Adaptive Weighted Graph Approach to Generate Multimodal Cancelable Biometric Templates

Gurjit Singh Walia, *Senior Member, IEEE*, Gaurav Jain, *Student Member, IEEE,* Nipun Bansal, *Member, IEEE,* and Kuldeep Singh, *Senior Member, IEEE*

***Abstract*— Multimodal biometric systems offer numerous advantages over unimodal counterparts and are being used extensively in diverse applications. However, fusion of biometric data is a non-trivial task and curtail employability of multimodal systems for a varying set of biometric characteristics with different type and dimension. Moreover, comprehensive solutions against adversary attacks that ensure template protection and prevent presentation attacks are not in place. In this article, a secure multimodal cancelable biometric system is proposed to address these concerns. This approach introduces key images based generic feature extraction technique which reduces feature dimension and achieves revocability. The non-invertibility and unlinkability are ensured through cross-diffusion of complementary information from different modalities. A new feature fusion method based on an adaptive graph is proposed to generate multimodal cancelable biometric templates. Robustness against presentation attack is accomplished through quality based adaptation of features. Extensive experimentation is performed on benchmark databases for fingerprint, face, and iris, to illustrate the efficacy of multimodal cancelable templates. The proposed approach is shown to perform favorably against state-of-the-art feature fusion methods. Furthermore, the resilience of the proposed approach against security and privacy attacks is demonstrated.**

***Index Terms*— Multimodal, cancelable, adaptive, fusion.**

I. INTRODUCTION

BIOMETRIC recognition systems are being extensively employed for security-critical applications. The rapid proliferation of biometric systems and their application in cloud environments has led to various concerns regarding system security and potential privacy breaches. These systems store biometric data that can be vulnerable not only to adversary attacks via public network but also to elicit disclosure under captive environments. Biometric data is considered as a piece of sensitive information because unlike passwords, biometric characteristics can neither be reissued nor be revoked. Compromise of biometric data results in permanent loss of an individual's identity, and hence, is a growing concern in today's digital world. Biometric systems can be compromised mainly due to issues, which can be loosely classified as: (1) *template database leakage*, and (2) *presentation attacks* (e.g., using gummy fingers, face mask, dismembered fingers from a legitimate user) [1]. While presentation attacks can induce illegitimate access, template leakage may risk in covert hearing and unauthorized access to private information. Hence, these vulnerabilities may incapacitate the application of biometric systems under cloud environments via public networks.

To protect biometric data, the concept of *cancelable biometrics* was introduced by Ratha *et al.* [2]. It involves an intentional transformation of original biometric templates such that enrolment and verification are performed in the transformed domain. Transformed templates should be robust to adversary attacks and hence must satisfy the following properties, (1) *Revocability*, (2) *Unlinkability*, (3) *Non-invertibility*, while preserving the (4) *Performance* [3]. Generally, cancelable biometric approaches can be classified into (1) *Biometric salting*, and (2) *Non-invertible transforms*. In biometric salting, the biometric template is mixed with an artificial pattern which may be random noise or synthetic pattern. The dilemma in deciding the relative magnitude of the noise to be added makes it difficult to employ salting techniques. Besides, if the artificial pattern is stolen, the original biometric characteristic can be extracted [4]. In contrast, non-invertible transformation based cancelable approaches mutate the original biometric templates such that it is infeasible to invert the transformed template. Predominantly used non-invertible transformation techniques are *Random Projections* [5], *Bloom Filters* [6], and *Biohashing* [7]. However, most of the non-invertible transform-based cancelable approaches were demonstrated for unimodal biometric systems [8], [9]. In unimodal systems, the trade-off between security and performance limits the success of cancelable approaches. Besides, unimodal systems suffer from the inevitable issues of non-universality, noisy data, inter-class variation, and presentation attacks.

Recently, cancelable biometrics has been extended from unimodal systems to multimodal systems [10]. Generally, multimodal systems are employed to compensate for the loss in accuracy and prevent presentation attacks [11]. Typically, multimodal schemes can be classified on the basis of the kind of information being fused such as *feature level* [6], *decision level* [11] , and *score level* [12]. Being more discriminative, feature level fusion is preferred over score or decision level fusion [11]. However, feature level fusion is limitedly investigated due to different type and dimension of captured biometric samples extracted from multiple sensors.

Manuscript received March 27, 2019; revised September 17, 2019 and November 2, 2019; accepted November 8, 2019. Date of publication November 20, 2019; date of current version January 27, 2020. The associate editor coordinating the review of this manuscript and approving it for publication was Dr. Karthik Nandakumar. *(Corresponding author: Gurjit Singh Walia.)*

G. S. Walia is with the SAG, Defence Research and Development Organization, New Delhi 110054, India (e-mail: gurjit.walia@gmail.com).

G. Jain and N. Bansal are with the Department of Computer Science and Engineering, Delhi Technological University, New Delhi 110042, India.

K. Singh is with the Department of Electronics and Communication Engineering, Malviya National Institute of Technology, Jaipur 302017, India.

Digital Object Identifier 10.1109/TIFS.2019.2954779

Additionally, presentation attacks were avoided through liveness detection which mainly exploits the image quality for its realisation [13]–[16]. However, most of the liveness detection approaches do not address template protection and adaptive fusion of multiple modalities. In sum, exhaustive solutions that cater to adversary attacks, and also maintains high performance are limitedly investigated. Our method is a comprehensive solution for multimodal biometric recognition that not only provides complete non-invertibility of the template but also drastically reduces feature dimension. Proposed key-based weighted graph fusion can be adapted to any modality irrespective of its dimension and type.

The rest of the paper is organized as follows: In Section II, closely related literature work is reviewed. In Section III, limitations of the existing works, and our contributions are highlighted. In Section IV we present the proposed multibiometric recognition system along with the cancelable template generation approach. Further, we perform experimental validation in Section V. Privacy and security of the proposed method are analyzed in Section VI. Finally, concluding remarks and future directions are drawn in Section VII.

II. Related Work

Biometric security has been rigorously investigated over the past decades. Readers are advised to refer the papers [3], [4] for detailed solutions for biometric security and privacy preservances. In this section, we categorically review the closely related literature mainly considering non-invertible transform for cancelable feature generation and also, countermeasures against presentation attacks.

Rathgeb *et al.* [17] introduced a bloom filter based non-invertible transform for template protection. In this approach, biometric features were mapped to an irreversible representation i.e. bloom filters. Further, unlinkability was achieved using an application-specific token. But, it was later proved by Bringer *et al.* [18] that bloom filter was susceptible to cross-matching attacks. To overcome this issue, Sadhya and Singh [19] proposed a modified approach on bloom filter, where application-specific token T, was replaced with a key matrix κ. However, this approach performed comparison in the original domain instead of the transformed domain and hence, it was prone to security concerns. Recently, Gomez- Barrero *et al.* [6] proposed a generic approach to generate cancelable biometric templates based on bloom filters. In this, the value of keys was computed through statistical analysis of the key features. Mostly, bloom filter based approaches for template protection fail to address the issues of unlinkability and cross-matching attacks [6], [18].

Besides bloom filters, random projections have also been explored to generate cancelable biometric templates. Recently, Kaur and Khanna [20] proposed a template transformation technique dubbed as Random Distance Method (RDM) for generating dimensionally reduced templates. However, non-invertibility was not an inherent property of RDM and was achieved by applying median filtering over the transformed templates. This work on RDM was further extended to address the security issues in cloud-based remote biometric authentication scenarios [21]. On similar lines, Qui *et al.* [22] experimentally validated that a certain amount of added noise can induce cancelable properties while still meeting the accuracy standards. The authors generated cancelable palmprint templates through random comparison and noise data. Further, hashing based approaches extend the random projection-based approaches by exploiting the properties of hash functions. For instance, Dwivedi *et al.* [23] employed a look-up table to generate cancelable iris templates. The look-up table was used to map a decimal encoded vector which was generated from the binary features. However, using a look-up table makes the approach vulnerable to inversion attacks, if the transformed features and look-up table are compromised. Sadhya and Raman [24], proposed a locality sensitive hashing based approach, dubbed as locality sampled code (LSC), to generate cancelable IrisCodes features. Despite generating a secure template with good recognition performance, this technique was limited to unimodal biometric systems having binary feature representations. Lai *et al.* [8] introduced "Indexing-First-One" (IFO) hashing to transform real-valued features into hashed code to generate cancelable iris templates. Similarly, Jin *et al.* [9] generated fingerprint cancelable templates using "Index-of-Max" (IoM) hashing which was based on a locality sensitive hashing. Although IoM and IFO display good recognition performance along with non-invertibility, application of these techniques was restricted to binary feature representations. In [25], the authors proposed to design a cancelable fingerprint template using an alignment-free minutia descriptor, namely Partial Local Structure (PLS) descriptor. Non-invertible transforms were applied over the PLS descriptor rather than the minutia descriptor using Permutated Randomized Non-Negative Least Square (PR-NNLS) to achieve the desired cancelable properties while maintaining performance. Again, the proposed approach is limited to only fingerprint related applications. Hence, an adaptation of these methods to any type and dimension of feature, along with countermeasure against presentation attacks remains a challenge.

Recently, multibiometric cancelable systems were realized to simultaneously protect biometric data and defeat presentation attacks. Multimodal systems were found to perform better than unimodal counterparts, mainly due to the presence of multiple discriminative sources of information which are difficult to spoof simultaneously [11]. For instance, Sadhya and Singh [26] fused soft biometric characteristics with primary biometric characteristics using a bayesian approach. However, in this approach performance degrades if the comparator's characteristics were not known. Also, soft biometric characteristics exhibit low discriminatory information. Yang *et al.* [27], proposed to fuse fingerprint and finger-vein using a non-invertible Enhanced Partial Discrete Fourier Transform (EP-DFT). In [12], the authors proposed to generate cancelable multibiometric templates using graph-based random walk cross-diffusion and optimal score fusion. Bio-hashing based data type conversion was applied to fuse fingerprint minutiae and finger-vein feature. Zhong *et al.* [28] proposed to combine the accuracy of palmprint and liveness detection capabilities of dorsal hand veins (DHV) to generate multibiometric cancelable templates. For each biometric characteristic, 128-bit binary encoding was generated using a deep hashing network (DHN), along with with a biometric graph matching (BGM) approach for effective biometric verification. Mostly, feature level fusion techniques are limited to a particular set of modalities, and cannot be extended to other feature representations. Hence, it is observed that compared to other levels of fusion, the potential of feature-level fusion has not been exploited as much. The complexity associated with the application of multibiometric systems led researchers to explore alternative solutions to prevent presentation attacks [29]. Mainly, liveness detection approaches were employed to address this issue [13]. In [14] image quality parameters like texture, contrast, brightness helped identify masqueraders and prevent presentation attacks. In [15], Fernandez *et al.* proposed a quality-based multibiometric system. In this, interoperability of this system was improved by conditionally fusing comparison scores, based on image quality. A similar approach was described by Poh *et al.* [16], which employed a quality-based score normalization technique for multimodal biometric fusion.

For security-critical applications, an adversary may not only camouflage as a legitimate user but also try to illicitly steal biometric data. Hence, comprehensive security against adversary attacks must consider both template security and prevention from presentation attacks.

