A Secure Face Recognition for IoT-Enabled Healthcare System

ALAMGIR SARDAR, Department of Computer Science & Engineering, Aliah University, India
SAIYED UMER, Department of Computer Science & Engineering, Aliah University, India
RANJEET KR. ROUT, Department of Computer Science & Engineering, National Institute of Technology, India
SHUI-HUA WANG, School of Mathematics and Computer Science, University of Leicester, UK
M. TANVEER*, Department of Mathematics, Indian Institute of Technology Indore, India

In Healthcare, the Internet of Things (IoT) enabled surveillance cameras capture thousands of images every day, where face recognition provides reliable security as well as smart treatment through patient sentiment analysis, emotion detection, automated nurse calls, and hospital traffic systems. In this paper, a secure face recognition system for the IoT-enabled Healthcare system has been proposed. Here each registered person will be identified by his/her face biometric with strong template protection schemes. To protect the biometric information, three steps template protection techniques have been proposed: (i) *Cancelable biometrics*, (ii) *BioCrypto-Circuit*, and (iii) *BioCrypto-Protection* schemes. The performance of the proposed system has been tested on four benchmark face databases CVL, IITK, Casia-Face-v5, and FERET. The results of the proposed system are reported in terms of the correct recognition rate and the equal error rate. These performances have also been compared with some state-of-the-art methods with respect to each employed database, which shows the novelty of the proposed system.

Additional Key Words and Phrases: Internet of Things, Healthcare, Face Recognition, Cancelable Biometrics, BioCryptosystem

1 INTRODUCTION

In the past few years, a new revolutionary technology called the Internet of Things (IoT) [10, 37] has been revolutionizing modern security systems. The advanced analytics and automation system deals with sensors, electronic devices, and software to capture and transfer data through the internet without human intervention. Smart devices are connected through wireless networks powered by advanced analytics and automation systems to improve facilities and securities in various sectors such as healthcare, business organization, transportation, retail, military, etc. IoT brings a revolution in the healthcare sector by enhancing automated patient monitoring and nurse call systems. Several smart devices, such as thermometers, electrocardiograms, pulse oximeters, and sphygmomanometers, measure patient data and send those to a patient monitoring system for analysis, which forecasts the patient's condition and alerts nurses or doctors to administer appropriate treatments. In this work, a biometric recognition system has been proposed with the advancements of IoT-enabled medical sensors for remotely monitoring patients [35]. Since billions of devices and services are connected through the internet that threatens the wireless IoT network. So, there is a need for efficient security and privacy protocols to ensure access

*Corresponding author

Authors' addresses: Alamgir Sardar, Department of Computer Science & Engineering, Aliah University, Kolkata, India, alamgir.india@gmail.com; Saiyed Umer, Department of Computer Science & Engineering, Aliah University, Kolkata, India, saiyedumer@gmail.com; Ranjeet Kr. Rout, Department of Computer Science & Engineering, National Institute of Technology, Srinagar, India, ranjeetkumarrout@nitsri.net; Shui-Hua Wang, School of Mathematics and Computer Science, University of Leicester, LE1 7RH, UK, shuihuawang@ieee.org; M. Tanveer, Department of Mathematics, Indian Institute of Technology Indore, Indore, M.P., India, mtanveer@iiti.ac.in.

Permission to make digital or hard copies of all or part of this work for personal or classroom use is granted without fee provided that copies are not made or distributed for profit or commercial advantage and that copies bear this notice and the full citation on the first page. Copyrights for components of this work owned by others than ACM must be honored. Abstracting with credit is permitted. To copy otherwise, or republish, to post on servers or to redistribute to lists, requires prior specific permission and/or a fee. Request permissions from permissions@acm.org.
© 2022 Association for Computing Machinery.
1550-4859/2022/5-ART $15.00
https://doi.org/10.1145/3534122

Just Accepted

control, authentication, confidentiality, and integrity, among others, in the IoT. Some examples of the security issues [21] of IoT based systems are: Botnet attacks, Brute force attack, hardware issues, hacking IoT Devices, home Invasions, insecure data storage issues, insecure data transmission issues, insecure interfaces, insufficient privacy protection, insufficient testing and updating, IoT malware and ransomware, IoT security risks, password issues, poor IoT device management, poor knowledge and awareness about the functionality of IoT, remote vehicle access, untrustworthy communication. The proposed system ensures all the mentioned software attacks, network attacks like channel attacks, and database attacks. The major issues are shown in Fig. 1.

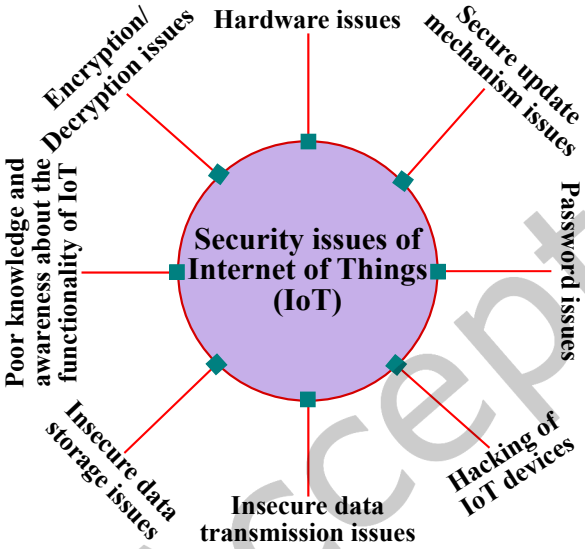


Fig. 1. Attacks on IoT-based recognition system.

As an emerging and reliable technology, the biometric system is widely used in access control, surveillance, forensics, border immigration control, emotion, sentiment, and behaviour analysis systems. However, there are some security and privacy concerns that make it challenging to protect biometric information from intruders or external entities from misuse. There are three possible solutions to protect biometrics from attack, such as (i) *template image transformation*, (ii) *cancelable biometrics/feature transformation*, and (iii) *biometric cryptosystem*. The use of cancelable biometrics [29] along with cryptosystems [20] is one of the best solutions for biometric template protection. The original biometric features are converted into another domain using a one-way function that makes it difficult to get back the original biometric features in cancelable biometrics. Another importance of cancelable biometrics is that the stored templates can be revoked if they are compromised, and then a new template can be regenerated from the same biometric. But only cancelable biometric is not secure enough since it suffers from several attacks [15]. So, to overcome the issues of cancelable biometrics, a biometric cryptosystem (i.e., BioCryptosystem) has been integrated with it. As a result, encrypted cancelable templates are stored in the database instead of original cancelable templates. In the BioCryptosystem, it is difficult for the attacker to decrypt the values and steal the original cancelable template from the database. The objectives of any BioCryptosystem are to (i) generate a key from the biometric features, (ii) encapsulate the features with the cryptographic functions, (iii) provide security at the higher levels, (iv) create computational difficulties for the intruder, and (v) overcome the difficulties of remembering long passwords. The working principle of the proposed BioCryptosystem has been shown in Fig. 2.

Just Accepted

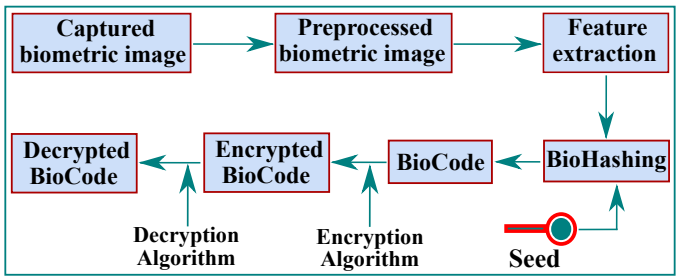


Fig. 2. Basic principle of Bio-Cryptography.

1.1 Objectives

The primary goal of this work is to design and construct a biometric system based on facial biometrics that encapsulates both cancelable and BioCryptographic approaches. In this work, we have five main goals: (i) implement an authentication system for patient monitoring in an IoT-based healthcare framework using face biometrics, (ii) overcome challenges such as illumination, pose, expression, and resolution of captured images in an unconstrained environment, (iii) secure the original facial features, (iv) improve the security levels of cancelable features without reducing the performance of the original features, and (v) reduce time complexity over traditional cryptographic algorithms.

1.2 Contributions

To meet the above objectives, this paper provides the following contributions:

- To implement an IoT-based healthcare framework with an authentication system for patient monitoring, we have employed an efficient face recognition system for challenging images where data is stored in a highly secure way and authentication is done in a secured domain.
- A novel handcrafted feature extraction technique has been adopted to overcome the challenges such as illumination, pose, expression, and resolution of captured images in an unconstrained environment.
- To secure the original feature, the existing FaceHashing technique has been improved to generate a cancelable feature that enhances the security of facial features and protects them from external attack and misuse.
- A BioCryptosystem has been proposed for securing cancelable features and the encrypted cancelable features are kept online for authentication of subjects, whereas the original features are kept offline.
- In the proposed BioCryptosystem, two novel cryptographic algorithms have been employed which are faster than existing cryptographic algorithms.

A secure face recognition system for the IoT-enabled Healthcare system is proposed in this research. Face recognition provides reliable security and smart treatment by patient sentiment analysis, mood detection, automated nurses call, and hospital traffic systems in healthcare, where the Internet of Things (IoT) enabled surveillance cameras gather millions of images every day. Here, we have developed three-tier template protection schemes: 'cancelable biometrics', 'BioCrypto-Circuit', and 'BioCrypto-Protection' mechanisms for robustness and security to the proposed system. The proposed 'BioCrypto-Circuit' and 'BioCrypto-Protection' are referred to here as 'FaceCrypto system'.

This paper is organized as follows: Related works have been described in Section 2. Section 3 discusses the methodology of the proposed system. Experimental results and discussions have been demonstrated in Section 4. Paper is concluded in Section 5. Table 1 describes the list of symbols used in this paper.

