International Journal on Artificial Intelligence Tools
Vol. 25, No. 1 (2016) 1550027 (30 pages)
© World Scientific Publishing Company
DOI: 10.1142/S021821301550027X

World Scientific
www.worldscientific.com

Biometric Template Protection Using Spiral Cube: Performance and Security Analysis

Chouaib Moujahdi*
Scientific Institute of Rabat, Mohammed V University, Rabat, Morocco
chouaib.moujahdi@fulbrightmail.org; moujahdi_chouaib.yahoo.fr

George Bebis
Department of Computer Science and Engineering, University of Nevada-Reno
Reno, NV 89577, USA
bebis@cse.unr.edu

Sanaa Ghouzali
Information Technology Department, CCIS, King Saud University
Riyad, Saudi Arabia
sghouzali@ksu.edu.sa

Mounia Mikram[†] and Mohammed Rziza[‡]
LRIT, associated unit to CNRST (URAC 29), Mohammed V University
Rabat, Morocco
[†]*mikram@ieee.org*
[‡]*rziza@fsr.ac.ma*

Received 26 October 2013
Accepted 5 May 2015
Published 23 February 2016

Personal authentication systems based on biometrics have given rise to new problems and challenges related to the protection of personal data, issues of less concern in traditional authentication systems. The irrevocability of biometric templates makes biometric systems very vulnerable to several attacks. In this paper we present a new approach for biometric template protection. Our objective is to build a non-invertible transformation, based on random projection, which meets the requirements of revocability, diversity, security and performance. In this context, we use the chaotic behavior of logistic map to build the projection vectors using a methodology that makes the construction of the projection matrix depend on the biometric template and its identity. The proposed approach has been evaluated and compared with Biohashing and BioPhasor using a rigorous security analysis. Our extensive experimental results using several databases (e.g., face, finger-knuckle and iris), show that the proposed technique has the ability to preserve and increase the performance of protected systems. Moreover, it is demonstrated that

*Corresponding author.

the security of the proposed approach is sufficiently robust to possible attacks keeping an acceptable balance between discrimination, diversity and non-invertibility.

Keywords: Template protection; random projection; logistic map; revocability; security.

1. Introduction

With the exponential growth of communications, both in volume and diversity (e.g., financial transactions, access to services, etc.), several international concerns have highlighted the necessity to fight against the problems of identity theft, fraud, crime and terrorism. Because of these political responsibilities and the need for a civil protection, personal authentication systems are experiencing a growing interest. Their common denominator is to provide reliable/simple techniques to authenticate a person without the assistance of another person. These systems must authenticate individuals while respecting several requirements, such as speed, reliability, accuracy and protection of user's privacy.

Traditional systems of personal authentication which use passwords and ID cards are not able to meet all these requirements. For example, most people use passwords which are based on letters or numbers and that can be easily recalled, such as names and birthdays. Indeed, this way makes these passwords easily guessed using a brute force attack or a dictionary attack. In addition, although it is advisable to use different passwords for different applications, most people use the same password in different systems. Thus, if only one password is compromised, all applications will be threatened. In practice, random and long passwords are more secure, but they are harder to remember; which prompts some users to write them in accessible locations.

Authentication systems based on biometrics, which use physiological (face, iris, etc.) and behavioral (signature, etc.) modalities, are more promising than traditional systems. Most biometric techniques have the advantage, over traditional systems, that they are universal, unique and permanent; in addition, they are more reliable since the biometric information cannot be lost, forgotten or easily guessed. However, while biometrics can improve security in a multitude of environments, biometric systems, like any other security system, have vulnerabilities and weaknesses. The increasing use of biometrics has led to a renewed interest in the research of new methods to attack biometric systems. These researches showed that biometrics has given rise to new problems and challenges related to the security and protection of personal data. Problems which are more complicated than that of traditional systems. For example, a person might leave his/her fingerprints on everyday touched surfaces while his/her face images can be seen everywhere. Consequently, many attacks can be launched against biometric systems, which can reduce the credibility of these systems. Therefore, although biometric technologies have inherent advantages over traditional methods of personal authentication, the problem of ensuring the security of biometric data is critical.

In practice, opponents exploit the structure of biometric systems to launch their attacks. In general, biometric systems consist of four main modules: sensor module, feature extraction module, database module, and classification module. Ratha *et al.*[1] have identified eight levels of attack in a biometric system; however, since the principle of some attacks is repeated, Jain *et al.*[2] have grouped them into four categories. First, attacks on the user interface (i.e., sensor), mainly due to the presentation of falsified biometric data; for example, *spoofing/mimicry* attacks.[4] Second, attacks on the interface between modules where an adversary can destroy or interfere communication interfaces between modules; for example, *replay* attacks[3] and *hill climbing* attacks.[4] Third, attacks on the software module where the executable program of a module can be modified so that it always returns the desired values of an opponent. This is known as *Trojan-horse* attack. Finally, attacks against the biometric templates stored in the database module which are considered among the most damaging attacks on a biometric system. For example, a biometric template can be replaced by an impostors template to obtain unauthorized access to the system. In addition, a physic parody (spoof) can be created from a stolen template[5] to obtain unauthorized access to the system. The irrevocability of biometric templates makes this kind of attack very dangerous. This is because in contrast to a stolen credit card or password that can be replaced, if a template is stolen it is not possible for a legitimate user to revoke his/her biometric templates and replace them with another set of identifiers. Therefore, the objective of all biometric template protection approaches is to make biometrics *revocable* (also called *cancelable* biometric[6]). In this work, we propose a new approach for biometric template protection which is based on random projection and the chaotic behavior of logistic map.

This work is an extension of our previous work which appeared in Ref. 7. Most studies on biometric template protection, including Ref. 7, analyze the performance and security of protection schemes assuming that biometric data are uniform. However, multiple acquisitions of the same biometric trait do not yield an identical set of features, which makes this kind of analysis unfaithful. In this work, we employ a rigorous security analysis and performed extensive experiments to evaluate the proposed approach. We have also compared our approach with Biohashing and BioPhasor by taking into consideration several factors that influence protection schemes.

The rest of the paper is organized as follows. Section 2 presents an overview of template protection approaches. In Section 3, first we review random projection, Biohashing, BioPhasor, and the phenomenon of chaos; then, we present the proposed approach. Section 4 presents the analytical equations used in our evaluation methodology of protection schemes. Our experimental results and comparisons are presented in Section 5. Our conclusions and perspectives for future work are provided in Section 6.

2. Overview of Template Protection Approaches

Personal authentication systems based on biometrics have given rise to problems and challenges related to the protection of personal data, issues of less importance in traditional authentication systems. Due to these problems of security and privacy, there are currently many research efforts underway to protect biometric systems against possible attacks. Solutions in the literature can be divided into two main categories: *preventive* and *palliative*. Each category can be further divided into two main approaches: *hardware* and *software*.

The objective of *palliative* solutions is, once the attack has been made, to minimize the probability of rupture in the system. Hardware approaches in this category try to add specific sensors (smell, blood pressure, etc.) to detect the liveliness/fraud of presented features. Among the software approaches in this category, one that has received more attention by researchers and industry is called *liveliness detection*. It should be mentioned that these solutions depend on the used biometric trait and there is no standard approach for all biometric systems.

Preventive solutions are designed to prevent the commission of an attack. In general, these solutions are trying to protect biometric templates. Hardware approaches in this category try to put all modules and interfaces of a biometric system on a chip card or a secure processor in general. Software approaches in this category are designed to protect the stored biometric templates. The idea is that instead of storing the templates themselves, a function is stored for each template which is used directly in the task of classification. Our work is primarily concerned with these solutions for template protection.

An ideal approach of biometric template protection must meet four requirements:[8]

- *Revocability*: it should be possible to revoke a template and replace it with a new template based on the same biometric data.
- *Diversity*: if a revoked template is replaced by a new model, it should not correspond with the former. This property ensures the privacy of the user.
- *Security*: it must be difficult, computationally, to obtain the original template from the protected template.
- *Performance*: The protection approach should not degrade the recognition performance of the system.

The major challenge in designing an approach for template protection, which meets all four requirements, is the presence of intra-subject variations: multiple acquisitions of the same biometric trait is very unlikely to lead to an identical set of features.

Jain *et al.*[2] have classified these approaches into three main categories: *feature transformation*, *biometric cryptosystem*,[9,10] and *hybrid*.[11] The basic idea of feature transformation approaches is to apply a transformation function F to the original biometric template T using a key K; the transformed template $\mathrm{F(T, K)}$ is then stored in the database. The function F is also used to transform the test template Q, and we can directly compare the transformed templates $\mathrm{F(T, K)}$ and $\mathrm{F(Q, K)}$ in the transformation domain to determine whether the user is accepted or not. Depending on the transformation function F, feature transformation schemes can be divided into two classes: *salting* and *non-invertible*. In Salting,[4,12] F is invertible; if an opponent has the key and the transformed template, he/she can recover the original biometric template (or an approximation of it). Therefore, the Salting scheme security is based on the security of the key. In the case of non-invertible transformations,[13–15] the function F is a one way function. The main advantage of this approach is that even if the key and/or the transformed template are known, it is difficult for an adversary to recover the original template (i.e., in terms of computational complexity). In biometric cryptosystems, the principle of classical cryptosystems is combined with the principle of biometrics to improve the security of personal authentication systems based on biometrics. The main objective of these schemes is to minimize the amount of biometric data stored in the database. In these approaches, an error correcting code is applied on the original template B and the key K to extract the helper data H. At the time of authentication, an error correcting code is applied on the helper data H and test template Q to recover the key K and make a decision. In the case of hybrid approaches, several basic principle (e.g, feature transformation approaches and biometric cryptosystems) are combined to improve the results.