III. Motivations and Contributions

Investigating the existing biometric security mechanisms revealed the following limitations:

- *Non-invertibility:* most of the non-invertible transformation approaches tend to be vulnerable to partial or complete inversion (e.g., [7], [30]). In the scheme proposed in [30], multiple swindled templates may result in inversion to obtain the original biometric characteristic. Achieving complete non-invertibility is particularly challenging because increased non-invertibility results in reduced template distinctiveness, which degrades the performance.
- *Generality:* cancelable template generation is often limited to a certain class of feature extraction methods. For instance, the application of hashing-based approach proposed by Lin *et al.* [9] was restricted to modalities that can be represented as binary features and have a fixed length. Similarly, in [20], random projection approach was restricted to features which have a fixed length represented as a one-dimensional vector. Also, the fusion of non-homogeneous feature representations is again a challenging task.
- *Image Quality Conundrum:* performance of most of the biometric systems is dependent on image quality. Poor image quality results in low-quality features and hence low recognition rates. However, this enables biometric systems to detect presentation attacks. Whereas, if the system is quality independent, presentation attack goes unnoticed but persistent performance levels are achieved.
- *Robustness to Adversary Attacks:* most of the cancelable biometric approaches concern with only one class of adversary attacks i.e., template security [9]. On the other hand, liveness detection and presentation attacks were dealt with separately [13] . Generally, the comprehensive solution against adversary attacks was not considered.

To overcome these limitations, we propose an adaptive weighted graph approach to generate multimodal cancelable templates. The main contributions of our work are as follows:

- We propose a general framework to generate multimodal cancelable biometric templates. This is achieved through the novel feature set computation algorithm, which generates similarity graphs using key images. The proposed framework is deemed as a universal framework which is independent of the biometric characteristic used, or the feature extraction method employed. In addition, the generated feature set is dimensionally reduced, improving speed and reducing space requirements.
- We introduce a nonlinear graph fusion approach which fuses complementary information from different biometric characteristics. The nonlinear graph fusion approach has multiple advantages. First, strong information from different modalities is captured, while any weak information is suppressed. Second, nonlinearity enables the fused templates to achieve non-invertibility.
- We put forward an adaptive approach to resolve the *"image quality conundrum"*. A no-reference image quality analysis is employed to weigh features from respective modalities. This enables fused templates to adapt to features having superior image quality and suppress features with low image quality. Through this, the proposed biometric system can differentiate between 'presentation attacks' and 'mere low-quality images'.
- We rigorously analyze the robustness against security and privacy concerns. In particular, non-invertibility, unlinkability of the generated templates are tested. Further, robustness against various attacks namely false accept attacks, brute-force attacks, ARM attacks, and substitution attacks is also highlighted.

The following section describes the proposed cancelable multibiometric framework in detail.

IV. Proposed Methodology

The proposed multimodal biometric system leverages key images based cancelable feature generation, along with its quality based adaptation for robust recognition in an adversarial environment. The system is realized to perform recognition using commonly used biometric characteristics, namely fingerprint (p), face (f), and iris (i). Fig. 1 illustrates the overview of the proposed multibiometric system. Generic feature extraction for each modality is performed through key images, which can be revoked on the compromise of biometric data. For this, input multibiometric data is captured for three modalities to extract raw features $\delta^{(p)}, \delta^{(f)}$ and $\delta^{(i)}$ respectively. Also, raw features for key images $K_j^{(k)}\ \forall j \in \{1, 2, \ldots, n\}, k \in \{p, f, i\}$ are extracted for three modalities as $\psi^{(p)}, \psi^{(f)}, \psi^{(i)}$ respectively. Here, a set of n key images were used for each modality, and these keys were common to all input and query images for all subjects. Association of query images $I^{(k)} \in \{I^{(p)}, I^{(f)}, I^{(i)}\}$ with the corresponding key images $K_j^{(k)}$

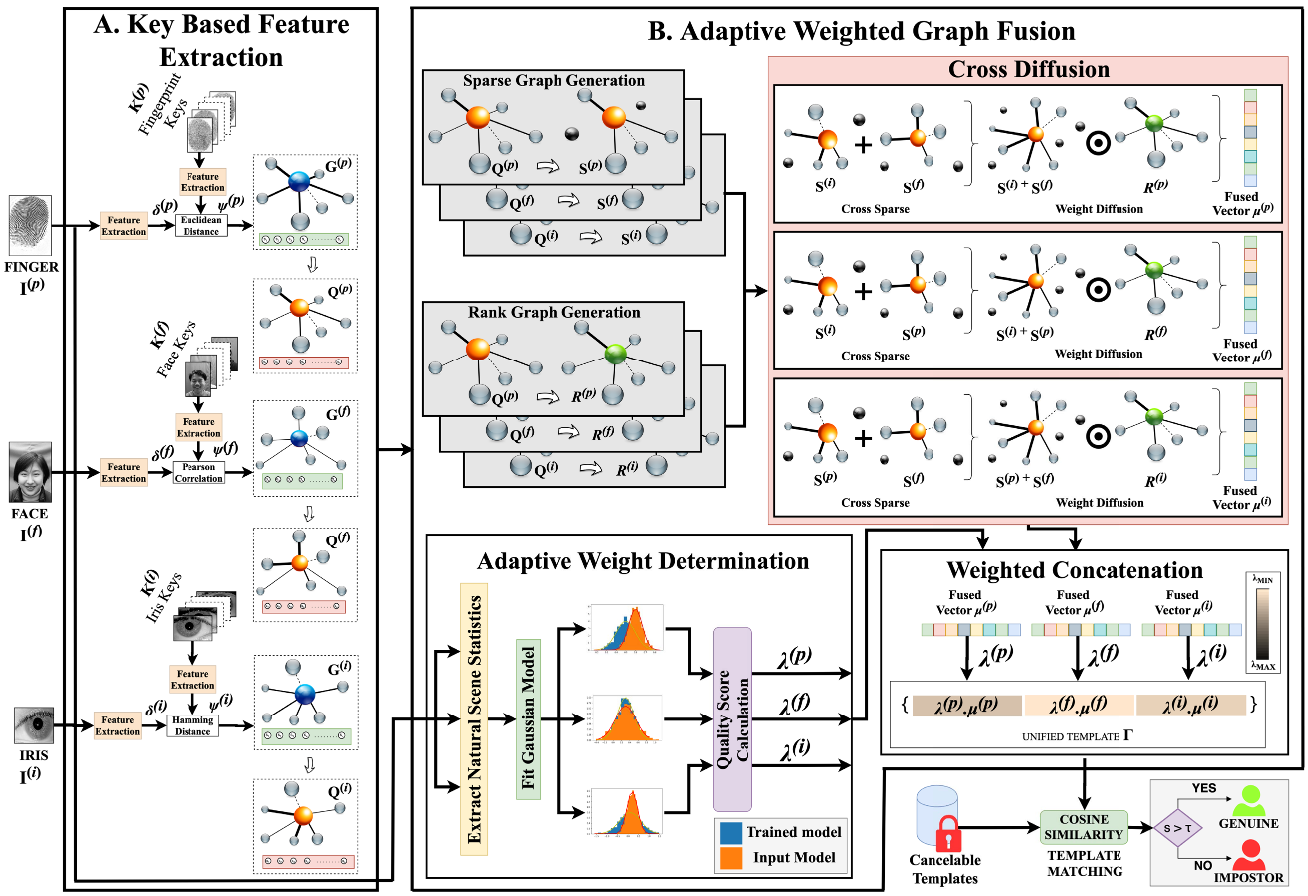

Fig. 1. Overview of the proposed multibiometric system. Normalized graphs constructed through key-based feature extraction is subjected to the proposed cross-diffusion to generate fused vectors. These fused vectors attain weights, determined adaptively using image quality, to generate a cancelable template.

$\forall j \in \{1, 2, \ldots, n\}$ is determined to construct similarity graphs $\mathbf{G}^{(k)} \in \{\mathbf{G}^{(p)}, \mathbf{G}^{(f)}, \mathbf{G}^{(i)}\}$. Further, anchored normalisation is applied over the individual similarity graphs to generate corresponding normalised graphs, $\mathbf{Q}^{(k)} \in \{\mathbf{Q}^{(p)}, \mathbf{Q}^{(f)}, \mathbf{Q}^{(i)}\}$. These normalised graphs are fused using the proposed *Adaptive Weighted Graph Fusion* (AWGF), which not only extracts complementary information from different modalities, but also adaptively weighs each modality in concurrence with image quality. For this, characteristic information of each modality is extracted as sparse graphs $\{\mathbf{S}^{(p)}, \mathbf{S}^{(f)}, \mathbf{S}^{(i)}\}$ and rank graphs $\{\mathcal{R}^{(p)}, \mathcal{R}^{(f)}, \mathcal{R}^{(i)}\}$. These graphs are diffused using proposed nonlinear graph fusion to generate fused vectors $\boldsymbol{\mu}^{(k)} \in \{\boldsymbol{\mu}^{(p)}, \boldsymbol{\mu}^{(f)}, \boldsymbol{\mu}^{(i)}\}$ for respective modalities. Fused vectors are assigned weights $\{\lambda^{(p)}, \lambda^{(f)}, \lambda^{(i)}\}$ adaptively by evaluating quality-metrics for each modality. A weighted concatenation results in the unified feature vector $\boldsymbol{\Gamma}_q$, which is the robust cancelable biometric template. The generated biometric template is compared using cosine similarity with stored database of templates for making decision about query subject. The proposed approach is elaborated in the following subsections.

A. Key Based Generic Feature Extraction

Generally, feature extraction from multiple modalities generates features with different type and dimension. This limits the applicability of feature fusion methods to only certain physiological characteristics. To overcome this, a key image based generic feature extraction is introduced, which not only achieves the generic nature of the proposal with reduced feature dimension but also ensures high revocability. In the case of template leakage, biometric templates can be regenerated either by changing the key order or by using a new set of key images for each biometric characteristic. Details about generic feature computation are as follows:

1) Graph Generation: Generic nature of the proposal is achieved through the establishment of an association of query images with a fixed set of key images, corresponding to each modality. This leads to construction of non-linear graphs $\mathbf{G}^{(k)} \in \{\mathbf{G}^{(p)}, \mathbf{G}^{(f)}, \mathbf{G}^{(i)}\}$, having a fixed number of nodes n, irrespective of the modality.

