Efficient chaotic-Baker-map-based cancelable face recognition

Article *in* Journal of Ambient Intelligence and Humanized Computing · October 2021

DOI: 10.1007/s12652-021-03398-0

CITATIONS
13

READS
354

9 authors, including:

Osama S. Faragallah
Menoufia University
246 PUBLICATIONS **4,464** CITATIONS
SEE PROFILE

Ensherah Naeem
Suez University
27 PUBLICATIONS **325** CITATIONS
SEE PROFILE

Walid El-Shafai
Menoufia University
353 PUBLICATIONS **4,196** CITATIONS
SEE PROFILE

Noha Ramadan
Menoufia University
10 PUBLICATIONS **113** CITATIONS
SEE PROFILE

Journal of Ambient Intelligence and Humanized Computing
https://doi.org/10.1007/s12652-021-03398-0

ORIGINAL RESEARCH

Efficient chaotic-Baker-map-based cancelable face recognition

Osama S. Faragallah[1] · Ensherah A. Naeem[2] · Walid El-Shafai[3,7] · Noha Ramadan[3,8] · Hossam El-din H. Ahmed[3] · Mustafa M. Abd Elnaby[4] · Ibrahim Elashry[5] · Said E. El-khamy[6] · Fathi E. Abd El-Samie[3,9]

Received: 20 September 2020 / Accepted: 13 July 2021

Abstract
Biometric recognition schemes are commonly utilized for security purposes. These schemes face two major challenges: security challenge and reliance on a particular biometric for authentication. The protection challenge comes from the use of basic biometrics in records. Therefore, if these records are compromised, the biometrics will no longer be valid. Consequently, it is necessary to preserve basic biometrics by protecting them from being used in biometric records. Cancelable biometric recognition systems rely on changing the information or biometric features to different formats, so that persons can use their specific biometric models in single or multiple systems. The mixture of chaos theory and cryptography shapes a crucial area for information security. The newest development in encryption systems is chaos-based for various distinctive attributes such as sensitivity to preliminary conditions, non-convergence, non-periodicity, and control parameters. This paper introduces a method to produce numerous encrypted biometric templates that are re-created by various convolution kernels generated from employing chaotic Baker map in different domains. Our proposed method has superior performance in treating variations in illumination, occlusion and facial expressions. It also has the added novelty of being able to perform authentication in the encrypted domain. In addition, the same approach can be applied on different databases. The chaotic map effect in different domains is evaluated on the widely-used AT&T, YALE, UFI, LFW, and FERET databases. The cancelable biometric system using the proposed Discrete Wavelet Transform (DWT) domain encryption with various keys has the best performance among all other implementations. In average, we achieved a 2% error probability, a 0.3 s authentication time, a 0.02% False Rejection Rate (FRR), a 0% False Acceptance Rate (FAR), a 0.0% Equal Error Rate (EER) and a 98.43% accuracy. Our proposed method also provides template diversity.

Keywords Biometrics · Chaotic Baker map · DWT · IWT · Face recognition · Image encryption

✉ Ensherah A. Naeem
ensherah_naeem@yahoo.com

[1] Department of Information Technology, College of Computers and Information Technology, Taif University, P.O. Box 11099, Taif 21944, Saudi Arabia

[2] Electrical Department, Faculty of Technology and Education, Suez University, Suez 43527, Egypt

[3] Department of Electronics and Electrical Communications Engineering, Faculty of Electronic Engineering, Menoufia University, Menouf 32952, Egypt

[4] Department of Electronics and Electrical Communications, Faculty of Engineering, Tanta University, Tanta, Egypt

[5] Department of Electronics and Electrical Communications, Kafrelsheikh University, Kafrelsheikh 61519, Egypt

[6] Department of Electrical Engineering, Faculty of Engineering, Alexandria University, Alexandria, Egypt

[7] Security Engineering Lab, Computer Science Department, Prince Sultan University, Riyadh 11586, Saudi Arabia

[8] Department of Electrical Engineering, Ahram Canadian University, 6th of October, Egypt

[9] Department of Information Technology, College of Computer and Information Sciences, Princess Nourah Bint Abdulrahman University, Riyadh 21974, Saudi Arabia

Published online: 06 October 2021

1 Introduction

Due to the rapid advancement of super-computer multimedia applications, biometric system technology has also been quickly established and used in our regular lives. As a result of the existence of different biometric features, it is very important to treat access problems and keep biometric privacy. The biometric technology allows verification and identification of individual characteristics in a precise, quick, and easy way to manage access to applications or systems (Vezzetti et al. 2013; Vezzetti and Marcolin 2014). Biometrics allow access to facilities that work only with personal physical characteristics (fingerprint, hand engineering, retina, iris scan, facial position) or logical characteristics (voice, gait, signature, keystroke pattern). The objective is to guarantee or measure the characteristics of the human body (Jain et al. 2004; Jegede et al. 2017; Khan et al. 2008, 2010; Rathgeb and Busch 2012). Typically, passwords are used to keep cryptographic keys confidential for an application or system. Unfortunately, most people use identical passwords on various systems, and cannot modify them to prevent the hassle of employing distinct lengthy passwords for separate applications. Consequently, if a certain password is leaked, it could lead to a violation of other systems security (Sinha and Singh 2005, 2013; Rajpoot and Jensen 2014; Enerstvedt 2017; Zheng 2017; Cheung et al. 2005).

Generally, corporations aim to preserve their features and provide methods to maintain access to these features. This policy guarantees that the appropriate user gets the right service. Over the years, conventional verification techniques, particularly Personal Identification Numbers (PINs) and passwords have been utilized. Recently, PINs and magnetic cards have been issued for more security (Vezzetti et al. 2013; Vezzetti and Marcolin 2014; Jain et al. 2004; Jegede et al. 2017; Khan et al. 2008). These conventional schemes of information security have several disadvantages (Khan et al. 2010). They identify some of the characters related to the individual rather than identifying the individual who truely generated them. The PINs can be forgotten, or stolen. These schemes can be effortlessly hacked or bypassed. In addition, they are not accurate enough.

In recent years, the protection of biological features of individuals, like face, palm print, iris, and fingerprint has seen an exponential growth. The problem is that these biometrics are always linked to an individual and should not be switched, not like passwords that are replacable if embezzled. To avoid the loss of user biometrics, it is advantageous to alter them using non-reversible schemes to create cancelable templates (Khan et al. 2008). The privacy and security are mandatory for biometric protection for the following reasons:

- Cryptographic passwords and secret keys are barely recognized to the individual, and therefore the confidentiality can be retained. On the other hand, biometrics like signature, face, fingerprint, and voice can be effortlessly taped and abused without the individual's approval.
- If a hacker finds a way to access the biometric models and introduce them to a system emulating a person's existence, the biometrics will no longer be trusted. In this scenario, the user biometrics will lose their importance. On the other hand, crypto-keys, PINs, and passwords can be updated if they are attacked.
- It is exceedingly advocated to use secret passwords in different applications. Nevertheless, user biometric-based verification techniques depend on the same user biometrics. If a user template model is hacked in a certain product, hacking of all other applications using the same biometric will be possible.

There is a growing trend to use biometrics in various fields including commercial applications that use intelligence-based security structures (e.g., passwords and PINs), administration applications that use symbolic structures (e.g., Badges and ID cards), and forensic applications that rely on individual professionals to compare biometric characteristics. In these instances, structure protection is difficult. When systems require a high level of trustworthy security, biometrics can serve for this task. Biometric-based recognition is a technique by which an individual establishes an identity based on his or her own biometric characteristics (Rathgeb and Busch 2012; Sinha and Singh 2005). Generally, the user biometric structure comprises four fundamental elements: input interface (sensors), Digital Signal Processing (DSP), information storage, and output interface (display) (Ross et al. 2008; Lu et al. 2015). In the traditional biometric-based recognition process, examples of biometrics are stored and different characteristics are obtained and collected in a storage database. Throughout the authentication phase, the newly-collected biometric attributes are matched with the stored templates.

Several methods (Dong et al. 2019; Połap et al. 2019; Połap 2018; Liu et al. 2019) have been proposed to perform face and voice recognition tasks. Dong et al. (2019) proposed an improved version of an evolutionary attack algorithm that is applicable for any face recognition model under the decision-based black-box attack settings. This algorithm can represent the local geometry and simultaneously decrease the search space dimensions. In Połap et al. (2019), the authors proposed an evolutionary decision model to verify voice samples. The speech signals can be treated by the selected mathematical transform in conjunction with a bio-inspired algorithm as a feature extractor, and a spiking neural network as a final classification tool. This model can search over the transformed voice samples without any

limitations. The author of Połap (2018) presented a model for identity verification based on voice and image samples by using a heuristic neural network. This model can process the sound and image files, simultaneously, to obtain features. The authors of Liu et al. (2019) introduced an adaptive face recognition model, which has three parts. The first part is the adaptive margin Softmax, which finds the appropriate margin for every class to adaptively minimize intra-class variations. The second part represents the hard prototype mining, which aims to make the model concentrated on hard classes by adaptively choosing prototypes. The last one is adaptive data sampling, which adaptively feeds valuable samples through a feedback channel from the classification layer to the data layer.

The biometric-based authentication scheme achieves adequate security features and minimal computational cost, especially in the field of telemedicine to protect user-information against offline password attacks (Arigbabu et al. 2016; Jianjun et al. 2019). Among traditional biometric identification and verification schemes, cross-matching schemes, and cross-application schemes, all systems and applications depend on personal biometrics that can be straightforwardly captured, when the biometric database template is known (Nandakumar and Jain 2015; Jain et al. 2006). Therefore, biometric cryptosystems can offer high security and privacy for biometric systems. In biometric-based cryptosystems, the user biometrics are safeguarded with the help of ciphering secret keys. In such structures, the unique biometric patterns are not deposited in the storage database, but they are initially converted to encrypted versions (Rachapalli and Kalluri 2017; Manzoor and Selwal 2018). Based on the ISO/IEC 24745 (Patel et al. 2015), biometric protection structures must attain three objectives of confidentiality, protection against reference cross-matching and privacy. Confidentiality means preventing the original biometrics from retrieval of an individuals' attributes by any unauthorized attempt. Biometric reference cross-matching is performed in a way such that different well-protected templates should be used for different applications. Privacy means that the users' biometrics should be protected from unauthorized access.

To achieve the above-mentioned requirements in biometric structures, straightforward encryption, or hash functions are utilized to increase confidentiality. Hash functions are very sensitive to small changes in the input. All biometric patterns vary with ecological circumstances. For example, iris and face biometrics are considerably influenced by brightness changes. Consequently, in practice, these structures are not employed directly, because they are only applied on accurate data. In encryption methods, when biometrics are ciphered, they must be deciphered to maintain compatibility. This establishes an assault if an unlicensed person has admittance to deciphered templates. Therefore, cancelable templates have earned a great advantage. In this approach, as an alternative to accumulating the unique user biometrics, a one-way scheme is used. This way of constructing biometric templates has shown desired features of allowing verification with cancelable biometric templates as shown in Fig. 1.

The hacked user biometrics can be re-initiated with an alternative transform or encryption algorithm. This characteristic maintains confidentiality as retrieving the original biometric from the mutated one is computationally difficult. In addition, cross-matching amongst databases is avoided, as each user application depends on a distinct transform or encryption algorithm. This strategy does not affect the correctness of the matching process as the characteristic features of the attributes are roughly preserved after the conversion or encryption algorithm (Patel et al. 2015).

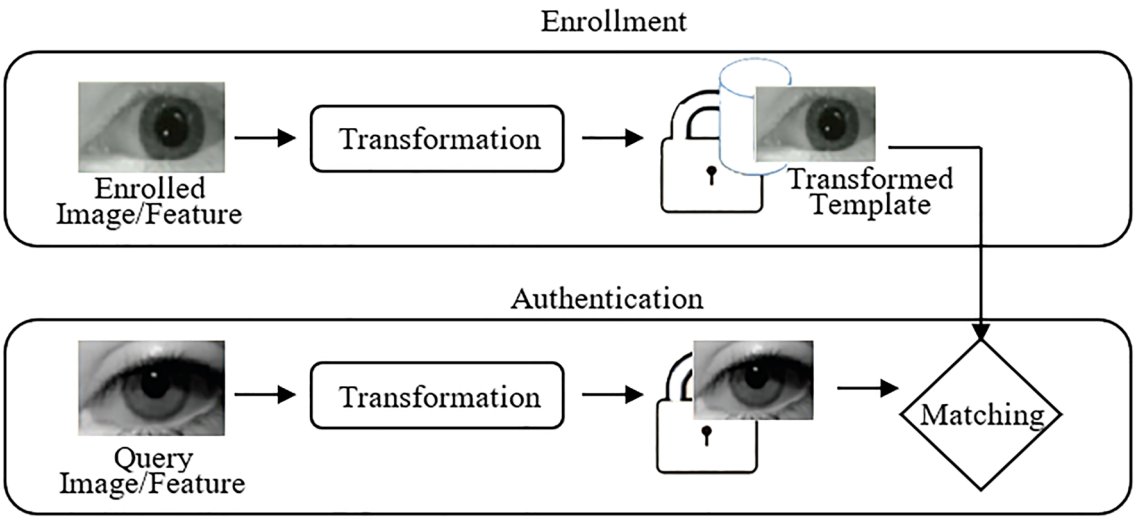


Fig. 1 Cancelable biometric system

A cancelable biometric transformation represents a deliberate distortion of the biometric signal based on a selected transform (Ratha et al. 2001). In such methods, the unique user biometric or collected characteristics are converted using a one-way process prior to storage. According to this definition, a cancelable biometric transformation increases the diversity and unlinkability. Therefore, different transformations can be applied on the same biometric template with different functions to avoid cross-matching between templates accumulated in different storage databases. Templates stored based on a single biometric data can be described as being irreversible (Patel et al. 2015) and the used transformations can be classified as being irreversible transformations (Grassi and Faundez 2009; Jeong and Teoh 2010; Moujahdi et al. 2012; Savvides et al. 2004; Kim and Toh 2007; Tarif et al. 2018). Particular transform constraints are adopted on the user biometric attributes to acquire the modified forms (Khan et al. 2010). On the other hand, a hybrid biometric cryptosystem (Ao and Li 2009; Feng et al. 2010; Sree and Radha 2016; Wu and Yuan 2010) combines two or more template security technologies to build a user-specific biometric cryptosystem. In addition, biometric patterns can

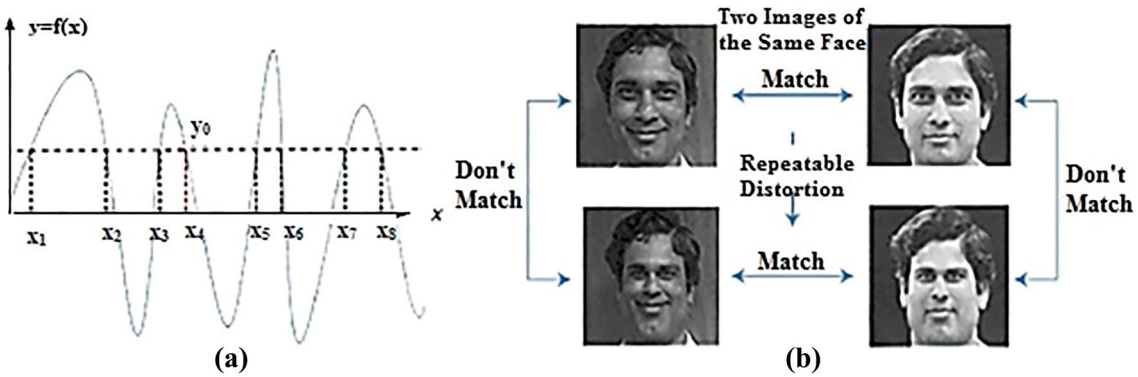
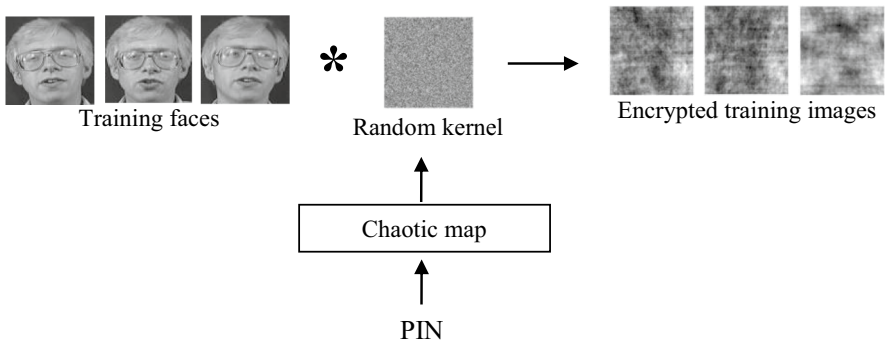
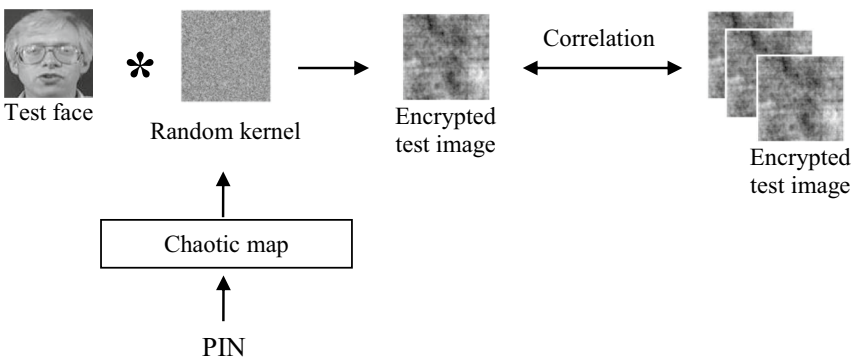


Fig. 2 An illustration of a nonlinear transformation employed to face biometrics

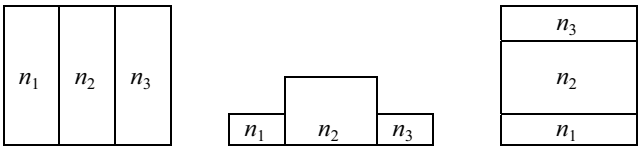
Fig. 3 **a** The enrollment module of the cancelable biometric system. **b** The authentication module of the cancelable biometric system



(a) Enrollment stage for cancelable biometric templates.



(b) Authentication stage for cancelable biometric templates.



(a) Generalized Baker chaos map encryption, N=8, n_1 = 2, n_2=4 and n_3=2.

$n_1 = 2$ $n_2 = 4$ $n_3 = 2$

S_1	S_2	S_3	S_4	S_5	S_6	S_7	S_8
S_9	S_{10}	S_{11}	S_{12}	S_{13}	S_{14}	S_{15}	S_{16}
S_{17}	S_{18}	S_{19}	S_{20}	S_{21}	S_{22}	S_{23}	S_{24}
S_{25}	S_{26}	S_{27}	S_{28}	S_{29}	S_{30}	S_{31}	S_{32}
S_{33}	S_{34}	S_{35}	S_{36}	S_{37}	S_{38}	S_{39}	S_{40}
S_{41}	S_{42}	S_{43}	S_{44}	S_{45}	S_{46}	S_{47}	S_{48}
S_{49}	S_{50}	S_{51}	S_{52}	S_{53}	S_{54}	S_{55}	S_{56}
S_{57}	S_{58}	S_{59}	S_{60}	S_{61}	S_{62}	S_{63}	S_{64}

→

S_{31}	S_{23}	S_{15}	S_7	S_{32}	S_{42}	S_{16}	S_8
S_{63}	S_{55}	S_{47}	S_{39}	S_{64}	S_{56}	S_{48}	S_{40}
S_{11}	S_3	S_{12}	S_4	S_{13}	S_5	S_{14}	S_6
S_{27}	S_{19}	S_{28}	S_{20}	S_{29}	S_{21}	S_{30}	S_{22}
S_{43}	S_{35}	S_{44}	S_{36}	S_{45}	S_{37}	S_{46}	S_{38}
S_{59}	S_{51}	S_{60}	S_{52}	S_{61}	S_{53}	S_{32}	S_{54}
S_{25}	S_{17}	S_9	S_1	S_{26}	S_{18}	S_{10}	S_2
S_{57}	S_{49}	S_{41}	S_{33}	S_{58}	S_{50}	S_{42}	S_{34}

(b) Discretized Baker chaos map encryption.

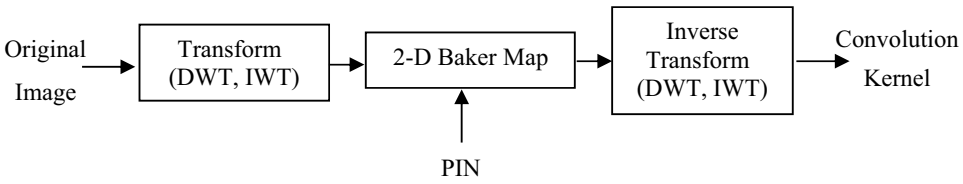


Fig. 4 The Baker chaos map encryption for an image with 8×8 pixels

Fig. 5 The proposed chaos map encryption scheme

be canceled or substituted with different patterns depending on an initial biometric information (Jin et al. 2016).

We present a method to produce a diversity of encrypted biometric templates through the utilization of different convolution kernels generated using chaotic Baker map. Convolution process is implemented in different domains. The authentication process is implemented in the encrypted domain. The proposed method can be applied on different databases.

The rest of this paper is structured as follows. Section 2 provides some work related to cancelable biometrics. Section 3 provides the structure and design of the cancelable biometric method based on chaotic encryption. Sections 4 and 5 show the test results and performance comparison. The concluding remarks are presented in Sect. 7.

2 Related work

The art of cancelable biometrics depends on the use of modified or distorted forms of user biometrics in the authentication process (Savvides et al. 2004). The renovation or conversion is intentional, and the templates that are subjected to hacking can be removed or replaced if necessary. The goal of cancelable biometrics is to increase privacy of the subscribers. A high level of performance of biometric systems needs to be maintained even with cancelable templates. These two requirements are conflicting, and hence there is a need for a trade-off between them.

One of the most basic procedures for creating cancelable user biometric patterns depends on a geometric non-invertible renovation (Rathgeb and Uhl 2011). A nonlinear transform is applied on face and fingerprint biometrics. The unique user biometric patterns are modified by employing feature-domain or signal-domain conversions as illustrated in Fig. 2. Figure 2a shows the feature-domain transformation for face biometrics. Every feature position is converted according to a function $y=f(x)$ that cannot be inverted. The x_0 position is planned to $y_0=f(x_0)$. If y_0 is known, reverse mapping is a many-to-one process. x_1, x_2, x_3, x_4, x_5, x_6, and x_7 are all valid inverse values for y. In Fig. 2b, the face is distorted in the original pixel domain before extracting features. The altered form does not match the real face, and the two cases of the altered faces contest each other.