Each of these approaches have their own advantages and limitations.[2] Overall, they do not meet, contemporaneously, the requirements of revocability, diversity, security and high performance recognition. Thus, there is no best approach for protecting biometric data and available protection schemes are not yet mature enough for widespread deployment.

In this paper, we propose a new non-invertible transformation approach that allows diversity, revocability, security and performance with no need for a user's key. The proposed method is based on random projection and the use of the chaotic behavior of logistic map to build the projection vectors. The proposed method makes the construction of the projection matrix depend on the biometric template and its identity. Next section describes the proposed approach.

3. Proposed Approach

In this Section, we present a non-invertible transformation approach for biometric template protection, based on the principle of random projection and the chaotic behavior of logistic map to build the projection vectors.

3.1. *Random projection, Biohashing and BioPhasor*

Random projection has been applied on various types of problems including biometric template protection.[16] It uses random orthogonal matrices to project the biometric templates in a space where distances are preserved. Random projection can be considered as a salting scheme. Several approaches for biometric template protection are based on the principle of random projection; for example, *BioHashing*[17] and *BioPhasor*[14] approaches. To make the projection non-invertible, a quantization step was included in Refs. 17 and 18. In practice, the non-invertible random projection principle coincides with the *Biohashing* approach. The stages of Biohashing are the following:

- Generate n random vectors using the user's key.
- Apply the Gram-Schmidt orthogonalization algorithm on the n random vectors to compute an orthogonal matrix Δ.
- Transform the original template z using the matrix Δ:

$$y = \Delta z \tag{1}$$

  — y is the transformed template.

- Quantize the transformed template y as follows:

$$t_i = \begin{cases} 0 & \text{if } y_i \leq \tau \\ 1 & \text{if } y_i > \tau \end{cases} \qquad \text{where} \quad i = 1, \ldots, n \tag{2}$$

  — τ is a preset threshold.
  — t is the quantized template of size n.

The *BioPahsor* approach[14] is a variant of Biohashing that address the security and invertibility requirements missing in the traditional random projection. The stages of BioPhasor are the following:

- Generate m random vectors and store them in a tamper-proof card.
- Apply the Gram-Schmidt orthogonalization on the m random vectors to compute an orthogonal matrix Δ.
- Transform the original template z (size n) using the following formulation:

$$y_i = \frac{1}{n} \sum_{i=1}^{n} atan\left(\frac{z_i}{\Delta_{ij}}\right) \tag{3}$$

  — $j = 1, \ldots, m$, $m \leq n$ and $\Delta_{ij} \neq 0$.
  — y is the transformed template.

- Quantize the transformed template y as follows:

$$t_i = \begin{cases} 0 & \text{if } 0 < y_i \leq \pi \\ 1 & \text{if } \pi < y_i \leq 0 \end{cases} \qquad \textit{where} \quad i = 1, \ldots, m \tag{4}$$

  — t is the quantized template of size m.

The Gram-Schmidt orthogonalization algorithm returns a set of orthogonal vectors if and only if the input vectors are linearly independent. Therefore, generating the random vectors from a user's key will be relatively limited by this requirement. This has motivated us to use the chaotic behavior of logistic map to generate linearly independent vectors that are used to construct the projection matrices.

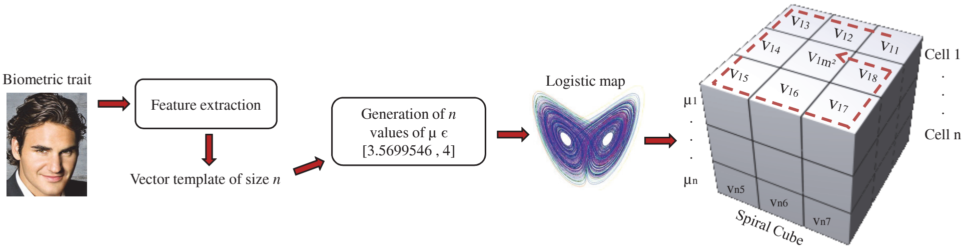


Fig. 1. Spiral cube construction.

3.1.1. *Logistic map*

The logistic map is a sequence whose recurrence is not linear. Specifically, its recurrence relation is given by:

$$x_{n+1} = \mu x_n (1 - x_n)\,. \tag{5}$$

Based to the value of μ, we can observe a chaotic behavior in the interval $[3.5699456, 4]$. Due to the fact that the logistic map is very sensitive to initial conditions, it has been used in several applications including the protection of data content. For example, random sequences of the chaotic zone can be used to cryptographically secure the transmission channels in telecommunications systems.

The instability of trajectories (or directions) is one of the chaos characteristics[19,20] due to the SIC property (Sensitivity to Initial Conditions). We can exploit this characteristic to generate several linearly independent vectors. In the case of logistic map, if n chaotic vectors are generated using n different values of μ (in the interval $[3.5699456, 4]$), each vector will have its own direction. Therefore, this family of vectors is a linearly independent family.

In our work, we use the logistic map to generate multiple random vectors. These vectors will be stored in a 4D matrix, called *Spiral Cube*, which will be used to construct the projection matrices. The Spiral Cube consists of several *cells* (3D square matrix), each cell contains several *boxes* and each box contains a chaotic vector generated using a specific value μ in the interval $[3.5699456, 4]$. It should be mentioned that the chaotic vectors are stored *spirally* in the cells to delude the opponent if the spiral cube is stolen (adding at the same time another alternative to the revocability of our approach).

The construction of spiral cube depends on the size of the original template (Fig. 1). Suppose that the feature vector contains n values, the spiral cube will consist of n cells and each cell corresponds to a specific value of μ (i.e., vectors in the same cell are generated using the same value of μ). The number of vectors in each cell must be greater than or equal to n and the cells must be square to be able to store *spirally* the chaotic vectors. We choose to generate m^2 chaotic vectors. m^2 is the first radical number greater than or equal to n (i.e., m is the nearest integer greater than or equal to $\sqrt{n}$). Therefore, each cell contains $m \times m$ boxes, and each box contains a vector, of size n, generated using the value μ that corresponds to the hosting cell.

3.2. *Proposed approach*

Our objective is to build a non-invertible transformation approach for biometric template protection that meets all the requirements of security and performance without requiring a user's key. In this context, we propose a non-linear mechanism of random projection. The proposed approach is applicable to any biometric system that employs *feature vectors* for classification. We describe below the main steps of our approach.

We assume that the training database contains x templates of size n from z identities where each identity is represented by y templates: $x = y \times z$. During enrollment, we perform the following steps:

- For each training template T, we calculate δ:

$$\delta = \frac{|\max(T) - \min(T)|}{m^2} \tag{6}$$

— m is the nearest integer greater than or equal to $\sqrt{n}$.

- Then, we calculate the quantized vector Q of the template T:

$$Q_i = \begin{cases} 1 & \text{if } t_i = \min(T) \\ m^2 & \text{if } t_i = \max(T) \\ \text{ceil}\left(\dfrac{|T_i - \min(T)|}{\delta}\right) & \text{else} \end{cases} \tag{7}$$

— $i \epsilon [1, n]$.
— $Q_i \epsilon [1, m^2]$.
— *ceil*(a) calculates the nearest integer greater than or equal to a.

- For each identity, we keep a single quantized vector (i.e, randomly chosen among the y vectors corresponding to that identity). Then, we obtain a matrix ϕ which contains the z quantized vectors chosen. We refer to it the *Cube Map*.
- For each identity, we construct a projection matrix using the *Spiral Cube* and the *Cube Map* (Fig. 2). We use the values of quantized vectors (stored in the Cube Map) to select the chaotic vectors (stored in the Spiral Cube).
- Let us assume that we calculate the projection matrix of identity 1 using Spiral Cube and Cube Map illustrated in Fig. 2. The first value of the quantized vector (first vector of the cube map corresponds to identity 1) is associated with the first cell in the spiral cube, and so on for the other values of this vector. For example, if the first value is 3, we extract vector number 3 of the first cell in the spiral cube. The last value is 5, we extract the vector number 5 of the cell number n (the last cell). Finally, we obtain n vectors and we apply the Gram Schmidt algorithm to construct the projection matrix of identity 1. We use the constructed matrix

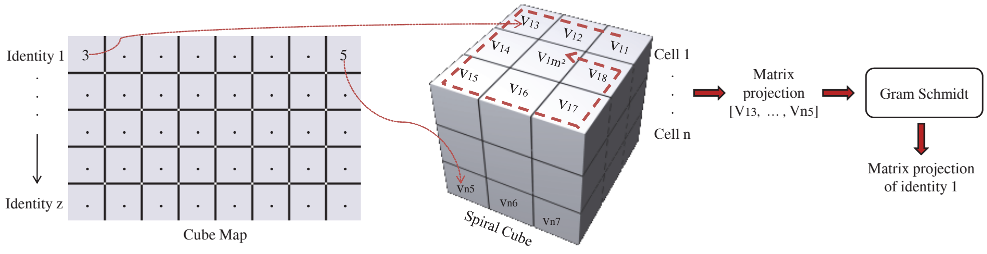


Fig. 2. Mechanism of projection matrix construction.

to project the reference templates of identity 1 (i.e., the template T). The same process is applied to compute the projection matrices for the other identities.

- We store the protected templates, spiral cube and cube map in the system database; the storage of the spiral cube and cube map is public.

During authentication, the protected system works as follows:

- Given a test template, we apply feature extraction and quantization (i.e., same process to that applied on the training templates during the enrollment stage).
- We use a KNN classifier to find the nearest vector in the *cube map* to the quantized test template.
- The closest vector is then used to find the projection matrix corresponding to the test vector and compute the protected test template.
- The protected template is then compared directly with the protected training templates; the comparison is being carried out according to the type of classifier used by the system.