Just Accepted

Table 1. List of used symbols

Symbol	Definition	First appears
t_s	User password/ token	Section 3.2
$\mathbb{K}$	User password based random key matrix	Section 3.3.1
$t_{\mathbb{F}}$	System assigned token	Section 3.2
$t'_{\mathbb{F}}$	System assigned token	Section 3.2
$\mathscr{C}$	Code-book/ bag-of-words	Section 3.1.2
K	Number of code-words in $\mathscr{C}$	Section 3.1.2
$\mathscr{F}$	Extracted face region	Section 3.1.1
$f_{\mathscr{F}}$	Original feature vector	Section 3.2
$\mathscr{D}$	Dimension of $f_{\mathscr{F}}$	Section 3.2
$C_{\mathscr{F}}$	Cancelable feature vector	Section 3.2
$\mathscr{T}$	Dimension of $C_{\mathscr{F}}$	Section 3.2
E_c	Encrypted feature vector of BioCrypto Circuit	Section 3.3.1
D_c	Decrypted feature vector of BioCrypto Circuit	Section 3.3.1
E_p	Encrypted feature vector of BioCrypto Protection	Section 3.3.2
D_p	Decrypted feature vector of BioCrypto Protection	Section 3.3.2

2 RELATED WORKS

This paper has studied the contributions related to face recognition and IoT-based smart systems. Patel et al. [22] proposed a face recognition system for patient identification in IoT-based healthcare systems. They have implemented a graphical user interface (GUI) for the new patient's registration using their face recognition and blood pressure, pulse rate, etc. The default parameters and the data is stored in the cloud database. Banka et al. [2] proposed an IoT based health monitoring module consisting of three sections such as health monitoring, emergency alert, and prediction of health status where patient's data is accessed using various sensors and stored in the online database, the system monitors health parameters constantly, predicts health condition then alerts family, doctor or nurses and additionally mobile apps can access status. Sam et al. [30] designed an IoT based healthcare module consisting of two sections-transmitter and a receiver where each section has three processes such as process-1: collects patient's live health details and transmit to next process, process-2: receives collected data and transform to digital form, process-3: digital data is analyzed and take immediate actions. Tacstan et al. [40] developed an android-based system to track patients' heart rate and body temperature through a wireless system that allows them to move about in the social environment. The developed system continuously monitors and tracks the patient's heart rate and body temperature. A Secure Dynamic Identity and Chaotic Maps Based User Authentication and Key Agreement Scheme for e-Healthcare Systems had been proposed by Li et al.[17]. Chen et al.[3] had built an Efficient and secure three-party mutual authentication key agreement protocol system for WSNs in IoT environments. Towards secure authenticating of cache in the reader for RFID-based IoT systems had been proposed in [16].

Qin et al. [26] proposed a hybrid method by combining linear discriminant analysis and Gabor wavelets for face recognition. Xi et al. [46] proposed a deep learning-based framework for face recognition using Local Binary Pattern Network. Napoleon and Alfalou [19] proposed a pose invariant face recognition system using an optimized 3D model to reconstruct faces from a single image with its different poses. Umer et al. [43] proposed the face recognition system for both frontal and profile faces that requires fewer computer configurations. Sardar et al. [31] proposed the FaceHashing technique to generate cancelable features followed by Bio-Cryptographic algorithm as a template protection scheme.

Masud et al. [18] proposed an automated face recognition system using a deep learning model in an IoT-cloud environment. Pawar et al. [23] had built the face recognition system in an IoT environment for smart home security.

Just Accepted

Ge et al. [7] had been designed an automated security analysis framework of IoT for the three scenarios such as environment monitoring, wearable healthcare monitoring, and the smart home. Wati et al. [45] designed a face recognition system for smart home security applications under various light angles, light intensity, distance, shirt color, and accessories. Kodali et al. [14] proposed IoT based in-hospital healthcare system. Elhoseny et al. [4] proposed IoT based healthcare system to transmit medical data securely.

Singh et al. [36] proposed an IoT-based application to fight against the COVID-19 pandemic where IoT is useful for identifying symptoms and providing better treatment for an infected patient with COVID-19. It can be helpful for patients, hospitals, physicians, surgeons. Moreover, from the recent surveys of IoT and IoT-based home security, the smart healthcare system in [10, 27, 33], and [37] we have learned various architecture, challenges, future scope, open issues, and their solutions. But, there are some serious security and privacy concerns like database and channel attacks. The existing systems are not sufficient to protect against these attacks. In this paper, we have introduced an efficient security scheme.

3 METHODOLOGY

In this work, the implementation of the proposed system has been divided into three components: (i) Face recognition, (ii) Cancelable biometrics using FaceHashing, (iii) FaceCrypto systems, and these are shown in Fig.3(a), and the block diagram of the proposed methodology has been shown in Fig.3(b). The detailed descriptions of these components are discussed in the following subsections.

3.1 Face Recognition

This component has tree sub-components.

3.1.1 Image preprocessing: The input images have various challenging issues like variations in poses, expressions, illuminations, lighting conditions, and poor-resolution artifacts that degrade the image quality. In this work, the challenges on the facial region such as frontal, profile, accessories (e.g., makeup, cap, spectacle), lighting, off-angle, rotation, motion-blurred have been considered. During face preprocessing, the face region is extracted out from a body silhouette image of each individual, and for this, a Tree Structure Part Model (TSPM) [28] has been employed. This model computes approximately 68 landmark points on frontal face (Fig.4(a)) and 39 landmark points on the challenging profile face (-45° to 45°) (Fig.4(e)). The model can also handle all the challenging issues such as at-a-distance, illuminations, rotations, poses, expressions, accessories, etc. Hence, based on the pixel position of computed landmark points by TSPM (Fig.4(b), 4(f)), we calculate four corner co-ordinates on each input image and then compute the face region $\mathscr{F}$ (Fig.4(c), 4(g)).

3.1.2 Feature Extraction: The extracted facial region (Fig.4(d), Fig.4(h)) are used for feature computation. These facial regions contain tones in regular or irregular patterns. These patterns are stated as bumpy, rough, smooth, silky, and ridged characteristics [39]. During feature computation, we analyzed these texture characteristics from the facial region to extract more discriminant and disjunctive features that overcome the problems of intra-inter class similarity or dissimilarity, poor image qualities, and open and closed set recognition problems. In this work, each preprocessed facial image has been divided into sub-regions. Then texture patterns are analyzed statistically in each sub-region. The statistical-based approaches applied to texture pattern is more convenient and practical than the structural and transformed-based approaches. Since the preprocessed face image $\mathscr{F}$ may have both regular and non-regular patterns. So, the statistical-based approaches are more suitable to analyze those patterns. Here, we have considered a small patch $w_{n\times n}$ over the face image $\mathscr{F}$ that slides horizontally and then vertically. Now, each patch $w_{n\times n}$ is normalized to a vector $u_{n^2\times 1}$ with zero mean and unit standard deviation. Then, from each $\mathscr{F}$, a collection U=$[u_1, u_2, ...u_N]$ of N normalized vectors are obtained. Then, a large set $\{U_1, U_2, ...U_M\}$ is obtained

Just Accepted

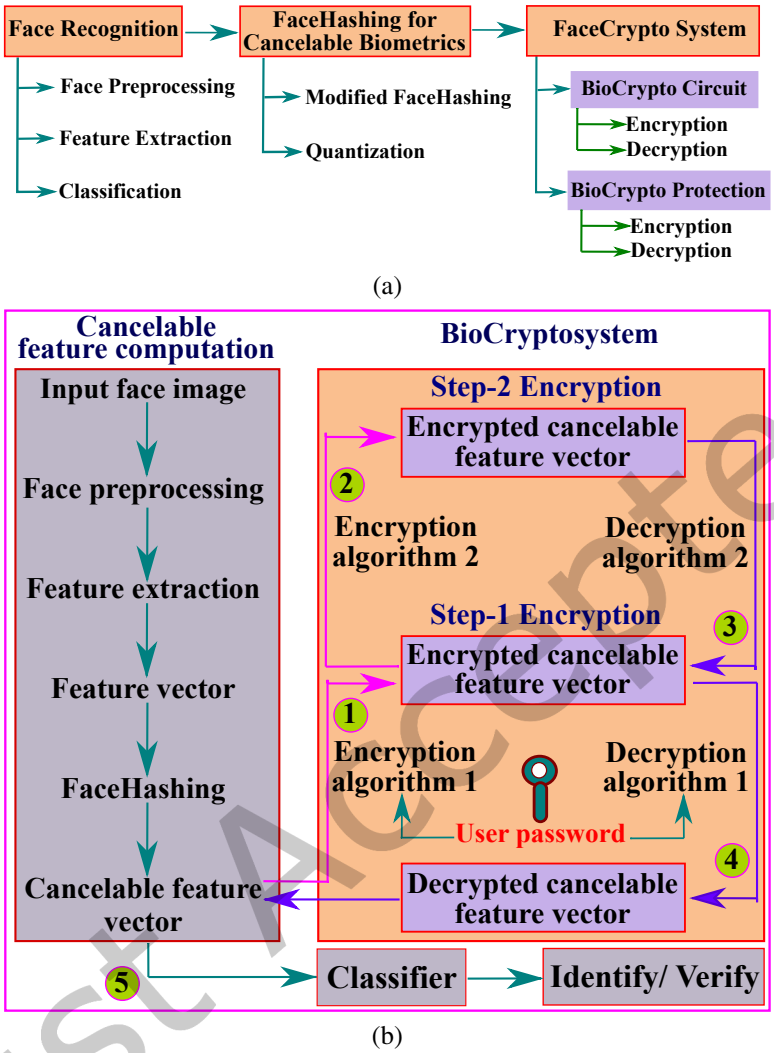


Fig. 3. (a) Components of the proposed system, (b) Block diagram of the proposed system where numeric values represents some working processes. Serial no. (1) indicates step-1 encryption of cancelable feature vector using user password, (2) indicates step-2 encryption of the encrypted feature vector, (3) & (4) indicates decryption of encrypted feature vector in reverse order, (5) indicates cancelable feature vector undergoes to classify the subjects.

Just Accepted

from M randomly chosen training samples. This large set undergoes to K-means clustering algorithm to compute a corpus $\mathscr{C} \in \mathbb{R}^{n^2 \times K}$ with K unique code-words.

For the proposed feature vector, both the corpus $\mathscr{C}$ and collection U (of u_is) from $\mathscr{F}$ have been considered. The dimension of feature vector $f_{\mathscr{F}}$ is set to K with assigning zero to all its elements. Then for each $u_i \in \mathscr{F}$, we compute the Euclidean distance d_i between u_i and every code-word of $\mathscr{C}$. Then we consider m least distances d_i (where m $\ll$ K) for feature computation. The rest (K-m) distances are assumed to be infinity and are not considered. Now the m distances of the respective cluster centers have been used to increase the count in the values of $f_{\mathscr{F}}$

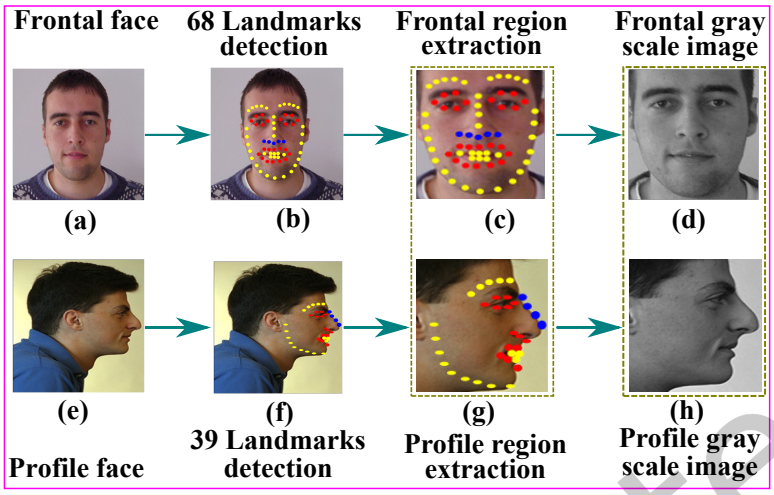


Fig. 4. The steps of face preprocessing for the proposed system.

corresponds to that indices. During feature computation, we have partitioned $\mathscr{F}$ into sub-regions to get more local information and finally, accumulate that local information to derive the global represented feature vector for $\mathscr{F}$. Steps for computing feature vector $f_{\mathscr{F}}$ are summarized in Algorithm 1. Moreover, we have also employed some deep learning-based convolution neural network models such as VGG16 [34], and ResNet50 [38] to extract features from the preprocessed face images. Here, we have used pre-trained VGG16 and ResNet50 models and then applied the transfer-learning technique followed by fine-tuning parameters. In transfer learning, a model trained on large datasets for one problem is effectively used as a generic model on other related problems. Fine-tune allows the higher-order feature representations of deep models to make them more relevant for the face recognition tasks. Hence, from VGG16, we have extracted 4096 dimensional feature vector $f_{\mathscr{F}}^{VGG}$ while from ResNet50 2048 dimensional feature vector $f_{\mathscr{F}}^{ResNet}$ have been extracted from each face image $\mathscr{F}$.

