Pattern Recognition Letters 174 (2023) 17–24

Contents lists available at ScienceDirect

Pattern Recognition Letters

journal homepage: www.elsevier.com/locate/patrec

Face recognition system with hybrid template protection scheme for Cyber–Physical-Social Services

Alamgir Sardar [a], Saiyed Umer [a], Ranjeet Kumar Rout [b], Chiara Pero [c,*]

[a] Department of Computer Science and Engineering, Aliah University, Kolkata, India
[b] Department of Computer Science and Engineering, National Institute of Technology, Srinagar, Jammu and Kashmir, India
[c] Department of Computer Science, University of Salerno, Fisciano, Italy

ARTICLE INFO

Editor: Maria De Marsico

MSC:
41A05
41A10
65D05
65D17

Keywords:
Face recognition
Cyber–Physical–Social Systems
FaceHashing
Cancelable biometric
BioCryptosystem
Hybrid Template Protection Scheme

ABSTRACT

This paper presents a secure face recognition system with advanced template protection schemes for Cyber–Physical–Social Services (CPSS). The implementation of the proposed system consists of five components. The initial step performs image preprocessing, where it detects the facial region from the captured image using the Tree-Structured Part Model (TSPM). The second phase involves feature extraction, where it utilizes the Scale Invariant Feature Transform (SIFT) descriptor to extract features from small patches of the preprocessed images, forming a collection of feature descriptors. The collection of feature descriptors is then clustered using the K-means clustering algorithm, returning the centers of K-clusters that serve as the vocabulary of a dictionary. Finally, a histogram is generated using the vocabularies and frequencies, referred to as the "Bag of Visual Words (BoVW)". Using this dictionary and a feature learning technique called Sparse Representation Coding (SRC), followed by Spatial Pyramid Mapping (SPM), the system generates feature vectors from training/testing image samples. In the third component, the modified FaceHashing technique is applied to the original feature vectors, generating cancelable feature vectors. The fourth component employs a Bio-Cryptographic technique to preserve the cancelable feature vectors in a database. Lastly, the fifth component utilizes a multi-class linear SVM classifier on the decrypted and query-cancellable feature vector to classify users. The system evaluates its performance using FERET and CASIA-FaceV5 benchmark databases, providing 100% identification accuracy for 200-dimensional cancelable feature vectors. The performance and security comparisons demonstrate the superiority of the proposed system over existing methods.

1. Introduction

In recent years, systems or devices have been upgraded into smart connected systems or devices, which are known as cyber–physical systems (CPSs) or the Internet of Things (IoT). By incorporating social networks into CPSs provides a new instance called CPSSs [1,2]. CPSSs enable device-to-device and human-to-device communications and create a constant interaction between humans and devices. CPSSs rely on various technologies such as artificial intelligence (AI), virtual reality (VR), big data, wireless sensor networks (WSN), 5G wireless communication networks, etc. CPSS assumes a pivotal role in propelling the data science revolution by systematically promoting a tri-space information resource encompassing cyber, physical, and social spaces [3]. The computation of large-scale data encounters security and privacy challenges within CPSSs [4]. Hence, it is crucial to integrate appropriate strategies to ensure privacy and security. Nowadays, biometric recognition systems are an effective alternative to password-based authentication systems [5]. These systems rely on facial, fingerprint, iris, palmprint, and voice biometric traits. Among these traits, facial biometrics are frequently preferred in recognition systems due to their ease of capture compared to other biometric traits. However, it is essential to note that facial features are also more vulnerable to attacks, including spoofing attacks [6] (i.e., attack by photocopy, plastic surgery, makeup, etc.), video attacks, 3D mask [7], and morphing [8]. Therefore, it is necessary to consider these attacks while preserving user-sensitive facial data. Protecting face data in the real-time face recognition system (FRS) is becoming challenging with its increasingly widespread adoption. There are various biometric template protection schemes such as (i) *image template transformation* that protects templates at the image level using watermarking, visual cryptography, and steganography methods, (ii) *feature template transformation* in the form of cancelable biometrics generated by transforming biometric features into a transformed domain by

* Corresponding author.
E-mail addresses: alamgir.cse.rs@aliah.ac.in (A. Sardar), saiyed.umer@aliah.ac.in (S. Umer), ranjeetkumarrout@nitsri.net (R.K. Rout), cpero@unisa.it (C. Pero).

https://doi.org/10.1016/j.patrec.2023.08.011
Received 29 May 2022; Received in revised form 14 July 2023; Accepted 23 August 2023
Available online 25 August 2023

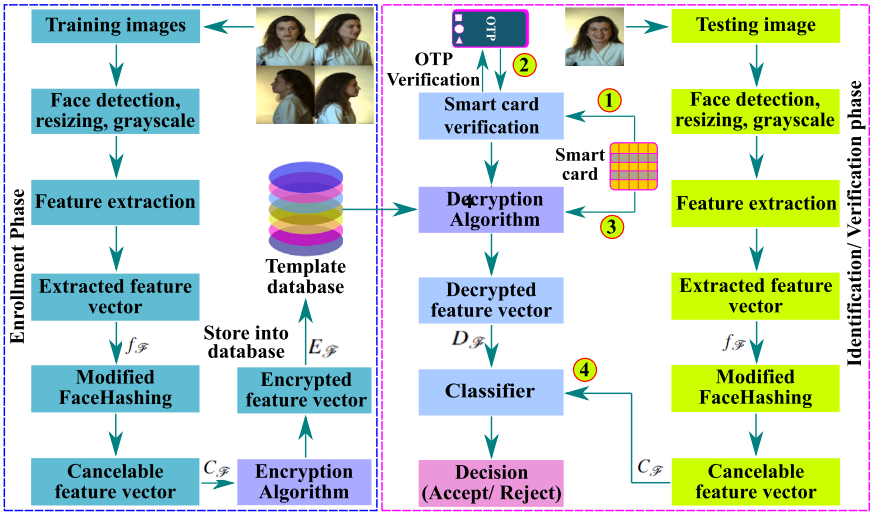

Fig. 1. Block diagram of the proposed smart-card-based FRS. The diagram consists of two phases: the enrollment phase and the authentication phase. In the enrollment phase of training, images are preprocessed through face detection, resizing variable-dimensional images to equal dimensions. Features are extracted from preprocessed image samples, cancelable feature vectors are computed from original feature vectors using a modified FaceHashing algorithm, and finally, cancelable feature vectors are stored in a template database in encrypted form. In the authentication phase, the user inserts a smart card into the system, and the system verifies this card by sending an OTP to the user's phone. At the same time, a sensor captures the user's face and generates cancelable biometrics in the same way as in the enrollment phase. If OTP verification is successful, a classification operation is performed between decrypted enrolled (training) cancelable feature vectors and tested cancelable feature vectors.

using passwords or token-based methods, and (iii) *biometric cryptosystem* that enables the encryption algorithms to encrypt the biometric or cancelable biometric features using a cryptographic algorithm during online authentication [9] to overcome the security issues of biometric template. The image template-based transformation techniques are unsuitable for the proposed system because the attacker can reconstruct the original image from the transformed one [10,11]. On the other hand, feature template transformations are more secure than image-based transformations, but a recent study [12] says that they are also vulnerable during authentication. Apart from the original image reconstruction issue, feature transformation-based template protection schemes suffer from database, channel, and score-matching attacks. A hybrid method consisting of feature transformation and a cryptographic algorithm (BioCryptosystem) can be used to overcome these issues. To sum it up, the contributions can be summarized as follows:

- an encrypted domain-based recognition system to perform the user's identification and verification while ensuring the system's impenetrable security utilizing two-layer security schemes such as cancelable biometrics followed by Bio-Cryptography;
- an extended cancelable biometric scheme employing the modified Rivest–Shamir–Adleman (RSA) cryptographic algorithm;
- a smart-card authentication scheme.

