically, HFR has relied on techniques such as image preprocessing, feature extraction, and standard subspace projection, which often encounter optimisation difficulties and performance issues. CMDN leverages relational learning and Unit-Class Loss to improve recognition accuracy across different modalities significantly. This method's key innovation is its ability to learn relational features between modalities rather than merely mapping them into a common subspace, enabling more flexible and accurate cross-modality face recognition. This advancement is crucial for surveillance and access control applications, where conditions can vary widely. CMDN provides a robust framework for effective face recognition in diverse security-focused domains by addressing the substantial disparities between modalities.

Ahmad et al. [2] focused on overcoming the limitations of facial disguises in recognition systems. Traditional facial recognition algorithms often struggle with disguises such as cosmetics, beards, and spectacles due to a lack of comprehensive training data. To tackle this, the researchers employed Generative Adversarial Networks (GANs) and Cycle-Consistency Loss to produce synthetic datasets of disguised faces. GANs are machine learning frameworks where two neural networks, a generator and a discriminator, compete to create synthetic data indistinguishable from actual data. Cycle consistency loss ensures that an image can be translated to another domain without losing essential information, thereby preserving the original content while applying new styles or features. This innovative approach enhances the resilience of facial recognition algorithms against disguises, improving their robustness and accuracy by providing high-quality synthetic training data.

Cheema and Moon [3] introduced the Deep Neighbourhood Difference Relational (DNDR) network coupled with Joint Discrimination Loss (JDL) to improve performance in hidden Heterogeneous Face Recognition (HFR). Prior approaches either focused on the synthesis of images or domain-invariant feature extraction, which often faced challenges such as the need for extensive training data, alignment issues, and difficulty maintaining distinguishing details in synthesised images. The DNDR network addresses these problems using deep feature relations instead of extensive preprocessing or domain gap reduction methods. This method significantly enhances identity representation and

cross-modality matching by incorporating JDL, further refining identity representation and improving cross-modality matching. The DNDR network's approach has shown superior performance to existing methods, particularly in dealing with hidden HFR difficulties, such as masks and varied imaging conditions.

Kowalski et al. [4] proposed an innovative approach for thermal-visible face verification, instrumental in challenging low-light or on-the-move situations. Previous research predominantly focused on face recognition using visible spectrum data, which, while accurate, struggled in low-visibility settings. The thermal-visible strategy bridges this gap by utilising thermal imagery that is less affected by lighting conditions. The triple triplet approach introduced by Kowalski et al. [4] incorporates several Convolutional Neural Networks (CNNs) to handle the different properties of thermal and visible spectra. This method significantly improves recognition accuracy and reliability, integrating data from visible and thermal spectra to enhance the resilience of the recognition process. The innovative triple triplet configuration allows the system to differentiate between genuine users and impostors more effectively, establishing a new standard for future research in this field.

Abdullah et al. [5] presented a method based on GANs, focusing on employing CycleGAN to produce thermal pictures from visible light pictures. The significance of this strategy lies in the restricted availability of thermal image data for training facial recognition algorithms, compared to the abundance of visible light pictures. The study showcases the efficacy of CycleGAN in acquiring stylistic attributes from thermal pictures and subsequently transferring them to visible light pictures, producing authentic thermal renditions. The findings from the conducted experiment, utilising the Sejong Face Dataset, demonstrate a remarkable similarity between the produced thermal pictures and authentic thermal images. This assertion is supported by quantitative measures such as the Fréchet Inception Distance (FID) and Kernel Inception Distance (KID). The study introduces a potentially fruitful avenue for improving the efficacy of thermal face recognition systems, focusing on its relevance in security and surveillance domains where thermal imaging plays a crucial role.

Ahmad et al. [6] explored the generation of synthetic disguised faces using GANs to improve system robustness against disguise attacks. This one-shot generation approach efficiently enhances facial recognition systems by adding diverse disguised faces to the training dataset, significantly improving recognition accuracy under various disguise conditions. The method leverages patchwise contrastive loss and cycle-consistency loss to generate high-quality disguised faces from a single sample per individual. This innovative approach reduces the data requirements for training robust models, making generating various disguised faces from a limited number of original images feasible. The study demonstrated that this method could improve model accuracy by

20-25 percent, depending on the disguise add-on used, thus contributing significantly to facial recognition.

Alkadi et al. [7] developed a multi-modal facial recognition system for (Automatic Teller Machines) ATM biometric authentication that integrates visible, IR, and thermal images. This system addresses presentation attacks and facial disguises by combining multiple imaging modalities, enhancing accuracy and security. The study investigated several machine learning algorithms, ultimately selecting ResNet-50 for its efficiency and effectiveness. Using the Sejong multi-modal disguise face dataset for training enabled the system to identify users with or without facial enhancements reliably. The system demonstrated high accuracy in real-time applications, even with standard facial accessories like sunglasses, face masks, and ethnic head covers. However, challenges were noted in identifying individuals who had undergone significant changes in appearance, such as wearing a Hijab after being photographed without one, highlighting areas for further improvement.

The advancements in facial recognition technology, mainly through multi-modal approaches, have significantly improved system robustness and accuracy. These methods, utilising diverse datasets and innovative algorithms, address critical challenges such as disguises and environmental variability. Continued research and development, supported by comprehensive datasets like the Sejong Face Database, are essential for further enhancing the reliability and applicability of facial recognition systems in various security and biometric applications.

Padmashree and Kotegar [8] introduced a novel approach that focuses on the skin regions of the face, which are less likely to be covered by disguises. Their method utilises a region-based marker-controlled watershed algorithm for skin segmentation and employs a CNN for feature extraction, followed by deep learning-based classification. This approach addresses several critical challenges in DFR, such as changes in facial features due to disguises, lack of training data, and variability in disguises. The method reduces noise and irrelevant information by concentrating on the skin region, thus improving recognition accuracy. The study also performed an ablation analysis to investigate the impact of various factors on the model's performance, such as image size and kernel filter size. This innovative approach demonstrated superior performance to traditional methods, significantly contributing to disguised face recognition.

Fuzzy Extractors have become crucial in combining biometric identification with cryptographic security. They allow for creating reliable cryptographic keys from biometric data, which is inherently noisy and subject to change [9], [10]. Fuzzy Extractors enable the secure production and renewal of cryptographic keys by addressing the variability in biometric data. This allows for the safe storage and transfer of biometric templates [11], [12].

Quantum computing has threatened standard encryption techniques, making them susceptible to quantum

attacks [13], [14]. Research has investigated post-quantum cryptography, including lattice-based and code-based cryptography, as a potential method to provide quantum-resistant security in biometric systems [15]. The McEliece cryptosystem, a cryptographic method based on codes, is well-known for its strong resistance against quantum assaults. This makes it a promising option for safeguarding biometric systems in the upcoming era of quantum computing [16], [17].

The combination of biometrics and cryptography also reveals numerous ethical and privacy concerns. The careful handling of privacy, permission, and data protection is crucial when dealing with storing, transmitting, and processing biometric data, especially regarding international data protection laws and ethical concerns [18], [19]. Therefore, the creation and execution of biometric systems must carefully navigate the intricate terrain of guaranteeing strong security while protecting ethical and privacy concerns.

Research and development in biometric authentication and cryptographic security are exploring new algorithms [20], [21], processes, and paradigms. This ongoing research is not just crucial; it is inspiring, as it has the potential to create biometric systems that are resilient, secure, and ethically sound. As professionals in the field, your role is integral to this process. The field of novel Fuzzy Extractors, especially those based on post-quantum cryptographic schemes, is gaining increasing importance. This research has the potential to lead to the development of biometric systems that are secure, user-friendly, and resistant to quantum threats, with your contributions being of utmost importance.

Several authors have tackled creating efficient Fuzzy Extractors for sources with big alphabets and non-hamming metrics.

Parente and van de Graaf suggested using LDLC (Low-Density Lattice Code) to develop Fuzzy Extractors designed for continuous sources [22]. Their approach naturally presupposes the presence of Gaussian noise and does not provide a specific implementation of the proposed system.

Jana and her colleagues introduced a concept called “Neural Fuzzy Extractors”, in which they developed a neural network for Fuzzy Extractors using LDLC as a foundation [23]. However, their research only presented findings from trials conducted on fingerprint data. Additionally, the security analysis is based on an upper limit rather than the actual level of security it provides.

Buhan et al. examined Fuzzy Extractors applied to continuous sources in their study. They demonstrated an upper limit on the length of the extracted string and the source’s error rate, as discussed in [24].

Verbitskiy et al. conducted a study on the impact of quantisation techniques on Fuzzy Extractors for continuous sources, as documented in their publication [25]. Both pieces need to improve their analysis of complex dimensions and tangible structures.

Zheng et al. utilised the integer lattice,  $q^Z^n$ , to develop a “fuzzy commitment” described in [26]. However, their

method relies on simulated Iris plant data, which only applies to our specific use case.

Li et al. introduced a Fuzzy Extractor that operates in the maximum norm [11]. Their experiment is devoid of any empirical biometric data and lacks rigorous security analysis.

There has been a renewed interest in Deep Learning models in recent years, leading to significant advancements in representation learning for biometric identities using deep neural networks. Tang et al. introduced Finger-Net, a comprehensive deep network to extract fingerprint minutiae [27]. The authors suggest a novel approach to constructing a deep convolutional network by integrating domain expertise with the powerful representation capabilities of deep learning. Regarding the estimate of orientation, segmentation, enhancement, and minutiae extraction, various conventional methods that demonstrated good performance on rolled/slap fingerprints have been converted into a convolutional approach and combined into a unified plain network. Darlow and Rosman [28] presented the concept of minutiae extraction as a machine-learning challenge. They introduced a deep neural network called MENet (Minutiae Extraction Network) to acquire a data-based representation of minutiae points. Menotti et al. [29] employed deep representations to detect spoofing in Iris, Face, and Fingerprint biometric systems. Similarly, Engelsma et al. [30] acquired knowledge about fingerprint representations. Jeon and Rhee [31] suggested three modifications to the VGGNet architecture for fingerprint categorisation.

A similar idea was put forward by Hammad et al. [32], who wanted to create a safe multimodal fingerprint system using a CNN and a QG-MSVM based on several different fusion levels. They created two authentication systems using two distinct fusion algorithms: one based on feature-level fusion and the other on decision-level fusion. A CNN extracts features from each modality individually. During this stage, they chose two layers from the CNN that had the highest level of accuracy. Each layer was considered as an individual feature descriptor. Subsequently, they merged the components mentioned earlier, utilising the suggested internal fusion technique to produce the biometric templates. Subsequently, they implemented one of the cancellable biometric approaches to safeguard these templates and enhance the security of the proposed system.

Similarly, Nayak and Narayan [33] studied multimodal biometric face and fingerprint identification. They utilised neural networks based on adaptive principal component analysis and multilayer perceptrons. Stojanovic et al. [34] introduced a new approach for separating latent overlapping fingerprints using neural networks. Nogueira et al. [35] employed CNNs to detect the authenticity of fingerprints.

Page et al. [36] utilised neural networks to detect QRS complex segments of Electrocardiogram (ECG) data and subsequently conducted user verification on these sections. It is important to note that Mai et al. [37] confidently applied multilayer perceptron and radial basis function neural networks

to perform biometric verification using ECG data. Salloum and Kuo [38] suggested employing different types of recurrent neural network (RNN) structures, including vanilla, long short-term memory (LSTM), gated recurrent unit (GRU), uni-directional, and bidirectional networks, to identify/classify and authenticating individuals based on ECG data. Labati et al. [39] introduce Deep-ECG, a CNN-based method for identifying, verifying, and periodically re-authenticating ECG signals. Deep-ECG utilises a deep CNN to extract significant characteristics from one or more leads. It then compares biometric templates by calculating efficient and rapid distance functions for verification or identification. El Khiyari and Wechsler [40] demonstrated the innovative application and efficacy of deep learning CNN structures for automatically extracting features instead of relying on manually designed features to achieve reliable face recognition over different time intervals. The study demonstrates that CNNs utilising VGG-Face deep networks provide extremely distinctive and compatible characteristics that are resistant to changes caused by ageing, even when dealing with a combination of different biometric datasets.

Fuzzy Extractors were initially developed in [10] as a secure method for handling user biometrics. User biometrics typically exhibit tiny variations between each entry but possess common primary traits. The concept was to store digests obtained by cryptographic hash functions instead of representative entries, which would be used for direct comparison with new entries during authentication requests. This approach effectively prevents biometric falsification.

The concept was promptly applied to different forms of biometric identification methods, such as those utilising fingerprints [41], [42], [43], [44], [45], iris scans [46], [47], [48], facial recognition [49], or gait analysis [50], [51].

Recently, Fuzzy Extractors have been at the forefront of advanced and specialised secure authentication systems. For instance, the system described in [52] is specifically designed for wireless sensor networks, such as body-area networks. Furthermore, they have been integrated into the systems discussed in [53] and [54], which handle the outputs of Physically Unclonable Functions (PUFs). These recent advancements in using Fuzzy Extractors are shaping the future of biometric security.

Pirbhulal et al. [55] developed a security mechanism that relies on the heartbeat sequence. They derived binary sequences from the heart rate by analysing the values of the time intervals between consecutive heartbeats. In 8 seconds, they generated a 128-bit binary sequence using ECG records obtained from the MIT-BIH Arrhythmia database. As a result, they decreased the time required to generate random binary sequences. The primary issue with using heartbeats for security is their inherent inconsistency over time. Kumari and Anjali [56] developed a dual encryption system to ensure the security of communication between nodes and the base station. Instead of using complicated mathematical procedures, essential mathematical functions are used to encrypt the data.

Due to this factor, the method requires less time than other systems that use intricate mathematical calculations. This is also seen as a drawback since it is quite simple for attackers to duplicate the key.

Dao et al. [57] introduced a multi-biometric encryption essential technique for encrypting biological data and securely storing it in a fuzzy vault. The fingerprint data is used as the input for encryption, whereby the minutia of the fingerprint is retrieved, and a 16-bit encoding algorithm is applied to the input data. In addition to encoding, the polynomial CRC building procedure is used to determine the polynomial value of the data. The encoded and produced polynomial values are merged to produce the polynomial projection value. Using both data, the chaff point creation algorithm creates chaff points or unreal points. The collection that contains both the chaff points and genuine points is known as the hazy vault. Chelani and Bagde [58] devised an Ad hoc On-demand Routing Protocol (AODV) approach, namely the IBDS (Improved Bait Detection Scheme), for detecting malicious nodes and preventing black hole attacks in MANETs (mobile ad hoc networks). This method is meant to include both reactive and proactive defence strategies. This technique may provide an enhanced packet-delivery ratio of around 18% and decrease energy usage to 8%.