For fingerprint, raw features extracted through minutiae-based approach [31] are subjected to fingerprint keys association for the generation of a nonlinear graph $\mathbf{G}^{(\mathbf{p})}$. To determine minutiae location, 3×3 sliding window (centred at pixel u) is traversed in a circularly anticlockwise manner, to generate the *crossing number* (CN):

$$\mathrm{CN}(u) = \frac{1}{2}\sum_{i=1}^{8} |\S(u_{(i \bmod 8)}) - \S(u_{i-1})| \quad (1)$$

where $\S(u_i) \in \{0, 1\}$, is the pixel intensity of the i^{th} block of the window, centred at pixel u. Each minutiae is represented as vector $M = [x, y, \mathrm{CN}, \theta, \mathit{flag}]$, where (x, y) represent the coordinates of a pixel u, θ defines the orientation of the minutiae, and $\mathit{flag} \in \{0, 1\}$. Hence, for query image $I^{(p)}$, raw feature $\delta^{(p)} \in \mathbb{R}^{m\times 5}$ containing m minutiae is formed such that $\delta^{(p)} = [M_1, M_2, \ldots, M_m]$. Similarly, raw features $\psi_j^{(p)}$, $\forall j \in \{1, 2, \ldots, n\}$ are extracted for fingerprint keys $K_j^{(p)}$. These extracted raw features lead to the formation of nonlinear graph $\mathbf{G}^{(p)} = \{V^{(p)}, E^{(p)}, \mathbf{W}^{(p)}\}$. Wherein, $n + 1$ nodes, i.e. $V^{(p)} = \{\delta^{(p)}, \psi_1^{(p)}, \psi_2^{(p)} \ldots \psi_n^{(p)}\}$ depicts the raw features for query $\delta^{(p)}$ and for fingerprint keys $\{\psi_1^{(p)}, \ldots, \psi_n^{(p)}\}$. Graph edges $E^{(p)} = \{(\delta^{(p)}, \psi_j^{(p)})|\forall j \in \{1, 2, \ldots, n\}\}$ represents similarity of query image with the fingerprint keys. Hence, each edge is assigned weight $\mathbf{W}_j^{(p)}$, which is defined as:

$$\mathbf{W}_j^{(p)}\left(\delta^{(p)}, \psi_j^{(p)}\right) = \frac{n_{match}^2}{n_{\delta^{(p)}}\ n_{\psi_j^{(p)}}}, \quad \forall j \in \{1, 2, \ldots, n\} \tag{2}$$

where $n_{\delta^{(p)}}$ and $n_{\psi_j^{(p)}}$ represent the total number of minutiae extracted from the query and j^{th} fingerprint key respectively, and n_{match} represents the number of minutiae that satisfy the error constraints for coordinates (x, y) and orientation (θ), defined as:

$$\begin{aligned} d(M_{\delta_m}, M_{\psi_m}) &= \sqrt{(x_{\delta_m} - x_{\psi_m})^2 + (y_{\delta_m} - y_{\psi_m})^2} < d_\alpha \\ d(M_{\delta_m}, M_{\psi_m}) &= \min(|\theta_{\delta_m} - \theta_{\psi_m}|, 360^{\cdot} - |\theta_{\delta_m} - \theta_{\psi_m}|) < d_\theta \end{aligned} \tag{3}$$

For second modality, i.e. face, raw features are extracted using 2D Gabor filters [32], where 2D Gabor filter is defined as:

$$\begin{aligned} G(x, y) &= \frac{\eta^2}{\pi\alpha\beta}\exp\left(-\frac{p^2 + \alpha^2 q^2}{2\sigma^2}\right)\exp\left(i2\pi\eta p + \phi\right) \\ p &= x\cos\theta + y\sin\theta; \quad q = -x\sin\theta + y\cos\theta \end{aligned} \tag{4}$$

where η represents the sinusoidal frequency, ϕ is the phase offset, θ is the orientation, σ is the standard deviation, and α is the spatial aspect ratio. Query image $I^{(f)}$, is convolved with 40 Gabor filters (5 scales, 8 orientations) to generate feature images. These feature images are then reshaped and concatenated to form a 1-D raw feature vector $\delta^{(f)}$. Similarly, each face keys $K_j^{(f)}$ is convolved with the Gabor filter bank to generate raw feature vector $\psi_j^{(f)}$, $\forall j \in \{1, 2, \ldots, n\}$.

These extracted raw feature vectors are exploited for the formation of nonlinear graph $\mathbf{G}^{(f)} = \{V^{(f)}, E^{(f)}, \mathbf{W}^{(f)}\}$. Nodes of the graph $V^{(f)} = \{\delta^{(f)}, \psi_1^{(f)}, \psi_2^{(f)} \ldots \psi_n^{(f)}\}$ are obtained using query image feature $\delta^{(f)}$, and n face keys features $\psi_j^{(f)}$, $\forall j \in \{1, 2, \ldots, n\}$. Graph edges $E^{(f)} = \{(\delta^{(f)}, \psi_j^{(f)})|\forall j \in \{1, 2, \ldots, n\}\}$ depict the association among the nodes. Hence, similarity weight matrix $\mathbf{W}^{(f)} = \{\mathbf{W}_1^{(f)}, \mathbf{W}_2^{(f)}, \ldots, \mathbf{W}_n^{(f)}\}$ is determined, where j^{th} edge weight $\mathbf{W}_j^{(f)}$ is defined as:

$$\mathbf{W}_j^{(f)}\left(\delta^{(f)}, \psi_j^{(f)}\right) = \mathrm{cov}(\delta^{(f)}, \psi_j^{(f)})/(\sigma_{\delta^{(f)}}.\sigma_{\psi_j^{(f)}}) \tag{5}$$

For iris trait, we employed 1D Log-Gabor filter method [33] to extract raw binary features. For this, segmented iris image is normalised using Daugman's rubber sheet model. Normalised iris image is convolved with 1D Log Gabor wavelets with frequency response defined as:

$$G(\eta) = \exp\left(\frac{-(\log(\eta/\eta_o))^2}{2(\log(\sigma/\eta_o))^2}\right) \tag{6}$$

where η_o is the centre frequency and σ controls the bandwidth. The extracted phase data is quantised to four levels. This results in a unique binary pattern, forming the raw feature template $\delta^{(i)}$ corresponding to iris query. Further, raw feature $\psi_j^{(i)}$ is generated for each iris key $K_j^{(i)}, \forall j \in \{1, 2, \ldots, n\}$.

Similarly, iris graph $\mathbf{G}^{(i)} = \{V^{(i)}, E^{(i)}, \mathbf{W}^{(i)}\}$ is constructed with $n + 1$ nodes. The width of the edges forms a similarity weight matrix $\mathbf{W}^{(i)}$. Elements of similarity weight matrix, $\mathbf{W}_j^{(i)}$ $\forall j \in \{1, 2, \ldots, n\}$, Eq. 7, are determined through radial basis function applied over Hamming distance ($\mathbf{H}_\mathrm{d}$).

$$\mathbf{W}_j^{(i)}\left(\delta^{(i)}, \psi_j^{(i)}\right) = \exp\left(-\mathbf{H}_\mathrm{d}(\delta^{(i)}, \psi_j^{(i)})^2/(2\sigma^2)\right) \tag{7}$$

where σ is scaling factor, and Hamming distance ($\mathbf{H}_\mathrm{d}$), Eq. 8, provides dissimilarity between the iris query and keys features.

$$\mathbf{H}_\mathrm{d}(\delta^{(i)}, \psi_j^{(i)}) = \frac{1}{N}\sum_{y=1}^{N}\delta_y^{(i)} \oplus \psi_{j_y}^{(i)} \tag{8}$$

In order to preserve individual subject privacy and system security, we have chosen the set of key images, such that $K^{(k)} \notin I^{(k)}, \forall k \in \{p, f, i\}$, which leads to indistinguishable generic features of individual modality. On the other hand, generic features of different modality are highly irregular and non-uniform due to differing environment and evaluation approach. Hence, non-linear graphs $\mathbf{G}^{(k)} \in \{\mathbf{G}^{(p)}, \mathbf{G}^{(\mathbf{f})}, \mathbf{G}^{(i)}\}$ are normalised to achieve distinguishable individual modality generic features. Details of graph normalisation process is discussed as follows.

2) Graph Normalisation: In order to obtain unbiased and distinguishable features, nonlinear graphs $\mathbf{G}^{(\mathbf{k})}$, are normalised using anchored normalisation to generate normalised similarity graphs $\mathbf{Q}^{(k)} \in \{\mathbf{Q}^{(p)}, \mathbf{Q}^{(f)}, \mathbf{Q}^{(i)}\}$. For this, each nonlinear graph $\mathbf{G}^{(k)}$ is normalised using an anchor $A^{(k)}$, which is derived from the impostor score distribution of the k^{th} modality, defined as: $A^{(k)} = A_{avg}^{(k)} + A_{std}^{(k)}$, where $A_{avg}^{(k)}$ and $A_{std}^{(k)}$ refer to the mean and standard deviation of the impostor score distribution of the k^{th} modality. Our approach modifies the approach described in [34], by considering only impostor scores for computing the anchor. To make the scores more distinguishable within a modality and scale the scores of different modalities to the same level, weight transformation, Eq. 9 has been applied to the get normalised graph $\mathbf{Q}^{(k)} \in \{\mathbf{Q}^{(p)}, \mathbf{Q}^{(f)}, \mathbf{Q}^{(i)}\}$, where the graph weight matrix $\mathcal{Q}_j^{(k)}$, $\forall j \in \{1, 2, \ldots, n\}$, $\forall k \in \{p, f, i\}$ are determined as:

$$\mathcal{Q}_j^{(k)} = \begin{cases} \dfrac{W_j^{(k)} - min\left(W^{(k)}\right)}{2\left(A^{(k)} - min\left(W^{(k)}\right)\right)}, & W_j^{(k)} \le A^{(k)} \\ 0.5 + \left(\dfrac{W_j^{(k)} - A^{(k)}}{max\left(W^{(k)}\right) - A^{(k)}}\right), & W_j^{(k)} > A^{(k)} \end{cases} \tag{9}$$

Algorithm 1 describes the proposed key based generic feature extraction technique. These normalised graphs with

Algorithm 1 : Key Based Generic Feature Extraction

Input: $I^{(k)}$, $K_j^{(k)}$ $\forall$ $j \in \{1, 2, \ldots, n\}$
Output: $\mathbf{Q}^{(k)} \in \{\mathbf{Q}^{(p)}, \mathbf{Q}^{(f)}, \mathbf{Q}^{(i)}\}$

```
for k ∈ {p, f, i} do
    extract raw features for I^(k), denoted as δ^(k)
    for j = 1 to n do
        extract raw features for K_j^(k), denoted as ψ_j^(k)
    end for
end for
for k ∈ {p, f, i} do
    for j = 1 to n do
        construct G_j^(k) using Eq. 2, Eq. 5, Eq. 7
        normalise G_j^(k) to Q_j^(k) using Eq. 9
    end for
end for
return Q^(k) ∈ {Q^(p), Q^(f), Q^(i)}
```

distinguishable scores are subjected to proposed fusion approach as discussed in the following subsection.

B. Adaptive Weighted Graph Fusion

Adaptive Weighted Graph Fusion (AWGF) is proposed to achieve complete non-invertibility and robustness to presentation attacks. It comprises of: (1) *Information Mining* to extract complementary information and suppress outliers, (2) *Cross Difussion* to ensure complete non-invertibility, and (3) *Adaptive Unification* to prevent presentation attacks. Details about the proposed AWGF is as follows:

1) Information Mining: To capture complementary information from three modilities, sparse graphs $\mathbf{S}^{(k)} \in \{\mathbf{S}^{(p)}, \mathbf{S}^{(f)}, \mathbf{S}^{(i)}\}$ and rank graphs $\mathcal{R}^{(k)} \in \{\mathcal{R}^{(p)}, \mathcal{R}^{(f)}, \mathcal{R}^{(i)}\}$ are constructed from the normalised graphs $\mathbf{Q}^{(k)} \in \{\mathbf{Q}^{(p)}, \mathbf{Q}^{(f)}, \mathbf{Q}^{(i)}\}$. Sparse graphs ensure robustness to noise and dynamic environments while preserving strong information and suppressing weak information from each modality. In our approach, we exploit the sparsity of normalized graphs by selecting those key images, that are strongly correlated to the query. Sparse graph, $\mathbf{S}^{(k)} = \{V^{(k)}, E^{(k)}, \xi^{(k)}\}$ is constructed using k-nearest neighbour (KNN) as follows:

$$\xi_j^{(k)} = \begin{cases} \mathcal{Q}_j^{(k)}, & \left(\mathcal{Q}_j^{(k)} \in \mathrm{KNN}_{\mathbf{Q}^{(k)}} | \kappa\right) \\ 0, & \text{Otherwise} \end{cases} \tag{10}$$

where κ controls the sparsity of the graph, and $\mathcal{Q}^{(k)}$ is the weight matrix of the normalised graph of the k^{th} modality such that $k \in \{p, f, i\}$. Edges corresponding to key images that are similar to the query image are retained, while remaining edges are removed, ensuring robustness to noise.