Palm hashing is a biometric system that hashes the palm print patterns using a group of pseudo-random secret keys to acquire distinctive codes known as palm hashes (Ratha et al. 2007). These codes for authentication can be deposited on compact machines such as tokens and smart cards. In Connie et al. (2005), the authors stated that one

Fig. 6 The 15 used training AT&T biometric images of sample1 dataset

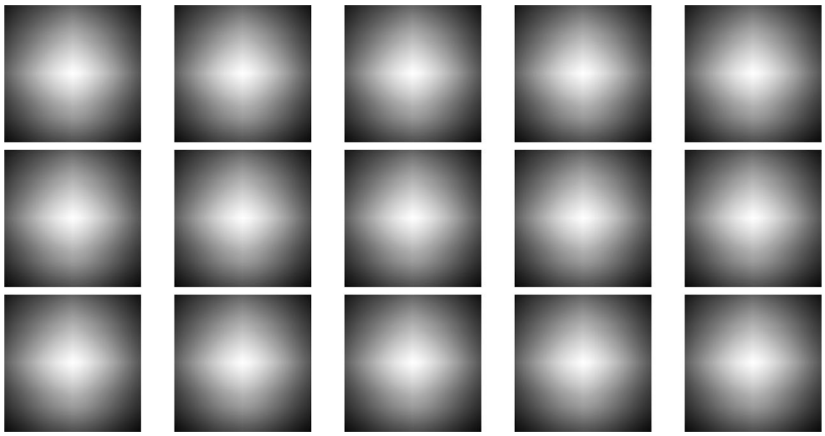


Fig. 7 The 15 encrypted training faces by equivalent kernels on sample1 dataset

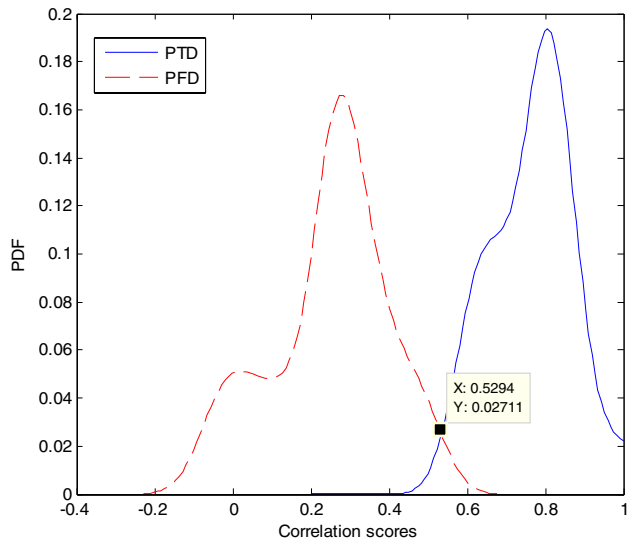


Fig. 8 The PTD and PFD using the circular encryption on the tested sample1 dataset

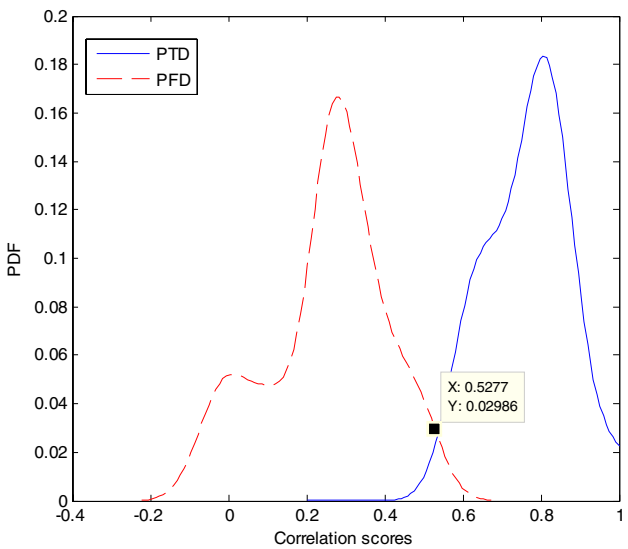


Fig. 9 The PTD and PFD using the encryption in the IWT domain on the tested sample1 dataset

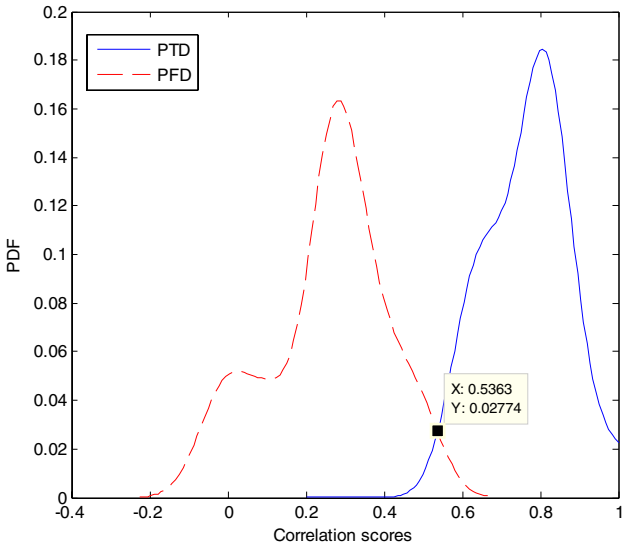


Fig. 10 The PTD and PFD using the encryption in the IWT domain with different keys on the tested sample1 dataset

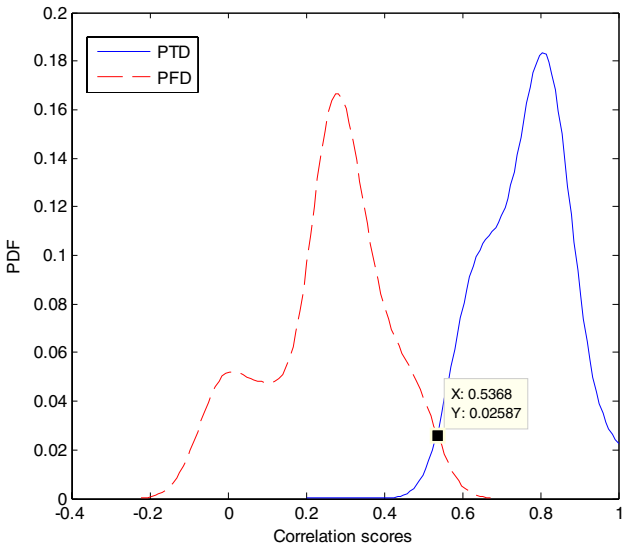


Fig. 11 The PTD and PFD using the encryption in the DWT domain on the tested sample1 dataset

of the objectives of cancelable biometrics is to safeguard confidentiality. To keep secrecy, cancelable user biometrics must be non-reversible, so that no evidence is disclosed from retractable biometric templates collected in storage databases for individual recognition/authentication. One of the ways to achieve this objective is to use non-invertible transformations. Recently, some new biometric recognition approaches have been proposed depending on bio-hashing. Those approaches use non-invertible transformations to obtain cancelable biometrics. In Cheung et al. (2005), the

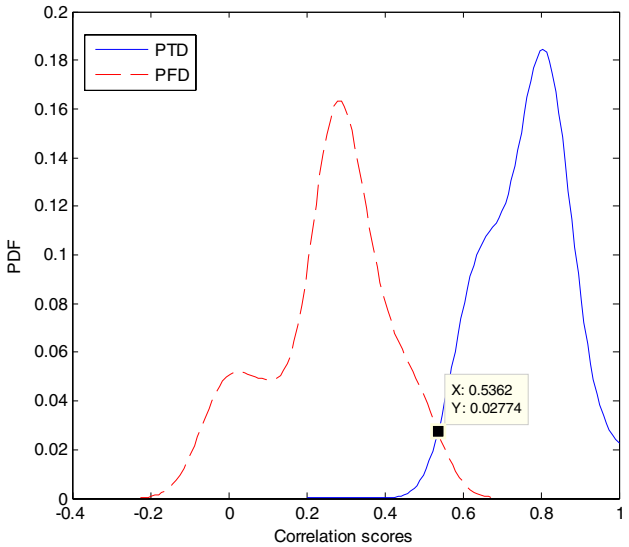


Fig. 12 The PTD and PFD using the encryption in the DWT Domain with different keys on the tested sample1 dataset

authors suggested some ideas for maintaining very low error rates, preventing the loss of the hash key, and improving the bio-hashing system for better performance.

In Lumini and Nanni (2007), the authors introduced a secure storage method for face templates by creating matrices and keys for cryptographic techniques with the help of biometric features. In Gaddam and Lal (2010), the authors suggested the encryption of biometric templates or training images. The seed utilized to produce the convolution kernel is applied as a PIN. Modified preparation images are utilized to obtain correlated filters. The encrypted filters are stored and used for authentication. Cancelable biometric filters are obtained with a specific encryption algorithm. This encryption algorithm takes place of the simple random number generator in Savvides et al. (2004), because for most users, the random sequence may be lost. In addition, there is a need to ensure that the accuracy is preserved and that the modified versions of the face images (cancelable biometric templates) can be used to discriminate between users.

Cancelable fingerprint identification systems follow a feature extraction procedure on a regular basis. Typically, features are collected from fingerprint images using the minutia of the fingerprints. In Savvides et al. (2004), the authors introduced a cancelable fingerprint recognition approach based on the use of polar and cartesian coordinates. This procedure achieves a good performance, while preserving the ability to cancel templates. In Ratha et al. (2007), the authors introduced various spiral curves based on a cancelable fingerprint identification system that adopts fuzzy rules. This fuzzy system was utilized for minutia feature ciphering. This approach succeeded in obtaining an EER of 1.17%.

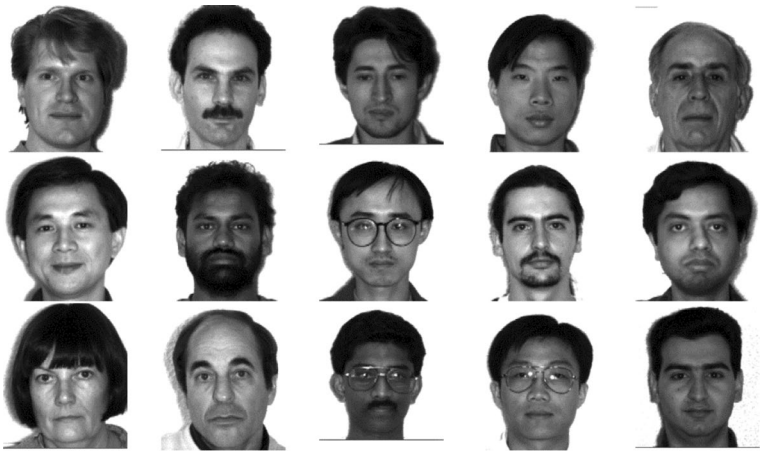


Fig. 13 The 15 used training YALE biometric images of sample2 dataset

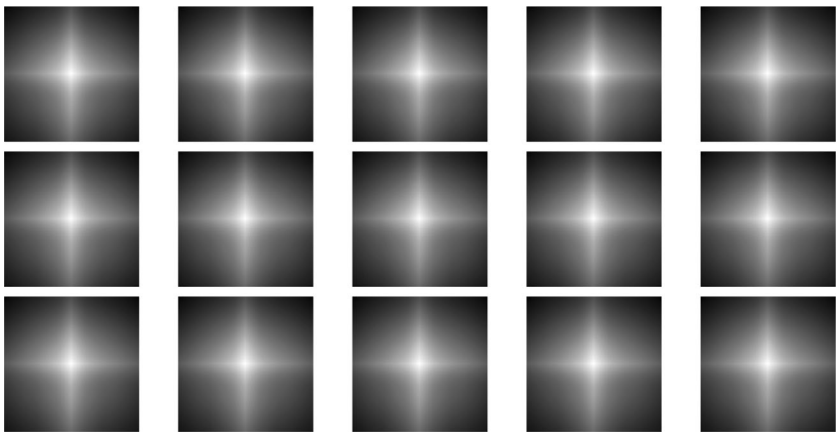


Fig. 14 The 15 encrypted training faces by equivalent kernels on sample2 dataset

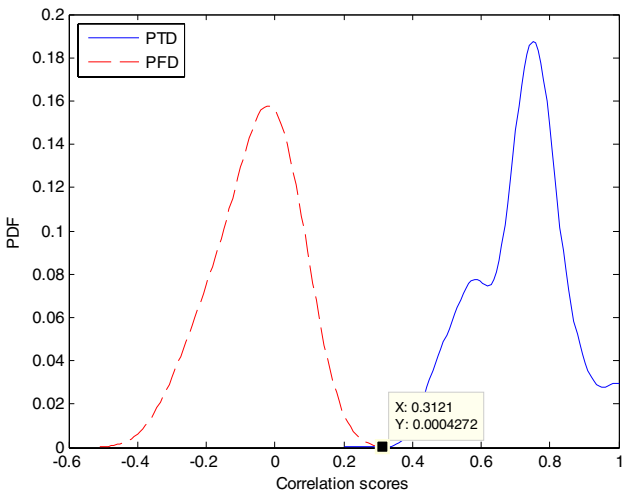


Fig. 15 The PTD and PFD using the circular encryption on the tested sample2 dataset

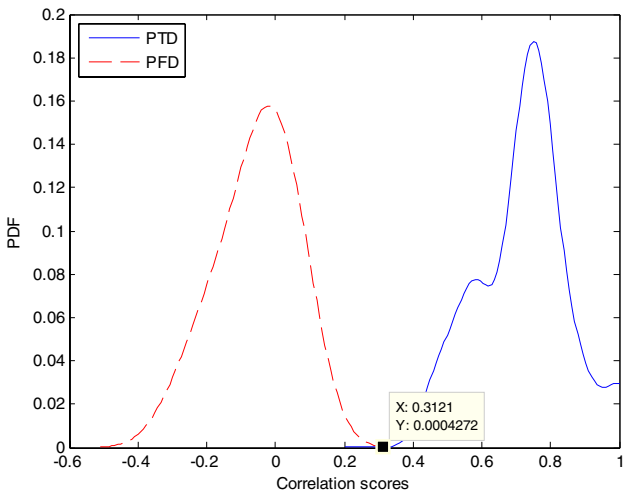


Fig. 16 The PTD and PFD using the encryption in the IWT domain on the tested sample2 dataset

Processing with filters like the Gabor filter has been adopted in cancelable palmprint identification systems similar to those utilized in fingerprint identification systems based on alignment. In Sandhya and Prasad (2017), a palmprint identification approach based on a look-up table and Gabor filters was introduced. The Gabor filter is utilized

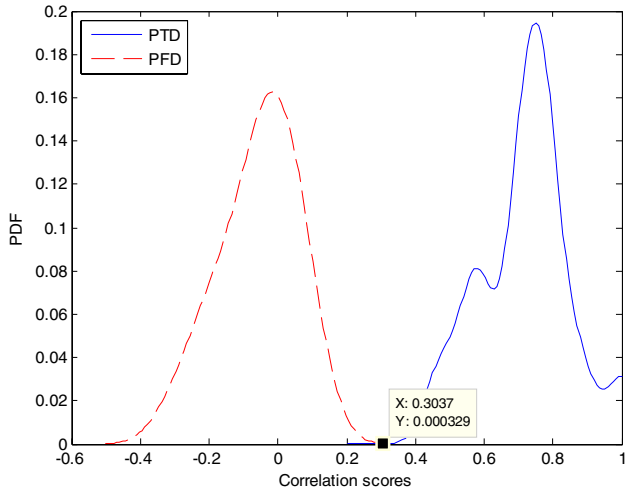


Fig. 17 The PTD and PFD using the encryption in the IWT domain with different keys on the tested sample2 dataset

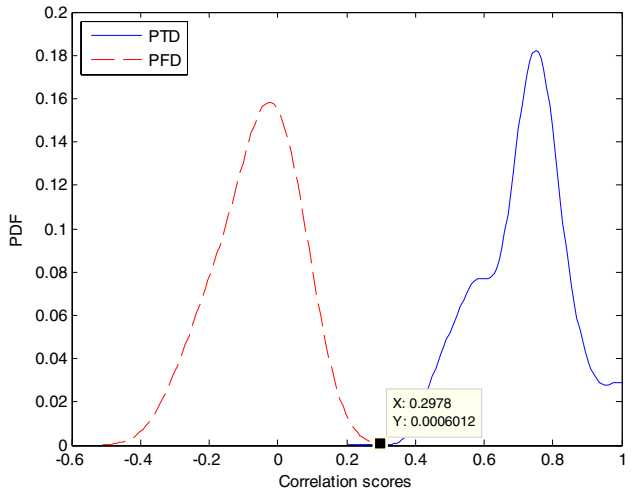


Fig. 18 The PTD and PFD using the encryption in the DWT domain on the tested sample2 dataset

to extract the characteristics from the palmprint patterns, which are then encoded using a look-up table. Chaotic matrices and Gabor filtering were utilized to obtain the characteristics in this methodology. Block-based processing is also implemented. The blocks are transformed into relevant decimal values, mapped with lookup tables, and the ultimate palmprint elements that can be used as cancelable templates are selected with check bits. This approach achieved an identification accuracy of 99.92%, while keeping the privacy of users.

Cancelable iris identification systems depend on the distinctive features of the iris area of the eye patterns. Procedures including normalization and localization are executed first, followed by the feature extraction process. The

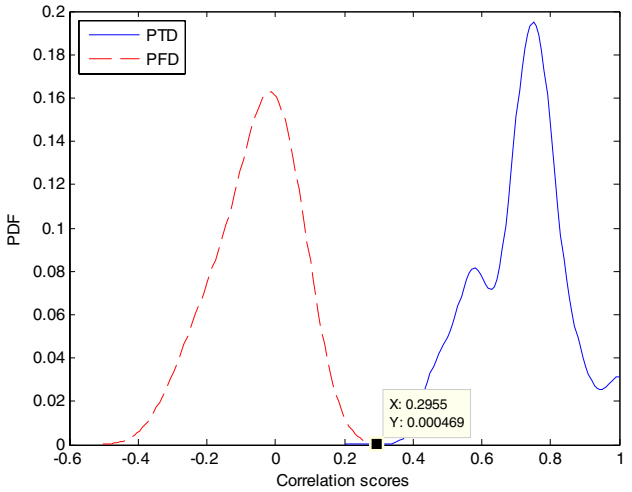


Fig. 19 The PTD and PFD using the encryption in the DWT domain with different keys on the tested sample2 dataset

fundamental concept of cancelable iris identification is to disguise the iris characteristics before storage. In Qiu et al. (2018), the authors introduced an iris identification system by employing a combination of non-invertible transformations and cryptography to hide iris features. They investigated the reversible biometric feature integration for iris identification through a non-invertible transformation using encryption and decryption and achieved a 99.9% recognition rate. In contrast, cancelable face identification methods follow an asymmetrical feature abstraction procedure. This procedure relies on cancelable multiple biometrics to provide better security, privacy, and authentication performance. It achieves high recognition accuracy and confidentiality. Ali and Tahir (2018) introduced a custom bloom-filter-based multi-biometric methodology for facial identification. This methodology succeeded in obtaining an EER of 0.4%.

Various methodologies have been introduced in previous studies for single-user biometric identification. These works led to iris recognition as iris images are believed to be the most distinctive biometrics. Over the past decade, cancelable iris recognition has been adopted to prevent iris templates from being hacked. In Rathgeb et al. (2015), a cancelable iris identification scheme based on three-level thresholding was introduced. Then, random projection was utilized to create ciphered iris characteristics that can be utilized for person authentication. Lyndon-Johnson Lemma-Strauss provides a hypothetical basis for this method. The system achieved a 99.67% identification accuracy and an 0.58% EER.

A method based on the generation of ciphered Gabor elements from iris patterns using convolution kernels obtained from chaos maps was presented by Soliman et al. 2019. Two types of chaos maps have been studied: logistic map and modified logistic map. In the modified logistic map,

Fig. 20 The 15 used training UFI biometric images of sample3 dataset

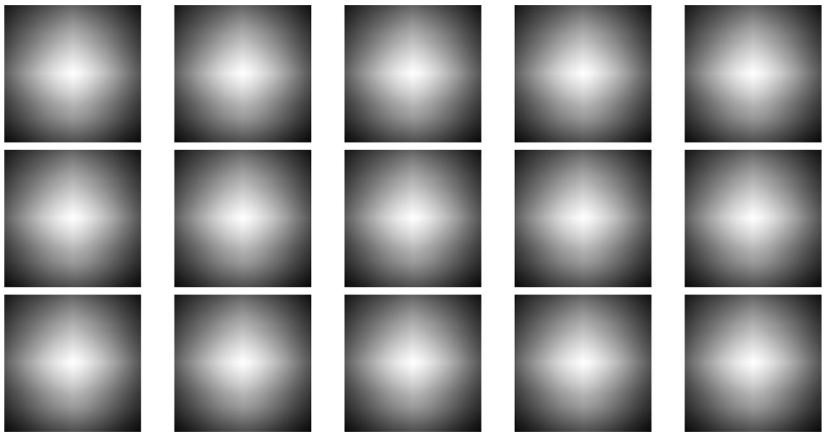


Fig. 21 The 15 encrypted training faces by equivalent kernels on sample3 dataset

the keyspace is increased, and therefore the confidentiality is increased. The ciphering secret key in this method is based on the obtained features. Therefore, the resulting ciphered features are dependent on the actual features and the secret key. Using the modified logistic map, the scheme achieved a 99.08% accuracy and a 1.17% EER. Also, in Soliman et al. (2018a), the DRPE technique has been effectively implemented in the cancelable face identification scheme.

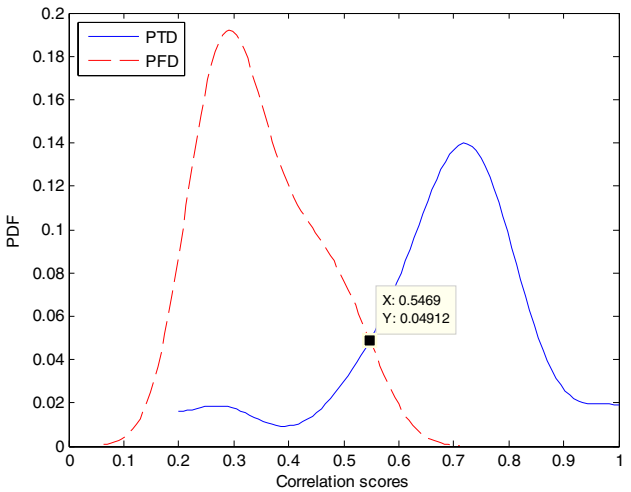


Fig. 22 The PTD and PFD using the circular encryption on the tested sample3 dataset

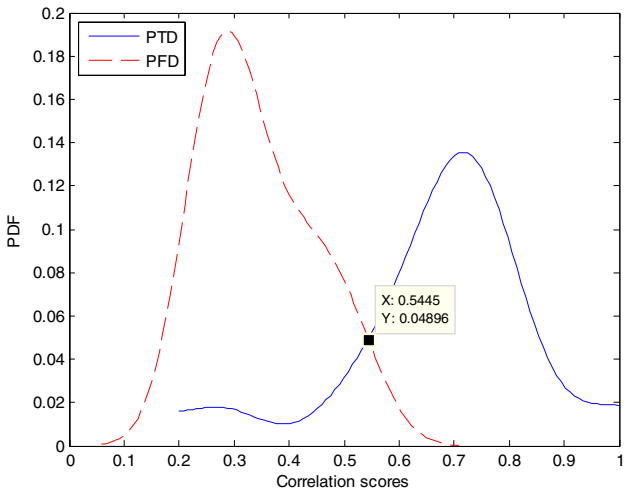


Fig. 23 The PTD and PFD using the encryption in the IWT domain on the tested sample3 dataset

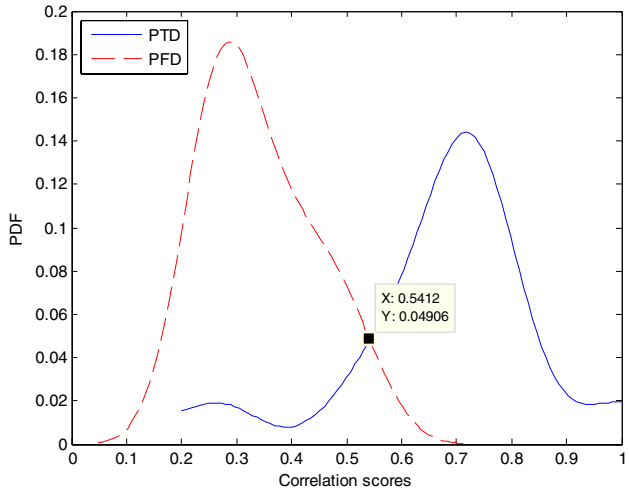


Fig. 24 The PTD and PFD using the encryption in the IWT domain with different keys on the tested sample3 dataset

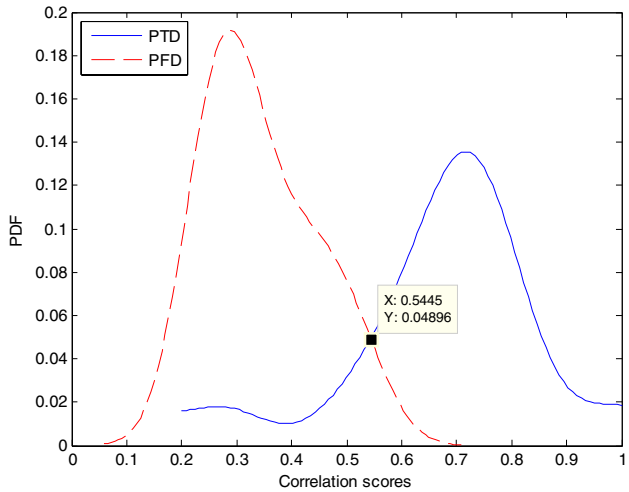


Fig. 25 The PTD and PFD using the encryption in the DWT domain on the tested sample3 dataset

The scheme uses an encrypted feature matrix in the bio-convolving strategy to ensure user privacy. The obtained outcomes for this cancelable biometric scheme confirms an 0.0017 EER, and an AROC of 0.993.

