An Effective Framework for Secure and Reliable Biometric Systems Based on Chaotic Maps

Lakhdar Laimeche\textsuperscript{1(✉)}, Abdallah Meraoumia\textsuperscript{1(✉)}, Lotfi Houam\textsuperscript{1(✉)}, and Amel Bouchemha\textsuperscript{2(✉)}

\textsuperscript{1} Laboratoire de Mathematics, Informatics and Systems (LAMIS), University of Larbi Tebessi, 12002 Tebessa, Algeria
\{lakhdar.laimeche,ameraoumia,lotfi.houam\}@univ-tebessa.dz

\textsuperscript{2} Laboratory of Electrical Engineering (LABGET), University of Larbi Tebessi, 12002 Tebessa, Algeria
amel.bouchemha@univ-tebessa.dz

Abstract. The last few years have plunged us at high speed into a new means of communication, namely the Internet, which has set a new trend for the next millennium. So, the rapid growth of online applications reflects the speed with which most countries can develop. An essential aspect of online communication is related to the trust of users and is a very necessary element to ensure the success of an online application. One of the main elements underlying this trust is the remote authentication of the user through its biometric features while of course protecting these features in different storage media. In this paper, we propose a new palmprint/palm-vein recognition framework based on a hand-craft image feature learning method is suggested. Furthermore, to increase the anti-spoof capability of the system, an effective biometric templates protection method based on chaotic systems was proposed. Experimental results have shown that high accuracy can be obtained with a very high level of template protection, which implies that the proposed cancelable biometric system can operate in highly secure applications.

Keywords: Feature extraction · Feature learning · Cancelable biometric · Chaos system · Template protection · Palmprint · Palm-vein

1 Introduction

For security purposes, most offline/online electronic applications are usually afforded with physical/logical access authorization request procedures. In such applications, the persons identity needs to be authenticated to know if the person is the one claiming it. It is a procedure that involves claiming a persons identity and then providing evidence to prove this. In recent years, the use of biometrics has been increasingly used as an alternative to traditional means in
the procedure of a person's identity authentication [1]. Biometrics addresses the physiological and/or behavioral characteristics that make each person unique for authentication purposes and encompasses any personal characteristic that can be used to uniquely verify the identity of a person [2]. Most noteworthy, in order to optimize the use of biometrics, systems have been developed to incorporate automated methods, generally performed by a computer, to verify the person's identity based on physiological characteristics such as faces, fingerprints and palmprints, and/or behavioral characteristics such as signatures, voices, and keystroke dynamics. Basically, a biometric system can involve [3] i) an acquisition module to capture biological data from a person, ii) a processing module to extract the unique identifiable features of this data (biometric template), iii) a matching module to compare the registered template with a template processed from a sample provided at the authentication time, and iv) a decision module for determining the final classification of the person using a similarity score obtained from the matching module. Indeed, the processing module (which essentially represents the feature extraction task) is one of the most important modules which has received a lot of work from researchers, due to its importance and its strong impact on the system accuracy.

Many applications in image processing and computational vision, including biometrics, rely upon the efficient representation of image features. Consequently, accurate estimates of this representation are of vital importance for higher levels of visual processing [4]. Nowadays, there are many hand-crafted methods that can be well used to extract the distinctive features of an image. However, most of them cannot work well on all types of applications (e.g. all biometric modalities). For example, unlike the deep learning methods which can be used to analyze the image at several levels, the hand-crafted methods are applied at one level and due to its limits, it is not possible to access the depth of the image to extract the distinctive features even when there are very high-resolution biometric images [5]. However, deep learning is not always effective, especially in large databases, due to its need for powerful devices to overcome their main limitations, which are memory capacity and processor speed [6]. For this, in recent times, most research efforts related to hand-crafted feature extraction methods have focused on improving their results by adapting it to images of the whole context. In general, this idea, which aims to provide the hand-crafted feature extraction method with a priori knowledge on the context, has proved remarkably effective because of its very impressive results compared to those which operate without learning [7]. In our new method, learning takes place once and for all during the first use of the system to extract specific information in the form of a projection matrix and a codebook which will then be used in the enrollment and classification phases. This information makes it possible to adapt the hand-crafted feature extraction method to the images processed to extract a distinct vector of discrimination and therefore improve the system performance (for more details, see Sect. 2).