The remainder of this paper is structured as follows: Section 2 presents the related works. Section 3 demonstrates the methodology of the proposed system. Section 4 describes the results of the experiments conducted, including the computational complexity of the system. Finally, Section 6 concludes by drawing some directions for future research.

2. Related work

Various FRS and face template protection schemes based on Bio-Cryptosystems and cancelable biometrics have been proposed in the last few years. Hahn et al. [13] investigated template protection schemes for the FRS based on Neural Network (NN). Chang et al. [14] proposed a cancelable multi-biometric user authentication scheme using a fuzzy extractor and a bit-wise encryption technique for feature-level template protection. Vijayarajan et al. [15] proposed a bio-key-generation scheme based on an Advanced Encryption Standard algorithm to transmit multimedia components through vulnerable networks. Aggarwal et al. [16] proposed a deep NN-based model for automated FRS in smartphones with the FedFace model as the learning framework, improving performance. Dev et al. [17] designed a face recognition module using deep face features. This module generates synthesized aged face images over age progression and is used for face matching. Zhou et al. [18] proposed a human emotion recognition method using electroencephalogram biometrics based on the valence lateralization feature representation technique of the brain connectivity reservoir for the CPSS. They achieved 85.55% emotion recognition. Zhou et al. [19] proposed a CPSS for personalized human activity recognition based on 2-dimensional federated learning (2DFL). Isern et al. [20] proposed a smart video surveillance system for future smart cities to provide critical infrastructure protection using a reconfigurable cyber–physical system. Tan et al. [21] proposed a CPSS Big Data using a blockchain-based access control framework. Access control permissions for CPSS big data are defined and stored on the blockchain. CPSS has been designed to achieve privacy-preserving access control, authorization and revocation, and auditing in blockchain-based access control CPSS. Moreover, to achieve privacy-preserving symmetric encryption, it has been employed. Wang et al. [22], Gati et al. [3], and Zhang et al. [23] presented a comprehensive review of three-tier data fusion, such as fusion of cyber, physical, and social spaces in the CPSS state-of-the-art and perspectives. Table 1 summarizes some recent FRS with template protection schemes.

3. Proposed methodology

The proposed FRS with the template protection scheme consists of two phases: (a) the enrollment phase and (b) the authentication phase. Both phases have some common steps, such as (i) face detection, (ii) feature extraction from the detected face, and (iii) feature transformation. Additionally, the enrollment phase consists of a BioCryptosystem where transformed features are encrypted and then stored in a database as a template, and the authentication phase consists of a classification task. This section covers all of these components, and Fig. 1 depicts the block diagram of our proposed methodology by describing each component of the proposed FRS.

Table 1
Summary of some recent FRS with template protection schemes. Here, GAR: Genuine Acceptance Rate, IR-1: Rank 1 Identification Rate, FPIR: False Positive Identification Rate, FNIR: False Negative Identification Rate.

Method	Year	Feature extraction	Databases used	Performance	Template protection	Limitations or flaws
[24]	2018	Deep CNN	PIE, Color FERET, PIE	91.91%, 94.85%, 96.05% IR-1	SHA3–512	All hardware/ software do not support SHA3
[25]	2019	Deep Learning	IJB-A, IJB-C	97.88% IR-1	Fuzzy commitment	Performance dropped
[26]	2019	Deep CNN	PIE, Extended Yale B	99.40%, 99.16% IR-1	Deep low-density parity check codes	No time complexity analysis
[27]	2019	Deep Learning	Caltech Faces, Georgia Tech	99.98%, 99.99% IR-1	BioCapsule	If feature vector is compromised then need to retake biometric.
[28]	2020	Classical	CASIA-V5, IITK, CVL, FERET	99.85%, 100%, 100%, 100% IR-1	RSA algorithm	Smaller key length, more execution time, need to remember public keys.
[29]	2020	Classical	FERET, FEI, PIE	98.11%, 99.44%, 96.54% GAR	Hashing	No empirical irreversibility, theoretical & empirical renewability criterion is mentioned.
[30]	2020	Deep Learning	FaceNet, ArcFace	98.50%, 99.03% IR-1	Post-quantum Cryptography	Database, channel attack
[31]	2020	Deep Learning	Color FERET, CMU-PIE, FRGC v2.0	98.55%, 99.00%, 99.81% GAR	Randomized CNN and secure sketch	Time complexity is not analyzed.
[32]	2020	FaceNet	FEI, LFW, Georgia Tech	99.99%, 96.10%, 99.97 GAR%	Homomorphic Encryption	Time complexity is not analyzed.
[33]	2021	Deep Learning	LFW, VGG2, IJB-C	99.86%, 99.77%, 81.36% IR-1	Fuzzy Vault	Time complexity is not analyzed.
[34]	2021	Deep Learning	MORPH	99.94% IR-1, 0.1% FPIR, 0.42% FNIR	Homomorphic Encryption	Time complexity is not analyzed.
[35]	2021	Deep Learning	FEI, FERET, LFW	99.82%, 99.79%, 99.84% IR-1	Homomorphic Encryption	Time complexity is not analyzed.
[34]	2021	Deep Learning	FERET	~ 5% FNIR, 1% FPIR	Homomorphic Encryption	No empirical irreversibility, theoretical & empirical renewability criterion is mentioned.
[36]	2022	Deep Learning	MegaFace, ImageNet	81.4%, 86.2% RR-1	Homomorphic Encryption	Complex key generation method.
[37]	2022	FaceNet	FERET, LFW	98.9%, 99.2% IR-1	Homomorphic encryption	Multiple key generation scheme increases execution time.
[38]	2022	Deep CNN	MOBIO (Facenet, Idiap)	99.87%, 99.85% IR-1	PolyProtect	Time complexity is not analyzed.

3.1. Image preprocessing

Illuminations, occlusion by accessories, frontal and profile face poses with expressions and accessories (makeup, cap, spectacles), variations in expressions, and low resolution are the challenging issues of the captured biometrics, which degrade the performance of the system. Here, we employed the TSPM [39] for the facial landmark detection of the input images. The TSPM detects four corner points, like a rectangular box representing the facial region, which are computed using the calculated landmark points. This detected facial region is then preprocessed to extract features, and these final preprocessed images are considered input image $\mathcal{F}$. The working principle of TSPM is that it calculates a Histogram of oriented Gradients (HoG) descriptors corresponding to each pixel in the image region. The motivation behind the use of TSPM is that it detects 68 and 39 landmark points from frontal (Fig. 2(a)) and profile (Fig. 2(e)) faces, respectively. These landmark points are nothing but the coordinate points computed on the action points of the face region. Here, we considered these landmark points as the coordinate points (x-abscissa, y-ordinate). The x-abscissas of these coordinates represent the columns, while the y-coordinates represent the given input rows in the digital imaging system. So, using the min–max principle applied to the x-abscissa (x_{min}, x_{max}) and similarly (y_{min}, y_{max}) of the y-ordinate of the coordinate points have been computed. The combination of (x_{min}, y_{min}), (x_{min}, y_{max}), (x_{max}, y_{min}), (x_{max}, y_{max}) forms the 4 points based on the computed landmark coordinate points. Considering these 4 points as corner points, a rectangular box of facial regions is extracted from the given input image. Hence, these assumed corner points help to compute the region of interest $\mathcal{F}$ (Fig. 2(c), 2(g)) from the selected 4 corner points of the pixels (Fig. 2(b), 2(f)).