Algorithm 1: $f_{\mathscr{F}}$ for $\mathscr{F}$

Input: $\mathscr{F}, \mathscr{C}$
Output: $f_{\mathscr{F}}$
(1) For each $\mathscr{F}$
  (a) $U = \rho$, empty set
  (b) Each patch w_i slides over $\mathscr{F}$
  (c) Compute normalized vectors u_i
  (d) $U = U\#u_i$, '#' indicates concatenation of u_i to U
(2) $f_{\mathscr{F}} \in \mathbb{R}^{1\times K}$=0
(3) For each $u_i \in U$
  (a) Compute D=$\{d_1, d_2, ...d_n\}$ such that d_j=$dist\left(u_i, \mathscr{C}_j\right)$ for $1 \leq j \leq n$ where 'dist' is Euclidean distance.
  (b) Choose d_j=m^{th} smallest element of D and then modify $d_{ij} = \begin{cases} d_{ij}, & \text{if } d_{ij} < d_j \\ \infty, & \text{else} \end{cases}$
  (c) Update $f_{\mathscr{F}}$(j)=$f_{\mathscr{F}}$(j)+$exp\{-\frac{d_{ij}}{n^2}\}$, n is the patch size

Just Accepted

3.1.3 Classification: The extracted feature vectors from the above method undergo classification tasks. A multi-class linear support vector machine classifier with a 5-fold cross-validation (CV) technique has been employed for classification purposes. Both verifications, as well as identification performance, have been reported concerning each used database. The correct matching of each subject matched over the total number of subjects with their actual class belonging is the correct recognition rate (CRR). This CRR is for identification performance. For verification performance, an equal error rate (EER) [5] is evaluated based on true-positive and false-positive rates computed for the subjects enrolled in the database.

3.2 Cancelable Biometrics using FaceHashing

In this section, we have discussed the implementation of our proposed cancelable face biometrics using FaceHashing technique. It is a class of BioHashing technique [13] used to generate FaceCode. This FaceHashing is based on [31] where existing FaceHashing technique (Eq.(1)) has been modified to Eq.(2) & Eq.(3). Existing FaceHashing technique generates a bit-vector $b \in \{0,1\}$ using a user specific token whereas in the modified FaceHashing, we have employed three tokens: one user specific token 't_s' and two system specific tokens '$t_{\mathscr{F}}$' and '$t'_{\mathscr{F}}$'. Using the subject' token 't_s', the random matrix $R_0 \in \mathbb{R}^{\mathscr{D}\times\mathscr{T}}$ is generated by the random number generator. The Gram-Schmidt ortho-normalization [42] method is applied on each column of R_0 to obtain $R \in \mathbb{R}^{\mathscr{D}\times\mathscr{T}}$, where $\mathscr{T} << \mathscr{D}$. Then the original feature vector $f_{\mathscr{F}}$ is projected on each column of R to compute the inner product $f'_i =< f_{\mathscr{F}}, R_i >$ that forms an element of vector $f' = \left[f'_1, f'_2, \cdots, f'_{\mathscr{T}}\right] \in \mathbb{R}^{1\times\mathscr{T}}$. The vector '$f'$' contains real values which are further quantified by selecting a threshold 'τ' (experimentally) to get binary code $b_{\mathscr{F}} = [b_1, b_2, ...b_{\mathscr{T}}]$, $b_i \in \{0,1\}^{\mathscr{T}}$ is defined in Eq.(1).

$$f_{\mathscr{F}} \odot R \xrightarrow{t_s} f' \xrightarrow{\{0,1\}} b_{\mathscr{F}} \tag{1}$$

The generated $b_{\mathscr{F}} \in \{0,1\}^{\mathscr{T}}$ is the cancelable FaceCode used only for the verification purposes. We called this here as CFR_1 (cancelable face recognition-1) system. For identification purpose and to increase the security levels, CFR_1 is modified to some extent to build CFR_2 system. In CFR_2, the feature vector $f' \in \mathbb{R}^{1\times\mathscr{T}}$ are scaled to $g_{\mathscr{F}} \in \{0, \cdots, 255\}^{\mathscr{T}}$. Now, each element $g_{\mathscr{F}i} \in g_{\mathscr{F}}$ is converted to 8-bit column vector i.e. $g_{\mathscr{F}} \rightarrow Q'_{8\times\mathscr{T}}$, Q' be the quick response code, will be stored as template in the database. CFR_2 system is defined in Eq.(2).

$$f_{\mathscr{F}} \odot R \xrightarrow{t_s} f' \xrightarrow{\{0,255\}} g_{\mathscr{F}} \rightarrow Q' \tag{2}$$

Now to introduce more security levels and also to increase the performance, CFR_2 is extended to CFR_3 which is our proposed FaceHashing technique. CFR_3 is defined in Eq.(3).

$$f_{\mathscr{F}} \odot R \xrightarrow{t_s} f' \xrightarrow{\pi_{t_1}(f')} f'' \xrightarrow{\pi_{t_2}(f'')} C_{\mathscr{F}} \rightarrow Q'' \tag{3}$$

where $t_1 = t_s + t_{\mathbb{F}}$, $t_{\mathbb{F}}$ is the system dependent token that is common for all subjects. Here, π is the permutation function that has been applied on the elements of vector f' to get f'' using token t_1. Again the permutation function π has been applied on the elements of vector f'' with token $t_2 = t_s + t'_{\mathbb{F}}$ to generate the vector $C_{\mathscr{F}} \in \mathbb{R}^{1\times\mathscr{T}}$. The permutation function 'π' on f'' not only enhances the security level but also improves the performance in terms of recognition. Here, cancelable feature vector $C_{\mathscr{F}}$ is more discriminant than f'' and is used in online mode for both identification and verification purposes while the original face feature vector $f_{\mathscr{F}}$ will be kept offline. The predictions of f'' from $C_{\mathscr{F}}$ and f' from f'' are very difficult even if the feature vector $C_{\mathscr{F}}$ is compromised. It is due to the fact that the cancelable feature vector $C_{\mathscr{F}}$ is obtained by performing $O\left(8^{\mathscr{T}} = 2^{\mathscr{T}} \times 2^{\mathscr{T}} \times 2^{\mathscr{T}}\right)$ permutations on $f_{\mathscr{F}}$. Therefore, it is impossible to recover $f_{\mathscr{F}}$ either from f'' or from $C_{\mathscr{F}}$. Hence $C_{\mathscr{F}}$ is the cancelable template

Just Accepted

for the proposed FaceHashing technique. Now each element of $C_{\mathscr{F}} \in \mathscr{T}$ is converted into 8-bit representation such that $C_{\mathscr{F}} \rightarrow Q \in (0,1)^{8\times\mathscr{T}}$. This Q'' is a quick response code (QRC) used as template in online to perform both verification and identification of the subjects. The security checking of these cancelable templates is very important for the implementation of any biometric recognition system. There are several ways for security analysis of cancelable templates but among them, Irreversibility, Renewability, Unlinkability, and Performance preservation [44] are important and these are discussed as follows:

- *Irreversibility*: The obtained cancelable templates are non-invertible, i.e., the original biometric feature can not be obtained reversibly back even if all the tokens are known to the intruder. The original feature vector $f_{\mathscr{F}}$ can not be constructed from the cancelable templates f', f' or f''. Hence, the proposed cancelable templates have successfully held the irreversibility property of security analysis.
- *Renewability*: Cancelable Biometric (CB) templates are renewable in nature. When a stored template is compromised, a new template can be generated by assigning a new token to correspond to that subject while there is no effect on the stored non-compromised templates. Here if the stored CB template f' or f'' is compromised, a new token will be assigned to that subject, and the newly generated template will replace the compromised template.
- *Unlinkability*: The property of non-linkability has also been preserved in the CB templates. The original features $f_{\mathscr{F}}$ are kept offline, and all the stored templates are compromised, then there is no way for hampering or modifying the original features by the intruders.
- *Performance preservation*: There is no effect on the performance of the recognition system by the original features ($f_{\mathscr{F}}$) and its transformation to the CB templates (f' or f''). Both intra-class similarities and inter-class dissimilarities are maintained in original and cancelable feature domains.

3.3 FaceCrypto System

In this section, we have described the FaceCrypto system, which consists of two components: (i) BioCrypto-Circuit and (ii) BioCrypto-Protection. These techniques are discussed here as follows:

3.3.1 BioCrypto Circuit. Here we have proposed a novel XOR based encryption-decryption technique. This algorithm has been applied on each cancelable template $C_{\mathscr{F}}$ to secure the database. The working flow diagram of the proposed BioCrypto-Circuit algorithm has been shown in Fig. 5. Here, at first, the QRC $Q''_{8\times\mathscr{T}}$ from the feature vector $C_{\mathscr{F}}$ is fragmented into two vertical parts say $A_{8\times\frac{\mathscr{T}}{2}}$ and $B_{8\times\frac{\mathscr{T}}{2}}$. Now using the subject assigned token t_s, the random number generator generates a random key matrix $\mathbb{K} \in \mathbb{R}^{8\times\frac{\mathscr{T}}{2}}$, where $\mathbb{K} \in \{0,1\}$. Then these A, B and K binary matrices undergo encryption and decryption of cancelable templates stored in the database. The encryption and decryption techniques are briefly described as follows:

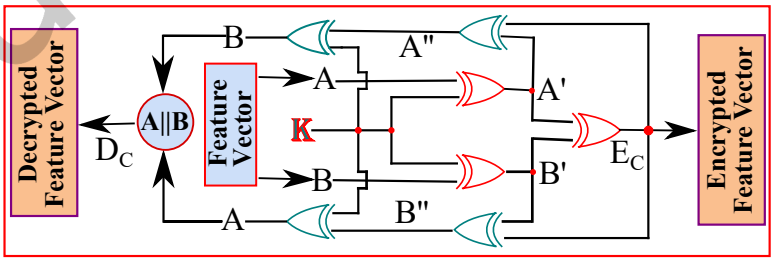


Fig. 5. Working-flow of proposed BioCrypto Circuit technique.