Moreover, in Soliman et al. (2018b), a cancelable multi-biometric iris identification system was introduced based on the combination of multiple models of biometric data. The biometric features created from the right and left irises of the same subject are merged into a specific protected iris code. The Fractional Fourier Transform (FrFT)-based DRPE method was presented to create irretrievable ciphered iris codes. The ciphering secret keys depend on random phase masks (RPM1 and RPM2). This system eliminates the need for sending the secret keys and increases verification

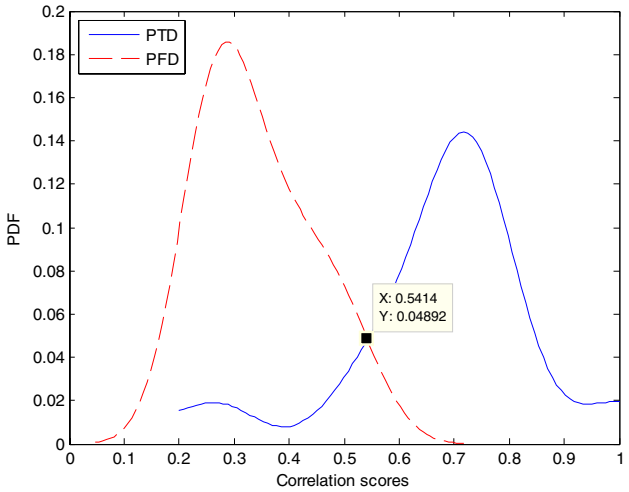


Fig. 26 The PTD and PFD using the encryption in the DWT domain with different keys on the tested sample3 dataset

and confidentiality, as every person has a distinctive secret key to acquire the ciphered iris codes. It improves privacy, while the authentication performance reveals an 0.63% EER and a 99.75% accuracy. The DRPE is an effective candidate, when it comes to implementing encryption to obtain cancelable biometric templates. Different variations can be explored based on various DRPE transformations for cancelable biometric recognition. In Soliman et al. (2018c), fingerprint recognition was studied using zone-based linear binary models. In this method, features are extracted from fingerprint patterns using binary linear templates. Each of the fingerprint patterns is partitioned into nine equal-size sectors, with linear patterns used for identification in each zone. The average detection accuracy is 94.28%.

3 Proposed chaos-based cancelable biometric system

To safeguard the person's biometric patterns and to guarantee that they can be revoked, the user patterns must be ciphered. Therefore, in the scenario of damage or theft, another ciphered biometric pattern can be obtained from the unique biometric model. Because chaotic maps are very sensitive to initial conditions, image encryption based on chaotic maps may be considered an ideal solution for the encryption of biometric templates. Cancelable biometrics can be effortlessly substituted with little variations in the preliminary state of the chaotic map utilized in ciphering if they are stolen in an application. This makes a dramatic difference in the reusable encrypted biometrics in the same application. The structure of the cancelable biometric system is defined in the subsequent paragraphs.

Fig. 27 The 15 used training LFW biometric images of sample4 dataset

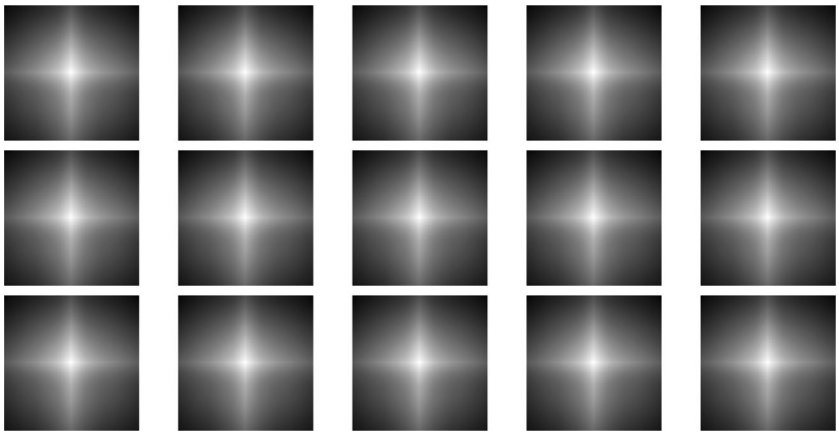


Fig. 28 The 15 encrypted training faces by equivalent kernels on sample4 dataset

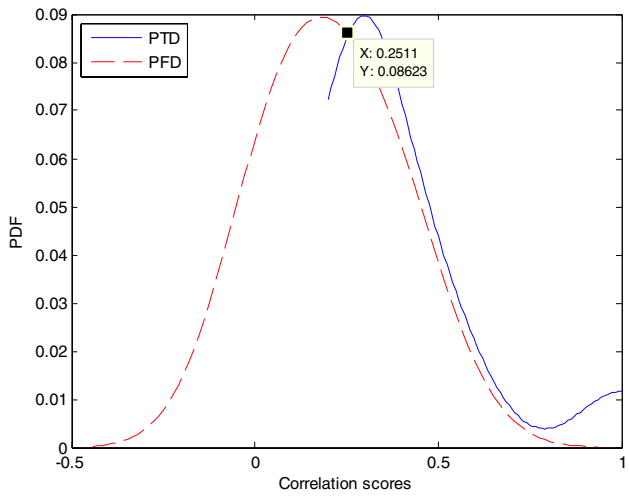


Fig. 29 The PTD and PFD using the circular encryption on the tested sample4 dataset

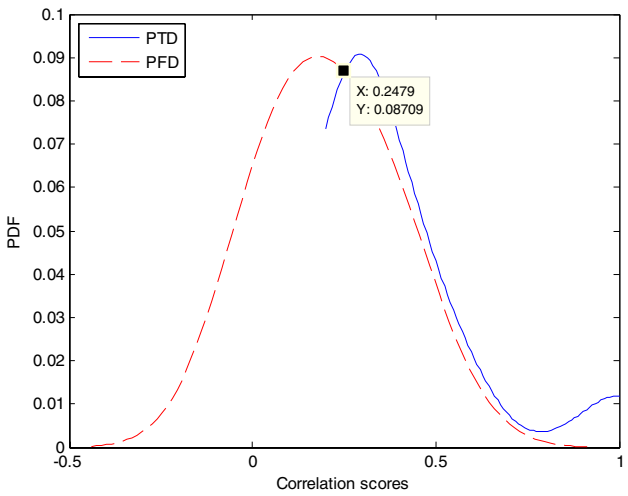


Fig. 30 The PTD and PFD using the encryption in the IWT domain on the tested sample4 dataset

3.1 Proposed system design

The suggested cancelable biometric system has two modules: the enrolment module and the authentication module as demonstrated in Fig. 3a and b. In the enrollment module shown in Fig. 3a, a face capturing device is used to acquire facial images. The training images are convolved with a random convolution kernel. The kernel is generated by the user

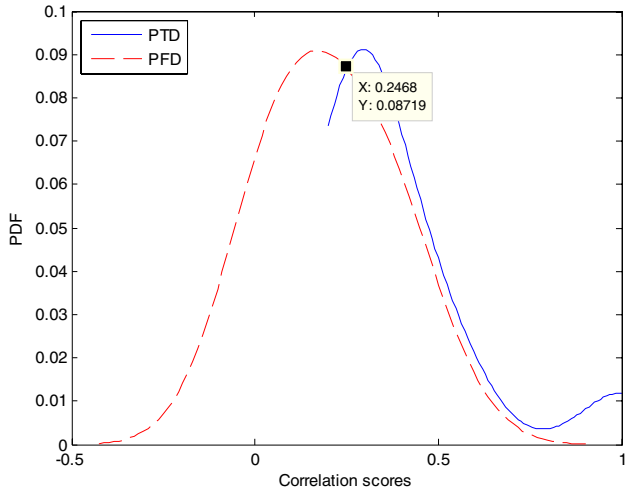


Fig. 31 The PTD and PFD using the encryption in the IWT domain with different keys on the tested sample4 dataset

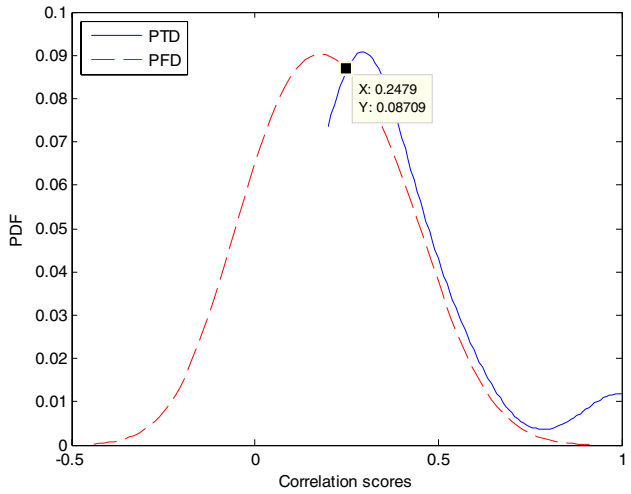


Fig. 32 The PTD and PFD using the encryption in the DWT domain on the tested sample4 dataset

selected PIN. This PIN is utilized as the primary state of the chaotic map to create the random kernel.

The resulting ciphered training images can be collected on a card, and subsequently utilized to know person identities. In case the card is stolen or lost, the enrollment module creates another kernel to generate different encrypted biometric images. If an attacker tries to renovate a user biometric from a purloined card, he should realize the covolution kernel utilized during the enrollment phase. To retrieve the original template, the attacker must de-convolve the image, which can be very difficult without realizing the person's PIN and the used ciphering approach (Savvides et al. 2004).

In the authentication module shown in Fig. 3b, the user PIN is displayed. This PIN is used to generate the

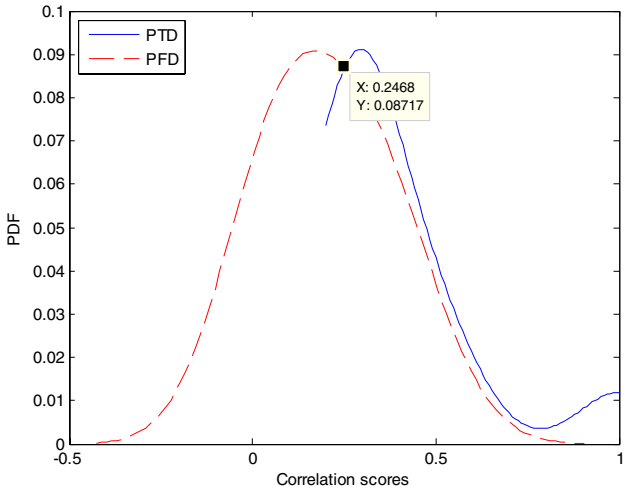


Fig. 33 The PTD and PFD using the encryption in the DWT domain with different keys on the tested sample4 dataset

convolution kernel. The resultant tested patterns after convolution are compared to the ciphered user biometric patterns, and the correlation output is tested for authentication. It is important to notice that the verification procedure is exclusively within the encryption domain. Furthermore, combining training patterns with any arbitrary convolution kernel before developing the encrypted biometric templates utilized for user biometric authentication does not alter the resultant correlation. This is done by changing the encryption domain used to generate the kernel.

3.2 Chaotic image encryption scheme

Chaotic cryptosystems are encryption schemes that rely on chaotic maps for template ciphering. These schemes are very vulnerable to preliminary conditions. If various constraints are utilized, a certain system operates in distinct trajectories, which are complicated to analyze and calculate. The resulting output structures of these systems have less correlation, and unpredictability (Gowthami and Mamatha 2015).

The Baker is a chaos map, which scrambles a square unit. The Baker chaos map (B) can be depicted as (Gowthami and Mamatha 2015):

$$\begin{aligned} B(x,y) &= (2x, y/2), && 0 \le x < 1/2 \\ B(x,y) &= (2x-1, y/2+1/2), && 1/2 \le x < 1 \end{aligned} \tag{1}$$

In fact, this straightforward strategy of splitting a square into two frames of identical size cannot be utilized for scrambling. Thence, there are two forms of the Baker chaos map, which use a secret key of transfer operator to separate the Baker chaos map. A vector with a secret random key k

Fig. 34 The 15 used training FERET biometric images of sample5 dataset

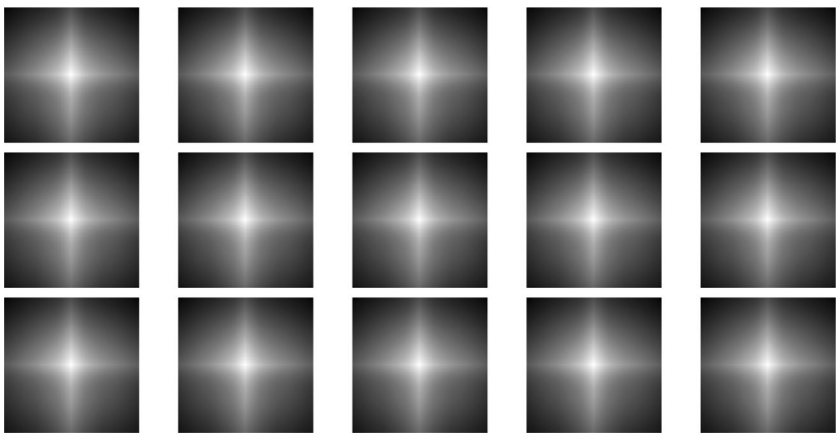


Fig. 35 The 15 encrypted training faces by equivalent kernels on sample5 dataset

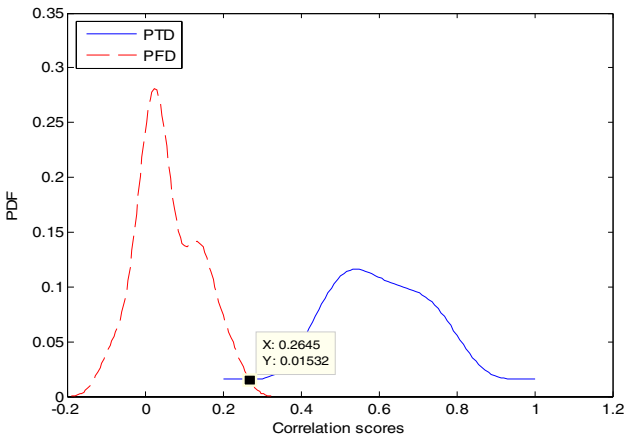


Fig. 36 The PTD and PFD using the circular encryption on the tested sample5 dataset

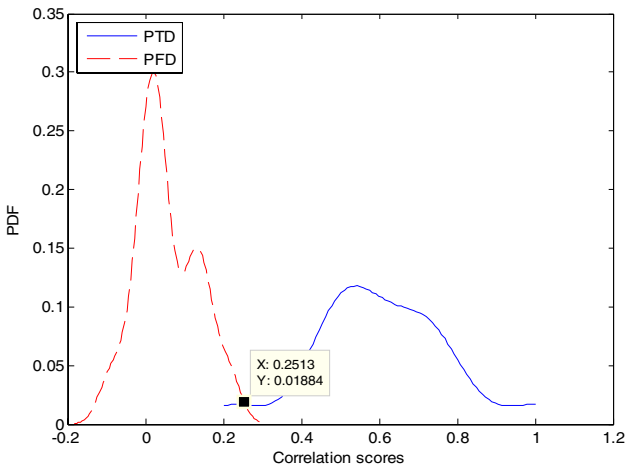


Fig. 37 The PTD and PFD using the encryption in the IWT domain on the tested sample5 dataset

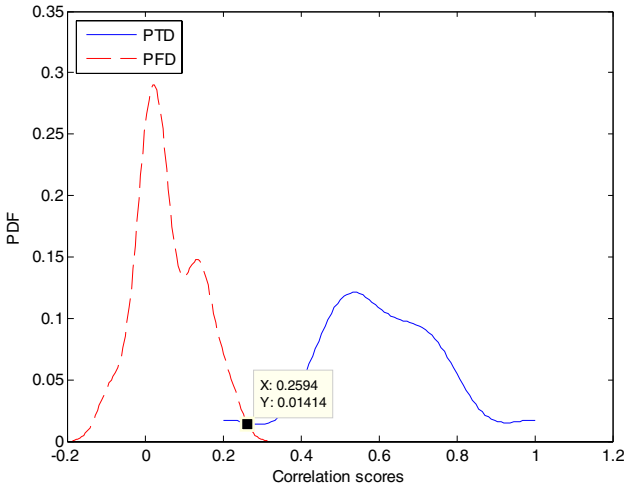


Fig. 38 The PTD and PFD using the encryption in the IWT domain with different keys on the tested sample5 dataset

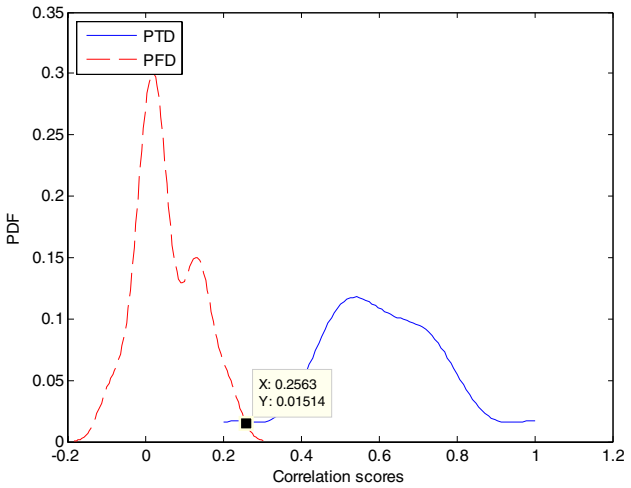


Fig. 39 The PTD and PFD using the encryption in the DWT domain on the tested sample5 dataset

elements, i.e. square unit is split into k vertical squares. The Baker chaos map generalization is done as follows:

1. An $N \times N$ rectangular matrix is split into vertical k squares of width n_i and height N, where $N = n_1 + n_2 + \cdots + n_k = N$.
2. The vertical generated squares should be horizontally extended.
3. The squares are arranged on the bottom left and the top right. It transfers in a bijective manner each pixel into another position.

The discrete Baker map is signified by $B(n_1, n_2, \ldots, n_k)$, where the series of k integers, $n_1, n_2, \ldots, n_k$, is selected, such that each integer n_i divides N, and $N_i = n_1 + \cdots + n_i$.

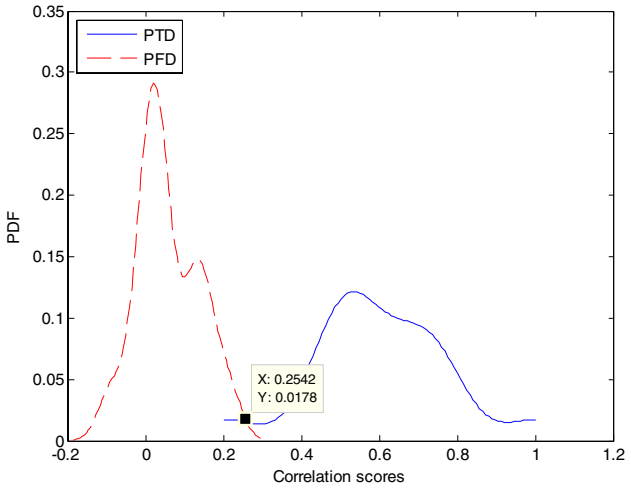


Fig. 40 The PTD and PFD using the encryption in the DWT domain with different keys on the tested sample5 dataset

The pixel at the position (r,s), with $N_i \le r < N_i + n_i$ and $0 \le s < N$ is mapped to (Gowthami and Mamatha 2015):

$$B_{(n_1,\ldots,n_k)}(r,s) = \left[\frac{N}{n_i}\left(r - N_i\right) + s \mod \left(\frac{N}{n_i}\right), \frac{n_i}{N}\left(s - s \mod \left(\frac{N}{n_i}\right)\right) + N_i\right] \quad (2)$$

A rectangular $N \times N$ matrix is split into k vertical squares of n_i width and N height. Subsequently, each vertical square of components $N \times n_i$ is split into n_i boxes; each contains N points. Every box is mapped to a row of pixels by mapping column-by-column, with the right one at the top and the left one at the bottom. An illustration of the scrambling for an 8×8 pixels image is demonstrated in Fig. 4. The secret key is selected as (2, 4, 2), which means that $N = 8$, $n_1 = 2$, $n_2 = 4$, and $n_3 = 2$. Figure 4a illustrates the comprehensive Baker chaos map encryption, while Fig. 4b indicates the discretized Baker chaos map encryption.

The chaotic 2-D Baker map based encryption is employed using a user PIN with IWT or DWT transformation as shown in Fig. 5. Identical or different keys are used to encrypt all bands of the transformed image.

Finally, the inverse transformation is performed to obtain the convolution kernel with a higher level of diffusion.