In order to distinguish significant key image from the insignificant ones, each key image is assigned weights according to its rank.

For this, ranks are assigned to each key image based on its similarity with the query image, which is determined by the edge weight between the query and the key image in normalized graph. The weight graph $\mathcal{R}^{(k)} = \{V^{(k)}, E^{(k)}, \boldsymbol{\Upsilon}^{(k)}\}$ having a weight matrix $\boldsymbol{\Upsilon}^{(k)}$ defined as:

$$\boldsymbol{\Upsilon}_j^{(k)} = Rank(\mathcal{Q}_j^{(k)}), \quad \forall j \in \{1, 2, \ldots, n\} \tag{11}$$

where *Rank*, assigns a rank $r \in \{1, 2, \ldots, n\}$ to each key image in concurrence with the relative score.

2) Cross Diffusion: Cross diffusion method is devised to effectively strengthen strong relationships between different modalities while suppressing any noise or weak links. To achieve this, we cross diffuse the distinctive information acquired through sparse graph $S^{(k)}$, and rank graph $\mathcal{R}^{(k)}$, $\forall k \in \{p, f, i\}$. While sparse graphs ensure removal of outliers, rank graphs prevent any bias of modality. Hence, cross diffusion of sparse and rank graph maintain a trade-off between removing insignificant information, without mistakenly missing out any information. Proposal is generic in nature and hence can be extended to any type and dimension of the modality. In addition, diffusion of information from multiple modalities makes it even more difficult for an adversary to regenerate biometric characteristics. Essentially, cross diffusion can be summed up as *ORing* of sparse graphs followed by their *ANDing* with rank graphs. To realise cross diffusion, we perform *cross sparse* (Eq. 12) by adding the sparse graphs of two other modalities to generate $\zeta^{(k^{(t)})}$, where $(k^{(t)})$ is t^{th} element of set k. This is followed by *weight diffusion* (Eq. 13) of the rank graph of the self modality with $\zeta^{(k^{(t)})}$ to generate fused vector $\mu^{(k^{(t)})}$.

$$\zeta^{(k^{(t)})} = \sum_{Z} \xi^{(Z)}, \quad \text{where } Z \in \{k\} - \{k^{(t)}\} \tag{12}$$

$$\mu^{(k^{(t)})} = \boldsymbol{\Upsilon}^{(k^{(t)})} \odot \zeta^{(k^{(t)})}, \quad \forall t \in \{1, 2, 3\} \tag{13}$$

To compute $\mu^{(k)}$, key images that are strongly correlated in two modalities obtain higher scores, which is then strengthened by the weight of the self modality that depends on relative rank. Hence, corresponding to each weight graph $\mathcal{R}^{(k)}$, we obtain unified graphs $\mu^{(k)}$ $\forall k \in \{p, f, i\}$. These generic unified graphs are further subjected to adaptive unification to obtain cancelable templates.

3) Quality Adaptive Unification: Unified graphs $\mu^{(k)}$ $\forall k \in \{p, f, i\}$ are weighted in concurrence with image quality of respective modality. This strategy not only improves system interoperability and recognition rates but also prevents presentation attack. It also adapts the system to a dynamic environment by suppressing low performing modality and simultaneously boosting high performing modality.

For this, we employ a Natural Image Quality Evaluation (NIQE) technique proposed in [35]. NIQE is a blind image quality analyzer that uses a priori knowledge of distortion-free images to construct a general understanding of the natural scene statistics (NSS). Deviation from the general properties indicates degraded image quality. Firstly, training biometric data is fed to extract statistical measures in order to fit a Multivariate Gaussian (MVG) Model $\mathcal{F}_{\mathrm{t}}^{(k)}$ for each modality, $k \in \{p, f, i\}$.

$$\mathcal{F}_{\mathrm{t}}^{(k)} = \frac{1}{(2\pi)^{x/2} |\sum_{\mathrm{t}}^{(k)}|^{1/2}} e^{\left(-\frac{1}{2}(a_x - \varphi_{\mathrm{t}}^{(k)})^T (\sum_{\mathrm{t}}^{(k)})^{-1} (a_x - \varphi_{\mathrm{t}}^{(k)})\right)} \tag{14}$$

such that a_x represents NSS features, $\varphi_{\mathrm{t}}^{(k)}$ denotes the mean and $\sum_{\mathrm{t}}^{(k)}$ represents the covariance matrix of the

Algorithm 2 Adaptive Weighted Graph Fusion (AWGF)

Input: $\mathbf{Q}^{(k)} \in \{\mathbf{Q}^{(p)}, \mathbf{Q}^{(f)}, \mathbf{Q}^{(i)}\}$, κ
Output: Unified Template $\mathbf{\Gamma}$

for $k \in \{p, f, i\}$ **do**
  construct $\mathbf{S}^{(k)}$ from $\mathbf{Q}^{(k)}$ using Eq. 10 given κ
  construct $\mathcal{R}^{(k)}$ from $\mathbf{Q}^{(k)}$ using Eq. 11
end for
for $k \in \{p, f, i\}$ **do**
  compute $\mu^{(k)}$ from $\{\mathbf{S}^{(Z)}\}$, $\mathcal{R}^{(k)}$ using Eq. 12, Eq. 13
  find $\lambda^{(k)}$ using Eq. 14, Eq. 15
end for
find $\mathbf{\Gamma}$ using Eq. 16
return $\mathbf{\Gamma}$

MVG model. Subsequently, for each query image, statistical features are extracted to fit another MVG i.e. $\mathcal{F}_{\mathrm{q}}^{(k)}$ to compute $\varphi_{\mathrm{q}}^{(k)}$ and $\sum_{\mathrm{q}}^{(k)}$. Distance between $\mathcal{F}_{\mathrm{q}}^{(k)}$ and $\mathcal{F}_{\mathrm{t}}^{(k)}$ is computed to determine the quality score ($\lambda^{(k)}$) for k^{th} modality, $\forall k \in \{p, f, i\}$, defined in Eq. 15. Quality score $\lambda^{(k)}$ is used to weigh corresponding unified vector $\mu^{(k)}$ prior to concatenation to ensure that higher weight is assigned to a more reliable modality.

$$\lambda^{(k)} = \frac{1}{\sqrt{(\varphi_{\mathrm{t}}^{(k)} - \varphi_{\mathrm{q}}^{(k)})^T \left(\frac{\sum_{\mathrm{t}}^{(k)} + \sum_{\mathrm{q}}^{(k)}}{2}\right)^{-1} (\varphi_{\mathrm{t}}^{(k)} - \varphi_{\mathrm{q}}^{(k)})}} \tag{15}$$

Unified template $\mathbf{\Gamma}_q$, is obtained by weighing each unified graph $\mu^{(k)}$ with quality score $\lambda^{(k)}$, followed by concatenation:

$$\mathbf{\Gamma}_q = <\lambda^{(p)} \cdot \mu^{(p)}, \lambda^{(f)} \cdot \mu^{(f)}, \lambda^{(i)} \cdot \mu^{(i)}> \tag{16}$$

Generated unified cancelable biometric templates are not only dimensionally reduced, but also non-invertible. These templates can be easily revoked either by using a new set of key images, or by changing the order of key images. In addition, quality based adaptation to dynamic environment achieves high distinguishability between presentation attack and mere low quality images. Pseudocode for proposed AWGF is depicted as Algorithm 2. Further, the proposed multi-modal biometric system is validated both quantitatively and qualitatively as discussed in following section.

V. Experimental Results and Discussions

A. Databases and Experimental Setup

The proposed multibiometric system is validated using benchmark databases. To validate the performance over a real multimodal database, experiments were conducted using the SDUMLA-HMT Multimodal Database [36], which is dubbed as DB-1 in our setup. Further, following databases have also been been used, CASIA-FingerprintV5 [37], FVC 2006 [38], MCYT [39] for fingerprint, CAS-PEAL [40], CASIA-FaceV5 [41] for face, IITD PolyU [42] and CASIA-IrisV3 [43] for iris. As highlighted by Sultana *et al.* [10] that correlation among different physiological characteristics could not be established, we formulated virtual multibiometric databases for our evaluation without any loss of generality. For this, unique one-to-one mapping between different unimodal databases is maintained for first N subjects to generate three multimodal databases: DB-2, DB-3, and DB-4. Table I summarizes the details about the multimodal databases used. For each subject, one image is randomly selected from five samples and the experiment is repeated five times to achieve 5-fold cross-validation. All experiments were carried out on Windows 10, 2.7 GHz $i7$ processor, 16GB RAM with MATLAB R2018a.

TABLE I
MULTIMODAL DATABASES USED FOR EXPERIMENTATION

Database	Fingerprint	Face	Iris
DB-1	SDUMLA-HMT Multimodal Database [36]		
DB-2	MCYT [39]	CAS-PEAL R1 (expression) [40]	IITD PolyU Iris [42]
DB-3	CASIA-Fingerprint V5 [37]	CASIA-FaceV5 [41]	CASIA Iris V3 (Interval) [43]
DB-4	FVC 2006 [38]	CAS-PEAL R1 (accessories) [40]	CASIA Iris V3 (lamp) [43]

B. Evaluation Metrics

Quantitative performance of the proposed multibiometric system is compared with state of the art fusion methods using performance metrics namely False Match Rate (FMR), False Non-Match Rate ($FNMR$), Genuine Accept Rate (GAR), False Accept Rate (FAR), and Equal Error Rate (EER). In addition, Decidability Index (DI) [44] is determined to gauge the separability between the genuine and impostor score distribution. DI is computed as:

$$\mathrm{DI} = |\mu_g - \mu_{im}|/(\sqrt{(\sigma_g^2 + \sigma_{im}^2)/2}\ ) \tag{17}$$

where μ_g and μ_{im} represent the mean and σ_g and σ_{im} represent the standard deviation of the genuine and impostor score distribution respectively. Further, identification performance is determined using Recognition Index (RI) which is estimated from the top m scores for a query subject.

C. Performance Validation

In this subsection, we validate the system performance from different perspectives namely adaptivity, accuracy, and complexity.