The majority of previous research in biometric recognition has focused on improving system accuracy (most often using an efficient feature extraction method), but attack resistance is also a central and important characteristic of any biometric system. Indeed, although biometrics effectively outperforms
the traditional token-based authentication methods, such as a passport or ID cards, and knowledge-based authentication methods, such as a password or PIN code, they also raise many security concerns that can affect user confidence [8]. So far, cancelable biometric technologies have attracted increasing attention and interest among researchers, in the hope that the possibility of canceled of the biometric template will improve the security performance of biometric systems and thereby overcome security concerns and privacy which, in turn, would increase users’ confidence in the system [9]. Therefore, to strengthen the proposed system against attack on the biometric template, we adopted the revocability technique so that the template can be canceled if it is stolen or spoofed. Of course, our scalable approach may not solve all system security issues, but it does reduce incidents of a security breach because not doing so can lead to insufficient security, which will undoubtedly make the system vulnerable to attack. In this study, a new biometric template protection scheme based on chaotic maps systems to guarantee both high performance and enhanced security is also proposed (for more details, see Sect. 2).

The rest of this paper is organized as follows: In Sect. 2, we detail the proposed cancelable biometric system architecture. This section describes the two main steps, which are feature learning and feature extraction. Experimental results relating to the biometric system performance and security analysis are presented and commented in Sect. 3. Finally, the conclusion and some future work are presented in Sect. 4.

2 System Description

The subject of this paper concerns the biometric system security. Indeed, a biometric system must be available to work correctly and reliably in all circumstances and therefore be resistant to abuse due to any spoofing. To achieve this objective, we decided to protect the biometric template by building a system capable of changing it in the event of spoofing. Thus, our proposed system includes three main phases, namely the training phase, the extraction phase, and the classification phase. Figure 1 shows the block diagram of the training (learning) phase which includes four stages.
2.1 Training Phase

As mentioned earlier, the hand-crafted feature extraction method can be improved by incorporating the concept of learning. This learning can provide prior knowledge (information) to extract the most precise feature vectors. Indeed, the knowledge provided is represented in the form of a codebook.

1) Observation vector: In our method, the image is analyzed block by block, and the observation vector of each block is extracted by the Histogram of Oriented Gradients (HOG) technique. Thus, the input $H \times W$-sized image is divided into square and overlapped blocks, each of which is then mapped into an observation vector $\nu \in \mathbb{R}^{\rho \times 1}$ via the HOG technique. The length of this vector ($\rho$) is a function of the number of HOG windows ($n_w$) and the number of histogram bins ($n_b$), $\rho = f(n_w, n_b)$. In addition, the number of observation vectors extracted from each image ($n_\nu$) is identical to the number of blocks and is equal to:

$$n_\nu = \left\lfloor \frac{H-o}{b-o} \right\rfloor \cdot \left\lfloor \frac{W-o}{b-o} \right\rfloor \quad (1)$$

where $o$ denotes the horizontal/vertical overlap between two adjacent blocks and $[\alpha]$ is the integer part of the value $\alpha$. Finally, the observation vectors extracted from all the blocks are concatenated into a single vector ($\upsilon$) in order to represent the preliminary feature of the entire image:

$$\upsilon_i = [\nu_{i1}, \nu_{i2}, \nu_{i3}, \ldots, \nu_{i n_\nu}]^T \in \mathbb{R}^{n_\nu \times \rho} \quad (2)$$

In order to determine the projection matrix and the codebook, we use $N$ images to extract $n_\nu \cdot N$ observation vectors.

$$\mathcal{V} = [v_1, v_2, v_3, \ldots, v_N]$$

$$= [\nu_{11}, \nu_{12}, \ldots, \nu_{21}, \nu_{22}, \ldots, \nu_{N1}, \nu_{N2}, \ldots, \nu_{N n_\nu}] \in \mathbb{R}^{(N \cdot n_\nu) \times \rho} \quad (3)$$

The vector $\mathcal{V}$ contains, after transformation (projection), the training base for generating the codebook. Of course, the higher the value of $N$, the more effective the learning.