Just Accepted

Encryption: To encrypt QRC (Q'') from the cancelable feature vector $C_{\mathscr{F}}$, we have performed bit-wise XOR operation between each column of 'A' and '$\mathbb{K}$' matrix and then computed $A' = A \oplus \mathbb{K}$ i.e. $\left[a_1 \oplus k_1, a_2 \oplus k_2, \cdots, a_{\frac{\mathscr{I}}{2}} \oplus k_{\frac{\mathscr{I}}{2}}\right]$, $A = \left[a_1, \cdots, a_{\frac{\mathscr{I}}{2}}\right]$ and $\mathbb{K} = \left[k_1, \cdots, k_{\frac{\mathscr{I}}{2}}\right]$. Similarly, compute $B' = B \oplus \mathbb{K}$ i.e. $\left[b_1 \oplus k_1, b_2 \oplus k_2, \cdots, b_{\frac{\mathscr{I}}{2}} \oplus k_{\frac{\mathscr{I}}{2}}\right]$, $B = \left[b_1, \cdots, b_{\frac{\mathscr{I}}{2}}\right]$. Finally, XOR operation is applied between the two resulting matrices (i.e. A' and B') and then we obtain $E_c \left(= A' \oplus B'\right)$. The obtained E_c is the encrypted QRC matrix and its values lie in between 0 and 1. This E_c is stored in the database which will be used for both verification and identification purpose after applying decryption algorithm on it. Here it is impossible to recover the cancelable QRC (Q'') from the encrypted cancelable feature matrix E_c without any knowledge of $\mathbb{K}$. Mathematically, the BioCrypto-Circuit has been defined in Eq.(5) and the detailed explanation has been discussed in Algorithm 2.

Decryption: To decrypt the encrypted feature matrix E_c, we have again applied two XOR operations (i) $E_c \oplus B'$ and (ii) $E_c \oplus A'$ to get A'' and B'' respectively. Further bit-wise XOR operations are performed between A'' and $\mathbb{K}$ and between B'' and $\mathbb{K}$ to generate B and A respectively. Finally, the matrices A and B are concatenated to obtain the decrypted feature matrix D_c from the encrypted matrix E_c. Each column of D_c is transformed into its decimal representation to get C'=$C_{\mathscr{F}}$. The mathematical expression for the proposed decryption process has been shown in Eq.(4) and the detailed explanation of this decryption processes have been demonstrated in Algorithm 3.

$$A'' = E_c \oplus B', \quad B'' = E_c \oplus A', \quad A = B'' \oplus \mathbb{K}, \quad B = A'' \oplus \mathbb{K} \tag{4}$$

$$A' = A \oplus \mathbb{K}, \quad B' = B \oplus \mathbb{K}, \quad E_c = A' \oplus B' \tag{5}$$

Fig.6 shows the example of BioCrypto-Circuit encryption-decryption technique applied on an image $\mathscr{I}$.

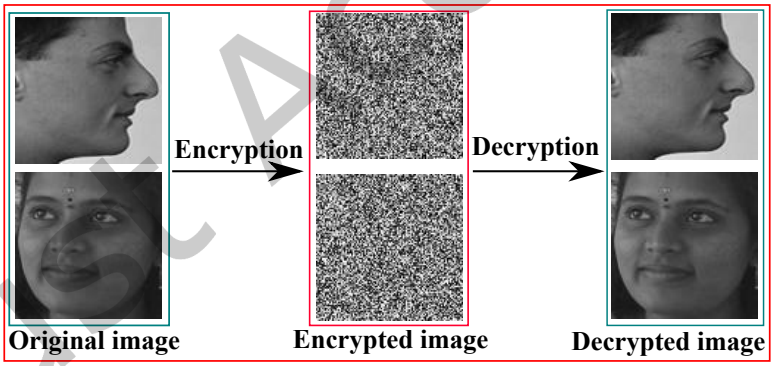


Fig. 6. Image encryption-decryption using BioCrypto Circuit.

3.3.2 BioCrypto Protection. In BioCrypto Circuit, A', B' and $\mathbb{K}$ are required to encrypt the QRC Q''. So, in order to improve security, another FaceCrypto technique called BioCrypto-Protection has been proposed in this part. The BioCrypto-Protection is the second step of the FaceCrypto system where the encrypted feature matrix E_c (using Algorithm 2) is further encrypted that provides much higher level of protection. The objectives for protecting E_c are: (i) the algorithm of BioCrypto-Circuit may be compromised/ revealed, so, the BioCrypto- Protection techniques will be used as backbone for encryption of templates, and (ii) the size of storing template will be much reduced and will create confusion to the intruder. Here, the intermediate encrypted feature matrix A' and B' from Algorithm 2

Just Accepted

Algorithm 2: BioCrypto-Circuit: Encryption

Input: Cancelable template $Q''_{\mathscr{F}} \in \mathbb{R}^{8\times\mathscr{T}}$, $\mathbb{K} \in \mathbb{R}^{8\times\frac{\mathscr{J}}{2}}$
Output: Encrypted $E_c \in (0,1)^{8\times\frac{\mathscr{J}}{2}}$ matrix

(1) Generate QRC $\left(Q''\right)$ from $C_{\mathscr{F}}$.
(2) Fragment Q'' vertically into two parts say $A\left(=[a_1, a_2, \cdots, a_{\frac{\mathscr{J}}{2}}]\right)$ and $B\left(=[b_1, b_2, \cdots, b_{\frac{\mathscr{J}}{2}}]\right)$.
(3) Consider each column (in 8 bit LEFT-MSB format, arrange bits of each digit column wise) of A, B, $\mathbb{K}$.
(4) Compute bit-wise XOR operation between A and $\mathbb{K}$ then B and $\mathbb{K}$ to get A', B' such that
(5) **for** $i \leftarrow 1$ to $\frac{\mathscr{J}}{2}$ **do**
(6) **for** $j \leftarrow 1$ to 8 **do**
(7) $A'(i,j) \leftarrow A(i,j) \oplus \mathbb{K}(i,j)$
(8) $B'(i,j) \leftarrow B(i,j) \oplus \mathbb{K}(i,j)$
(9) **end for**
(10) **end for**
(11) Compute XOR between A' and B' to get E_c.
(12) **for** $i \leftarrow 1$ to $\frac{\mathscr{J}}{2}$ **do**
(13) **for** $j \leftarrow 1$ to 8 **do**
(14) $E_c(i,j) \leftarrow A'(i,j) \oplus B'(i,j)$
(15) **end for**
(16) **end for**

Algorithm 3: BioCrypto-Circuit: Decryption

Input: Encrypted matrix E_c, $\mathbb{K}$, $A' \in (0,1)^{8\times\frac{\mathscr{J}}{2}}$, $B' \in (0,1)^{8\times\frac{\mathscr{J}}{2}}$
Output: Decrypted matrix D_c

(1) Perform bit-wise XOR operations between E_c, A' and E_c, B'
(2) **for** $i \leftarrow 1$ to $\frac{\mathscr{J}}{2}$ **do**
(3) **for** $j \leftarrow 1$ to 8 **do**
(4) $A''(i,j) \leftarrow E_c(i,j) \oplus A'(i,j)$
(5) $B''(i,j) \leftarrow E_c(i,j) \oplus B'(i,j)$
(6) **end for**
(7) **end for**
(8) Perform bit-wise XOR operation between B'' and $\mathbb{K}$ then between A'' and $\mathbb{K}$ to get A, B
(9) **for** $i \leftarrow 1$ to $\frac{\mathscr{J}}{2}$ **do**
(10) **for** $j \leftarrow 1$ to 8 **do**
(11) $A(i,j) \leftarrow B''(i,j) \oplus \mathbb{K}(i,j)$
(12) $B(i,j) \leftarrow A''(i,j) \oplus \mathbb{K}(i,j)$
(13) **end for**
(14) **end for**
(15) $D_c = A \,\|\, B$, $\|$ refers to concatenation operator

Just Accepted

are used to generate the encrypted E_c. In BioCrypto-Protection at first all the $(i,j)^{th}$ bit from the matrices (E_c), A' and B' are kept in a single matrix $\mathscr{E}$ such that each element of $\mathscr{E}$ contains the binary to decimal conversion of the bit sequence i.e. d=$2^2 \times e_{ij} + 2^1 \times a'_{ij} + 2^0 \times b'_{ij}$, e_{ij}, a'_{ij}, b'_{ij} are the bits at the $(i,j)^{th}$ position in matrix E_c, A', and B' respectively. The working principle of BioCrypto-Protection technique has been shown in Fig. 7. Here, Fig. 7(a) is the E_c matrix, 7(b) is the A' matrix, 7(c) is the B' matrix, 7(d) is the G matrix and 7(e) is the integer matrix $\mathscr{E} \in (0,\cdots,7)^{8\times\frac{\mathscr{T}}{2}}$.

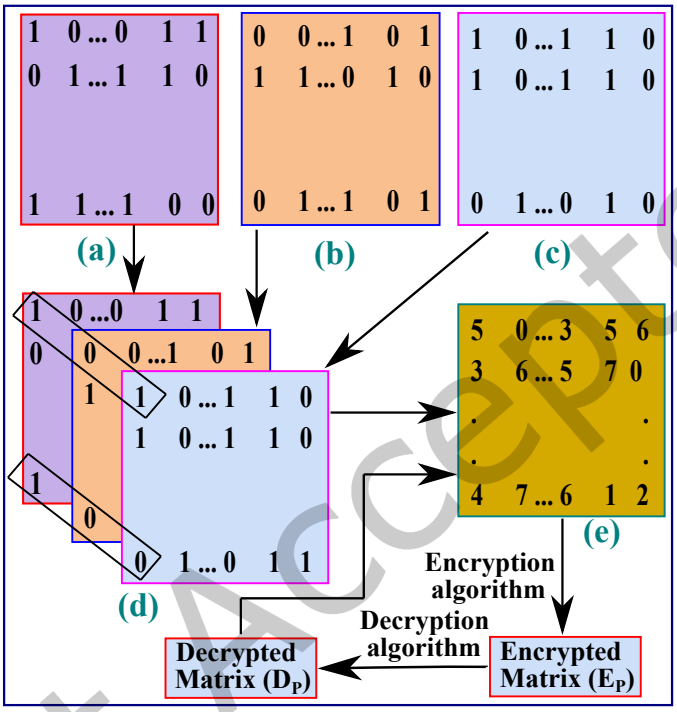


Fig. 7. Working-flow of the proposed BioCrypto Protection technique.