1) Adaptivity Analysis: Adaptiveness of the proposed method is evaluated under the dynamic environment by considering its ability to extract distinctive features from different modalities. For this, we plot the point-set distributions of (a) extracted generic features of individual modality and (b) fused feature to analyze their inter-class and intra-variations. As shown in Fig. 2, normalised features for two multimodal subjects q_1 and q_2 are depicted where $q_1^{(a)}$ and $q_1^{(b)}$ represent two samples of subject q_1. Fig. 2(a) depicts highly distinct features for face modality $Q^{(f)}$, while those extracted from fingerprint $Q^{(p)}$, and iris $Q^{(i)}$, generate a feature with low distinction between subjects q_1 and q_2. In fused features Γ, AWGF efficiently extracts strong correlations between features from different modalities and generates a template which is highly distinct as shown in Fig. 2(b). This is achieved through the cross-diffusion process, where strong information from one modality is fused with information of

TABLE II

IMAGE QUALITY ANALYSIS: COMPARISON OF $EER(\%)$ AND DI FOR ADAPTIVE AND NON-ADAPTIVE MODES OF AWGF. GAUSSIAN NOISE WITH $\mu = 0$, $\sigma = 0.01$ ADDED TO DIFFERENT SUBSETS OF MODALITIES

AWGF Mode	**EER**(%)								**Decidability Index (DI)**							
	Original	$(p'fi)$	$(pf'i)$	(pfi')	$(p'f'i)$	$(p'fi')$	$(pf'i')$	$(p'f'i')$	Original	$(p'fi)$	$(pf'i)$	(pfi')	$(p'f'i)$	$(p'fi')$	$(pf'i')$	$(p'f'i')$
Non-Adaptive	1.25	7.72	8.00	8.55	10.05	9.88	12.34	15.12	5.00	2.93	2.90	2.84	2.07	1.85	1.95	1.53
Adaptive	1.02	3.37	2.76	4.00	6.11	5.00	8.78	14.58	5.25	4.14	4.97	3.83	3.47	3.37	2.69	1.68

TABLE III

PERFORMANCE EVALUATION AND COMPARISON. AVERAGE DECIDABILITY INDEX (DI), EER (%) AND RECOGNITION INDEX (RI) FOR FUSED TEMPLATES USING STATE-OF-THE-ART FEATURE FUSION TECHNIQUES AT 95% SIGNIFICANCE LEVEL

Performance Metric	**Decidability** (DI)				**EER (%)**				**Recogniton Index** (RI)			
Method/ Database	DB-1	DB-2	DB-3	DB-4	DB-1	DB-2	DB-3	DB-4	DB-1	DB-2	DB-3	DB-4
CCA-FFS I *(f + i)* [45]	2.21 ± 0.2	2.78 ± 0.8	3.01 ± 0.8	3.11 ± 0.3	6.02 ± 1.1	6.09 ± 1.0	6.00 ± 1.1	5.71 ± 0.6	86.31 ± 2.4	76.31 ± 1.6	91.31 ± 2.3	83.58 ± 1.4
CCA-FFS II *(f + i)* [45]	2.79 ± 0.1	2.66 ± 0.5	2.98 ± 0.9	2.96 ± 0.4	6.34 ± 0.9	7.00 ± 1.1	7.50 ± 1.6	6.02 ± 0.9	79.58 ± 1.3	84.04 ± 1.6	77.22 ± 1.3	82.58 ± 2.1
CCA-FFS I *(f + p)* [45]	3.32 ± 0.3	2.60 ± 0.2	2.36 ± 0.8	2.15 ± 0.5	6.04 ± 0.4	6.46 ± 1.0	5.52 ± 1.1	6.49 ± 0.7	77.13 ± 1.6	76.40 ± 1.9	92.84 ± 1.3	88.87 ± 1.1
CCA-FFS II *(f + p)* [45]	1.99 ± 0.6	2.46 ± 0.4	2.10 ± 0.9	2.25 ± 0.8	7.10 ± 1.0	7.02 ± 1.2	7.00 ± 1.3	6.09 ± 1.2	91.13 ± 1.9	84.13 ± 1.5	79.26 ± 1.5	89.88 ± 2.5
RDM *(f + i)* [20]	3.37 ± 0.1	2.31 ± 0.8	2.28 ± 0.3	2.34 ± 0.3	4.55 ± 0.6	4.00 ± 0.3	5.83 ± 1.0	4.79 ± 1.1	85.28 ± 1.2	87.49 ± 1.6	90.40 ± 1.2	78.72 ± 2.2
RDM *(f + p)* [20]	3.91 ± 0.7	2.42 ± 0.4	3.95 ± 0.5	3.19 ± 0.7	3.96 ± 0.4	6.02 ± 0.2	4.21 ± 0.5	4.67 ± 0.7	89.62 ± 1.4	88.84 ± 1.7	92.91 ± 1.8	87.75 ± 1.1
DCT *(f + i)* [46]	2.43 ± 0.2	2.00 ± 0.4	2.22 ± 0.5	2.08 ± 0.1	5.97 ± 1.1	5.68 ± 0.5	6.22 ± 1.3	7.63 ± 0.7	94.66 ± 1.7	89.35 ± 1.3	92.66 ± 0.9	84.47 ± 0.7
DCT *(f + p)* [46]	2.03 ± 0.4	2.05 ± 0.9	2.47 ± 0.4	2.90 ± 0.3	7.76 ± 1.5	5.96 ± 0.6	5.51 ± 1.1	6.17 ± 0.4	77.96 ± 1.9	93.31 ± 1.6	87.09 ± 1.4	83.59 ± 1.8
Ours *(non-adaptive)*	4.68 ± 0.5	5.09 ± 0.5	4.23 ± 0.4	3.97 ± 1.0	3.12 ± 0.3	1.19 ± 0.1	3.05 ± 0.8	3.44 ± 0.4	96.66 ± 2.1	98.09 ± 0.9	95.88 ± 2.0	91.78 ± 1.3
Ours *(adaptive)*	**4.71 ± 0.3**	**5.38 ± 0.5**	**4.72 ± 0.6**	**4.42 ± 1.1**	**2.03 ± 0.9**	**1.00 ± 0.1**	**1.52 ± 0.5**	**2.35 ± 0.7**	**97.98 ± 1.2**	**99.22 ± 0.5**	**96.66 ± 0.8**	**95.57 ± 1.0**

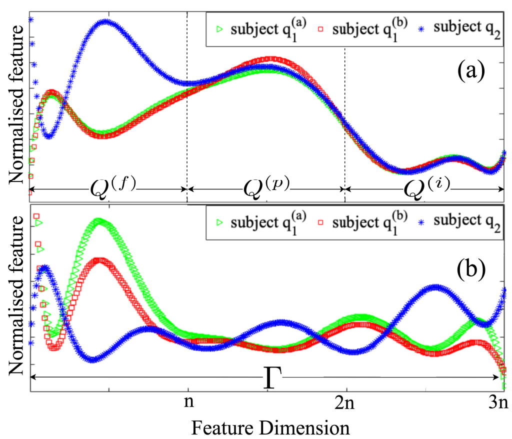

Fig. 2. Feature distinctiveness comparison using point-set distribution of (a) Individual modality generic features, $Q^{(k)}$ and (b) Fused feature, Γ.

other modalities. In addition, the generated template has no direct correlation with extracted features as shown in Fig. 2, validating the cancelable properties.

To further evaluate the adaptivity, tolerance of AWGF in (1) *adaptive* and (2) *non-adaptive* modes is compared. By adaptive we refer to AWGF which uses image quality to weigh features, whereas non-adaptive mode has $\lambda^{(k)} = 1, \forall k \in \{p, f, i\}$. For this, performance is compared by adding noise to subsets of input biometric data as tabulated in Table II for DB-2. Wherein, $k' \in \{p', f', i'\}$ represents a noisy modality with, Gaussian noise added with mean $\mu = 0$, and variance $\sigma = 0.01$. Average $EER(\%)$ for single noisy input was observed to be 3.37 and 8.09, and when two inputs were noisy was 5.55 and 9.965 for adaptive and non-adaptive modes respectively. Hence, the adaptive mode performs better with noisy inputs than its counterpart. This behavior is attributed to the fact that adaptive mode adds another dimension, i.e. *image quality* to suppress weak information and ensures high magnitude allocation to more discriminatory information. However, when all three modalities possess noisy information, $EER(\%)$ shoots up to 14.58 and 15.12 for adaptive and non-adaptive respectively. Hence, performance for non-adaptive increase linearly with an increase in noise, while adaptive mode understands the dynamic environments and responds accordingly by differentiating between ‘low-quality images’ and ‘presentation attack’.

2) Fusion Method Comparison: In this subsection, the performance of AWGF in the stolen token scenario is compared with various baseline systems and state of the art fusion methods. Table III reports the accuracy results in terms of average $EER(\%)$, DI and RI at 95% significance level. Further, Detection-Error Tradeoff (DET) curves (Fig. 3) help to analyze the system performance under higher security i.e. at low error rates and support the $EER(\%)$, while CMC curves (Fig. 4) support RI. For comparison, performance of prominent feature fusion methods which can be applied to 1D feature vectors such as Canonical Correlation Analysis (CCA) [45], and Discrete Cosine Transform (DCT) [46] have also been included for different combinations of modalities. Also, recently proposed transformation based cancelable approach RDM [20] is also evaluated for a comprehensive comparison. To ensure a direct and fair comparison of fusion methods, templates are generated using the same normalized graphs ($Q^{(k)}$) as input features. It is observed that AWGF outperforms the state-of-the-art fusion methods across all databases with an average EER of 1.73%, and RI of 97.35. This is because the proposed method successfully integrates complementary information from different modalities and effectively adapts to information with high reliability. Further, CCA and DCT primarily focus on fusing information without any non-invertibility consideration. Whereas, RDM achieves non-invertibility by using Median Filtering, which is not an inherent property of the fusion process. In contrast, the proposed method generates highly non-invertible templates without any loss in performance.

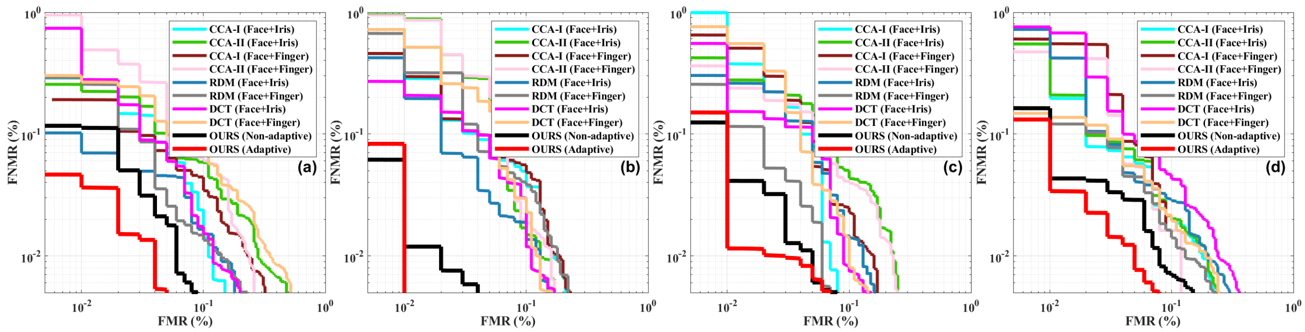

Fig. 3. Detection-Error Tradeoff (DET) Curves, (a) DB-1, (b) DB-2, (c) DB-3, (d) DB-4.