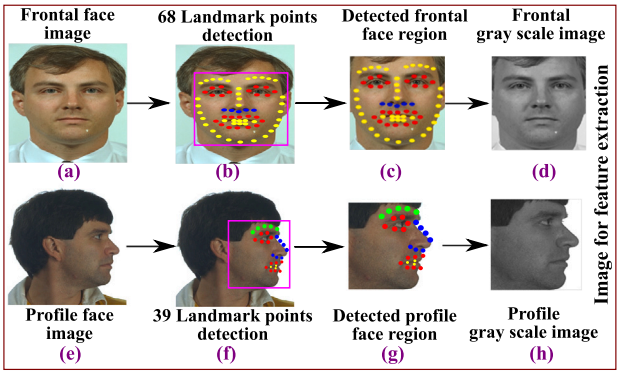

Fig. 2. Image preprocessing steps in the proposed system.

Due to the different dimensions of the detected facial regions, input images are scaled into equal-sized square dimensions, i.e., 200 × 200. Smaller dimensional images provide less information, which is unsuitable for extracting useful patterns. On the other hand, high-dimensional images need more recognition and encryption/decryption time. Hence, the intermediate image sizes are considered.

3.2. Feature extraction

The preprocessed 200 × 200 grayscale images are used for feature computation. This feature computation technique consists of two

steps such as (1) codebook formation, then (2) feature computation using codebook. During dictionary formation, we considered a small patch $w \in \mathbb{R}^{25\times25}$ over M training samples of $\mathcal{F}$ overlapping p pixels horizontally and then vertically. Then the dense-SIFT descriptor is used as the feature extractor which forms a visual descriptor vector $d_{SIFT(w_i)} = [d_1, d_2, d_3, \dots, d_R]^T \in \mathbb{R}^{R\times128}$ from each patch w_i, where R is the number of descriptor of each patch w_i and the value 128 indicates the dimension of each descriptor d_i. These vectors are combined to form a single collection of descriptor vectors $D_{SIFT(w)} = [d_{SIFT(w_1)}, d_{SIFT(w_2)}, \dots, d_{SIFT(w_{(N-1)})}, d_{SIFT(w_N)}]^T = [d_1, d_2, \dots, d_i, d_{i+1}, \dots, d_S]^T \in \mathbb{R}^{S\times128}$ where N = number of patches of an image $\mathcal{F}$ and $S = N \times R$. $D_{SIFT(w)}$ contains sufficient local texture information and provides good performance. The vlfeat [40] software has been employed for this purpose. Hence, M training image samples generate MS number of SIFT descriptors i.e. $D_{SIFT} = \left[D_{SIFT_1}, D_{SIFT_2}, D_{SIFT_3}, \dots, D_{SIFT_{MS}}\right]$. Then the K-means clustering algorithm is applied on $D_{SIFT(w)}$ to cluster the descriptors. K-means separates the data points into K clusters/ groups and returns cluster center (i.e. centroid of the clusters) and these cluster centers are considered as the vocabulary of a dictionary/ codebook $C = [c_1, c_2, \dots c_K]^T \in \mathbb{R}^{K\times128}$. Then, for each image, a histogram is built based on the codebook (along the x-axis) and its frequency (along the y-axis). These histograms are used as the bag-of-visual-words (BOVW) [41]. During feature extraction, we extracted collection of descriptor vectors from the training/ testing image samples in the same way. Then the SRC technique is used on collection of descriptor vectors as the feature learning technique to generate similar codes for similar descriptors from training/ testing image samples with the help of the dictionary C. Finally, we obtain the spectrum of codebooks ($c_i's$) of an input image $\mathcal{F}$ and these generate non-statistical descriptors $\alpha_i = (\alpha_{i1}, \alpha_{i2}, \alpha_{i3}, \dots \alpha_{iK})^T \in \mathbb{R}^{K\times1}$ where linear combination of each α_{ij} with code-words c_j generates β_i such that $\beta_i = (\alpha_{i1}.c_1 + \alpha_{i2}.c_2 + \alpha_{i3}.c_3 + \dots + \alpha_{iK}.c_K)$ for $\beta_i \in D_{SIFT(w)}$. The descriptor α_i is computed by solving the constrained least square fitting problem (Eq. (1)).

$$\arg\min_{\alpha} \sum_{i=1}^{S} \|\beta_i - C\alpha_i\|^2,$$
$$\text{such that } \|\alpha_i\|l_0 = \|\alpha_i\|l_1 = 1 \ \alpha_{ji} \geq 0, \ \forall i \tag{1}$$

The constraint $\|\alpha_i\|l_0$ indicates that there is only one non-zero element in each vector α_i, and the constraint $\|\alpha_i\|l_1$ indicates that the non-zero coding weight α_{ij} for β_i is 1 i.e., $\alpha_i = (0, 0, \dots, 0, 1, 0, 0, \dots, 0)^T$. This optimization problem obtains the index of a non-zero element in α_i, which corresponds to the belonging of β_i in C, i.e. if $\alpha_{ij} = 1$ then β_i is represented by c_j. This technique is termed the Bag-of-Visual-Words (BoVW) model, and the image descriptor becomes the histogram or frequency distribution of the code-word c_j.

To overcome the quantization error in this optimization technique, the sparsity regularization term is introduced in each α_i by relaxing the constraint $\|\alpha_i\|l_0 = 1$ and selecting the constraint $\|\alpha_i\|l_1 = 1$. This feature learning technique is known as SRC [42] and is defined in Eq. (2). The main objective of SRC is to generate similar codes for similar descriptors, resulting in good classification performance.

$$\arg\min_{\alpha} \sum_{i=1}^{S} \|\beta_i - C\alpha_i\|^2 + \lambda\|\alpha_i\|l_1$$
$$\text{such that } \sum_j \alpha_{ij} = 1, \ \alpha_{ij} \geq 0, \ \forall i \tag{2}$$

Here $\|\alpha_j\|_1 = 1$ is the sparsity regularization constraint with regularization parameter λ. The constraint $\|\alpha_j\|l_0 = 1$ is l_1-norm that is the sum of $\alpha_{ij} \in \alpha_j$. The SPM [43] technique has been applied on α's to improve BoVW by partitioning images to get more sub-regions. Then from each of these sub-regions, we have obtained a histogram of coefficients (α). Finally, the histograms are concatenated to form a feature vector $f_{\mathcal{F}} \in \mathbb{R}^{1\times5000}$ from each image $\mathcal{F}$ using SRC followed by SPM (see Fig. 3).