2) Vectors transformation: In this step, the projection matrix $\mathcal{M}_k$ is created. By using this matrix, the biometric template can be protected by changing the secret key ($\mathcal{K}$), which in turn modifies this matrix. This change allows us to extract different vectors for the same person. In our scheme, the matrix $\mathcal{M}_k$ was generated using 1D logistics maps [10] (see Eq. 4) due to its simplicity and efficiency.

$$x_{n+1} = \mathcal{L}(x_n) = \mu x_n (1 - x_n), \quad \mu \in [3.57, 4], \quad x_n \in [0, 1] \quad (4)$$

where $x_n$ is the state of the system (for $n = 0, 1, 2, \ldots$) and $\mu$ is the control parameter. This system generates pseudo-random sequences by means of an
initial state $x_0$ and a fixed control parameter $\mu$. Thus, the two parameters ($x_0$ and $\mu$) can be used as a secret key ($K$).

The role of this matrix is to transform each vector ($\nu_{ij} \in \mathcal{V}$) of dimension $\rho \times 1$ into a vector $\tilde{\nu}_{ij}$ of dimension $\eta \times 1$. To create this matrix, each column is generated with a chaotic system. Therefore, we used ($\eta + 1$) logistics maps, one of which is the main system ($\mathcal{L}_k$), and the rest ($\eta$) are secondary systems ($\mathcal{L}_i | i = 1, 2, 3, \ldots, \eta$). The initial state of each secondary system ($\mathcal{L}_i$) is determined as:

$$x_{0i} = S_k(L_i), \quad i = 1, 2, \ldots, \eta,$$

and

$$S_k = \{x_j\}_{j=1}^{\max(L_i)}$$

where $S_k$ is a sequence generated with $L_k$ and $L_i$ are predefined integer values. In addition, the control parameters of the secondary systems ($\mu_i | i = 1, 2, 3, \ldots, \eta$) are determined by an optimization method (in our work, we used the Bat Algorithm (BA) optimization [11]) in order to maximize the biometric identification rate. Finally, for a given secret key ($K$) and after optimization of the recognition rate, we obtain the final projection matrix ($\mathcal{M}_k$) which takes the following form:

$$\mathcal{M}_k = [w_1, w_2, w_3, \ldots, w_\eta] \in \mathbb{R}^{\rho \times \eta}$$

The values of $L_i$ and $\eta$ can be modified in order to achieve better performance.

3) Codebook learning: Indeed, the observation vectors extracted from all the training images represent the different features that can be found in the work context. Intuitively, all of these features (for example, features in the palmprint for several persons) have a finite dimension. Consequently, many vectors (features) in the training base after the transformation ($\tilde{\mathcal{V}}$) can be very close. For this, an unsupervised clustering process was carried out to select only the most discriminating vectors (features) of the work context. After clustering, the resulting vectors form a so-called codebook ($\mathcal{C}_k$), which represents prior knowledge which is presented to the hand-crafted feature extraction method to effectively represent the feature of the image.

In our study, we used the Linde-Buzo-Gray (LBG) [12] as a clustering technique. This algorithm takes a set of feature vectors $\tilde{\mathcal{V}} \in \mathbb{R}^{\eta \times (N \cdot n_\nu)}$ as input and generates a representative subset of feature vectors (codebook $\mathcal{C}_k$) with a $\ell \ll N \cdot n_\nu$ specified by the user at the output according to the similarity measure.

$$\mathcal{C}_k = \mathcal{F}_{\text{LBG}}(\tilde{\mathcal{V}}) \in \mathbb{R}^{\eta \times \ell} \quad \text{and} \quad \tilde{\mathcal{V}} = \mathcal{V} \cdot \mathcal{M}_k \in \mathbb{R}^{\eta \times (N \cdot n_\nu)}$$

The initial codebook, the distortion, and the threshold are the parameters that control the convergence of the algorithm, which generally requires a maximum number of iterations to ensure this convergence.