The encryption and decryption techniques under this scheme are discussed as follows:

Encryption: The obtained matrix $\mathscr{E}$ is further used to encrypt it into E_p. During encryption, the matrix $\mathscr{E}$ is divided into 8 arrays such that $\mathscr{E} = [\mathscr{E}_1, \mathscr{E}_2, \cdots \mathscr{E}_8]^T$, $\mathscr{E}_i \in \{0,\cdots,7\}^{1\times\frac{\mathscr{T}}{2}}$ and T stands for transpose of the matrix. Now each array $\mathscr{E}_i$ is transformed to E_i such that $E_i = \left[\Sigma_{j=1}^{\frac{\mathscr{T}}{2}}\mathscr{E}_j - \mathscr{E}_{ij}\right]_{j=1}^{\frac{\mathscr{T}}{2}}$, $\left(i = 1,2,\cdots 8\right)$ and the encrypted matrix $E_p = [E_1, E_2, \cdots E_8]^T$. The step by step process of this encryption technique has been elaborated in Algorithm 4.

Decryption: Now, the encrypted matrix E_p from the above process is decrypted such that $E_p \rightarrow D_p$, D_p is the decrypted matrix, $D_p = [D_1, D_2, \cdots D_8]^T$, where each $D_i = \left[\left(\frac{1}{(\mathscr{N})-1}\Sigma_{j=1}^{\frac{\mathscr{T}}{2}}E_j\right) - E_{ij}\right]_{j=1}^{\frac{\mathscr{T}}{2}}$ $(\mathscr{N})$=number of rows in E. The step by step of this decryption process has been demonstrated in Algorithm 5.

Fig.8 demonstrates the image encryption-decryption using BioCrypto Protection technique.

Just Accepted

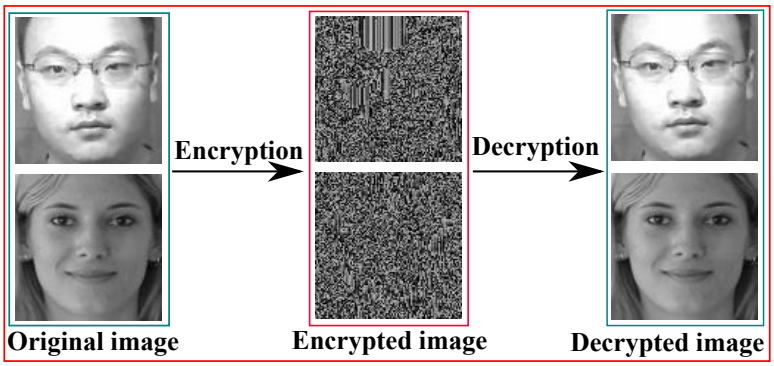


Fig. 8. Image encryption-decryption using BioCrypto Protection technique

Algorithm 4: BioCrypto Protection: Encryption

Input: Encrypted matrix E_c, intermediate encrypted matrix A' and B'

Output: Encrypted feature matrix $E_p \in (0,\cdots,7)^{8\times\frac{\mathscr{T}}{2}}$

(1) Consider $(i,j)^{th}$ bit from each of the E_c, A' and B'.
(2) **for** $i \leftarrow 1$ to $\frac{\mathscr{T}}{2}$ **do**
(3) **for** $j \leftarrow 1$ to 8 **do**
(4) $G(i,j) \leftarrow E_c(i,j) \,\|\, A'(i,j) \,\|\, B'(i,j)$
(5) **end for**
(6) **end for**
(7) Generate an integer matrix $\mathscr{E}$ from G such that each element of $\mathscr{E}$ contains the binary to decimal conversion of the bit sequence i.e. d=$2^2 \times e_{ij} + 2^1 \times a'_{ij} + 2^0 \times b'_{ij}$, e_{ij}, a'_{ij}, b'_{ij} are the bits at the $(i,j)^{th}$ position in matrix E_c, A', and B' respectively.
(8) Divide $\mathscr{E}$ into 8-equal arrays such that $\mathscr{E} = [\mathscr{E}_1, \mathscr{E}_2, \cdots \mathscr{E}_8]^T$, $\mathscr{E}_i \in \{0,\cdots,7\}^{1\times\frac{\mathscr{T}}{2}}$ and T=transpose.
(9) Transform each array $\mathscr{E}_i$ to E_i such that $E_i = \left[\Sigma_{j=1}^{\frac{\mathscr{T}}{2}} \mathscr{E}_j - \mathscr{E}_{ij}\right]_{j=1}^{\frac{\mathscr{T}}{2}}$, $\left(i = 1,2,\cdots 8\right)$
(10) Obtain the encrypted matrix $E_p = [E_1, E_2, \cdots E_8]^T$.

Therefore, the final proposed cancelable FaceCrypto system is given by Eq.(6), (7) and (8) respectively.

$$f_{\mathscr{F}} \odot R \xrightarrow{t_s} f' \xrightarrow{\pi_{t_1}(f')} f'' \xrightarrow{\pi_{t_2}(f'')} C_{\mathscr{F}} \rightarrow Q''_{8\times\mathscr{T}} \tag{6}$$

$$Q''_{8\times\mathscr{T}} \xrightarrow{Algorithm\ 2} E_c \xrightarrow{Algorithm\ 4} E_p \tag{7}$$

$$E_p \xrightarrow{Algorithm\ 4} D_p \xrightarrow{\cong} E_c \xrightarrow{Algorithm\ 3} D_c \xrightarrow{\cong} Q''_{8\times\mathscr{T}} \tag{8}$$

Just Accepted

Algorithm 5: BioCrypto Protection: Decryption

Input: Encrypted feature matrix E_p
Output: Decrypted feature matrix D_p

(1) Consider the i^{th} array E_i from E_p.
(2) Transform E_i to D_i such that $D_i = \left[\left(\frac{1}{(\mathscr{N}-1)}\Sigma_{j=1}^{\frac{\mathscr{T}}{2}} E_j\right) - E_{ij}\right]_{j=1}^{\frac{\mathscr{T}}{2}}$. ($\mathscr{N}$)=number of rows in E
(3) Keep each D_i vertically to form D_p such that $D_p = [D_1, D_2, \cdots D_8]^T$.

Just Accepted

4 EXPERIMENTS

In this section, we have discussed the experiments by analyzing the results for implementing the proposed methodology. We have performed experiments on the Windows 10 operating system, Intel Core i5 processor of 3GHz, and 8GB RAM of speed 2667 MHz with the MATLAB R2016a version.

4.1 Databases Used

During experimentation, four benchmark facial databases namely: FERET [25], IITK [12], CASIA-faceV5 [1] and CVL [24] have been employed for the proposed system. FERET database contains 994 subjects, each with five color image samples of size 256×384. The samples of this database have different profiles and pose such as half-right, half-left, profile-right, frontal with facial expressions. IITK database contains 61 subjects, each with eight color image samples of size 350×350, where the images of this database vary from frontal to profile with facial expressions. CASIA-FaceV5-Crop database contains 500 subjects, each with five color samples of variable size, intra-class variations, poses, illumination, expression, imaging distances, eyeglasses, etc. The fourth database is CVL, composed of image samples of 114 different subjects. These samples have variations in poses and non-uniform illumination. The sample images of employed databases have been shown in Fig. 9.

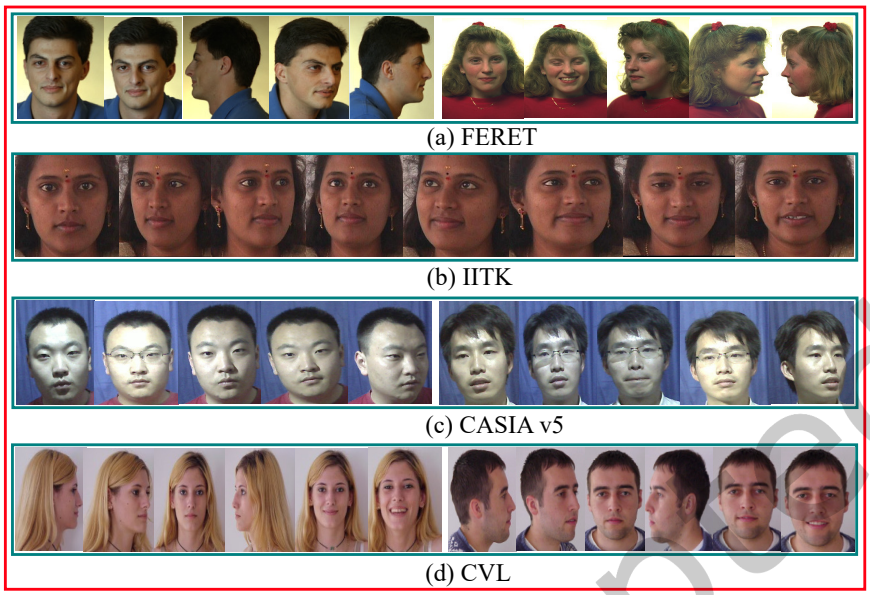


Fig. 9. Some image samples from the employed face databases.

4.2 Results and Discussions

In the face preprocessing task, a 200×200 face region ($\mathscr{F}$) has been segmented out from the input image $\mathscr{I}$. Then a patch $w \in \mathbb{R}^{n \times n}$, $n = 25$ over $\mathscr{F}$ is considered horizontally, and then vertically. Each selected patch $w \in \mathbb{R}^{n \times n}$ has been transformed to be a vector $v \in \mathbb{R}^{n^2 \times 1}$ which is further normalized to $v' \in \mathbb{R}^{n^2 \times 1}$ such that each element $v'_i \in v'$ lies in between 0 and 1. This transformation preserves the texture information due to brightness and non-uniform illumination variations in the facial region $\mathscr{F}$. A collection of these vectors v's are used to compute the feature vector $f_{\mathscr{F}}$. The dimension of the feature vector depends on the size of the corpus elements. Some $M = 200$ random training samples have been considered from FERET, IITK, CASIA-V5 and CVL databases and then from each training sample $v' \in \mathbb{R}^{n^2 \times N}$ vectors have been extracted. Then a *k-means* clustering algorithm has been applied on MN-v' vectors to derive a corpus $\mathscr{C} \in \mathbb{R}^{n^2 \times K}$ with $K = 250$ code-words. The corpus $\mathscr{C}$ and extracted vectors $v' \in \mathbb{R}^{n^2 \times N}$ from the facial region $\mathscr{F}$, are used to compute the feature vector $f \in \mathbb{R}^{1 \times \mathscr{K}}$ that corresponds to that facial image $\mathscr{F}$.

