Received May 20, 2020, accepted May 28, 2020, date of publication June 3, 2020, date of current version June 16, 2020.

*Digital Object Identifier 10.1109/ACCESS.2020.2999656*

# A Novel Cancelable FaceHashing Technique Based on Non-Invertible Transformation With Encryption and Decryption Template

**ALAMGIR SARDAR[1], SAIYED UMER[1], CHIARA PERO[2], AND MICHELE NAPPI[2], (Senior Member, IEEE)**

[1]Department of Computer Science and Engineering, Aliah University, Kolkata 700156, India
[2]Department of Computer Science, University of Salerno, 84084 Fisciano, Italy

Corresponding author: Chiara Pero (cpero@unisa.it)

This work was supported in part by the Italian National Research Project PRIN 2015 (201548C5NT) entitled "COntactlesS Multibiometric mObile System in the wild: COSMOS."

**ABSTRACT** A novel cancelable FaceHashing technique based on non-invertible transformation with encryption and decryption template has been proposed in this paper. The proposed system has four components: face preprocessing, feature extraction, cancelable feature extraction followed by the classification, and encryption/decryption of cancelable face feature templates. During face preprocessing, the facial region of interest has been extracted out to speed the process for evaluating discriminant features. In feature extraction, some optimization techniques such as Sparse Representation Coding, Coordinate descent, and Block coordinates descent have been employed on facial descriptors to obtain the best representative of those descriptors. The representative descriptors are further arranged in a spatial pyramid matching structure to extract more discriminant and distinctive feature vectors. To preserve them, the existing BioHashing technique has been modified and extended to some higher levels of security attacks and the modified BioHashing technique computes a cancelable feature vector by the combined effect of the facial feature vector and the assigned token correspond to each user. The elements of computed cancelable feature vector are in a numeric form that has been employed to perform both verifications as well as identification task in online while the original facial feature vectors are kept offline either in hard drive or disc. Then, to enhance more security levels and also to preserve the cancelable face features, an RSA based encryption-decryption algorithm has been introduced. The proposed system has been tested using four benchmark face databases: CASIA-FACE-v5, IITK, CVL, and FERET, and performance are obtained as correct recognition rate and equal error rate. The performance are compared to the state-of-the-art methods for the superiority of the proposed feature extraction technique and individual performance analysis has been performed at all the security levels of the proposed Cancelable FaceHashing Technique. These comparisons show the superiority of the proposed system.

**INDEX TERMS** Cancelable, FaceHashing, feature extraction, encryption, classification.

## I. INTRODUCTION

Nowadays, the most rising technology for person recognition is based on human biometrics traits. Among the various biometric traits face biometric has vast applications, including surveillance systems, border security, law enforcement, access control, and entertainment systems. Compared to other biometric traits face is easily captured during standing and walking of a person without his/her interaction with the system. The facial recognition system plays an important role in the human perception systems [1] where the eyes, nose, mouth, jaw are very crucial features. The face biometric is more suitable and convenient than the other biometric traits such as Palmprint, Fingerprint, DNA, Signature, and Voice as it has intangible characteristics. The face biometric gives the dynamic features to the authentication system for the large organizations such as in the educational institutions, the offices with thousands of employees, the borders security checking, etc. This recognition system is cheaper than the others biometric system but it suffers from various challenging issues like lighting variations, different emotional expressions (anger, happy, sad, surprise, disgust, fear), wearing of

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

accessories (such as cap, scarf, glass), hairstyle, eyebrows, mustache, bread with frontal and profile faces [2]. Due to these challenges, there may be the possibility of performance degradation of the recognition system.

Authentication using biometric traits is more difficult than the text-based techniques using email and ATMs [3]. These weak authentication techniques give rise to different types of attacks like replay, fraud customer, malicious code, man-in-middle, session hijacking and many more [4]. Rui and Yan [5] had reviewed the existing biometric authentication systems by focusing on the security and their privacy solutions. Biometric trait contains sensitive information and permanent to each person. Unfortunately, if it is stolen or compromised then there will be a high risk for the system that the users' privacy may be compromised. A biometric template protection scheme must have the following characteristics [6]: (i) *Diversity* means to ensure privacy and avoid cross-matching between the templates, (ii) *Revocability* means the compromised templates can be revoked and can be replaced by the new template generated from the original biometric treat, (iii) *Security* will ensure that the original template cannot be regenerated from the unsecured template, (iv) *Performance* of the biometric system can not be reduced by the employed template protection scheme.

The objectives of this paper are to (i) provide security to the original face biometric template, (ii) handle the situation when the face biometric template is compromised, (iii) enhance the security level of template protection without reducing the performance of the face recognition system. Hence to fulfill these objectives, the contributions of this work are as follows:

- A novel faceHashing technique has been proposed where the implementation of the proposed system has been divided into four components.
- In the first component, the image preprocessing task has been applied on the input image to extract the facial region which is extracted by the tree-structured part model (landmarks detector on the facial region) and then from the detected facial region, the texture patterns are analyzed statistically by applying some optimization techniques such as sparse representation, coordinate descent, and block coordinate descent techniques.
- In the second component, the extracted feature vectors from the face samples undergo the proposed template protection scheme where both cancelable and encrypted biometric feature extraction schemes have been proposed. The proposed cancelable biometric scheme provides better resolution of regeneration or reissue of new temples when the stored template is crashed or compromised and also preserves the original facial features from unpacking and irreversible security requirements. Here the cancelable biometric scheme works for both verification (authentication) and identification (recognition) tasks.

**TABLE 1. List of notations and symbols.**

| Symbol | Definition |
|---|---|
| $\mathscr{F}$ | Extracted facial region |
| $f$ | Input feature vector, $f \in \mathbb{R}^d$ |
| $q_j$ | A SIFT descriptor, $q_j \in \mathbb{R}^D$ |
| $\alpha_j$ | Sparse co-efficient of $q_j$ |
| $\mathscr{C}$ | a corpus to yield $\alpha$ |
| $\lambda$ | Regularization parameter |
| $\mathscr{S}$ | different matching similarity scores |
| CRR | Correct Recognition Rate |
| EER | Equal Error Rate |
| $g$ | Bio-Hash code (bit-vector) $g \in \{0,1\}^n$ |
| $n$ | The length of the bit string ($n \leq d$) |
| $d$ | Feature vector dimension |
| $R_i$ | A set of pseudo-random vectors $\{R_i \in \mathbb{R}^{d\times n} \mid$ i=1, ...,n } |
| $O_i$ | An ortho-normal set of vectors $\{O_i \in \mathbb{R}^d \times n \mid$ i=1, ...,n } |
| $\rho$ | A present threshold |
| '$t_s$' | Subject specific token |
| '$t_{\mathbb{F}}$' & '$t'_{\mathbb{F}}$' | Systems dependent tokens |
| $Z_{\mathscr{F}}$ | Cancelable feature vector |
| $t_{RSA}$ | System token for RSA algorithm |
| $CFR$ | Cancelable Face Recognition |

- In the third component, the cancelable facial feature vectors are being encrypted by applying the RSA algorithm to provide a higher level of the template protection scheme for better security requirements. Here the RSA algorithm has been modified in such a way that it uses two keys: public and private where the size of these keys is typical $2^{10}$ or $2^{11}$ that enhances the strength of the encryption algorithm exponentially and will protect the system from the infeasible task for breaking the keys.
- Finally, the proposed cancelable face features undergo to the multi-class subject (person) identification system to obtain the performance of the face recognition system.

The organization of this paper is as follows: Section II describes the preliminary analysis and the related works for the proposed system. Section III describes the implementation of the proposed system. The experimental results and discussions are reported in Section IV. Section V concludes this paper. The Table 1 summarizes the major symbols used in this paper.

## II. PRELIMINARY ANALYSIS

### A. BIOMETRIC-ATTACKS

In literature, the Cancelable Biometric System is subject to various security attacks, i.e. sensor level, application level, and database level. Biometric-attacks are the types of attacks through which the biometrics information is compromised. There exist several attacks in the biometric system. Ratha *et al.* [7] and Malhotra and Kant [8] had illustrated various possible attacks that had compromised the database or the channel between the different steps of the biometric authentication system. Brute force, Attack via Multiplicity, Lost token, Dictionary-based, Spoofing, Intrusion, Cryptanalysis, Hill climbing, Inverse, and Pre-image attack is just some of the existing attacks [9]. In the Lost token attack, an intruder knows some information i.e. user token/ password. Through a Brute force attack, an impostor attempts various combinations of password/key to log into the system. In a Dictionary-based attack, an intruder determines decryption

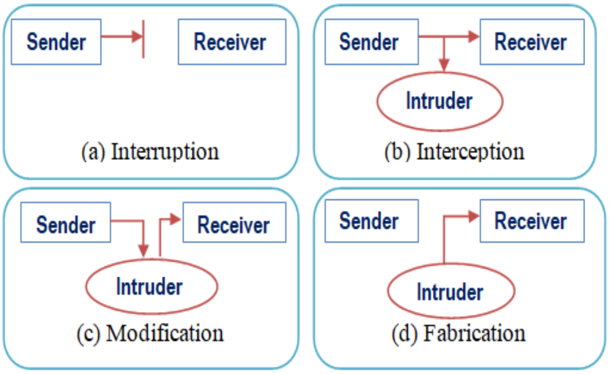

**FIGURE 1.** Examples of attacks in the biometric system.

key or passphrase by trying hundreds or sometimes millions of likely possibilities. The Crypto-analysis attack assumes that the attacker has access only to a set of ciphertexts. Biometric spoofing [10] is one of the most persistent attacks which is related to spoofing attack on biometric templates. Singh *et al.* [11] had described some possible attacks during data transmission such as (a) Interruption attack where information of the system becomes unusable or unavailable and destroyed (i.e message corruption, malicious code insertion, and making information unavailable), (b) Interception attack where an unauthorized person gains the data access i.e. illegal file copy, wiretapping to capture information within the network, etc., (c) Modification attack where the unauthorized person not only access the system but also tampers the data i.e. changing the values in a file, modify the message contents, and alter the programming codes, etc., (d) Fabrication attack where the unauthorized person inserts the false information to the system i.e. insertion of a fictitious message during online-authentication. Fig. 1 demonstrates these attacks.

### B. BIOMETRIC-PROTECTION

Biometric templates can be protected by (a) Hardware-based techniques and (b) Software-based techniques. Hardware-based template protections can be performed by a smart card assisted hardware which is known as match-on-card technique. Software-based biometric template security can be achieved by (i) Template Image Transformation based techniques, (ii) Feature Transformation based techniques and (iii) Biometric Cryptosystems based techniques. The detailed classification of these biometric template protection schemes is shown in Fig. 2. Jain *et al.* [12] had classified the different biometric template protection methods as (i) Feature Transformation methods and (ii) Biometric Encryption methods. These are the basic template protection techniques that are further extended to other template protection techniques shown in Fig. 2. A comprehensive overview of existing privacy preserving biometric schemes with various guidance for future privacy preserving biometric methods have been demonstrated by Natgunanathan *et al.* [13].