3.3. Cancelable face template

The proposed cancelable biometric phase consists of four steps such as:

1. **Projection operation** between original feature vector $f_{\mathcal{F}} \in \mathbb{R}^{1\times D}$ and a matrix $R \in \mathbb{R}^{D\times m}$ ($D \gg m$) which is computed from a randomly generated matrix $R_0 \in \mathbb{R}^{D\times m}$ normalized by Gram Schmidth Orthogonalization method i.e., $x_{\mathcal{F}} =< f_{\mathcal{F}} \odot R >= \left[x_1, \dots, x_m\right] \in \mathbb{R}^{1\times m}$ and projection operation is performed with the help of a subject specific token $t_{subject}$ (shown in Eq. (3)). $x_{\mathcal{F}}$ is called level-1 cancelable feature vector.
2. **Permutation** of the elements of $x_{\mathcal{F}}$ with the help of permutation function π and token $t_1 = t_{subject} + t_{system}$ (t_{system} is system dependent token) which generates level-2 cancelable feature vector $x'_{\mathcal{F}}$ (shown in Eq. (4)). This permutation operation improves both the performance and security of the system.
3. Another **permutation** of the elements of $x'_{\mathcal{F}}$ with the help of permutation function π and token $t_2 = t_{subject} + t'_{system}$ (t'_{system} is system dependent token) which generates level-3 cancelable feature vector $x''_{\mathcal{F}}$ (shown in Eq. (5)). This permutation operation improves both the performance and security of the system than first permutation and $x''_{\mathcal{F}}$ is more discriminant than $x'_{\mathcal{F}}$. The original feature vector $f_{\mathcal{F}}$ will be preserved in offline mode whereas $x''_{\mathcal{F}}$ will be used for authentication in online mode.
4. Finally, $x''_{\mathcal{F}}$ is transformed into integer domain $C_{\mathcal{F}} \in \mathbb{Z}^{1\times m}$ as the resulting cancelable feature vector.

$$f_{\mathcal{F}} \odot R \xrightarrow{t_{subject}} x_{\mathcal{F}} \xrightarrow[\text{to } \mathbb{Z}]{\text{Convert}} C_{\mathcal{F}} \tag{3}$$

$$f_{\mathcal{F}} \odot R \xrightarrow{t_{subject}} x_{\mathcal{F}} \xrightarrow{\pi_{t_1}(x_{\mathcal{F}})} x'_{\mathcal{F}} \xrightarrow[\text{to } \mathbb{Z}]{\text{Convert}} C_{\mathcal{F}} \tag{4}$$

$$f_{\mathcal{F}} \odot R \xrightarrow{t_{subject}} x_{\mathcal{F}} \xrightarrow{\pi_{t_1}(x_{\mathcal{F}})} x'_{\mathcal{F}} \xrightarrow{\pi_{t_2}\left(x'_{\mathcal{F}}\right)} x''_{\mathcal{F}} \xrightarrow[\text{to } \mathbb{Z}]{\text{Convert}} C_{\mathcal{F}} \tag{5}$$

In the following sections, instead of $x''_{\mathcal{F}} \in \mathbb{R}^{1\times m}$, $C_{\mathcal{F}} \in \mathbb{Z}^{1\times m}$ is considered as the cancelable feature vector. To enhance the system's security, we have used a cryptographic encryption algorithm on $C_{\mathcal{F}}$. Moreover, we employed BioCryptography on the generated cancelable biometrics to preserve those in the database which is used during authentication.

3.4. BioCryptosystem using modified RSA algorithm

For the proposed BioCryptosystem, we have modified the existing RSA algorithm [44] by introducing four prime numbers instead of two prime numbers to encrypt the extracted cancelable feature vector more securely. The RSA algorithm is an asymmetric key cryptographic algorithm that employs two distinct keys: the public key ($\mathcal{P}_u$) and the private key ($\mathcal{P}_r$). The public key is used to encrypt the cancelable feature vector, and the private key is stored in a smart card to decrypt the encrypted cancelable feature vector during authentication.

3.5. Classification

In classification, we computed the correct recognition rate (CRR%) and equal error rate (EER%) using a multi-class linear SVM classifier [45] as the identification and verification performances of the system, respectively. The motivation behind the use of a multi-class linear SVM classifier is that the low variability between inter (dissimilarity) class images or high variability between intra (similarity) class images complicates the recognition system. While exhibiting sufficient distinctiveness for inter-class images and significant similarity for intra-class images, the SVM classifier also displayed outstanding performance compared to the other classifiers. Apart from these, the SVM classifier controls the trade-off between the errors in the recognition system

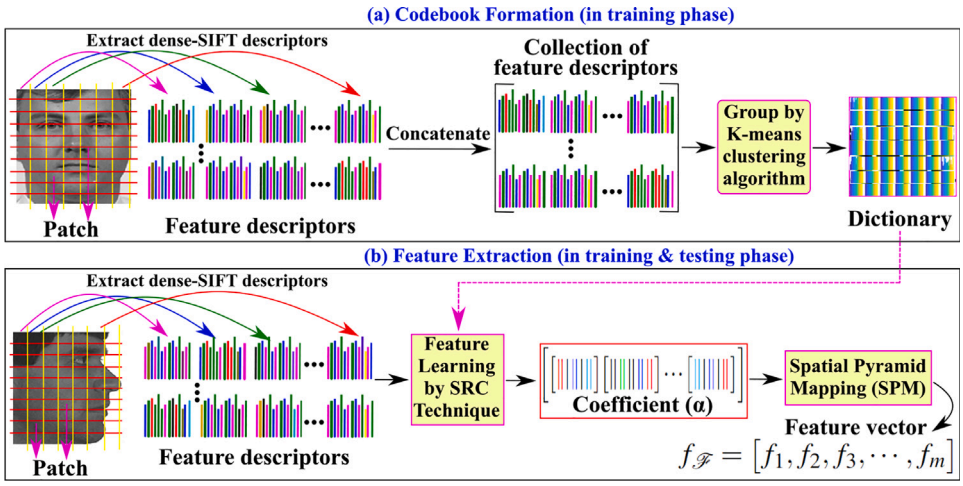

Fig. 3. Proposed feature extraction technique.

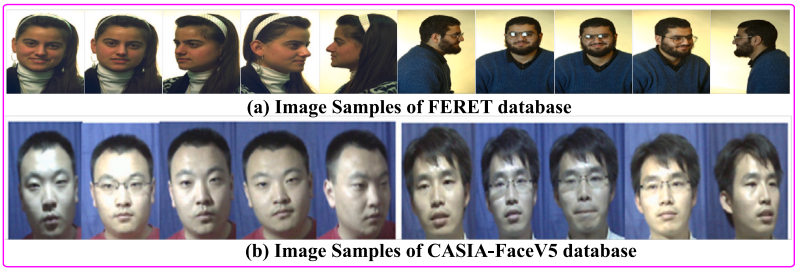

Fig. 4. Image samples of the FERET and CASIA-FAceV5 databases.

during the classification task. The kernel-based SVM provides a better solution for various complex problems due to its convex optimization nature and helps find the separating hyperplanes to handle the high-dimensional data.

4. Experiments

In our experiments, Intel Core i5 processor running at 3 GHz and DDR4 8 GB RAM, 2666 MHz are used as hardware platforms, and Windows 10, MATLAB R2016a, and Java as software platforms, respectively.