In addition, to further improve the protection of the template, we shuffle (redistribute) the vectors in the codebook. Thus, let $S_c$ the sequence, with integer components, generated by the chaotic system $\mathcal{L}_c$:

$$S_c = \{y_i\}_{i=1}^{\ell}, \quad y_i = [(10^4 \cdot x_i) \mod (\ell)]$$
We divide this sequence into two subsequences ($S_c^1$ and $S_c^2$) as:

$$S_c^1 = \{y_i\}_{i=1,3,5,\ldots,\ell-1} \quad S_c^2 = \{y_i\}_{i=2,4,6,\ldots,\ell} \quad (9)$$

Then a simple permutation between the components of $C_k$ is applied:

$$C_k(S_c^1(i)) \leftrightarrow C_k(S_c^2(i)) \leftrightarrow C_k(y_i^1) \leftrightarrow C_k(y_i^2), \quad i = 1, 2, 3, \ldots, \frac{\ell}{2} \quad (10)$$

In the case of spoofing, it is possible either to redistribute only the vectors of the codebook ($C_k$) or to re-estimate the projection matrix ($M_k$), in which a new codebook is created.

2.2 Feature Extraction

The role of this phase is to represent the feature of the image using the projection matrix ($M_k$) and the codebook ($C_k$) previously obtained in the learning phase. Thus, the sequence diagram for this phase is illustrated in Fig. 2. In this phase, the observation vectors are extracted from the input image in the same way as the training phase (using the HOG technique). After having projected these vectors, a coding process is applied. Let $v_i$ be the extracted observation vectors from the input image $i$:

$$v_i = [v_{i1}, v_{i2}, v_{i3}, \ldots, v_{in_{\nu}}]^T \in \mathbb{R}^{n_{\nu} \times \rho} \quad (11)$$

The vector $v_i$ is then transformed (projected) using the matrix $M_k$:

$$\tilde{v}_i = \mathcal{F}_{\text{proj}}(v_i) = v_i \cdot M_k \in \mathbb{R}^{\eta \times n_{\nu}} \quad (12)$$

To obtain the final feature representation of the image, the vector obtained ($\tilde{v}_i$) must be encoded. In this case, each column on the vector $\tilde{v}_i$ is replaced by the coordinate of the nearest vector in the codebook. Thus, for each column, the system calculates the similarity between it and all the vectors in the codebook.

$$D_i = [d_1, d_2, d_3, \ldots, d_\ell] \in \mathbb{R}^{1 \times \ell}, \quad i \in [1 \cdot n_{\nu}] \quad (13)$$
After that, the system determines the coordinates based on the lowest similarity score as follows:

\[ c_i = \arg \min_{c_i \in [1 \cdots \ell]} (D_i) \]  

(14)

Encode all the columns of the vector \( \tilde{v}_i \), we obtain the final feature representation of the image \( \mathcal{X}_i \):

\[ \mathcal{X}_i = \mathcal{F}_{\text{cod}}(\tilde{v}_i) = [c_1, c_2, c_3, \cdots c_{n_v}] \in \mathbb{R}^{1 \times n_v}, \quad c_i \in [1 \cdots \ell] \]  

(15)

This representation makes it possible to hide the feature of the image in a compact form, it plays the role of pooling.

### 2.3 Classification Phase

In all biometric systems, before the classification phase (identification or verification), the person must be enrolled in the system database. In the two phases (enrollment and classification), the image feature is represented as we described in Subsect. 2.2. Thus, in the classification phase and before the matching step, the feature vector must be decoded using the same codebook \( (C_k) \) as is used in the enrollment phase. Let \( \mathcal{X}_i \) be the feature vector of the person to be classified, where \( \mathcal{X}_i \) is defined as in Eq. 15. This vector is decoded as follows:

\[ \tilde{v}_i = \mathcal{F}_{\text{dec}}(\mathcal{X}_i) = \mathcal{F}_{\text{dec}}([c_1, c_2, c_3, \cdots c_{n_v}]) \in \mathbb{R}^{\eta \times n_v} \\
= [C_k(c_1), C_k(c_2), C_k(c_3), \cdots, C_k(c_{n_v})] \quad \mathcal{F}_{\text{dec}}(c_i) = C_k(c_i) \]  

(16)

In the feature matching step, the decoded feature vector is compared to the previously stored vectors to produce a matching score. In our scheme, we use the Sum of Absolute Difference (SAD) function defined as:

\[ d_{ij} = \sum_{n=0}^{\eta-1} \sum_{m=0}^{n_v-1} |\tilde{v}_i(n, m) - \tilde{v}_j(n, m)|, \quad j \in [1, 2, \cdots, N_p] \]  

(17)

where \( d_{ij} \) indicates the similarity score between the examined feature vector \( \tilde{v}_i \) and the stored feature vectors \( \tilde{v}_j \) \( j = 1, 2, 3, \cdots, N_p \) and \( N_p \) is the number of persons in the system database.