The IWT of the signal presents the original signal decomposition as a group of integer constants from which the input signal can be retrieved without any damage using the inverse IWT (Gao et al. 2006). The lifting scheme is considered an effective realization of IWT. It utilizes the function of the round-off *Int* as follows (Tong and Cui 2008):

Table 1 Comparative study of the encryption domain effect on the tested AT&T face biometric dataset

Domain	Mean		Threshold	Error probability (%)	Correct detection probability (%)	Authentication time
	Authorized patterns	Unauthorized patterns				
Spatial	0.7674	0.2494	0.5294	10.4865	89.5135	1.329065
IWT	0.7687	0.2518	0.5277	11.1450	88.855	0.402298
IWT with vaious keys	0.7683	0.2549	0.5363	10.7271	89.2729	0.295722
DWT	0.7687	0.2518	0.5368	11.1450	88.855	0.308763
DWT with various keys	0.7683	0.2548	0.5362	10.7264	89.2736	0.295722

Table 2 Comparative study of the encryption domain effect on the tested YALE face biometric dataset

Domain	Mean		Threshold	Error probability (%)	Correct detection probability (%)	Authentication time
	Authorized patterns	Unauthorized patterns				
Spatial	0.7223	− 0.0565	0.3121	9.7666	90.2334	1.329455
IWT	0.7212	− 0.0608	0.3144	9.7437	90.2563	0.404288
IWT with vaious keys	0.7206	− 0.0572	0.3037	10.7288	89.2712	0.295911
DWT	0.7212	− 0.0608	0.2978	9.7437	90.2563	0.308643
DWT with various keys	0.7206	− 0.0571	0.2955	10.7442	89.2558	0.295722

Table 3 Comparative study of the encryption domain effect on the tested UFI face biometric dataset

Domain	Mean		Threshold	Error probability (%)	Correct detection probability (%)	Authentication time (s)
	Authorized patterns	Unauthorized patterns				
Spatial	0.6016	0.3472	0.5469	5.4350	94.565	1.329065
IWT	0.5995	0.3439	0.5445	5.3651	94.6349	0.402277
IWT with vaious keys	0.5982	0.3413	0.5412	5.0420	94.958	0.295721
DWT	0.5995	0.3439	0.5445	5.3651	94.6349	0.308843
DWT with various keys	0.5982	0.3412	0.5414	5.0323	94.9677	0.295722

Table 4 Comparative study of the encryption domain effect on the tested LFW face biometric dataset

Domain	Mean		Threshold	Error probability (%)	Correct detection probability (%)	Authentication time (Sec)
	Authorized patterns	Unauthorized patterns				
Spatial	0. 2718	0. 2069	0.2511	4.2862	95.7138	1.329065
IWT	0.2700	0.2037	0.2479	4.2718	95.7282	0.402277
IWT with vaious keys	0. 2693	0. 2020	0.2468	4.3462	95.6538	0.295721
DWT	0. 2700	0. 2037	0.2479	4.2718	95.7282	0.308843
DWT with various keys	0. 2692	0. 2020	0.2468	4.3452	95.6548	0.295722

Table 5 Comparative study of the encryption domain effect on the tested FERET face biometric dataset

Domain	Mean		Threshold	Error probability (%)	Correct detection probability (%)	Authentication time
	Authorized patterns	Unauthorized patterns				
Spatial	0.6025	0.0566	0.2645	8.0130	91.987	1.329065
IWT	0.6003	0.0547	0.2594	8.7863	91.2137	0.402298
IWT with vaious keys	0.6017	0.0518	0.2513	8.4423	91.5577	0.295722
DWT	0.6003	0.0547	0.2542	8.8052	91.1948	0.308763
DWT with various keys	0.6017	0.0518	0.2563	8.4423	91.5577	0.295722

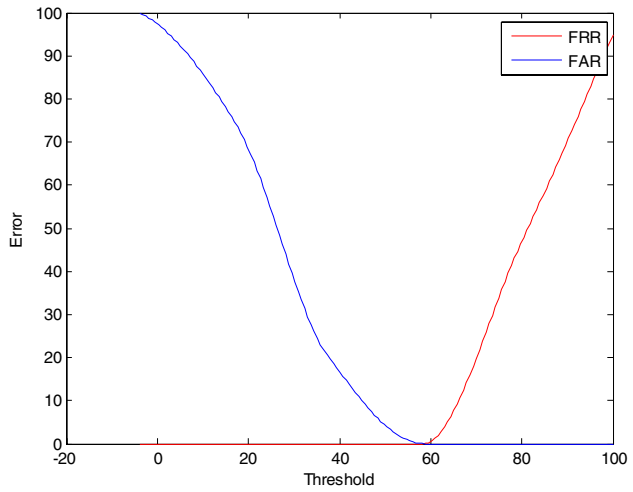


Fig. 41 FRR vs FAR for the cancelable biometric scheme using circular encryption on the tested sample1 dataset

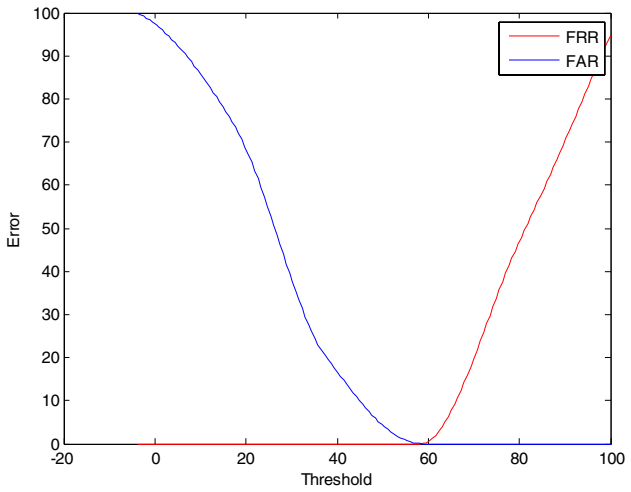


Fig. 43 FRR vs FAR for the cancelable biometric scheme using IWT domain with different keys on the tested sample1 dataset

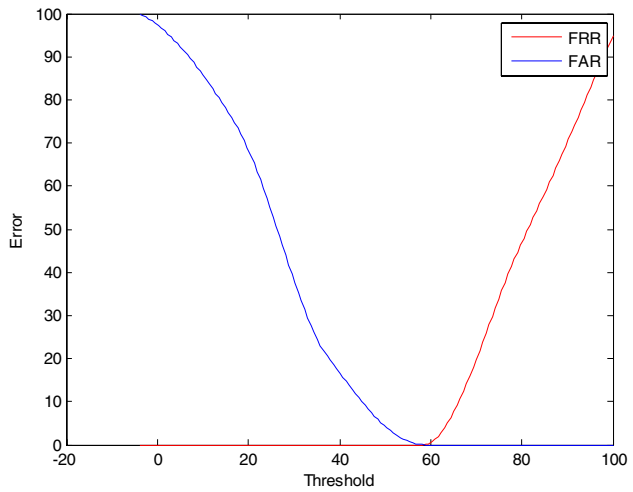


Fig. 42 FRR vs FAR for the cancelable biometric scheme using IWT domain on the tested sample1 dataset

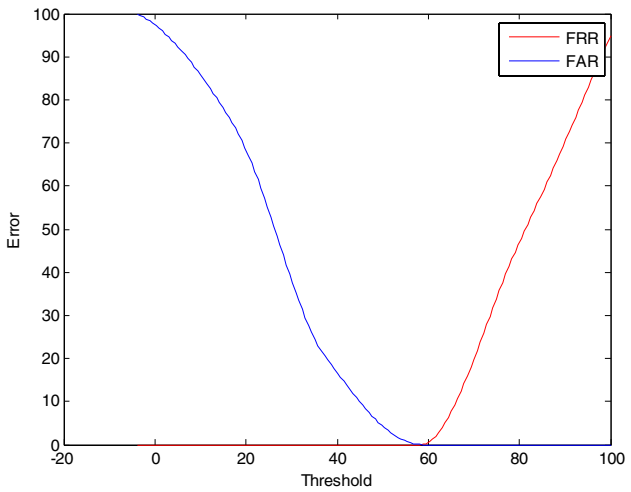


Fig. 44 FRR vs FAR for the cancelable biometric scheme using DWT domain on the tested sample1 dataset

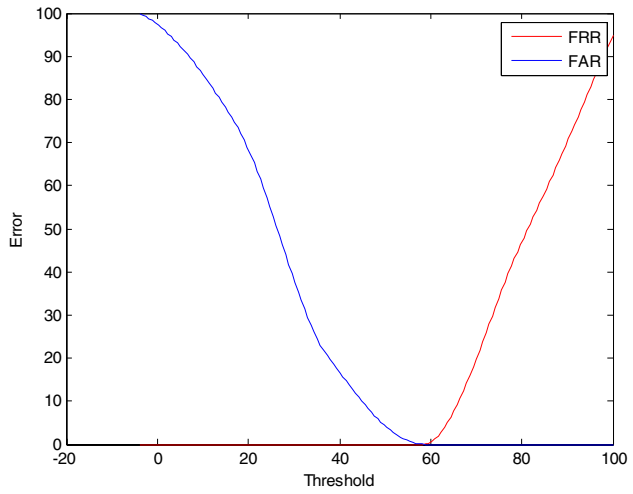


Fig. 45 FRR vs FAR for the cancelable biometric scheme using DWT domain with different keys on the tested sample1 dataset

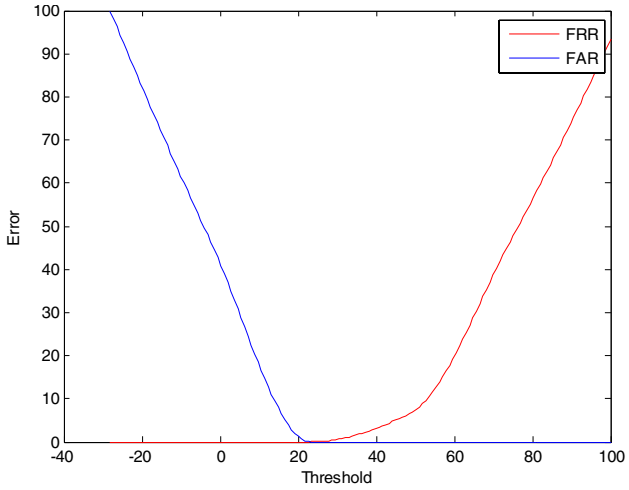


Fig. 47 FRR vs FAR for the cancelable biometric scheme using IWT domain on the tested sample2 dataset

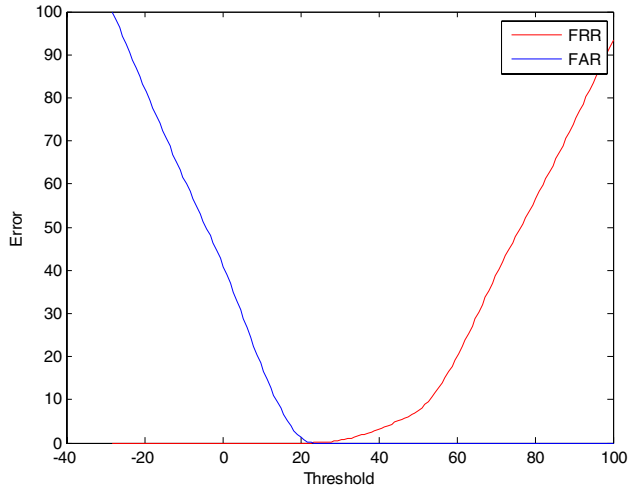


Fig. 46 FRR vs FAR for the cancelable biometric scheme using circular encryption on the tested sample2 dataset

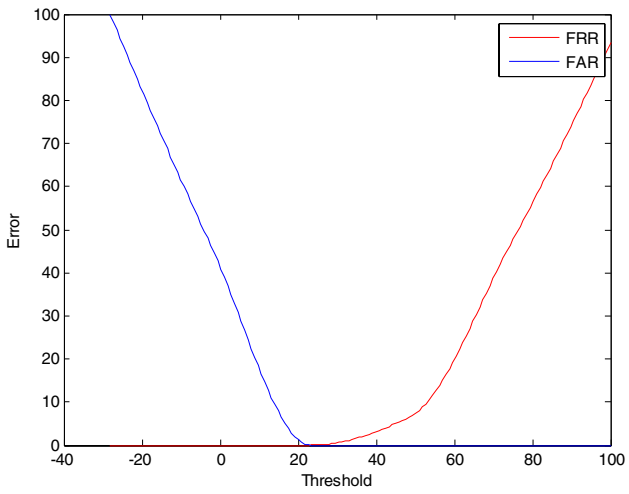


Fig. 48 FRR vs FAR for the cancelable biometric scheme using IWT domain with different keys on the tested sample2 dataset

$$\begin{aligned} d_i^{l+1} &= s_{2i+1}^l - Int\Big(\frac{9}{16}\big(s_{2i}^l + s_{2i+2}^l\big) - \frac{1}{16}\big(s_{2i-2}^l + s_{2i+4}^l\big)\Big) \\ s_i^{l+1} &= s_{2i}^l + Int\Big(\frac{1}{4}\big(d_{i-1}^{l+1} + d_i^{l+1}\big)\Big) \end{aligned} \tag{3}$$

where at the $l+1$-th decomposition level, the signals s_i^l, and d_i^{l+1} are the input at time i, and the high-frequency output at level $l+1$ and time i. s_i^{l+1} is the low-frequency output at level $l+1$ and time i.

In contrast, the DWT is implemented using multi-level filter banks. A single level decomposition of a 1-D signal $x(k)$ can be mathematically conveyed as follows (Guan et al. 2005; Ma et al. 2017; Jiang et al. 2016; Jung and Huh 2019; Huh 2018):

$$y_{high}(k) = \sum_n x(k)g(2k-n) \tag{4}$$

$$y_{low}(k) = \sum_n x(k)h(2k-n) \tag{5}$$

where $y_{high}(k)$ and $y_{low}(k)$ are the outputs of the high-pass and low-pass filters, respectively, after sub-sampling by two. Encryption is performed on all bands with identical or different keys.

3.3 Verification quality metrics

The score of correlation is utilized to reveal the relationship between a new test model and the user biometric patterns

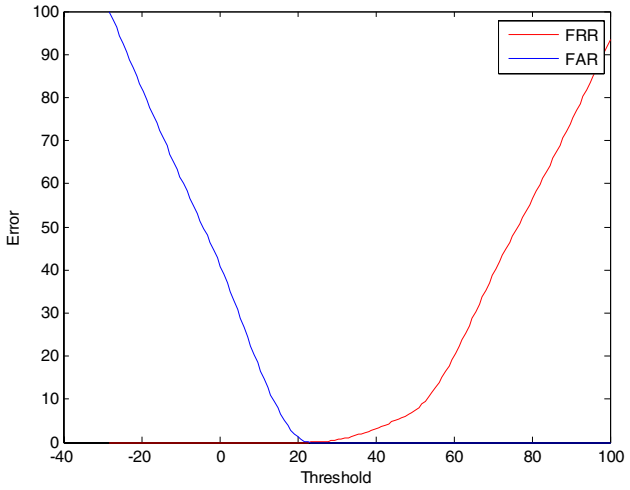


Fig. 49 FRR vs FAR for the cancelable biometric scheme using DWT domain on the tested sample2 dataset

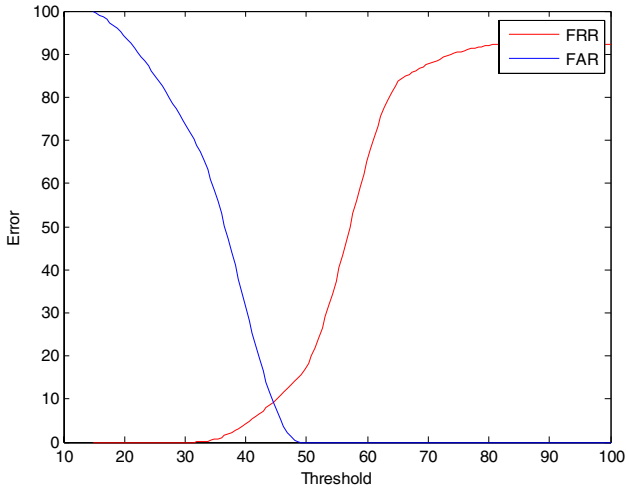


Fig. 51 FRR vs FAR for the cancelable biometric scheme using circular encryption on the tested sample3 dataset

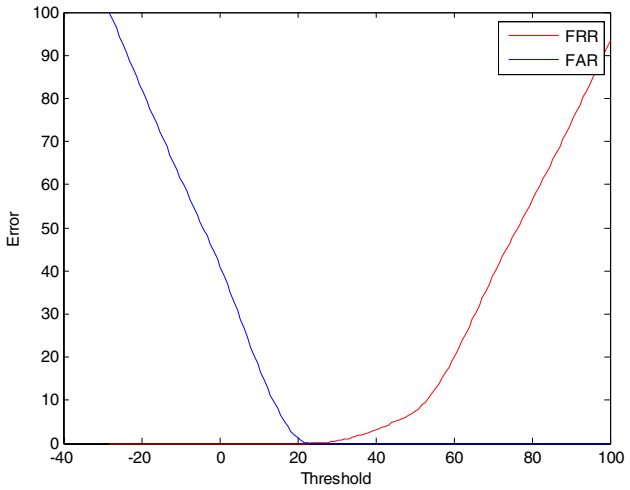


Fig. 50 FRR vs FAR for the cancelable biometric scheme using DWT domain with different keys on the tested sample2 dataset

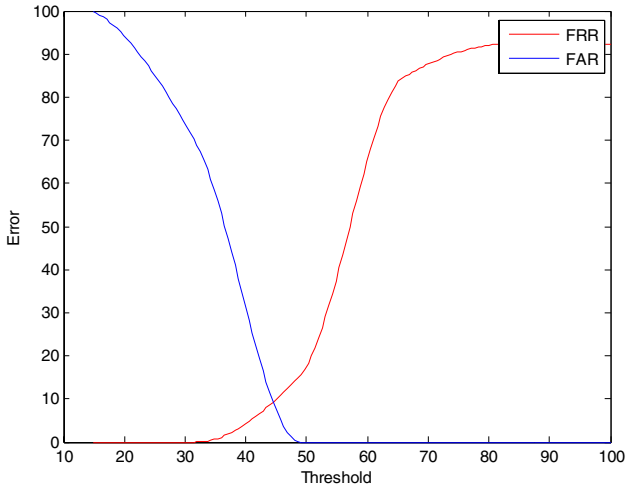


Fig. 52 FRR vs FAR for the cancelable biometric scheme using IWT domain on the tested sample3 dataset

in a database. The larger the obtained score is, the higher the relationship between models. The system accessibility is guaranteed if the test person score exceeds a certain level (He et al. 2013; Xiaodong et al. 2019; Osadchy et al. 2010; Jin et al. 2015). In real-world biometric systems for a number of reasons, unauthorized models may generate higher scores than those of some authorized models. For this reason, it is a fact that some taxonomic errors may occur even when selecting the classification threshold. For illustration, the threshold can be selected with a too extreme value, and certainly unapproved records should not surpass this threshold. Consequently, the system does not accept any incorrect patterns. On the other hand, authorized models with lower scores than the threshold are incorrectly rejected. Conversely, we can select a range that does not incorrectly reject the identified patterns. Alternatively, some illegal models are mistakenly approved. If we select the boundary between these two positions, good performance can be achieved (Souza et al. 2018; Huh 2017; Le et al. 2011; Huang and Qu 2011; Schmidhuber 2015).

In the biometric verification process, the examination data includes unauthorized and authorized samples. The records of every sample are averaged to give a unified record. The average record of the authorized samples is greater than that of the unlicensed samples. The system depends on the correlation records that arise during the verification process. The Probability of True Distribution (PTD) and the

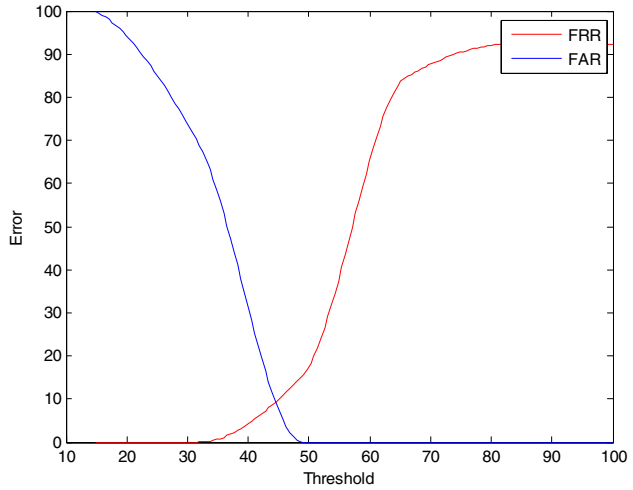


Fig. 53 FRR vs FAR for the cancelable biometric scheme using IWT domain with different keys on the tested sample3 dataset

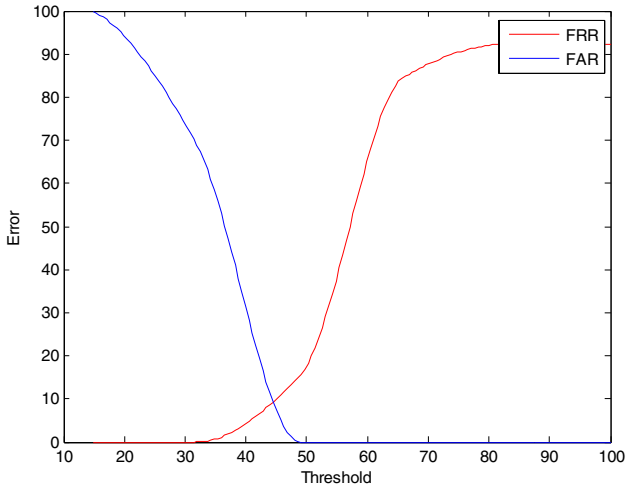


Fig. 55 FRR vs FAR for the cancelable biometric scheme using DWT domain with different keys on the tested sample3 dataset

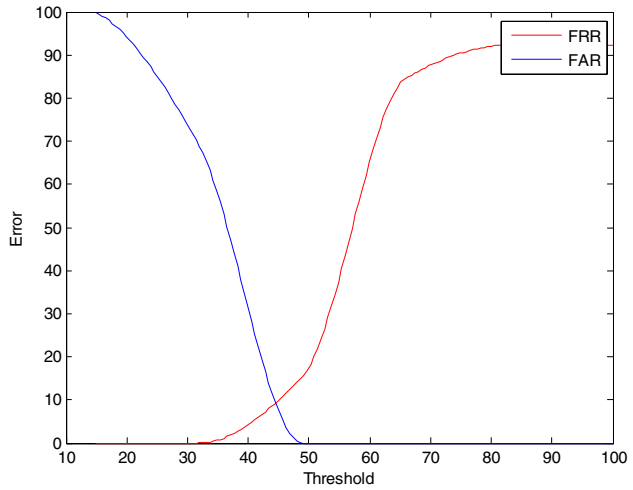


Fig. 54 FRR vs FAR for the cancelable biometric scheme using DWT domain on the tested sample3 dataset

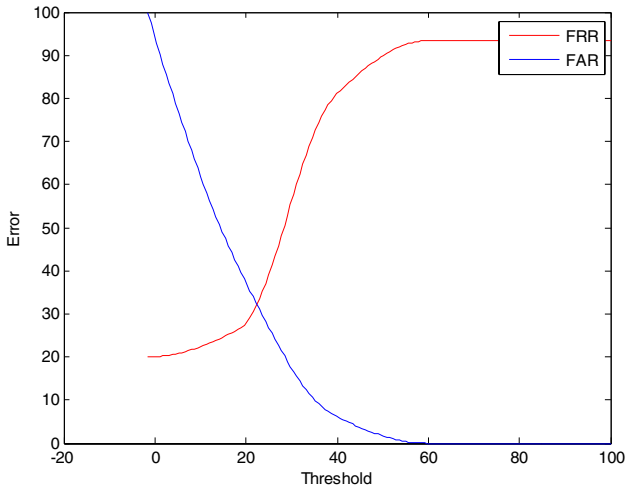


Fig. 56 FRR vs FAR for the cancelable biometric scheme using circular encryption on the tested sample4 dataset

Probability of False Distribution (PFD) are estimated. The PTD is the correlation distribution for real approved templates. The PFD is the correlation distribution for unauthorized templates.

The most important evaluation metrics that are used to evaluate the performance of a biometric recognition scheme are the False Acceptance Rate (*FAR*), the False Rejection Rate (*FRR*), the Equal Error Rate (*EER*), the True Acceptance Rate (*TAR*), the decidability index (D_i) and the accuracy.

False Accept Rate (FAR)/False Positive Rate (FPR):

The FAR shows if a system incorrectly recognizes an intruder. *FAR* indicates the probability that the system incorrectly authorizes a non-authorized person, due to falsely matching the biometric input with a template. *FAR/FPR* is defined as the fraction of impostor scores exceeding the threshold η. *FAR/FPR* is calculated as follows:

$$FAR/FPR = \frac{FP}{FP + TN} \tag{6}$$

where False Positive (*FP*) signifies imposter scores exceeding the threshold. True Negative (*TN*) shows the true imposter user. Total imposter score is represented by $FP + TN$.