4.1. Databases

The performance evaluation of this system has been conducted using two benchmark facial databases: CASIA-FaceV5 [46] and FERET [47]. There are 2500 images in the CASIA-FaceV5 database of 500 individuals, each with five samples and intra-class variations, including pose, expressions, eyeglasses, illumination, imaging distance, etc. The image resolution is 640 × 480 pixels for all 16-bit color BMP files. FERET database contains 4970 images of 994 subjects, each with five samples with intra-class variations, including poses, expressions, eyeglasses, illumination, etc., of frontal and profile faces. Image samples of the proposed databases are shown in Fig. 4.

4.2. Results and discussions

Table 2 shows the CRR% and EER% performances of the system. Table 3 compares the performance of some state-of-the-art FRS with the proposed system for the original feature vector $f_{\mathcal{F}} \in \mathbb{R}^{1\times5000}$ with several training-testing percentages. Compared to other competing methods, the proposed feature vectors provide better performance, as shown in Table 3.

Table 2
Performance of the proposed face recognition system using original feature vector $f_{\mathcal{F}}$.

Database	Percentage of training samples-testing samples									
	50%–50%		60%–40%		70%–30%		80%–20%		90%–10%	
	CRR	EER	CRR	EER	CRR	EER	CRR	EER	CRR	EER
FERET	54.63	0.1520	62.89	0.0981	70.52	0.0892	74.66	0.0710	86.32	0.0188
CASIA-FaceV5	78.82	0.1307	79.84	0.0865	80.32	0.0632	81.90	0.0489	83.50	0.0296

Table 3
Performance comparison between existing methods and the proposed method for FERET and CASIA-FaceV5 database.

Methods	Training/ Testing	CRR (%)	EER (%)	Methods	Training/ Testing	CRR (%)	EER (%)
FERET				CASIA-FaceV5			
Huang et al. [48]	(90%–10%)	85.17	0.0079	Feng et al. [49]	(60%–40%)	37.60	0.1891
Yang et al. [50]	(90%–10%)	84.72	0.0180	Umer et al. [51]	(60%–40%)	67.56	0.1301
Yin et al. [52]	(90%–10%)	68.98	0.1201	Benamara et al. [53]	(80%–20%)	99.26	0.75
Kumar et al. [24]	(90%–10%)	94.85	2.16	Lu et al. [54]	(80%–20%)	95.00	–
Osorio et al. [35]	(90%–10%)	99.79	0.86	Liu et al. [55]	(80%–20%)	98.80	–
Roman et al. [37]	(90%–10%)	98.90	–	Sun et al. [56]	(80%–20%)	87.30	–
Dang et al. [29]	(90%–10%)	98.11	0.9300	Qi et al. [57]	(80%–20%)	99.35	–
Proposed	(90%–10%)	**86.32**	0.0188	**Proposed**	(80%–20%)	**81.90**	0.0489

To improve performance and security of the original feature $f_{\mathcal{F}}$, we employed the FaceHashing technique, which generates the feature vector $x_{\mathcal{F}}$ from $f_{\mathcal{F}}$, $x'_{\mathcal{F}}$ from $x_{\mathcal{F}}$, and $x''_{\mathcal{F}}$ from $x'_{\mathcal{F}}$ using Eq. (3), Eq. (4), and Eq. (5), respectively. The generated feature vectors obtained after applying Eq. (3), Eq. (4), and Eq. (5) are referred to as CFR_1 (Cancelable Face Recognition level-1), CFR_2, and CFR_3 respectively.

In CFR_1, $f_{\mathcal{F}} \in \mathbb{R}^{1\times5000}$ is transformed to $m = 100$, $m = 200$, and $m = 500$ dimensional feature vectors by projection operation (shown in Eq. (3)) with the orthonormalized random matrix $R \in \mathbb{R}^{5000\times m}$ to generate $x_{\mathscr{F}} \in \mathbb{R}^{1\times m}$ i.e. $x_{\mathcal{F}} \in \mathbb{R}^{1\times100} = \left[f_{\mathcal{F}} \in \mathbb{R}^{1\times5000} \odot R \in \mathbb{R}^{5000\times100}\right]$. The performance obtained in CFR_1 is reported in Table 4.

Table 4
Performance of the proposed CFR_1 in CRR (%) and EER, *dim* stands for dimension of feature vector.

Database	100 *dim*		200 *dim*		500 *dim*	
	CRR	EER	CRR	EER	CRR	EER
FERET	95.25	0.08347	100	0.0000	100	0.0000
CASIA-FaceV5	98.12	0.0436	100	0.0000	100	0.0000

Table 5
Performance of the proposed CFR_2 in CRR (%) and EER.

Database	100 *dim*		200 *dim*		500 *dim*	
	CRR	EER	CRR	EER	CRR	EER
FERET	95.70	0.0352	100	0.0000	100	0.0000
CASIA-FaceV5	98.26	0.0125	100	0.0000	100	0.0000

Table 6
Performance of the proposed CFR_3 in CRR (%) and EER.

Database	100 *dim*		200 *dim*		500 *dim*	
	CRR	EER	CRR	EER	CRR	EER
FERET	96.72	0.0063	100	0.0000	100	0.0000
CASIA-FaceV5	98.71	0.0015	100	0.0000	100	0.0000

In CFR_2, a permutation operation (shown in Eq. (4)) is performed on x_F using system-specific token t_1 to compute x'_F which is more secure than x_F because it is very difficult to revert x_F from x'_F. The performance obtained in CFR_2 is shown in Table 5 which shows that the performance of CFR_2 is better than CFR_1.

Furthermore, another permutation operation (shown in Eq. (5)) is performed on x'_F using system specific token t_2 to compute x''_F which is CFR_3. The performance obtained in CFR_3 is reported in Table 6 where identification accuracy (CRR%) is 100% for the 200-dimensional feature vectors. Compared to the performance of CFR_2, CFR_3 is better and CFR_3 is also more secure because it is almost impossible to revert to the original feature vector f_F from x''_F by applying reverse operation of $\pi_{t_2}(x'_{\mathscr{F}})$, $\pi_{t_1}(x_{\mathscr{F}})$, and $f_{\mathscr{F}} \odot R$, respectively.

Additionally, to increase the security of the database template for online authentication, the modified RSA algorithm has been used to encrypt the cancelable feature vector C_F, before storing the encrypted feature vector E_F as a template. During system access, the user will insert a smart card, and the system will send a one-time password (OTP) via mail or message. The user then provides the OTP as input, and the system will verify it. After a successful OTP verification, the system will decrypt the user's stored biometric template and classify the query image captured by the onboard camera. Finally, the system identifies or verifies a user as authentic or fake.

5. Analysis of hybrid template protection scheme (HTPS)

To be a reliable and practical cryptographic method, it must have a high computational complexity of the parameters and fast execution of both encryption and decryption operations, which are both necessary and sufficient criteria. In the following subsections, we discuss these criteria for the proposed HTPS.

5.1. Computational complexity analysis of the HTPS

The computational complexity of the proposed system depends on the various parameters used for modified FaceHashing and modified RSA algorithms and the computational approach used in different functions. The Table 7 presents a summary of the time complexity in different steps of the HTPS. All the execution times presented in Table 8 are computed on the reduced 200 dimensional feature vector of CFR_3 for both FERET and CASIA-FaceV5 databases.