### III. DATABASES

This section provides an overview of the datasets employed in conjunction with the SFD throughout this investigation. The SFD [59] is an extensive database created to aid in developing disguised FR systems suitable for use in commercial applications like security checkpoints, where such systems are necessary. The SFD has pictures of 100 individuals split into two groups. Thirty participants (16 men and 14 women) were included in Subset-A, and they all contributed a single picture across all modalities. Seventy participants (44 men and 26 women) contributed five or more pictures across all modalities in Subset-B. Subset-A has 1,500 pictures, whereas Subset-B contains 23,100. The visible (VIS) ( $4032 \times 3024$ ), visible plus infrared (VIS-IR) ( $1680 \times 1050$ ), infrared (IR) ( $1680 \times 1050$ ), and thermal (Th) ( $768 \times 756$ ) spectra are all used to record each face picture. Eight different facial accessories (such as a false beard, wig, spectacles, etc.) and seven different permutations of these accessories are included in the database to produce a wide range of disguised face pictures, as demonstrated in Figure 1. The pictures were retaken two weeks apart to account for variations, including facial hair development. Gender-specific extensions are supported, and a wide range of races and sexes are represented in the database. The subject ID, accessory type, and imaging mode are clearly labelled on every picture. In [59], this organised naming practice aids research into face detection and identification systems, especially in cases of disguise and occlusion. To showcase the database's complexity and ability to contribute to developing algorithms for disguised face identification, we conducted baseline tests involving face

detection, classification, and verification. The trials highlighted the necessity of upgrading current face identification algorithms to enhance resistance against facial add-ons.

There are 215 participants included in the USTC-NVIE collection of face expressions, which contains VIS-Th picture pairings [60], [61]. The database is then split in half, with one half including pictures of the peak of facial expressions (the “posed” database) and the other half containing images of the beginning and end of facial expressions (the “spontaneous” database). The pictures are taken with three different kinds of lighting: left, right, and front. In [1], VIS-Th HFR uses the Expression Recognition Database, as represented in Figure 2. Among the 215 participants, 126 were determined to have useable data (sufficient pictures in both modalities). In order to maximise the total quantity of training and test data, researchers employ both sub-datasets. A total of 16002 picture pairings (VIS and Th) were used in the training, with 100 participants contributing data. The sample size for this test was 4162 picture pairings from 26 different people.

The TUFTS [62] database has data that falls into many categories, including two-dimensional VIS, Th, IR, 3D, 3D LYTRO, sketch, and video. The database comprises a collection of pictures exhibiting variances, such as facial expressions and the presence of sunglasses. In order to mitigate the added complexity of position variations, only frontal photos exhibiting differences in facial expression and the presence of spectacles were utilised for both the training and testing phases and, in [1], employed thermal and visual image corpus for HFR as illustrated in Figure 3. The training entailed utilising a dataset containing 4812 pairs of images, including visual and thermal images obtained from 74 subjects. In [1], the researchers used a total of 2472 picture pairings from 38 participants were utilised for testing purposes.

UND-X1 [62], [63] has 82 participants with different lighting, facial expressions, and time-lapses in LWIR and visible light picture pairings. Images from 50 of the 82 participants were utilised for the training set, as demonstrated in Figure 4. Forty different picture pairs represented each person. The training was conducted with 50 individuals and 10002 image pairings. A total of 32 participants and 12802 picture pairings were used for the analysis.

There are 725 participants represented by pairs of VIS and IR images in the CASIA NIR-VIS 2.0 [64] database. VIS and IR pictures of the participant have anything from 1-22 and 5-50 frames, respectively. The database offers a dual perspective on the testing procedures. The first viewpoint is utilised for instruction, while the second is tested. Using VIS pictures as a gallery and NIR pictures as the probe, researchers may model real-world scenarios [1]. The gallery collection has merely a single VIS image of each participant. View-2’s standard testing technique compares our results to those of other studies, as illustrated in Figure 5.

The FaceScrub dataset, as described in [65], comprises a comprehensive assortment of uncontrolled viewable

photographs, including 530 individuals. Approximately 200 pictures were acquired for every participant, resulting in 106,863 pictures. The dataset exhibits an equal distribution of individuals, with an equal number of men and women participants, as shown in Figure 6. The variation in the characteristics of pictures is observed throughout the whole collection.

The CUHK Face Sketch (CUFS) database [66] has a total of 188 facial pictures sourced from the student database of the Chinese University of Hong Kong, 123 facial pictures taken from the AR database [67], and 295 facial pictures taken from the XM2VTS [68] database. An artist has created a drawing for each face, utilising a picture captured in a frontal stance, including a neutral expression, and taken under standard lighting conditions, as illustrated in Figure 7.

The dataset I<sup>2</sup>BVSD [69], [70] comprises frontal position pictures of individuals with neutral facial expressions recorded under consistent lighting conditions. The database encompasses a range of disguise variants, including but not limited to artificial facial hair, headwear consisting of hats, wigs, masks, and eyewear, such as spectacles, as represented in Figure 8. The database has a sample size of 75 individuals of South Asian descent, consisting of 60 men and 15 women. The database contains five discrete categories of disguises, specifically variants in hairstyles, beards, moustaches, spectacles, hats, and masks. An alternative approach involves the utilisation of many disguises in combination.

Nevertheless, the database lacks disguise labels, posing challenges to advancing disguised facial recognition models. In [2], the dataset included 681 photos for each modality. It is important to note that each modality includes at least one frontal face image and a varying number of frontal concealed images per person, ranging from five to nine.

The BRSU Spoof Database [71], [72] is a comprehensive database encompassing many spectral bands, including VIS-IR modalities, with picture acquisitions conducted at 935, 1060, 1200, and 1550 nm wavelengths. The database exhibits several complexities that provide challenges, including but not limited to differences in expression, composition, three-dimensional masks, artificial beards, eyewear, counterfeit noses, and presentation-based attacks, as demonstrated in Figure 9. Nevertheless, the database has a limited selection of five themes, each including several additional components ranging from nine to thirty. The primary focus of the BRSU Spoof DB is in the realm of multispectral analysis.

There are natural and disguised pictures of the faces of 54 men in the Spectral Disguise Face Database [73]. The database’s images range from 530 to 1000 nanometres, encompassing visible (VIS) and near-infrared (NIR) spectrums. This database is then split in half again, with the first half containing only authentic, unmasked pictures and the second half including authentic and disguised versions of the same image. Unfortunately, only two beard lengths are available using this disguise: standard and extended, as shown in Figure 10. The genuine sample consists of 22 individuals with

beards and the remainder with moustaches. This database's lack of diversity in disguises makes it impossible to train a universal disguise detection algorithm effectively.

The CASIA SURF collection is an extensive collection of different types of face presentation attacks [250]. There are 1000 Chinese people in it in three modes: Red-Green-Blue (RGB), Depth, and IR. The database has six types of attacks, but most are done by individuals holding a picture of their face written on paper in six different shapes, as shown in Figure 11. This information cannot be used to train a public FR app because these threats do not work in public places like airport security.

The IIIT-D Sketch database [74] includes viewable sketches, semi-forensic sketches, and forensic sketches that may be examined by the naked eye, as illustrated in Figure 12. The suggested technique [3] was evaluated using the IIIT-D viewed sketch and IIIT-D Semiforensic sketch data subsets. Two hundred and thirty-eight picture pairings make up the IIIT-D seen sketch subset; the drawings for 67, 99, and 72 pictures come from the FG-Net ageing database [75], the Labelled Faces in the Wild (LFW) database [76], and the IIIT-D students and staff database, correspondingly. The IIIT-D Visible-drawing subset includes 140 pairs of pictures; each pair represents a drawing created from the memory of a digital picture seen just once.

The AT&T (ORL) database, also known as the AT&T Laboratories Cambridge face database or the ORL (Olivetti Research Laboratory) face database, as illustrated in Figure 13, is a highly regarded compilation of facial photographs widely used in computer vision and research on facial recognition [77]. The dataset was established throughout the 1990s and consists of 400 grayscale photos featuring 40 unique persons. Each participant has contributed ten different images. The photos in question include various facial expressions, angles, and lighting situations, making them suitable for testing and refining facial recognition systems. The database comprises individuals of both genders, with the photos standardised to a resolution of  $92 \times 112$  pixels. The AT&T (ORL) database has emerged as a crucial asset for academics and developers, facilitating progress in biometric identification, security systems, and human-computer interface technologies.

The Yale Face Database B is an extensive compilation of facial photographs primarily used for computer vision research in face identification and facial expression analysis [78]. The database consists of 5,760 photographs captured under a single light source. These images belong to 10 persons, each with 576 photos. Every person was captured in 64 distinct lighting circumstances, including diverse angles of light sources that spanned azimuth and height changes. The photographs were taken with facial emotions, such as standard, happy, sad, shocked, asleep, and winking. This dataset is valuable for assessing the effectiveness of face recognition algorithms in different lighting and expressive situations. The meticulous management of environmental conditions and

precise documentation of lighting angles make the Yale Face Database B an invaluable asset for developing FR algorithms, as represented in Figure 14.

The FERET Database, also known as the Face Recognition Technology Database, is a thorough compilation of face photos primarily utilised to enhance the progress and assessment of facial recognition algorithms [79]. The U.S. Department of Defense established the database in the 1990s. It contains many face photos from over a thousand individuals in different settings to replicate real-life situations. This includes differences in illumination, facial expression, body position, and photographs taken at different points in time to consider the effects of ageing. The FERET Database has played a crucial role in evaluating face recognition systems by offering a consistent dataset for researchers to assess the effectiveness and precision of their algorithms. This has resulted in biometric technology and security application advancements, as shown in Figure 15.

The CMU PIE (Pose, Illumination, and Expression) Database is an extensive compilation of face photographs specially tailored for researching facial identification and analysis [80]. The database, curated by Carnegie Mellon University, has more than 41,000 photographs of 68 people collected in diverse situations. The dataset includes 13 unique positions, 43 various lighting conditions, and four varied facial expressions, making it a valuable tool for investigating the impact of these variables on face recognition systems. The wide range of options allows researchers to create and evaluate robust face recognition algorithms that can operate accurately in several real-world situations. The CMU PIE Database has played a crucial role in advancing computer vision, namely in creating algorithms that can effectively deal with the challenges posed by changes in stance, lighting, and facial expressions, as demonstrated in Figure 16.

The UMIST Face Database is an extensive compilation of black-and-white facial photos used mainly for research in computer vision, facial recognition, and machine learning [81]. The database, created by UMIST, consists of 564 photos of 20 individuals showcasing various ethnic origins and genders. The collection has many photographs of each participant, captured from different perspectives, offering a diverse range of facial emotions and positions. The photos, including a resolution of  $220 \times 220$  pixels, enable rigorous testing and advancement of algorithms designed to detect and analyse human faces in various situations and perspectives. This database plays a crucial role in developing technology related to biometric authentication, surveillance systems, and human-computer interaction, as represented in Figure 17.

The AR Face Database, as illustrated in Figure 18, is an extensive compilation of more than 4,000 photos in colour showcasing the facial features of 126 people, consisting of 70 males and 56 females [67]. This database was created by capturing individuals in two separate sessions, with a two-week gap between them. Every participant is shown

in 13 different settings during every session, which include variations in facial expressions, lighting situations, and occlusions. The variants include a range of emotions, including neutrality, happiness, wrath, intense vocalisation, and diverse face coverings such as sunglasses and scarves. The main objective of the AR Face Database is to facilitate research in face recognition by offering a comprehensive collection of varied and demanding photos for evaluating algorithms in actual scenarios. The database is extensively used in academic and commercial environments to augment the precision and resilience of face recognition systems.

The FG-NET Aging Database is an extensive and well-employed resource in computer vision and age progression research [82]. The dataset comprises 1,002 precisely curated photos of 82 participants, comprehensively representing the natural ageing process over time. The photos of each person cover a wide range of ages, from infancy to senior years, making it an excellent dataset for investigating patterns of face ageing. The photos are labelled with accurate age annotations and essential facial landmarks, which greatly assist in creating and testing advanced algorithms for age estimation, face recognition, and age progression technologies, as shown in Figure 19. The database's comprehensive and intricate characteristics make it indispensable for researchers aiming to improve the precision and efficiency of age-related computer vision applications.

The Mobio Database is an extensive and well-organised compilation of biometric data, specifically created to facilitate study and advancement in mobile and biometric identification technology [83]. The dataset comprises a comprehensive collection of multi-modal biometric samples, including facial photos and voice recordings. These samples were gathered from various people, considering different environmental circumstances, as demonstrated in Figure 20. The database is designed to simplify the assessment of algorithms for activities such as verifying identification, authenticating biometrics, and enhancing security systems. The Mobio Database collects data from controlled and uncontrolled environments, prioritising its practical usefulness. This approach guarantees the database's strength and dependability in real-world applications. This resource's detailed annotations and high-quality standards make it indispensable for academics, developers, and engineers at the forefront of biometric technology.

The Labelled Faces in the Wild (LFW) database is a renowned benchmark dataset extensively used in computer vision and machine learning, specifically for creating and assessing face recognition systems [76]. The dataset consists of more than 13,000 facial photos obtained from the internet. Each image is accompanied by a corresponding label indicating the name of the individual shown. The dataset has 5,749 distinct people's photos exhibiting unique lighting, position, and expression situations, as illustrated in Figure 21. This makes it a demanding and varied dataset suitable for training and testing strong models. The LFW database has promoted

face verification and identification task research. It has served as a benchmark for evaluating and validating new algorithms and approaches in this field.

The following offers a comprehensive overview of the datasets utilised in facial recognition research, excluding the SFD. These datasets encompass various modalities, scenarios, and challenges, making them valuable for developing and evaluating facial recognition algorithms. Table 1 summarises these additional databases' essential features, descriptions, and uses, highlighting their significance in advancing biometric authentication and facial recognition technologies.

#### IV. ADOPTED RESEARCH METHODOLOGIES

This section provides a comprehensive overview of the many methodologies utilised and included in the investigations mentioned above. The research approach employed in the study entails the construction of a comprehensive CMDN for HFR [1]. The CMDN uses a Deep Relational Discriminator (DRD) module to learn about the connections between pictures from different domains. Additionally, the network employs a Unit-Class Loss to optimise the network. This loss function is specifically developed to ensure stability and accuracy, surpassing other metric-learning loss functions.

The initial weights for the backbone network of the CMDN are obtained from VGGFace2. Subsequently, fine-tuning is performed on the IRIS face database to enable visual and thermal face categorisation. The DRD module is then included in the backbone network for HFR training. The neural network obtains facial embedding vectors and conducts HFR classification, resulting in a fusion of the embedding vectors and probabilities associated with the classification. The network's performance is evaluated on various datasets, including TUFTS, UND-X1, USTC-NVIE, CASIA NIR-VIS, and the Sejong Face Database.