The features computed locally over $\mathscr{F}$ are then concatenated to form its local to global representation, and it gives better performance [43]. Based on these facts, in this work, we have partitioned the facial region $\mathscr{F}$ into different ways of partitioning approaches such as S_H (partitioning horizontally into two halves), S_V (partitioning vertically into two halves), and S_{HV} (partitioning into two-equal halves horizontally and then two-equal halves vertically). Based on these partitioning approaches, due to S_H on $\mathscr{F}$, $f_H \in \mathbb{R}^{1 \times 500}$, S_V, $f_V \in \mathbb{R}^{1 \times 500}$ and for S_{HV}, $f_{HV} \in \mathbb{R}^{1 \times 1000}$ feature vectors have been computed. The multi-class linear Support Vector Machine (SVM) classifier employs K-fold cross-validation techniques on the computed feature vectors. The performance of the proposed system due to these different image partitioning approaches is shown in Table 2. Here, the performance has been reported in terms of accuracy (%) by finding the correct recognition rate (CRR) over the testing samples. For dissimilarity scores, the Euclidean metric and for the similarity score, cosine metric are being used.

From the performance reported in Table 2, it has been observed that the proposed system has obtained better performance due to $f_V \in \mathbb{R}^{1 \times 500}$ feature vector for dissimilarity score measures. In support of this experiment, the

Just Accepted

Table 2. Performance in CRR (%) using different image partitioning approaches.

Database	f	f_H	f_V	f_{HV}
Feature vectors computed using dissimilarity scores				
FERET	95.48	93.12	**97.60**	94.91
IITK	94.19	93.00	**95.76**	93.65
CASIA-V5	94.67	92.32	**95.84**	93.60
CVL	92.69	92.47	**95.18**	93.94
Feature vectors computed using similarity scores				
FERET	95.84	92.77	95.38	92.59
IITK	94.59	93.13	94.77	91.63
CASIA-V5	94.23	92.72	95.22	92.52
CVL	92.28	91.25	93.66	92.57

Table 3. Performance of the proposed system in CRR (%) and EER corresponds to the ways of segments S_H, S_V, S_{HV}.

Image Partitioning Ways	50%-50%		60%-40%		70%-30%		80%-20%		90%-10%	
	FERET									
	CRR	EER	CRR	EER	CRR	EER	CRR	EER	CRR	EER
S_H	77.90	0.0528	79.86	0.0453	82.57	0.0349	82.78	0.0588	83.14	0.0701
S_V	78.98	0.0613	79.94	0.0945	82.79	0.0391	82.84	0.0724	85.36	0.0296
S_{HV}	76.50	0.0778	77.74	0.0629	81.80	0.0476	83.40	0.0535	83.56	0.0241
	IITK									
S_H	71.51	0.0781	74.24	0.0724	78.99	0.0901	80.53	0.0901	82.37	0.1102
S_V	71.92	0.0481	74.38	0.0610	81.55	0.0712	81.55	0.0831	83.19	0.0291
S_{HV}	70.59	0.0934	76.50	0.0378	81.35	0.1031	80.63	0.0734	83.19	0.0410
	CASIA-V5									
S_H	72.12	0.2771	78.78	0.2016	80.62	0.1825	82.33	0.2107	83.13	0.1562
S_V	74.62	0.2918	79.17	0.2761	81.63	0.1910	84.33	0.2099	87.79	0.1019
S_{HV}	73.93	0.2045	79.09	0.2451	80.36	0.2061	83.09	0.1734	86.78	0.2104
	CVL									
S_H	51.52	0.1849	59.77	0.1409	64.37	0.1930	70.15	0.1034	80.34	0.0523
S_V	54.78	0.1392	62.94	0.0920	70.29	0.0891	74.84	0.0912	86.27	0.0092
S_{HV}	52.89	0.1421	62.56	0.1034	68.34	0.1945	71.56	0.0451	81.56	0.0342

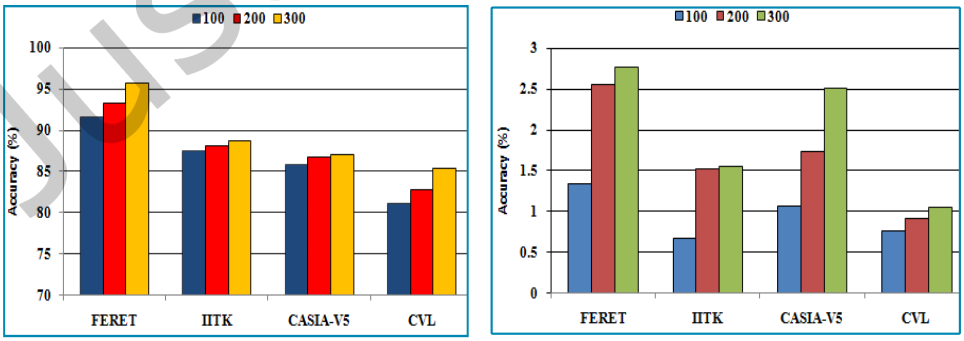
Just Accepted

performance of the proposed system has also been obtained due to the different training-testing protocols with different ways of image partitioning approaches. These performances have been reported in Table 3 where both identification in CRR (%) and verification in EER have been shown. From this table, it has also been observed that the proposed system has obtained better performance for $f_V \in \mathbb{R}^{1\times 500}$ feature vector. Hence, for further experimentation, we have adopted $f_{\mathscr{F}} = f_V \in \mathbb{R}^{1\times 500}$ feature vector for the proposed face recognition system. In this work, we have compared the performance of the proposed system with some existing state-of-the-art methods. These comparisons have been demonstrated in Table 4 with respect to both identification (CRR (%)) and verification (EER) modes. From Table 4 it has been observed that the proposed system has obtained better performance, and it outperforms other competing methods with respect to each database.

Table 4. Performance comparison of the existing and proposed system for FERET, IITK, CASIA-V5 and CVL database.

Method	(Tr-Ts)	CRR(%)	EER	Method	(Tr-Ts)	CRR(%)	EER
FERET				CVL			
VGG16 [34]	(90%-10%)	63.19	0.3191	VGG16 [34]	(90%-10%)	29.79	0.3719
ResNet50 [38]	(90%-10%)	71.73	0.0938	ResNet50 [38]	(90%-10%)	31.67	0.3218
Yin [48]	(90%-10%)	69.50	0.2183	Gou [9]	(90%-10%)	41.64	0.2112
Huang [11]	(90%-10%)	84.40	0.0081	Goel [8]	(90%-10%)	50.60	0.1961
Yang [47]	(90%-10%)	86.02	0.0177	Umer [41]	(90%-10%)	56.36	0.1034
Sardar [31]	(90%-10%)	86.27	0.0092	Sardar [31]	(90%-10%)	57.79	0.1002
Proposed	(90%-10%)	**87.18**	0.0241	**Proposed**	(90%-10%)	**70.15**	0.0451
IITK				CASIA-V5			
VGG16 [34]	(50%-50%)	43.78	0.5031	VGG16 [34]	(40%-60%)	32.81	0.2991
ResNet50 [38]	(50%-50%)	56.98	0.3215	ResNet50 [38]	(40%-60%)	37.75	0.1215
Sarode [32]	(50%-50%)	62.18	0.1034	Feng [6]	(40%-60%)	36.47	0.1981
Umer [41]	(50%-50%)	68.85	0.1004	Umer [41]	(40%-60%)	58.60	0.1201
Sardar [31]	(50%-50%)	71.92	0.0761	Sardar [31]	(40%-60%)	74.18	0.0421
Proposed	(50%-50%)	**72.38**	0.0063	**Proposed**	(40%-60%)	**74.21**	0.0397

Now for the proposed FaceHashing system, we have employed $f_{\mathscr{F}} = f_V \in \mathbb{R}^{1\times 500}$ feature vector for computing cancelable feature vector $C_{\mathscr{F}}$. Here, the implementation of the proposed FaceHashing has been divided into three steps: CFR_1 (Eq.(1)), CFR_2 (Eq.(2)) and CFR_3 (Eq.(3)), respectively. In CFR_1, the original feature vector $f_{\mathscr{F}} \in \mathbb{R}^{1\times 500}$ has been projected on the columns of $R \in \mathbb{R}^{500\times m}$ to generate $f'_{\mathscr{F}} \in \mathbb{R}^{1\times m}$ which is further quantized into $b_{\mathscr{F}} \in \{0,1\}^{1\times m}$ which is a FaceCode used mostly for the verification purpose. This CFR_1 technique has been used in several existing cancelable biometric systems where a subject gets authenticated by using his/her biometric feature vectors with his/her assigned token. To build this system also for identification purpose, the CFR_1 (Eq.(1)) has been modified to CFR_2 (Eq.(2)) where the element of generated FaceCode $g_{\mathscr{F}} \in S$ in between 0 and 255). During experimentation, the different dimensions of cancelable features $b_{\mathscr{F}} \in \{0,1\}^{1\times m}$ and $g_{\mathscr{F}} \in \{0,1\}^{1\times m}$, $m = \{100, 200, 300\}$ have been extracted for both CFR_1 and CFR_2, respectively. The performance of these Facecode for CFR_1 and CFR_2 have been demonstrated in Fig.10 and Fig.11, respectively.

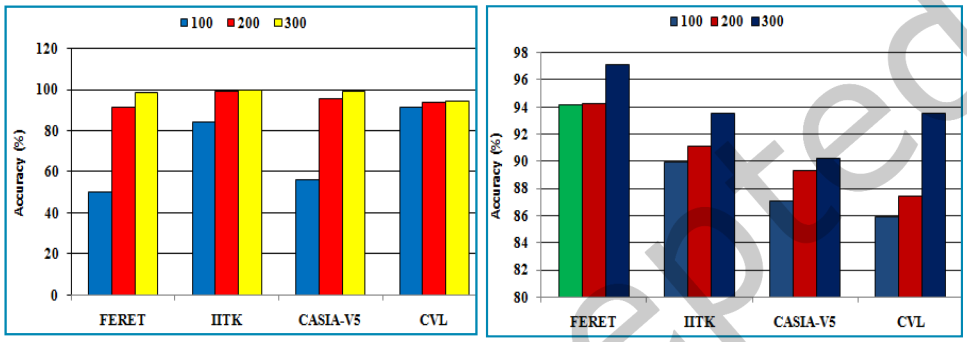


(a) Verification **(b) Identification**

Fig. 10. (a) Verification and (b) Identification performance of CFR_1 for the proposed cancelable face recognition system.

Just Accepted

From Fig.10 and Fig.11, it has been observed that, the cancelable face recognition system CFR_1 has very inferior performance than CFR_2 with respect to all databases for the identification purposes. So, the objectives of CFR_2 experimentation are to: (i) obtain identification performance for the proposed system, (ii) assess the effectiveness of the employed quantization $S \in \{0, \cdots, (2^8 - 1)\}$ in the proposed system. Moreover, the cancelable face recognition system CFR_2 has two levels of securities such that in the first level, the original facial features $f_{\mathscr{F}} = f_V \in \mathbb{R}^{1\times 500}$ have been transformed with reduced dimension to the cancelable domain $f'_{\mathscr{F}} = f_V \in \mathbb{R}^{1\times 100}$ while in the second level, the elements of $f'_{\mathscr{F}} = f_V \in \mathbb{R}^{1\times 100}$ are quantized in $S \in \{0, \cdots, (2^8 - 1)\}$ to produce $g_{\mathscr{F}} = f_V \in \mathbb{R}^{1\times 100}$. The transformation of original features in the cancelable domain is irreversible transformation i.e. it is impossible to get $f_{\mathscr{F}}$ from $f'_{\mathscr{F}}$ and also $f'_{\mathscr{F}}$ from $g_{\mathscr{F}}$.