Table 7
Time complexity of the proposed HTPS. Here, where d=total number of decimals, b=binary bit length, M=number of integers in C_F or D_F.

Operations	Expression	Time complexity
	Cancelable biometrics	
Projection	$x_F = [f_F \in \mathbb{R}^{1\times D} \odot R \in \mathbb{R}^{D\times m}]$ $x_F = [x_1, \ldots, x_m] \in \mathbb{R}^{1\times m}$	$O(1\times D\times m)$ $= O(Dm)$
Permutation of x_F	$x_{\mathscr{F}} \xrightarrow{\pi_{t_1}(x_{\mathscr{F}})} x'_{\mathscr{F}}$	$O(2^m)$
Permutation of x'_F	$x'_{\mathscr{F}} \xrightarrow{\pi_{t_2}(x'_{\mathscr{F}})} x''_{\mathscr{F}}$	$O(2^m)$
Integer conversion	$x''_{\mathscr{F}} \xrightarrow[\text{to } \mathbb{Z}]{\text{Convert}} C_{\mathscr{F}}$	$O(db)$
	BioCryptosystem	
Key generation	GCD(Φ, e_k)=1 $e_k \times d_k \equiv 1 (\text{mod } \Phi)$	$O\left(log(min(\Phi, e_k))\right)$ $O(log(\Phi))$
Key distribution	$\mathcal{P}_u = <e_k, N>$ $\mathcal{P}_r = <d_k, N>$	$O(1)$
Encryption	$E_F(\text{i, j}) = [C_F(i,j)]^{e_k} (\text{mod } N)$	$O(M \times log(e_k)(logN)^2)$
Decryption	$D_F(\text{i, j}) = [E_F(i,j)]^{d_k} (\text{mod } N)$	$O(M \times log(d_k)(logN)^2)$
Overall time complexity of the HTPS	$= max\left(O(Mlog(e_k)(logN)^2), O(2^m)\right) = O\left(2^m\right)$	

In particular, the reply attack, insider attack, brute force attack, chosen cipher attack, dictionary attack, and lost/stolen smart-card-based attacks were all addressed by the OTP-based smart-card access control system. The system will generate an OTP and send it to the registered phone number when the imposter inserts this card; without this, the imposter cannot proceed further. The attacker will not be able to access the system even if they copy the card and obtain all of the information on it.

5.2. Comparative analysis of the proposed modified RSA

This subsection compares the execution times of the existing and modified RSA algorithms. Table 9 shows that in terms of key generation, encryption, decryption, and overall execution time, the modified RSA algorithm is faster compared to the existing RSA algorithm. Here, only the results obtained from the FERET database are used in the comparisons with the existing systems.

5.3. Novelty of the proposed HTPS

With the proposed HTPS, image-related attacks such as pre-image attacks, replay/print attacks, image reconstruction, etc., and most of the network-related issues such as channel attacks, database attacks, brute-force attacks, chosen cipher attacks, and dictionary attacks can be overcome. The Table 9 shows that, compared to existing RSA-based systems [44,58,59], the modified RSA is faster.

6. Conclusion

This paper presents a face recognition system with a hybrid template protection scheme for CPSS. To achieve better performance of the proposed face recognition system, we implemented an efficient face detection technique (TSPM), a feature extraction technique consisting of SIFT-descriptor, SRC as a feature learning technique, and SPM to improve BoVW. A further extended FaceHashing technique has been employed to generate cancelable biometrics. Using a multiclass linear SVM classifier with a K-fold cross-validation technique, we obtained 100% identification accuracy of the cancelable feature vectors reduced from 5000 to 200 dimensions. The cancelable biometrics provide irreversibility, reusability, unlinkability, and performance preservation. It also provides security support such as reply attacks, print attacks, spoofing attacks, etc. But cancelable biometrics may suffer from key-based

Table 8
Execution time (in milliseconds) for 200 dimensional feature vector in cancelable biometrics phase, Bio-Cryptography phase, enrollment phase, and authentication phase of the proposed system. Enrollment time includes cancelable biometrics phase, key generation, and encryption, whereas authentication time includes cancelable biometrics phase and decryption.

Number of bits in P, Q, R, S	Key length (in bits)	Execution time (in milliseconds) of 200 dimensional feature vector of CFR_3							
		Cancelable biometrics phase			Bio-Cryptography phase			Total time for enrollment	Total time for authentication
		Preprocessing (per sample)	Feature extraction	Modified FaceHashing	Key generation (Prime numbers +Public+Private)	Encryption	Decryption		
FERET									
128	512	198.7	632	217.2	78	10	17	**1135.9**	**1064.9**
256	1024	198.7	632	217.2	113	13	33	**1173.9**	**1080.9**
512	2048	198.7	632	217.2	163	15	45	**1225.9**	**1092.9**
1024	4096	198.7	632	217.2	185	21	322	**1253.9**	**1396.9**
2048	8192	198.7	632	217.2	720	112	2178	**1879.9**	**3225.9**
4096	16384	198.7	632	217.2	3895	328	11952	**5270.9**	**12999.9**
CASIA-FaceV5									
128	512	185.7	643	215.5	81	11	19	**1136.2**	**1063.2**
256	1024	185.7	643	215.5	115	14	27	**1173.2**	**1071.2**
512	2048	185.7	643	215.5	159	15	45	**1218.2**	**1089.2**
1024	4096	185.7	643	215.5	263	20	309	**1327.2**	**1353.2**
2048	8192	185.7	643	215.5	705	117	2195	**1866.2**	**3239.2**
4096	16384	185.7	643	215.5	3907	325	11988	**5276.2**	**13032.2**

Table 9
Comparison between the existing RSA algorithm and the proposed modified RSA algorithm in terms of key generation, encryption, decryption and total execution time.

Article	Length of P, Q, R, S (in bits)	Execution time (in millisecond)			Total execution time (in millisecond)
		Key generation	Encryption	Decryption	
Rivest et al. [44]	128	92	1.1	1.1	94.2
Ivy et al. [58]		144	2.5	2.2	148.7
Thangavel et al. [59]		165	2	2	169
Proposed		**78**	**0.0500**	**0.0850**	**78.1350**
Rivest et al. [44]	256	133	1	1.1	135.1
Ivy et al. [58]		216	4	3	223
Thangavel et al. [59]		237	3	2	242
Proposed		**113**	**0.0650**	**0.1650**	**113.2300**
Rivest et al. [44]	512	352	3	3	358
Ivy et al. [58]		313	21	23	357
Thangavel et al. [59]		389	16	16	421
Proposed		**163**	**0.0750**	**0.2250**	**163.3000**
Rivest et al. [44]	1024	889	21	22	932
Ivy et al. [58]		922	170	169	1261
Thangavel et al. [59]		1168	105	106	1379
Proposed		**185**	**0.1050**	**1.6100**	**186.7150**
Rivest et al. [44]	2048	4315	183	169	4667
Ivy et al. [58]		7471	1393	1379	10243
Thangavel et al. [59]		11164	784	745	12693
Proposed		**720**	**0.5600**	**10.8900**	**731.4500**
Rivest et al. [44]	4096	91542	1380	1381	94303
Ivy et al. [58]		93899	10907	10957	115763
Thangavel et al. [59]		181811	6620	6647	195078
Proposed		**3895**	**1.6400**	**59.7600**	**3956.4000**

attacks (brute force), database attacks (intrusion, dictionary-based), cryptanalysis attacks, forgery-level attacks (lost or stolen key), channel attacks, etc. Hence, the modified RSA cryptographic algorithm has been employed on the cancelable feature vectors to preserve the biometric templates in a template database. Additionally, the OTP-based smart-card access control protects against unauthorized smart-card access. A faster computing technique, a deep learning-based framework, and anti-spoofing mechanisms need to be incorporated in the future to improve the proposed approach.