The technique significantly emphasises leveraging deep feature relations to facilitate cross-domain face matching and the derivation of modality-independent embedding vectors. Using the Unit-Class Loss function plays a crucial role in augmenting the feature learning process by taking into account the characteristics of individual samples and the overall distributions of classes. The efficacy of the network is evidenced by notable enhancements over prevailing state-of-the-art techniques across diverse datasets.

The study [3] presents a unique methodology for addressing the challenges associated with disguised HFR, surpassing existing techniques' constraints. The approach has three essential elements: the DNDR Network, the JDL, and a training plan that involves many stages. The DNDR network has been specifically developed to possess modality independence, allowing it to process and analyse data from various modalities effectively. Its training process involves exposure to both same-modality and cross-modality datasets. The primary objective of this study is to investigate the correlation between deep characteristics of cross-modality pictures while disregarding distinct features on real-to-disguise face



areas throughout the training process. The LJD algorithm aims to enhance the network's ability to extract picture embeddings that effectively capture identification information, hence maximising the performance of cross-modality matching. Implementing a multi-stage training scheme facilitates the acceleration of training processes and enhances the network's overall performance. The technology has enhanced performance compared to existing methods on several HFR databases.

The technique employed in [4] encompasses a multi-faceted approach that integrates many stages, including data acquisition, algorithm choice, and experimental framework. The study starts with database preparation and annotation, whereby datasets are categorised according to several parameters, such as the existence of spectacles, due to their potential influence on thermal-visible face identification. Two distinct face detection algorithms were devised for thermal and visual photos. In order to perform feature extraction, a series of CNNs were trained on classification tasks. This training used a combined dataset of visible and thermal pictures. The CNNs were first pre-trained using the ImageNet database.

The study subsequently examined different methodologies, encompassing Siamese-based, Triplet-based, and Verification by Identification procedures. One notable innovation is the triple triplet technique, wherein three distinct CNNs are employed inside each branch of a triplet architecture [4]. This approach facilitates the computation of feature vectors, with the ultimate objective of enhancing the system's ability to differentiate between impostors and genuine individuals, leading to enhanced performance. The training procedure encompassed the use of transfer learning techniques with cutting-edge CNNs. This approach used the FaceScrub database as a starting point, followed by integrating the joint dataset, including D4FLY and IOE\_WAT datasets.

The efficacy of the established methodology was assessed by testing studies conducted on participants both with and without glasses, utilising diverse datasets. The technique employed in this study is distinguished by its complete approach to managing diverse datasets and its emphasis on developing a resilient and efficient thermal-visible face recognition system.

The method used in [2] comprises several essential parts. First, it suggests using a GAN to make fake faces that look real. This is done with cycle-consistency loss, a method that keeps the unique features of the original faces while adding fake hair, makeup, and glasses to make them look different. The SFD is used as the seed database at the start of the process. Many disguise add-ons and subject names are used to add more face images to the fake database.

It also adds a method for automatic screening. This programme is meant to sort through the fake images made and eliminate the ones that are not very good. This way, only the best, most realistic images are used. This filtering is vital to keep the data used for face recognition training and trials safe.

An essential part of the study is doing many experiments to see how well the fake faces work. These tests aim to see how well fake data works compared to actual data regarding training face recognition systems. The results show that facial recognition works better when taught on the suggested fake database. This shows that the method for making high-quality, fake facial images is proper.

New infrared and thermal face pictures are generated using GANs [5]. CycleGAN, an unpaired image-to-image translation model, translates style characteristics from a data distribution to target pictures. Because thermal face recognition training data was scarce, this method was chosen. They used 400 pairs of visual and thermal photos of 70 patients from a subset of the SFD for validation. Subject IDs were used to separate training and test data. CycleGAN was then used to learn from visible pictures and create thermal versions. Nvidia GTX 3080s and Pytorch used Fréchet Inception Distance (FID) and Kernel Inception Distance (KID) measurements to test the approach. The findings showed that the pictures produced closely mirrored the data and were high quality and natural. Method efficacy was demonstrated by FID and KID scores.

The technology employed in [6] produces synthetic disguised facial pictures using a single sample photo per person. This method was developed to fortify face recognition programmes against deception techniques. The approach is based on Contrastive Unpaired Training (CUT) and a cycle consistency loss-based method for generating masked faces. CUT streamlines training by requiring a single picture and network (a generator and a discriminator). This research, however, combines CUT's patchwise contrastive loss with CycleGAN's cycle-consistency loss, employing a dual-generator and a dual-discriminator setup to overcome its shortcomings. StyleGAN2 is then used to fine-tune the combination for single-image translation from unmasked to concealed facial features. Most of the pictures and the various disguise enhancements used in the training process come from the SFD's more significant subset B. The process's ultimate goal is to generate unique face databases or incorporate this technology into existing face recognition training pipelines to boost recognition precision while wearing disguises.

The approach [7] is to provide ATMs with a multi-modal biometric authentication system based on machine learning. This system uses multi-modal imaging (VIS, IR, and thermal imaging) to record photos of a user's face and is then taught to recognise that face even after it has been altered by factors such as hair and facial accessories.

This variety aids in thwarting threats like false identity theft and presentation assaults. The Sejong multi-modal disguised face dataset has photos in visible, IR, thermal, and a mix of IR and visible spectra, as well as some other enhancements. After initial processing, the data is split into training, testing, and validation. In addition, we use ML algorithms for facial recognition, such as VGG-16, InceptionV3, and ResNet-50.

TABLE 1. Overview of facial recognition databases.



References	Name of the Database	Description	Use Case	Sample Images
[59]	Sejong Face Database	The Sejong Face Database is a comprehensive disguised face database containing images of 100 subjects with various facial add-ons captured in visible, infrared, thermal, and visible-plus-infrared modalities. It aims to aid research in disguised face recognition.	The Sejong Face Database is primarily used for developing and evaluating facial recognition systems, particularly those for recognising faces under disguise in security checkpoints, border control, public surveillance, and access control systems. Its diverse modalities and disguises enable robust testing and improvement of facial recognition algorithms.	<div style="display: flex; justify-content: space-around; text-align: center;"> <span>Visible</span> <span>Infrared</span> <span>Thermal</span> <span>VisIr</span> </div> 
[60]	USTC-NVIE (Natural Visible and Infrared Facial Expression)	It contains visible-thermal image pairings used for expression recognition and emotion inference. It includes images of 215 participants, with a split between "posed" and "spontaneous" facial expressions taken under different lighting conditions (left, right, and front).	Research on expression recognition, emotion inference, and cross-modality facial recognition.	

Figure 1: Examples of pictures for a particular theme in the suggested library.

Figure 2: Illustration of photos depicting the six facial expressions of a subject, including happiness, disgust, fear, surprise, sadness, and rage.

TABLE 1. (Continued.) Overview of facial recognition databases.

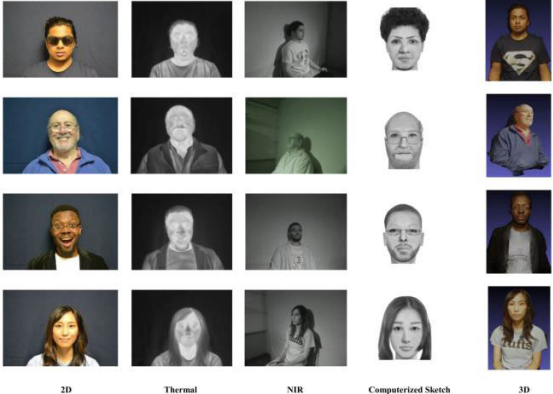
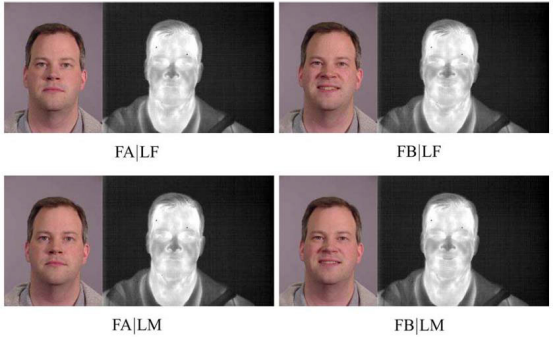

<p>[84]</p>	<p>TUFTS</p>	<p>It includes diverse data types, such as 2D visible, thermal infrared, 3D, and more, used to study the effects of facial expressions and accessories on recognition accuracy. It includes images captured from various angles and under different lighting conditions.</p>	<p>This research explores the analysis of facial expressions, recognizing emotions across different sensory modalities, and investigating how accessories can impact recognition accuracy.</p>	 <p><b>Figure 3:</b> These pictures are chosen from the Tufts Face database, encompassing various nations, ages, and cultural origins.</p>
<p>[63]</p>	<p>UND-X1</p>	<p>This database provides visible and long-wave infrared (LWIR) images for studying the effects of lighting, expressions, and time-lapse on recognition accuracy. It includes photos of 82 participants, 50 used for training and 32 for testing.</p>	<p>Exploring the impact of different lighting conditions, varied facial expressions, and time-lapse effects on recognition.</p>	 <p><b>Figure 4:</b> The University of Notre Dame acquired four images with varying lighting and expressions in visible and infrared pictures. The photos are labelled as follows: FA for "neutral expression," FB for "smiling expression," LF for "FERET style lighting," and LM for "mugshot lighting."</p>
<p>[64]</p>	<p>CASIA NIR-VIS 2.0</p>	<p>This database features visible and near-infrared (NIR) images commonly used to model real-world scenarios for cross-modality facial recognition. It includes photos of 725 participants with varying numbers of frames.</p>	<p>Analysing and recognising faces across different data types, such as images and videos, to simulate and understand real-life situations.</p>	 <p><b>Figure 5:</b> Examples of VIS and NIR face pictures of the same person vary in sharpness, lighting, pose, and age.</p>

TABLE 1. (Continued.) Overview of facial recognition databases.



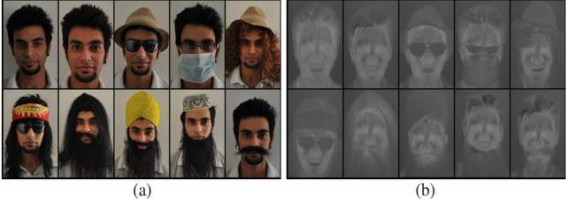

<p>[65]</p>	<p>FaceScrub</p>	<p>The FaceScrub dataset contains 530 individuals with approximately 200 pictures per participant, totalling 106,863. It includes a balanced distribution of genders.</p>	<p>General face recognition research, testing algorithms on large, diverse datasets.</p>	 <p>Figure 6: Examples of visible face pictures.</p>
<p>[66]</p>	<p>CUHK Face Sketch (CUFS)</p>	<p>The CUHK Face Sketch database contains 188 facial pictures from various sources, with artist-created sketches for each face for photo-sketch synthesis and recognition.</p>	<p>Engaging in research focused on the synthesis and recognition of photo sketches.</p>	 <p>Figure 7: Illustrations of a facial photograph and a hand-drawn rendering.</p>
<p>[69]</p>	<p>I<sup>2</sup>BVSD</p>	<p>The I<sup>2</sup>BVSD database includes pictures of the frontal position with various disguises, such as facial hair, headwear, and eyewear, from 75 participants.</p>	<p>They disguised facial recognition research.</p>	 <p>Figure 8: Some examples are (a) photos obtained in the visible spectrum and (b) comparable images collected in the thermal spectrum.</p>
<p>[71]</p>	<p>BRSU Spoof</p>	<p>This database encompasses many spectral bands, including VIS-IR modalities and pictures acquired at specific wavelengths. It includes various disguises and presentation attacks.</p>	<p>Anti-spoofing research, multispectral analysis.</p>	 <p>Figure 9: Instances of assessed spoofing attacks.</p>

TABLE 1. (Continued.) Overview of facial recognition databases.


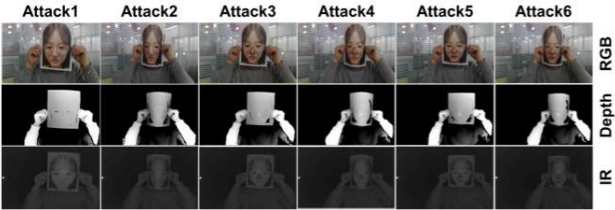


<p>[73]</p>	<p>Spectral Disguise Face</p>	<p>The Spectral Disguise Face Database includes images from visible to NIR spectrums, focusing on disguised and authentic images.</p>	<p>The Spectral Disguise Face database facilitates designing and evaluating face recognition algorithms for security, surveillance, and forensic investigation.</p>	 <p>(a) (b) (c)</p> <p>Figure 10: Different facial appearances of the same person under disguise: (a) Clean-shaven face, (b) Short beard, (c) Long beard.</p>
<p>[85]</p>	<p>CASIA SURF</p>	<p>A large-scale multi-modal benchmark for face anti-spoofing includes images of 1000 Chinese participants in RGB, Depth, and IR modes.</p>	<p>Analysing facial features to identify individuals in different lighting conditions and wavelengths helps to detect fake attempts, such as using masks or photos.</p>	 <p>Attack1 Attack2 Attack3 Attack4 Attack5 Attack6</p> <p>RGB</p> <p>Depth</p> <p>IR</p> <p>Figure 11: Sample of images containing six attack styles.</p>
<p>[86]</p>	<p>IIIT-D Sketch</p>	<p>This database includes sketches and photographs, focusing on both viewed and forensic sketches. It is designed to test the performance of face recognition algorithms on sketch-based inputs.</p>	<p>Sketch-based face recognition research.</p>	 <p>Figure 12: Samples of forensic sketches where face features are exaggerated.</p>
<p>[77]</p>	<p>AT&amp;T (ORL)</p>	<p>The AT&amp;T (formerly ORL) database contains 400 images of 40 subjects, with 10 photos of each subject taken at different times, lighting conditions, facial expressions, and facial details (glasses/no glasses).</p>	<p>Testing and validating face recognition algorithms, particularly those involving variations in pose and expression.</p>	 <p>Figure 13: Sample of images with glasses and without glasses.</p>

TABLE 1. (Continued.) Overview of facial recognition databases.