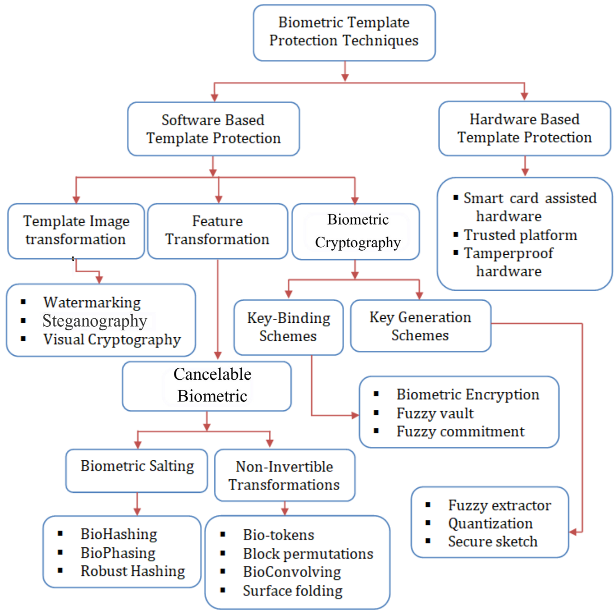

**FIGURE 2.** List of template protection schemes in the biometric system.

The Template Image Transformation can be done by watermarking, steganography and visual cryptography. In *biometric watermarking* technique, if any imposter tries to replace the biometric template then he/she must have the concept about pixel values where the watermark information is kept invisible [8]. In Feature Transformation, a transformation function $f$ is applied to transform a biometric template $\mathscr{T}$ into $\mathscr{T}' = f(\mathscr{T}, k)$, using a random generated key $k$. Feature transformations are of two types: (i) invertible (e.g. BioHashing) and (ii) non-invertible (e.g. Cancelable biometrics) [14]. In invertible transformation, the generated key $k$ is applied to get back the original template $\mathscr{T}$ and in non-invertible transformation, the key $k$ is one-way and hence it is difficult or maybe impossible to revert into original template $\mathscr{T}$, even $k$ is known [15]. In cancelable biometrics, if biometric templates are compromised then it can never be replaced like other traditional systems such as PIN, password or token-based security systems. To overcome these issues Radha and Karthikeyan [16] had introduced the non-invertible transformation as cancelable biometric for fingerprint security so that the biometric templates can be canceled or replaced and this can be done simply by changing the transformation parameters when misplaced. If the imposter knows the transformation parameter then the transformation parameter will be unsecured. The other major drawback of cancelable biometric is that the recognition performance of the biometric systems is reduced due to the distortion of biometric data during transformation. A cancelable Delaunay triangle-based fingerprint matching algorithm for the insulin pump had been proposed by Zheng *et al.* [17] where the nonlinear fingerprint image distortion and the influence of missing or spurious minutiae had been preserved. Murakami *et al.* [18] had proposed the Cancelable Permutation-Based indexing scheme that was promising with regard to both security and efficiency for the face, fingerprint, and finger-vein biometrics identification system. In literature, there are many transformations adopted

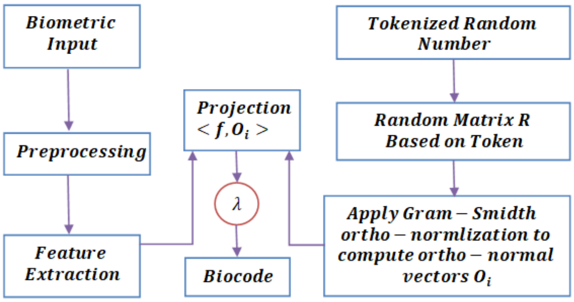
Biometric Input
Preprocessing
Feature Extraction
Projection $< f, O_i >$
$\lambda$
Biocode
Tokenized Random Number
Random Matrix R Based on Token
Apply Gram – Smidth ortho – normlization to compute ortho – normal vectors $O_i$

**FIGURE 3.** A schematic diagram of existing BioHashing.

for generating cancelable biometric templates. In [19] the authors propose an non-invertible template transformation approach using random projection technique and Discrete Fourier transformation to shield the binary biometric pseudo-random representations. A Cancelable ECG Biometric based recognition system using Compressive Sensing-Generalized Likelihood Ratio Test had been proposed by Kim & Chun in [20]. A one-factor cancelable palmprint biometric recognition scheme based on Orthogonal Index of Maximum hash and Minimum Signature Hash had been proposed by Wang and Li [21]. Recently, Kaur and Khanna [22] proposed a novel transformation technique, called Random Distance Method (RDM), in order to generate a pseudo-biometric identities and dimensionally reduced templates and Punithavathi *et al.* [23] introduced a cloud-based lightweight cancelable fingerprint authentication system.

### C. BIOMETRIC-HASHING (BioHashing)

BioHashing [24], [25] is one of the reliable Biometric template protection techniques are used at present. BioHashing was proposed by Teoh et al (2004) [26]. The objective of BioHashing is to generate a binary BioCode. Fig. 3 demonstrates the principle of BioCode generation using BioHashing. In the BioHashing technique, biometric features are combined with a tokenized random number (TRN) to generate BioCodes. This technique is used while enrolment and verification of the subjects. In enrolment, the generated BioCode is stored and during verification, BioCode is recomputed during authentication of the subject. The BioHashing technique uses a random projection technique to reduce the dimension of the original biometric feature vector. It is done after the biometric feature extraction task. The BioHashing procedure demonstrates various advantages; firstly, it presents a clear separation of the genuine and the imposter populations and zero EER level. BioHashing template has also high tolerance to data acquisition offsets so that the same biometric trait captured at different times will produce highly correlated bit strings (BioHashes) [27]. The BioHashing technique addresses the problem of irrevocability of biometric features: if the attacker compromises the stored templates, the user can easily replace the one-way transform function with a new one by using a different secret seed for enrolment or replace the token [27], [28]. The main drawback of the BioHash approach is the degradation in matching performance when an adversary has access to a user's secret key (seed) and uses the legitimate key with their own biometric features in order to fool the authentication system. Hammad *et al.* [29] have applied modified BioHashing and Matrix Operation techniques a human authentication system based on ECG signals.

BioHashing technique yields a bit-vector $g \in \{0, 1\}^n$ where a biometric feature vector $f \in \mathbb{R}^d$ is reduced to the bit-vector $g \in \{0, 1\}^n$ with bit-length n ($n \leq d$). The algorithm for generating the bit-vector $g$ is as follows:

1) Given subject specific token, 't' (i.e. hash key used as secret key) generates the series of random numbers to produce set of pseudo-random vectors $\{R_i \in \mathbb{R}^{d\times n} \, |i = 1, 2, 3, \ldots, \mathrm{n}\}$ bases on seed values.
2) Applying Gram–Schmidt ortho-normalization algorithm to transform the random vectors $\{R_i \in \mathbb{R}^{d\times n}$ into set of ortho-normal vectors $\{O_i \in \mathbb{R}^d \times n$ $|i = 1, 2, 3, \ldots, \mathrm{n}\}$.
3) Perform inner product (i.e. projection) between biometric feature vector (f) and ortho-normal vectors ($O_i$) such that $\langle f, O_i \rangle$
4) Choose a threshold '$\rho$' to get the BioCode, $g = [g_1, g_2, \ldots, g_n]$ using (1).

$$g_i = \begin{cases} 0, & \text{if } \langle f | O_i \rangle \leq \rho \\ 1, & \text{if } \langle f | O_i \rangle > \rho \end{cases} \tag{1}$$

Fig. 3 demonstrates the existing BioHashing technique.

### D. BIOMETRIC-CRYPTOGRAPHY

This system is a combination of "Biometrics" and "Cryptography" [30]. It is one of the techniques to protect biometric information during authentication/recognition. Since the keys (PIN, password) are easy to keep in mind as well as easy to hack. Moreover, the complex keys are difficult to memorize and crack. Therefore, these keys are used to protect from unauthorized access. To overcome these problems the cancelable biometric recognition system has been extended to Bio-Cryptography [31] system. The Bio-Cryptographic system gives an opportunity to increase the security and convenience of many applications like access control, financial transactions, mobile devices, ATMs, etc. It ensures the biometric systems with the maximum security level. The Bio-Cryptographic [32], [33] had been introduced for two purposes (i) to generate a strong cryptographic key from the biometric features and (ii) to protect the biometric features using strong cryptographic keys.

Ross *et al.* [34] had classified the BioCryptosystems into *Key Generation* and *Key Binding* where in *Key Generation*, the biometric key is directly generated from the biometric data [35] while in *Key Binding*, the biometric template and the secret key are tied up within a cryptographic framework and makes the system impossible to decode the biometric template or the key without any prior knowledge of biometric data [36]. The keys used for encryption and

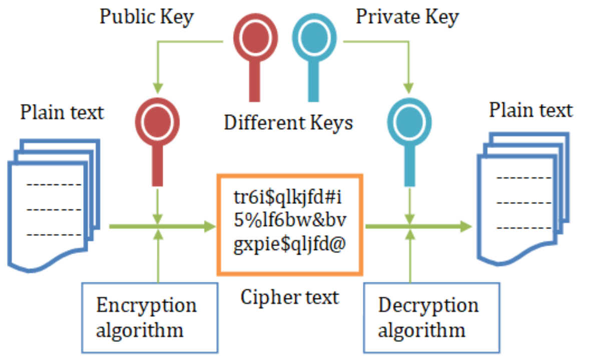

**FIGURE 4.** Asymmetric key encryption.

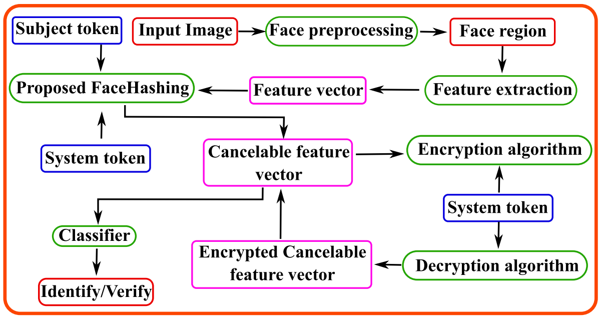

**FIGURE 5.** Block diagram of the proposed system.

decryption cryptography can be further classified into two types: (i) *Symmetric key* also known as *secret key* or private key cryptography where both sender and receiver uses the same key for encryption and decryption and (ii) the *Asymmetric key* or *public key* uses one public key and another one private key. The sender uses the public keys to encrypt the message while the receiver uses the private key to decrypt the message. Public key cryptosystems were first introduced by Diffie and Hellman [37]. The proposed method belongs to public key Cryptography. An example of Asymmetric key cryptography has shown in Fig. 4.

Teoh *et al.* [38] proposed a two-stage cryptographic key generation method based on FaceHashing wherein first stage, biometric image is discretized to generate FaceHash while in the second stage, FaceHash is reduced to a cryptographic key. Nagar and Chaudhury [39] had designed an asymmetric cryptosystem based on biometrics where a new biometric-based cryptosystem had been revealed for fingerprint biometrics by modifying the fuzzy vault scheme. Maiorana *et al.* [40] had developed the non-invertible transformation based template protection technique for an online signature authentication system using the Hidden Markov Model technique. Islam *et al.* [41] had employed a watermarking template protection scheme with the hidden password encryption-based algorithm for fingerprint and palmprint biometrics. Lalithamani and Soman [42] had built an irrevocable cryptographic key generation method from the cancelable fingerprint templates. Chin *et al.* [43] had developed the bit-string generation method for the multimodal biometric template protection scheme. Rua *et al.* [44] had built the biometric template protection approach by using fuzzy commitment and Eigen spaces feature representation. A Smart Card Based Cancelable Finger-Vein Bio-Cryptosystem for securing mobile healthcare data through fuzzy commitment biometric cryptographic technique had been proposed by Yang *et al.* [45]. Kanagalakshmi and Chandra [46] had built 'Complex Conjugate Phase Transform Technique' to generate the cancelable and irrevocable template for fingerprint biometric. Yang and Martiri [47] had introduced a template generation method based on machine learning techniques with cryptographic hash values. Mwema *et al.* [48] had surveyed on various biometric template protection techniques for fingerprint biometric templates. Chee *et al.* [49] had integrated the template protection technique by using '2D Winner Takes All Hashing' technique to protect the templates. Umer *et al.* [50] have developed the cancelable biometric system for both verification and identification purposes for iris biometrics.