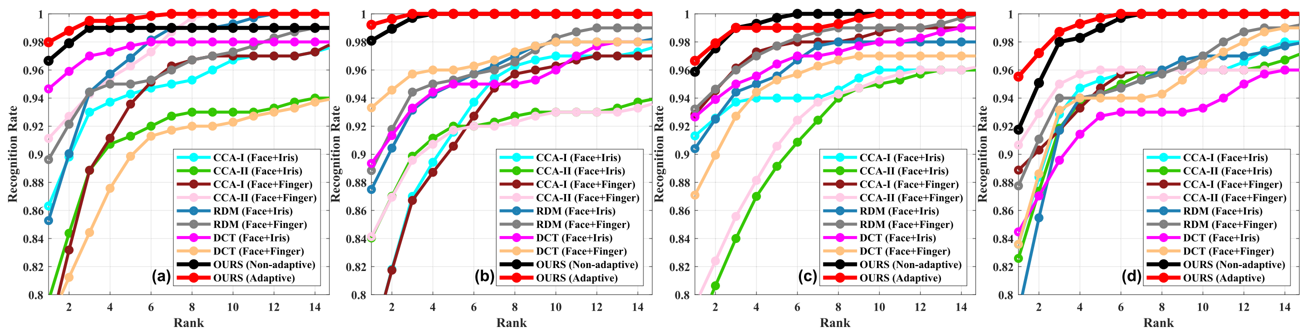

Fig. 4. Cumulative Matching Characteristic (CMC) Curves, (a) DB-1, (b) DB-2, (c) DB-3, (d) DB-4.

TABLE IV

TIME COMPLEXITY ANALYSIS

Method	Time (milliseconds)
RDM	75.0
CCA - I	48.0
CCA - II	49.5
DCT	66.7
Ours (*non-adaptive*)	60.0
Ours (*adaptive*)	61.0

3) Time and Space Complexity: In this subsection, we analyze the time and space complexity of the proposed approach. Table IV summarises the comparison of time required to generate multimodal biometric templates from the normalized graphs $Q^{(k)}$ as features. Results reveal that the proposed method is computationally efficient due to small feature dimension, which only depends upon the size of the keys. In addition, the proposed method has a significantly smaller space requirement, compared to Gabor features (3.3 MB). Further, the space required by biometric template generated using the proposed method (0.76 KB) is comparable to binary templates for iris like the IrisCodes (1.67 KB) and minutia based features (0.66 KB). However, comparing minutia based features is not as trivial as comparing similarity-based comparison approaches. In sum, the proposed feature extraction generates generic features with small dimension, which in turn reduces the time complexity for both fusion and comparison process.

VI. PRIVACY AND SECURITY ANALYSIS

Major threats that surround biometric systems involve theft of biometric data, i.e. *privacy* concerns, and illegitimate access, i.e. *security* concerns. The detailed analysis of these concerns are as follows:

A. Privacy Analysis

The privacy concerns of the proposed multimodal biometric system are analyzed through non-invertibility, attacks via record multiplicity, and finally test the unlinkability property of the proposed approach.

1) Non-Invertibility Analysis: Cancelable biometric templates must non-invertible to ensure the privacy of biometric data, in case the biometric system is compromised. In the worst case, the adversary has access to key images. To analyse the non-invertibility, we try to recover the biometric data, i.e. query images $I^{(k)} \in \{I^{(p)}, I^{(f)}, I^{(i)}\}$, from the stored biometric template Γ, and assess the complexity involved. Each element of the template Γ is a real number that may presume any value and has no direct relationship with the key images. Thus, we first assess the complexity of generating λ from template Γ. $(1/\lambda) \in (0, 100)$. To obtain quality scores, one requires the query image itself, making a recursive requirement. Hence, the complexity involved in guessing the quality of all three modalities is $\left(2 \times 10^6\right)^3$, for decimal with 4 places. Further, to invert the fused vector to obtain normalized graphs $Q^{(k)}$, rank graphs $\mathcal{R}^{(k)}$ and sparse graphs $S^{(k)}$ would be required. Assuming rank graphs by brute force, and using Eq. 12 and Eq. 13, relationship between the sparse graphs can be inferred with a complexity of 3n!. To generate sparse graphs, only the parameter κ is unknown, hence to obtain normalized graph $Q^{(k)}$ a complexity of $(n-\kappa)7.5 \times 10^3$ exists. Further, to generate non-linear graphs $G^{(k)}$, anchors $A^{(k)}$ are required and the complexity involved in generating

TABLE V
WORST CASE COMPLEXITY ANALYSIS FOR INVERTIBILITY

Generate y from $x : x \to y$	Complexity	Element Required
$\Gamma \to \mu^{(k)}$	8×10^{18}	$\lambda^{(k)}$
$\mu^{(k)} \to \mathbf{Q}^{(\mathbf{k})}$	$3n!$	$\mathcal{R}^{(k)}$
	$(n-\kappa)7.5 \times 10^3$	$\mathbf{S}^{(k)}$
$\mathbf{Q}^{(\mathbf{k})} \to \mathbf{G}^{(\mathbf{k})}$	10^{12}	$A^{(k)}$
Total	$n!(n-\kappa)1.8 \times 10^{35}$	

anchors $A_{avg}^{(k)}$ and $A_{std}^{(k)}$ is $\left(10^4\right)^3$. Given key images, one can correlate them with the non-linear graphs $G^{(k)}$ to obtain biometric data. Table V summarises the worst-case complexity of inverting a template to obtain biometric data i.e. $n!(n-\kappa)1.8\times 10^{35}$. Hence, the proposed biometric cancelable templates are highly non-invertible, which cannot be realized in practical scenarios.

2) Attacks via Record Multiplicity (ARM): ARM attacks is a more severe attack against the privacy of the biometric data, it uses multiple instances of compromised templates to find a correlation between the templates and biometric data. However, with the proposed biometric fusion, biometric data is cross diffused and transformed into another space where no direct correlation exists between the biometric data and the templates. Hence, ARM attack complexity is the same as mentioned in Table V, making the system robust against this attack.

3) Unlinkability Analysis: In this section, we evaluate the system's unlinkability using the framework presented by Gomez-Barrero *et al.* [47]. Two templates are said to be linkable if the adversary can conclude with certainty that the two templates generated, stem to the same biometric identity. The property of unlinkability is desirable to ensure that the renewed biometric templates and the compromised biometric templates, belonging to the same biometric identity do not correlate. To validate the unlinkability of the proposed system, mated and non-mated pairs are generated. Mated template pairs refer to the biometric templates generated for the same biometric identity using different keys. Whereas, non-mated templates are generated for different biometric identities using different keys. The score distribution obtained by comparing the mated and non-mated template pairs is used for quantitative measurement of unlinkability. The system is said to be unlinkable if the mated score distribution completely overlaps the non-mated score distribution. To evaluate this overlap, we compute the global metric $\mathbf{D}_{\leftrightarrow}^{sys}$, defined in [47]. $\mathbf{D}_{\leftrightarrow}^{sys} \in [0, 1]$, where the system is completely unlinkable if $\mathbf{D}_{\leftrightarrow}^{sys} = 0$, and completely linkable if $\mathbf{D}_{\leftrightarrow}^{sys} = 1$. For this, mated and non-mated template pairs are generated using two scenarios, (a) by using the same set of keys and changing only the order of keys and (b) by changing the key set completely. $\mathbf{D}_{\leftrightarrow}^{sys}$ is calculated for the two scenarios for all four databases DB-1, DB-2, DB-3 and DB-4. Table VI validates the unlinkability of the proposed system wherein unlinkable metric $\mathbf{D}_{\leftrightarrow}^{sys}$ is observed to be close to zero for all four databases. Also, changing the order of keys, and changing the key set completely has the same effect on the unlinkability. This suggests that in order to generate biometric templates, the adversary requires not only the key images but also the order of key images. To further verify that the unlinkability property of the system, we plot the mated and non-mated score distribution in Fig. 5. where the two distributions display a significant overlap. Therefore, we assert that the proposed system supports unlinkability.

TABLE VI
UNLINKABILITY ANALYSIS FOR TEMPLATES GENERATED BY CHANGING (A) KEY ORDER, AND (B) KEY SET

Database	$\mathbf{D}_{\leftrightarrow}^{sys}$ (Change Key Order)	$\mathbf{D}_{\leftrightarrow}^{sys}$ (Change Key Set)
DB-1	0.13095	0.12881
DB-2	0.07453	0.09439
DB-3	0.10572	0.09894
DB-4	0.10638	0.11491

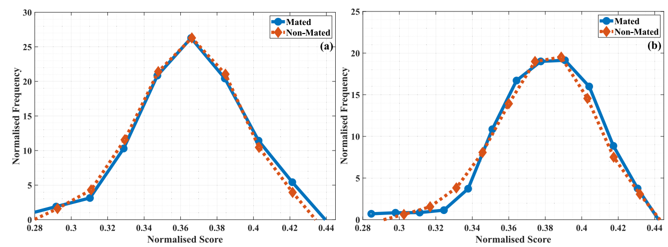

Fig. 5. Unlinkability Analysis: Changing (a) key order and (b) key set.

B. Security Analysis

Security attacks differ from privacy attacks in the fact that they are meant to gain illegitimate access into the system by either randomly guessing the biometric feature, i.e. (1) brute-force, or using instances of stolen templates to find correlation between template and biometric data, i.e. (2) ARM, or exploit the system's robustness to reject false identities, i.e. (3) false accept attacks. Additionally, (4) substitution attack complexity is assessed to scrutinize the ability of the system to resist denial of service attacks. Revocability property of the proposed approach is analyzed to ensure that the generated templates are robust. Finally, robustness against presentation attacks is investigated over benchmarked databases.

1) Brute-Force Attack: The attacker in a brute-force attack has no information about the transformation process, keys or the original templates [3]. In a brute-force attack, all possible combinations are tried by the attacker, hoping to guess a legitimate template. For multibiometric data with 3 modalities, template $\Gamma \in \mathbb{R}^{1\times 3n}$ is generated, where n keys are used. Value of each element in the template lies in the range $[0, \infty)$. A real-valued template has infinite guesses and can never be guessed. However, if the range of template values is stolen, an attacker might have a better chance. Therefore, to generate a template we consider the upper limit of the template value equivalent to 1000. It requires $3n^{1000}$ guesses to generate the correct template which is computationally infeasible. To analyze robustness against these attacks, random feature templates were generated and compared with the stored templates for DB-2. Fig. 6 validates the theoretical explanation, where impostor scores were plotted with brute-force attack genuine and impostor scores. Brute-force attack scores overlap completely with the impostor scores and support the claim of the infeasibility of brute-force attacks. Templates generated (a) using image quality and (b) without image quality are both robust to such attacks.

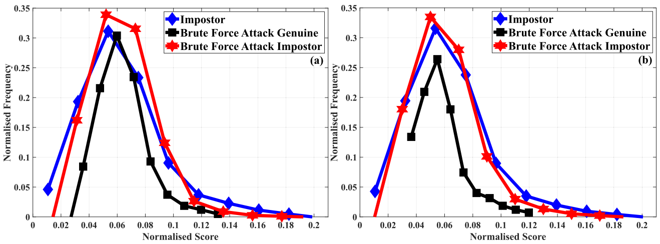

Fig. 6. Brute Force Attack Analysis: Impostor distribution and brute force attack genuine and impostor distribution (a) Adaptive, (b) Non-Adaptive.

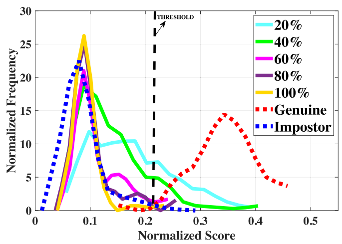

Fig. 7. Score distribution for partial knowledge of template, based on percentage of unknown or incorrectly guessed information about the template.