The proposed technique meets the requirements of revocability, diversity and security. Given that multiple acquisitions of the same biometric trait will not in general yield an identical set of features, the dynamics of our approach allow us to create different templates for the same identity in the presence of these variations. In addition, we can protect a compromised template by changing partially the cube map (e.g., we can change the quantized vector corresponding to the identity of the compromised template, either by redoing the quantization or by changing partially this quantized vector). Thus, the revocability and diversity are assured. It should be noted that changing the spiral cube, or the order of cells in the spiral cube, requires redoing the steps of the enrollment stage; this is a weak point of our approach which we plan to address in future work. We analyze the security requirements of the proposed method in the next section.

4. Analysis study

The security analysis of existing methods is mainly based on the complexity of brute force attacks assuming that biometric data is uniform. First, let us analyze the scenario where the adversary has access to the protected template and the spiral cube. To recover the original template, one needs to find the projection matrix used. In this scenario, there are $(m^2 \times n)^n$ possible projection matrices. For example, if $n = 100$, the number of possible matrices is 100^{200} which provides high robustness against brute force attacks. Let us assume now that the opponent has access to the protected template, the spiral cube and the cube map (all public data). The number of possibilities in this scenario is $(m^2 \times z)^n$. Based on the complexity of brute force attack, we can say that even in the worst case scenario where the adversary has all the public data and the protected template, the security of our system is enough to be robust to attacks.

In practice, however, an adversary can exploit the non-uniform structure of data to launch an attack that may require far fewer attempts to compromise the security of the system. A rigorous security analysis, like Refs. 21 and 22, would be necessary in this case. Nagar *et al.*[21] proposed some criteria for assessing the overall security/privacy of protected systems. In particular, the authors emphasized the vulnerability of *feature transformation* approaches to *intrusion* and *cross-matching* attacks. This can be staged in the scenario of a protected template theft, to access illegitimately the system using falsified templates or to monitor users, covertly, in other systems.

The analytical equations presented in Refs. 21 and 22 are entirely based on the principle of calculating the *False Reject Rate* (FRR) and *False Accept Rate* (FAR). Although these statistical values are intuitively easy to understand, using them to set a clear and universal definition is very difficult and several factors should be taken into consideration. This is because these measures depend not only on the biometric system but also on the users data as well the thresholds used. Therefore, the comparison of biometric systems using these measures is reasonable only if their definitions coincide.

4.1. *Usability of biometric systems*

FAR is the probability that an unauthorized person is accepted by the system. FAR is a pertinent measure of security because a false acceptance can often lead to critical damage. The probability of success against a legitimate person θ is:

$$\mathrm{FAR}(\theta) = \frac{\text{number of successful fraud attacks}}{\text{total number of fraud attacks}} \tag{8}$$

— In a fraud attack, the system is attacked by unauthorized person template.
— The fraud attack is successful if the distance between the template of the person θ and the opponent template is *less than or equal* to a threshold ϵ.

The final FAR for Φ users is the average of all $\mathrm{FAR}(\theta)$ (for a single value of ϵ):

$$\mathrm{FAR} = \frac{1}{\Phi} \sum_{\theta=1}^{\Phi} \mathrm{FAR}(\theta)\,. \tag{9}$$

FRR is the probability that a legitimate person is rejected. FRR is a comfort criterion because a false rejection minimizes the credibility of biometric systems. The failure probability of a legitimate person θ is:

$$\mathrm{FRR}(\theta) = \frac{\text{number of rejected verifications}}{\text{total number of verifications}} \tag{10}$$

— Verification is a special case of identification. The biometric template is compared with a single identity in the system.
— A verification is rejected if the distance between the template of the person θ and the reference template is *strictly greater* than a threshold ϵ.

The final FRR for Φ users is the average of all $\mathrm{FRR}(\theta)$ (for a single value of ϵ):

$$\mathrm{FRR} = \frac{1}{\Phi}\sum_{\theta=1}^{\Phi} \mathrm{FRR}(\theta)\,. \tag{11}$$

We can measure the *usability* of a system, by plotting the ROC curve, in two scenarios: the original ROC_o (i.e., before protection) and the transformed ROC_t to indicate the performance degradation due to protection schemes. Belguechi *et al.*[21] proposed another criterion to measure the efficiency/usability which will be used in our analysis:

$$\text{Efficiency} = 1 - \frac{\mathrm{AUC}(\mathrm{ROC}_t)}{\mathrm{AUC}(\mathrm{ROC}_o)}\,. \tag{12}$$

— AUC is the area under the ROC curve

The value of this measure should be positive and as close to 1 as possible.

4.2. *Vulnerability to intrusion attack*

To measure the vulnerability of feature transformation approaches to intrusion attacks, we consider the scenario where *a* protected template is stolen from the database and the transformation parameters are known by the attacker. In this scenario, the opponent will try to recover the original template and replay the recovered template (in the *same* system) using the transformation parameters. Nagar *et al.* referred to this criterion as IRIS (*Intrusion Rate due to Inversion for the Same biometric system*):

$$\mathrm{IRIS}(\epsilon) = P\left[D(f(f^{-1}(T_i, k_i), k_i), T_i) < \epsilon\right]. \tag{13}$$

— D is the distance function.
— f is the transformation function.
— f^{-1} is the inverse transform function.
— $T_i = f(t_i, k_i)$ is the stolen transformed template.
— t_i is the original template of the identity i.
— k_i are the transformation parameters of identity i.

Considering the previous scenario, let us now assume that the opponent attacks another biometric system that contains the same stolen identity, assuming that the attacker knows the transformation parameters of the second system. Nagar *et al.* referred to this criterion as IRID (*Intrusion Rate due to Inversion for a Different biometric system*):

$$\mathrm{IRID}(\epsilon) = P\left[D(f(f^{-1}(T_i, k_i), k'_i), T'_i) < \epsilon\right]. \tag{14}$$

— $T'_i = f(t'_i, k'_i)$ is the transformed template of the identity i in the second system.
— t'_i is the original template of the identity i in the second system.
— k'_i are the transformation parameters of identity i in the second system.

IRIS and IRID depend on the threshold ϵ. It is easy to reverse a biometric template, for a transformation approach, if IRIS and IRID are near or equal to 1.

4.3. *Vulnerability to cross-matching attack*

The vulnerability of feature transformation approaches to *cross-matching* attacks can be measured by considering the scenario where the enemy has stolen *two* the biometric templates of the same identity from two different systems that use the same protection scheme, and he/she knows the transformation parameters of these two systems. The opponent can launch his attack either in the original domain or in the transformation domain. We can calculate CMR (*cross-matching rate*) in these two domains as follows:

$$\mathrm{CMR}_o(\epsilon) = P\left[D(f^{-1}(T_i, k_i), f^{-1}(T'_i, k'_i)) < \epsilon\right]. \tag{15}$$

— CMR_o is the cross-matching rate in the original domain.

$$\mathrm{CMR}_t(\epsilon) = P\left[D(f(t_i, k_i), f(t'_i, k'_i)) < \epsilon\right]. \tag{16}$$

— CMR_t is the cross-matching rate in the transformation domain.

A study of cross-matching attack is very useful to measure the *diversity* of protection schemes. We propose to apply the *Kolmogorov-Smirnov* test to measure the distributions of legitimate/impostor scores. The closer the *Kolmogorov-Smirnov* test is to 1, the more the scores are separated, which means that diversity is high.

5. Experimental Results

In this section, we evaluate the *Spiral Cube* approach using the analytical equations presented in the previous section and several real databases. Moreover, we compare its security/performance with *Biohashing* and *BioPhasor*.

5.1. *Data sets establishment and experimental procedure*

We have considered three modalities and four databases in our experimentation: the YALE and SHEFFIELD databases for face recognition, the PolyU FKP database

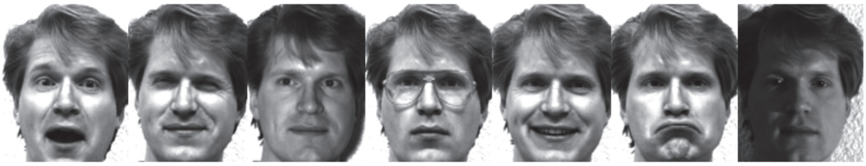


Fig. 3. Examples from YALE database.

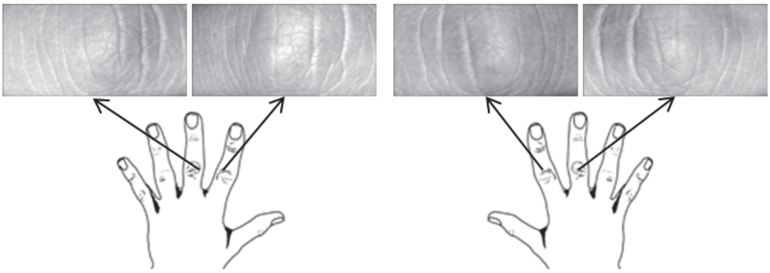


Fig. 4. Examples from PolyU FKP database.

for finger-knuckle-print recognition and the CASIA-Iris-Interval database for iris recognition.

The YALE face database (Fig. 3) consists of 165 face images from 15 distinct persons. The database covers a mixed range of race, gender and appearance; images are characterized by variations in facial expressions and lighting conditions. We have considered 11 identities as legitimate users and 4 identities as impostors. Each legitimate user was represented by 5 images. Thus, our training set contains 55 templates while our test set contains 66 images. Each impostor has the possibility of launching 11 fraud attacks.