## III. PROPOSED SCHEME

In the proposed system we have considered the face biometric for the face recognition system. The face biometric is more non-invasive and needs less contact with the user during image acquisition. Moreover, sometimes the images are captured at varying distances while subjects are moving due to these issues, the captured images suffer from distortion, motion-blurred, results in insufficiency of texture patterns in the facial region. The face recognition works at the time of eye blinking, off-angle, different facial poses, etc. So, the face biometric has been considered here for faceRecognition, faceHashing, and faceCrypto system. The diagrammatic description of the proposed system has been shown in Fig. 5 which shows the four steps of the proposed system such as preprocessing, feature extraction, classification and template protection. In the preprocessing step, the face region is detected from the input image. Then features are computed from the preprocessed face region in the second step. During classification, the features are classified and the scores obtained for each subject (person) have been used to obtain the final decision for the identification of the subjects in the third step. In the fourth step, a modified BioHashing technique has been proposed for FaceHashing which is further extended to the FaceCrypto system. So, the proposed system has following advantages: (i) Both identification and verification performance of the proposed face recognition system is much higher than the state-of-the-art methods and it is due to the employed feature representation technique that uses the combined effect of Sparse Representation Coding, Coordinate Descent and Block Coordinate Descent optimization techniques with the descriptors extracted locally from the facial region. (ii) Here the proposed FaceHashing system has obtained better performance in terms of both verification and identification with much higher accuracy and it is due to the transformation of the numeric-form of cancelable features whereas the existing BioHashing can perform only

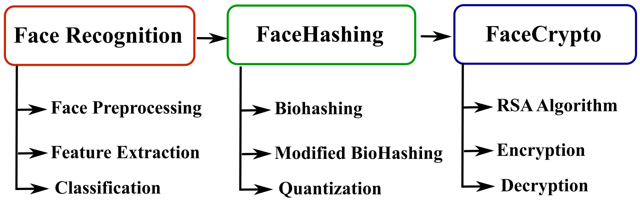

**FIGURE 6. Component division of the proposed system.**

verification performance as elements of cancelable templates in those BioHashing are in 1/0 bit string form. (iii) The proposed FaceHashing system provides a higher level of securities to the original feature vectors in such a way that the recognition tasks will be performed online while the original feature vectors may be kept offline in the external hard disc or derive. (iV) The proposed FaceHashing system offers a better solution of reissuing/regenerating a new feature template when the stored template is crashed or compromised. (v) Even with smaller feature dimensions, the proposed system achieves high accuracy in case of both verification and identification of a subject by preserving its distinctive and discriminating nature. (vi) A novel encryption-decryption technique based on the RSA algorithm has been introduced in the proposed FaceHashing system to provide a higher level of the template protection scheme for better security requirements.

## *A. FACE RECOGNITION*

The working flow diagram of the proposed system with different sub-components in each component has been shown in Fig. 6.

### 1) IMAGE PREPROCESSING

The captured images in an unconstrained environment carry numerous challenging issues like lighting variations, different expressions, poses, occlusion by accessories, and low-resolution artifacts. Due to these variations, the quality of the images degrade. To handle these situations, here we have employed a unified Tree-Structured Part Model (TSPM) [51] to extract the face region from the input image $\mathscr{F}$. The TSPM simplifies the face detection, facial landmarks detection and poses estimation. The working principle of TSPM is based on the combination of trees where each tree $\mathbb{T}$ represents a node that contains two elements i.e. the facial landmarks as parts $\mathbb{V}$ and the connection between those parts i.e. $\mathbb{E}$. Hence each tree $\mathbb{T} = (\mathbb{V}, \mathbb{E})$. The TSPM performs the global composition of capturing the topological changes due to different viewpoints of face region and for the TSPM uses a separate template which is the mixture of each tree i.e. $\mathbb{T}_m = (\mathbb{V}_m, \mathbb{E}_m)$, 'm' indicates a mixture and $\mathbb{V}_m \subseteq \mathbb{V}$. At each template, it computes the histogram of orientated gradient (HoG) descriptors and performs the Tree-structured part model on those descriptors to find 68 landmark points for frontal face region while 39 landmark points for profile face region. The demonstration of face pre-processing tasks for the proposed system has been illustrated in Fig. 7.

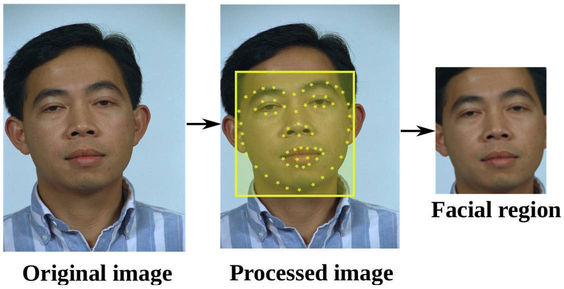

**FIGURE 7. Preprocessed face region for the proposed system.**

### 2) FEATURE EXTRACTION

The extracted face region from the above processes undergoes to feature computation. The extraction of features from the input image is the transformation of the input image to a set of features which have distinctive and discriminate information. During image acquisition, the images are captured in uncontrolled environments that make the images more challenging by introducing noise artifacts that result in the degradation of image quality. Hence, the smaller regions are very much important for feature computation, so, an efficient and discriminatory feature representation scheme has been required to handle various challenging issues and also to handle the degradation factors of the biometric data. During feature computation from biometric data, the images are considered as textures and the patterns (texels) in those textures are analyzed. For this analysis of texture patterns mainly transformed, structural, and statistical approaches [52] are employed. The transformed approaches obtain the gradient information from the texture patterns by analyzing the patterns in the multi-resolution ways while the structural approaches extract the geometric information such as blobs, shapes, contours, etc from the texture patterns. Apart from these approaches, the statistical approach derives the distribution of texture patterns in terms of descriptors (e.g. histogram of oriented gradients, scale-invariant feature transform, local binary pattern) and then use these descriptors to obtain the feature representation of descriptors by applying some optimization techniques that obtain more discriminant features. A multimodal biometric authentication system using convolution neural network based on different level fusion of ECG and fingerprint biometric had been proposed by Hammad *et al.* [53].

In this work, from each facial region $\mathscr{F}$, we consider a patch $p_i \in \mathbb{R}^{n \times n}$ over $\mathscr{F}$ by 75% overlapping of pixels along both horizontal and then vertical directions. From each $p_i$, densely SIFT descriptors $Q_{p_i} = \{q_1, q_2, \ldots q_z\} \in \mathbb{R}^{D \times z}$, where $D$ be the dimension of each descriptor $q_i$ and $z$ is the number of descriptors from each patch $p_i$. Thus for $\mathscr{M}$ number of patches, the descriptors from $\mathscr{F}$ can be obtained as $\mathscr{Q} = \{Q_1, Q_2, \ldots Q_i, Q_{i+1}, \ldots Q_L\} \in \mathbb{R}^{D \times L}$ where $L = \mathscr{M} \times z$. Here for dense SIFT feature extraction we have employed *vlfeat* [54] software. Since from each patch $p_i$, $z$ number of descriptors are obtained while each descriptor $q_j$ contains scale invariant gradient features along with noise artifacts, so (i) to extract useful information from each descriptor $q_j$, (ii) to handle the large collection of descriptors $\mathscr{Q}$ simultaneously, and (iii) to achieve good performance by extracting distinctive and discriminant features, some extra optimization algorithms have been employed. The optimization algorithm performs feature learning task on each descriptor $q_j$ and obtains its representation in another feature space i.e $q_j \rightarrow \alpha_j$.

During feature learning we have employed Sparse Representation Coding (SRC) [55], Coordinate-descend (CD) [56] and block coordinate descent (BCD) [57] techniques. Here each feature learning technique considers the descriptors $\mathscr{Q}$ and a corpus $\mathscr{C}$ to yield $\alpha$ (co-efficient). Here from $M$ training samples, the SIFT descriptors are extracted and obtain a collection $\{\mathscr{Q}_1, \cdots, \mathscr{Q}_M\} \in \mathbb{R}^{D\times(M\times L)}$. Then descriptors from $\{\mathscr{Q}_1, \cdots, \mathscr{Q}_M\} \in \mathbb{R}^{D\times(M\times L)}$ are grouped by applying the dictionary learning algorithm [58] to obtain a corpus $\mathscr{C} = [c_1, \cdots, c_k] \in \mathbb{R}^{D\times k}$. The objective of feature learning techniques is to represent each facial region $\mathscr{F}$ as the spectrum of code-words from corpus $\mathscr{C}$ which give rise to $\alpha_j = (\alpha_{j1}, \alpha_{j2}, \ldots, \alpha_{jk})^T \in \mathbb{R}^{k\times 1}$, a non-local statistical descriptor i.e. coefficients for each descriptor $q_j$. This $\alpha_j$ is the coefficients for $q_j = \alpha_{j1}.c_1 + \alpha_{j2}.c_2 + \ldots + \alpha_{jk}.c_k$ representation and it is obtained by solving the following optimization technique:

$$\begin{aligned} &\arg\min_{\alpha} \sum_{j=1}^{L} ||q_j - \mathscr{C}\alpha_j||^2 + \lambda||\alpha_j||_1 \\ &\text{such that} \sum_i \alpha_{ji} = 1, \quad \alpha_{ji} \geq 0, \ \forall j \end{aligned} \tag{2}$$

where the constraint $||\alpha_j||_1 = 1$ is the sparsity regularization term with regularization parameter $\lambda$. Here this constraint $||\alpha_j||_0 = 1$ is $l_1$-norm which is the sum of absolute values of $\alpha_{ji} \in \alpha_j$. The functioning nature of $l_1$-norm is non-smooth, non-differential, convex and a square with $45^o$ in 2-dimensional space. The solutions of $l_1$-norm minimization are sparse in nature. The SRC technique in (2) generates the similar codes for similar descriptors that results good classification performance in the mean while the regularization term with $||\alpha_j||_1$ in (2) is not smooth and sometimes it selects different code-words for similar descriptors $q_j$s which is due to the over-completeness of corpus $\mathscr{C}$. To overcome the problems of over-completeness, the (2) has been modified as follows:

$$\begin{aligned} &\arg\min_{\alpha} \sum_{j=1}^{L} ||q_j - \mathscr{C}\alpha_j||^2 + \lambda||\alpha_j||_1 + \frac{\lambda^2}{2}||\alpha_j||_2^2 \\ &\text{such that} \sum_i \alpha_{ji} = 1, \quad \alpha_{ji} \geq 0, \ \forall j \end{aligned} \tag{3}$$

where $||\alpha_j||_2$ is $l_2$-norm and its functioning nature is convex, smooth, differential and a circle in 2-dimensional space. The (3) is Coordinate-descend (CD) technique which is powerful and simple and it generates the coefficient matrix $A = [\alpha_1, \cdots, \alpha_L] \in \mathbb{R}^{k\times L}$ where each $\alpha_j \in A$ is corresponding to $q_j$. The CD technique in (3) uses heuristics and results better performance when the code-words in corpus have high correlation between them. Apart from this, a block coordinate descent (BCD) technique has been obtained from the CD technique which uses both $l_1$ and $l_2$-norm minimization where for a given set of descriptors $\mathscr{Q} = [q_1, \cdots, q_N]$, and corpus $\mathscr{C}$, the BCD technique returns $A = [A_1, \cdots, A_N] \in \mathbb{R}^{k\times N}$ solution, where $A_i \in \mathbb{R}^{k\times\beta}$, which is an approximate solution for the following problem.

$$\begin{aligned} &\arg\min_{A_i} \sum_{j=1}^{N} ||\mathscr{Q}_j - \mathscr{C}.A_j||^2 + \frac{\lambda}{\sqrt{\beta}}||A_j||_{l_2,l_1} \\ &\text{such that} \sum_j \sum_i A_{ji} = 1, \quad A_{ij} \geq 0, \ \forall j \end{aligned} \tag{4}$$

This BCD method provides fast convergence and is free from parameters. Moreover, it does not require any learning rate during tuning [57]. During feature computation, the spatial relationships play an important role and for this, the spatial pyramid mapping (SPM) [59] has been employed which performs pyramid matching technique on the coefficients $\alpha$s obtained corresponding to the image descriptors and this can work by partitioning the image into increasing fine sub-regions. Then from each sub-region, the histogram of coefficients is obtained and finally, the histogram from each sub-region is concatenated to form a feature vector for the image $\mathscr{F}$. Hence, the obtained $\alpha$ from SRC or CD or BCD technique undergoes to SPM to level $\ell = 0, \cdots, p$, the corresponding feature vectors say $f_S$ or $f_C$ or $f_B$ are obtained respectively, such that the dimension of each feature vector is $k \times \sum_{\ell=0}^{P} 2^{2\times\ell}$, where $k$ is the number of code-words in $\mathscr{C}$.