False Reject Rate (FRR)/ False Negative Rate (FNR):

The *FRR* is the percentage of valid inputs, which are incorrectly rejected for an authorized person. The *FRR* is the percentage of times, when an individual record is not matched to his own stored template. In other words, *FRR* is the percentage of the genuine scores, which are lower

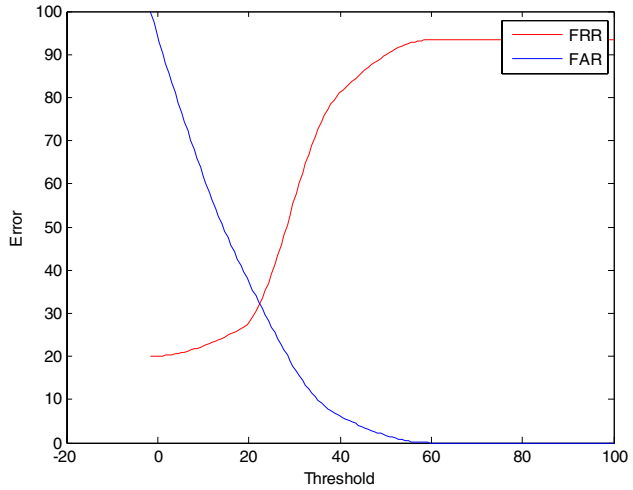


Fig. 57 FRR vs FAR for the cancelable biometric scheme using IWT domain on the tested sample4 dataset

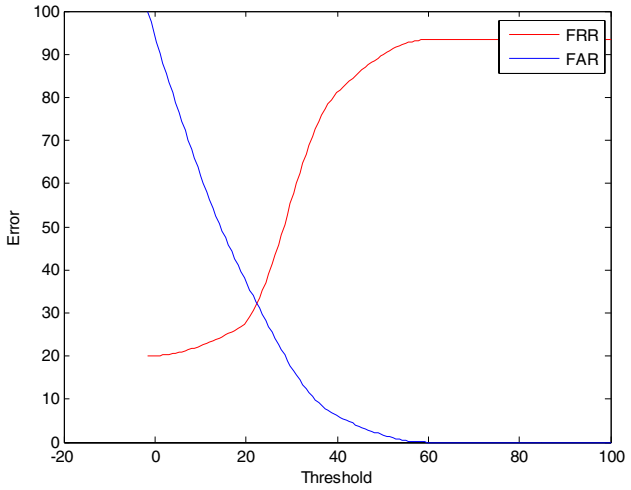


Fig. 59 FRR vs FAR for the cancelable biometric scheme using DWT domain on the tested sample4 dataset

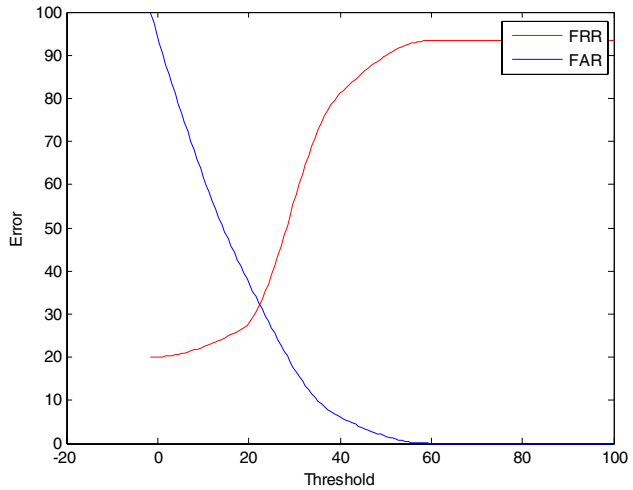


Fig. 58 FRR vs FAR for the cancelable biometric scheme using IWT domain with different keys on the tested sample4 dataset

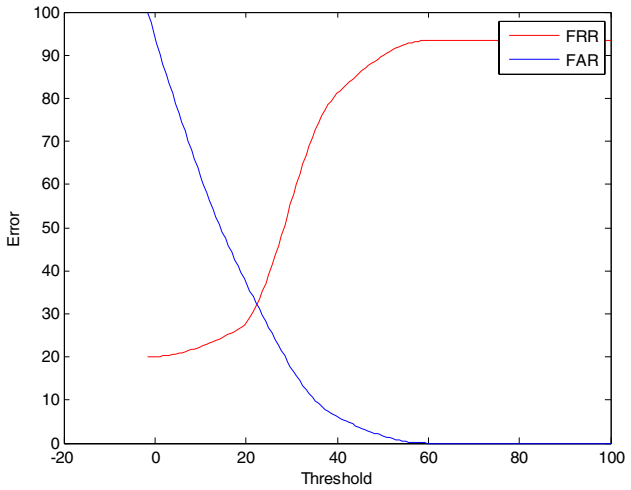


Fig. 60 FRR vs FAR for the cancelable biometric scheme using DWT domain with different keys on the tested sample4 dataset

than the decision threshold and are incorrectly rejected. The *FRR* is an empirical estimate of the probability at which the system incorrectly rejects the identity of the genuine user. The *FRR/FNR* is defined as the fraction of genuine user score that is less than the threshold η. The *FRR/FNR* is calculated as follows:

$$FRR/FNR = \frac{FN}{TP + FN} \tag{7}$$

where False Negative (*FN*) denotes genuine user scores below the threshold, and the True Positive (*TP*) represents the authorized users. Total genuine score is represented by $TP + FN$.

Equal Error Rate (EER)/Crossover Error Rate (CER)/Break Even Point (BEP):

The Equal Error Rate (*EER*) denotes the rate at the threshold value for which both *FAR* and *FRR* are equal, where genuine and impostor error rates are lose to zero. *EER/CER/BEP* is the rate at which the *FAR* is equal to the *FRR*.

True Acceptance Rate (TAR) or Genuine Accept Rate (GAR):

TAR/GAR is defined in terms of *FRR* as follows:

$$TAR = 1 - FRR \tag{8}$$

Decidability Index (D_i):

In order to measure separation between score distribution of genuine and imposter classes, we have used decidability index D_i as a performance metric. The decidability index is the normalized distance between means of genuine

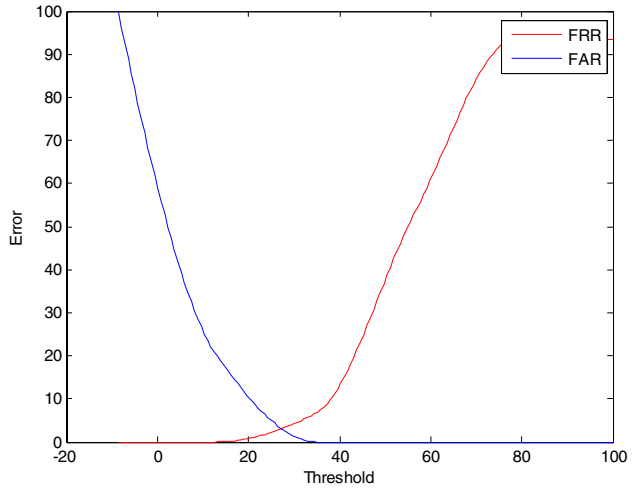


Fig. 61 FRR vs FAR for the cancelable biometric scheme using circular encryption on the tested sample5 dataset

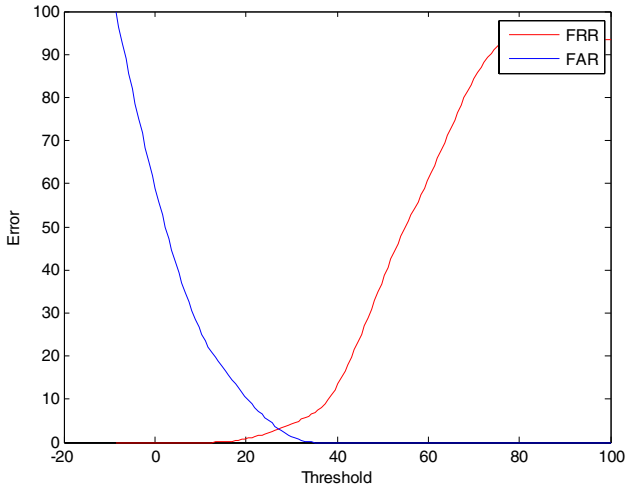


Fig. 63 FRR vs FAR for the cancelable biometric scheme using IWT domain with different keys on the tested sample5 dataset

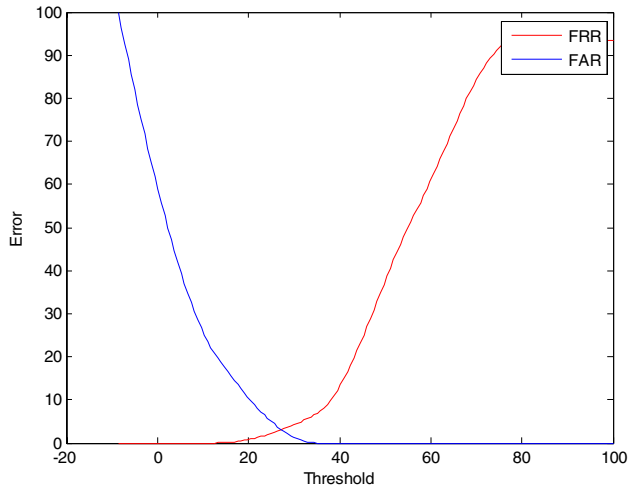


Fig. 62 FRR vs FAR for the cancelable biometric scheme using IWT domain on the tested sample5 dataset

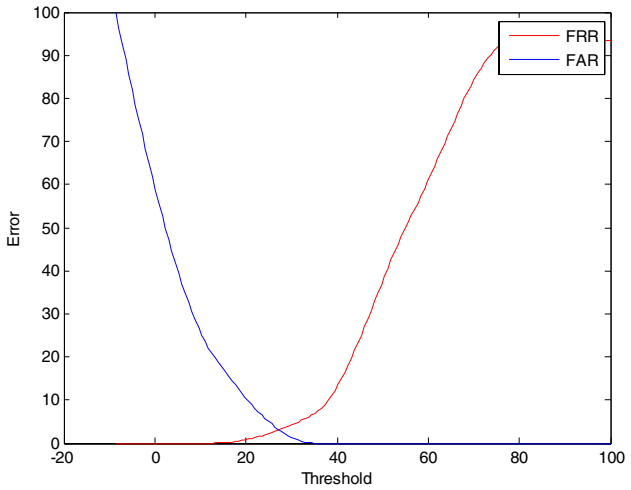


Fig. 64 FRR vs FAR for the cancelable biometric scheme using DWT domain on the tested sample5 dataset

and imposter probability distributions in standard deviation units, and it is determined using the following equation.

$$D_i = \frac{\left|\mu_{Geniune} - \mu_{Imposter}\right|}{\sqrt{\left(0.5\left(\sigma^2_{Geniune} + \sigma^2_{Imposter}\right)\right)}} \tag{9}$$

Here μ and σ are the means and standard deviations of the genuine and impostor distributions respectively. A higher D_i value indicates better performance.

Accuracy:

It is ratio between true cases (both true positive and true negative) and all possible cases. It is defined as follows:

$$Accuracy = \frac{TP + TN}{TP + FP + TN + FN} \tag{10}$$

4 Simulation results

To illustrate the impact of using the proposed encryption scheme for the introduced cancelable biometric system, we consider four different standard large-volume datasets. In the simulation result presentation, we will only display sample results of 15 different faces for 15 different individuals from AT&T, YALE, UFI, LFW, and FERET. These faces

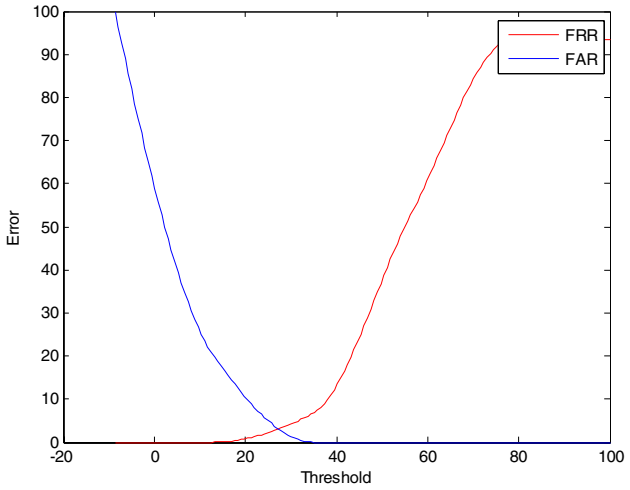


Fig. 65 FRR vs FAR for the cancelable biometric scheme using DWT domain with different keys on the tested sample5 dataset

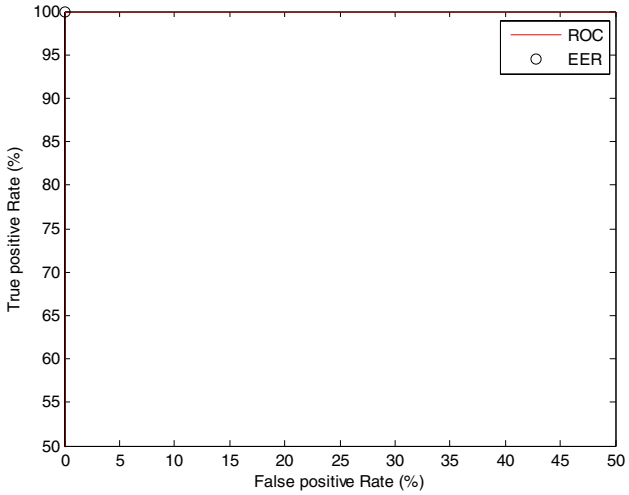


Fig. 67 ROC curve for the cancelable biometric scheme using IWT domain on the tested sample1 dataset

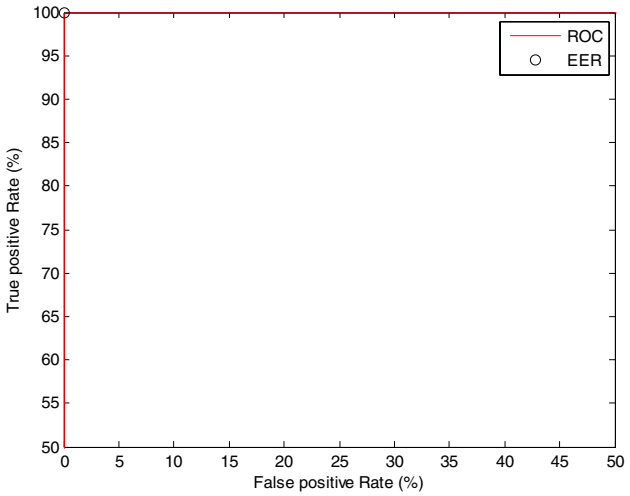


Fig. 66 ROC curve for the cancelable biometric scheme using circular encryption on the tested sample1 dataset

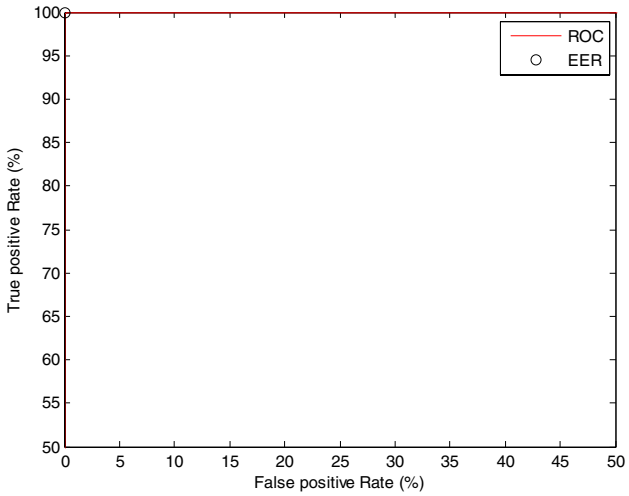


Fig. 68 ROC curve for the cancelable biometric scheme using IWT domain with different keys on the tested sample1 dataset

have been used in the tests as shown in Figs. 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 32, 33, 34, 35, 36, 37, 38, 39 and 40. Each face has 128 × 128 pixels. Figures 6, 13, 20, 27, and 34 show the original biometric templates of AT&T, YALE, UFI, LFW, and FERET datasets, respectively. Figures 7, 14, 21, 28, and 35 show the encrypted biometric templates using the equivalent kernels on the tested AT&T, YALE, UFI, LFW, and FERET datasets. The proposed image encryption scheme was used on different transform domains to create random kernels. The initial chaotic Baker map status is changed according to the PIN submitted by each user. Finally, all encryption domains are compared to each other.

During the enrollment phase, each user enters his personal PIN, which gives an equivalent kernel to convolve with the training face. The resulting encrypted biometric patterns are put in storage in the system database. During the verification stage, two faces are considered. One belongs to an authorized user and the other to an unauthorized user. In both cases, test users log in using the PIN to create a random convolution kernel for encryption. An authorized user is assumed to know the correct PIN. Correlation coefficients between a new encrypted face and those in the database are calculated. Finally, as shown in Figs. 8, 9, 10, 11, 12, 15, 16, 17, 18, 19, 22, 23, 24, 25, 26, 29, 30, 31, 32, 33, 36, 37, 38, 39 and 40, it is easy to plot two-dimensional curves, PTD and PFD, for specific encryption algorithms across different domains to determine the limitations and

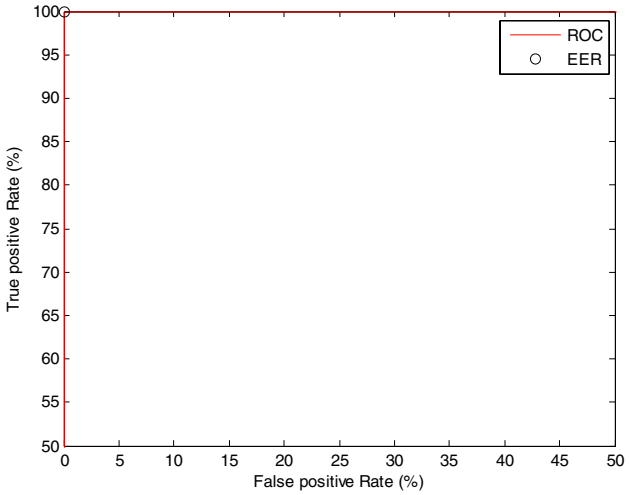


Fig. 69 ROC curve for the cancelable biometric scheme using DWT domain on the tested sample1 dataset

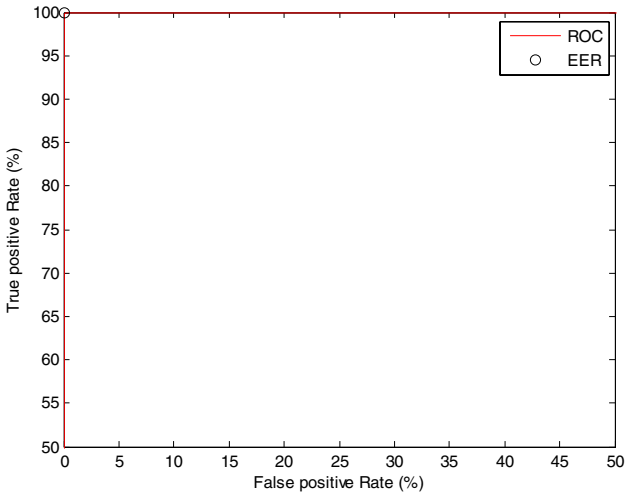


Fig. 70 ROC curve for the cancelable biometric scheme using DWT domain with different keys on the tested sample1 dataset

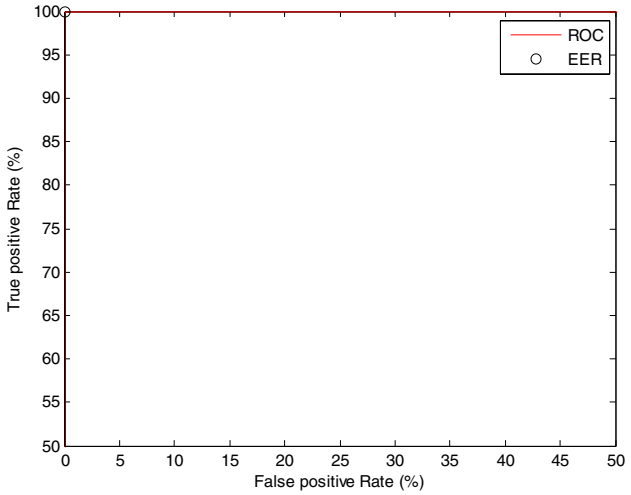


Fig. 71 ROC curve for the cancelable biometric scheme using circular encryption on the tested sample2 dataset

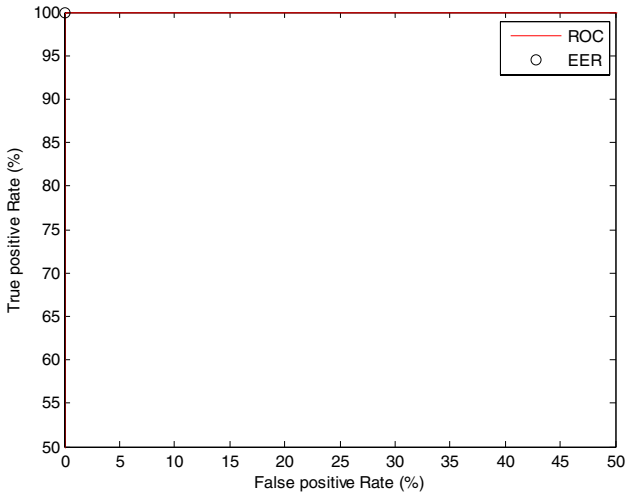


Fig. 72 ROC curve for the cancelable biometric scheme using IWT domain on the tested sample2 dataset

error probability. The intersection between the two curves determines the entry value used to determine whether this user is an authorized user or not.

The separation between PTD and PFD for authorized and unauthorized users is sufficiently great and increased for the YALE dataset. The PTD and PFD plots of AT&T, YALE, UFI, and FERET dataset are better than those of LFW dataset. The variation of illumination, pose and expression in AT&T, YALE, UFI, and FERET datasets is suitable for our proposed schemes, which is not achieved for the LFW dataset due to the background effect. It is noticed also that the correlation scores for authorized users approach one and for unauthorized users approach zero.

5 Comparative study between the proposed encryption schemes in different encryption domains

This section discusses the effect of the chaotic Baker map in different transform domains on the mean values of the authorized patterns, the threshold values, the error probability, and the authentication time on the tested AT&T, YALE, UFI, LFW and FERET face datasets as shown in Tables 1, 2, 3, 4 and 5, respectively.

The error probability changes according to the domain. It is noticed from the presented results that the DWT domain encryption with different keys has the lowest probability of error among all tested domains. The mean values of the

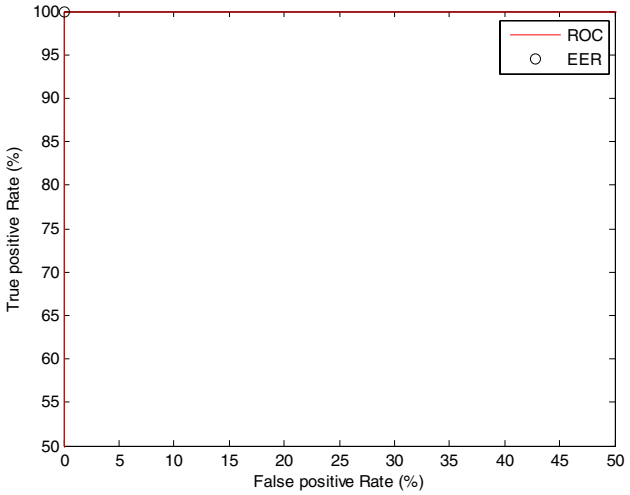


Fig. 73 ROC curve for the cancelable biometric scheme using IWT domain with different keys on the tested sample2 dataset

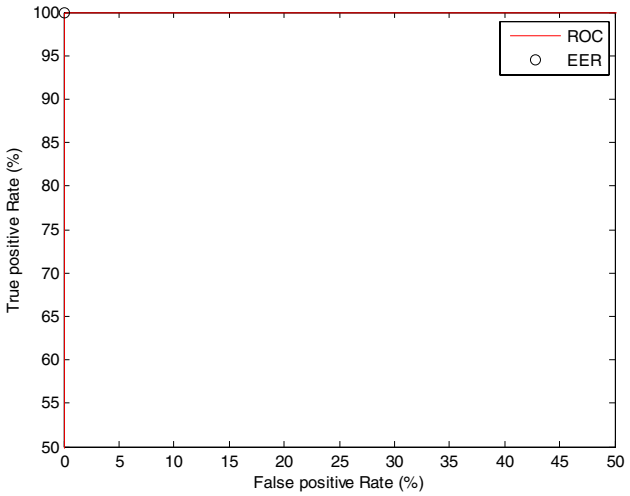


Fig. 74 ROC curve for the cancelable biometric scheme using DWT domain on the tested sample2 dataset

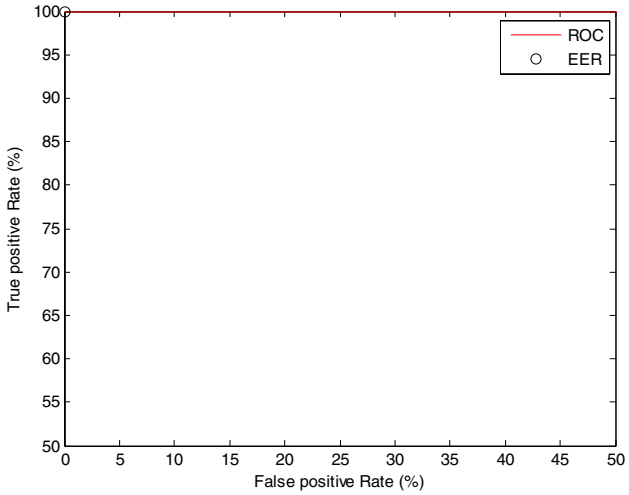


Fig. 75 ROC curve for the cancelable biometric scheme using DWT domain with different keys on the tested sample2 dataset

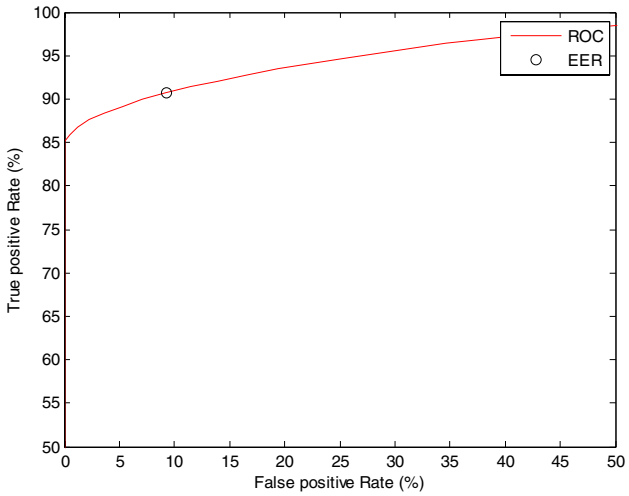


Fig. 76 ROC curve for the cancelable biometric scheme using circular encryption on the tested sample3 dataset

authorized/unauthorized patterns are nearly the same for all encryption domains. The difference in the threshold values between cancelable biometric schemes with different encryption domains is very small, because the convolution of the training templates with arbitrary convolution kernels generated from the chaotic map does not change the correlation output. Hence, the authentication truthfulness is kept. Furthermore, the proposed cancelable biometric recognition schemes have short authentication times over all the tested domains. In addition, various cancelable biometric patterns can be created from the same pattern by basically altering the PIN, which directly affects the chaotic Baker map, and consequently leads to adjustments in the convolution kernels.