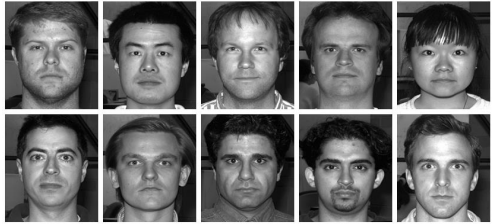







<p>[78]</p>	<p>Yale Face Database B</p>	<p>It contains 5760 single-light source images of 10 subjects, each seen under 576 viewing conditions (9 poses × 64 illumination conditions). This database is designed to test algorithms under variations in lighting and pose.</p>	<p>Research in lighting variation and pose changes in face recognition systems.</p>	 <p>Figure 14: Illustrations of the ten individuals featured in the Yale Face Database B.</p>
<p>[79]</p>	<p>FERET</p>	<p>The FERET database includes 14,051 images of 1,199 individuals, with each subject having pictures taken at different angles, expressions, and lighting conditions. It was created to encourage the development of facial recognition algorithms.</p>	<p>They were conducting benchmarks for facial recognition systems, especially in their ability to handle variations in appearance and environmental conditions.</p>	 <p>Figure 15: Illustrations of the photos contained in the FERET database.</p>
<p>[80]</p>	<p>CMU PIE</p>	<p>The CMU PIE (Pose, Illumination, and Expression) database contains more than 41,000 images of 68 individuals captured under 13 different poses, 43 different illumination conditions, and 4 different expressions.</p>	<p>Studying the effects of pose, illumination, and expression changes on facial recognition systems.</p>	 <p>Figure 16: Detailed photographs depicting an individual during the four recording sessions. In session 1, the researchers captured a smiling and neutral expression.</p>
<p>[81]</p>	<p>UMIST Face</p>	<p>The UMIST database contains 564 images of 20 individuals, each shown in various poses from profile to frontal views.</p>	<p>Research into face recognition under different poses.</p>	 <p>Figure 17: Samples of photos were used in the UMIST face database.</p>

TABLE 1. (Continued.) Overview of facial recognition databases.

<p>[67]</p>	<p>AR Face</p>	<p>The AR Face database consists of over 4,000 colour images of 126 people's faces (70 men and 56 women). Each person has pictures taken in two sessions (14 days apart), with variations including different facial expressions, illumination conditions, and occlusions (such as sunglasses and scarves).</p>	<p>Research in facial recognition with occlusions, expression changes, and illumination variations.</p>	 <p>Figure 18: Some photos were obtained during the initial session.</p>
<p>[82]</p>	<p>FG-NET Aging</p>	<p>The FG-NET Aging Database contains 1,002 images of 82 subjects aged from infancy to 69. The database captures the natural ageing process.</p>	<p>They have examined the impacts of ageing on facial recognition systems.</p>	 <p>Figure 19: Some examples of images utilised in the FG-NET Aging Database.</p>
<p>[83]</p>	<p>Mobio</p>	<p>The MOBIO database is designed for mobile biometrics research and contains video and audio recordings of 152 people captured in real-world scenarios using mobile devices.</p>	<p>Mobile biometric authentication research focusing on face and voice recognition.</p>	 <p>Figure 20: Illustration showing two distinct persons. There is a noticeable variance in attitude and illumination among the pictures. Furthermore, there is an appreciable variation in the facial hair, specifically in sections (e) to (h), as well as in the hairstyle and make-up, specifically in sections (a) to (d).</p>
<p>[76]</p>	<p>Labelled Faces in the Wild (LFW)</p>	<p>LFW contains 13,000 labelled images of faces from the web, designed to study unconstrained face recognition. It includes photos of 5,749 different individuals with various backgrounds and lighting conditions.</p>	<p>They have Benchmarked unconstrained face recognition algorithms.</p>	 <p>Figure 21: Examples of images for the LFW database.</p>

The prepared dataset is used to train the models. They tested the machine learning models in various contexts, including those with diverse demographics and modified faces. Moreover, these models' incorporation into an ATM system for user authentication guarantees the system's resistance against various disguises and presentation assaults without sacrificing accuracy or usability. Therefore, this technology aims to reliably identify individuals in various settings and with a wide range of face alterations, all while increasing security without sacrificing usability.

Padmashree and Kotegar [8] developed a novel method for disguised face recognition by focusing on the skin regions of the face, which are less likely to be covered by disguises. Their approach begins with pre-processing and face detection, where faces are detected from raw images using a YOLO face detector. These detected faces are then resized to various scales ( $32 \times 32$ ,  $64 \times 64$ ,  $128 \times 128$ , and  $224 \times 224$ ) to facilitate feature extraction and recognition.

The core of their method involves skin segmentation using a region-based marker-controlled watershed algorithm. This algorithm extracts the skin regions from the detected faces by converting the images into topographical representations through gradient transformation. Markers are then placed on the high and low areas of the gradient image, and the watershed algorithm is applied to segment the skin regions. This process employs both HSV and YCbCr colour spaces to enhance the accuracy of skin region extraction [8].

Following skin segmentation, feature extraction is performed using a deep CNN. The CNN architecture designed by the authors consists of three parallel branches, each processing the input image separately before combining their outputs for classification. This multi-branch design allows the network to capture a wide range of features at different scales and levels of detail, which is crucial for accurate recognition [8].

Finally, the classification block consists of a convolutional layer with 2048 filters, followed by ReLU activation, batch normalisation, max pooling, dropout, and global average pooling. The final classification is achieved through a dense layer with softmax activation, which outputs the recognition results. This combination of skin segmentation and deep learning-based classification significantly improves the robustness and accuracy of the model in recognising disguised faces [8].

In recent years, the implementation of Fuzzy Logic with Face Recognition has significantly transformed multiple study fields.

As previously mentioned, dealing with variations in illumination is a complicated problem in face recognition systems. Various techniques have been suggested over the past few decades, but they have yet to address variations in lighting successfully. The efficacy of fuzzy set theory in this regard has been empirically demonstrated. It has made a significant scientific contribution to developing feature

representations in machine intelligence [87], [88]. Preliminary research efforts [89], [90], [91], [92], [93] showed remarkable outcomes when fuzzy set theories were applied to face recognition systems.

The study classifies the examined literature into several application areas where deep learning and fuzzy systems have been integrated [94], such as prediction, sentiment analysis, transportation forecasting, and medical systems. For example, complex models such as the chaotic type-2 transient-fuzzy deep neuro-oscillatory network make financial forecasts in the prediction field [95], [96]. These models efficiently deal with problems like overtraining and impasse. The use of CNN, Recurrent Neural Networks (RNN), and fuzzy logic systems in sentiment analysis enables the deduction of intricate emotions from text and other forms of data while attaining reduced computing complexity compared to conventional classifiers [97]. The accuracy and efficiency of transportation forecasting may be improved by using a hybrid framework that incorporates CNN, Long Short-Term Memory (LSTM), and fuzzy logic systems to estimate traffic flow. In medical systems, hybrid models such as ANFIS (adaptive neuro-fuzzy inference system) and deep learning handle tasks such as illness severity assessment [98], [99]. These models have shown considerable performance increases compared to traditional techniques. The study assesses the integration of several deep learning algorithms with fuzzy systems, including ANFIS, CNN, and LSTM. It examines their efficacy and progress in many disciplines due to this combination [100], [101], [102], [103].

Mahendran and Velusamy [104] developed a biometric essential authentication technique for Body Sensor Networks (BSNs) in the Internet of Medical Things (IoMT). This scheme utilises ECG data's distinctive and fluctuating characteristics to improve security. Conventional biometric techniques that rely on fixed data, such as fingerprints, can be easily replicated, compromising their security. This approach entails the acquisition of biological signals via body sensors, their transformation into identifier variables via fuzzy encoding, and their subsequent decoding at base stations for authentication. The data is protected by a fuzzy vault, with changed thresholds to rectify transmission faults. The Discrete Wavelet Transform (DWT) isolates the prominent characteristics (P, Q, R, S, T waves) from ECG signals. These features are further divided into frequency sub-bands to enable effective encryption. The signal values undergo a conversion process to transform them into fuzzy values. These fuzzy values are then encrypted using the device's host address, which serves as the public key. Finally, the encrypted data is safely stored. The biometric data is encrypted and kept in a fuzzy vault with chaff points to enhance security. The encrypted data is then registered at the base station. During the authentication process, decrypted signals are compared to stored values using the Euclidean distance metric. This ensures safe identification by differentiating genuine data points from irrelevant or misleading ones. This



methodology surpasses the constraints of prior methodologies, delivering improved security and efficiency in biometric key authentication for Internet of Medical Things (IoMT) applications.

The study technique in [105] included a series of essential stages to assess the efficacy and safeguarding of a biometric authentication system using code-based Fuzzy Extractors for face recognition. The researchers acquired high-resolution facial photos from freely available datasets and used pre-processing techniques such as normalisation, transformation, and encoding using the face recognition package [106]. The Fuzzy Extractor was implemented in a controlled computational environment with the McEliece cryptosystem and error correction codes to guarantee consistent and dependable outcomes [20], [21]. The Fuzzy Extractor's performance was assessed using 100 photos of one person to calculate the False Rejection Rate (FRR) and 100 photos of another person to get the False Acceptance Rate (FAR). The effectiveness of the extractor was evaluated by comparing the experimental and theoretical values of FRR and FAR [105].

The system performance was also shown by plotting the Receiver Operating Characteristic (ROC) curve, which shows how the system performs at different thresholds. Thorough evaluations revealed differences between the actual and predicted values, especially when the mistake rates were low. This showed that the system is quite strict in rejecting legitimate users in real-life situations. The examination of the ROC curve revealed the trade-offs between security and comfort, as lower FRR values improved user convenience while higher FAR values presented possible security problems. This technique offered a meticulous strategy for assessing the system's capacities and constraints by combining theoretical concepts with real applications [105].

Rajawat et al. [107] suggested an approach for detecting sadness via facial expressions [108] encompassing many essential steps. The process begins with data collecting and preparation, during which facial expression photos are gathered, normalised, and converted to a standardised format to ensure consistency in the input data. The feature extraction process combines fuzzy logic and CNNs. The Fuzzy Min-Max (FMM) approach splits the data for various purposes: training, rule extraction, rule selection, and testing [109], [111], [111]. This phase accurately captures the subtle characteristics of facial expressions that are linked to depression. The classification process entails using the extracted characteristics to assess degrees of depression using the Fuzzy Logic and Deep Learning (FFL-DL) method, which combines fuzzy logic principles with the decision-making skills of CNNs [112], [113], [114]. The classification structure comprises numerous layers, guaranteeing accurate analysis of incoming data. The system's performance is assessed by measuring accuracy, sensitivity, and specificity. Comparative analysis shows substantial improvements in classification accuracy and robustness.

## V. RESULTS AND DISCUSSION

In this section, the detailed experimental findings. Cheema et al. [1] proposed a CMDN to address challenges in HFR by effectively bridging the gap between visible and thermal modalities. Experimental results showed that CMDN achieved a 99.7% Rank-1 recognition rate on the USTC-NVIE dataset, a 92.4% Rank-1 recognition rate on the Sejong Face dataset, and substantial improvements in other datasets such as TUFTS and CASIA NIR-VIS 2.0. These results highlight the significant improvement in recognition accuracy across different modalities, making CMDN a robust surveillance and access control application framework. The CMDN's ability to learn relational features between modalities rather than merely mapping them into a common subspace enables more flexible and accurate cross-modality face recognition. This advancement is crucial for scenarios with varied environmental conditions, such as security-focused domains.

Ahmad et al. [2] focused on overcoming the limitations posed by facial disguises in recognition systems by employing GANs and Cycle-Consistency Loss to produce synthetic datasets of disguised faces. Experimental findings indicated that using the synthetic database enhanced the rank-1 recognition rate by 68.3%. This demonstrates the effectiveness of the proposed methodology in improving the robustness and accuracy of facial recognition algorithms against disguises. By generating high-quality synthetic data, this approach addresses the scarcity of comprehensive training data for disguised faces, thus enhancing training efficiency and recognition accuracy.

Cheema and Moon [3] introduced the DNDR network coupled with JDL to improve performance in hidden HFR. Experimental results showed that the DNDR network achieved a 1.76% improvement in VIS-NIR tests and a 3.68% improvement in VIS-THE tests compared to previous methods. This demonstrates the superior performance of DNDR in handling hidden HFR difficulties, particularly in dealing with faces with masks and varied imaging conditions. By focusing on deep feature relations rather than extensive pre-processing or domain gap reduction methods, the DNDR network enhances identity representation and cross-modality matching. This method's effectiveness in improving recognition accuracy makes it a valuable contribution to facial recognition technologies.

Kowalski et al. [4] proposed a thermal-visible face verification system using a triple triplet approach incorporating several CNNs. This method significantly improved recognition accuracy, achieving TAR @FAR 1% values up to 90.61%. The experimental results highlighted the robustness of this method in various challenging conditions, making it a new standard for future research in thermal-visible face recognition. Effectively integrating thermal and visible data is a reliable method for addressing variations in lighting and motion commonly encountered in real-world scenarios. This method's ability to differentiate between genuine

users and impostors more effectively enhances security and accuracy.

The “Synthetic Disguised Face Database” in [2] trains and tests face recognition algorithms for disguises. The database contains 13 synthetic disguises. CycleGAN learns domain mappings using cycle-consistency loss, guaranteeing that produced pictures match the original data. An automatic filtration technique eliminates low-quality photos to prevent training deterioration. The approach employs a SqueezeNet-based FR model trained on actual and disguised pictures. The method prevents overfitting and human intervention. The results show remarkable facial recognition advances.

Any FR system may be far more resistant to presentation and disguise assaults by including the Synthetic Disguised Face Database. Additionally, researchers may enhance FR technology by adding new disguise variations to facial datasets using the suggested GAN and cycle-consistency loss technique. Security applications that require FR to be resilient to spoofing and presentation attacks might find this approach especially beneficial because of its efficacy in managing disguises. Training and assessing FR algorithms, mainly when disguises are widespread, may be accomplished using the synthetic database and methodology. Furthermore, additional domains of computer vision and machine learning that place a premium on data enhancement and quality control of training data can incorporate the concepts of automated filtering and synthetic picture synthesis. Last but not least, collaborating with industry partners to put these approaches to the test in real-world settings might yield helpful information for improving and using them.

The numerical results in [5], which were checked using the FID and KID, showed that the CycleGAN’s created thermal images were very close to the original data. Qualitative results also showed that these two things were similar. The study finds that GANs, especially CycleGAN, can successfully turn visible light images into thermal images. This can help with tasks that need thermal imagery data, like face recognition.

Face recognition can achieve higher accuracy in low-light conditions when GANs are employed in monitoring and security systems. This method can address the absence of thermal and infrared imaging data by generating synthetic thermal images, which can be incorporated into training datasets for face recognition models. Both law enforcement and rescue teams can benefit from this technology. Additionally, further research is needed to explore image translation across different modes. For instance, it may be possible to transform images into representations resembling radar or sonar. Collaborating with government and business partners could facilitate the practical application of these advancements and drive further progress.

Ahmad et al. [6] explored the generation of synthetic disguised faces using GANs to improve system robustness against disguise attacks. Experimental results

demonstrated that this method could improve model accuracy by 20 to 25 percent, depending on the disguise add-on used. This shows the significant contribution of this method to the field of facial recognition, particularly in enhancing the robustness of recognition systems against disguises. The one-shot generation approach efficiently enhances facial recognition systems by adding diverse disguised faces to the training dataset, making it feasible to generate a wide variety of disguised faces from a limited number of original images. This approach is beneficial when collecting large datasets of disguised faces is impractical.