Since, partial knowledge of the template may result in a successful comparison with the enrolled templates, we further analyze the vulnerability of the system against partial matches. For this, we consider the case where an adversary manages to correctly guess $(100 - x)\%$ of the template values and rest of the $x\%$ are either unknown or incorrect. Fig. 7, compares the score distribution for genuine, impostor and pseudo-impostor for variable values of $x \in \{20\%, 40\%, 60\%, 80\%, 100\%\}$. Here, $x = 100\%$ represents the ideal brute-force attack case, where no prior information is known about the template. As x increases, the amount of randomly generated (or unknown values) in the template increases. This results in the pseudo-impostor distribution overlapping with the impostor distribution. From Fig. 7, it can be observed that even for low values of x, the score distribution peak for pseudo-impostors is near to the impostor distribution and only a small number of attempts successfully subvert the system by crossing the threshold at the operating point ($FAR = FRR$). Apart from this, even after the assumption of correctly guessing $(100-x)\%$ of the template values, estimation of remaining $x\%$ is quite complex for values of x, as low as 20% is $0.2 \times 3n^{1000}$. Therefore, the overall complexity for successfully executing a brute-force attack is computationally infeasible due the real numbered template (Γ), generated by a complex diffusion process.

2) Attacks via Record Multiplicity: Attacks via record multiplicity (ARM), also known as correlation attacks [48] utilizes multiple instances of templates that belong to the same biometric identity, but generated using a different set of parameters. Using multiple instances of a template, the attacker tries to determine the correlation between different parameters for reconstructing the original biometric data or the pre-image of the template. Considering two unified feature templates $\mathbf{\Gamma}_1$ and $\mathbf{\Gamma}_2$, which generated using the same biometric data, but different parameters: (a) set of key images, $K_j^{(k)} \in \{1, 2, \ldots, n\}$, (b) order of key images, (c) κ for KNN, and (d) $\lambda^{(k)} \in \{\lambda^{(p)}, \lambda^{(f)}, \lambda^{(i)}\}$. Unlinkability between these two templates has already been established experimentally. Also, j^{th} value in the template does not correspond to the j^{th} key image and is achieved using a complex computation that involves fusing information from different modalities at varying intensities. Further, another layer of protection is added by weighing the intermediary graphs using the image quality of the query image, and these weights cannot be obtained without the query image. Thereby, making it infeasible to either generate a pre-image or determine the correlation between templates $\mathbf{\Gamma}_1$ and $\mathbf{\Gamma}_2$. Therefore, the complex fusion of information from different modalities along with the involvement of an adaptive weighing technique accounts for the failure of an adversary to utilize multiple instances of templates to find a correlation and forge the system.

TABLE VII
FALSE ACCEPT ATTACK ANALYSIS

Original Database	Simulated Publicly Available Databases	EER (%)	
		Same Key	Different Key
DB-1	DB-2 + DB-3 + DB-4	0.278	0.264
DB-2	DB-1 + DB-3 + DB-4	0.208	0.215
DB-3	DB-1 + DB-2 + DB-4	0.230	0.205
DB-4	DB-1 + DB-2 + DB-3	0.351	0.273

3) False Accept Attack: A more sophisticated approach to gain illegitimate access is a false accept attack or dictionary attack, where the attacker is well versed with the template generation process. This increases the odds of generating a legitimate template [9], [48]. To perform a false accept attack, an adversary collects publicly available databases and generates templates using the template generation process. These pseudo-templates are used to access the system with a probability, equal to the False Accept Rate (FAR). To test the proposed system against false accept attacks, we simulate such an attack using all four databases used for performance evaluation. A subset of one database is generated by randomly selecting m subjects to represent the original template, and the remaining three databases are used to generate pseudo-templates using (a) same set of keys for both original and pseudo-templates and (b) different set of keys for original and pseudo-templates. This process is repeated for each database. Table III. reports the EER(%) for the experiment. For both the key scenarios, the proposed method system displays almost zero FAR, which confirms that the proposed system is robust to false accept attacks. Note that changing the key set does not affect the FAR by much, hence we assert that the proposed fusion process is robust to false accept attacks even for lost key scenarios.

4) Substitution Attack: In such attacks, an adversary may inject its biometric data and replace it with an enrolled biometric record ($\mathbf{\Gamma}_{user}$) [49]. However, the user may or may not possess the knowledge about the algorithms used in a system. Consequently, the enrolled bona fide user may witness a denial of service. This attack is majorly concerned with the security of the database and presents no loopholes in the proposed fusion approach. In AWGF, generating $\mathbf{\Gamma}_{attack}$ from the attacker's biometric data not only requires the knowledge of the complex multibiometric fusion algorithm, but also the

TABLE VIII

REVOCABILITY ANALYSIS FOR TEMPLATES GENERATED BY CHANGING (A) KEY ORDER, AND (B) KEY SET

Database	Impostor Mean	Genuine Mean	Change Key Order		Change Key Set	
			Pseudo-Impostor Mean	EER (%)	Pseudo-Impostor Mean	EER (%)
DB-1	0.0869	0.3310	0.0871	2.05	0.0873	2.10
DB-2	0.0851	0.3412	0.0851	1.02	0.0857	1.09
DB-3	0.0852	0.3296	0.0854	1.57	0.0853	1.55
DB-4	0.0879	0.3396	0.0880	2.31	0.0879	2.30

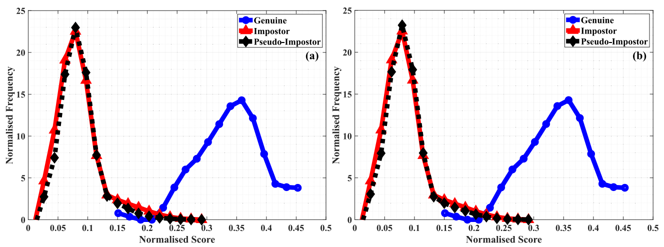

Fig. 8. Revocability Analysis: Plotting impostor, pseudo-impostor and genuine score distributions by changing (a) key order and (b) key set.

complex keys, i.e. key images. In the worst-case scenario where the attacker manages to crack the set of key images along with the order of key images, it would still be a futile exercise. This is because during enrollment all users share the same key images and generate highly distinct biometric templates. Further, generating a combination of all three biometric characteristics (fingerprint, face, and iris) is even more difficult to achieve. Thus, a multibiometric system that fuses information with complex keys is difficult to replicate. Hence, amalgamation with the enrolled user's biometric record would result in a denial of service attack at worst, preventing system access to both user and attacker. To reinstate the access for the enrolled user, templates can be revoked easily as discussed in the next subsection.

5) Revocability: In this subsection, we analyze the revocability of the proposed approach. Templates are renewed by changing the (a) order of keys, and (b) key set completely. For both scenarios, we plot impostor, pseudo-impostor and genuine score distributions [9] . In this, pseudo-impostors scores are generated by comparing two templates corresponding to the same subject that are generated using different keys. From Fig. 8, it is observed that the impostor and pseudo-impostor distributions for DB-2 show significant overlap, at the same time the genuine distribution is completely offset from the two distributions. This confirms the revocability of the proposed multibiometric system. To further validate the revocability, Table VIII reports the mean of these distributions along with the $EER(\%)$ corresponding to each database. It is interesting to note that changing the order of the keys has the same effect as changing the key set completely. Therefore, the proposed system need not find new key images in case the system is compromised, it just needs to change the order of the key images to revoke the templates.

6) Presentation Attack: Most biometric recognition systems evaluate performance under the ideal scenarios without considering the possibility of presentation attacks. In real-life scenarios, an adversary may supplant the enrolled user's biometric data with an acquired artifact and present it to the biometric capture subsystem in a malicious effort to subvert it.

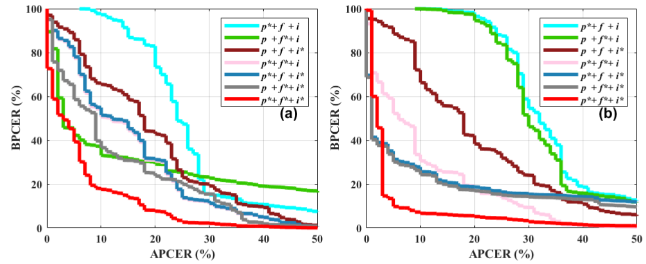

Fig. 9. DET curves for (a) non-adaptive and (b) adaptive AWGF for PAD analysis. $k^* =$ spoofed, $k =$ real, $\forall k \in \{p, f, i\}$.

To achieve reliability against such attacks, while ensuring unhindered access to bona fide users, image quality of the captured biometric data is employed in the adaptive mode of AWGF. In this section, we compare the performance of the non-adaptive and adaptive modes of AWGF to validate the effectiveness of incorporation of image quality against presentation attacks. For this, experiments are conducted using publicly available benchmark databases for presentation attacks, namely, Replay-Attack database [50] for face, Clarkson LivDet-Iris 2017 database for iris [51], and LivDet-fingerprint 2015 database [52] for fingerprint. Three subsets: *train*, *test* and *attack*, were formed such that *train* was used for enrollment, *test* and *attack* were employed as probe biometric data. For evaluation, we compute the Attacks Presentation Classification Error Rate (APCER): ratio of presentation attacks wrongly classified as bona fide or real; and Bona Fide Presentation Classification Error Rate (BPCER): ratio of bona fide presentations wrongly classified as presentation attacks.

Fig. 9 plots the DET curves between APCER and BPCER for both non-adaptive and adaptive AWGF for different combination of spoofed biometric characteristics. The result reveals that for single spoofed modality, the non-adaptive mode observes lower error rates than the adaptive version due to poor quality of spoofed images. In this, adaptive mode reduces the weights ($\lambda^{(k)}_{\text{spoof}} \forall k \in \{p, f, i\}$), and makes the decision based on comparatively high quality captured biometric characteristics. Further, when two modalities are spoofed, the cross fusion of forged information plays a pivotal role, along with the lowered weights for two modalities. Consequently reducing error rates more than the non-adaptive mode. Finally, when all three modalities are spoofed extremely low error rates are achieved, thus ensuring security against presentation attacks.

In sum, proposed key-based generic feature extraction in combination with AWGF provides robustness to security attacks and ensures cancelable properties like revocability, unlinkability, and non-invertibility in an effective manner.

VII. CONCLUSION

In this paper, we have proposed a multibiometric system to achieve high performance along with data protection. Key images based generic feature extraction makes template revocability a facile procedure where simply changing the order of keys results in renewed templates. Also, this drastically reduces feature dimension and hence require low computation and space requirements for realization in real-time. Cross diffusion of rank and sparse graphs extracts complementary information from three modalities, namely fingerprint, face, and iris. AWGF ensures complete non-invertibility and unlinkability of generated biometric templates. Adaptation of features with image quality faithfully resolves the *image quality conundrum*. For this, the non-linear relation between image noise and $EER(\%)$ is exploited to distinguish between 'mere low-quality images' and 'presentation attacks'. The proposed system performs favorably against various security and privacy attacks and hence suitable for security-critical applications.