The PolyU FKP database (Fig. 4) consists of 7920 finger-knuckle-print images from 165 distinct persons. The basic idea behind this new modality is to use the area around the phalange seal of one's finger as a biometric trait. Each person is represented by 48 images from 4 fingers (middle/index right fingers and middle/index left fingers). We have considered 100 identities as legitimate users and 65 identities as impostors. Each legitimate user is represented by 4 images. Thus, our training set contains 400 templates while our test set contains 4400 images. Each impostor has the possibility of launching 8 fraud attacks. The main objective to use this modality (which is characterized by average intra-subject variations) is to evaluate protection schemes in the presence of a significant number of identities.

The CASIA-Iris-Interval database (Fig. 5) contains iris images from 249 distinct persons; we keep only 122 persons who have images both for left and right iris. We build the biometric templates using the technique proposed in Ref. 23. We have considered 100 identities as legitimate users and 22 identities as impostors. Each legitimate user was represented by 2 images. Thus, our training set contains 200

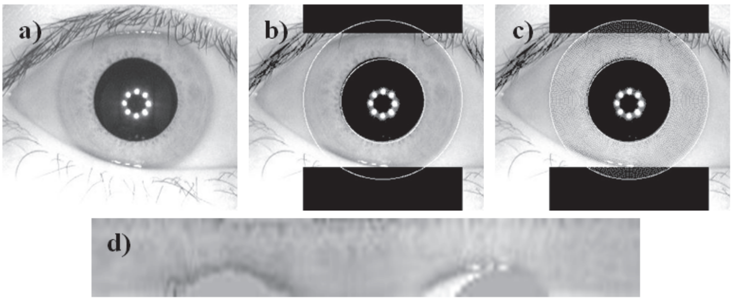


Fig. 5. (a) Eye image from CASIA database, (b) iris detection, (c) segmentation and (d) normalization.

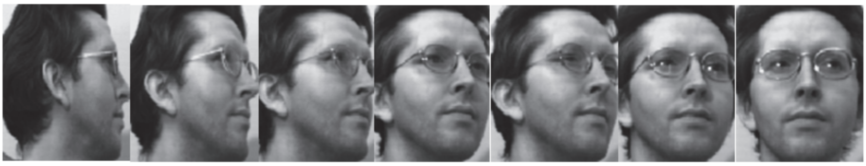


Fig. 6. Examples from SHEFFIELD database.

templates while our test set contains 200 images. Each impostor has the possibility of launching 2 fraud attacks. The iris modality provides, despite errors during iris extraction from eye images, perfect reliability and high uniqueness (i.e., the probability of finding two identical irises is 10^{-72} according to Ref. 26). The design of a robust system requires representing each class by several iris templates. The main objective to use this modality is to evaluate protection schemes in a non optimal design of unprotected system, containing a large number of identities, where each identity is represented by two templates (i.e., left and right iris).

The SHEFFIELD face database (Fig. 6), previously called UMIST, consists of 564 face images from 20 distinct persons. Faces in the database cover a wide range of poses from profile (90°) to frontal (0°) views. Our objective in using this database is to evaluate and compare the security of protection schemes in the presence of serious intra-subject variations. For the SHEFFIELD database, each person was represented by 6 images and the *leave-one-out* approach was used for testing.

For each database, we applied three protection schemes: Spiral Cube, Biohashing, and BioPhasor. Results were compared and analyzed using the criteria given in Section 4. The use of analytical equations requires the recovery of the original template z from the protected template y, assuming that the adversary has the orthogonal matrix Δ. To recover a close approximation of the transformed vector y from the quantized template t, we solve first a least-squares problem:

$$\operatorname{argmin}\|z - r\|_2 \quad \text{subject to} \begin{cases} y_i \leq \tau & \text{if} \quad t_i = 0 \\ y_i > \tau & \text{if} \quad t_i = 1 \end{cases} \tag{17}$$

— $i = 1, \ldots, n$ and $y_i = \sum_{j=1}^{n} \Delta_{ij} z_i$.
— r is a random vector of size n where $r \times z \leq \tau$.
— n is the size of the original and transformed templates.

Second, to optimize the approximation of z, we solve the problem for k different values of r. The final approximation $\tilde{z}$ is calculated as follows:

$$\tilde{z} = \frac{\sum_{i=1}^{k} \frac{z_i}{d_i^2}}{\sum_{i=1}^{k} \frac{1}{d_i^2}} . \tag{18}$$

— z_i is the original estimated vector using r_i.
— $d_i = \frac{1}{d'_i}$ where d'_i is the Hamming distance between z_i and t.

For BioPhasor, the optimization problem is more complicated given the effect of the *arctan* transformation. To recover an acceptable approximation, we use the same procedure applied in Biohashing (with $\tau = \pi$) by adding this optimization step on $\tilde{z}$:

$$\tilde{z}_i = \Delta_{i1} \times \tan\left(m\tilde{z}_1 - \sum_{j=2}^{m} \operatorname{atan}\left(\frac{1}{\Delta_{ij} \times \tilde{z}_j} \right) \right) . \tag{19}$$

— $m \leq n$ and $i = 1, \ldots, n$.
— $\hat{z}$ is the final approximation for BioPhasor template.

5.2. *Feature extraction*

The biometric system used in our experimentation is based on a feature extraction method based on the Laplacian Smoothing Transform (LST)[24] and a KNN classifier for recognition. The size of original and protected templates is 100. A common drawback of statistical methods is that each pixel is considered independently, ignoring correlations with its neighbors. LST is used to represent the image in the frequency domain keeping the connection between pixels and their neighbors. Compared to Discrete Cosine Transform (DCT) and Discrete Wavelet Transform (DWT),[25] LST was shown to be more robust.[24] The main steps of LST approach are:

- Calculate a weight matrix W of size $MN \times MN$ (M and N are the dimensions of the image):

$$W(\lceil x, y \rceil \lceil x', y' \rceil) = \begin{cases} 1 & \text{if } |x - x'| + |y - y'| = 1 \\ 0 & \text{if } |x - x'| + |y - y'| \neq 1 \end{cases} \tag{20}$$

  — $\lceil x, y \rceil = x \times N + y$
  — x and y are pixel coordinates.

- Calculate D, a diagonal matrix whose entries are column (or row) sums of W (i.e., since W is symmetric):

$$D(\lceil x,y\rceil\lceil x,y\rceil) = \sum_{\lceil x,y\rceil} W(\lceil x,y\rceil\lceil x',y'\rceil) \tag{21}$$

- Calculate the *Laplacian Matrix*:

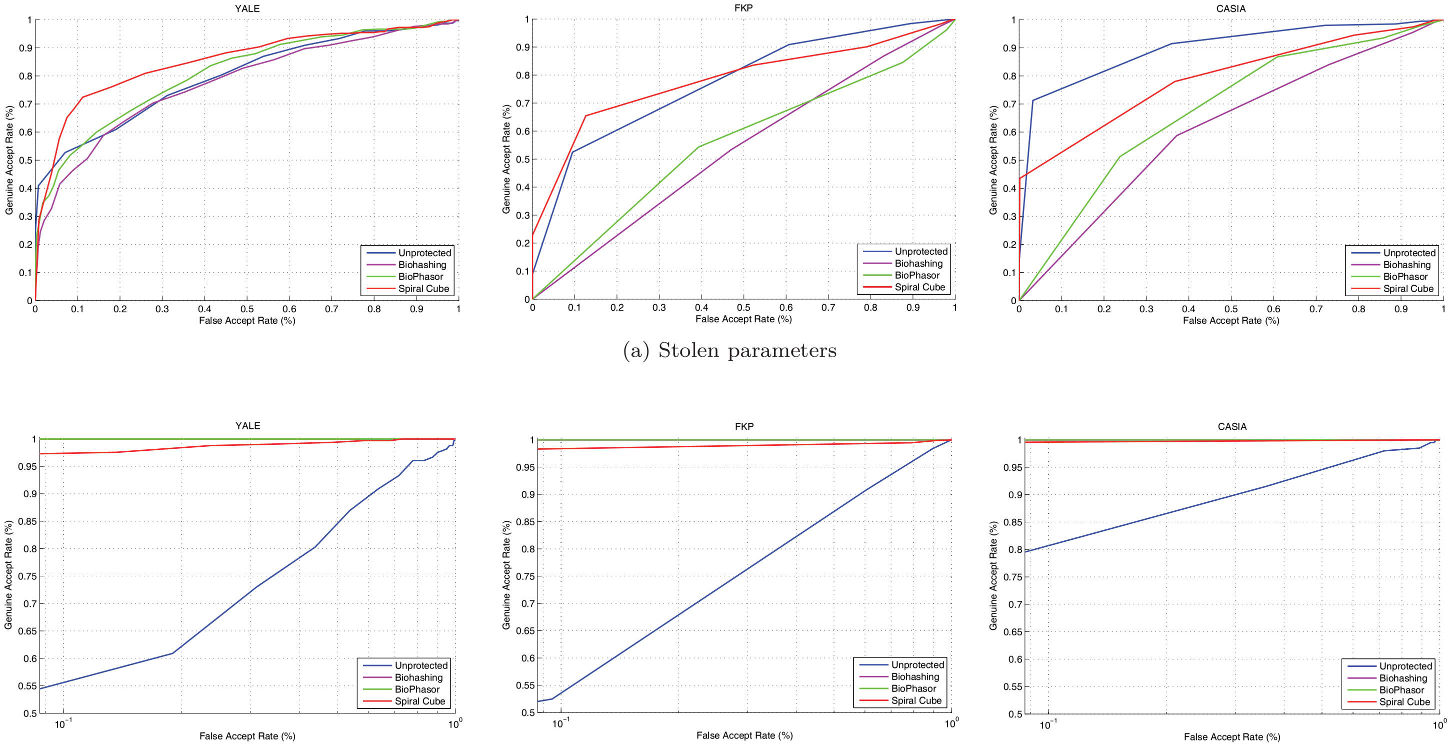
$$L_{MN} = D - W \tag{22}$$

- Compute the first k eigenvalues and corresponding eigenvectors E_k (i.e., k depends on the number of adequate low frequencies).
- Project training and test images using E_k.