### 3 Experimental Results an Discussion

The purpose of this section is to discuss in detail the experimental results obtained in this study for user identification via palmprint/palm-vein recognition. Therefore, experiments were conducted on an accessible and public Multispectral palmprint dataset provided by the Hong Kong Polytechnic University (PolyU) [13]. In our experiments, we used a database of 300 persons, which is similar to the number of employees in a small to medium-sized enterprise. In this dataset, each person has twelve samples for each biometric modality. In the
Fig. 3. Selection of parameters for our learned hand-crafted feature extraction method for better biometric system performance \( \{K \equiv (x_0, \mu) = (0.4191, 3.8841)\} \). (a) 128-sized codebook, (b) 256-sized codebook, (c) 512-sized codebook and (d) 1024-sized codebook.

enrollment phase, we randomly used three samples from each person’s biometric modality to register them, while the other nine samples of the person were used to evaluate the system performance. By comparing the nine test samples with all those enrolled in the database, we can obtain 282375 matching scores divided into 2250 scores for client experiments and 280125 scores for impostor experiments. The set of experiences of our work is divided into two sub-parts. In the first one, we present the palmprint/palm-vein based system performance. In this sub-part, we perform several tests in order to best choose the parameters of the proposed method. The second sub-part focuses on the biometric system security, in which their performance against attacks is examined.
3.1 System Accuracy Analysis

In a biometric system, the final representation of the images’ feature has a major impact on the system recognition rate. Since our proposed method depends on several parameters, we performed an empirical test to choose the best ones that can improve the system accuracy. It should be noted that only three parameters were examined, namely the analysis block size \(b\), the length of the transformed feature vector (after projection) \(\eta\), and the codebook length \(\ell\). Consequently, the remaining parameters, which are the number of HOG windows \(n_w\), the number of histogram bins \(n_b\), and the blocks overlap ratio \(o\), are fixed at 11, 7, and 50\%, respectively. In these preliminary tests, we used the palmprint modality and we tried to choose the parameters \(b\), \(\eta\), and \(\ell\), from the set of values \(\{20, 30, 40\}\), \(\{100, 200, 300, 400\}\) and \(\{128, 256, 512, 1024\}\), respectively.

Since varying these parameters can produce many feature representations, we can experimentally select a combination \((b, \eta, \ell)\) that can effectively improve the system accuracy by changing one of them each time and by choosing the best that gives the best performance. Thus, in order to see the effect of these parameters \((b, \eta, \ell)\) on the biometric system performance, we clearly illustrate, in Fig. 3, the results of the closed-set identification system (Rank-One Recognition (ROR)) operating with a secret key \((\mathcal{K})\) equal to \(\equiv (x_0, \mu) = (0.4191, 3.8841)\). From these curves, we can find four important cases: 

1) Acceptable performances can be obtained with all possible combinations since an actual identification rate (ROR) higher than 94\% has already been obtained.

2) Generally, the smaller the analysis block, the higher the identification rate. The average RORs obtained by a block size of \(20 \times 20\) is better than those obtained by a block size of
40 × 40, particularly in the lower codebook sizes. iii) System performance can be improved by using long codebook lengths. Thus, the average RORs obtained by a codebook length of 1024 is better than those obtained by codebook lengths of 128, 256, and 512. iv) Finally, increasing the feature vector length (η) effectively improves system performance. From Fig. 3, it is clear that the combinations (b, η, ℓ) equal to (40 × 40, 400, 1024) and (40 × 40, 300, 1024) offer better results in terms of ROR (100% with a Rank of Perfect Recognition (RPR) equal to 1), see Fig. 3.(d). But when the identification system works in open-set mode, the first combination (40 × 40, 400, 1024) gives the best performance (Equal Error Rate (EER) equal to 0.2334% (T_o = 0.5357) instead of 0.2721% (T_o = 0.5492)). Henceforth, we have considered the best parameters (b×b = 40 × 40, η = 400 an ℓ = 1024) in order to conduct several experiments to compare the effectiveness of the biometric system using palmprint/palm-vein biometric modalities. As these modalities give a perfect closed-set identification performance (ROR = 100% with RPR = 1), we only represent in Fig. 4 the open-set identification performance. From the curves in Fig. 4.(a) (DET curves), it is clear that the palmprint modality offers better results than the palm-vein modality in terms of EER (0.234% (T_o = 0.5541) instead of 0.389% (T_o = 0.5761)). In this case, a performance improvement of 39.846% is obtained. Finally, to summarize this series of tests, graphs showing the Receiver Operating Characteristic (ROC) curves using the two biometric modalities were generated in Fig. 4.(b).