(a) Verification **(b) Identification**

Fig. 11. (a) Verification and (b) Identification performance of CFR_2 for the proposed cancelable face recognition system.

We have also compared the performance of the proposed CFR_2 with the other cancelable features obtained by applying Eq.(2) on the competing methods described in Table 4 respect to each database. Here Eq.(2) is applied on the extracted feature vectors corresponding to each method, and then the obtained cancelable templates undergo comparisons which are reported in Table 5. This table shows that the proposed cancelable CFR_2 has an outstanding performance than the cancelable system of other competing methods.

Hence, the CFR_2 system is more secure and effective for preserving biometric information from external attacks and misuse. In the CFR_2 system, if the cancelable templates compromise, then that subject will be assigned a new token, and the existing cancelable feature vector will be replaced by a new one. Hence, FaceHashing using CFR_2 is very effective for the proposed recognition system. In the further implementation of FaceHashing technique, we have extended CFR_2 (Eq.(2)) to CFR_3 (Eq.(3)), where $f'_{\mathscr{F}}$ from Eq.(2) has been again randomly permuted by another token t_2 (π_{t_2}) to generate $f''_{\mathscr{F}}$. Here, the elements of $f''_{\mathscr{F}}$ are scaled in S to obtain the proposed cancelable feature vector $C_{\mathscr{F}}$. This cancelable feature vector $C_{\mathscr{F}}$ has three levels of securities that are eligible to handle several external attacks and misuse while preserving the biometric information from being compromised and stolen. Hence, the CFR_3 system provides both: (i) a higher level of security and (ii) outstanding performance with a small dimensional of cancelable feature vectors. Both verification and identification performance of CFR_3 system are shown in Table 6. This table shows that the proposed CFR_3 gives nearly 100% verification and identification performance using 20-dimensional cancelable feature vectors.

In CFR_3 the prediction of f' from f'' and f from f' are very difficult even if $C_{\mathscr{F}}$ is compromised. Now, to protect Q'' of $C_{\mathscr{F}}$ from modification, deletion, and interception attack by the intruder, the encryption-decryption algorithms have been applied in two steps. In the first step of encryption, the Q'' has been fragmented vertically into two equal parts $Q'' = (A, B)$. Then bit-wise XOR operation is performed on user password-based random matrix and each

Just Accepted

Table 5. Performance comparison of CFR_2 with the existing cancelable biometric system, the first row shows identification performance (in CRR (%)) and second row shows verification (in EER).

FERET				IITK			
Methods	100 *dim*	200 *dim*	300 *dim*	Methods	100 *dim*	200 *dim*	300 *dim*
VGG16 [34]	67.35 0.3190	69.75 0.2108	72.89 0.1912	VGG16 [34]	45.91 0.3721	49.95 0.3219	52.67 0.3102
ResNet50 [38]	74.56 0.1067	77.18 0.1009	79.05 0.1003	ResNet50 [38]	58.85 0.2618	61.78 0.2108	65.45 0.2107
Yin [48]	71.19 0.1178	71.67 0.1179	73.33 0.1018	Yin [48]	48.91 0.3219	52.55 0.2176	56.09 0.2311
Huang [11]	88.34 0.0934	89.19 0.0911	91.10 0.0634	Sarode [32]	65.51 0.1928	68.09 0.1910	69.17 0.1821
Yang [47]	89.05 0.0805	91.33 0.0310	92.19 0.0791	Umer [41]	71.91 0.1823	76.65 0.1171	79.91 0.1008
Sardar [31]	87.56 0.0819	89.15 0.0721	92.05 0.0619	Sardar [31]	81.89 0.1034	83.56 0.0934	87.05 0.0901
Proposed	93.79 0.0734	94.23 0.0661	97.45 0.0419	**Proposed**	90.19 0.1017	91.71 0.0877	93.89 0.0533
CASIA-V5				CVL			
Methods	100 *dim*	200 *dim*	300 *dim*	Methods	100 *dim*	200 *dim*	300 *dim*
VGG16 [34]	41.67 0.3810	45.78 0.3210	53.34 0.2971	VGG16 [34]	38.19 0.4803	39.56 0.4210	42.90 0.3978
ResNet50 [38]	48.91 0.3171	53.87 0.2918	61.78 0.2108	ResNet50 [38]	37.90 0.4107	42.61 0.3910	46.91 0.2981
Feng [6]	42.78 0.4019	49.91 0.2889	54.67 0.2010	Goel [8]	55.08 0.2716	59.78 0.2431	61.89 0.2719
Umer [41]	61.90 0.2516	67.45 0.1791	72.78 0.1643	Umer [41]	59.15 0.2321	63.34 0.2190	68.41 0.2056
Sardar [31]	84.89 0.1171	89.79 0.1083	92.17 0.0926	Sardar [31]	62.65 0.1934	68.08 0.1872	72.89 0.1834
Proposed	86.13 0.1091	89.41 0.1017	91.56 0.0832	**Proposed**	85.05 0.1287	87.17 0.0981	93.55 0.0811

Table 6. Performance of the proposed CFR_3 in CRR (%) and EER, *dim* stands for dimensional of the feature vector.

Database	10 *dim*		20 *dim*		30 *dim*	
	CRR	EER	CRR	EER	CRR	EER
FERET	98.09	0.0031	100	0.0000	100	0.00000
IITK	100	0.0000	100	0.0000	100	0.00000
CASIA-V5	95.40	0.0062	100	0.0000	100	0.00000
CVL	99.09	0.0010	100	0.0000	100	0.00000

segment of the feature vectors individually (Algorithm 2). Then we obtained two intermediate encrypted matrices A' and B'. After that, a bit-wise XOR operation has been performed to generate the encrypted cancelable feature

Just Accepted

vector E_c of step-1 (BioCrypto Circuit). E_c is encrypted to E_p using BioCrypto-Protection. This E_p is stored into a chip or hard drive and is kept online as the reference template of the particular subject in the database as a Quick Response Code (QRC). This QRC will be used as a future reference to authenticate or to recognize each individual by applying the decryption algorithm to get D_p from E_p followed by the decryption algorithm of BioCrypto-Circuit to get back $D_c\,(= C_{\mathscr{F}})$ from D_p, respectively.

Table 2 illustrates the performance of the face recognition system based on the original feature vectors computed using dissimilarity and similarity scores, respectively. In Table 3, we show the performance of the proposed method in CRR (%) and EER for images partitioned into S_H, S_V and S_{HV} with different percentages of training-testing image samples. Table 4 shows the performance comparison of exiting state-of-the-art methods and the proposed method for FERET, CVL, IITK and CASIA-V5 databases. Table 5 compares CFR_2 with the existing cancelable biometric system where the first row shows identification performance (in CRR (%)) and the second row shows verification performance (in EER). The table 6 shows the performance of the proposed CFR_3 in CRR (%) and EER for 10, 20 and 30 dimensional feature vector.

4.3 Security analysis of the proposed system

The proposed system provides template security in three steps:

(1) *Feature transformation:* A one-way transformation function is used to transform face features into the distorted format. These transformed features are free from cross-matching across databases, and in case of a compromise of a template, a new one can be generated by changing the password for the user. Hence, irreversibility, unlinkability, and renewability properties hold in the proposed FaceHashing technique.
(2) *BioCrypto-Circuit:* To protect the template database from insertion, deletion, modification, and channel attack we have employed the BioCrypto-Circuit algorithm which works along with user passwords.
(3) *BioCrypto-Protection:* Furthermore, to provide higher-level security we have employed the BioCrypto-Protection algorithm that is independent of the user password. Finally, encrypted feature vectors are stored in the database.

To generate cancelable feature vector $C_{\mathscr{F}}$ from the original feature vector $f_{\mathscr{F}}$ we need $O\left(2^{\mathscr{T}} \times 2^{\mathscr{T}} \times 2^{\mathscr{T}}\right) = O\left(8^{\mathscr{T}}\right)$ computations. Then encryption of $C_{\mathscr{F}}$ by both BioCrypto-Circuit and BioCrypto-Protection requires $O(n^2)$ computations. Hence it is almost impossible to retrieve the original feature vector from the cancelable feature vector $C_{\mathscr{F}}$. The proposed BioCryptosystem is novel in that it combines two heterogeneous encryption algorithms; no traditional replacement policy is used, so algorithms are immune to dictionary attacks; the first encryption is password dependent, while the second is password independent; and the nature of encryption is completely different for the two algorithms, so traditional brute-force attacks are impossible; encryption is not keyspace dependent; both the encryption has time complexity $O\left(n^2\right)$; moreover, the BioCryptosystem is based on computational complexity instead of time complexity. Therefore, combining the advantages of both cancelable biometrics and BioCryptosystem, the proposed system's security is too high.

5 CONCLUSION

This paper presents an efficient biometric template protection scheme for the IoT-based healthcare framework. Patients can be recognised more accurately with the proposed system while their biometric data is protected from external attacks and misuse. Furthermore, this system contributes to creating a smart healthcare system that constantly receives information from patients through hand-held devices and notifies the practitioners accordingly. Introducing the BioCryptosystem scheme with FaceHashing has increased the security levels and made the system more robust and challenging. For the BioCryptosystem, we have employed two different techniques: *BioCrypto-Circuit* and *BioCrypto-Protection*. Finally, the proposed system was tested on four benchmark databases: FERET, IITK, CASIA-FaceV5, and CVL. Its performance compared to other state-of-the-art methods concerning these

Just Accepted

databases, showing it to be superior. The novelties of this work are: (i) security issues of cancelable biometrics systems are resolved by integrating BioCryptosystem with it; (ii) two heterogeneous algorithms are employed in the proposed BioCryptosystem, which is based on computational complexity; and (iii) time complexity is too less for the employed BioCryptosystem.

According to our investigation, this paper has a few research gaps. The issue of image occlusion is the most challenging in the current (COVID-19) situation, and it is not handled in this work. We sacrificed time complexity to boost security because three-level FaceHashing followed by the BioCryptographic algorithm takes slightly longer than existing single-level FaceHashing solutions.

REFERENCES

[1] 2009. CASIA face Image Databases Service Team. *CAS Institute of Automation, http://biometrics.idealtest.org/* (2009).

[2] Shubham Banka, Isha Madan, and SS Saranya. 2018. Smart healthcare monitoring using IoT. *International Journal of Applied Engineering Research* 13, 15 (2018), 11984–11989.