### 3) CLASSIFICATION

The feature vectors extracted from the above feature learning techniques undergo to the classification task. For classification, we have employed the multi-class linear SVM classifier [60] with K-fold cross-validation (CV) scheme. Here a variant of k-fold CV method i.e. train-test split scheme has been employed. In the train-test split method, the value of K is set to 2 such that the single train-test split is created to evaluate the model and the performance is obtained for the test dataset. This procedure is repeated ten times and the averaged performance has been reported for the proposed system. Here the identification performance has been obtained for each subject where $\mathscr{S}$ different scores (similarity) are obtained by comparing the test sample with each of the $\mathscr{S}$ prototypes of the subjects enrolled in the database. Then these $\mathscr{S}$ scores are arranged in descending order and a rank is assigned to each sorted score. The subject corresponding to the highest rank (i.e. *Rank* 1) is declared as the identity of the test sample. So, the number of correct matching of *Rank* 1 of each subject over the total number of subjects in the database will show the correct recognition rate (CRR). Here the identification performance has been obtained in terms of correct recognition rate (CRR) in %. Here we have also presented the verification performance which is evaluated through the true-positive rate and the false-positive rate and for this equal error rate (EER) [61] has been reported.

### B. FaceHashing

FaceHashing is a variant of BioHashing [26] to generate FaceCode ($\mathbb{F}$) from the feature vector extracted from the facial region. To perform the proposed FaceHashing technique, we have used three tokens: one subject specific token '$t_s$' and two system dependent tokens '$t_{\mathbb{F}}$' and '$t'_{\mathbb{F}}$'. Using subject assigned token '$t_s$', the random number generator generates a random matrix $R_0 \in \mathbb{R}^{\mathscr{D}\times m}$. Then $R_0$ is normalized using Gram-Schmidth Orthogonalization method on each column of $R_0$ to obtain $R \in \mathbb{R}^{\mathscr{D}\times m}$, where $m \ll \mathscr{D}$. Then the original feature vector $f_{\mathscr{F}}$ from the face region (extracted above) is projected on each column of $R$ matrix and compute the inner product $y_i =< f_{\mathscr{F}}, R_i >$ which is an element of vector $Y = [y_1, \cdots, y_m] \in \mathbb{R}^{1\times m}$. The vector '$Y$' contains real values and the elements of '$Y$' are further quantized by selecting a threshold $\tau$ (experimentally) to get $g_{\mathscr{F}} = [g_1, g_2, \dots g_m]$ i.e. $g_i \in \{0, 1\}$. This is existing FaceHashing technique described in (5).

$$f_{\mathscr{F}} \odot R \xrightarrow{t_s} Y \xrightarrow{\{0,1\}} g_{\mathscr{F}} \tag{5}$$

The obtained $g_{\mathscr{F}}$ is the cancelable FaceCode and its values lie in between 0 and 1. This FaceCode is used only for verification purposes. For identification purpose and to enhance more the security level, the existing FaceHashing technique has been modified to build the proposed FaceHashing technique. The proposed FaceHashing technique has been shown in (6).

$$f_{\mathscr{F}} \odot R \xrightarrow{t_s} Y \xrightarrow{\pi_{t_1}(Y)} Y' \xrightarrow{\pi_{t_2}(Y')} Y'' \xrightarrow{S} Z_{\mathscr{F}} \tag{6}$$

where $t_1 = t_s + t_{\mathbb{F}}$, $t_{\mathbb{F}}$ is the system assigned token which is common for all subjects. $\pi$ is the permutation function that has been applied $t_1$ times on the elements of vector $Y$ to generate $Y'$. Again the permutation function $\pi$ is being applied on the elements of vector $Y'$ with token $t_2 = t_s + t'_{\mathbb{F}}$ to generate the vector $Y'' \in \mathbb{R}^{1\times m}$. Applying the permutation function $\pi$ on $Y'$ not only enhances the security level but also $Y''$ is more discriminant than $Y'$. The elements of $Y''$ are further quantized to $\mathbb{S} = \{0, \cdots, (2^{11} - 1)\}$ to obtain $Z_{\mathscr{F}} \in \mathbb{S}^{1\times m}$. This feature vector $Z_{\mathscr{F}}$ will be used online for identification purpose and the original face features $f_{\mathscr{F}}$ are kept offline. It has been observed that the prediction of $Y'$ from $Y''$ & $Y$ from $Y'$ is very hard even if the quantized feature vector $Z_{\mathscr{F}}$ is compromised. Moreover, the feature vector $Y''$ has been obtained from $Y$ by performing $O(4^m = 2^m \times 2^m)$ number of permutations on $f_{\mathscr{F}}$. Therefore, it is impossible to recover $f_{\mathscr{F}}$ either from $Z_{\mathscr{F}}$ or from $Y''$. Hence the feature vector $Z_{\mathscr{F}}$ is our proposed FaceHashing code. Fig. 8 shows the proposed FaceHashing technique.

### C. FaceCrypto

In this section, we will describe the proposed FaceCrypto system. Here we have extended our work to some more security level by introducing the concept and techniques of Biometric Cryptography to the proposed FaceHashing code $Z_{\mathscr{H}}$. This FaceCrypto system not only extends the security levels but also preserves the cancelable feature (derived at the higher security level) for more secure communication at the time of online authentication. During implementation we have applied a public key encryption/decryption algorithm to protect the cancelable feature vector $Z_{\mathscr{F}}$ using RSA algorithm (described in section III-C) which is defined as follows:

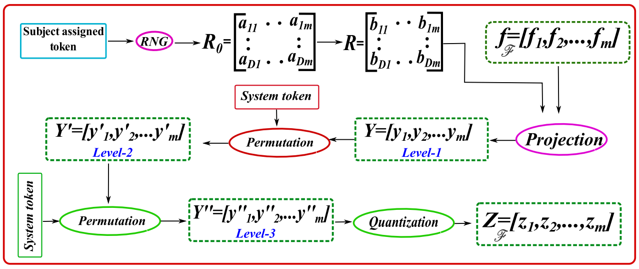
Subject assigned token
RNG
$R_0=\begin{bmatrix} a_{11} & \cdot\cdot & a_{1m} \\ \vdots & & \vdots \\ a_{D1} & \cdot\cdot & a_{Dm} \end{bmatrix}$
$R=\begin{bmatrix} b_{11} & \cdot\cdot & b_{1m} \\ \vdots & & \vdots \\ b_{D1} & \cdot\cdot & b_{Dm} \end{bmatrix}$
$f_{\mathscr{F}}=[f_1,f_2,\dots,f_m]$
System token
Projection
Permutation
$Y=[y_1,y_2,\dots y_m]$
Level-1
$Y'=[y'_1,y'_2,\dots y'_m]$
Level-2
System token
Permutation
$Y''=[y''_1,y''_2,\dots y''_m]$
Level-3
Quantization
$Z_{\mathscr{F}}=[z_1,z_2,\dots,z_m]$

FIGURE 8. The proposed FaceHashing technique.

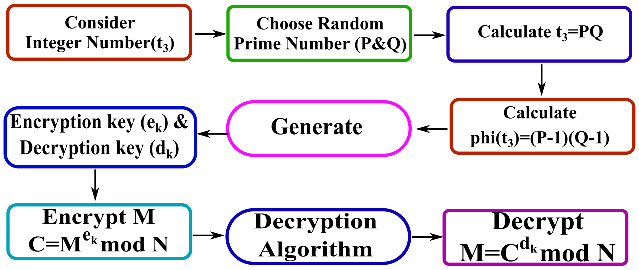
Consider Integer Number($t_3$)
Choose Random Prime Number (P&Q)
Calculate $t_3$=PQ
Calculate phi($t_3$)=(P-1)(Q-1)
Generate
Encryption key ($e_k$) & Decryption key ($d_k$)
Encrypt M C=$M^{e_k}$mod N
Decryption Algorithm
Decrypt M=$C^{d_k}$mod N

FIGURE 9. The work flow diagram for RSA Algorithm.

$$Z_{\mathscr{F}} \xrightarrow[e_k]{RSA} Z^{E}_{\mathscr{F}} \xrightarrow[d]{RSA} Z^{D_k}_{\mathscr{F}} \tag{7}$$

where $e_k$ is the encryption key and $d_k$ is the decryption key corresponding to the subject $\mathscr{F}$ to obtain the encrypted $Z^{e_k}_{\mathscr{F}}$ and decrypted $Z^{d_k}_{\mathscr{F}}$ cancelable face features respectively. These encryption/decryption keys are depend on an integer number which is a password (token) corresponds to each subject. So, here we have used $t_3 = t_s + t_{RSA}$ token, $t_{RSA}$ is system assigned token and input to RSA algorithm. Hence, combining (6) and (7), the proposed system is given by (8).

$$\begin{aligned} f_{\mathscr{F}} \odot R \xrightarrow{t_s} Y \xrightarrow{\pi_{t_1}(Y)} Y' \xrightarrow{\pi_{t_2}(Y')} Y'' \\ Y'' \xrightarrow{S} Z_{\mathscr{F}} \xrightarrow[t_3]{RSA} Z^{E}_{\mathscr{F}} \xrightarrow[t_3]{RSA} Z^{D}_{\mathscr{F}} \end{aligned} \tag{8}$$

Here, the $Z_{\mathscr{F}} \in \mathbb{S}^{1\times m}$ vector is converted to a binary matrix of size $16 \times m$ which is the binary representation of each $i^{th}$ column for each of $Z_{\mathscr{F}}$ vector then RSA algorithm has been applied on each column to obtain $Z^{E}_{\mathscr{F}}$ binary matrix named as quick response code (QRC). This QRC is kept as a reference for the online authentication of subjects.

#### 1) WORKING PRINCIPLE OF RSA ALGORITHM

The working flow diagram of the RSA algorithm for the proposed template protection scheme has been shown in Fig 9.

The RSA algorithm [62] is a public-key cryptosystem proposed by Ronald Rivest, Adi Shamir, and Leonard Adleman and, according to their names, this algorithm is known as RSA. This algorithm uses the asymmetric key encryption-decryption technique where the two separate keys i.e. one for encryption of messages (public key $\mathscr{P}_u$) and another one for decryption of messages (private key $\mathscr{P}_r$). It may be noted that the RSA algorithm can be applied only to integer values. The public key $\mathscr{P}_u$ may be known to anyone but the private key $\mathscr{P}_r$ will be kept secret from everyone. Since its innovation, RSA is regarded as one of the most secure cryptosystems in existence, which can be used for encryption, signature, and key exchange purposes. It relies on the assumption that it is difficult to find the factors of large integers. In RSA cryptosystem, $P = Q$ are large prime numbers. To achieve it, the most important factor is the efficiency in generate large prime numbers. The RSA algorithm executes into four steps: (a) key generation, (b) key distribution, (c) encryption, and (d) decryption. These procedures are discussed as follows:

- *Key generation:*
  1) Determine two distinct random prime numbers $P$ and $Q$ such that the bit length of $P$ and $Q$ must be same.
  2) Calculate $N = P \times Q$.
  3) Calculate Euler's totient function $\phi(N) = (P - 1)(Q - 1)$, keeping $\phi(N)$ secret.
  4) Choose a random prime number $e_k$ (known as encryption key) so that $1 < e_k < \phi(N)$ and $e_k, \phi(N)$ are coprime that is gcd(e, $\phi(N)$) = 1 and $e_k$ is a part of public key.
  5) Apply extended Euclidean algorithm to determine another random prime number $d_k$ (known as decryption key) so that $1 < d_k < \phi(N)$ and $d_k \times e_k \equiv 1 \pmod{\phi(N)}$ and $d_k$ is a part of private key.
- *Key distribution:*
  1) The public key contains the encryption key $e_k$ and modulus $N$ i.e $P_u =< e_k, N >$.
  2) The private key contains the decryption key $d$ and modulus $N$ i.e $P_r =< d_k, N >$. Hence, $d_k$, $P$, $Q$ and $\phi(N)$ must be kept secret because they are used to compute $d_k$.

  So, the RSA key distribution assigns ($e_k$, $N$) as public key and $d_k$ as private key. The public key, encryption key and decryption key are all created. Then, the process of encryption and decryption is as follows:
- *Encryption:* the encryption process uses the exponential function in modular $n$. During encrypting, the template matrix $m(M)$ is generated from $Z_{\mathscr{F}}$, where each element $M \in \mathbb{Z}$, $0 \leq M < N$ and encryption is performed by using $m(E) \equiv [m(M)]^e(modN)$, m(E) is the encrypted cancelable biometric feature matrix.
- *Decryption:* the decryption process represents an inverse of RSA encryption. Just like the encryption algorithm, the RSA decryption is a modular exponential function $n$ by using the private key. This step takes decryption key ($d_K$) from user and $N$ from system then decrypt the encrypted matrix $m(E)$. Decryption has been performed by using $m(D) \equiv [m(E)]^d(modN)$.
- *Verification:* encryption algorithm and verification process both use the same mathematical operation with the public key; if the value of $m(M) = m(D)$ then the user is authentic.