It should be noted that any feature extraction method could have been used here to construct the templates; this is because our interest is on evaluating the effect of protection schemes on performance rather than improving performance. In particular, our interest in evaluating performance using large size templates (i.e., subsection 5.5) and our past experience motivated us to use LST. In contrast to traditional methods, such as PCA and LDA, the computational requirements of LST are not strongly related to the dimensionality of the original data but depend on the number of eigenvectors of the *sparse* Laplacian matrix L_{MN} which needs to be calculated for an MN×MN image.

5.3. *Evaluation using the YALE, FKP and CASIA databases*

Figure 7 shows the ROC curve of the unprotected system as well as the ROC curves of the three protection schemes considered in this study. First, we discuss the zero effort attack scenario (Fig. 7(a)) where the transformation parameters are known by the opponent who has tried to circumvent the system using their own templates. For the YALE database, small performance degradation can be observed in the case of Biohashing while classification performance is increased in the case of Biophasor and Spiral Cube. In practice, the three approaches need additional information (key, password, Spiral Cube, Cube Map, etc.) during authentication/identification. In the case of Biohashing, the key is used without additional processing. On the contrary, in the case of BioPhasor and Spiral Cube, even if the opponent has additional information, further processing is required to deploy the stolen parameters correctly. In the case of the FKP database, we can observe a significant degradation of the performance in the case of Biohashing and BioPhasor. In contrast, the classification performance is increased in the case of Spiral Cube. In practice, the presence of intra-subject variations and a large number of identities can help the opponent to reach the system's security and increase the success chance of the zero effort attack. For the CASIA database, matching performance for the unprotected scheme is significantly degraded compared to the three protection schemes. Among them, Spiral Cube has the best performance with a degradation of 10.14% (see Table 1).



(a) Stolen parameters

(b) Unknown parameters

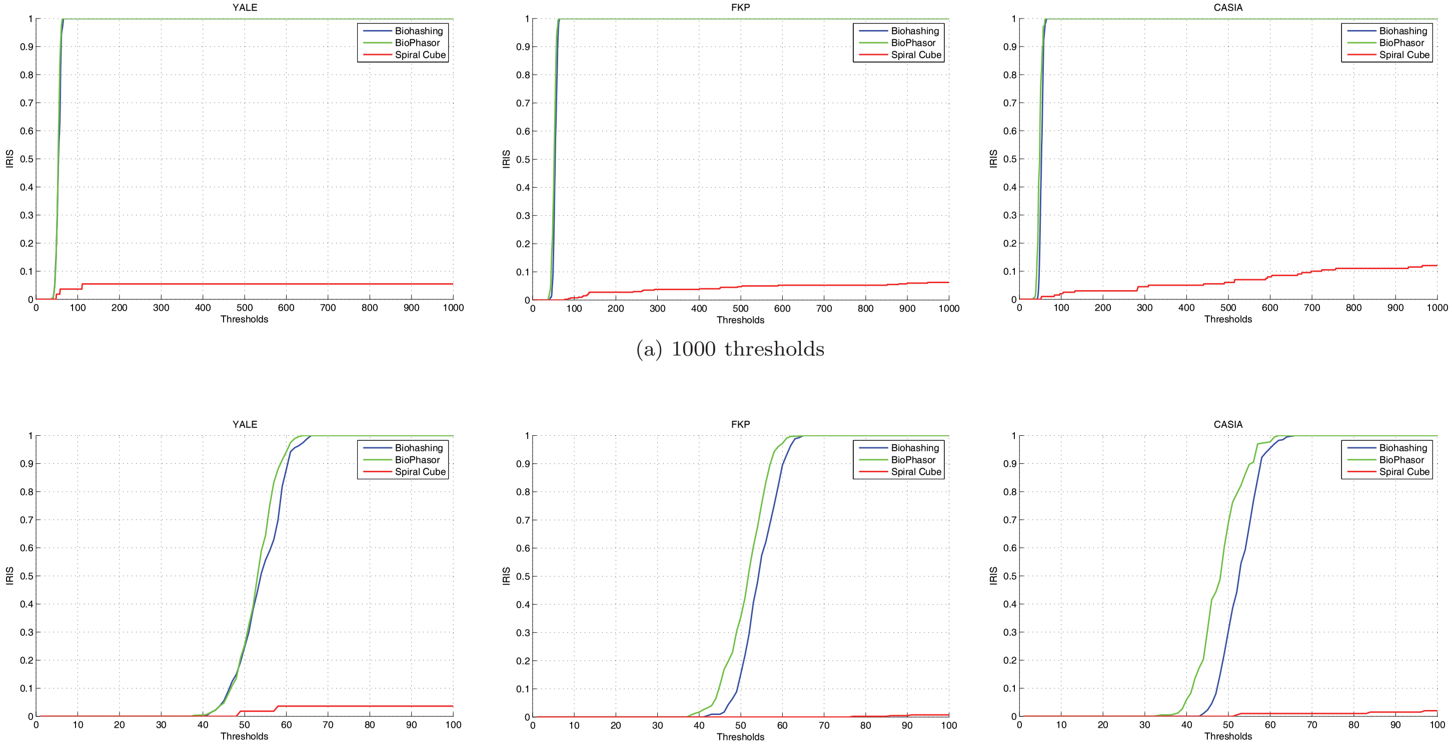
Fig. 7. ROC curves using YALE, FKP and CASIA databases.

The increase in FRR, which is mainly due using a low number of templates per identity, justifies this result.

In the scenario where the opponent does not have the transformation parameters (Fig. 7(b)). For the three Databases, we observe a significant increase in performance for the three protected systems in comparison with the unprotected system. The reduction of FAR, due to using a specific key for each user, makes this result evident. We can also notice a small performance degradation of the Spiral Cube approach in comparison with the Biohashing and BioPhasor approaches. This can be explained by the different ways that additional information is being used. At the time of authentication, the user is required to present his/her key in Biohashing/BioPhasor protected systems. In the case of the Spiral Cube approach, authentication takes place with no need of a key. Therefore, Biohashing and BioPhasor require additional cooperation of users which makes these protected systems similar to those using passwords and ID cards. This binding requires users to comply with the technical requirements of these protection schemes, which is usually a drawback of effectiveness and acceptance. In this context, we can claim that our approach aims to provide a balance between security and performance but also user acceptance which is a requirement of biometric systems.

Figure 8 shows the IRIS curves of the three protection schemes. For the YALE database, we can observe in the interval $[0, 38]$ of thresholds that the three protection schemes resist 100% against intrusion and inversion of protected templates. Biohashing and BioPhasor become very vulnerable against this attack in the interval $[38, 62]$. In contrast, Spiral Cube maintains a very low IRIS and it is able of resisting against intrusion into the same system. After threshold value 65, the success rate of the attack is 100% for Biohashing and BioPhasor. The Spiral Cube approach maintains a success rate of 5.45%. In the case of the FKP database, It can be observed that the protection schemes resist perfectly to intrusion and inversion of protected templates in the $[0, 40]$ interval of thresholds. Biohashing and BioPhasor become very vulnerable against this attack in the interval $[40, 65]$. Unlike the YALE database experiments, we can notice a small degradation of BioPhasor resistance compared to Biohashing, which proves the effectiveness of our proposed optimization step to recover an approximation of a BioPhasor template. After threshold value 65, the success rate of the attack is 100% for Biohashing/BioPhasor protected systems. The Spiral Cube approach maintains a success rate of 6.25%. For the CASIA database, Biohashing and BioPhasor resist to 100% for the first 43 and 32 thresholds respectively. Then, IRIS rate increases rapidly and the protected systems become vulnerable to 100% after threshold value 65. The Spiral Cube approach maintains a success rate of 12% (6.25% for FKP experiments), which confirms that the unprotected systems design influences the efficiency of protection schemes.

