Spiral Cube for Biometric Template Protection

C. Moujahdi[1], S. Ghouzali[1,2], M. Mikram[1,3], M. Rziza[1] and G. Bebis[4]

[1] LRIT, Faculty of Sciences, Mohammed V-Agdal University, Rabat, Morocco
[2] Information Technology Department, CCIS, King Saud University, Saudi Arabia
[3] The School of Information Science, Rabat, Morocco
[4] Dept of Computer Science and Engineering, University of Nevada, Reno
moujahdi_chouaib@yahoo.fr

Abstract. In this paper we present a new approach for biometric template protection. Our objective is to build a preliminary non-invertible transformation approach, based on random projection, which meets the requirements of revocability, diversity, security and performance. We use the chaotic behavior of logistic map to build the projection vectors using a new technique that makes the construction of the projection matrix depend on the biometric template and its identity. Experimental results conducted on several face databases show the ability of our technique to preserve and increase the performance of protected systems. Moreover, we demonstrate that the security of our approach is sufficiently robust to possible attacks.
Keywords: Template protection; random projection; logistic map; revocability; security.

1 Introduction

The growing concern for the problem of identity theft and the urgent need for individual privacy make the conception of personal authentication / identification systems increasingly important. These systems must authenticate users respecting several requirements, like speed, reliability, accurately and protection of user's privacy. Traditional systems of personal authentication which use passwords or ID cards are not able to meet all these requirements. For against, authentication systems based on biometrics, which use physiological (face, iris, etc.) and behavioral (signature, etc.) modalities, have proven a priority over traditional systems. But while biometrics ensure uniqueness, they do not provide the secrecy. For example, a person let his fingerprints on every touched surface and face images can be seen everywhere. Consequently, many attacks can be launched against the biometric systems, which reduce the credibility of these systems. Therefore, although biometric technologies have inherent advantages over traditional methods of personal authentication / identification, the problem of ensuring the security of biometric data is critical.

In practice, opponents exploit the structure of biometric systems to launch their attacks. All biometric systems consist of four main modules (Fig. 1): the sensor module. The feature extraction module that selects the most significant characteristics in an image sent by the sensor and builds a biometric template test. The module of the da-

tabase containing the biometric templates of legitimate users, and the module of comparison or classification is responsible for comparing the test templates with the templates stored in the database to make a final decision. *Ratha et al* have identified eight points or levels of attack in a biometric system [1] (Fig. 1), but since the principle of some attacks is repeated, *Jain et al* include them into four categories [2]. Firstly, the attacks on the user interface (sensor), mainly due to the presentation of falsified biometric data, for example *spoofing* / *mimicry* attacks [4] (Level 1). Secondly, the attacks on the interface between modules, an adversary can either destroy or interfere communication interfaces between modules, for example *replay* attacks [3] and *hill climbing* attacks [4] (Levels 2, 4, 7 and 8). Thirdly, the attacks on software modules, the executable program on a module can be modified so that it always returns the desired values by the opponent. It is the *Trojan-horse* attacks (Levels 3 and 5). Finally, the attacks on database (Level 6), one of the most damaging attacks on a biometric system is against the biometric templates stored in the database system. For example, a biometric template can be replaced by an impostor 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 attack very dangerous, because, unlike a stolen credit card or password, if a template is stolen it is not possible for a legitimate user to revoke their biometric templates and replace them with another set of identifiers.

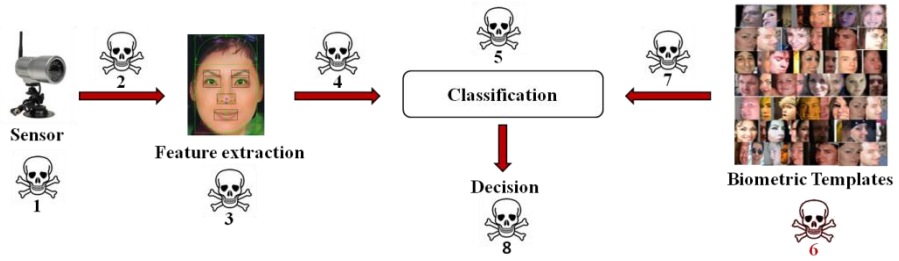

Fig. 1. The eight levels of attack in a biometric system

Because of these security issues, several schemes and methods have been proposed for biometric template protection. The concept of *revocable* (also called *cancelable*) biometric has been proposed, for the first time, as a template security solution by *Ratha et al* [6]. Revocability means that we can revoke a compromised template and replace it with another in the same way as a stolen password is. All the proposed approaches are based on this concept. In this work, we propose a new approach for the protection of biometric template based on the random projection and the phenomenon of chaos, that meets several requirements including the revocability.

The rest of the paper is organized as follows. Section 2 presents an overview of template protection approaches. Section 3 describes the technique of random projection, the phenomenon of chaos, the proposed approach and a security analysis. Experimental results are discussed in Section 4, conclusions and perspectives are drawn in Section 5.