Declaration of competing interest

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

Data availability

Data will be made available on request.

Acknowledgments

This work was partially supported by the project Information Disorder Awareness (IDA) included in the Spoke 2 - Misinformation and Fakes of the Research and Innovation Program PE00000014, “SEcurity and RIghts in the CyberSpace (SERICS)”, under the National Recovery and Resilience Plan, Mission 4 “Education and Research” - Component 2 “From Research to Enterprise” - Investment 1.3, funded by the European Union - NextGenerationEU.

References

[1] Y. Zhou, F.R. Yu, J. Chen, Y. Kuo, Cyber-physical-social systems: A state-of-the-art survey, challenges and opportunities, IEEE Commun. Surv. Tutor. 22 (1) (2019) 389–425.
[2] R. Reine, F.H. Juwono, Z.A. Sim, W. Wong, Cyber-physical-social systems: An overview, Smart Connected World: Technol. Appl. Shap. Future (2021) 25–45.
[3] N.J. Gati, L.T. Yang, J. Feng, X. Nie, Z. Ren, S.K. Tarus, Differentially private data fusion and deep learning framework for cyber–physical–social systems: State-of-the-art and perspectives, Inf. Fusion 76 (2021) 298–314.
[4] J. Feng, L.T. Yang, N.J. Gati, X. Xie, B.S. Gavuna, Privacy-preserving computation in cyber-physical-social systems: A survey of the state-of-the-art and perspectives, Inform. Sci. 527 (2020) 341–355.
[5] G. Singh, G. Bhardwaj, S.V. Singh, V. Garg, Biometric identification system: Security and privacy concern, Artif. Intell. Sustain. Ind. 4.0 (2021) 245–264.
[6] T. Izu, Y. Sakemi, M. Takenaka, N. Torii, A spoofing attack against a cancelable biometric authentication scheme, in: 2014 IEEE 28th International Conference on Advanced Information Networking and Applications, IEEE, 2014, pp. 234–239.
[7] S. Jia, G. Guo, Z. Xu, A survey on 3D mask presentation attack detection and countermeasures, Pattern Recognit. 98 (2020) 107032.
[8] U. Scherhag, C. Rathgeb, J. Merkle, R. Breithaupt, C. Busch, Face recognition systems under morphing attacks: A survey, IEEE Access 7 (2019) 23012–23026.
[9] U. Uludag, S. Pankanti, S. Prabhakar, A.K. Jain, Biometric cryptosystems: Issues and challenges, Proc. IEEE 92 (6) (2004) 948–960.

[10] A. Nestor, A.C. Lee, D.C. Plaut, M. Behrmann, The face of image reconstruction: Progress, pitfalls, prospects, Trends in Cognitive Sciences 24 (9) (2020) 747–759.

[11] A. Tuan Tran, T. Hassner, I. Masi, G. Medioni, Regressing robust and discriminative 3D morphable models with a very deep neural network, in: Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition, 2017, pp. 5163–5172.

[12] G. Mai, K. Cao, P.C. Yuen, A.K. Jain, On the reconstruction of face images from deep face templates, IEEE Trans. Pattern Anal. Mach. Intell. 41 (5) (2018) 1188–1202.

[13] V.K. Hahn, S. Marcel, Biometric template protection for neural-network-based face recognition systems: A survey of methods and evaluation techniques, 2021, arXiv preprint arXiv:2110.05044.

[14] D. Chang, S. Garg, M. Hasan, S. Mishra, Cancelable multi-biometric approach using fuzzy extractor and novel bit-wise encryption, IEEE Trans. Inf. Forensics Secur. 15 (2020) 3152–3167.

[15] R. Vijayarajan, P. Gnanasivam, R. Avudaiammal, Bio-key based AES for personalized image cryptography, Comput. J. 62 (11) (2019) 1695–1705.

[16] D. Aggarwal, J. Zhou, A.K. Jain, FedFace: Collaborative learning of face recognition model, 2021, arXiv preprint arXiv:2104.03008.

[17] D. Deb, D. Aggarwal, A.K. Jain, Identifying missing children: Face age-progression via deep feature aging, in: 2020 25th International Conference on Pattern Recognition, ICPR, IEEE, 2021, pp. 10540–10547.

[18] J. Zhou, T. Zhao, Y. Xie, F. Xiao, L. Sun, Emotion recognition based on brain connectivity reservoir and valence lateralization for cyber-physical-social systems, Pattern Recognit. Lett. 161 (2022) 154–160.

[19] X. Zhou, W. Liang, J. Ma, Z. Yan, I. Kevin, K. Wang, 2D federated learning for personalized human activity recognition in cyber-physical-social systems, IEEE Trans. Netw. Sci. Eng. 9 (6) (2022) 3934–3944.

[20] J. Isern, F. Barranco, D. Deniz, J. Lesonen, J. Hannuksela, R.R. Carrillo, Reconfigurable cyber-physical system for critical infrastructure protection in smart cities via smart video-surveillance, Pattern Recognit. Lett. 140 (2020) 303–309.

[21] L. Tan, N. Shi, C. Yang, K. Yu, A blockchain-based access control framework for cyber-physical-social system big data, IEEE Access 8 (2020) 77215–77226.

[22] P. Wang, L.T. Yang, J. Li, J. Chen, S. Hu, Data fusion in cyber-physical-social systems: State-of-the-art and perspectives, Inf. Fusion 51 (2019) 42–57.

[23] S. Zhang, L.T. Yang, J. Feng, W. Wei, Z. Cui, X. Xie, P. Yan, A tensor-network-based big data fusion framework for cyber–physical–social systems (CPSS), Inf. Fusion 76 (2021) 337–354.

[24] A. Kumar Jindal, S. Chalamala, S. Kumar Jami, Face template protection using deep convolutional neural network, in: Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition Workshops, 2018, pp. 462–470.

[25] D.D. Mohan, N. Sankaran, S. Tulyakov, S. Setlur, V. Govindaraju, Significant feature based representation for template protection, in: CVPR Workshops, 2019, pp. 2389–2396.

[26] L. Chen, G. Zhao, J. Zhou, A.T. Ho, L.-M. Cheng, Face template protection using deep LDPC codes learning, IET Biometrics 8 (3) (2019) 190–197.

[27] T. Phillips, X. Zou, F. Li, N. Li, Enhancing biometric-capsule-based authentication and facial recognition via deep learning, in: Proceedings of the 24th ACM Symposium on Access Control Models and Technologies, 2019, pp. 141–146.

[28] A. Sardar, S. Umer, C. Pero, M. Nappi, A novel cancelable FaceHashing technique based on non-invertible transformation with encryption and decryption template, IEEE Access 8 (2020) 105263–105277.