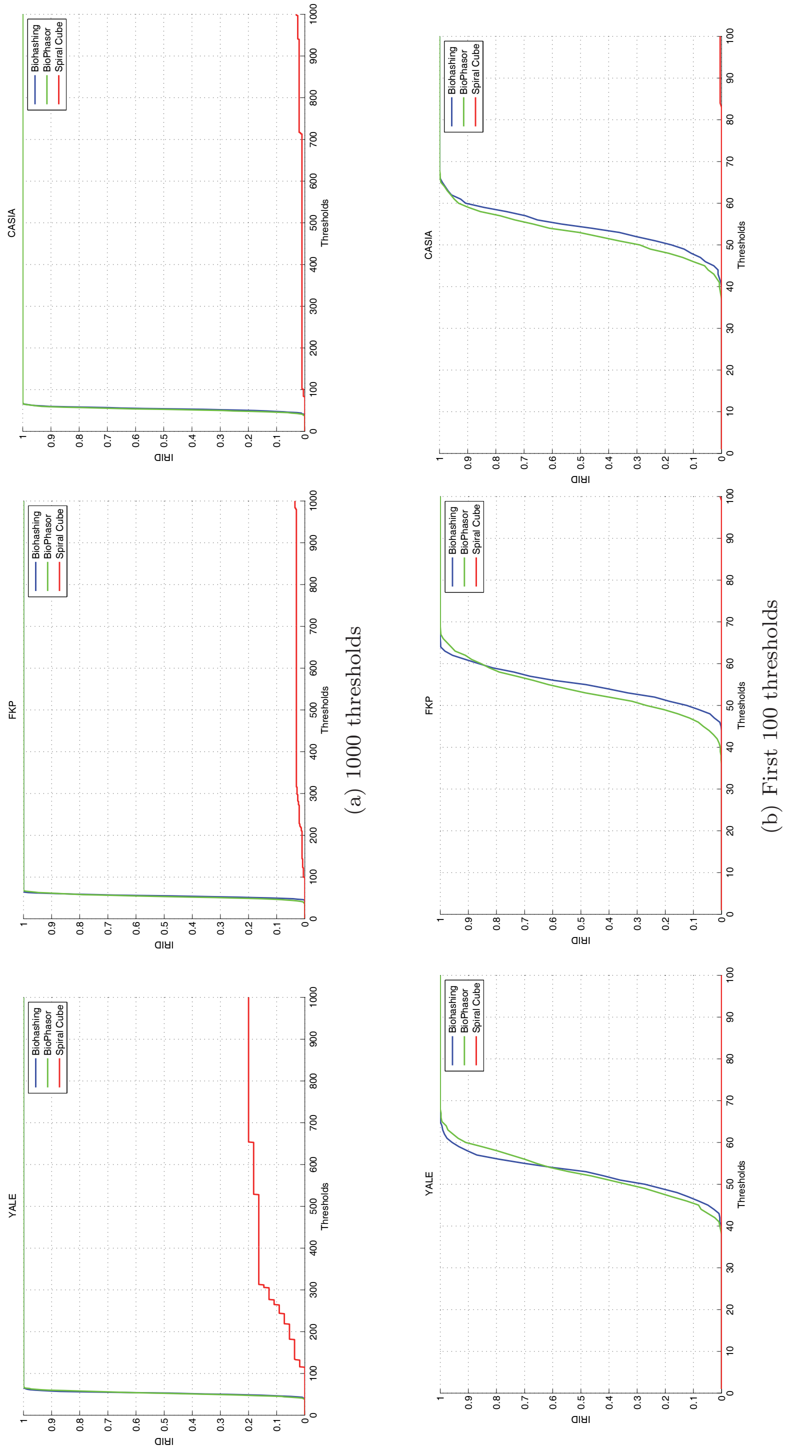
For IRID curves (Fig. 9), we discuss the scenario where the intrusion takes place in a different system containing the same compromised identity. For YALE database, the Biohashing and BioPhasor schemes resist 100% for the first 40 thresholds. Then, IRID increases rapidly and protected systems become vulnerable to



(a) 1000 thresholds

(b) First 100 thresholds

Fig. 8. (Color online) IRIS curves using YALE, FKP and CASIA databases.



(a) 1000 thresholds

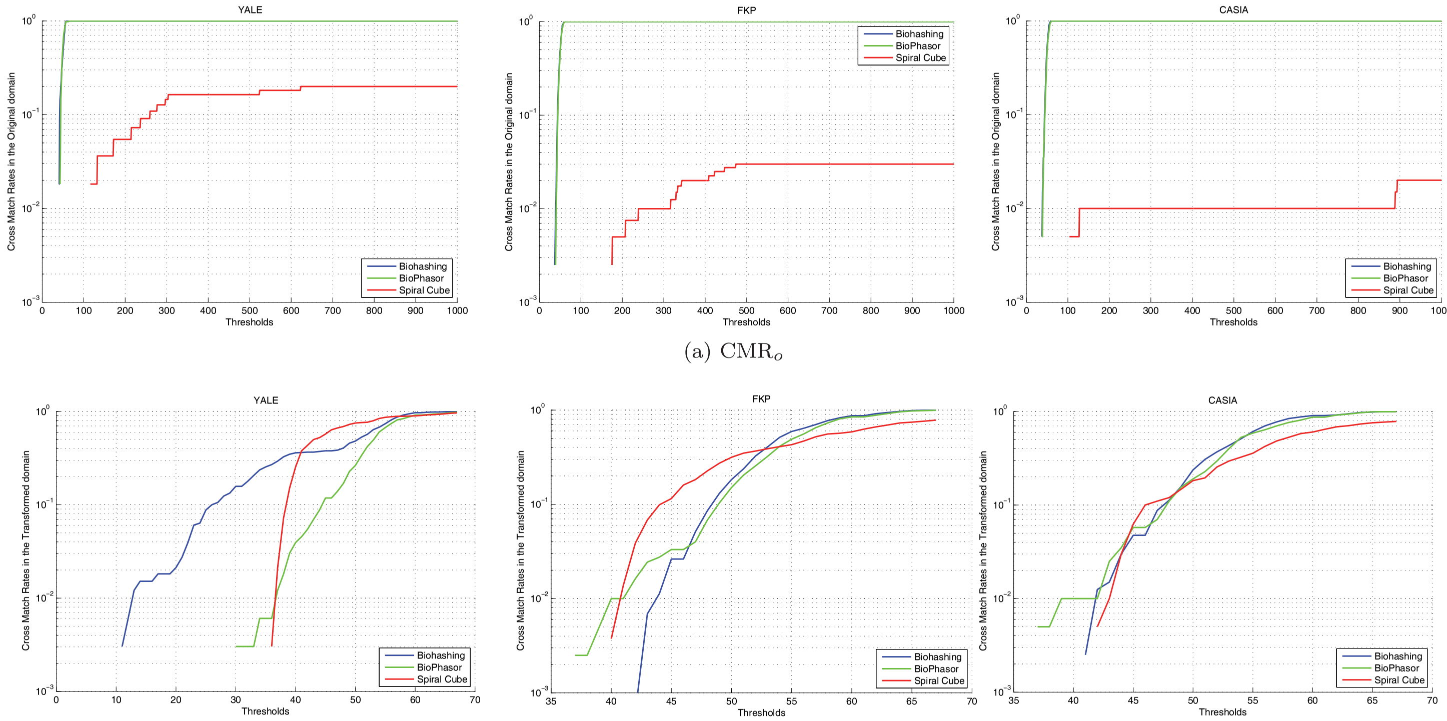
(b) First 100 thresholds

Fig. 9. (Color online) IRID curves using YALE, FKP and CASIA databases.

100% after threshold value 65. For the Spiral Cube, the attack fails to 100% until threshold value 120; it retains a success rate of 20% even after 1000 thresholds. These results show clearly that the Spiral Cube protection scheme provides a very high level of security in comparison to Biohashing and BioPhasor. Therefore, it can be concluded that it provides a high non-invertibility to biometric templates. In the case of the FKP database, Biohashing and BioPhasor resist to 100% respectively for the first 46 and 40 thresholds respectively. Then, IRID increases rapidly and the protected systems become vulnerable to 100% after threshold value 65. For Spiral Cube, the attack fails to 100% until threshold value 99 and it retains a very small success rate of 3.5% (20% for YALE experimentation) even after 1000 thresholds. These results show clearly that Spiral Cube's security significantly increases if the number of identities is large as we have theoretically shown in the section 4. For the CASIA database, the unprotected system design has this time an opposite effect on an intrusion attack using a stolen template from a different biometric system (in comparison to YALE and FKP experiments). Spiral Cube retains a very small success rate of 2.5% (20% and 3.5% for the YALE and PolyU FKP experiments) even after 1000 thresholds.

Figure 10 illustrates the success of cross-matching of two protected templates, of the same identity, which are stolen from two different systems. In the original domain (Fig. 10(a)); for the YALE database, the two templates can be easily linked after threshold values 40 and threshold 44 respectively in the case of Biohashing and BioPhasor; this is reasonable as we have already shown in Fig. 8 that inversion becomes easy after these threshold values. The success rate is 100% after threshold value 55. In the case of the Spiral Cube approach, the success rate is 0% until threshold value 120; it retains a success rate of 20% even after 1000 thresholds. For the FKP database, the results of Biohashing/BioPhasore schemes are very similar to those obtained using the YALE database. For the Spiral Cube approach, the success rate is 0% until threshold value 174 and it is stable at 3% (20% for YALE experimentation) even after 1000 thresholds. Spiral Cube's resistance to cross-matching is significantly increased, compared to the YALE database experiments, because inversion becomes very difficult in the presence of a large number of identities. In the case of the CASIA database, the results of protection schemes are relatively similar to those obtained using the PolyU FKP database. A small degradation can be observed in the case of Spiral Cube (i.e., the success rate is 0% for the first 100 thresholds for the CASIA-iris database and 0% for the first 174 thresholds for the PolyU FKP database) due to the degradation of IRIS which is primarily due to the unprotected systems design in our CASIA-iris experimentation.

The study of cross-matching in the transformation domain (Fig. 10(b)) is very useful to measure the diversity of protection schemes. For the YALE database, the success rate is 0% for Biohashing, BioPhasor and Spiral Cube before threshold values 12, 30 and 37 respectively. After threshold 37 for Biohashing and 42 for BioPhasor, to threshold value 52, these two schemes are becoming more resistant



(a) CMR_o

(b) CMR_t

Fig. 10. (Color online) CMR curves using YALE, FKP and CASIA databases.

than the Spiral Cube. After threshold value 52, they become more vulnerable than Spiral Cube. In the case of the FKP database, the success rate is 0% for Biohashing, BioPhasor and Spiral Cube after threshold values 41, 36 and 39 respectively. After threshold value 40, Biohashing and BioPhasor are more resistant than Spiral Cube. Then, after threshold value 54, they become more vulnerable than Spiral Cube. For the CASIA database, the success rate is 0% for Biohashing, BioPhasor and Spiral Cube after threshold values 40, 36 and 31 respectively. After threshold value 50, Biohashing and BioPhasor are more vulnerable than Spiral Cube.