2 Overview of template protection approaches

Personal authentication systems based on biometrics have shown new problems and challenges related to the protection of personal data, inexistent in traditional authentication systems. Because of these problems of security and privacy, there are currently many research efforts to protect biometric systems against the possible attacks. We can divide the proposed solutions into two main categories: *preventive* solutions and *palliative* solutions. Each category can be divided into two main types: *hardware* approaches and *software* approaches.

The objective of *palliative* solutions is, once the attack has been made, to minimize the probability of rupture in the system. The hardware approaches of these solutions try to add specific devices (smell, blood pressure, etc.) in biometric sensors to detect the liveliness / fraud of presented features. Among software approaches of these solutions, one has received more attention from researchers and industry, called *liveliness detection*. The design of these solutions depends on the used biometric trait and there is no one 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. The hardware approaches of these solutions try to put all the modules and interfaces of biometric system on a chip card or a secure processor in general. The software approaches of these solutions are designed to protect the stored biometric templates. The idea is, instead of storing the templates themselves, to store a function of each template used directly in the task of classification. This work is primarily concerned with these solutions of template protection.

An ideal approach of biometric template protection must meet four requirements [7]:

- *Revocability*: it should be possible to revoke a template and put 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 system.

The major challenge to design an approach of template protection, which meets all requirements, is the presence of intra-subject variations, because multiple acquisitions of the same biometric trait do not lead an identical set of features.

Jain et al have classified these approaches into three main categories [2]: *feature transformation* approaches, *biometric cryptosystem* approaches and *hybrid* approaches. The basic idea of feature transformation approaches is to apply a transformation function F to the original biometric template T using a key K, and the transformed template $F(T, K)$ is stored in the database. The function F is also used to transform the test template Q, and we can directly compare the transformed templates $F(T, K)$ and $F(Q, K)$ 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: *biohashing* and *non-invertible transformation*. For biohashing [4][8], 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 *biohashing* scheme security is based on the security of the key. For non-invertible transformation [9][10][11], the function F is not invertible. The main property 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 (in terms of computational complexity). In biometric cryptosystems, the principle of classical cryptosystems is combined with the principle of biometrics to improve 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 on the original template B and the key K are applied to extract the helper data H. At the time of authentication, an error correcting code on the helper data H and test template Q are applied to recover the key K and make a decision.

Each of these approaches has its own advantages and limitations [2]. 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. Our method is based on random projection, a technique that has been applied on various types of problems. We also use the chaotic behavior of logistic map to build the projection vectors which makes the construction of the matrix depend on the biometric template and its identity. The 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 use the chaotic behavior of logistic map to build the projection vectors.

3.1 Random projection

Random projection has been applied on various types of problems [12] including the biometric template protection. It uses orthogonal random matrices to project the biometric templates in a space where distances are preserved. To make the projection non-invertible, a quantization step was included in [13].

Stages of the non-invertible random projection are (Fig. 2):

- Generate *m* random vectors from user key.
- Apply the Gram-Schmidt orthogonalization algorithm on the *m* random vectors to compute an orthogonal matrix A ($AA^t = I$).

- Transform the original template z using the matrix A:

$$y = Az$$

  - y is the transformed template.

- Apply quantization on the transformed template y.

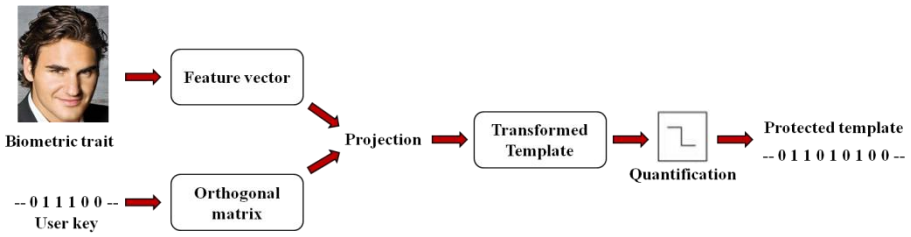

Fig. 2. The non-invertible random projection

The generation of projection matrices using Gram-Schmidt orthogonalization algorithm is time consuming, but there are less expensive methods which do not require this algorithm. For example, *Achlioptas* [14] has proposed a new approach which yields significant computational savings during the computation of the matrix A and the projection Az. Testing this algorithm is one of our objectives in the future work.

In the other hand, the Gram-Schmidt orthogonalization algorithm returns a set of orthogonal vectors if and only if the input vectors are linearly independent. Therefore, the generation of random vectors from the used 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 will be used to construct the projection matrices.

3.2 Logistic map

Logistic map is a sequence whose recurrence is not linear. Its recurrence relation is:

$$x_{n+1} = \mu x_n(1 - x_n)$$

According to the values of μ, we can observe a chaotic behavior in the val $[3.5699456, 4]$. Thus, logistic map is very sensitive to initial conditions. According to this feature, logistic map was used in several applications, such as the protection of data content. For example, random sequences of the chaotic zone can be used to cryptographically secure the transmission channels in several telecommunications systems.