### 2) SECURITY ANALYSIS OF RSA ALGORITHM

The security of RSA algorithm depends on the strengths of two functions: Key Generation and Encryption function. The strength of which is based on the difficulty of factoring the large numbers. Encryption Function is considered as a irreversible function i.e. one-way function for converting the plain-text to cipher-text and it can be reversed if and only if the intruder has the knowledge of private key $d_k$. Key generation function provides the difficulty of determining the private key from the public key and it is equivalent to factoring the modulus '$N$'. An attacker cannot determine private key using the knowledge of public key unless he can factor $N$. Being a one way function, obtaining modulus $N$ from $P$ and $Q$ is easy but going reverse is impossible. Hence the security analysis of RSA algorithm are as follows:

- RSA algorithm is based on the computational complexity of factorization between the two large integers $P$ and $Q$ where the security depends on key length i.e. larger $P$ and $Q$ computes too large number $N = P \times Q$ and extraction of $P$ and $Q$ from $N$, is difficult and time consuming.
- The public key consists of two numbers: one number is multiplication of two large prime numbers, and private key is also derived from the same two prime numbers. So if somebody can factorize the large number, the private key is compromised. Therefore, encryption strength totally lies on the key size and if we double or triple the key size, the strength of encryption increases exponentially. Here the RSA keys are typically $2^{10}$ or $2^{11}$ bits long and it is infeasible task to break the keys.
- In a *Timing attack*, the imposter could exploit the timing variation of modular exponential implementations.However, there are several countermeasures that can be used against this attack [63].
- In a *Brute force attack*, the attacker tries all possible combinations to guess the private key. This attack cannot be applied in RSA algorithm as there exists several keys and for decrypting the message is time consuming. In addition, this attack can be easily circumvented by choosing the large key.
- *Dictionary attack* would not work in RSA algorithm as it works on numeric values and guessing these values by frequent analysis of digits, is impossible.
- There is no specific rules to hack RSA based cipher message and due to the difficulty of breaking RSA and hence, it is safe and secure due its complex mathematics. Moreover, *Mathematical attacks* can be prevented by

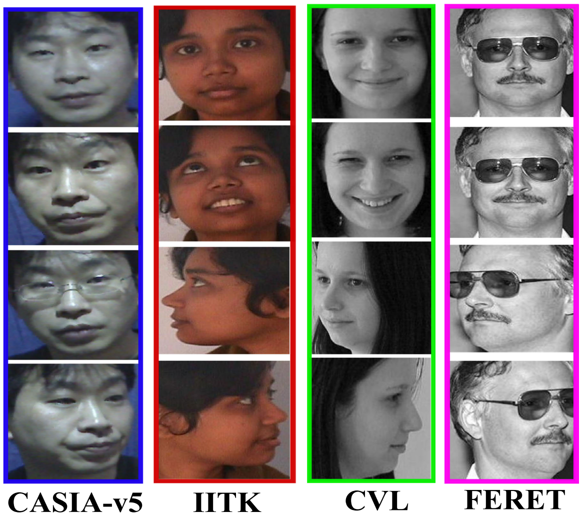

**FIGURE 10.** Examples of image samples from employed databases after image preprocessing.

increasing the length of key. So, it is hard to crack because of its prime factorization.

- Both public key ($\mathscr{P}_u$) and private key ($\mathscr{P}_r$) contains two parts and for this the security can be maintained until the private key ($\mathscr{P}_r$) i.e. both $e_k$ and $N$ are compromised. So, if $N$ is kept in systems side and $e_k$ is provided to the users as password then it will be impossible to access the template database.

## IV. EXPERIMENTAL RESULTS

### A. DATABASES USED

In this work, we have employed four benchmark face databases: CASIA-FaceV5-crop [64], IITK [65], CVL [66] and FERET [67] for the performance evaluation of the proposed system. CASIA-FaceV5-crop (say CASIA-V5) database has 2500 color facial images of 500 subjects where each subject contains 5 samples with varying in expressions (E), poses (P) and lighting (L) at different imaging distances. IIT Kanpur database has 488 color facial images of 61 subjects where each subject contains 8 samples with variations in pose (P) to frontal (F) views with different expressions (E).

CVL database contains 660 image samples of 110 subjects with 6 samples for each subject. The major drawbacks of this database are that it suffers from high pose variations with non-uniform illumination conditions. FERET face database contains 4970 image samples of 994 subjects with 5 samples for each subject. In this database, five samples are named as fa (FE), fb (FE), hl (Half left) with $-67.5°$, hl (Half right) with $+67.5°$ and pr (profile right) with 90°. These image samples are in different facial expressions (E) and poses (P). Fig. 10 shows some image samples of these databases after image preprocessing and Table 2 summarizes the characteristics of these databases where A stands for accessory, E stands for Expression, F stands for Frontal, L stands for Lighting and P stands for Pose.

**TABLE 2.** Face databases have employed for the proposed system.

| Database | Subjects | Samples/Subject | Characteristics |
|---|---|---|---|
| CASIA-V5 | 500 | 5 | A, E, P, L |
| IITK | 61 | 8 | A, E, F, P |
| CVL | 110 | 6 | E, F, P |
| FERET | 994 | 5 | P, E |

**TABLE 3.** Execution time (in seconds) for feature extraction from face region $\mathscr{F}$.

| Feature vector | dense-SIFT extraction | coefficient ($\alpha$) | SPM | Total (sec.) |
|---|---|---|---|---|
| $f_S$ | 0.3241 | 0.8759 | 0.0112 | 1.2112 |
| $f_C$ | 0.3241 | 0.9127 | 0.0421 | 1.2789 |
| $f_B$ | 0.3241 | 0.8912 | 0.0271 | 1.2424 |

### B. RESULTS AND DISCUSSIONS

All the experiments for the proposed system have been performed in MATLAB 2016a version on Windows 10 operating system, 8GB RAM of speed 2667 MHz and Intel Core i5 processor of 3GHz. The multi-class linear SVM classifier has been employed to do the classification task where the performance has been evaluated respect to each database by partitioning them into training-testing datasets.

During face preprocessing, we have detected 200 × 200 face region $\mathscr{F}$ from each input image $\mathscr{I}$. Then a patch $p \in \mathbb{R}^{n \times n}$, $n = 20$ has been considered over $\mathscr{F}$ horizontally and then vertically. Then densely SIFT descriptors with 75% overlapping of pixels, have been extracted from each patch $p$. During dictionary learning $M = 100$ training samples have been used to obtain the corpus $\mathscr{C} \in \mathbb{R}^{128 \times K}$ with $K = 1000$ code-words by learning the dictionary parameters. Then from each sample $F$, we compute the feature vector $f_S \in \mathbb{R}^{1 \times 5000}$ using SRC, $f_C \in \mathbb{R}^{1 \times 5000}$ using CD and $f_B \in \mathbb{R}^{1 \times 5000}$ using BCD optimization techniques followed by SPM with level $l = 0, 1$ respectively. The execution time due to feature extraction using these optimization techniques have been demonstrated in Table 3. Here the average time of CASIA-v5 dataset has been shown.

The performance of the proposed system due to $f_S, f_C$ and $f_B$ feature vectors have been shown in Table 4 in terms of CRR, EER, Precision (Pre.) and Recall (Rec.). Here the verification performance is evaluated through the true-positive rate and false-positive rate and for this EER, Precision (Pre.) and Recall (Rec.) have been reported while CRR has been used to show identification performance. From this Table, it is shown that CASIA-v5, IITK, CVL and FERET database attain better performance for $f_S \leq f_C \leq f_B$ and also the performance increases by increasing the training dataset size.

The fused performance due to SRC, CD and BCD optimization methods may increase the performance of the recognition system but the objective of this paper is to build the cancelable feature vector from the original face feature vector. The cancelable feature will be employed to perform recognition tasks online while the original feature vectors may be kept offline in the external hard disc or derive. To show the effectiveness and discrimination of the proposed system, the performance of original feature vectors due to SRC, CD, and BCD followed by SPM have been compared with some state-of-the-art face recognition systems in Table 5 and from

**TABLE 4. The performance of the proposed system in CRR, EER, Precision (Pre.) and Recall (Rec.) using SRC, CD and BCD optimization techniques followed by SPM technique.**

| Method | 50%-50% | | | | 60%-40% | | | | 70%-30% | | | | 80%-20% | | | | 90%-10% | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | CASIA-V5 | | | | | | | | | | | | | | | | | | | |
| | CRR | EER | Pre. | Rec. | CRR | EER | Pre. | Rec. | CRR | EER | Pre. | Rec. | CRR | EER | Pre. | Rec. | CRR | EER | Pre. | Rec. |
| $f_S$ | 78.98 | 0.061 | 0.799 | 0.784 | 79.94 | 0.094 | 0.801 | 0.792 | 80.29 | 0.039 | 0.815 | 0.795 | 81.84 | 0.072 | 0.832 | 0.822 | 83.36 | 0.029 | 0.842 | 0.839 |
| $f_C$ | 76.50 | 0.077 | 0.779 | 0.765 | 77.74 | 0.063 | 0.794 | 0.765 | 81.80 | 0.048 | 0.767 | 0.798 | 83.40 | 0.053 | 0.845 | 0.832 | 83.56 | 0.024 | 0.851 | 0.875 |
| $f_B$ | 77.90 | 0.053 | 0.787 | 0.710 | 79.86 | 0.045 | 0.824 | 0.817 | 82.57 | 0.035 | 0.849 | 0.839 | 82.78 | 0.058 | 0.847 | 0.829 | 83.14 | 0.071 | 0.856 | 0.839 |
| | IITK | | | | | | | | | | | | | | | | | | | |
| | CRR | EER | Pre. | Rec. | CRR | EER | Pre. | Rec. | CRR | EER | Pre. | Rec. | CRR | EER | Pre. | Rec. | CRR | EER | Pre. | Rec. |
| $f_S$ | 71.92 | 0.048 | 0.731 | 0.719 | 74.38 | 0.061 | 0.763 | 0.729 | 81.55 | 0.071 | 0.831 | 0.823 | 81.55 | 0.083 | 0.819 | 0.810 | 83.19 | 0.029 | 0.842 | 0.861 |
| $f_C$ | 70.59 | 0.093 | 0.742 | 0.736 | 76.50 | 0.037 | 0.783 | 0.766 | 81.35 | 0.103 | 0.829 | 0.821 | 80.63 | 0.073 | 0.817 | 0.801 | 83.19 | 0.041 | 0.863 | 0.829 |
| $f_B$ | 71.51 | 0.078 | 0.732 | 0.727 | 74.24 | 0.072 | 0.763 | 0.745 | 78.99 | 0.090 | 0.811 | 0.795 | 80.53 | 0.090 | 0.793 | 0.785 | 82.37 | 0.110 | 0.810 | 0.807 |
| | CVL | | | | | | | | | | | | | | | | | | | |
| | CRR | EER | Pre. | Rec. | CRR | EER | Pre. | Rec. | CRR | EER | Pre. | Rec. | CRR | EER | Pre. | Rec. | CRR | EER | Pre. | Rec. |
| $f_S$ | 44.62 | 0.291 | 0.471 | 0.464 | 49.17 | 0.276 | 0.539 | 0.510 | 51.63 | 0.191 | 0.542 | 0.521 | 52.33 | 0.209 | 0.541 | 0.529 | 57.79 | 0.101 | 0.628 | 0.591 |
| $f_C$ | 43.93 | 0.204 | 0.477 | 0.453 | 49.09 | 0.245 | 0.512 | 0.532 | 50.36 | 0.206 | 0.521 | 0.510 | 53.09 | 0.173 | 0.551 | 0.529 | 56.78 | 0.210 | 0.573 | 0.561 |
| $f_B$ | 42.12 | 0.277 | 0.453 | 0.439 | 48.78 | 0.201 | 0.541 | 0.518 | 50.62 | 0.182 | 0.529 | 0.519 | 54.33 | 0.210 | 0.581 | 0.575 | 53.13 | 0.156 | 0.564 | 0.525 |
| | FERET | | | | | | | | | | | | | | | | | | | |
| | CRR | EER | Pre. | Rec. | CRR | EER | Pre. | Rec. | CRR | EER | Pre. | Rec. | CRR | EER | Pre. | Rec. | CRR | EER | Pre. | Rec. |
| $f_S$ | 54.78 | 0.139 | 0.578 | 0.543 | 62.94 | 0.092 | 0.639 | 0.621 | 70.29 | 0.089 | 0.729 | 0.718 | 74.84 | 0.091 | 0.769 | 0.742 | 86.27 | 0.009 | 0.883 | 0.873 |
| $f_C$ | 52.89 | 0.142 | 0.539 | 0.519 | 62.56 | 0.103 | 0.649 | 0.621 | 68.34 | 0.195 | 0.703 | 0.693 | 71.56 | 0.045 | 0.693 | 0.682 | 81.56 | 0.034 | 0.839 | 0.824 |
| $f_B$ | 51.52 | 0.185 | 0.554 | 0.581 | 59.77 | 0.140 | 0.621 | 0.593 | 64.37 | 0.193 | 0.664 | 0.649 | 70.15 | 0.103 | 0.738 | 0.729 | 80.34 | 0.052 | 0.849 | 0.828 |