[29] T.M. Dang, L. Tran, T.D. Nguyen, D. Choi, Fehash: Full entropy hash for face template protection, in: Proceedings of the IEEE/CVF Conference on Computer Vision and Pattern Recognition Workshops, 2020, pp. 810–811.

[30] J. Kolberg, P. Drozdowski, M. Gomez-Barrero, C. Rathgeb, C. Busch, Efficiency analysis of post-quantum-secure face template protection schemes based on homomorphic encryption, in: 2020 International Conference of the Biometrics Special Interest Group, BIOSIG, IEEE, 2020, pp. 1–4.

[31] G. Mai, K. Cao, X. Lan, P.C. Yuen, Secureface: Face template protection, IEEE Trans. Inf. Forensics Secur. 16 (2020) 262–277.

[32] A.K. Jindal, I. Shaik, V. Vasudha, S.R. Chalamala, R. Ma, S. Lodha, Secure and privacy preserving method for biometric template protection using fully homomorphic encryption, in: 2020 IEEE 19th International Conference on Trust, Security and Privacy in Computing and Communications, TrustCom, IEEE, 2020, pp. 1127–1134.

[33] X. Dong, S. Kim, Z. Jin, J.Y. Hwang, S. Cho, A.B.J. Teoh, Secure chaff-less fuzzy vault for face identification systems, ACM Trans. Multimidia Comput. Commun. Appl. 17 (3) (2021) 1–22.

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

[35] D. Osorio-Roig, C. Rathgeb, P. Drozdowski, C. Busch, Stable hash generation for efficient privacy-preserving face identification, IEEE Trans. Biometrics, Behav., Identity Sci. 4 (3) (2021) 333–348.

[36] J.J. Engelsma, A.K. Jain, V.N. Boddeti, HERS: Homomorphically encrypted representation search, IEEE Trans. Biometrics, Behav., Identity Sci. 4 (3) (2022) 349–360.

[37] R. Román, R. Arjona, P. López-González, I. Baturone, A quantum-resistant face template protection scheme using kyber and saber public key encryption algorithms, in: 2022 International Conference of the Biometrics Special Interest Group, BIOSIG, IEEE, 2022, pp. 1–5.

[38] V.K. Hahn, S. Marcel, Towards protecting face embeddings in mobile face verification scenarios, IEEE Trans. Biometrics, Behav., Identity Sci. (2022).

[39] D. Ramanan, X. Zhu, Face detection, pose estimation, and landmark localization in the wild, in: Proceedings of the 2012 IEEE Conference on Computer Vision and Pattern Recognition, CVPR, Citeseer, 2012, pp. 2879–2886.

[40] A. Vedaldi, B. Fulkerson, VLFeat: An open and portable library of computer vision algorithms, in: Proceedings of the 18th ACM International Conference on Multimedia, ACM, 2010, pp. 1469–1472.

[41] S. Gidaris, A. Bursuc, N. Komodakis, P. Pérez, M. Cord, Learning representations by predicting bags of visual words, in: Proceedings of the IEEE/CVF Conference on Computer Vision and Pattern Recognition, 2020, pp. 6928–6938.

[42] J. Wang, J. Yang, K. Yu, F. Lv, T. Huang, Y. Gong, Locality-constrained linear coding for image classification, in: 2010 IEEE Computer Society Conference on Computer Vision and Pattern Recognition, Citeseer, 2010, pp. 3360–3367.

[43] S. Lazebnik, C. Schmid, J. Ponce, Beyond bags of features: Spatial pyramid matching for recognizing natural scene categories, in: Computer Vision and Pattern Recognition, 2006 IEEE Computer Society Conference on, Vol. 2, IEEE, 2006, pp. 2169–2178.

[44] R.L. Rivest, A. Shamir, L. Adleman, A method for obtaining digital signatures and public-key cryptosystems, Commun. ACM 21 (2) (1978) 120–126.

[45] C.-P. Lee, C.-J. Lin, A study on L2-loss (squared hinge-loss) multiclass SVM, Neural Comput. 25 (5) (2013) 1302–1323.

[46] CASIA face image databases service team, 2009, CAS Institute of Automation, http://biometrics.idealtest.org/.

[47] P.J. Phillips, H. Wechsler, J. Huang, P.J. Rauss, The FERET database and evaluation procedure for face-recognition algorithms, Image Vis. Comput. 16 (5) (1998) 295–306.

[48] H. Huang, H. He, Super-resolution method for face recognition using nonlinear mappings on coherent features, NNs, IEEE Trans. 22 (1) (2011) 121–130.

[49] Q. Feng, C. Yuan, J.-S. Pan, J.-F. Yang, Y.-T. Chou, Y. Zhou, W. Li, Superimposed sparse parameter classifiers for face recognition, IEEE Trans. Cybern. 47 (2) (2017) 378–390, http://dx.doi.org/10.1109/TCYB.2016.2516239.

[50] M. Yang, L. Zhang, S.C.-K. Shiu, D. Zhang, Robust kernel representation with statistical local features for face recognition, IEEE Trans. Neural Netw. Learn. Syst. 24 (6) (2013) 900–912.

[51] S. Umer, B.C. Dhara, B. Chanda, Biometric recognition system for challenging faces, in: 2015 Fifth National Conference on Computer Vision, Pattern Recognition, Image Processing and Graphics, NCVPRIPG, IEEE, 2015, pp. 1–4.

[52] J. Yin, L. Wei, M. Song, W. Zeng, Optimized projection for collaborative representation based classification and its applications to face recognition, Pattern Recognit. Lett. 73 (2016) 83–90.

[53] N.K. Benamara, M. Keche, M. Wellington, Z. Munyaradzi, Securing E-payment systems by RFID and deep facial biometry, in: 2021 1st International Conference on Artificial Intelligence and Data Analytics, CAIDA, IEEE, 2021, pp. 151–157.

[54] Z. Lu, X. Liang, G. Yang, D. Liu, Small-scale convolutional neural networks with learnable gabor filter for image classifications, in: 2021 4th International Conference on Information Communication and Signal Processing, ICICSP, IEEE, 2021, pp. 425–431.

[55] X. Liu, F. Shen, J. Zhao, C. Nie, RSTAM: An effective black-box impersonation attack on face recognition using a mobile and compact printer, 2022, arXiv preprint arXiv:2206.12590.

[56] G. Sun, H. Hu, Y. Su, Q. Liu, X. Lu, ApaNet: Adversarial perturbations alleviation network for face verification, Multimedia Tools Appl. 82 (5) (2023) 7443–7461.

[57] X. Qi, C. Wu, Y. Shi, H. Qi, K. Duan, X. Wang, et al., A convolutional neural network face recognition method based on BiLSTM and attention mechanism, Comput. Intell. Neurosci. 2023 (2023).

[58] B.P.U. Ivy, P. Mandiwa, M. Kumar, A modified RSA cryptosystem based on 'n'prime numbers, Int. J. Eng. Comput. Sci. 1 (2) (2012) 63–66.

[59] M. Thangavel, P. Varalakshmi, M. Murrali, K. Nithya, An enhanced and secured RSA key generation scheme (ESRKGS), J. Inf. Secur. Appl. 20 (2015) 3–10.