In addition, the confidence of the functionality of a proposed cancelable biometric scheme is determined by some specific graphs and metrics such as the FRR vs FAR graph, the ROC curve, EER value, D_i and accuracy.

Figures 41, 42, 43, 44, 45, 46, 47, 48, 49, 50, 51, 52, 53, 54, 55, 56, 57, 58, 59, 60, 61, 62, 63, 64 and 65 show the performance of proposed system in terms of FRR and FAR for all encryption domains.

Figures 66, 67, 68, 69, 70, 71, 72, 73, 74, 75, 76, 77, 78, 79, 80, 81, 82, 83, 84, 85, 86, 87, 88, 89 and 90 show the ROC curve of the proposed method. The curve is obtained by plotting the true accept rate (*TAR*) against the false accept rate (*FAR*).

The *EER*, D_i and Accuracy results for the chaotic Baker map in different transform domains are tabulated in Tables 6,

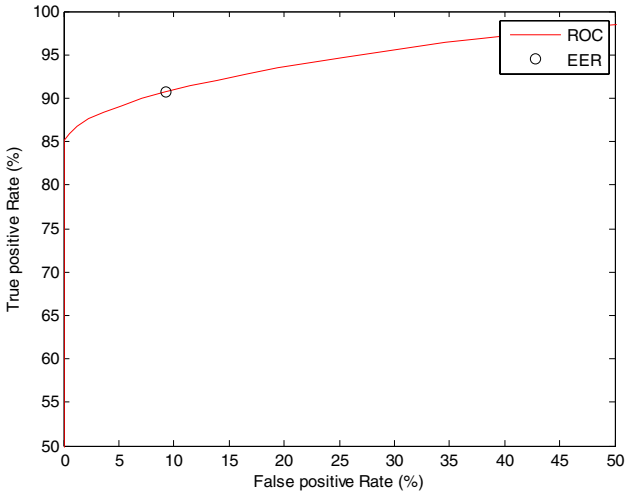


Fig. 77 ROC curve for the cancelable biometric scheme using IWT domain on the tested sample3 dataset

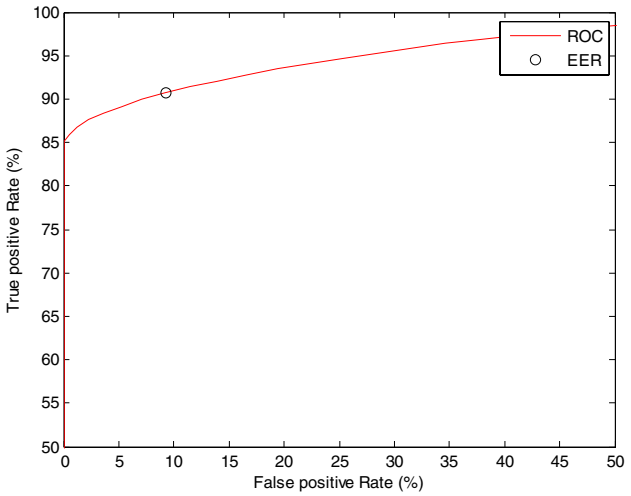


Fig. 78 ROC curve for the cancelable biometric scheme using IWT domain with different keys on the tested sample3 dataset

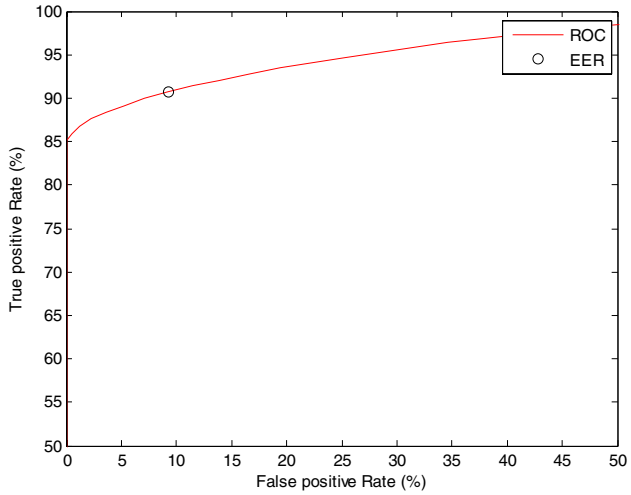


Fig. 79 ROC curve for the cancelable biometric scheme using DWT domain on the tested sample3 dataset

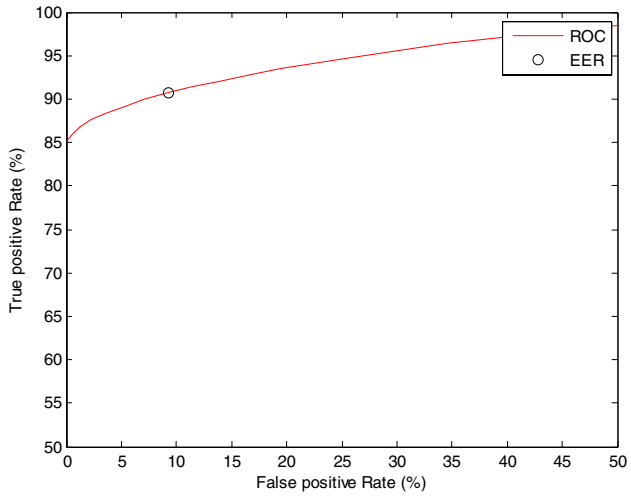


Fig. 80 ROC curve for the cancelable biometric scheme using DWT domain with different keys on the tested sample3 dataset

7, 8, 9 and 10 for the tested AT&T, YALE, UFI, LFW and FERET face datasets, respectively.

One can see that for the ATT and YALE datasets, the cancelable biometric scheme has an incredible performance of zero EER in all encryption domains and it has an ideal ROC curve. The larger the region covered by the ROC curve is, the better the performance of the scheme.

The D_i and the overall accuracy of the proposed scheme increase very much with AT&T, YALE, UFI, and FERET datasets. Hence, it can be concluded that the proposed scheme is robust to illumination, pose and expression variations.

The scheme proposed in this paper also provides template diversity, i.e., it is able to generate completely different cancelable templates from the same biometric for using them in various applications. This is achieved by changing the shuffling/transformation key. The two transformed templates generated from the same image using two different shuffling keys do not match with each other. In order to prove this characteristic, we carried out three experiments on all tested datasets with each proposed encryption domain: (1) each image is shuffled with different shuffling keys and the resultant shuffled images are compared with each other,

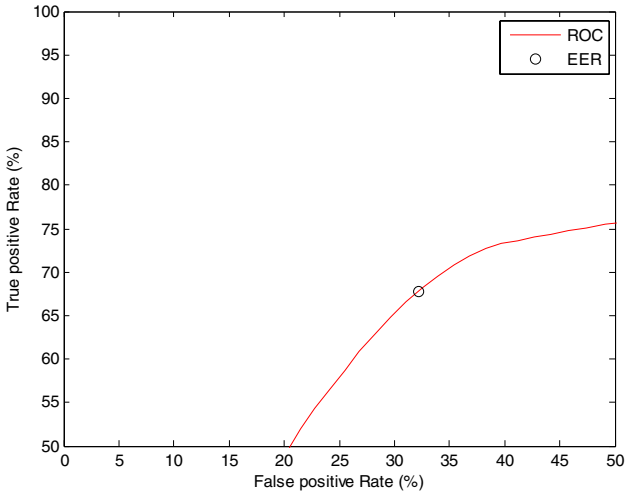


Fig. 81 ROC curve for the cancelable biometric scheme using circular encryption on the tested sample4 dataset

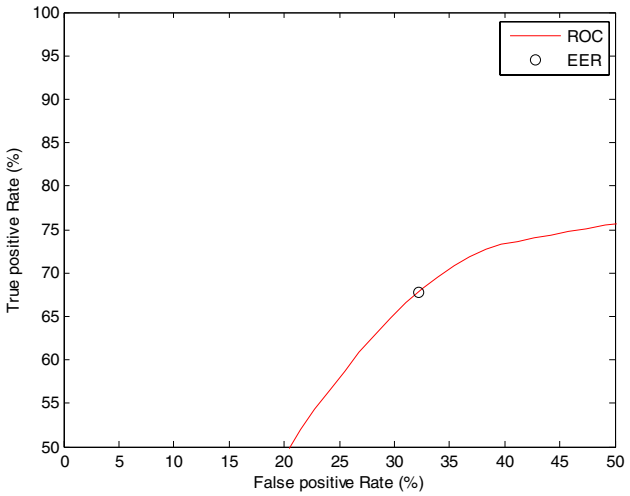


Fig. 82 ROC curve for the cancelable biometric scheme using IWT domain on the tested sample4 dataset

(2) one sample of the person is shuffled with different shuffling keys and the results are compared with each other, and (3) different samples of the same person are shuffled with different shuffling keys and the results are compared with each other. For comparison purposes, the distributions of the three experiments are shown in the same figure. The plots of the impostor Hamming distance distributions for the proposed scheme using the different encryption domains are shown in Figs. 91, 92, 93, 94, 95, 96, 97, 98, 99, 100, 101, 102, 103, 104, 105, 106, 107, 108, 109, 110, 111, 112, 113, 114 and 115. It is clear from the figures that the scheme can generate different templates for each user which are comparable with random image templates.

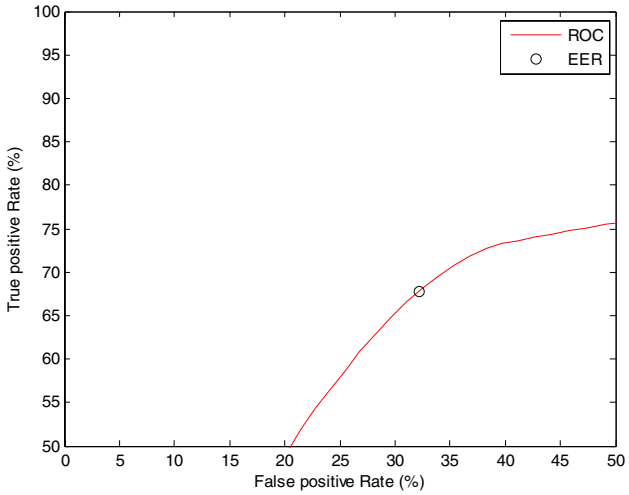


Fig. 83 ROC curve for the cancelable biometric scheme using IWT domain with different keys on the tested sample4 dataset

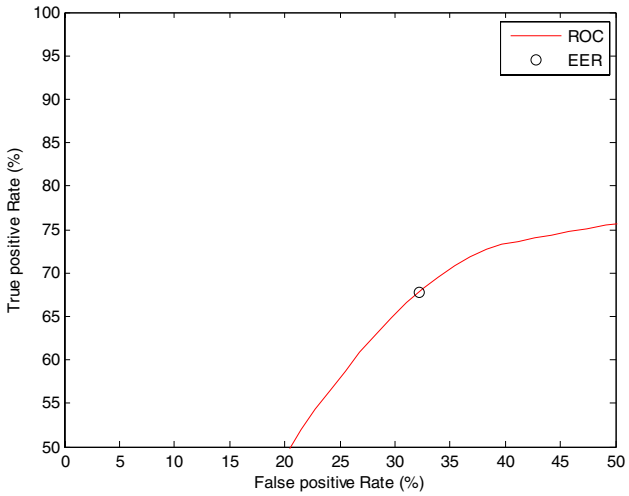


Fig. 84 ROC curve for the cancelable biometric scheme using DWT domain on the tested sample4 dataset

6 Comparative study between the proposed cancelable biometric scheme and other existing schemes

Tables 11, 12 and 13 present a cursory summary of a selection of different schemes from the literature with the one presented in this paper. The algorithms used for the comparison purpose are listed below:

Feng et al. (2010) proposed a hybrid approach based on random projection, Discriminability-Preserving (DP) transform, and fuzzy commitment scheme. Teoh et al. (2006) proposed a Random Multispace Quantization (RMQ) processing as an analytic mechanism for bio-hashing of biometrics and external random inputs. Kaur and Khanna (2015)

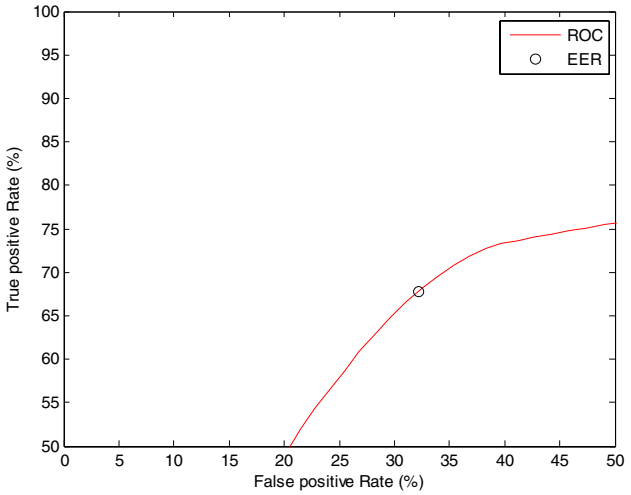


Fig. 85 ROC curve for the cancelable biometric scheme using DWT domain with different keys on the tested sample4 dataset

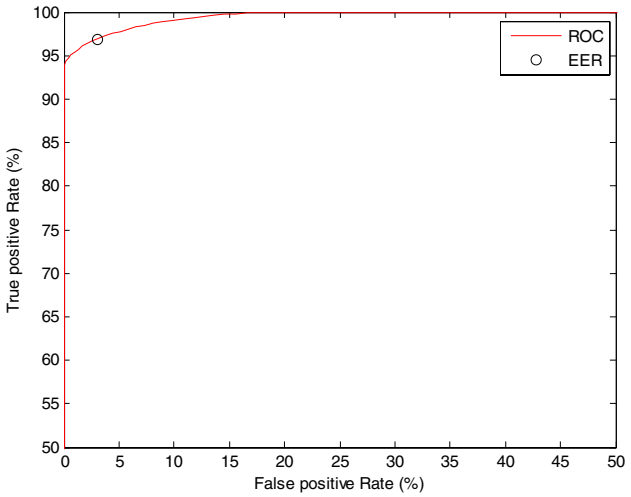


Fig. 86 ROC curve for the cancelable biometric scheme using circular encryption on the tested sample5 dataset

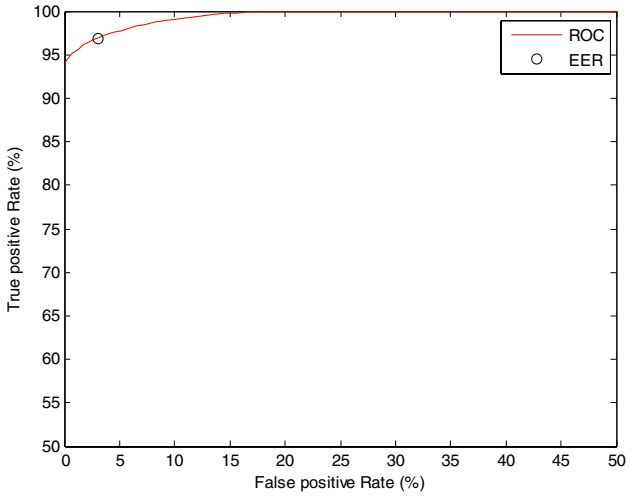


Fig. 87 ROC curve for the cancelable biometric scheme using IWT domain on the tested sample5 dataset

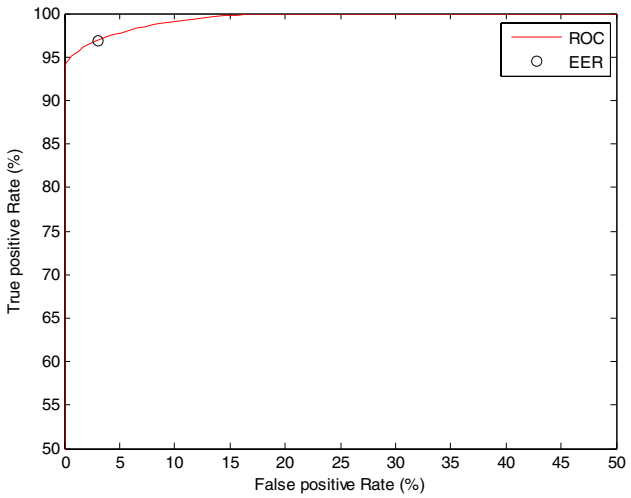


Fig. 88 ROC curve for the cancelable biometric scheme using IWT domain with different keys on the tested sample5 dataset

proposed random projection for generating cancelable templates of palmprint and face images. Syafeeza et al. (2014) proposed a robust four-layer Convolutional Neural Network (CNN) architecture for the face recognition problem. Lingli and Jianghuang (2010) proposed a security algorithm of face recognition, which is based on Local Binary Patterns (LBPs) and random projection. Nazari et al. (2014) proposed a novel face template protection scheme based on a biohashing and permutation approach. Kamencay et al. (2017) proposed a new method for face recognition using Convolutional Neural Networks (CNNs) with three well-known image recognition methods such as Principal Component Analysis (PCA), Local Binary Patterns Histograms (LBPH) and K–Nearest Neighbour (KNN) Abuzneid and Mahmood (2018) presented an enhanced approach to improve human face recognition using a Back-Propagation Neural Network (BPNN) and feature extraction based on the correlation between the training images. Mohammadzade et al. (2018) proposed pixel alignment rather than eye alignment as a pre-processing step by mapping the geometry of a face to a reference face, while keeping its own texture. Oloyede et al. (2018) proposed face recognition systems (FRS), which comprises an effective image enhancement technique for face image preprocessing, alongside a new set of hybrid features.

As compared to various schemes, the EERs of the proposed scheme on FERET and YALE databases are

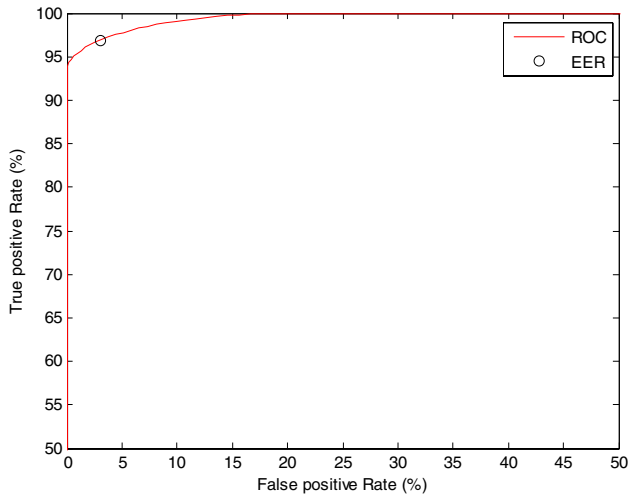


Fig. 89 ROC curve for the cancelable biometric scheme using DWT domain on the tested sample5 dataset

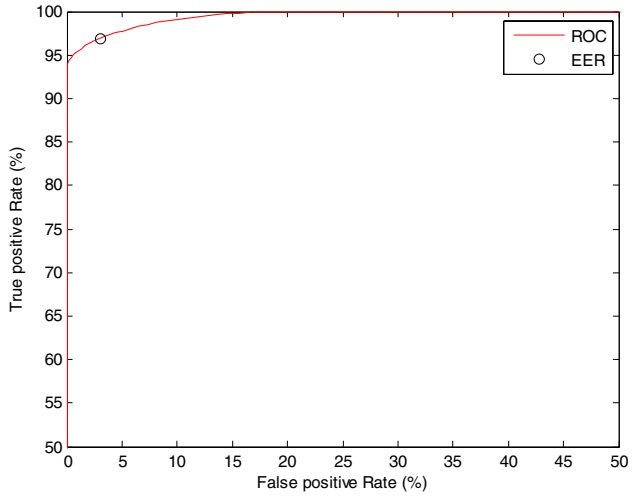


Fig. 90 ROC curve for the cancelable biometric scheme using DWT domain with different keys on the tested sample5 dataset

0.014976% and 0%, respectively. This is significantly better than the EER of the other algorithms of Feng et al. (2010), Teoh et al. (2006) and Kaur and Khanna (2015). Kaur et al. have achieved a D_i value of 4.568 for PCA and 5.936 for LDA, but these values are lower than those of our proposed scheme. Furthermore, we achieved the highest accuracy on FERET dataset. The accuracy of the proposed scheme is 96.77039%, whilst those of the schemes of Syafeeza et al. (2014) and Lingli and Jianghuang (2010) are 85.71% and 72%, respectively. On AT&T dataset, the proposed scheme is the best with an accuracy of 98.620%. The methods of Lingli and Jianghuang (2010), Abuzneid and Mahmood (2018) and Oloyede et al. (2018) have lower accuracies of 66%, 97.70%

Table 6 The encryption domain effect on AT&T images

Domain	FAR/FPR	FRR/FNR	EER	TAR	D_{ii}	Accuracy%
Spatial	0.00015	0.02715	0.0280	0.9728	3.9685	98.63
IWT	0.000149	0.0267	0.027859	0.97329	3.9624	98.657
IWT with various keys	0.00015	0.0274	0.02734	0.97257	3.9876	98.620
DWT	0.000149	0.0267	0.02785	0.97329	3.9624	98.657
DWT with various keys	0.000151	0.02743	0.02733	0.9725	3.9881	98.620

Table 7 The encryption domain effect on YALE images

Domain	*FAR/FPR*	*FRR/FNR*	*EER*	*TAR*	D_i	*Accuracy %*
Spatial	0.00022	0.0338	0	0.96614	6.4050	98.2956
IWT	0.000227	0.0339	0	0.9660	6.4231	98.29333
IWT with various keys	0.00023	0.03357	0	0.96642	6.3823	98.309435
DWT	0.000227	0.0339	0	0.96609	6.4231	98.293331
DWT with various keys	0.0002321	0.033576	0	0.966423	6.3811	98.30956