Alkadi et al. [7] developed a multi-modal facial recognition system for ATM biometric authentication, integrating visible, IR, and thermal images. Experimental results showed that the system achieved over 99% recognition accuracy on the Sejong dataset, even with standard facial accessories like sunglasses, face masks, and ethnic head covers. These results demonstrate the system’s high effectiveness in real-time applications. However, challenges were noted in identifying individuals who had undergone significant changes in appearance, such as wearing a Hijab after being photographed without one. Using multi-modal data allows the system to leverage the strengths of each modality, such as the detail captured in visible light and the disguise-resistance of thermal images, leading to a more robust and reliable authentication process.

Padmashree and Kotegar’s [8] proposed model was evaluated on the Sejong Face Database, achieving a high accuracy of 94.92% on  $64 \times 64$  image sizes. The study included an ablation analysis to assess the impact of different factors on the model’s performance, such as image size and kernel filter size. The proposed model demonstrated superior performance to traditional methods, particularly in handling various disguises. The focus on skin segmentation significantly improves the accuracy of disguised face recognition by reducing noise and irrelevant information. This method effectively isolates skin-related features, such as texture and colour, which exhibit high discriminative power for individual recognition. The model captures fine-grained and coarse-grained details by employing multiple filter and kernel sizes, enhancing overall performance. The study’s findings address critical challenges in DFR, such as changes in facial features, lack of training data, and variability in disguises, making it a promising solution for real-world applications in security and surveillance.

The fuzzy fisher face classifier, developed by Kwak and Pedrycz [90], is an early face recognition model based on fuzzy logic. The suggested approaches utilised a progressive amount of projection to determine the membership grade of a class, resulting in enhanced classification outcomes due to the increased level of discrimination. Moreover, a fuzzy K-nearest neighbour classification method is employed while acting on feature vectors created using Principal Component Analysis (PCA). The categorisation results show substantial enhancements, which are further

**TABLE 2.** Analyse and compare different face recognition techniques and evaluate their performance on different datasets.

References	Used Database(s)	Approaches	Results	Limitations
[1] Cheema et al.	USTC-NVIE, TUFTS, UND-X1, Sejong Face, CASIA NIR-VIS 2.0.	Cross Modality Discriminator Network (CMDN).	Significant improvements in recognition rates: 99.7% Rank-1 on USTC-NVIE, 92.4% Rank-1 on Sejong Face, In TUFTS, HFR and FUS significantly improved 21.3% and 22.8% over current methods, 95.21% Rank-1 accuracy in UND-X1, and 99.5% Rank-1 in CASIA NIR-VIS 2.0.	The high cost of thermal imaging devices, the lack of large-scale visible-thermal datasets, and significant differences in modalities are all challenging factors.
[2] Ahmad et al.	I <sup>2</sup> BVSD, BRSU Spoof, Spectral Disguise Face, CASIA SURF, Sejong Face.	Generative Adversarial Network (GAN), Cycle-Consistency Loss.	It improved rank-1 recognition rate by 68.3%.	Gender bias in disguise add-ons, issues identifying covered faces, low-quality generated images, and high computational complexity.
[3] Cheema and Moon	Sejong Face, TUFTS, CASIA NIR-VIS 2.0, CUHK Face Sketch (CUFS), IIIT-D Sketch.	Profound Neighbourhood Difference Relational (DNDR) Network, Joint Discrimination Loss (JDL).	It improved performance over state-of-the-art methods in multiple datasets.	Challenges include the need for extensive training and computational resources, concerns about generalisability, and reliance on data quality.
[4] Kowalski et al.	D4FLY Thermal and 2D Face, IOE_WAT, Speaking Faces, Sejong Face, FaceScrub.	Triple Triplet Method using CNN features.	They were achieved TAR @FAR 1% up to 90.61%.	Challenges include data bias, underrepresentation of racial diversity, potential performance issues related to individuals wearing glasses, and significant computational complexity.
[5] Abdulllah et al.	Sejong Face.	Generative Adversarial Network (GAN), CycleGAN.	High-quality and natural-looking thermal images.	Training takes up a lot of time and resources, there are concerns about how applicable the results are, and it relies heavily on having high-quality data.
[6] Ahmad et al.	Sejong Face.	Patchwise Contrastive Loss, Cycle-Consistency Loss.	It improved model accuracy by 20-25%.	They are limited to a single image per subject for training and have high computational complexity.
[7] Alkadi et al.	I <sup>2</sup> BVSD, BRSU Spoof, Spectral Disguise Face, Sejong Face (as reference).	ResNet-50, VGG-16, InceptionV3.	The Sejong dataset has over 99% recognition accuracy and is effective with facial accessories.	The difficulties are associated with significant alterations in one's appearance, such as the decision to wear a hijab.
[8] Padmashree and Kotegar	Sejong Face Database.	Skin Segmentation-Based Disguised Face Recognition using a region-based marker-controlled watershed algorithm for skin segmentation, CNN for feature extraction, and deep learning-based classification.	They have achieved an impressive 94.92% accuracy on a 64×64 image size and a remarkable precision of 95.57%. They outperformed state-of-the-art models in terms of recall and F1 Score.	The study did not address the computational complexity of the segmentation and classification processes. The approach may require significant preprocessing time, and its effectiveness may vary with different lighting conditions and skin tones.

**TABLE 2. (Continued.) Analyse and compare different face recognition techniques and evaluate their performance on different datasets.**

[90] Kwak. and Pedrycz	ORL, Yale – B, and CNU	Fuzzy Fisher	94.12%, 94.80%, and 96.80% correspondingly	Relying on PCA to reduce the number of dimensions at the start of classification jobs might not be the best approach. How sensitive it is to changing parameters, especially the number of close neighbours (k). The fuzzy sorting step made the computations more difficult. - Has a hard time with the dataset's large amounts of noise and outliers. Assessments are based on small databases, which could make them harder to apply to other situations.
[92] Yang et al.	FERET Yale – B	CFLDA (Complete Fuzzy Linear Discriminant Analysis)	52.17% 89.17%	More information from the sample distribution needs to be used. The within-class scatter matrix is singular in the PCA-converted space. Disregarded discriminatory data in the zero space of the fuzzy within-class scatter matrix. The computational complexity is high. The dependence on the selection of parameters is crucial.
[115] Li	ORL, Yale – B, and FERET	Fuzzy 2D – PCA	98.83%, 88.5%, and 59.67% respectively	The skill to perceive slight variations in the angle of light, the position of the face, and the emotions and intentions conveyed through facial expressions. The mean matrix estimation is inaccurate because of the short sample size and the presence of outliers. The computational complexity is high. The dependence on the selection of parameters is crucial. The analysis was conducted on specified databases, which may not fully represent real-world settings.
[117] Huang et al.	ORL, CMU-PIE, and FERET	FLRDP (Fuzzy Linear Regression Discriminant Projection)	96%, 97.69%, and 90.70% correspondingly	The impact of parameter selection, namely the parameter $k$ , is quite significant. It is compatible with LRC but not with other classifiers such as NNC (Nearest Neighbor Classifier) and MDC (Minimum Distance Classifier). Performance is restricted to using LRC (Light Responsive Cells). Further research is crucial to effectively manage the variables in the selection challenge while preserving the advantageous characteristics of the technique.
[120] Sing et al.	At and T, UMIST, FERET, and AR	CFG-FRLF (Introduced Confidence Factor Weighted Gaussian Function with Fuzzy Rank-Level Fusion)	98.79%, 98.36%, 66.87%, and 64.91% correspondingly	The dependence on the selection of parameters is crucial. Optimisation of parameters is necessary. The computational complexity is high because of parallel processing. Datasets with limited scope may need to accurately reflect the full range of variability in the actual world. They are embracing diverse forms of biometric characteristics.

**TABLE 2.** (Continued.) Analyse and compare different face recognition techniques and evaluate their performance on different datasets.

<p>[121] Rejeesh</p>	<p>ORL, and Ext. YB</p>	<p>ANFIS-ABC (Interest Point Based Face Recognition using Adaptive Neuro-Fuzzy Inference System)</p>	<p>96%, and 95% respectively.</p>	<p>Possible difficulties may arise because of the fluctuating lighting circumstances and the many facial positions and emotions that may be encountered.  The computational complexity is linked to optimisation techniques. The analysis is constrained to specific datasets, which may impact the capacity to apply the findings to a broader context.</p>
<p>[116] Oulefki et al.</p>	<p>EYale-B, Mobio, FERET, and CMU-PIE</p>	<p>Fuzzy Reasoning Model (FRM)</p>	<p>-</p>	<p>It investigated algorithm efficiency, computation time, excessive or insufficient improvements, noise amplification issues, and the challenges associated with non-uniform illumination conditions. There is a need to improve a specific section of the face that is being targeted.  Relying just on visual evaluation is inadequate when making assertions about the accuracy of face recognition.  There are discrepancies noted in the image quality measures (IQM) and datasets.</p>
<p>[119] Du et al.</p>		<p>Fuzzy LDA (Fuzzy Linear Discriminant Analysis)</p>	<p>-</p>	<p>Performance steadiness is affected by how sensitive it is to parameter selection.  The flexible sorting process has made the computations more difficult.  Trouble dealing with significant changes in posture and facial emotions.  The outcome relies on the initial selection of variables, including the fuzzification constant. Only some tests were done on different data sets, making it harder to use the results in other situations.</p>

validated by the experimental findings from the face databases of Yale, ORL, and CNU (Chungbuk National University).

Li [115] introduced a face recognition technique based on fuzzy 2DPCA. This algorithm incorporates the fuzzy K-nearest neighbour method and computes the membership degree matrix of the training samples. The membership degree matrix is then used to determine the fuzzy means of each class. The calculated fuzzy means are included in the definition of the general scatter matrix, resulting in a prediction that can enhance classification outcomes. The FERET, ORL, and YALE face datasets assess the suggested model. The experimental results demonstrate the method's effectiveness even in a challenging environment characterised

by variations in illumination, facial expressions, and position limitations.

From the inception of face recognition research, dealing with light variance has consistently posed a significant challenge in achieving precise results. Oulefki et al. [116] propose a fuzzy reasoning model that addresses lighting variations through an image enhancement technique grounded in fuzzy theory. The model is a method that improves the visibility of non-uniform lighting and low contrasts by making adjustments based on the surrounding conditions. As depicted in Figure 22, the proposed method enhances the original image's luminosity and differentiation. Additionally, the utilisation of fuzzy logic reveals the concealed intricacies of the provided image.

**TABLE 3.** Analyse and compare the strengths and weaknesses of different facial recognition methods.

References	Approaches	Strengths	Weaknesses
[5]	GAN, CycleGAN.	Addresses data scarcity for thermal images; Uses CycleGAN for realistic image generation; Improves recognition performance with generated data	May still require substantial computational resources for GAN training; Quality dependent on training data diversity
[6]	Patchwise Contrastive Loss, Cycle-Consistency Loss.	Effective with minimal training data; Combines patchwise contrastive loss and cycle-consistency loss; significantly improved recognition accuracy.	Requires separate models for each subject and add-on combination; Initial implementation complexity
[7]	ResNet-50, VGG-16, InceptionV3.	Uses multiple modalities to improve accuracy; Overcomes challenges of disguise and presentation attacks; Applicable for practical security implementations	Implementation complexity due to multiple ML models Requires diverse training datasets for each modality.
[8]	Skin Segmentation-Based Disguised Face Recognition using a region-based marker-controlled watershed algorithm for skin segmentation, CNN for feature extraction, and deep learning-based classification.	Improves recognition accuracy using deep learning for skin segmentation; Robustness against various disguises.	High computational cost for deep learning models; Dependence on quality of skin segmentation
[1]	CMDN	Effective cross-modality recognition; Uses unit-class loss for improved accuracy; Can handle visible and thermal/infrared images.	Complex implementation due to cross-modality processing Requires extensive training data for all modalities.
[4]	Triple Triplet Method using CNN features	It uses CNN features and triple triplet configuration for enhanced recognition on the move; it is effective in real-time applications.	High computational requirements for real-time processing; Requires diverse training data for different conditions.
[3]	DNDR, JDL	It utilises significant neighbourhood difference relational networks for recognising disguised faces and handles variations in heterogeneous data.	Complex model architecture: Requires substantial computational resources for training.

TABLE 3. (Continued.) Analyse and compare the strengths and weaknesses of different facial recognition methods.

[2]	GAN, Cycle-Consistency Loss	Combines cycle-consistency loss and automated filtering for generating realistic disguised faces; Enhances training data quality	Quality of generated images dependent on initial training data; Computationally intensive
[105]	Code-Based Fuzzy Extractors	High security with robust error correction, resistant to quantum attacks	High computational complexity may not be suitable for real-time applications.
[23]	Neural Fuzzy Extractors	Combines neural networks with Fuzzy Extractors for enhanced security, adaptability to various biometrics	Potentially high training times and resource requirements, complexity in implementation
[94]	Fusion of Deep Learning and Fuzzy Systems	Leverages deep learning for improved accuracy, handles complex patterns and variability	Requires large datasets for training, computationally intensive, potential overfitting
[122]	Classical Face Recognition Approaches	Well-established methods, with extensive research and development, are effective in controlled environments.	Less effective in uncontrolled environments, susceptible to spoofing and disguise

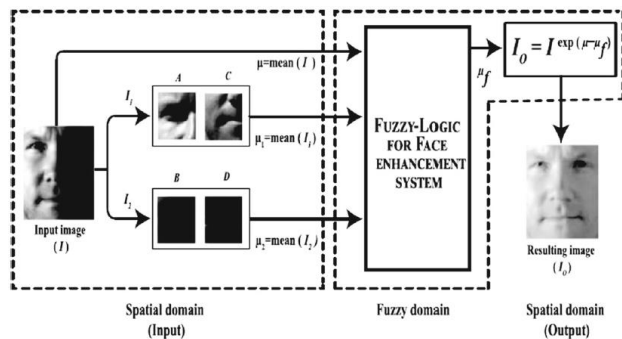


FIGURE 22. A paradigm for improving lighting using a generic structure, adapted from [116].

Through the utilisation of four reference picture quality measures derived from the input visual face, the fuzzy reasoning model has been evaluated. Subsequently, a fuzzy logic system is employed to extract information from the four matrices (A, B, C, and D) to reconstruct an improved image. The authors have performed a comparative analysis using six state-of-the-art methodologies to assess the proposed model. The system yields significant performance results on famous face datasets such as Yale-B, Mobio, FERET, and Carnegie Mellon University, specifically regarding position, illumination, and expression. Similarly, other researchers, such as Pu Huang et al. [117], proposed a fuzzy linear regression discriminant projection model. Still, Campomanes-Álvarez et al. [118] developed a fuzzy distance-based model for skull-face overlay in craniofacial superimposition. These models

use fuzzy logic to address pose, illumination, and contrast variations.