**TABLE 5. Comparison of performance achieved by existing methods and the proposed method for CASIA-V5, IITK, CVL and FERET database.**

| Method | Training/ Testing | CRR (%) | EER |
|---|---|---|---|
| CASIA-V5 | | | |
| Feng et al. [68] | (40%-60%) | 36.47 | 0.1981 |
| Umer et al. [69] | (40%-60%) | 58.60 | 01201 |
| **Proposed** ($f_S$) | (40%-60%) | **74.18** | 0.0421 |
| IITK | | | |
| Sarode et al. [70] | (50%-50%) | 62.18 | 0.1034 |
| Umer et al. [69] | (50%-50%) | 68.85 | 0.1004 |
| **proposed** ($f_S$) | (50%-50%) | **71.92** | 0.0761 |
| CVL | | | |
| Gou et al. [71] | (90%-10%) | 41.64 | 0.2112 |
| Goel et al. [72] | (90%-10%) | 50.60 | 0.1961 |
| Umer et al. [69] | (90%-10%) | 56.36 | 0.1034 |
| **proposed** ($f_S$) | (90%-10%) | **57.79** | 0.1002 |
| FERET | | | |
| Huang et al. [73] | (90%-10%) | 84.40 | 0.0081 |
| Yang et al. [74] | (90%-10%) | 86.02 | 0.0177 |
| Yin et al. [75] | (90%-10%) | 69.50 | 0.1183 |
| **proposed** ($f_S$) | (90%-10%) | **86.27** | 0.0092 |

**TABLE 6. Performance of the proposed *CFR*$_1$ in CRR (%) and EER, *dim* stands for dimensional of the feature vector.**

| Methods | 100 *dim* | | 200 *dim* | | 500 *dim* | |
|---|---|---|---|---|---|---|
| | CRR | EER | CRR | EER | CRR | EER |
| | CASIA-V5 | | | | | |
| $f_S$ | 99.44 | 0.0002 | 100 | 0.0000 | 100 | 0.0000 |
| $f_C$ | 92.88 | 0.0017 | 99.80 | 0.0000 | 100 | 0.0000 |
| $f_B$ | 95.40 | 0.0062 | 100 | 0.0000 | 100 | 0.0000 |
| | IITK | | | | | |
| $f_S$ | 100 | 0.0000 | 100 | 0.0000 | 100 | 0.0000 |
| $f_C$ | 99.39 | 0.0002 | 100 | 0.0000 | 100 | 0.0000 |
| $f_B$ | 100 | 0.0000 | 100 | 0.0000 | 100 | 0.0000 |
| | CVL | | | | | |
| $f_S$ | 100 | 0.0000 | 100 | 0.0000 | 100 | 0.0000 |
| $f_C$ | 99.24 | 0.0007 | 100 | 0.0000 | 100 | 0.0000 |
| $f_B$ | 99.09 | 0.0010 | 100 | 0.0000 | 100 | 0.0000 |
| | FERET | | | | | |
| $f_S$ | 96.56 | 0.0023 | 100 | 0.0000 | 100 | 0.0000 |
| $f_C$ | 95.80 | 0.0065 | 99.12 | 0.0001 | 99.52 | 0.0001 |
| $f_B$ | 98.09 | 0.0031 | 100 | 0.0000 | 100 | 0.0000 |

this Table, it has been observed that $f_S$ has obtained better performance than the other competing methods. Here we have noted the performance of the competing methods from their respective papers with their training-testing protocols.

So, in this work, $f_S$ feature vector has been employed to compute the cancelable feature vector. Here in cancelable face recognition system (FaceHashing), we have divided the performance of the cancelable feature into three categories i.e $CFR_1$ (cancelable face recognition), $CFR_2$ and $CFR_3$ respectively. In $CFR_1$ we have obtained the performance of the recognition system due to the system $f_{\mathscr{S}} \odot R \xrightarrow{t_s} Y \xrightarrow{S} Z_{\mathscr{F}}$ i.e. the original face vector $f_{\mathscr{S}} \in \mathbb{R}^{1\times 5000}$ has been projected on $R \in \mathbb{R}^{5000\times m}$ (generated using subject specific token $t_s$) to yield $Y \in \mathbb{R}^{1\times m}$ which is further quantized into $S \in \{0, \cdots, (2^{11}-1)\}$. Here $f_{\mathscr{S}}$ is transformed into $m = 100$, $m = 200$ and $m = 500$ dimensional feature vectors. The objectives of $CFR_1$ experimentation are to (i) obtain the identification performance of the proposed system, (ii) measure the effectiveness about the quantization $S \in \{0, \cdots, (2^{11}-1)\}$ employed in the proposed system. This $CFR_1$ shows the level-1 security of the proposed FaceHashing technique and its performance has been shown in Table 6. From this Table it is observed that the proposed system has obtained outstanding performance for 500 dimensional cancelable feature $Z_{\mathscr{F}}$.

For $CFR_2$ we have performed the experimentation for $f_{\mathscr{F}} \odot R \xrightarrow{t_s} Y \xrightarrow{\pi_{t_1}(Y)} Y'$ system which has level-2 security for the proposed FaceHashing system. In $CFR_2$, the recognition will be performed using $Y'$ cancelable features which are depended on one subject specific token ($t_s$) and another one system specific token ($t_{\mathscr{F}}$). Here the original face feature vector $f_{\mathscr{F}} \in \mathbb{R}^{1\times 5000}$ has been transformed using token $t_s$ into $Y \in \mathbb{R}^{1\times m}$ which is further permuted using token $t_1 = t_s + t_{\mathscr{F}}$ to obtain $Y' \in \mathbb{R}^{1\times m}$. The performance of $CFR_2$ system has been shown in Table 7 and from this Table it is observed that $CFR_2$ has improved performance than $CFR_1$ and also $CFR_2$ has higher security level than $CFR_1$ system.

**TABLE 7.** Performance of the proposed $CFR_2$ in CRR (%) and EER.

| Methods | 100 *dim* | | 200 *dim* | | 300 *dim* | |
|---|---|---|---|---|---|---|
| | CRR | EER | CRR | EER | CRR | EER |
| | CASIA-V5 | | | | | |
| $f_S$ | 99.40 | 0.0010 | 100 | 0.0000 | 100 | 0.0000 |
| $f_C$ | 93.76 | 0.0024 | 99.84 | 0.0000 | 100 | 0.0000 |
| $f_B$ | 95.84 | 0.0103 | 100 | 0.0000 | 100 | 0.0000 |
| | IITK | | | | | |
| $f_S$ | 100 | 0.0000 | 100 | 0.0000 | 100 | 0.0000 |
| $f_C$ | 99.80 | 0.0002 | 100 | 0.0000 | 100 | 0.0000 |
| $f_B$ | 99.59 | 0.0010 | 100 | 0.0000 | 100 | 0.0000 |
| | CVL | | | | | |
| $f_S$ | 99.85 | 0.0033 | 100 | 0.0000 | 100 | 0.0000 |
| $f_C$ | 99.33 | 0.0007 | 100 | 0.0000 | 100 | 0.0000 |
| $f_B$ | 98.79 | 0.0049 | 100 | 0.0000 | 100 | 0.0000 |
| | FERET | | | | | |
| $f_S$ | 97.14 | 0.0035 | 100 | 0.0000 | 100 | 0.0000 |
| $f_C$ | 96.24 | 0.0048 | 99.56 | 0.0004 | 99.89 | 0.0001 |
| $f_B$ | 98.39 | 0.0081 | 100 | 0.0000 | 100 | 0.0000 |

**TABLE 8.** Performance of the proposed $CFR_3$ in CRR (%) and EER.

| Methods | 10 *dim* | | 20 *dim* | | 30 *dim* | |
|---|---|---|---|---|---|---|
| | CRR | EER | CRR | EER | CRR | EER |
| | CASIA-V5 | | | | | |
| $f_S$ | 99.44 | 0.0009 | 100 | 0.0000 | 100 | 0.0000 |
| $f_C$ | 92.88 | 0.0056 | 99.80 | 0.0000 | 100 | 0.0000 |
| $f_B$ | 94.40 | 0.0210 | 100 | 0.0000 | 100 | 0.0000 |
| | IITK | | | | | |
| $f_S$ | 100 | 0.0000 | 100 | 0.0000 | 100 | 0.0000 |
| $f_C$ | 99.39 | 0.0010 | 100 | 0.0000 | 100 | 0.0000 |
| $f_B$ | 100 | 0.0000 | 100 | 0.0000 | 100 | 0.0000 |
| | CVL | | | | | |
| $f_S$ | 100 | 0.0000 | 100 | 0.0000 | 100 | 0.0000 |
| $f_C$ | 99.24 | 0.0028 | 100 | 0.0000 | 100 | 0.0000 |
| $f_B$ | 99.09 | 0.0019 | 100 | 0.0000 | 100 | 0.0000 |
| | FERET | | | | | |
| $f_S$ | 96.56 | 0.0079 | 100 | 0.0000 | 100 | 0.0000 |
| $f_C$ | 95.80 | 0.0167 | 99.12 | 0.0001 | 99.52 | 0.0001 |
| $f_B$ | 98.09 | 0.0001 | 100 | 0.0000 | 100 | 0.0000 |

**TABLE 9.** Execution time (in seconds) of the proposed system $CFR_3$ for the employed database.

| Database | Preprocessing | Face Features | Cancelable Feature | Encryption & Decryption Time | Avg. |
|---|---|---|---|---|---|
| CASIA-V5 | 0.2121 | 1.1312 | 0.02094 | 0.00040 | 1.3646 |
| IITK | 0.2231 | 1.0125 | 0.02179 | 0.00043 | 1.2577 |
| CVL | 0.2491 | 1.0191 | 0.02377 | 0.00046 | 1.2923 |
| FERET | 0.2726 | 1.0810 | 0.02627 | 0.00034 | 1.381 |

The $CFR_3$ is the proposed FaceHashing system which is $f_{\mathscr{F}} \odot R \xrightarrow{t_s} Y \xrightarrow{\pi_{t_1}(Y)} Y' \xrightarrow{\pi_{t_2}(Y')} Y'' \xrightarrow{S} Z_{\mathscr{F}}$. This system uses one subject assigned token $t_s$ and two system assigned tokens $t_{\mathscr{F}}$ and $t'_{\mathscr{F}}$ i.e. one subject dependent and two system independent tokens. This system has level-3 security plus i.e. the original face feature vector $f_{\mathscr{F}} \in \mathbb{R}^{1\times 5000}$ has been transformed using token $t_s$ into $Y \in \mathbb{R}^{1\times m}$ which is further permuted using token $t_1 = t_s + t_{\mathscr{F}}$ to obtain $Y' \in \mathbb{R}^{1\times m}$. This $Y' \in \mathbb{R}^{1\times m}$ has again permuted using $t_2 = t_s + t'_{\mathscr{F}}$ token to obtain $Y'' \in \mathbb{R}^{1\times m'}$, $m'$, $<< m$. Moreover, the elements of $Y''$ have further been quantized in $S \in \{0, \cdots, (2^{11}-1)\}$ to yield $Z_{\mathscr{F}}$, this also increases the security level of the proposed FaceHashing system. The performance of $CFR_3$ is shown in Table 8 where it has been observed that 30 dimensional feature vector sufficiently identify the subjects of employed databases with nearly 100% correct recognition rate. The average execution time of the proposed $CFR_3$ has been shown in Table 9.