Table 8 The encryption domain effect on UFI images

Domain	*FAR/FPR*	*FRR/FNR*	*EER*	*TAR*	D_i	*Accuracy %*
Spatial	0.000315	0.174	0.04899	0.8259	1.2412	91.283
IWT	0.000326	0.175066	0.04959	0.82493	1.2463	91.2303
IWT with various keys	0.00035	0.17591	0.0483	0.8240	1.2494	91.1864
DWT	0.00032	0.17506	0.049596	0.82493	1.2463	91.230
DWT with various keys	0.000351	0.17591	0.0482699	0.824083	1.2499	91.18657

Table 9 The encryption domain effect on LFW images

Domain	*FAR/FPR*	*FRR/FNR*	*EER*	*TAR*	D_i	*Accuracy %*
Spatial	0.000315	0.41572	0.0858	0.58427	0.2755	79.1982
IWT	0.000318	0.417854	0.0867	0.58214	0.2820	79.0913
IWT with various keys	0.000314	0.41744	0.0868	0.58255	0.2854	79.1118
DWT	0.000318	0.41785	0.08676	0.58214	0.2820	79.0913
DWT with various keys	0.000314	0.41749	0.0868	0.5825	0.2854	79.10954

Table 10 The encryption domain effect on FERET images

Domain	*FAR/FPR*	*FRR/FNR*	*EER*	*TAR*	D_i	*Accuracy %*
Spatial	0.000183	0.06183	0.01581	0.93816	3.9421	96.8991
IWT	0.00018368	0.0613	0.016158	0.938696	3.9743	96.9256
IWT with various keys	0.00018362	0.064336	0.0150	0.93566	3.9114	96.7740
DWT	0.0001836	0.06130	0.01615	0.9386962	3.9743	96.92562
DWT with various keys	0.0001836	0.06440	0.014976	0.93559	3.9097	96.77039

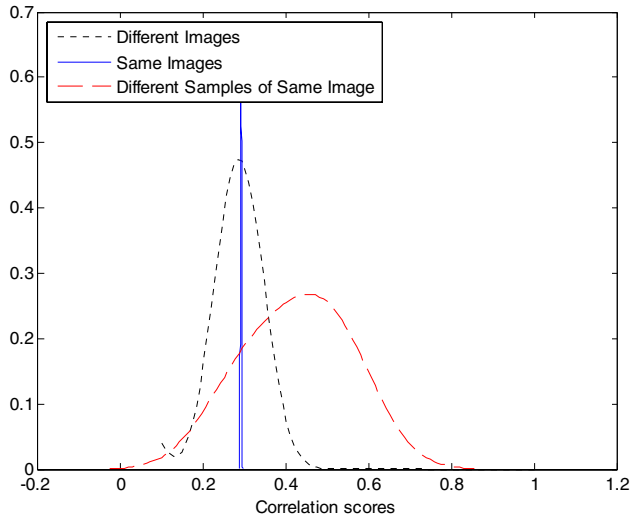


Fig. 91 Impostor Hamming distance distributions for the proposed cancelable biometric scheme using circular encryption on the tested sample1 dataset

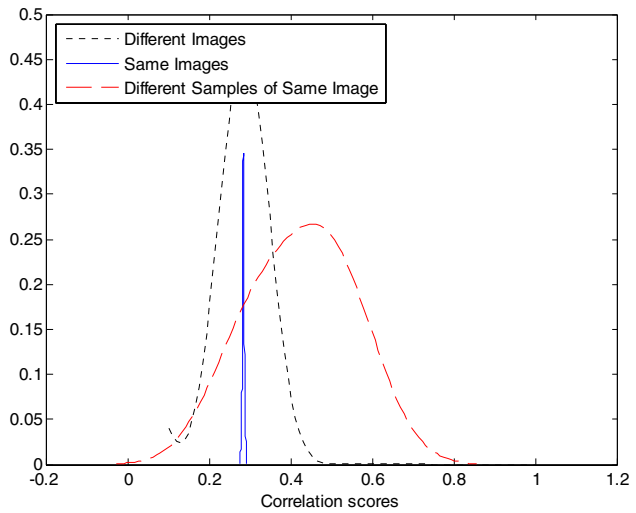


Fig. 92 Impostor Hamming distance distributions for the proposed cancelable biometric scheme using IWT domain on the tested sample1 dataset

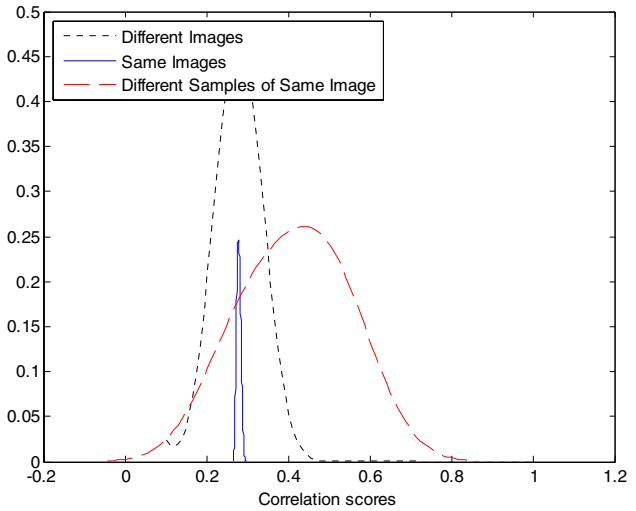


Fig. 93 Impostor Hamming distance distributions for the proposed cancelable biometric scheme using IWT domain with different keys on the tested sample1 dataset

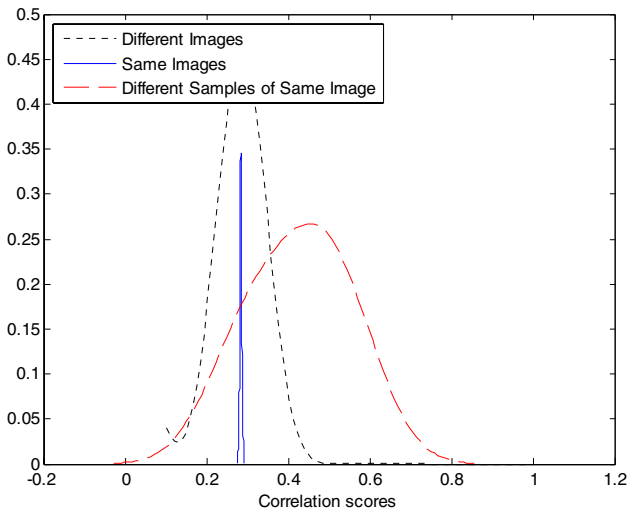


Fig. 94 Impostor Hamming distance distributions for the proposed cancelable biometric scheme using DWT domain on the tested sample1 dataset

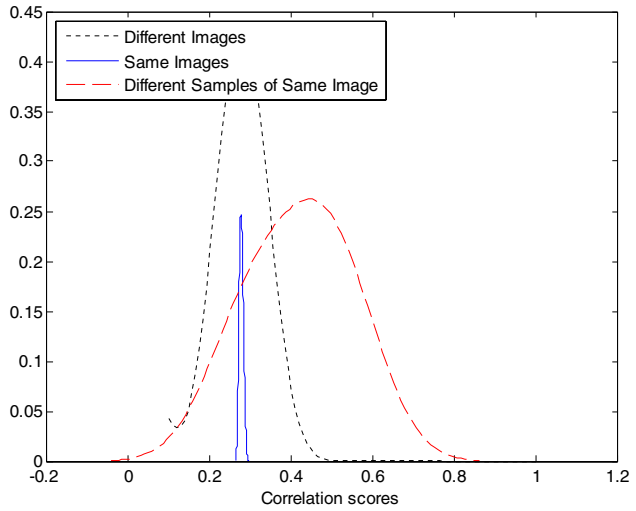


Fig. 95 Impostor Hamming distance distributions for the proposed cancelable biometric scheme using DWT Domain with different keys on the tested sample1 datasetc

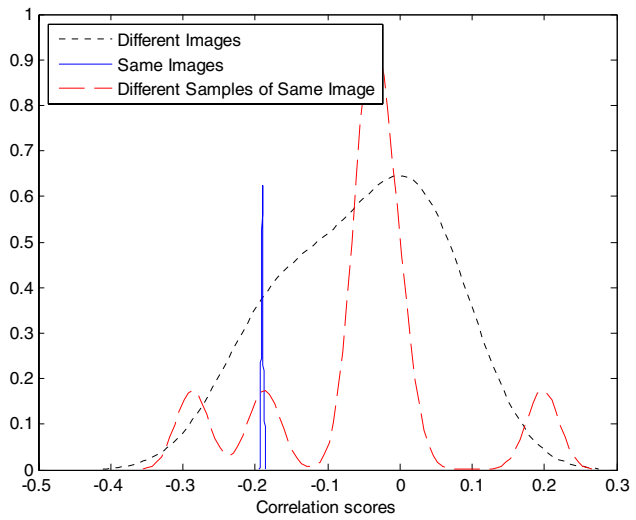


Fig. 96 Impostor Hamming distance distributions for the proposed cancelable biometric scheme using circular encryption on the tested sample2 dataset

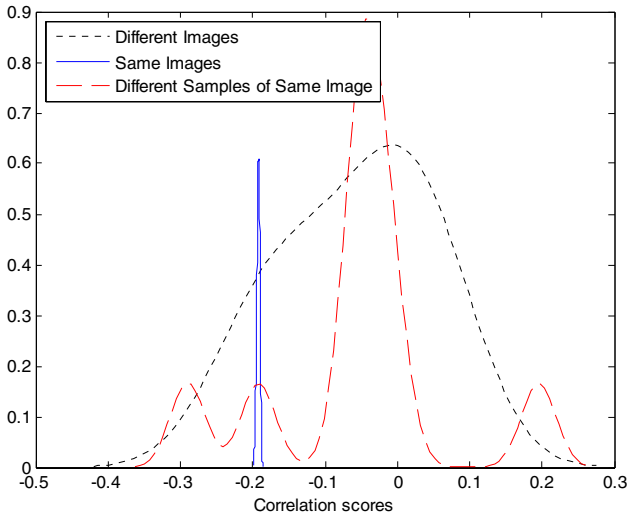


Fig. 97 Impostor Hamming distance distributions for the proposed cancelable biometric scheme using IWT domain on the tested sample2 dataset

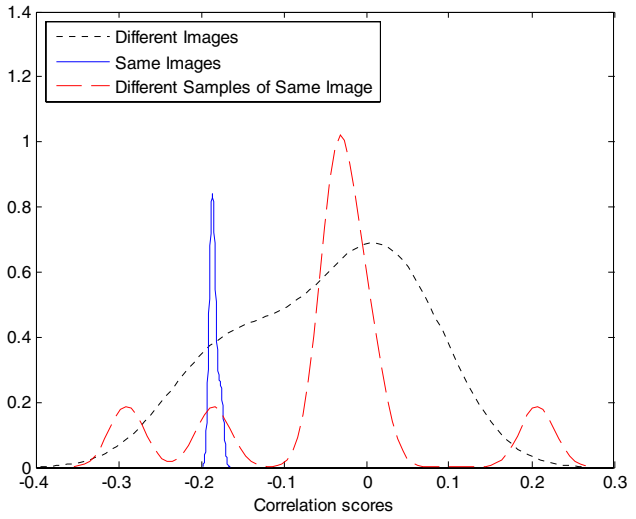


Fig. 98 Impostor Hamming distance distributions for the proposed cancelable biometric scheme using IWT domain with different keys on the tested sample2 dataset

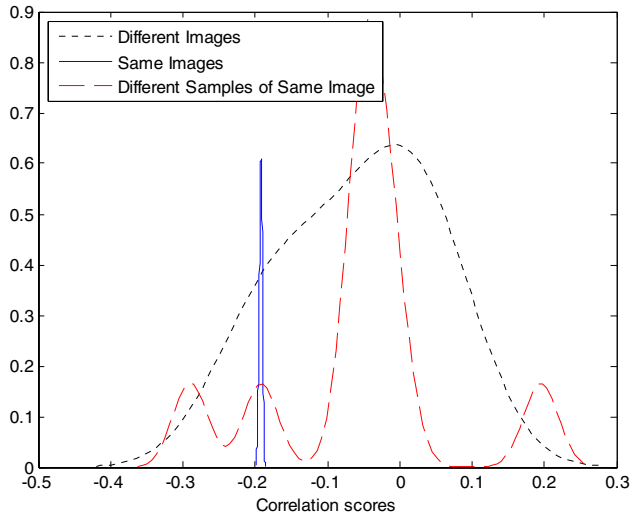


Fig. 99 Impostor Hamming distance distributions for the proposed cancelable biometric scheme using DWT domain on the tested sample2 dataset

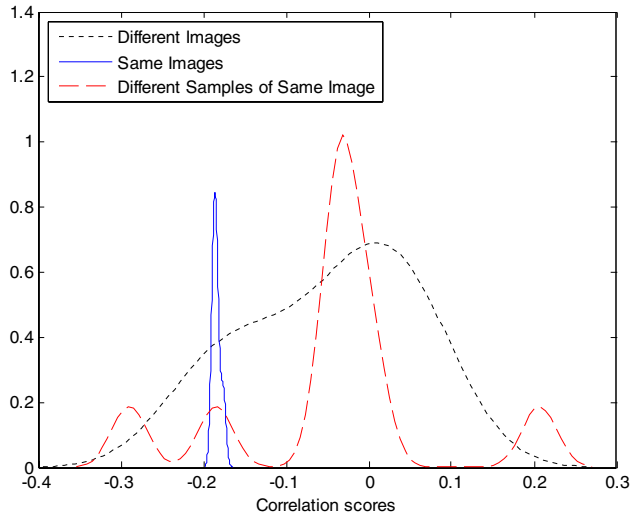


Fig. 100 Impostor Hamming distance distributions for the proposed cancelable biometric scheme using DWT domain with different keys on the tested sample2 dataset

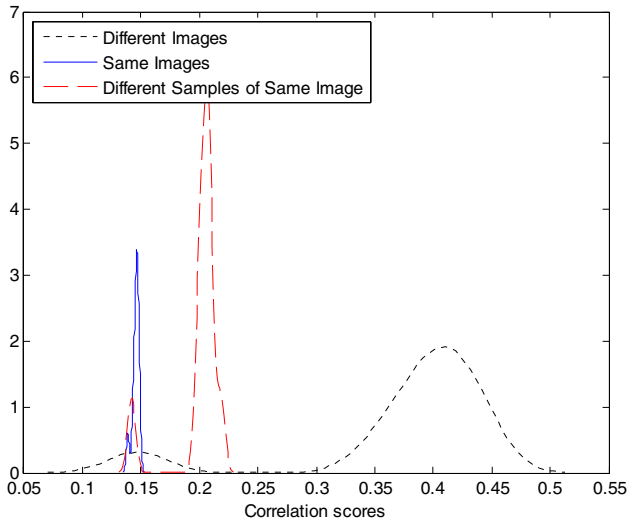


Fig. 101 Impostor Hamming distance distributions for the proposed cancelable biometric scheme using circular encryption on the tested sample3 dataset

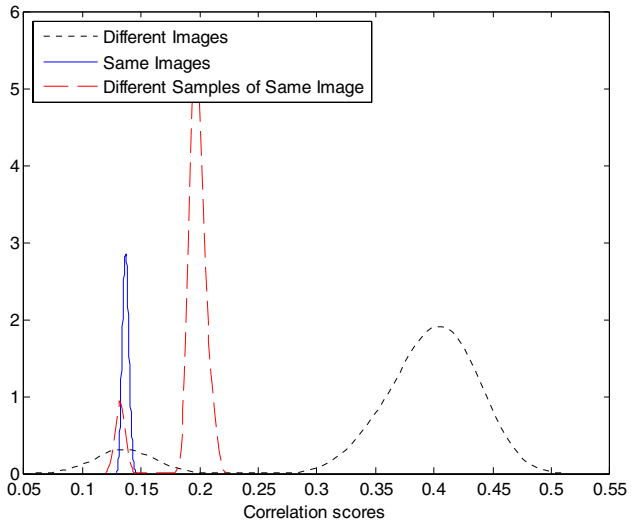


Fig. 102 Impostor Hamming distance distributions for the proposed cancelable biometric scheme using IWT domain on the tested sample3 dataset

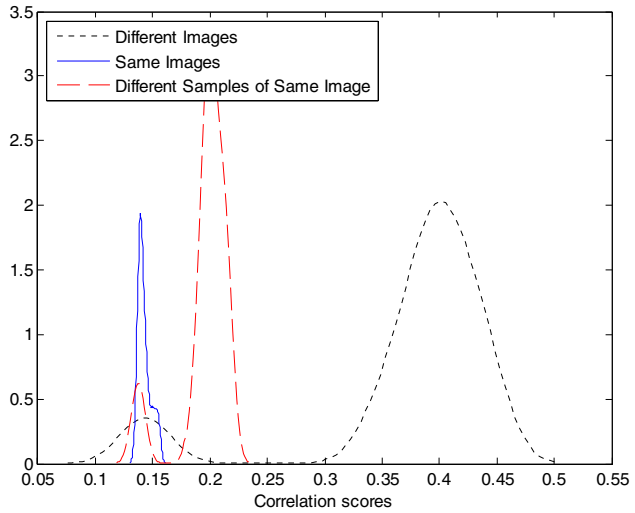


Fig. 103 Impostor Hamming distance distributions for the proposed cancelable biometric scheme using IWT domain with different keys on the tested sample3 dataset

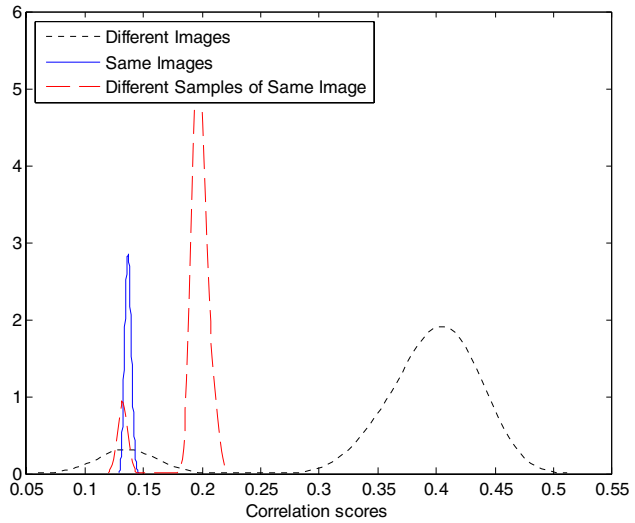


Fig. 104 Impostor Hamming distance distributions for the proposed cancelable biometric scheme using DWT domain on the tested sample3 dataset

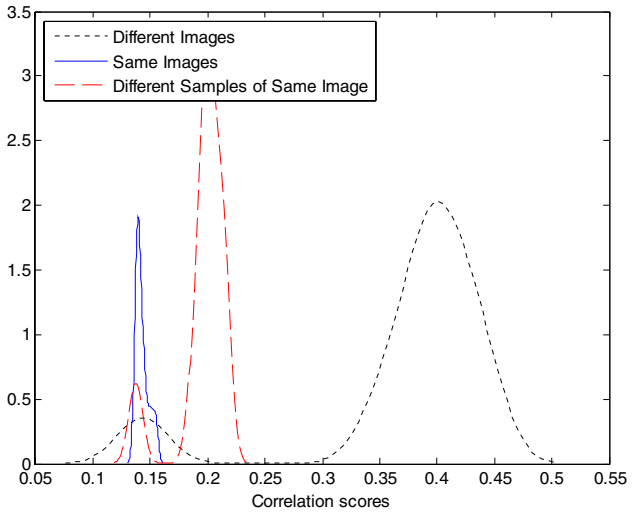


Fig. 105 Impostor Hamming distance distributions for the proposed cancelable biometric scheme using DWT Domain with different keys on the tested sample3 dataset

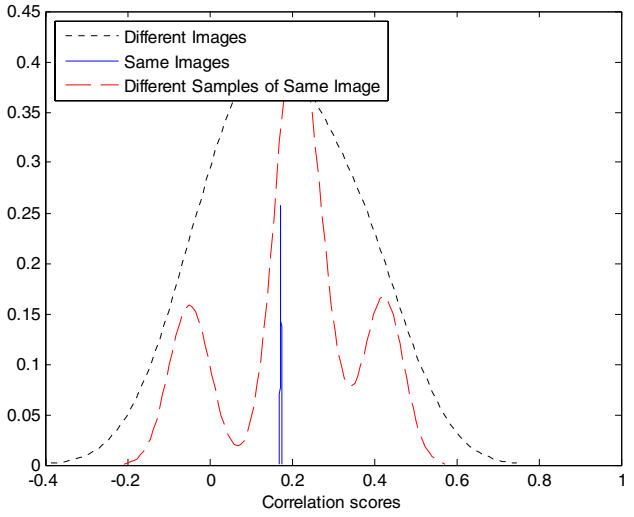


Fig. 106 Impostor Hamming distance distributions for the proposed cancelable biometric scheme using circular encryption on the tested sample4 dataset

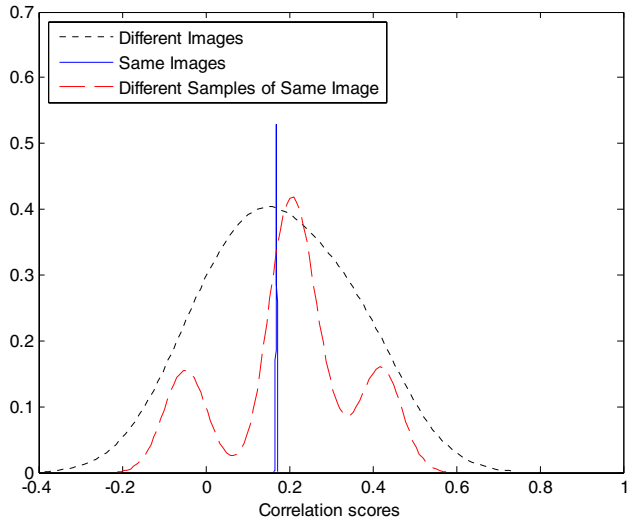


Fig. 107 Impostor Hamming distance distributions for the proposed cancelable biometric scheme using IWT domain on the tested sample4 dataset

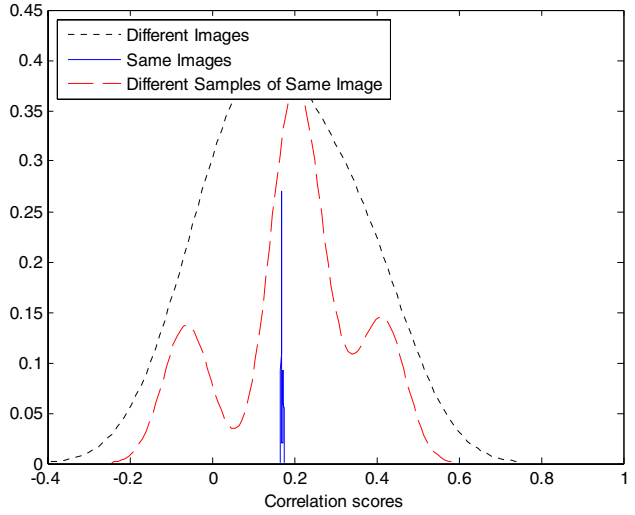


Fig. 108 Impostor Hamming distance distributions for the proposed cancelable biometric scheme using IWT domain with different keys on the tested sample4 dataset

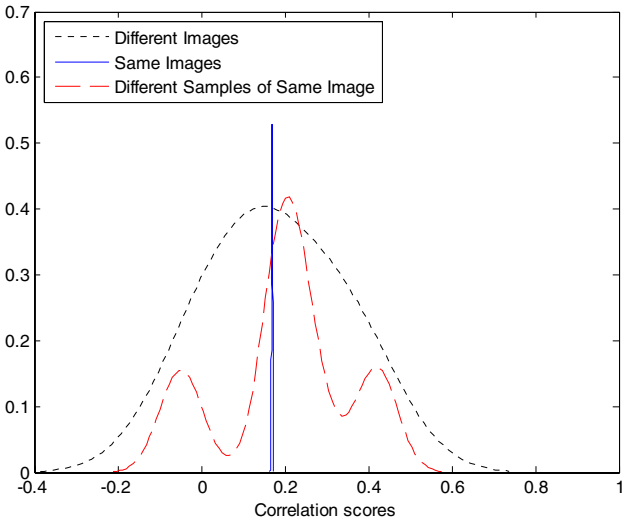


Fig. 109 Impostor Hamming distance distributions for the proposed cancelable biometric scheme using DWT domain on the tested sample4 dataset