Since the emergence of biometric systems, interest in the use of several biometric modalities has increased due to their potential to overcome certain important limitations of unimodal systems, in particular the low identification rate [14]. Thus, the aim of this part is to examine whether the performance of the open-set identification system can be improved by integrating complementary information which comes mainly from different modalities (palmprint and palm-vein). In our work, we use a rule-based technique to fuse the matching scores produced by the different unimodal identification systems. Thus, the sum rule (SUM) and the product rule (MUL) are used. The experimental results for the open-set/closed-set identification mode, respecting the two fusion rules, are presented, as EER and ROR, in Table 1. The results in this table show that, generally, the use of fusion allows effectively improve open-set biometric identification system performance with an improvement of 68.974% and 81.331% (using MUL rule)

|                          | OPEN-SET | CLOSED-SET |
|--------------------------|----------|------------|
|                          | T_o      | EER        | RPR | ROR |
| PALMPRINT                | 0.5541   | 0.2340     | 1   | 100.00 |
| PALM-VEIN                | 0.6030   | 0.3889     | 1   | 100.00 |
| FUSION (SUM)             | 0.5837   | 0.0798     | 1   | 100.00 |
| FUSION (MUL)             | 0.3381   | 0.0726     | 1   | 100.00 |
compared to palmprint and palm-vein, respectively. In conclusion, the obtained identification rates are identical to those obtained in several previous works in literature and make our proposed method sufficient for several applications.

3.2 System Security Analysis

Given the encouraging results obtained with our proposed system in identifying persons, in this section we will try to assess the security level against potential attacks (templates protection level). In this security analysis, we will take into account that the system structure is already known to attackers and we will try to evaluate attempts to retrieve the biometric template. In general, the high-security level is obtained when:

i) Impossibility of retrieving the biometric template by exhaustive searches (so the key space must be sufficiently large) and

ii) a slight change in the secret key gives completely different templates.

i) Key space analysis: According to Fig. 1, the security of our system is guaranteed by \((\eta+2)\) chaotic systems, one of which is main (\(L_k\)) and \((\eta+1)\) secondary \((L_i|_{i=1}^{\eta})\) and \(L_c\). The role of the main chaotic system is to vary the initial state of the \((\eta+1)\) secondary chaotic systems, while the role of the \((\eta+1)\) chaotic systems is to change the projection matrix and to mix the extracted template. In a chaotic system, the secret-key space is calculated using all the mean absolute errors \((E)\) between two sequences generated by two close secret keys [15]. So let \(S^x\) and \(\tilde{S}^x\) (or \(S^\mu\) and \(\tilde{S}^\mu\)) two sequences generated by the same system under \(x_0\) and \(x_0 + d^x\) (or \(\mu\) and \(\mu + d^\mu\)): The \(E^x\) (or \(E^\mu\)) is defined as:

\[
E^x(S^x, \tilde{S}^x) = \frac{1}{L} \sum_{i=1}^{L} |S^x(i) - \tilde{S}^x(i)|
\]

(18)

where \(L\) denotes the sequence length which is different from one system to another. Thus, the key space for \(x_0\) called \(s_x\) (or \(s_\mu\) for \(\mu\)) is equal to \(1/d_x\) (or \(1/d_\mu\)), where \(d_x\) (or \(d_\mu\)) is the value of \(d^x\) (or \(d^\mu\)) when \(E^x\) (or \(E^\mu\)) becomes 0. So, the total key space in our system is equal to:

\[
S = (s_{x_k} \cdot s_{\mu_k}) \cdot (s_{x_\mu} \cdot s_{\mu_\mu}) \cdot \prod_{i=1}^{\eta} (s_{x_i} \cdot s_{\mu_i})
\]