**TABLE 10.** Comparison of performance achieved by existing cancelable biometric related authentication methods and the proposed FaceHashing method $CFR_3$ for CASIA-V5, IITK, CVL, and FERET database.

| Method | CRR (%) | EER |
|---|---|---|
| CASIA-V5 | | |
| Umer et al. [50] | 93.61 | 0.0045 |
| Arpit et al. [76] | 96.32 | – |
| **Proposed** ($CFR_3$) | **99.85** | 0.0000 |
| IITK | | |
| Umer et al. [50] | 98.19 | 0.0015 |
| Arpit et al. [76] | 97.69 | – |
| **Proposed** ($CFR_3$) | **100** | 0.0000 |
| CVL | | |
| Kim et al. [77] | – | 0.1271 |
| Umer et al. [50] | 96.33 | 0.0018 |
| **Proposed** ($CFR_3$) | **100** | 0.0000 |
| FERET | | |
| Oh et al. [78] | – | 0.0023 |
| Kim et al. [77] | – | 0.1041 |
| Abdellate et al. [79] | 93.86 | – |
| Umer et al. [50] | 95.74 | – |
| **Proposed** ($CFR_3$) | **100** | 0.0000 |

In $CFR_3$, we have shown the performance of the proposed FaceHashing. Here the prediction of $Y'$ from $Y''$ and $Y$ from $Y'$ are very hard even if $Z_{\mathscr{F}}$ is compromised. Moreover, $Y$ has been permuted $4^m$ times to yield $Y''$, so, it is impossible to recover $f_{\mathscr{F}}$ either from $Y''$ or from $Z_{\mathscr{F}}$. Now to extend the security level, the encryption, and decryption of templates, have been performed on $Z_{\mathscr{F}}$. Here one extra token $t_3 = t_s + t_{RSA}$ ($t_{RSA}$ system assigned token for RSA algorithm) has been introduced, is a large integer number $N$ from which the encryption and decryption keys have been derived. Now based on this encryption key $Z_{\mathscr{F}}$ is converted to $Z^E_{\mathscr{F}}$ and it is kept online as reference template in the database for that subject in the quick response code (QRC) form. Now during authentication or recognition, $Z^E_{\mathscr{F}}$ is decrypted using decryption key to obtain $Z^D_{\mathscr{F}}$ $(=Z_{\mathscr{F}})$ to perform recognition task. Further, we have compared the performance of the FaceHashing method $CFR_3$ in Table 10 with some existing state-of-the-art cancelable biometric related verification/identification methods under same training-testing protocols and the performance of the competing methods show the superiority of the proposed FaceHashing system.

The performance analysis due to the proposed cancelable feature vectors have been shown in Table 6 (for $CFR_1$), Table 7 (for $CFR_2$) and Table 8 (for $CFR_3$) and from these tables it has been observed that the performance are more or less same in both Table 6 and 7 but the level of security is high in Table 7 ($CFR_2$) than Table 6 ($CFR_1$) whereas the performance in Table 8 ($CFR_3$) is higher and also the level of security is much higher. Hence from these observations it has been explained that (i) the employed techniques for providing security to the feature vectors may be either correlate or be stable with the performance of the recognition system, (ii) at every level of security, the dimension of the feature vector reduces while preserving its distinctive and discriminating nature, (iii) additionally, the encryption-decryption of templates has extended the security level much higher to the proposed system.

## V. CONCLUSION

In this paper, a novel cancelable FaceHashing technique based on non-invertible transformation with encryption/decryption of templates has been proposed. For the proposed system, the face biometric trait has been considered where from an input image, the face region has been extracted by applying the preprocessing task. The extracted face region undergoes to feature computation task where various optimization techniques such as sparse representation, coordinate descent, block coordinate descent techniques have been employed on the extracted SIFT descriptors from the face region. Then sparse representation technique followed by a spatial pyramid matching technique has been finally considered to extract the feature vector from the face region. The extracted feature vector is being transformed by the proposed FaceHashing technique which facilitates the higher level of template protection schemes with improving the recognition performance while preserving the original feature vector from attacks and compromise. To provide more security and also to preserve the face feature vectors from external hazardous and misuse the encryption/decryption based RSA algorithm has been introduced to FaceHashing where the derived cancelable features are further encrypted and are kept online for authentication or recognition purpose. The proposed system has been tested on four benchmark databases: CASIA-Face-v5, IITK, CVL, and FERET. Extensive experimentation has been performed using these databases and the performance has been compared with state-of-the-art methods. Finally, the effectiveness and improvement of performance have also been shown with proper justification and explanations that show the superiority of the proposed system.

## REFERENCES

[1] W. Zhao, R. Chellappa, P. J. Phillips, and A. Rosenfeld, "Face recognition: A literature survey," *ACM Comput. Surv.*, vol. 35, no. 4, pp. 399–458, 2003.

[2] S. Umer, B. C. Dhara, and B. Chanda, "Face recognition using fusion of feature learning techniques," *Measurement*, vol. 146, pp. 43–54, Nov. 2019.

[3] G. J. Simmons, "A survey of information authentication," *Proc. IEEE*, vol. 76, no. 5, pp. 603–620, May 1988.

[4] A. Ramesh and S. P. Setty, "Analysis on biometric encryption using RSA algorithm," *Int. J. Multidisciplinary Educ. Res.*, vol. 1, no. 3, pp. 302–307, 2013.

[5] Z. Rui and Z. Yan, "A survey on biometric authentication: Toward secure and privacy-preserving identification," *IEEE Access*, vol. 7, pp. 5994–6009, 2019.

[6] D. Maltoni, D. Maio, A. K. Jain, and S. Prabhakar, *Handbook of Fingerprint Recognition*. Springer, 2009.

[7] N. K. Ratha, J. H. Connell, and R. M. Bolle, "An analysis of minutiae matching strength," in *Proc. Int. Conf. Audio-Video-Based Biometric Person Authentication*. Berlin, Germany: Springer, 2001, pp. 223–228.

[8] S. Malhotra and D. C. Kant, "A novel approach for securing biometric template," *Int. J. Adv. Res. Comput. Sci. Softw. Eng.*, vol. 3, no. 5, pp. 397–403, 2013.

[9] Manisha and N. Kumar, "Cancelable biometrics: A comprehensive survey," *Artif. Intell. Rev.*, vol. 53, pp. 3403–3446, 2020.

[10] V. Brindha, "Biometric template security using dorsal hand vein fuzzy vault," *J. Biometric Biostat.*, vol. 3, no. 145, p. 2, 2012.

[11] S. K. Singh, M. Singh, and D. K. Singh, "A survey on network security and attack defense mechanism for wireless sensor networks," *Int. J. Comput. Trends Technol.*, vol. 1, no. 2, pp. 9–17, 2011.

[12] A. K. Jain, K. Nandakumar, and A. Nagar, "Biometric template security," *EURASIP J. Adv. Signal Process.*, vol. 2008, pp. 1–17, Jan. 2008.

[13] I. Natgunanathan, A. Mehmood, Y. Xiang, G. Beliakov, and J. Yearwood, "Protection of privacy in biometric data," *IEEE Access*, vol. 4, pp. 880–892, 2016.

[14] C. Rathgeb and A. Uhl, "A survey on biometric cryptosystems and cancelable biometrics," *EURASIP J. Inf. Secur.*, vol. 2011, no. 1, p. 3, 2011.

[15] N. Radha and S. Karthikeyan, "A study on biometric template security," *ICTACT J Soft Comput.*, vol. 1, no. 1, pp. 37–41, 2010.

[16] N. Radha and S. Karthikeyan, "An evaluation of fingerprint security using noninvertible biohash," *Int. J. Netw. Secur. Appl.*, vol. 3, no. 4, pp. 1–11, 2011.

[17] G. Zheng, W. Yang, C. Valli, R. Shankaran, H. Abbas, G. Zhang, G. Fang, J. Chaudhry, and L. Qiao, "Fingerprint access control for wireless insulin pump systems using cancelable delaunay triangulations," *IEEE Access*, vol. 7, pp. 75629–75641, 2019.

[18] T. Murakami, R. Fujita, T. Ohki, Y. Kaga, M. Fujio, and K. Takahashi, "Cancelable permutation-based indexing for secure and efficient biometric identification," *IEEE Access*, vol. 7, pp. 45563–45582, 2019.

[19] P. Punithavathi and S. Geetha, "Random projection-based cancelable template generation for sparsely distributed biometric patterns," *Indonesian J. Electr. Eng. Comput. Sci.*, vol. 7, no. 3, pp. 877–886, 2017.

[20] H. Kim and S. Y. Chun, "Cancelable ECG biometrics using compressive sensing-generalized likelihood ratio test," *IEEE Access*, vol. 7, pp. 9232–9242, 2019.

[21] X. Wang and H. Li, "One-factor cancellable palmprint recognition scheme based on OIOM and minimum signature hash," *IEEE Access*, vol. 7, pp. 131338–131354, 2019.

[22] 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.

[23] P. Punithavathi, S. Geetha, M. Karuppiah, S. H. Islam, M. M. Hassan, and K.-K.-R. Choo, "A lightweight machine learning-based authentication framework for smart IoT devices," *Inf. Sci.*, vol. 484, pp. 255–268, May 2019.

[24] K. H. Cheung, A. Kong, D. Zhang, M. Kamel, J. T. You, and H. W. Lam, "An analysis on accuracy of cancelable biometrics based on biohashing," in *Proc. Int. Conf. Knowl.-Based Intell. Inf. Eng. Syst.* Berlin, Germany: Springer, Sep. 2005, pp. 1168–1172.

[25] A. Lumini and L. Nanni, "An improved BioHashing for human authentication," *Pattern Recognit.*, vol. 40, no. 3, pp. 1057–1065, Mar. 2007.

[26] 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, Nov. 2004.

[27] A. Siswanto, N. Katuk, K. R. Ku-Mahamud, and E. A. Kadir, "An overview of fingerprint template protection approaches," in *Proc. ICoSET*, vol. 8, 2017, p. 80.

[28] J. Zhang and P. Fang, "Finger vein template encryption scheme based on BioHashing," in *Proc. Int. Conf. Sens., Diagnostics, Prognostics, Control (SDPC)*, Aug. 2018, pp. 681–685.

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

[30] J. A. Unar, W. C. Seng, and A. Abbasi, "A review of biometric technology along with trends and prospects," *Pattern Recognit.*, vol. 47, no. 8, pp. 2673–2688, Aug. 2014.

[31] K. Xi and H. Jiankun, "Bio-cryptography in handbook of information and communication security," 2010.

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

[33] A. Cavoukian, A. Stoianov, and F. Carter, "Keynote paper: Biometric encryption: Technology for strong authentication, security and privacy," in *Policies and Research in Identity Management*. Boston, MA, USA: Springer, 2008, pp. 57–77.

[34] A. A. Ross, K. Nandakumar, and A. K. Jain, *Handbook Multibiometrics*, vol. 6. Springer, 2006.

[35] M. Blanton and M. Aliasgari, "Analysis of reusability of secure sketches and fuzzy extractors," *IEEE Trans. Inf. Forensics Security*, vol. 8, no. 9, pp. 1433–1445, Sep. 2013.

[36] V. Schmitt and J. Jordaan, "Establishing the validity of MD5 and SHA-1 hashing in digital forensic practice in light of recent research demonstrating cryptographic weaknesses in these algorithms," *Int. J. Comput. Appl.*, vol. 68, no. 23, pp. 40–43, Apr. 2013.

[37] W. Diffie and M. Hellman, "New directions in cryptography," *IEEE Trans. Inf. Theory*, vol. 22, no. 6, pp. 644–654, Nov. 1976.