In future, the proposed fusion approach can be improved to inherently adapt to varying security requirements through a dynamic thresholding mechanism. This would enable the system to operate at an application-specific accuracy-performance tradeoff. The proposed fusion approach displays moderately inferior time complexity compared to other state-of-the-art methods. Hence, this work can be investigated to ameliorate time complexity by carrying out independent computations in parallel. Also, the combination of multibiometric systems and image quality can be investigated for designing a standalone PAD module. Further, AWGF can be extended to other domains of computer vision bearing multimodal environments.

REFERENCES

[1] A. K. Jain and K. Nandakumar, "Biometric authentication: System security and user privacy," *Computer*, vol. 45, no. 11, pp. 87–92, Nov. 2012.

[2] N. K. Ratha, J. H. Connell, and R. M. Bolle, "Enhancing security and privacy in biometrics-based authentication systems," *IBM Syst. J.*, vol. 40, no. 3, pp. 614–634, Apr. 2001.

[3] K. Nandakumar and A. K. Jain, "Biometric template protection: Bridging the performance gap between theory and practice," *IEEE Signal Process. Mag.*, vol. 32, no. 5, pp. 88–100, Sep. 2015.

[4] V. M. Patel, N. K. Ratha, and R. Chellappa, "Cancelable biometrics: A review," *IEEE Signal Process. Mag.*, vol. 32, no. 5, pp. 54–65, Sep. 2015.

[5] J. K. Pillai, V. M. Patel, R. Chellappa, and N. K. Ratha, "Secure and robust iris recognition using random projections and sparse representations," *IEEE Trans. Pattern Anal. Mach. Intell.*, vol. 33, no. 9, pp. 1877–1893, Sep. 2011.

[6] M. Gomez-Barrero, C. Rathgeb, G. Li, R. Ramachandra, J. Galbally, and C. Busch, "Multi-biometric template protection based on bloom filters," *Inf. Fusion*, vol. 42, pp. 37–50, Jul. 2018.

[7] A. T. B. Jin, D. N. C. Ling, and A. Goh, "BioHashing: Two factor authentication featuring fingerprint data and tokenised random number," *Pattern Recognit.*, vol. 37, no. 11, pp. 2245–2255, Apr. 2004.

[8] Y.-L. Lai *et al.*, "Cancellable iris template generation based on indexing-first-one hashing," *Pattern Recognit.*, vol. 64, pp. 105–117, Apr. 2017.

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

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

[11] A. M. P. Canuto, F. Pintro, and J. C. Xavier-Junior, "Investigating fusion approaches in multi-biometric cancellable recognition," *Expert Syst. Appl.*, vol. 40, no. 6, pp. 1971–1980, 2013.

[12] G. S. Walia, S. Rishi, R. Asthana, A. Kumar, and A. Gupta, "Secure multimodal biometric system based on diffused graphs and optimal score fusion," *IET Biometrics*, vol. 8, no. 4, pp. 231–242, Jul. 2019.

[13] T. Chugh, K. Cao, and A. K. Jain, "Fingerprint spoof buster: Use of minutiae-centered patches," *IEEE Trans. Inf. Forensics Security*, vol. 13, no. 9, pp. 2190–2202, Sep. 2018.

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

[15] F. Alonso-Fernandez, J. Fierrez, D. Ramos, and J. Gonzalez-Rodriguez, "Quality-based conditional processing in multi-biometrics: Application to sensor interoperability," *IEEE Trans. Syst., Man, Cybern. A, Syst., Humans*, vol. 40, no. 6, pp. 1168–1179, Nov. 2010.

[16] N. Poh, J. Kittler, and T. Bourlai, "Quality-based score normalization with device qualitative information for multimodal biometric fusion," *IEEE Trans. Syst., Man, Cybern. A, Syst., Humans*, vol. 40, no. 3, pp. 539–554, May 2010.

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

[18] J. Bringer, C. Morel, and C. Rathgeb, "Security analysis of Bloom filter-based iris biometric template protection," in *Proc. Int. Conf. Biometrics (ICB)*, May 2015, pp. 527–534.

[19] D. Sadhya and S. K. Singh, "Providing robust security measures to Bloom filter based biometric template protection schemes," *Comput. Secur.*, vol. 67, pp. 59–72, Jun. 2017.

[20] H. Kaur and P. Khanna, "Random distance method for generating unimodal and multimodal cancelable biometric features," *IEEE Trans. Inf. Forensics Security*, vol. 14, no. 3, pp. 709–719, Mar. 2019.

[21] H. Kaur and P. Khanna, "Privacy preserving remote multi-server biometric authentication using cancelable biometrics and secret sharing," *Future Gener. Comput. Syst.*, vol. 102, pp. 30–41, Jan. 2020.

[22] J. Qiu, H. J. Li, and C. Zhao, "Cancelable palmprint templates based on random measurement and noise data for security and privacy-preserving authentication," *Comput. Secur.*, vol. 82, pp. 1–14, May 2019.

[23] R. Dwivedi, S. Dey, R. Singh, and A. Prasad, "A privacy-preserving cancelable iris template generation scheme using decimal encoding and look-up table mapping," *Comput. Secur.*, vol. 65, pp. 373–386, Mar. 2017.

[24] D. Sadhya and B. Raman, "Generation of cancelable iris templates via randomized bit sampling," *IEEE Trans. Inf. Forensics Security*, vol. 14, no. 11, pp. 2972–2986, Nov. 2019.

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

[26] D. Sadhya and S. K. Singh, "Construction of a Bayesian decision theory-based secure multimodal fusion framework for soft biometric traits," *IET Biometrics*, vol. 7, no. 3, pp. 251–259, May 2018.

[27] W. Yang, S. Wang, J. Hu, G. Zheng, and C. Valli, "A fingerprint and finger-vein based cancelable multi-biometric system," *Pattern Recognit.*, vol. 78, pp. 242–251, Jun. 2018.

[28] D. Zhong, H. Shao, and X. Du, "A hand-based multi-biometrics via deep hashing network and biometric graph matching," *IEEE Trans. Inf. Forensics Security*, vol. 14, no. 12, pp. 3140–3150, Dec. 2019.

[29] I. Chingovska, A. R. dos Anjos, and S. Marcel, "Biometrics evaluation under spoofing attacks," *IEEE Trans. Inf. Forensics Security*, vol. 9, no. 12, pp. 2264–2276, Dec. 2014.

[30] S. Wang and J. Hu, "A blind system identification approach to cancelable fingerprint templates," *Pattern Recognit.*, vol. 54, pp. 14–22, Jun. 2016.

[31] A. S. Chaudhari, G. K. Patnaik, and S. S. Patil, "Implementation of minutiae based fingerprint identification system using crossing number concept," *Inf. Economica*, vol. 18, no. 1, pp. 17–26, 2014.

[32] M. Haghighat, S. Zonouz, and M. Abdel-Mottaleb, "CloudID: Trustworthy cloud-based and cross-enterprise biometric identification," *Expert Syst. Appl.*, vol. 42, no. 21, pp. 7905–7916, Nov. 2015.

[33] A. T. Kahlil and F. E. M. Abou-Chadi, "Generation of iris codes using 1D Log-Gabor filter," in *Proc. Int. Conf. Comput. Eng. Syst.*, Nov./Dec. 2010, pp. 329–336.

[34] W. Kabir, M. O. Ahmad, and M. N. S. Swamy, "Normalization and weighting techniques based on genuine-impostor score fusion in multi-biometric systems," *IEEE Trans. Inf. Forensics Security*, vol. 13, no. 8, pp. 1989–2000, Aug. 2018.

[35] A. Mittal, R. Soundararajan, and A. C. Bovik, "Making a 'completely blind' image quality analyzer," *IEEE Signal Process. Lett.*, vol. 20, no. 3, pp. 209–212, Mar. 2013.

[36] Y. Yin, L. Liu, and X. Sun, "SDUMLA-HMT: A multimodal biometric database," in *Proc. Chin. Conf. Biometric Recognit.*, 2011, pp. 260–268.

[37] *CASIA-FingerprintV5*. Accessed: Feb. 13, 2019. [Online]. Available: http://biometrics.idealtest.org/

[38] R. Cappelli, M. Ferrara, A. Franco, and D. Maltoni, "Fingerprint verification competition 2006," *Biometric Technol. Today*, vol. 15, pp. 7–9, Jul./Aug. 2007.

[39] J. Ortega-Garcia *et al.*, "MCYT baseline corpus: A bimodal biometric database," *IEE Proc.-Vis., Image Signal Process.*, vol. 150, no. 6, pp. 395–401, Dec. 2003.

[40] W. Gao *et al.*, "The CAS-PEAL large-scale Chinese face database and baseline evaluations," *IEEE Trans. Syst., Man, Cybern. A, Syst., Humans*, vol. 38, no. 1, pp. 149–161, Jan. 2008.

[41] *CASIA-FaceV5*. Accessed: Feb. 13, 2019. [Online]. Available: http://biometrics.idealtest.org/

[42] A. Kumar and A. Passi, "Comparison and combination of iris matchers for reliable personal authentication," *Pattern Recognit.*, vol. 43, no. 3, pp. 1016–1026, 2010.

[43] *CASIA Iris Image Database*. Accessed: Feb. 13, 2019. [Online]. Available: http://biometrics.idealtest.org/

[44] G. O. Williams, "The use of d' as a 'decidability' index," in *Proc. 30th Annu. Int. Carnahan Conf. Secur. Technol.*, Oct. 1996, pp. 65–71.

[45] Q.-S. Sun, S.-G. Zeng, Y. Liu, P.-A. Heng, and D.-S. Xia, "A new method of feature fusion and its application in image recognition," *Pattern Recognit.*, vol. 38, no. 12, pp. 2437–2448, Dec. 2005.

[46] M. I. Ahmad, W. L. Woo, and S. Dlay, "Non-stationary feature fusion of face and palmprint multimodal biometrics," *Neurocomputing*, vol. 177, pp. 49–61, Feb. 2016.

[47] M. Gomez-Barrero, J. Galbally, C. Rathgeb, and C. Busch, "General framework to evaluate unlinkability in biometric template protection systems," *IEEE Trans. Inf. Forensics Security*, vol. 13, no. 6, pp. 1406–1420, Jun. 2018.

[48] B. Tams, P. Mihăilescu, and A. Munk, "Security considerations in minutiae-based fuzzy vaults," *IEEE Trans. Inf. Forensics Security*, vol. 10, no. 5, pp. 985–998, May 2015.

[49] W. J. Scheirer and T. E. Boult, "Cracking fuzzy vaults and biometric encryption," in *Proc. Biometrics Symp.*, Sep. 2007, pp. 1–6.

[50] I. Chingovska, A. Anjos, and S. Marcel, "On the effectiveness of local binary patterns in face anti-spoofing," in *Proc. Int. Conf. Biometrics Special Interest Group (BIOSIG)*, Sep. 2012, pp. 1–7.

[51] D. Yambay *et al.*, "LivDet iris 2017—Iris liveness detection competition 2017," in *Proc. IEEE Int. Joint Conf. Biometrics (IJCB)*, Oct. 2017, pp. 733–741.

[52] V. Mura, L. Ghiani, G. L. Marcialis, F. Roli, D. A. Yambay, and S. A. Schuckers, "LivDet 2015 fingerprint liveness detection competition 2015," in *Proc. IEEE 7th Int. Conf. Biometrics Theory, Appl. Syst.*, Sep. 2015, pp. 1–6.