(19)

For the \(L_k\) system, the pair \((s_x, s_\mu)\) is equal to \((1.1420 \cdot 10^{16}, 0.5248 \cdot 10^{16})\). This pair is equal to \((1.2541 \cdot 10^{16}, 0.8542 \cdot 10^{16})\) for \(L_c\). Finally, for any \(L_i|_{i=1}^{\eta}\) system, \((s_x, s_\mu)\) becomes \((2.0248 \cdot 10^{16}, 1.3125 \cdot 10^{16})\). Therefore, the total key space of our system becomes:

\[
S = (0.6420 \cdot 10^{64}) \cdot (2.6576^\eta \cdot 10^{32\eta}) = (0.6420) \cdot (2.6576^\eta) \cdot 10^{32(\eta+2)}
\]

(20)

In our proposed biometric identification system, the value of \(\eta\) must be high enough to obtain high accuracy for the identification of persons, and therefore the security level is guaranteed \((\eta = 400 \Rightarrow \text{key space is too high})\).
**ii) Key sensitivity analysis:** In order to test the system sensitivity to slight variations of the key, we test in this subpart the system behavior resulting from many closest secret keys. Therefore, we used three different keys: $K_c$: correct key $(x_0, \mu) = (0.4191, 3.8841)$, $K_1$: wrong key $(0.4140, 3.8511)$, and $K_2$: wrong key $(0.4191 + 10^{-16}, 3.8841)$). In order to assess the security level, we enrolled all persons with the correct key ($K_c$), and then we tested the open-set/closed-set identification, using palmprint and palm-vein, with the three keys ($K_c$, $K_1$ and $K_2$). The system performance under the three keys is illustrated in Fig. 5 for the two biometric modalities.

![Fig. 5. Biometric system performance during an attack (theft of the biometric template for a spoofing attempt). (a) Palmprint based open-set identification system, (b) Palmprint based closed-set identification system, (c) Palm-vein based open-set identification system and (d) Palm-vein based biometric system](image-url)
For open-set identification systems, Fig. 5. (a) (for the palmprint) and Fig. 5. (c) (for the palm-vein) presents the distribution of genuine and impostor scores obtained using the correct key \((K_c)\) as well as the distribution of genuine scores when the changing the key due to an attack (scores obtained by keys other than the correct secret key, therefore wrong keys \((K_1 \text{ and } K_2)\)). In these figures, it is clear that all the attack scores are completely displaced above the security threshold \((\gg T_o)\), and thus have become impostor scores for the system. In addition, a greater confidence interval between genuine and attack scores was obtained \(([0.567 - 0.648] \text{ for palmprint and } [0.621 - 0.648] \text{ for palm-vein})\), which reflects the effectiveness and robustness of our proposed cancelable biometric system against any possible attack.

Similar to the open-set identification mode, Fig. 5. (b) (for the palmprint) and Fig. 5. (d) (for the palm-vein) show the correct and incorrect score distributions (due to attacks) obtained in using the correct key and the wrong keys in the closed-set identification mode. Since the closed-set identification mode does not use a threshold to determine the person’s identity but to know if the calculated score is obtained by correct or incorrect keys, a threshold must be used whose purpose is to separate the two distributions resulting from the correct/incorrect keys. Consequently, if the calculated score is higher than the threshold, the biometric template is then refused (the key has been changed), otherwise the biometric template is accepted and the system will, therefore, determine the person’s identity. In our system, the threshold can be effectively chosen in the intervals \([0.572 - 0.652]\) and \([0.614 - 0.611]\) for the palmprint modality and the palm-vein modality, respectively. A serious analysis of the previous results shows that overall, our method can considerably improve the level of security of the system through the use of the revocability principle, which allows them to be used in applications requiring high security.