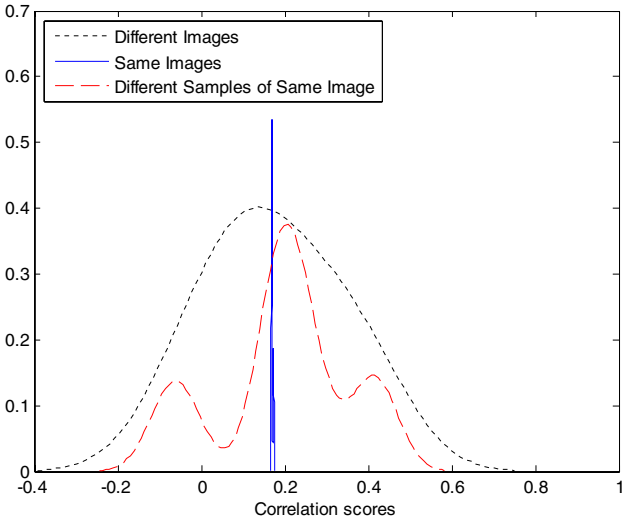


Fig. 110 Imposter Hamming distance distributions for the proposed cancelable biometric scheme using DWT domain with different keys on the tested sample4 dataset

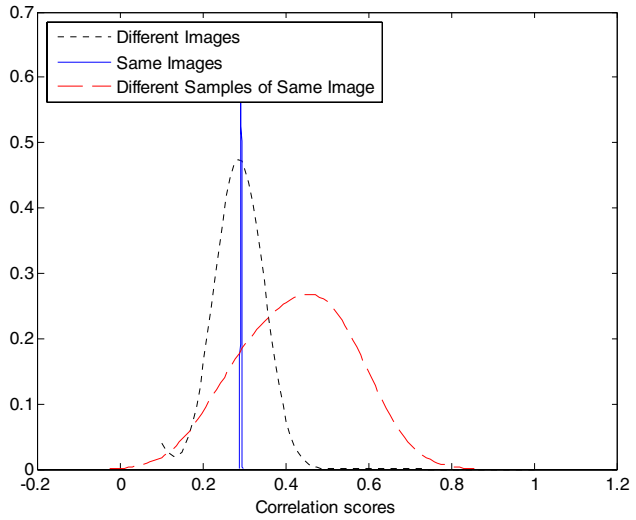


Fig. 111 Imposter Hamming distance distributions for the proposed cancelable biometric scheme using circular encryption on the tested sample5 dataset

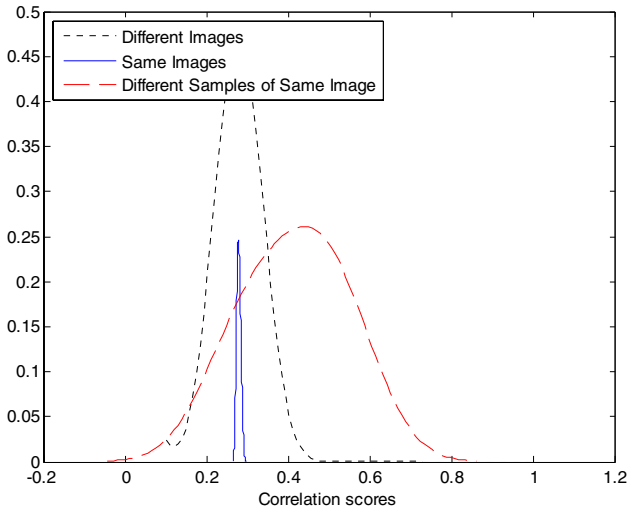


Fig. 113 Imposter Hamming distance distributions for the proposed cancelable biometric scheme using IWT domain with different keys on the tested sample5 dataset

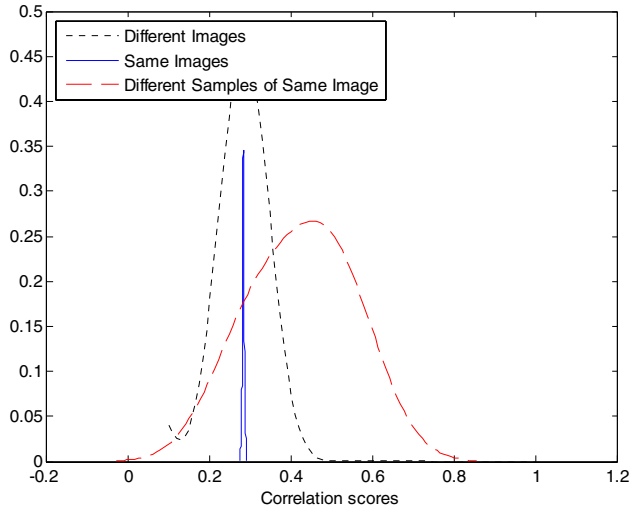


Fig. 112 Imposter Hamming distance distributions for the proposed cancelable biometric scheme using IWT domain on the tested sample5 dataset

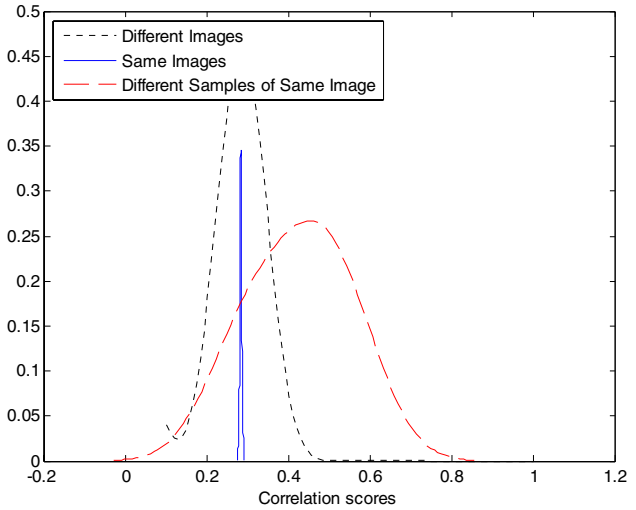


Fig. 114 Imposter Hamming distance distributions for the proposed cancelable biometric scheme using DWT domain on the tested sample5 dataset

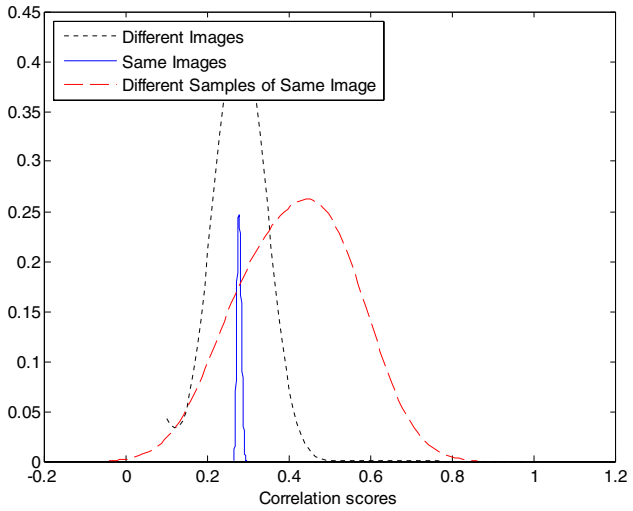


Fig. 115 Imposter Hamming distance distributions for the proposed cancelable biometric scheme using DWT domain with different keys on the tested sample5 dataset

Table 11 EER comparison of the proposed scheme with other ones

Author(s)	Dataset	*EER*	Proposed scheme
Feng et al. (2010)	FERET	8.55%	0.014976%
Teoh et al. (2006)	FERET	12.83%	
Kaur and Khanna (2015)	YALE	0.03% for PCA 0.08% for LDA	0

Table 12 D_i comparison with various cancelable biometric schemes

Author(s)	Dataset	D_i	Proposed scheme
Kaur and Khanna (2015)	YALE	4.568 for PCA 5.936 for LDA	6.3811

and 94.60% on YALE dataset, respectively. Our proposed scheme gives the highest accuracy of 98.30956%. This comparison shows that the proposed scheme has a superior performance in handling variations in illumination, occlusion and facial expressions and it could be applied on different datasets.

7 Conclusions and future work

Encryption or hashing methods are often used to protect biometric templates. There are two problems with these methods. First, the encrypted biometrics must be decrypted for matching. If they are decrypted, this opens the door for hackers to attack the decryption point. In the case of hash functions, secure hash matching is very sensitive to any slight changes in the input user biometric. In practice, all user biometric patterns are adapted according to environmental circumstances. Therefore, these functions cannot be used directly. The novelty of this paper is that it introduces the hypothesis of cancelable biometrics as an answer to the previous two challenges. The proposed cancelable biometric scheme allows us to create numerous encrypted biometric templates, which can be reproduced in different domains using different convolution kernels created by the chaotic Baker map. Our proposed scheme has superior performance in handling variations in illumination, occlusion and facial expressions. The same approach can be applied on different datasets. This allows verification immediately in the ciphered domains. The simulation results show that an arbitrary confusion kernel can be utilized. Additionally, this pre-processing step does not affect the authentication performance. Verification in encryption domains helps to protect the biometrics during the authentication phase from attempts to steal decrypted images. Although the attacker succeeds in stealing the biometric templates, he needs a key for the decryption and retrieval process. The effect of chaotic maps in different

Table 13 Accuracy comparison with various cancelable biometric schemes

Author(s)	Database	Accuracy	Proposed scheme
Syafeeza et al. (2014)	FERET	85.71%	96.77039%
Lingli and Jianghuang 2010	FERET	72%	
	AT&T(ORL)	93%	98.620%
Nazari et al. (2014)	AT&T(ORL)	58.5% for PCA 67.4% for LDA	
Kamencay et al. (2017)	AT&T(ORL)	98.30%	
Abuzneid and Mahmood (2018)	AT&T(ORL)	98.00%	
Mohammadzade et al. (2018)	AT&T	94.00%	
Lingli and Jianghuang (2010)	YALE	66%	98.30956%
Abuzneid and Mahmood (2018	YALE	97.70%	
Oloyede et al. (2018)	YALE	94.60%	

domains on the widely-used AT&T, YALE, UFI, LFW, and FERET datasets has been studied in detail. From the submitted results, the cancelable biometric system using encryption in the DWT domain is the best choice. In average, we achieved a 2% error probability, a 0.3 s authentication time, a 0.02% False Rejection Rate *(FRR)*, a 0% False Acceptance Rate *(FAR)*, a 0.0% Equal Error Rate *(EER)* and a 98.43% accuracy. Our proposed scheme also provides template diversity.

In our future research project, we will implement a multi-stage cancelable user biometric protection framework with various steganography and ciphering algorithms along with hiding schemes for trustworthy biometric storage. In addition, we are motivated to incorporate in-depth practice-based reversible security applications for biometric storage and transmission.

Acknowledgements The authors would like to thank the Deanship of Scientific Research, Taif University Researchers Supporting Project number (TURSP-2020/08), Taif University, Taif, Saudi Arabia for supporting this research work.

Funding This study was funded by the Deanship of Scientific Research, Taif University Researchers Supporting Project number (TURSP-2020/08), Taif University, Taif, Saudi Arabia.

References

Abuzneid MA, Mahmood A (2018) Enhanced human face recognition using LBPH descriptor, multi-KNN, and BPNN. IEEE Access 6:20641–20651

Ali M, Tahir N (2018) Cancelable biometrics technique for iris recognition. In: IEEE symposium on computer applications and industrial electronics (ISCAIE), pp 434–437

Ao M, Li S (2009) Near infrared face based biometric key binding. In: International conference on biometrics, Springer, Berlin, Heidelberg, pp 376–385

Arigbabu OA et al (2016) Smile detection using hybrid face representation. J Ambient Intell Humaniz Comput 7:1–12

Cheung K, Kong A, You J, Zhang D (2005) An analysis on invertibility of cancelable biometrics based on biohashing. In: IEEE CISST, pp 40–45

Connie T, Teoh A, Goh M, Ngo D (2005) Palmhashing: a novel approach for cancelable biometrics. Inf Process Lett 93(1):1–5

Technical Document About FAR, FRR and ERR (2004) Version 1.0. © 2004 by SYRIS Technology Corporation

Dong Y, Su H, Wu B, Li Z, Liu W et al. (2019) Efficient decision-based black-box adversarial attacks on face recognition. In: The IEEE conference on computer vision and pattern recognition (CVPR)

Enerstvedt O (2017) Analysis of privacy and data protection principles. In: Enerstvedt OM (ed) Aviation security, privacy, data protection and other human rights: technologies and legal principles. Springer, Cham, pp 307–394

Feng Y, Yuen P, Jain A (2010a) A hybrid approach for generating secure and discriminating face template. IEEE Trans Inf Forensics Secur 5(1):103–117

Gaddam S, Lal M (2010) Efficient cancelable biometric key generation scheme for cryptography. IJ Netw Secur 11(2):61–69

Gao H, Zhang Y, Liang S, Li D (2006) A new chaotic algorithm for image encryption. Chaos Solitons Fractals 29(2):393–399

Gowthami A, Mamatha H (2015) Fingerprint recognition using zone based linear binary patterns. Proc Comput Sci 58:552–557

Grassi M, Faundez M (2009) Protecting DCT templates for a face verification system by means of pseudo-random permutations. In: International work-conference on artificial neural networks, Springer, Berlin, Heidelberg, pp 1216–1223

Guan Z, Huang F, Guan W (2005) Chaos-based image encryption algorithm. Phys Lett A 346(1–3):153–157

He W, Wang E, Xiong T (2013) Intelligent face recognition based on manifold learning and genetic-chaos algorithm optimized Kernel extreme learning machine. J Commun 8(10):658–664

Huang F, Qu X (2011) Design of image security system based on chaotic maps group. J Multimed 6(6):510

Huh J (2017) PLC-based design of monitoring system for ICT-integrated vertical fish farm. HCIS 7(1):20

Huh J (2018) Big data analysis for personalized health activities: machine learning processing for automatic keyword extraction approach. Symmetry 10(4):93

Jain A, Ross A, Prabhakar S (2004) An introduction to biometric recognition. IEEE Trans Circuits Syst Video Technol 14(1):4–20

Jain A, Bolle R, Pankanti S (2006) Biometrics: personal identification in networked society. Springer, Berlin, p 479

Jegede A, Udzir N, Abdullah A, Mahmod R (2017) Cancelable and hybrid biometric cryptosystems: current directions and open research issues. Int J Adv Appl Sci 4:65–77

Jeong M, Teoh A (2010) Cancellable face biometrics system by combining independent component analysis coefficients. In: International workshop on computational forensics, Springer, Berlin, Heidelberg, pp 78–87

Jiang R, Al-Maadeed S, Bouridane A, Crookes D, Celebi M (2016) Face recognition in the scrambled domain via salience-aware ensembles of many kernels. IEEE Trans Inf Forensics Secur 11(8):1807–1817

Jianjun Wu, Sun X, Wang Z (2019) Shearlet feature manifold for face recognition. J Ambient Intell Humaniz Comput 10(9):3453–3460

Jin X, Liu Y, Li X, Zhao G, Chen Y, Guo K (2015) Privacy preserving face identification in the cloud through sparse representation. In: Chinese conference on biometric recognition, Springer, Cham, pp 160–167

Jin Z, Teoh A, Goi B, Tay Y (2016) Biometric cryptosystems: a new biometric key binding and its implementation for fingerprint minutiae-based representation. Pattern Recogn 1(56):50–62

Jung S, Huh J (2019) A novel on transmission line tower big data analysis model using altered K-means and ADQL. Sustainability 11(13):3499

Kamencay P et al (2017) A new method for face recognition using convolutional neural network. Digit Image Process Comput Graph 15(4):663–672

Kaur H, Khanna P (2015) Gaussian random projection based non-invertible cancelable biometric templates. Proc Comput Sci 1(54):661–670

Khan M, Zhang J, Wang X (2008) Chaotic hash-based fingerprint biometric remote user authentication scheme on mobile devices. Chaos Solitons Fractals 35(3):519–524

Khan M, Xie L, Zhang J (2010) Chaos and NDFT-based spread spectrum concealing of fingerprint-biometric data into audio signals. Digit Signal Process 20(1):179–190

Kim Y, Toh K (2007) A method to enhance face biometric security. In: First IEEE international conference on biometrics: theory, applications, and systems, pp 1–6

Le Q, Ngiam J, Coates A, Lahiri A, Prochnow B, Ng A (2011) On optimization methods for deep learning. In: Proceedings of the 28th international conference on international conference on machine learning, Omnipress, pp 265–272

Lingli Z, Jianghuang L (2010) Security algorithm of face recognition based on local binary pattern and random projection. In: Cognitive informatics (ICCI), vol 9, IEEE, pp 733–738

Liu H et al. (2019) AdaptiveFace: adaptive margin and sampling for face recognition. In: IEEE conference on computer vision and pattern recognition, pp 11947–11956

Lu Y, Li L, Peng H, Yang Y (2015) An enhanced biometric-based authentication scheme for telecare medicine information systems using elliptic curve cryptosystem. J Med Syst 39(3):1–32

Lumini A, Nanni L (2007) An improved biohashing for human authentication. Pattern Recogn 40(3):1057–1065

Ma Y, Wu L, Gu X, He J, Yang Z (2017) A secure face-verification scheme based on homomorphic encryption and deep neural networks. IEEE Access 5:16532–16538

Manzoor S, Selwal A (2018) An analysis of biometric based security systems. In: IEEE Fifth international conference on parallel, distributed and grid computing (PDGC), pp 306–311

Mohammadzade H et al (2018) Pixel-level alignment of facial images for high accuracy recognition using ensemble of patches. J Opt Soc Am A 35(7):1149–1159

Moujahdi C, Ghouzali S, Mikram M, Rziza M, Bebis G (2012) Spiral cube for biometric template protection. In: International conference on image and signal processing, Springer, Berlin, Heidelberg, pp 235–244

Nandakumar K, Jain A (2015) Biometric template protection: bridging the performance gap between theory and practice. IEEE Signal Process Mag 32(5):88–100

Nazari S, Moin MS, Kanan HR (2014) Cancelable face using chaos permutation. In: International symposium on telecommunications (IST), vol 7, IEEE, pp 925–928

Oloyede MO et al (2018) Improving face recognition systems using a new image enhancement technique, hybrid features and the convolutional neural network. IEEE Access 6:75181–75191

Osadchy M, Pinkas B, Jarrous A, Moskovich B (2010) Scifi-a system for secure face identification. In: IEEE symposium on security and privacy, pp 239–254

Patel V, Ratha N, Chellappa R (2015a) Cancelable biometrics: a review. IEEE Signal Process Mag 32(5):54–65

Połap D (2018) Model of identity verification support system based on voice and image samples. J Univ Comput Sci 24(4):460–474

Połap D, Woźniak M et al (2019) Bio-inspired voice evaluation mechanism. Appl Soft Comput 80:342–357

Qiu J, Li H, Dong J (2018) Design of cancelable palmprint templates based on look up table. IOP Conf Ser Mater Sci Eng IOP Publ 322(5):50–52

Rachapalli D, Kalluri H (2017) A survey on biometrie template protection using cancelable biometric scheme. In: IEEE second international conference on electrical, computer and communication technologies (ICECCT), pp 1–4

Rajpoot Q, Jensen C (2014) Security and privacy in video surveillance: requirements and challenges. In: International information security conference, Springer, Berlin, Heidelberg (IFIP), pp 169–184

Ratha N, Connell J, Bolle R (2001) Enhancing security and privacy in biometrics-based authentication systems. IBM Syst J 40(3):614–634

Ratha N, Chikkerur S, Connell J, Bolle R (2007) Generating cancelable fingerprint templates. IEEE Trans Pattern Anal Mach Intell 29(4):561–572

Rathgeb C, Busch C (2012) Multi-biometric template protection: issues and challenges. New Trends and Developments in Biometrics, pp 173–190

Rathgeb C, Uhl A (2011) A survey on biometric cryptosystems and cancelable biometrics. EURASIP J Inf Secur 1:3

Rathgeb C, Gomez M, Busch C, Galbally J, Fierrez J (2015) Towards cancelable multi-biometrics based on bloom filters: a case study on feature level fusion of face and iris. In: 3rd IEEE international workshop on biometrics and forensics (IWBF), pp 1–6

Ross A, Nandakumar K, Jain A (2008) Introduction to multibiometrics. Handbook of biometrics. Springer, pp 271–292

Sandhya M, Prasad M (2017) Cancelable fingerprint cryptosystem using multiple spiral curves and fuzzy commitment scheme. Int J Pattern Recognit Artif Intell 31(04):1756004

Savvides M, Kumar B, Khosla P (2004) Cancelable biometric filters for face recognition. In: IEEE Proceedings of the 17th international conference on pattern recognition (ICPR), pp 922–925

Schmidhuber J (2015) Deep learning in neural networks: an overview. Neural Netw 61:85–117

Sinha A, Singh K (2005) Image encryption by using fractional Fourier transform and jigsaw transform in image bit planes. Opt Eng 44(5):057001

Sinha A, Singh K (2013) Image encryption using fractional Fourier transform and 3D Jigsaw transform. Opt Eng 9:158–166

Soliman R, Ramadan N, Amin M, Ahmed H, El-Khamy S, El-Samie F (2018a) Efficient cancelable iris recognition scheme based on modified logistic map. In: Proceedings of the National Academy of Sciences, India Section A: physical sciences, pp 1–7

Soliman R, El Banby G, Algarni A, Elsheikh M, Soliman N, Amin M, El-Samie F (2018b) Double random phase encoding for cancelable face and iris recognition. Appl Opt 57(35):10305–10316

Soliman R, Amin M, El-Samie F (2018c) A double random phase encoding approach for cancelable iris recognition. Opt Quant Electron 50(8):326

Soliman R, Amin M, El-Samie F (2019) A modified cancelable biometrics scheme using random projection. Ann Data Sci 6(2):223–236

Souza D, Burlamaqui A, Souza F (2018) Improving biometrics authentication with a multi-factor approach based on optical interference and chaotic maps. Multimed Tools Appl 77(2):2013–2032

Sree S, Radha N (2016) Cancellable multimodal biometric user authentication system with fuzzy vault. In: IEEE international conference on computer communication and informatics (ICCCI), pp 1–6

Syafeeza R et al (2014) Convolutional neural network for face recognition with pose and illumination variation. Int J Eng Technol 6:44–57

Tarif E, Wibowo S, Wasimi S, Tareef A (2018) A hybrid encryption/hiding method for secure transmission of biometric data in multimodal authentication system. Multimed Tools Appl 77(2):2485–2503

Teoh A, Goh A, Ngo D (2006) Random multispace quantization as an analytic mechanism for biohashing of biometric and random identity inputs. IEEE Trans Pattern Anal Mach Intell 28(12):1892–1901

Tong X, Cui M (2008) A novel image encryption scheme based on feedback and 3D Baker. In: IEEE 4th international conference on wireless communications, networking and mobile computing, pp 1–4

Vezzetti E, Marcolin F (2014) 3D Landmarking in multiexpression face analysis: a preliminary study on eyebrows and mouth. Aesthetic Plast Surg 38(4):796–811

Vezzetti E, Marcolin F, Stola V (2013) 3D human face soft tissues landmarking method: an advanced approach. Comput Ind 64(9):1326–1354

Wu L, Yuan S (2010) A face based fuzzy vault scheme for secure online authentication. In: ieee second international symposium on data, privacy, and e-commerce, pp 45–49

Xiaodong L, Qing H, Xin J (2019) A secure and efficient face-recognition scheme based on deep neural network and homomorphic encryption. In: IEEE international conference on virtual reality and visualization (ICVRV), pp 1–8

Zheng X (2017) The application of information security encryption technology in military data system management. In: International conference on man-machine-environment system engineering, Springer, Singapore, pp 423–428