[38] A. B. J. Teoh, D. C. L. Ngo, and A. Goh, ''Personalised cryptographic key generation based on FaceHashing,'' *Comput. Secur.*, vol. 23, no. 7, pp. 606–614, Oct. 2004.

[39] A. Nagar and S. Chaudhury, ''Biometrics based asymmetric cryptosystem design using modified fuzzy vault scheme,'' in *Proc. 18th Int. Conf. Pattern Recognit. (ICPR)*, vol. 4, 2006, pp. 537–540.

[40] E. Maiorana, M. Martinez-Diaz, P. Campisi, J. Ortega-García, and A. Neri, ''Template protection for HMM-based on-line signature authentication,'' in *Proc. IEEE Comput. Soc. Conf. Comput. Vis. Pattern Recognit. Workshops*, Jun. 2008, pp. 1–6.

[41] M. R. Islam, M. S. Sayeed, and A. Samraj, ''Biometric template protection using watermarking with hidden password encryption,'' in *Proc. Int. Symp. Inf. Technol.*, vol. 1, Aug. 2008, pp. 1–8.

[42] N. Lalithamani and K. P. Soman, ''Towards generating irrevocable key for cryptography from cancelable fingerprints,'' in *Proc. 2nd IEEE Int. Conf. Comput. Sci. Inf. Technol.*, 2009, pp. 563–568.

[43] Y. J. Chin, T. S. Ong, A. B. J. Teoh, and M. K. O. Goh, ''Multimodal biometrics based bit extraction method for template security,'' in *Proc. 6th IEEE Conf. Ind. Electron. Appl.*, Jun. 2011, pp. 1971–1976.

[44] E. A. Rua, E. Maiorana, J. L. A. Castro, and P. Campisi, ''Biometric template protection using universal background models: An application to online signature,'' *IEEE Trans. Inf. Forensics Security*, vol. 7, no. 1, pp. 269–282, Feb. 2012.

[45] W. Yang, S. Wang, J. Hu, G. Zheng, J. Chaudhry, E. Adi, and C. Valli, ''Securing mobile healthcare data: A smart card based cancelable finger-vein bio-cryptosystem,'' *IEEE Access*, vol. 6, pp. 36939–36947, 2018.

[46] K. Kanagalakshmi and E. Chandra, ''Novel complex conjugate-phase transform technique for cancelable and irrevocable biometric template generation for fingerprints,'' *Int. J. Comput. Sci. Issues*, vol. 9, no. 4, p. 426, 2012.

[47] B. Yang and E. Martiri, ''Using honey templates to augment hash based biometric template protection,'' in *Proc. IEEE 39th Annu. Comput. Softw. Appl. Conf.*, vol. 3, Jul. 2015, pp. 312–316.

[48] J. Mwema, M. Kimwele, and S. Kimani, ''A simple review of biometric template protection schemes used in preventing adversary attacks on biometric fingerprint templates,'' *Int. J. Comput. Trends Technol.*, vol. 20, no. 1, pp. 8–12, 2015.

[49] K.-Y. Chee, Z. Jin, W.-S. Yap, and B.-M. Goi, ''Two-dimensional winner-takes-all hashing in template protection based on fingerprint and voice feature level fusion,'' in *Proc. Asia–Pacific Signal Inf. Process. Assoc. Annu. Summit Conf. (APSIPA ASC)*, Dec. 2017, pp. 1411–1419.

[50] S. Umer, B. C. Dhara, and B. Chanda, ''A novel cancelable iris recognition system based on feature learning techniques,'' *Inf. Sci.*, vols. 406–407, pp. 102–118, Sep. 2017.

[51] X. Zhu and D. Ramanan, ''Face detection, pose estimation, and landmark localization in the wild,'' in *Proc. IEEE Conf. Comput. Vis. Pattern Recognit.*, Jun. 2012, pp. 2879–2886.

[52] R. M. Haralick, ''Statistical and structural approaches to texture,'' *Proc. IEEE*, vol. 67, no. 5, pp. 786–804, May 1979.

[53] 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, 2018.

[54] A. Vedaldi and B. Fulkerson, ''VLFeat: An open and portable library of computer vision algorithms,'' in *Proc. 18th ACM Int. Conf. Multimedia*, 2010, pp. 1469–1472.

[55] J. Yang, K. Yu, Y. Gong, and T. Huang, ''Linear spatial pyramid matching using sparse coding for image classification,'' in *Proc. IEEE Conf. Comput. Vis. Pattern Recognit.*, Jun. 2009, pp. 1794–1801.

[56] K.-W. Chang, C.-J. Hsieh, and C.-J. Lin, ''Coordinate descent method for large-scale L2-loss linear support vector machines,'' *J. Mach. Learn. Res.*, vol. 9, pp. 1369–1398, Jun. 2008.

[57] J. Mairal, F. Bach, J. Ponce, and G. Sapiro, ''Online learning for matrix factorization and sparse coding,'' *J. Mach. Learn. Res.*, vol. 11, pp. 19–60, Mar. 2010.

[58] H. Lee, A. Battle, R. Raina, and A. Y. Ng, ''Efficient sparse coding algorithms,'' in *Proc. Adv. Neural Inf. Process. Syst.*, 2006, pp. 801–808.

[59] S. Lazebnik, C. Schmid, and J. Ponce, ''Beyond bags of features: Spatial pyramid matching for recognizing natural scene categories,'' in *Proc. IEEE Comput. Soc. Conf. Comput. Vis. Pattern Recognit.*, vol. 2, Jun. 2006, pp. 2169–2178.

[60] C.-P. Lee and C.-J. Lin, ''A study on L2-loss (squared hinge-loss) multiclass SVM,'' *Neural Comput.*, vol. 25, no. 5, pp. 1302–1323, May 2013.

[61] T. Fawcett, ''An introduction to ROC analysis,'' *Pattern Recognit. Lett.*, vol. 27, no. 8, pp. 861–874, Jun. 2006.

[62] R. L. Rivest, A. Shamir, and L. Adleman, ''A method for obtaining digital signatures and public-key cryptosystems,'' *Commun. ACM*, vol. 21, no. 2, pp. 120–126, Feb. 1978.

[63] A. A. Hasib and A. A. M. M. Haque, ''A comparative study of the performance and security issues of AES and RSA cryptography,'' in *Proc. 3rd Int. Conf. Converg. Hybrid Inf. Technol.*, vol. 2, Nov. 2008, pp. 505–510.

[64] CAS Institute of Automation. (2009). *Casia Face Image Databases Service Team*. [Online]. Available: http://biometrics.idealtest.org/

[65] V. Jain, *The Indian Face Database/Vidit Jain, Amitabha Mukherjee*. Kanpur, India: Indian Institutes of Technology, 2002.

[66] P. Peer, ''CVL face database,'' Ph.D. dissertation, Dept. Comput. Inf. Sci., Comput. Vis. Lab., Univ. Ljubljana, Ljubljana, Slovenia, 2005. [Online]. Available: http://www.lrv.fri.uni-lj.si/facedb.html

[67] 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.

[68] Q. Feng, C. Yuan, J.-S. Pan, J.-F. Yang, Y.-T. Chou, Y. Zhou, and W. Li, ''Superimposed sparse parameter classifiers for face recognition,'' 2016.

[69] S. Umer, B. C. Dhara, and B. Chanda, ''Biometric recognition system for challenging faces,'' in *Proc. 5th Nat. Conf. Comput. Vis., Pattern Recognit., Image Process. Graph. (NCVPRIPG)*, Dec. 2015, pp. 1–4.

[70] J. P. Sarode and A. D. Anuse, ''A framework for face classification under pose variations,'' in *Proc. ICACCI*, Sep. 2014, pp. 1886–1891.

[71] G. Gou, D. Huang, and Y. Wang, ''A hybrid local feature for face recognition,'' in *Proc. Pacific Rim Int. Conf. Artif. Intell.* Berlin, Germany: Springer, 2012, pp. 64–75.

[72] N. Goel, G. Bebis, and A. Nefian, ''Face recognition experiments with random projection,'' in *Proc. Int. Soc. Opt. Photon. Biometric Technol. Hum. Identificat. II*, vol. 5779, 2005, pp. 426–437.

[73] H. Huang and H. He, ''Super-resolution method for face recognition using nonlinear mappings on coherent features,'' *IEEE Trans. Neural Netw.*, vol. 22, no. 1, pp. 121–130, Jan. 2011.

[74] M. Yang, L. Zhang, S. C.-K. Shiu, and D. Zhang, ''Robust kernel representation with statistical local features for face recognition,'' *IEEE Trans. Neural Netw. Learn. Syst.*, vol. 24, no. 6, pp. 900–912, Jun. 2013.

[75] J. Yin, L. Wei, M. Song, and W. Zeng, ''Optimized projection for collaborative representation based classification and its applications to face recognition,'' *Pattern Recognit. Lett.*, vol. 73, pp. 83–90, Apr. 2016.

[76] D. Arpit, I. Nwogu, G. Srivastava, and V. Govindaraju, ''An analysis of random projections in cancelable biometrics,'' 2014, *arXiv:1401.4489*. [Online]. Available: http://arxiv.org/abs/1401.4489

[77] Y. Kim, A. B. J. Teoh, and K.-A. Toh, ''A performance driven methodology for cancelable face templates generation,'' *Pattern Recognit.*, vol. 43, no. 7, pp. 2544–2559, Jul. 2010.

[78] B.-S. Oh, K.-A. Toh, K. Choi, A. Beng Jin Teoh, and J. Kim, ''Extraction and fusion of partial face features for cancelable identity verification,'' *Pattern Recognit.*, vol. 45, no. 9, pp. 3288–3303, Sep. 2012.

[79] E. Abdellatef, N. A. Ismail, S. E. S. A. Elrahman, K. N. Ismail, M. Rihan, and F. E. A. El-Samie, ''Cancelable fusion-based face recognition,'' *Multimedia Tools Appl.*, vol. 78, no. 22, pp. 31557–31580, 2019.

**ALAMGIR SARDAR** received the B.Sc. and M.Sc. degrees in computer science from Aliah University, Kolkata, India, in 2011 and 2013, respectively, where he is currently pursuing the Ph.D. degree with the Department of Computer Science and Engineering. His research interests include biometric, computer vision, and machine learning.

**SAIYED UMER** received the B.Sc. degree (Hons.) in mathematics from Vidyasagar University, India, in 2005, the M.C.A. degree from the West Bengal University of Technology, India, in 2008, the M.Tech. degree from the University of Kalyani, India, in 2012, and the Ph.D. degree from the Department of Information Technology, Jadavpur University, Kolkata, India. He was a Research Personnel with the Indian Statistical Institute (ISI), Kolkata, from November 2012 to April 2017. He is currently an Assistant Professor with the Department of Computer Science and Engineering, Aliah University, Kolkata. His research interests include computer vision, machine learning, and deep learning.

**CHIARA PERO** received the B.S. and M.S. *(cum Laude)* degrees in computer science from the University of Salerno, Italy, in 2016 and 2018, respectively, where she is currently pursuing the Ph.D. degree in computer science with the Biometric and Image Processing Laboratory (BIPLAB). Her research interests include machine learning technics in facial recognition, image processing, behavioral profiling, and activity recognition.

**MICHELE NAPPI** (Senior Member, IEEE) received the Laurea degree *(cum laude)* in computer science from the University of Salerno, Italy, in 1991, the M.Sc. degree in information and communication technology from I. I. A. S. S. E. R. Caianiello, in 1997, and the Ph.D. degree in applied mathematics and computer science from the University of Padua, Italy, in 1997. He is currently a Full Professor of computer science with the University of Salerno. He is also the Team Leader of the Biometric and Image Processing Laboratory (BIPLAB). He is the author of more than 160 articles in peer-reviewed international journals, international conferences, and book chapters. He is a Co-Editor of several international books. His research interests include pattern recognition, image processing, image compression and indexing, multimedia databases and biometrics, human–computer interaction, and VR/AR. He is a member of TPC of international conferences and GIRPR/IAPR. He received several international awards for scientific and research activities. He serves as an Associate Editor and a Managing Guest Editor for several international journals. In particular, he serves as an Associate Editor for *Pattern Recognition Letters* and promoted many special issues for this journal. He has been the President of the Italian Chapter of the IEEE Biometrics Council. In 2014, he was one of the founders of the spin off biometric system for security and safety (BS3).