4 Conclusion and Further Works

Recently, biometrics has become one of the most important means used to identify a person’s identity. Despite this success, the attack on the system and the theft of the biometric template can pose a real problem in terms of a person’s privacy. Because this template is intrinsically linked to the person and cannot be changed, the fear of losing it can be one of the most important users’ distrust. Therefore, many of the emerging work has focused on template protection, and perhaps the most important of these is cancelable biometric systems. The purpose of our scheme lies in the possibility of extracting a biometric template so that they can be canceled when an attack occurs, and of course, the biometric system performance must be preserved. Therefore, this study is mainly related to the biometric feature extraction task. In this paper, we have established two main objectives. The first consists in proposing a new feature extraction method based on the learning principle to increase their efficiency in extracting the distinctive template. While the second concerns the template protection by canceling it in any attack. By decomposing the image on several blocks, we used
the HOG technique to extract the observation vector from each block. Using observation vectors of several images, a codebook was created, which aims to provide a priori knowledge of the working context in order to effectively represent the image in the two phases of the system (enrollment and identification). To protect the template, we used the transformation method by projecting the template into a matrix created by chaotic systems and optimized by the genetic algorithm. The experimental results show the robustness against template theft with a high identification rate, which can also be improved by combining the two biometric methods. As future work, we plan to change the HOG technique used to extract the feature vector of the blocks with the DCT and oBIF techniques. We will also try to test some hyperchaotic systems.

References

1. Wei, J., Zhang, B., Lu, J., Zhu, Y., Yang, Z., Zuo, W., et al.: Palmprint recognition based on complete direction representation. IEEE Trans. Image Process. 26(9), 4483–4498 (2017)
2. Fang, Y., Wu, Q., Kang, W.: A novel finger vein verification system based on two-stream convolutional network learning. Neurocomputing 290(17), 100–107 (2018)
3. Unar, J., Seng, W., Abbasi, A.: A review of biometric technology along with trends and prospects. Pattern Recognit 47(8), 2673–2688 (2014)
4. Wang, Q., Li, B., Chen, X., Luo, J., Hou, Y.: Random sampling local binary pattern encoding based on Gaussian distribution. IEEE Signal Process. Lett. 24(9), 1358–1362 (2017)
5. Genovese, A., Piuri, V., Scotti, F.: Palmprint biometrics. Touchless Palmprint Recognition Systems. AIS, vol. 60, pp. 49–109. Springer, Cham (2014). https://doi.org/10.1007/978-3-319-10365-5_4
6. Sundararajan, K., Woodard, D.L.: Deep learning for biometrics: a survey. J. ACM Comput. Surv. (CSUR) 51(3), 1–34 (2018)
7. Feng, Z., et al.: DLANet: a manifold-learning-based discriminative feature learning network for scene classification. Neurocomputing 157, 11–21 (2015)
8. Yu, J., Zhang, B., Kuang, Z., Lin, D., Fan, J.: iPrivacy: image privacy protection by identifying sensitive objects via deep multi-task learning. IEEE Trans. Inf. Forensics Secur. 12(5), 1005–1016 (2017)
9. Nandakumar, K., Jain, A.: Biometric template protection: bridging the performance gap between theory and practice. IEEE Signal Process. Mag 32(5), 88–100 (2015)
10. Farsana, F.J., Gopakumar, K.: Private key encryption of speech signal based on three dimensional chaotic map. In: International Conference on Communication and Signal Processing, pp. 2197–2201 (2017)
11. Laimeche, L., Meraoumia, A., Bendjenna, H.: Enhancing LSB embedding schemes using chaotic maps systems. Neural Comput. Appl. 32(21), 16605–16623 (2019). https://doi.org/10.1007/s00521-019-04523-z
12. Li, Z., Li, X., Liu, Y., Cai, Z. (eds.): ISICA 2012. CCIS. Springer, Heidelberg (2012). https://doi.org/10.1007/978-3-642-34289-9
13. Hong Kong Polytechnic University (PolyU) multispectral palmprint database (2011). http://www.comp.polyu.edu.hk/~biometrics
14. Sunil Khandelwal, C., Maheshewari, R., Shinde, U.B.: Review paper on applications of principal component analysis in multimodal biometrics system. Procedia Comput. Sci. 92, 481–486 (2016)

15. Bhatnagar, G., Wu, Q.M.J.: Chaos-based security solution for fingerprint data during communication and transmission. IEEE Trans. Instrum. Meas. 61(4), 876–887 (2012)