[3] Chi-Tung Chen, Cheng-Chi Lee, and Iuon-Chang Lin. 2020. Correction: Efficient and secure three-party mutual authentication key agreement protocol for WSNs in IoT environments. *Plos one* 15, 6 (2020), e0234631.

[4] Mohamed Elhoseny, Gustavo Ramírez-González, Osama M Abu-Elnasr, Shihab A Shawkat, N Arunkumar, and Ahmed Farouk. 2018. Secure medical data transmission model for IoT-based healthcare systems. *Ieee Access* 6 (2018), 20596–20608.

[5] Tom Fawcett. 2006. An introduction to ROC analysis. *Pattern recognition letters* 27, 8 (2006), 861–874.

[6] Qingxiang Feng, Chun Yuan, Jeng-Shyang Pan, Jar-Ferr Yang, Yang-Ting Chou, Yicong Zhou, and Weifeng Li. 2016. Superimposed Sparse Parameter Classifiers for Face Recognition. (2016).

[7] Mengmeng Ge, Jin B Hong, Walter Guttmann, and Dong Seong Kim. 2017. A framework for automating security analysis of the internet of things. *Journal of Network and Computer Applications* 83 (2017), 12–27.

[8] Navin Goel, George Bebis, and Ara Nefian. 2005. Face recognition experiments with random projection. In *Defense and Security*. ISOP, 426–437.

[9] Gaopeng Gou, Di Huang, and Yunhong Wang. 2012. A hybrid local feature for face recognition. In *Pacific Rim International Conference on Artificial Intelligence*. Springer, 64–75.

[10] Vikas Hassija, Vinay Chamola, Vikas Saxena, Divyansh Jain, Pranav Goyal, and Biplab Sikdar. 2019. A survey on IoT security: application areas, security threats, and solution architectures. *IEEE Access* 7 (2019), 82721–82743.

[11] Hua Huang and Huiting He. 2011. Super-resolution method for face recognition using nonlinear mappings on coherent features. *NNs, IEEE Transactions on* 22, 1 (2011), 121–130.

[12] Vidit Jain and Amitabha Mukherjee. 2002. The Indian face database. *URL http://vis-www.cs.umass.edu/vidit/IndianFaceDatabase/* (2002).

[13] Andrew Teoh Beng Jin, David Ngo Chek Ling, and Alwyn Goh. 2004. Biohashing: two factor authentication featuring fingerprint data and tokenised random number. *Pattern recognition* 37, 11 (2004), 2245–2255.

[14] Ravi Kishore Kodali, Govinda Swamy, and Boppana Lakshmi. 2015. An implementation of IoT for healthcare. In *2015 IEEE Recent Advances in Intelligent Computational Systems (RAICS)*. IEEE, 411–416.

[15] Nitin Kumar and Manisha Rawat. 2020. RP-LPP: a random permutation based locality preserving projection for cancelable biometric recognition. *Multimedia Tools and Applications* 79, 3 (2020), 2363–2381.

[16] Chun-Ta Li, Cheng-Chi Lee, Chi-Yao Weng, and Chien-Ming Chen. 2018. Towards secure authenticating of cache in the reader for RFID-based IoT systems. *Peer-to-Peer Networking and Applications* 11, 1 (2018), 198–208.

[17] Chun-Ta Li, Cheng-Chi Lee, Chi-Yao Weng, and Song-Jhih Chen. 2016. A secure dynamic identity and chaotic maps based user authentication and key agreement scheme for e-healthcare systems. *Journal of medical systems* 40, 11 (2016), 1–10.

[18] Mehedi Masud, Ghulam Muhammad, Hesham Alhumyani, Sultan S Alshamrani, Omar Cheikhrouhou, Saleh Ibrahim, and M Shamim Hossain. 2020. Deep learning-based intelligent face recognition in IoT-cloud environment. *Computer Communications* 152 (2020), 215–222.

[19] Thibault Napoléon and Ayman Alfalou. 2017. Pose invariant face recognition: 3D model from single photo. *Optics and Lasers in Engineering* 89 (2017), 150–161.

[20] Devyani Panchal. 2013. *Bio-Crypto System*. Ph.D. Dissertation. Doctoral Dissertation. IIT, Kharagpur.

[21] Shivani Panchiwala and Manan Shah. 2020. A comprehensive study on critical security issues and challenges of the IoT world. *Journal of Data, Information and Management* 2, 4 (2020), 257–278.

[22] Kanubhai K Patel, Jignesh J Patoliya, and Miral M Desai. 2021. IoT based Smart Health Monitoring System with Patient Identification using Face Recognition. *Available at SSRN 3879620* (2021).

Just Accepted

[23] Suraj Pawar, Vipul Kithani, Sagar Ahuja, and Sunita Sahu. 2018. Smart home security using IoT and face recognition. In *2018 Fourth International Conference on Computing Communication Control and Automation (ICCUBEA)*. IEEE, 1–6.
[24] Peter Peer. 2005. Cvl face database. *Computer vision lab., faculty of computer and information science, University of Ljubljana, Slovenia. Available at http://www. lrv. fri. uni-lj. si/facedb. html* (2005).
[25] P Jonathon Phillips, Harry Wechsler, Jeffery Huang, and Patrick J Rauss. 1998. The FERET database and evaluation procedure for face-recognition algorithms. *IVC* 16, 5 (1998), 295–306.
[26] Shu Qin, Zhengzhou Zhu, Yuhang Zou, and Xiaowei Wang. 2020. Facial expression recognition based on Gabor wavelet transform and 2-channel CNN. *International Journal of Wavelets, Multiresolution and Information Processing* 18, 02 (2020), 2050003.
[27] Ashikur Rahaman, Md Milon Islam, Md Rashedul Islam, Muhammad Sheikh Sadi, and Sheikh Nooruddin. 2019. Developing IoT Based Smart Health Monitoring Systems: A Review. *Rev. d'Intelligence Artif.* 33, 6 (2019), 435–440.
[28] Deva Ramanan and Xiangxin Zhu. 2012. Face detection, pose estimation, and landmark localization in the wild. In *Proceedings of CVPR*. Citeseer, 2879–2886.
[29] Nalini K Ratha, Sharat Chikkerur, Jonathan H Connell, and Ruud M Bolle. 2007. Generating cancelable fingerprint templates. *IEEE Tran. PAMI* 29, 4 (2007), 561–572.
[30] Dahlia Sam, S Srinidhi, VR Niveditha, S Amudha, and D Usha. 2020. Progressed iot based remote health monitoring system. *International Journal of Control and Automation* 13, 2s (2020), 268–273.
[31] Alamgir Sardar, Saiyed Umer, Chiara Pero, and Michele Nappi. 2020. A Novel Cancelable FaceHashing Technique Based on Non-Invertible Transformation With Encryption and Decryption Template. *IEEE Access* 8 (2020), 105263–105277.
[32] Jagdish P Sarode and Alwin D Anuse. 2014. A framework for face classification under pose variations. In *ICACCI*. IEEE, 1886–1891.
[33] Kinza Shafique, Bilal A Khawaja, Farah Sabir, Sameer Qazi, and Muhammad Mustaqim. 2020. Internet of things (IoT) for next-generation smart systems: A review of current challenges, future trends and prospects for emerging 5G-IoT scenarios. *Ieee Access* 8 (2020), 23022–23040.
[34] Karen Simonyan and Andrew Zisserman. 2014. Very deep convolutional networks for large-scale image recognition. *arXiv preprint arXiv:1409.1556* (2014).
[35] Debabrata Singh, Bibudhendu Pati, Chhabi Rani Panigrahi, and Shrabanee Swagatika. 2020. Security issues in iot and their countermeasures in smart city applications. *Advanced Computing and Intelligent Engineering* 1089 (2020), 301–313.
[36] Ravi Pratap Singh, Mohd Javaid, Abid Haleem, and Rajiv Suman. 2020. Internet of things (IoT) applications to fight against COVID-19 pandemic. *Diabetes & Metabolic Syndrome: Clinical Research & Reviews* 14, 4 (2020), 521–524.
[37] Maria Stoyanova, Yannis Nikoloudakis, Spyridon Panagiotakis, Evangelos Pallis, and Evangelos K Markakis. 2020. A survey on the internet of things (IoT) forensics: challenges, approaches, and open issues. *IEEE Communications Surveys & Tutorials* 22, 2 (2020), 1191–1221.
[38] Christian Szegedy, Vincent Vanhoucke, Sergey Ioffe, Jon Shlens, and Zbigniew Wojna. 2016. Rethinking the inception architecture for computer vision. In *Proceedings of the IEEE conference on computer vision and pattern recognition*. 2818–2826.
[39] Xiaoyang Tan and Bill Triggs. 2010. Enhanced local texture feature sets for face recognition under difficult lighting conditions. *IEEE TIP* 19, 6 (2010), 1635–1650.
[40] Mehmet Taştan. 2018. IoT based wearable smart health monitoring system. *Celal Bayar University Journal of Science* 14, 3 (2018), 343–350.
[41] Saiyed Umer, Bibhas Chandra Dhara, and Bhabatosh Chanda. 2015. Biometric recognition system for challenging faces. In *2015 NCVPRIPG*. IEEE, 1–4.
[42] Saiyed Umer, Bibhas Chandra Dhara, and Bhabatosh Chanda. 2017. A novel cancelable iris recognition system based on feature learning techniques. *Information Sciences* 406 (2017), 102–118.
[43] Saiyed Umer, Bibhas Chandra Dhara, and Bhabatosh Chanda. 2019. Face Recognition Using Fusion of Feature Learning Techniques. *Measurement* (2019).
[44] Hanrui Wang, Xingbo Dong, Zhe Jin, Andrew Beng Jin Teoh, and Massimo Tistarelli. 2020. Security analysis of cancellable biometrics using constrained-optimized similarity-based attack. *arXiv preprint arXiv:2006.13051* (2020).
[45] Dwi Ana Ratna Wati and Dika Abadianto. 2017. Design of face detection and recognition system for smart home security application. In *2017 2nd International conferences on Information Technology, Information Systems and Electrical Engineering (ICITISEE)*. IEEE, 342–347.
[46] Meng Xi, Liang Chen, Desanka Polajnar, and Weiyang Tong. 2016. Local binary pattern network: A deep learning approach for face recognition. In *2016 ICIP*. IEEE, 3224–3228.
[47] Meng Yang, Lei Zhang, Simon Chi-Keung Shiu, and David Zhang. 2013. Robust kernel representation with statistical local features for face recognition. *IEEE Tran. on NNLS* 24, 6 (2013), 900–912.
[48] Jun Yin, Lai Wei, Miao Song, and Weiming Zeng. 2016. Optimized projection for Collaborative Representation based Classification and its applications to face recognition. *PRL* 73 (2016), 83–90.

Just Accepted