Du et al. [119] have emphasised the significance of uncertainty in face recognition and employed an interval-type-2-based fuzzy linear discriminant analysis model to address the uncertainty in a highly intricate face recognition setting. The text introduces a supervised interval type-2 fuzzy C-Mean (IT2FCM) algorithm to utilise classified information effectively. Subsequently, it is integrated into a linear discriminant analysis model to mitigate the impact of noise and achieve accurate local distribution. The IT2LDA technique employs the IT2FCM model to assign weights to each face pattern for individual classes and compute the average for each class. Subsequently, they are used to calculate the fuzzy within-class and fuzzy between-class scatter matrices, respectively. The suggested IT2FLDA framework is adept at identifying the optimal directions for optimising the fuzzy within-class and fuzzy between-class scatter matrix ratios. The resulting feature space is characterised by increased discriminability and resilience, making it more suitable for recognition. Sing et al. [120] have revealed a breakthrough that involves a confidence factor-weighted Gaussian function combined with parallel fuzzy rank-level fusion. The suggested system generates fuzzy rankings using a Gaussian function, which is determined by the confidence level of a classifier. Unlike the usual ranking, this fuzzy ranking considers the relationships between a classifier’s outputs (confidence factors). The final ranks for face recognition are determined by fusing the fuzzy ranks generated by several representations of a face image, with each rank weighted

**TABLE 4. Components of a framework for assessing the effectiveness of biometric authentication methods.**

References	Framework Component	Details
[23, 105]	Metrics for Evaluation	Incorporates FRR, FAR, and ROC curves to measure system performance and trade-offs between security and convenience.
[94, 105]	Cryptographic Integration	It uses Fuzzy Extractors to generate cryptographic keys from noisy biometric data without storing raw templates.
[23, 105]	Post-Quantum Cryptographic Resilience	For long-term security, adopt post-quantum cryptographic schemes, such as the McEliece cryptosystem.
[94]	Adaptive and Context-Aware Algorithms	It includes adaptive algorithms to adjust dynamically based on biometric data quality and reliability.
[94, 105]	Ethical and Privacy Considerations	Ensures compliance with global data protection regulations and implements privacy-preserving mechanisms.
[105]	Practical Implementation and Evaluation	The document details the procedures for acquiring data, preprocessing, experimental design, and analytical analysis.

according to the associated confidence factors of the classifier. Similarly, Rejeesh [121] proposed a face recognition method that utilises interest points and an adaptive neural fuzzy inference system.

Fuzzy-based approaches have effectively addressed complicated face recognition challenges, particularly those related to illumination and pose change.

Table 2 thoroughly summarises different research publications that have used the Sejong Face Database and other datasets in face recognition technology. These articles examine multi-modal face recognition in security, biometrics, and identity verification. The table provides a comprehensive overview of the databases used, the methodologies employed, the outcomes achieved, and their constraints, including particular investigations on fuzzy-based face recognition systems. This research compares the identification rates of these algorithms with conventional approaches on relevant datasets, emphasizing the performance and difficulties involved with each methodology. The comprehensive findings demonstrate substantial improvements in identification rates and accuracy across diverse datasets but acknowledge constraints such as increased computing complexity, reliance on data quality, and disparities in modality.

Each study contributes to the field of facial recognition, addressing challenges like the high cost of imaging devices, data scarcity, and the need for robust algorithms capable of handling disguised and multi-modal face recognition. Despite their advancements, these studies highlight ongoing challenges and the need for further research in this rapidly evolving field.

In the realm of FR and biometric authentication, numerous methods have been proposed and developed to enhance the accuracy and robustness of these systems, particularly in the presence of challenges such as disguises and changing environmental conditions. Table 3 briefly summarises the pros and cons of several prominent methodologies, encompassing both traditional approaches and advanced techniques that integrate Fuzzy Extractors with machine learning. This comparative analysis provides an overview of each method’s practical applicability, computational requirements, and potential limitations, offering valuable insights for researchers and professionals seeking to select or develop an optimal face recognition system.

In the current biometric authentication context, providing a solid framework for classifying and evaluating biometric systems is crucial. This framework will help address the challenges and compromises related to security, user convenience, and privacy. A comprehensive framework must consider many biometric modalities and utilise sophisticated metrics and algorithms for a thorough comparative study. Table 4 comprehensively summarises the innovative classification and assessment system used to compare various biometric authentication methods.

## VI. CONCLUSION AND FUTURE WORK

This survey offers a comprehensive overview of recent advancements in facial recognition technology, focusing on multi-modal face recognition and its applications in security biometrics and identity verification. The study emphasises the significant progress in developing robust



facial recognition systems that can accurately identify faces under various conditions and disguises. Researchers have explored various aspects of facial recognition, such as hidden and disguised face recognition, cross-modality analysis, and thermal-visible face recognition, by leveraging extensive and diverse datasets such as the Sejong Face Database (SFD).

However, there are still several knowledge gaps and challenges in the current state of facial recognition technology. These include the high cost of thermal imaging devices, the lack of large-scale visible-thermal face datasets, significant differences between visible and thermal/infrared modalities, and the dependence on data quality and availability. Additionally, challenges related to the resource-intensive nature of network implementation and training, limited adaptability to rapid technological changes, and complications in handling subjects wearing glasses or undergoing significant appearance changes persist. Integrating Fuzzy Extractors and combining biometric verification with cryptographic security presents opportunities and challenges. Future research should focus on developing more efficient Fuzzy Extractors for continuous biometric data sources and integrating them with post-quantum cryptographic methods. These efforts are vital for improving the security and privacy of biometric systems, especially given the emerging threats posed by quantum computing.

In order to tackle these general challenges, it is crucial to continue researching and developing facial recognition technology. Future research should prioritise the following:

1. **Improving Generalisability and Scalability of Models:** Focus on developing models that can maintain high accuracy and robustness across diverse environments, lighting conditions, and demographic variations.
2. **Development of Comprehensive and Diverse Datasets:** Create large-scale, diverse datasets with various modalities such as visible light, infrared, and thermal images to train more robust models.
3. **Advanced Cross-Modality Techniques:** Explore advanced cross-modality techniques to improve recognition accuracy between different types of images, such as visible to thermal.
4. **Enhancing Real-Time Processing Capabilities:** Improve facial recognition algorithms' computational efficiency to enable real-time processing by optimising deep learning models and more efficient hardware solutions.
5. **Integration with Cryptographic Methods:** Combine biometric authentication with advanced cryptographic techniques, especially those resistant to quantum computing threats.
6. **Exploring GAN-based Data Augmentation:** Generative Adversarial Networks (GANs) can be used to create synthetic training data, enhancing the robustness of recognition systems against disguises.
7. **Fuzzy Extraction:** Develop more efficient Fuzzy Extractors for continuous biometric data sources and integrate them with post-quantum cryptographic

methods. Additionally, future research should focus on enhancing security and privacy measures, optimising real-time applications, and expanding Fuzzy Extractors to other biometric modalities.

Incorporating cryptographic methods and sophisticated cross-modality approaches provides the most immediate and substantial advantages. Incorporating cryptographic techniques tackles the essential need for heightened security, particularly in light of impending quantum risks. Conversely, enhanced cross-modality approaches enhance the system's resilience and versatility in many settings and circumstances, which is crucial for practical applications.

Consequently, we would prioritise integrating cryptographic methods and advanced cross-modality techniques, as they effectively handle face recognition technology's security and functional robustness aspects.

## REFERENCES

- [1] U. Cheema, M. Ahmad, D. Han, and S. Moon, "Heterogeneous visible-thermal and visible-infrared face recognition using unit-class loss and cross-modality discriminator," 2021, *arXiv:2111.14339*.
- [2] M. Ahmad, U. Cheema, M. Abdullah, S. Moon, and D. Han, "Generating synthetic disguised faces with cycle-consistency loss and an automated filtering algorithm," *Mathematics*, vol. 10, no. 1, p. 4, Dec. 2021.
- [3] U. Cheema and S. Moon, "Disguised heterogeneous face recognition using deep neighborhood difference relational network," *Neurocomputing*, vol. 519, pp. 44–56, Jan. 2023.
- [4] M. Kowalski, A. Grudzień, and K. Mierzejewski, "Thermal-visible face recognition based on CNN features and triple triplet configuration for on-the-move identity verification," *Sensors*, vol. 22, no. 13, p. 5012, Jul. 2022.
- [5] M. Abdullah, A. Lee, and D. Han, "GAN based visible to thermal image translation," in *Proc. IEEE Int. Conf. Consum. Electron.-Asia (ICCE-Asia)*, Oct. 2022, pp. 1–3.
- [6] M. Ahmad, M. Abdullah, and D. Han, "One-shot synthetic disguised face generation to improve robustness against disguise attacks," in *Proc. 37th Int. Tech. Conf. Circuits/Syst., Comput. Commun. (ITC-CSCC)*, Jul. 2022, pp. 1038–1041.
- [7] A. M. Alkadi, R. A. AlMahdawi, S. M. Anwahi, and B. Soudan, "Biometric authentication based on multi-modal facial recognition using machine learning," in *Proc. Adv. Sci. Eng. Technol. Int. Conferences (ASET)*, Feb. 2023, pp. 1–6.
- [8] G. Padmashree and K. A. Kotegar, "Skin segmentation-based disguised face recognition using deep learning," *IEEE Access*, vol. 12, pp. 51056–51072, 2024.
- [9] Y. Dodis, L. Reyzin, and A. Smith, "Fuzzy extractors," in *Security With Noisy Data: On Private Biometrics, Secure Key Storage and Anti-Counterfeiting*. Berlin, Germany: Springer, 2007, pp. 79–99.
- [10] Y. Dodis, R. Ostrovsky, L. Reyzin, and A. Smith, "Fuzzy extractors: How to generate strong keys from biometrics and other noisy data," *SIAM J. Comput.*, vol. 38, no. 1, pp. 97–139, Jan. 2008.
- [11] N. Li, F. Guo, Y. Mu, W. Susilo, and S. Nepal, "Fuzzy extractors for biometric identification," in *Proc. IEEE 37th Int. Conf. Distrib. Comput. Syst. (ICDCS)*, Jun. 2017, pp. 667–677.
- [12] J. M. Kirss, "Biometrics in splitkey using fuzzy extraction," *Cybernetica AS*, Tallinn, Estonia, Tech. Rep. D-2-456/2022, 2022.
- [13] E. Grumbling and M. Horowitz, *Quantum Computing: Paragress and Prospects*. Washington, DC, USA: National Academy of Sciences, 2018.
- [14] J. Preskill, "Quantum computing in the NISQ era and beyond," 2018, *arXiv:1801.00862*.
- [15] D. J. Bernstein and L. Tanja, "Post-quantum cryptography," *Nature*, vol. 549, no. 7671, pp. 188–194, 2017.
- [16] R. Overbeck and N. Sendrier, "Code-based cryptography," in *Post-Quantum Cryptography*. Cham, Switzerland: Springer, 2009, pp. 95–145.
- [17] R. J. McEliece, "A public-key cryptosystem based on algebraic," *Coding Thv.*, vol. 4244, pp. 114–116, Apr. 1978.
- [18] I. Chingovska, N. Erdogmus, A. Anjos, and S. Marcel, "Face recognition systems under spoofing attacks," in *Face Recognition Across the Imaging Spectrum*. Singapore: Springer, 2016, pp. 165–194.