It should be noted that the main drawback of non-invertible transformation approaches is the non-ability to design techniques that meet *discrimination*, *diversity* and *non-invertibility* simultaneously. Discrimination is the capacity to minimize intra-subject distances and increase inter-subject distances. In this context, we can explain the results of Fig. 10 as follows. Spiral Cube demonstrated high non-invertibility compared to the Biohashing and BioPhasor which justifies its ability to be more resistant against cross-matching in the original domain. In the transformation domain, results are quite similar for all three approaches. Overall, the Spiral Cube approach can increase non-invertibility without degrading diversity and discrimination even in systems containing a large number of identities or its design is non optimal.

Table 1 presents several other criteria that demonstrate the robustness of Spiral Cube and confirm the results of the performance/security analysis curves. In the stolen parameters scenario, Spiral Cube provides the best performance, diversity and efficiency. For the YALE database, the three approaches increase the performance and maintain the diversity/efficiency. However, in the case of the FKP database, Biohashing and BioPhasor lose efficiency completely. Moreover, we can observe a significant degradation in diversity. Spiral Cube maintains very acceptable values for all criteria. For the CASIA database, the performance of the three protection schemes is degraded compared to the unprotected system and efficiency is lost due to the non optimal design of unprotected system. In the unknown parameters scenario, a significant increase in performance, diversity and efficiency due to using a specific key for each user (reduction of FAR). In general, the three protection schemes have similar performance; a small degradation can be noticed for the Spiral Cube approach due to our interest in meeting the discrimination, diversity, non-invertibility and user acceptance simultaneously.

5.4. *Evaluation using the SHEFFIELD database*

The purpose of this experiment is to study the security in the presence of important intra-subject variations (i.e., multi-view in our case). In addition, we aim to study security in a system that uses small size templates and contains a small number of identities (i.e., we have already shown that the security of Spiral Cube is enhanced with increasing the number of identities and template size). Thus, this experiment aims to evaluate Spiral Cube's security in a non-ideal conditions.

Table 1. Usability/efficiency criteria of YALE, FKP and CASIA databases.

		YALE			FKP			CASIA		
	Protection Approach	EER	K-S Test	Efficiency	EER	K-S Test	Efficiency	EER	K-S Test	Efficiency
	Unprotected	28.85%	0.4613	———	31.22%	0.4624	———	19%	0.7224	———
Stolen parameters	Biohashing	26.53%	0.4285	0.0527	46.84%	0.0633	−1.0427	39.56%	0.1201	−2.7847
	BioPhasor	25.93%	0.4554	0.1740	43.23%	0.0736	−0.9581	36.53%	0.2624	−2.1380
	Spiral Cube	21.58%	0.6185	0.2705	27.68%	0.6857	0.0419	29.14%	0.5806	−1.0460
Unknown parameters	Biohashing	0.27%	0.9935	0.9999	1%	0.9948	0.9903	1%	0.9974	0.9755
	BioPhasor	0.48%	0.9927	0.9998	2%	0.9900	0.9802	0.98%	0.9933	0.9785
	Spiral Cube	2.73%	0.9686	0.9574	3.35%	0.8007	0.9520	4.92%	0.8260	0.9070

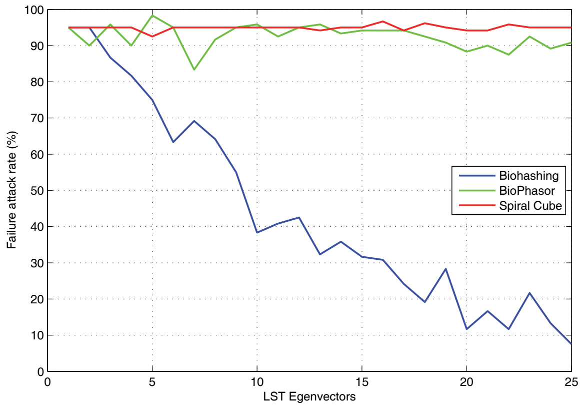
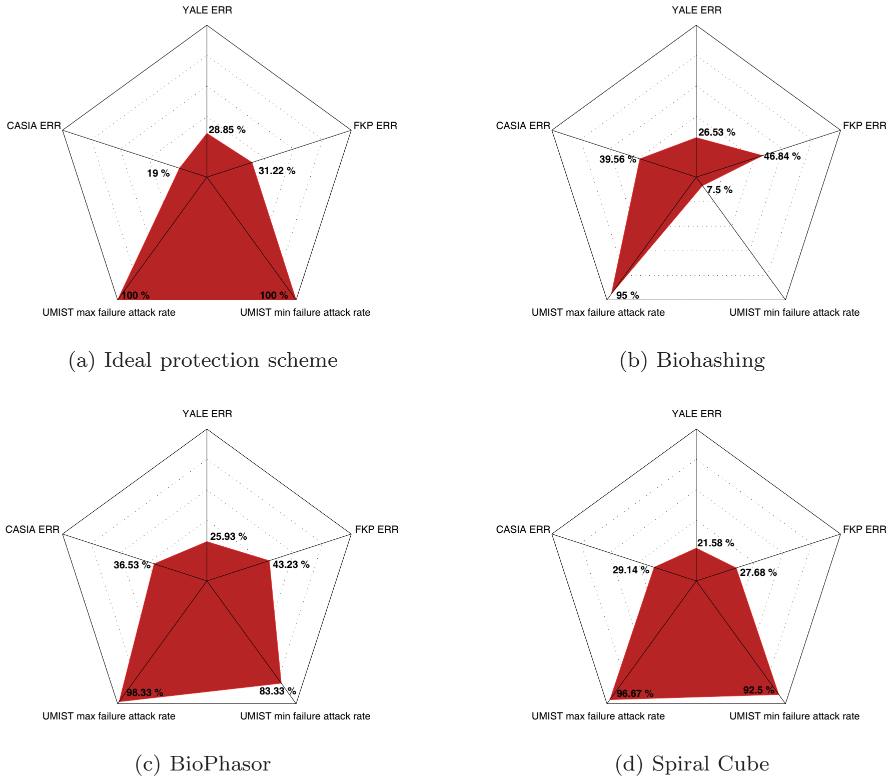


Fig. 11. (Color online) Failure rate of the proposed attack.

For the SHEFFIELD database, we have adopted a leave-one-out approach in order to evaluate the three protection schemes. In this context, each algorithm is ran N times. Each time, N-1 samples are used for training and the remaining sample is supposed to be a stolen sample from the system. The opponent tries to recover the original template (i.e., we assume that he/she knows the transformation parameters of the stolen template). Then, the approximation is used to access the system. If the opponent is accepted, the attack success of that run would be 100%, otherwise it would be 0%. The overall attack success is the mean success of all N runs.

Figure 11 shows the results of the three protection schemes. We observe that Biohashing is very vulnerable in these test conditions and that the opponent can easily compromise security. Spiral Cube and BioPhasor have shown great non-invertibility even when the number of identities and template size are small. Spiral Cube performs slightly better than BioPhasor. Therefore, the security of our approach is sufficiently robust to possible attacks in non-ideal test conditions.

Figure 12 summarizes the results of the three protection schemes in the case where the size of original and protected templates is 100 for the databases YALE, FKP and CASIA, and it summarizes also the results of Fig. 11 using the SHEFFIELD database. For the Equal Error Rate (EER), we have considered only the scenario where the transformation parameters are known by the opponent. Figure 12(a) illustrates the desired results of an ideal protection scheme which is able to maintain, at least, the EER of an unprotected system and it is resistant to 100% against attacks. For the YALE database, which is characterized by negligible intra-subject variations and limited number of identities, the three schemes meet the required performance and spiral cube has the best performance. For the FKP database, which is characterized by average intra-subject variations and large number of identities, we can observe a significant degradation of performance in the case of Biohashing and BioPhasor. The performance of spiral cube is increased. In the case of the CASIA database, where the design of unprotected system is non



(a) Ideal protection scheme

(b) Biohashing

(c) BioPhasor

(d) Spiral Cube

Fig. 12. Illustration of protection schemes results.

optimal, the performance of the three protection schemes is degraded. In the case of the SHEFFIELD database, BioPhasor and Spiral Cube proved high level of security while Biohashing is very vulnerable in these conditions of experimentation. Overall, Spiral Cube is the closest to an ideal protection scheme.

In the previous subsection, performance evaluation/comparison of Spiral Cube with Biohashing and BioPhasor takes place using a template size of 100. The next subsection aims to extend our experiments on YALE, FKP and CASIA databases using large sizes of original and protected templates.

5.5. *Performance evaluation using large size template*

Table 2 illustrates the performance, diversity and efficiency criteria in the case of the YALE, FKP and CASIA databases using different template sizes including three large sizes. In our evaluation, we have considered only the scenario where the transformation parameters are known by the opponent. When the transformation parameters are unknown, we have shown in the previous subsections that all evaluation criteria for the three protection schemes improve significantly regardless evaluation conditions.

Table 2. Usability / efficiency criteria using different template sizes.