- [19] T. V. Hamme, G. Garofalo, S. Joos, D. Preuveneers, and W. Joosen, "Ai for biometric authentication systems," in *Security and Artificial Intelligence: A Crossdisciplinary Approach*. Cham, Switzerland: Springer, 2022, pp. 156–180.
- [20] A. Kuznetsov, A. Kiyani, A. Uvarova, R. Serhienko, and V. Smirnov, "New code based fuzzy extractor for biometric cryptography," in *Proc. Int. Sci.-Practical Conf. Problems InfoCommun. Sci. Technol.*, Oct. 2018, pp. 119–124.
- [21] A. Kuznetsov, D. Zakharov, E. Frontoni, L. Romeo, and R. Rosati, "Science and technology (PIC S&T)," in *Proc. IEEE 9th Int. Conf. Problems Infocommun., Sci. Technol.*, Oct. 2022, pp. 421–426.
- [22] V. P. Parente and J. van de Graaf, "A practical fuzzy extractor for continuous features," in *Proc. Int. Conf. Inf. Theoretic Secur.* Cham, Switzerland: Springer, 2016, pp. 241–258.
- [23] A. Jana, B. Paudel, M. K. Sarker, M. Ebrahimi, P. Hitzler, and G. T. Amariuca, "Neural fuzzy extractors: A secure way to use artificial neural networks for biometric user authentication," 2020, [arXiv:2003.08433](https://arxiv.org/abs/2003.08433).
- [24] I. Buhan, J. Doumen, P. Hartel, and R. Veldhuis, "Fuzzy extractors for continuous distributions," in *Proc. 2nd ACM Symp. Inf., Comput. Commun. Secur.*, Mar. 2007, pp. 353–355.
- [25] E. A. Verbitskiy, P. Tuyls, C. Obi, B. Schoenmakers, and B. Skorik, "Key extraction from general nondiscrete signals," *IEEE Trans. Inf. Forensics Security*, vol. 5, no. 2, pp. 269–279, Jun. 2010.
- [26] G. Zheng, W. Li, and C. Zhan, "Cryptographic key generation from biometric data using lattice mapping," in *Proc. 18th Int. Conf. Pattern Recognit. (ICPR)*, 2006, pp. 513–516.
- [27] Y. Tang, F. Gao, J. Feng, and Y. Liu, "FingerNet: An unified deep network for fingerprint minutiae extraction," in *Proc. IEEE Int. Joint Conf. Biometrics (IJCB)*, Oct. 2017, pp. 108–116.
- [28] 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.
- [29] D. Menotti, G. Chiachia, A. Pinto, W. R. Schwartz, H. Pedrini, A. X. Falcão, and A. Rocha, "Deep representations for iris, face, and fingerprint spoofing detection," *IEEE Trans. Inf. Forensics Security*, vol. 10, no. 4, pp. 864–879, Apr. 2015.
- [30] J. J. Engelsma, K. Cao, and A. K. Jain, "Fingerprints: Fixed length representation via deep networks and domain knowledge," 2019, [arXiv:1904.01099](https://arxiv.org/abs/1904.01099).
- [31] W.-S. Jeon and S.-Y. Rhee, "Fingerprint pattern classification using convolution neural network," *Int. J. FUZZY Log. Intell. Syst.*, vol. 17, no. 3, pp. 170–176, Sep. 2017.
- [32] 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.
- [33] P. K. Nayak and D. Narayan, "Multimodal biometric face and fingerprint recognition using neural network," *Int. J. Eng.*, vol. 1, no. 10, pp. 1–6, 2012.
- [34] B. Stojanovic, A. Neskovic, and O. Marques, "A novel neural network based approach to latent overlapped fingerprints separation," *Multim. Tools Appl.*, vol. 76, no. 10, pp. 12775–12799, 2017.
- [35] R. F. Nogueira, R. de Alencar Lotufo, and R. Campos Machado, "Fingerprint liveness detection using convolutional neural networks," *IEEE Trans. Inf. Forensics Security*, vol. 11, no. 6, pp. 1206–1213, Jun. 2016.
- [36] A. Page, A. Kulkarni, and T. Mohsenin, "Utilizing deep neural nets for an embedded ECG-based biometric authentication system," in *Proc. IEEE Biomed. Circuits Syst. Conf. (BioCAS)*, Oct. 2015, pp. 1–4.
- [37] V. Mai, I. Khalil, and C. Meli, "ECG biometric using multilayer perceptron and radial basis function neural networks," in *Proc. Annu. Int. Conf. IEEE Eng. Med. Biol. Soc.*, Aug. 2011, pp. 2745–2748.
- [38] R. Salloum and C.-C. J. Kuo, "ECG-based biometrics using recurrent neural networks," in *Proc. IEEE Int. Conf. Acoust. Speech Signal Process. (ICASSP)*, May 2017, pp. 2062–2066.
- [39] R. Donida Labati, E. Muñoz, V. Piuri, R. Sassi, and F. Scotti, "Deep-ECG: Convolutional neural networks for ECG biometric recognition," *Pattern Recognit. Lett.*, vol. 126, pp. 78–85, Sep. 2019.
- [40] H. El Khiyari and H. Wechsler, "Face recognition across time lapse using convolutional neural networks," *J. Inf. Secur.*, vol. 7, no. 3, pp. 141–151, 2016.
- [41] A. Arakala, J. Jeffers, and K. J. Horadam, "Fuzzy extractors for minutiae-based fingerprint authentication," in *Proc. Adv. Biometrics, Int. Conf.*, Seoul, South Korea. Cham, Switzerland: Springer, Aug. 2007, pp. 760–769.
- [42] W. Yang, J. Hu, and S. Wang, "A Delaunay triangle-based fuzzy extractor for fingerprint authentication," in *Proc. IEEE 11th Int. Conf. Trust, Secur. Privacy Comput. Commun.*, Apr. 2012, pp. 66–70.
- [43] K. Xi, J. Hu, and F. Han, "An alignment free fingerprint fuzzy extractor using near-equivalent dual layer structure check (NeDLSC) algorithm," in *Proc. 6th IEEE Conf. Ind. Electron. Appl.*, Jun. 2011, pp. 1040–1045.
- [44] Q. Li, M. Guo, and E.-C. Chang, "Fuzzy extractors for asymmetric biometric representations," in *Proc. IEEE Comput. Soc. Conf. Comput. Vis. Pattern Recognit. Workshops*, Jun. 2008, pp. 1–6.
- [45] V. V. T. Tong, H. Sibert, J. Lecœur, and M. Girault, "Biometric fuzzy extractors made practical: A proposal based on fingerprints," in *Proc. Adv. Biometrics, Int. Conf.*, Seoul, South Korea. Cham, Switzerland: Springer, Aug. 2007.
- [46] R. Álvarez Mariño, F. Hernández Álvarez, and L. Hernández Encinas, "A crypto-biometric scheme based on iris-templates with fuzzy extractors," *Inf. Sci.*, vol. 195, pp. 91–102, Jul. 2012.
- [47] F. H. Álvarez, L. H. Encinas, and C. S. Ávila, "Biometric fuzzy extractor scheme for iris templates," in *Proc. Int. Conf. Secur. Manage.*, 2009, pp. 1–8.
- [48] J. Bringer, H. Chabanne, G. Cohen, B. Kindarji, and G. Zemor, "Optimal iris fuzzy sketches," in *Proc. 1st IEEE Int. Conf. Biometrics, Theory, Appl. Syst.*, Aug. 2007, pp. 1–8.
- [49] Y. Sutcu, Q. Li, and N. Memon, "Design and analysis of fuzzy extractors for faces," *Proc. SPIE*, vol. 7306, pp. 327–338, May 2009.
- [50] T. Hoang and D. Choi, "Secure and privacy enhanced gait authentication on smart phone," *Sci. World J.*, vol. 2014, no. 1, 2014, Art. no. 438254.
- [51] T. Hoang, D. Choi, and T. Nguyen, "Gait authentication on mobile phone using biometric cryptosystem and fuzzy commitment scheme," *Int. J. Inf. Secur.*, vol. 14, no. 6, pp. 549–560, Nov. 2015.
- [52] A. K. Das, "A secure and effective biometric-based user authentication scheme for wireless sensor networks using smart card and fuzzy extractor," *Int. J. Commun. Syst.*, vol. 30, no. 1, p. e2933, Jan. 2017.
- [53] D. Gu, I. Verbauwhede, M. Hiller, and M. Yu, "Efficient fuzzy extraction of PUF-induced secrets: Theory and applications," in *Proc. Int. Conf. Cryptograph. Hardw. Embedded Syst.* Cham, Switzerland: Springer, 2016, pp. 412–431.
- [54] Z. Liao, G. T. Amariuca, R. K. W. Wong, and Y. Guan, "The impact of discharge inversion effect on learning SRAM power-up statistics," in *Proc. Asian Hardw. Oriented Secur. Trust Symp. (AsianHOST)*, Oct. 2017, pp. 31–36.
- [55] S. Pirbhulal, H. Zhang, W. Wu, S. C. Mukhopadhyay, and Y.-T. Zhang, "Heartbeats based biometric random binary sequences generation to secure wireless body sensor networks," *IEEE Trans. Biomed. Eng.*, vol. 65, no. 12, pp. 2751–2759, Dec. 2018.
- [56] P. Kumari and T. Anjali, "Securing a body sensor network," in *Proc. 9th Int. Conf. Commun. Syst. Netw. (COMSNETS)*, Jan. 2017, pp. 514–519.
- [57] V. H. Dao, Q. D. Tran, and T. H. L. Nguyen, "A multibiometric encryption key algorithm using fuzzy vault to protect private key in BioPKI based security system," in *Proc. IEEE RIVF Int. Conf. Comput. Commun. Technol., Res., Innov. Vis. Future (RIVF)*, Nov. 2010, pp. 1–6.
- [58] P. L. Chelani and S. T. Bagde, "Detecting collaborative attacks by malicious nodes in MANET: An improved bait detection scheme," in *Proc. Int. Conf. Commun. Electron. Syst. (ICCES)*, Oct. 2016, pp. 1–6.
- [59] U. Cheema and S. Moon, "Sejong face database: A multi-modal disguise face database," *Comput. Vis. Image Understand.*, vols. 208–209, Jul. 2021, Art. no. 103218.
- [60] S. Wang, Z. Liu, S. Lv, Y. Lv, G. Wu, P. Peng, F. Chen, and X. Wang, "A natural visible and infrared facial expression database for expression recognition and emotion inference," *IEEE Trans. Multimedia*, vol. 12, no. 7, pp. 682–691, Nov. 2010.
- [61] S. Wang, Z. Liu, Z. Wang, G. Wu, P. Shen, S. He, and X. Wang, "Analyses of a multimodal spontaneous facial expression database," *IEEE Trans. Affect. Comput.*, vol. 4, no. 1, pp. 34–46, Jan. 2013.
- [62] P. J. Flynn, K. W. Bowyer, and P. J. Phillips, "Assessment of time dependency in face recognition: An initial study," in *Audio- and Video-Based Biometric Person Authentication*. Cham, Switzerland: Springer, Jun. 2003.
- [63] X. Chen, P. J. Flynn, and K. W. Bowyer, "IR and visible light face recognition," *Comput. Vis. Image Understand.*, vol. 99, no. 3, pp. 332–358, Sep. 2005.

- [64] S. Li, D. Yi, Z. Lei, and S. Liao, "The casia nir-vis 2.0 face database," in *Proc. IEEE Conf. Comput. Vis. Pattern Recognit. Workshops*, 2013, pp. 348–353.
- [65] H.-W. Ng and S. Winkler, "A data-driven approach to cleaning large face datasets," in *Proc. IEEE Int. Conf. Image Process. (ICIP)*, Oct. 2014, pp. 343–347.
- [66] X. Wang and X. Tang, "Face photo-sketch synthesis and recognition," *IEEE Trans. Pattern Anal. Mach. Intell.*, vol. 31, no. 11, pp. 1955–1967, Nov. 2008.
- [67] A. Martinez and R. Benavente, "The ar face database: Cvc technical report, 24," Comput. Vis. Center (CVC), Barcelona, Spain, Tech. Rep. 24, 1998.
- [68] K. Messer, J. Matas, J. Kittler, J. Luetttin, and G. Maitre, "XM2 VTSDB: The extended M2 VTS database," in *Proc. 2nd Int. Conf. Audio Video-Based Biometric Person Authentication*, Princeton, NY, USA, 1999, pp. 965–966.
- [69] T. I. Dhamecha, A. Nigam, R. Singh, and M. Vatsa, "Disguise detection and face recognition in visible and thermal spectrums," in *Proc. Int. Conf. Biometrics (ICB)*, Jun. 2013, pp. 1–8.
- [70] T. I. Dhamecha, R. Singh, M. Vatsa, and A. Kumar, "Recognizing disguised faces: Human and machine evaluation," *PLoS ONE*, vol. 9, no. 7, Jul. 2014, Art. no. e99212.
- [71] H. Steiner, A. Kolb, and N. Jung, "Reliable face anti-spoofing using multispectral SWIR imaging," in *Proc. Int. Conf. Biometrics (ICB)*, Jun. 2016, pp. 1–8.
- [72] H. Steiner, S. Sporrer, A. Kolb, and N. Jung, "Design of an active multispectral SWIR camera system for skin detection and face verification," *J. Sensors*, vol. 2016, pp. 1–16, Jul. 2016.
- [73] R. Raghavendra, N. Vetrekar, K. B. Raja, R. S. Gad, and C. Busch, "Detecting disguise attacks on multi-spectral face recognition through spectral signatures," in *Proc. 24th Int. Conf. Pattern Recognit. (ICPR)*, Aug. 2018, pp. 3371–3377.
- [74] H. S. Bhatt, S. Bharadwaj, R. Singh, and M. Vatsa, "Memetically optimized MCWLD for matching sketches with digital face images," *IEEE Trans. Inf. Forensics Security*, vol. 7, no. 5, pp. 1522–1535, Oct. 2012.
- [75] Y. Fu, T. M. Hospedales, T. Xiang, S. Gong, and Y. Yao, "Interestingness prediction by robust learning to rank," in *Proc. European Conf. Comput. Vis. Cham, Switzerland: Springer*, 2014, pp. 488–503.
- [76] L. J. Karam and T. Zhu, "Quality labeled faces in the wild (QLFW): A database for studying face recognition in real-world environments," *Proc. SPIE*, vol. 9394, pp. 87–96, Mar. 2015.
- [77] F. S. Samaria and A. C. Harter, "Parameterisation of a stochastic model for human face identification," in *Proc. IEEE Workshop Appl. Comput. Vis.*, Jun. 1994, pp. 138–142.
- [78] A. S. Georghiades, P. N. Belhumeur, and D. J. Kriegman, "From few to many: Illumination cone models for face recognition under variable lighting and pose," *IEEE Trans. Pattern Anal. Mach. Intell.*, vol. 23, no. 6, pp. 643–660, Jun. 2001.
- [79] P. J. Phillips, H. Wechsler, J. Huang, and P. J. Rauss, "The FERET database and evaluation procedure for face-recognition algorithms," *Image Vis. Comput.*, vol. 16, no. 5, pp. 295–306, Apr. 1998.
- [80] R. Gross, I. Matthews, J. Cohn, T. Kanade, and S. Baker, "Multi-pie," *IVC*, vol. 28, no. 5, pp. 807–813, 2010.
- [81] D. B. Graham and N. M. Allinson, "Characterising virtual eigensignatures for general purpose face recognition," in *Face Recognition: From Theory To Applications*. Cham, Switzerland: Springer, 1998, pp. 446–456.
- [82] A. Lanitis, C. Draganova, and C. Christodoulou, "Comparing different classifiers for automatic age estimation," *IEEE Trans. Syst., Man Cybern., B (Cybern.)*, vol. 34, no. 1, pp. 621–628, Feb. 2004.
- [83] C. McCool, S. Marcel, A. Hadid, M. Pietikäinen, P. Matejka, J. Cernocký, N. Poh, J. Kittler, A. Larcher, C. Lévy, D. Matrouf, J.-F. Bonastre, P. Tresadern, and T. Cootes, "Bi-modal person recognition on a mobile phone: Using mobile phone data," in *Proc. IEEE Int. Conf. Multimedia Expo Workshops*, Jul. 2012, pp. 635–640.
- [84] K. Panetta, Q. Wan, S. Agaian, S. Rajeev, S. Kamath, R. Rajendran, S. P. Rao, A. Kaszowska, H. A. Taylor, A. Samani, and X. Yuan, "A comprehensive database for benchmarking imaging systems," *IEEE Trans. Pattern Anal. Mach. Intell.*, vol. 42, no. 3, pp. 509–520, Mar. 2020.
- [85] S. Zhang, A. Liu, J. Wan, Y. Liang, G. Guo, S. Escalera, H. J. Escalante, and S. Z. Li, "CASIA-SURF: A large-scale multi-modal benchmark for face anti-spoofing," *IEEE Trans. Biometrics, Behav., Identity Sci.*, vol. 2, no. 2, pp. 182–193, Apr. 2020.
- [86] H. S. Bhatt, S. Bharadwaj, R. Singh, and M. Vatsa, "On matching sketches with digital face images," in *Proc. 4th IEEE Int. Conf. Biometrics, Theory, Appl. Syst. (BTAS)*, 2010, pp. 1–7.
- [87] F. Pujol, M. Pujol, A. Jimeno-Morenilla, and M. Pujol, "Face detection based on skin color segmentation using fuzzy entropy," *Entropy*, vol. 19, no. 1, p. 26, Jan. 2017.
- [88] S. Ramalingam, "Fuzzy interval-valued multi criteria based decision making for ranking features in multi-modal 3D face recognition," *Fuzzy Sets Syst.*, vol. 337, pp. 25–51, Apr. 2018.
- [89] V. Chatzis, A. G. Bors, and I. Pitas, "Multimodal decision-level fusion for person authentication," *IEEE Trans. Syst., Man, Cybern. A, Syst. Humans*, vol. 29, no. 6, pp. 674–680, Jun. 1999.
- [90] K.-C. Kwak and W. Pedrycz, "Face recognition using a fuzzy Fisherface classifier," *Pattern Recognit.*, vol. 38, no. 10, pp. 1717–1732, Oct. 2005.
- [91] X. Li and A. Song, "Fuzzy MSD based feature extraction method for face recognition," *Neurocomputing*, vol. 122, pp. 266–271, Dec. 2013.
- [92] W. Yang, H. Yan, J. Wang, and J. Yang, "Face recognition using complete fuzzy LDA," in *Proc. 19th Int. Conf. Pattern Recognit.*, Dec. 2008, pp. 1–4.
- [93] Y. Zheng, J. Yang, W. Wang, Q. Wang, J. Yang, and X. Wu, "Fuzzy kernel Fisher discriminant algorithm with application to face recognition," in *Proc. 6th World Congr. Intell. Control Autom.*, 2006, pp. 9669–9672.
- [94] Y. Zheng, Z. Xu, and X. Wang, "The fusion of deep learning and fuzzy systems: A state-of-the-art survey," *IEEE Trans. Fuzzy Syst.*, vol. 30, no. 8, pp. 2783–2799, Aug. 2022.
- [95] R. S. T. Lee, "Chaotic type-2 transient-fuzzy deep neuro-oscillatory network (CT2TFDNN) for worldwide financial prediction," *IEEE Trans. Fuzzy Syst.*, vol. 28, no. 4, pp. 731–745, Apr. 2020.
- [96] T.-C. Lin, C.-H. Kuo, and V. E. Balas, "Real-time recurrent interval type-2 fuzzy-neural system identification using uncertainty bounds," in *Proc. IEEE Int. Conf. Fuzzy Syst.*, Jun. 2012, pp. 1–8.
- [97] X. Chen, D. Li, P. Wang, and X. Yang, "A deep convolutional neural network with fuzzy rough sets for FER," *IEEE Access*, vol. 8, pp. 2772–2779, 2020.
- [98] M. Guzel, I. Kok, D. Akay, and S. Ozdemir, "ANFIS and deep learning based missing sensor data prediction in IoT," *Concurrency Comput., Pract. Exper.*, vol. 32, no. 2, p. e5400, 2020.
- [99] W. L. Tung and C. Quek, "Financial volatility trading using a self-organising neural-fuzzy semantic network and option straddle-based approach," *Expert Syst. Appl.*, vol. 38, no. 5, pp. 4668–4688, May 2011.
- [100] X. Zhang, J. Zhou, and W. Chen, "Data-driven fault diagnosis for PEMFC systems of hybrid tram based on deep learning," *Int. J. Hydrogen Energy*, vol. 45, no. 24, pp. 13483–13495, May 2020.
- [101] V. Anitha, N. R. Behera, P. V. Krishna, R. NamdeoraoJogekar, and K. Singh, "Detection of lung cancer using optimal hybrid segmentation and classification," *Int. J. Comput. Inf. Syst. Ind. Manage. Appl.*, vol. 15, p. 11, Jan. 2023.
- [102] Z. Zhang, M. Huang, S. Liu, B. Xiao, and T. S. Durrani, "Fuzzy multilayer clustering and fuzzy label regularization for unsupervised person reidentification," *IEEE Trans. Fuzzy Syst.*, vol. 28, no. 7, pp. 1356–1368, Jul. 2020.
- [103] L. Chen, W. Su, M. Wu, W. Pedrycz, and K. Hirota, "A fuzzy deep neural network with sparse autoencoder for emotional intention understanding in Human–Robot interaction," *IEEE Trans. Fuzzy Syst.*, vol. 28, no. 7, pp. 1252–1264, Jul. 2020.
- [104] R. K. Mahendran and P. Velusamy, "A secure fuzzy extractor based biometric key authentication scheme for body sensor network in Internet of medical things," *Comput. Commun.*, vol. 153, pp. 545–552, Mar. 2020.
- [105] O. Kuznetsov, "Achieving enhanced security in biometric authentication: A rigorous analysis of code-based fuzzy extractor," in *Proc. IT&I*, 2023, pp. 330–339.
- [106] G. Hua, L. Schintler, and C. McNeely, "Facial recognition technologies, in encyclopedia of big data," in *Encyclopedia of Big Data*. Cham, Switzerland: Springer, 2022, pp. 475–479.
- [107] A. S. Rajawat, P. Bedi, S. B. Goyal, P. Bhaladhare, A. Aggarwal, and R. S. Singhal, "Fusion fuzzy logic and deep learning for depression detection using facial expressions," *Proc. Comput. Sci.*, vol. 218, pp. 2795–2805, Apr. 2023.
- [108] J. Hou, "Deep learning-based human emotion detection framework using facial expressions," *J. Interconnection Netw.*, vol. 22, no. 1, Mar. 2022, Art. no. 2141018.
- [109] B. Ghansah, "Convolutional locality-sensitive dictionary learning for facial expressions detection," *Int. J. Data Analytics*, vol. 3, no. 1, pp. 1–28, Mar. 2022.

- [110] S. Aggarwal, S. K. Tomar, and A. Aggarwal, "Performance analysis of soft handoff algorithm using fuzzy logic in CDMA systems," in *Proc. 2nd IEEE Int. Conf. Parallel, Distrib. Grid Comput.*, Dec. 2012, pp. 586–591.
- [111] A. Kumar, A. Aggarwal, and Charu, "Performance analysis of MANET using elliptic curve cryptosystem," in *Proc. 14th Int. Conf. Adv. Commun. Technol. (ICACT)*, Feb. 2012, pp. 201–206.
- [112] T. Hata and Y. Miyagi, "Recognition of fetal facial expressions using artificial intelligence deep learning," *Donald School J. Ultrasound Obstetrics Gynecol.*, vol. 15, no. 3, pp. 223–228, Sep. 2021.
- [113] M. K. Goyal and A. Aggarwal, "Composing signatures for misuse intrusion detection system using genetic algorithm in an offline environment," in *Proc. Adv. Comput. Inf. Technol., Proc. 2nd Int. Conf. Adv. Comput. Inf. Technol. (ACITY)*, vol. 1. Cham, Switzerland: Springer, 2012, pp. 151–157.
- [114] M. Chakradar, A. Aggarwal, X. Cheng, A. Rani, M. Kumar, and A. Shankar, "A non-invasive approach to identify insulin resistance with triglycerides and HDL-c ratio using machine learning," *Neural Process. Lett.*, vol. 55, no. 1, pp. 93–113, Feb. 2023.
- [115] X. Li, "Face recognition method based on fuzzy 2DPCA," *J. Electr. Comput. Eng.*, vol. 2014, pp. 1–7, May 2014.
- [116] A. Oulefki, A. Mustapha, E. Boutellaa, M. Bengherabi, and A. A. Tifarine, "Fuzzy reasoning model to improve face illumination invariance," *Signal, Image Video Process.*, vol. 12, no. 3, pp. 421–428, Mar. 2018.
- [117] P. Huang, G. Gao, C. Qian, G. Yang, and Z. Yang, "Fuzzy linear regression discriminant projection for face recognition," *IEEE Access*, vol. 5, pp. 4340–4349, 2017.
- [118] C. Campomanes-Álvarez, B. R. Campomanes-Álvarez, S. Guadarrama, O. Ibáñez, and O. Córdón, "An experimental study on fuzzy distances for skull-face overlay in craniofacial superimposition," *Fuzzy Sets Syst.*, vol. 318, pp. 100–119, Jul. 2017.
- [119] Y. Du, X. Lu, W. Zeng, and C. Hu, "A novel fuzzy linear discriminant analysis for face recognition," *Intell. Data Anal.*, vol. 22, no. 3, pp. 675–696, May 2018.
- [120] J. K. Sing, A. Dey, and M. Ghosh, "Confidence factor weighted Gaussian function induced parallel fuzzy rank-level fusion for inference and its application to face recognition," *Inf. Fusion*, vol. 47, pp. 60–71, May 2019.
- [121] M. Rejeesh, "Interest point based face recognition using adaptive neuro fuzzy inference system," *Multimedia Tools Appl.*, vol. 78, no. 16, pp. 22691–22710, Aug. 2019.
- [122] W. Ali, W. Tian, S. U. Din, D. Iradukunda, and A. A. Khan, "Classical and modern face recognition approaches: A complete review," *Multimedia Tools Appl.*, vol. 80, no. 3, pp. 4825–4880, Jan. 2021.



**GEORGE KUMI KYEREMEH** was born in Ghana. He received the B.Sc. degree in electrical engineering from the Kwame Nkrumah University of Science and Technology, Ghana, and the M.Sc. degree in advanced biomedical engineering and the Ph.D. degree in the development of novel multimodal biometrics system by fusing fingerprint and finger vein from the University of Bradford, U.K., in 2020. He was a Research Fellow with European Union's Horizon-MSCA-RISE-2019-2024, Marie

Skłodowska-Curie, Research, and Innovation Staff Exchange (RISE) program, titled: Secure and Wireless Multimodal Biometric Scanning Device for Passenger Verification Targeting Land and Sea Border Control. He contributes to regenerative medicine and tissue engineering, specifically, stem cell niche microenvironment. His research interest includes fingerprint and finger vein recognition.

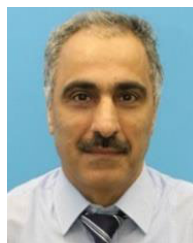


**RAMI QAHWAJI** (Senior Member, IEEE) received the M.Sc. degree in control and computer engineering and the Ph.D. degree in AI and signal/image processing. He is currently a Professor of visual computing with the University of Bradford. He has been with different industries in the fields of satellite/space imaging, communications, remote sensing, digital health and imaging, biometrics, AI, and data visualization developing intelligent systems in collaboration with NASA,

ESA, NHS, and different SMEs. He attracted millions of pounds in research funding from various U.K. and European funding agencies. He has over 140 refereed journal and conference publications and has been invited to deliver many keynote speeches at national and international conferences. He has supervised 31 completed Ph.D. projects and is an external examiner for several U.K. and international universities. He is heavily involved in the organization of international activities and public engagement events. He is a fellow of the Institution of Engineering and Technology, a Chartered Engineer, a fellow of the Higher Education Academy, an IET Technical Assessor, and sets on the IET's Healthcare Sector Executive Committee.



**MOHAMED ABDUL-AL** was born in Sidon, Lebanon. He received the B.Sc. degree in computer and communication engineering with a minor in biomedical engineering and biomedical sciences from American University of Science and Technology, Beirut, Lebanon, and the M.Sc. degree in advanced biomedical engineering and the Ph.D. degree in the development of novel multimodal biometrics system by fusing face and infrared information from the University of Bradford, U.K., in 2020. He was a Research Fellow with European Union's Horizon-MSCA-RISE-2019-2024, Marie Skłodowska-Curie, Research, and Innovation Staff Exchange (RISE) program, titled: Secure and Wireless Multimodal Biometric Scanning Device for Passenger Verification Targeting Land and Sea Border Control. He contributes to wireless communication and radio frequencies. In addition, he is involved in regenerative medicine and tissue engineering, specifically, the development of biomaterials for breast reconstruction, stem cell niche microenvironment, glioblastoma, and encapsulation techniques in the ocular and respiratory systems. His research interests include face recognition using different modalities, such as visible, infrared, thermal, and visible and infrared.



**NAZAR T. ALI** (Senior Member, IEEE) received the Ph.D. degree in electrical and electronic engineering from the University of Bradford, U.K., in 1990. From 1990 to 2000, he held various posts with the University of Bradford, as a Researcher and a Lecturer. He worked on many collaborative research projects in U.K., under the umbrella of the Centre of Research Excellence, the Department of Trade and Industry (DTI), and EPSERC. This involved a consortium of a number of universities and industrial companies. He is currently an Associate Professor with Khalifa University, United Arab Emirates. He has more than 100 papers published in peer-reviewed high-quality journals and conferences. His current research interests include antennas and RF circuits and systems, indoor and outdoor localization techniques, and RF measurements.



**RAED A. ABD-ALHAMEED** (Senior Member, IEEE) has been a Research Visitor with Wrexham University, Wales, since 2009, covering the wireless and communications research areas, and an Adjunct Professor with the College of Electronics Engineering, Ninevah University, since 2019, and the Department of Information and Communication Engineering, College of Science and Technology, Basrah University, Basrah, Iraq. He is currently a Professor of electromagnetic and

radiofrequency engineering with the University of Bradford, U.K. He is also the Leader of radiofrequency, propagation, sensor design, and signal processing of the School of Engineering and Informatics, University of Bradford, where he is also leading the Communications Research Group. He is a Chartered Engineer. He has many years of research experience in the areas of radio frequency, signal processing, propagations, antennas, and electromagnetic computational techniques. He is a Principal Investigator for several funded applications to EPSRCs, Innovate U.K., and British Council, and the Leader of several successful knowledge Transfer Programs, such as with Arris (previously known as Pace plc), Yorkshire Water plc, Harvard Engineering plc, IETG Ltd., Seven Technologies Group, Emkay Ltd., and Two World Ltd. He has also been a co-investigator in several funded research projects, including H2020-MSCA-RISE-2024-2028, total, £1.2 million, UoB share £2204 k; Marie Skłodowska-Curie, Research and Innovation Staff Exchange (RISE), titled “6G Terahertz Communications for Future Heterogeneous Wireless Network;” HORIZON-MSCA-2021-SE-01-01, Type of Action: HORIZON-TMA-MSCA-SE 2023-2027: ROBUST: Proposal titled “Ubiquitous eHealth Solution for Fracture

Orthopaedic Rehabilitation;” Horizon 2020 Research and Innovation Program; H2020 MARIE Skłodowska-CURIE ACTIONS: Innovative Training Networks Secure Network Coding for Next Generation Mobile Small Cells 5G-US; European Space Agency: Satellite Network of Experts V, Work Item 2.6: Frequency selectivity in phase-only beamformed user terminal direct radiating arrays; Nonlinear and Demodulation Mechanisms in Biological Tissue (Department of Health, Mobile Telecommunications and Health Research Program; and Assessment of the Potential Direct Effects of Cellular Phones on the Nervous System (EU: collaboration with six other major research organizations across Europe). He has published more than 800 academic journals and conference papers; in addition, he has co-authored seven books and several book chapters, including seven patents. His research interests include computational methods and optimizations, wireless and mobile communications, sensor design, EMC, beam steering antennas, energy-efficient PAs, and RF predistorter design applications. He is a fellow of the Institution of Engineering and Technology and the Higher Education Academy. He was a recipient of the Business Innovation Award for the successful KTP with Pace and Datong companies on the design and implementation of MIMO sensor systems and antenna array design for service localizations. He is the chair of several successful workshops on energy-efficient and reconfigurable transceivers: approach toward energy conservation and CO2 reduction that addresses the biggest challenges for future wireless systems. He has been the General Chair of the IMDC-IST International Conference, since 2020; a Co-Editor of *Electronics* (MDPI), since 2019; and a Guest Editor of *IET Science, Measurement and Technology*, since 2009.

• • •