		YALE			FKP			CASIA		
Size	Protection Approach	EER	K-S Test	Efficiency	EER	K-S Test	Efficiency	EER	K-S Test	Efficiency
10	Unprotected	32.48%	0.4344	———	40.96%	0.5745	———	33.53%	0.6647	———
	Biohashing	36.87%	0.2893	−0.0386	48.94%	0.0389	−0.3756	45.23%	0.1423	−0.6265
	BioPhasor	37.08%	0.2607	−0.1315	48.85%	0.0408	−0.3724	44.68%	0.1211	−0.5649
	Spiral Cube	22.79%	0.4785	+0.3142	42.30%	0.2415	−0.1820	37.36%	0.2524	−0.2670
50	Unprotected	30.34%	0.4691	———	31.76%	0.5459	———	20.13%	0.7532	———
	Biohashing	32.41%	0.3530	−0.2549	47.82%	0.0627	−1.1666	41.67%	0.1786	−2.6809
	BioPhasor	29.70%	0.4390	−0.0695	47.79%	0.0597	−1.1713	43.18%	0.6450	−2.8618
	Spiral Cube	21.03%	0.5541	+0.2762	24.73%	0.7016	+0.1187	36.95%	0.5507	−1.8250
100	Unprotected	28.85%	0.4613	———	31.22%	0.4624	———	19%	0.7224	———
	Biohashing	26.53%	0.4285	+0.0527	46.84%	0.0633	−1.0427	39.56%	0.1201	−2.7847
	BioPhasor	25.93%	0.4554	+0.1740	43.23%	0.0736	−0.9581	36.53%	0.2624	−2.1380
	Spiral Cube	21.58%	0.6185	+0.2705	27.68%	0.6857	+0.0419	29.14%	0.5806	−1.0460
250	Unprotected	29.07%	0.9498	———	34.54%	0.3522	———	18.48%	0.6796	———
	Biohashing	28.85%	0.4968	−0.0202	45.12%	0.1307	−0.4959	36.68%	0.2672	−1.9708
	BioPhasor	24.18%	0.5262	+0.2035	46.92%	0.0647	−0.5719	34.67%	0.1783	−1.6197
	Spiral Cube	21.36%	0.5460	+0.2729	27.37%	0.7580	+0.3405	15.38%	0.8191	+0.1228
500	Unprotected	28.65%	0.9577	———	38.27%	0.2660	———	19.96%	0.6474	———
	Biohashing	29.51%	0.4218	−0.0775	44.26%	0.1157	−0.2740	33.75%	0.3250	−1.3152
	BioPhasor	25.87%	0.5183	+0.1604	46.55%	0.0694	−0.3588	37.33%	0.2062	−1.5129
	Spiral Cube	24%	0.4001	+0.1266	38.12%	0.3903	−0.0238	30.93%	0.6231	−0.8046
1000	Unprotected	28.74%	0.8601	———	40.79%	0.2154	———	23.66%	0.5578	———
	Biohashing	27.55%	0.4573	+0.0267	39.68%	0.1180	+0.0347	28.91%	0.3756	−0.2825
	BioPhasor	23.89%	0.5452	+0.2034	45.57%	0.0798	−0.1793	39.69%	0.1955	−1.0498
	Spiral Cube	18.73%	0.5920	+0.4422	42.62%	0.7269	+0.0044	27.60%	0.7501	−0.1817

For the YALE database, Biohashing and BioPhasor maintain the performance/diversity of the unprotected system; however, their efficiency decreases for template sizes of 10 and 50 in both approaches and template sizes of 250 and 500 in the case of Biohashing. Spiral Cube improves performance and maintains the diversity/efficiency of the unprotected system under different template sizes. For the FKP database, we can observe some degradation in performance/diversity both for Biohashing and BioPhasor. Moreover, efficiency is lost for different template sizes. Spiral Cube provides very acceptable values for all criteria (except efficiency for template sizes 10 and 500). In the case of the CASIA database, the performance/diversity of the three protection schemes are degraded while efficiency is lost for most template sizes. However, even the non optimal design of unprotected system, we can observe that Spiral Cube provides acceptable values for all criteria in the case of template size 250. In general, the results of Table 2 are consistent with the results presented in previous subsections. Spiral Cube provides the best performance, diversity and efficiency. In general, we can conclude that the efficiency of protection schemes is affected by the design of unprotected systems, the presence of intra-subject variations and the number of identities.

6. Conclusion

In this paper, we proposed a new approach for biometric template protection based on random projection and the chaotic behavior of logistic map. We used the logistic map to generate linearly independent vectors for random projection. These vectors were stored in a spiral cube, which was then used to generate the protection matrices. Our vector selection mechanism makes the projection matrices depend on the template to be protected and its identity. Our approach meets revocability, diversity and security, which are required in an ideal method for template protection. In addition, it does not only preserve recognition performance but increases it (i.e., due to using a dynamic projection matrix for each identity). Thus, it manages better intra-subject variations. Our results, based on several protection schemes and modalities, indicate that the design of unprotected systems influences relatively the efficiency of protection schemes. Moreover, our results confirm that the presence of intra-subject variations make non-invertible transformation approaches less resistant to possible attacks which require far fewer attempts to compromise the security in this case.

For future work, we plan to test the proposed approach on large database applications. Moreover, generating the projection matrices using Gram-Schmidt orthogonalization is time consuming, however, there are less expensive methods which do not require applying orthogonalization such as (Ref. 27). Testing this algorithm is among our future work objectives. It should be noted that the proposed approach is appropriate for biometric systems employing vector templates; we plan to extend the Spiral Cube approach to other types of templates, for example, minutiae-based templates in fingerprint-based systems.

Acknowledgments

The first author is a fulbright visiting scholar, to University of Nevada-Reno, of the Moroccan-American Commission for Educational and Cultural Exchange. The first author would like to thank Dr. Abdul Wadood (Computer Engineering Department, CCIS, King Saud University, Riyadh, Saudi Arabia) for his pedagogic assistance.

References

1. N. K. Ratha, J. H. Connell and R. M. Bolle, An analysis of minutiae matching strength, *Third Int. Conf. on Audio- and Video-Based Biometric Person Authentication* (Halmstad, Sweden, 2001).
2. A. K. Jain, K. Nandakumar and A. Nagar, Biometric template security, *EURASIP Journal on Advances in Signal Processing* (Hindawi Publishing Corp., 2008).
3. P. Syverson, A taxonomy of replay attacks, *The Computer Security Foundations Workshop* (Franconia, NH, 1994).
4. A. Adler, Vulnerabilities in biometric encryption systems, *Int. Conf. on Audio- and Video-Based Biometric Person Authentication* (Hilton Rye Town, NY, 2005).
5. A. Adler, Images can be regenerated from quantized biometric match score data, *The Canadian Conference on Electrical and Computer Engineering* (2004).
6. N. K. Ratha, J. H. Connell and R. M. Bolle, Enhancing security and privacy in biometrics based authentication system, *IBM Systems Journal* (2004).
7. C. Moujahdi, S. Ghouzali, M. Mikram, M. Rziza and G. Bebis, Spiral cube for biometric template protection, *5th Int. Conf. on Image and Signal Processing* (Agadir, Morocco, 2012).
8. J. Breebaart, B. Yang, I. B. Dulman and C. Busch, Biometric template protection: The need for open standards, *Privacy and Data Security Journal* (2009).
9. A. Nagar, K. Nandakumar and A. K. Jain, Multibiometric cryptosystems based on feature-level fusion, *IEEE Transactions on Information Forensics and Security* (2012).
10. F. M. Bui, K. Martin, H. Lu, K. N. Plataniotis and D. Hatzinakos, Fuzzy key binding strategies based on quantization index modulation (QIM) for biometric encryption (BE) applications, *IEEE Transactions on Information Forensics and Security* (2010).
11. Y. C. Feng, P. C. Yuen and A. K. Jain, A hybrid approach for generating secure and discriminating face template, *IEEE Transactions on Information Forensics and Security* (2010).
12. K. Lam and T. Beth, Timely authentication in distributed systems, *The European Symposium on Research in Computer Security*, (London, UK, 1992).
13. R. M. Bolle, J. H. Connell and N. K. Ratha, Biometric perils and patches, *Pattern Recognition* (2002).
14. A. B. J. Teoh, K. A. Toh and W. K. Yip, 2N discretisation of BioPhasor in cancellable biometrics, *Int. Conf. on Biometrics* (Seoul, Korea, 2007).
15. B. Yang, D. Hartung, K. Simoens and C. Busch, Dynamic random projection for biometric template protection, *7th Framework Programme of the European Union*, Project TURBINE (ICT-2007-216339) (2010).
16. N. Goel, G. Bebis and A. Nefian, Face recognition experiments with random projection, *SPIE Defense and Security Symposium* (*Biometric Technology for Human Identification*) (Orlando, 2005).
17. A. T. B. Jin, D. N. C. Ling and A. Goh, Biohashing: Two factor authentication featuring fingerprint data and tokenised random number, *Pattern Recognition* (2004).

18. Y. Wang and K. N. Plataniotis, Face based biometric authentication with changeable and privacy preservable templates, *Biometrics Symp.* (Baltimore, MD, 2007).
19. P. Manneville, *Dynamique non linéaire et chaos. Séminaire E2PHY*, Pôle Scientifique de Paris-Sud (2005).
20. J. Kappraff, J. Jablan, J. Adamson and J. Sazdanovich, Golden fields, generalized fibonacci sequences and chaotic matrices, *Forma Journal* (2004).
21. A. Nagar, K. Nandakumar and A. K. Jain, Biometric template transformation: A security analysis, SPIE digital library (2010).
22. R. Belguechi, E. Cherrier, M. El Abed and C. Rosenberger, Evaluation of cancelable biometric systems: Application to finger-knuckle-prints, *Int. Conf. on Hand-Based Biometrics* (Hong Kong, 2011).
23. L. Masek and P. Kovesi, *Matlab Source Code for a Biometric Identification System Based on Iris Patterns*, The School of Computer Science and Software Engineering (The University of Western Australia, 2003).
24. S. Gu, Y. Tan and X. He, *Laplacian Smoothing Transform for Face Recognition*, Science in China Series F-Information Sciences (2009).
25. M. Yu, G. Yan and Q. W. Zhu, New face recognition method based on DWT/DCT combined feature selection, *5th Int. Conf. Machine Learning and Cybernetics* (Dalian, China, 2006).
26. J. Daugmann, How iris recognition works, *IEEE Transactions on Circuits and Systems for Video Technology* (2004).
27. D. Achlioptas, Database-friendly random projections, *ACM Symp. on the Principles of Database Systems* (Santa Barbara, California, USA, 2001).