In our work, we use logistic map to generate multiple random vectors. These vectors will be stored in a 4D matrix, called *spiral cube*. Spiral cube will be used to construct the projection matrices. The construction of cubic spiral depends on the size of the original template. Suppose that the feature vector contains n values, the cube will consist of n spiral cells (3D matrix), each cell being of size $m \times m$ (m is the nearest

integer greater than or equal to $\sqrt{n}$) and each cell corresponds to a specific value of μ. Therefore, each cell contains an $m \times m$ box, and each box contains a vector generated using the values μ in the interval $[3.5699456\ , 4]$ (Fig. 3).

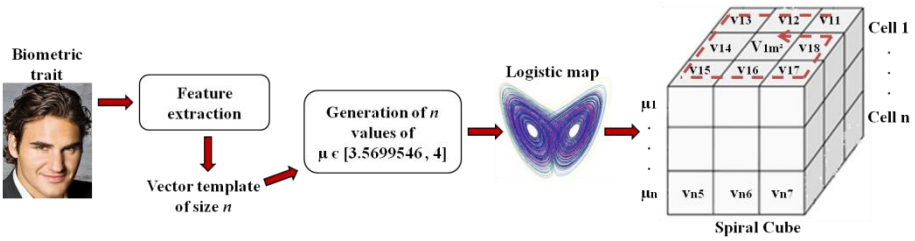

Fig. 3. Spiral cube construction

3.3 Proposed approach

We propose a non-linear mechanism of random projection. Our objective is to build a non-invertible method for biometric template protection that meets all the requirements of security and performance with no need for a user's key. It should be noted that the proposed approach is applicable to any biometric system that uses *feature vectors* for classification.

During enrollment, after the extraction of the features from the training templates, (i.e., we assume that the training database contains x templates of size n, each identity is presented by y templates, assuming z identities: $x = y \times z$). Our approach and the mechanism of protection start with the following steps:

- For each training template T, we calculate ∂:

$$\partial = \frac{|\max(T) - \min(T)|}{m^2} \qquad (1)$$

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

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

$$Q_i = \begin{cases} 1 & if \quad T_i = \min(T) \\ m^2 & if \quad T_i = \max(T) \\ ceil\left(\dfrac{|T_i - \min(T)|}{\partial}\right) & else \end{cases} \quad i \in [1, n] \ \ and \ \ Q_i \in [1, m^2] \qquad (2)$$

  - $ceil(a)$ calculates the nearest integer greater than or equal to a.

- At the end of the previous step, we have x quantized vectors. For each identity, we keep a single quantized vector (randomly chosen among the y vectors). Finally, we obtain a matrix $\emptyset$ which contains z quantized vectors. We call it the *map cube*.

- We construct the projection matrices for each identity using the *spiral cube* and the *map cube* (Fig. 4). Assuming that we calculate the projection matrix of identity 1 (first vector of the map cube), the first value of the quantified vector (size n) of this identity corresponds to the first cell in the spiral cube, and so on for the other values. For example, if the first value is 3, we extract the vector number 3 of the first cell of the spiral cube. Finally, we obtain n vectors and we apply the Gram Schmidt algorithm to construct the projection matrix of the identity 1. The principle is similar for the other identities.
- Finally, we store the protected templates, spiral cube and cube map in the system database (storage of spiral cube and cube map is public).

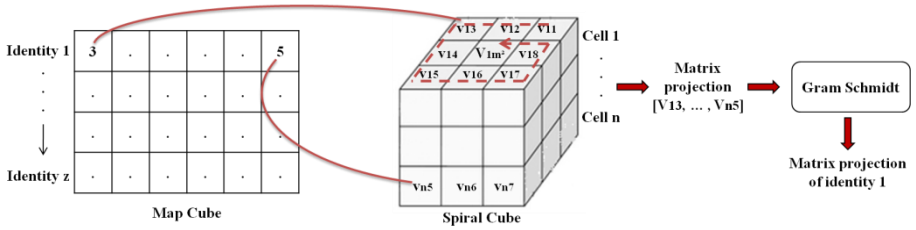

Fig. 4. Mechanism of projection matrix construction

During authentication, after the extraction of the features from the test template, the protected system works as follows:

- We apply quantization on the template test which is similar to that applied on the training templates during enrollment stage (equations 1 and 2).
- We use a KNN classifier to find the nearest vector in the *map cube* to the quantized test template.
- The closest vector is used to find the projection matrix corresponding to the test vector (Fig. 4).
- The protected template is compared directly with the protected training templates; the comparison will be carried out according to the type of classifier used by the system.

3.4 Analysis study

The proposed technique meets the requirements of revocability, diversity and security. Knowing that multiple acquisitions of the same biometric trait do not 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 map cube. We change, specifically, 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 the change of the spiral cube, or the order of cells in the cube, require to redo the training

task again for all templates in the database; this is a weak point in our approach which we plan to address in our future work.

The security analysis of existing methods is mainly based on the complexity of brute force attacks which assume that biometric data are uniform. We assume that the size of the original template is n. We analyze the scenario where the adversary has access to the protected template and the spiral cube. To find the original template we need to find the used projection matrix. In this scenario, we have $(m^2 \times n)^n$ (m is the nearest integer greater than or equal to $\sqrt{n}$) 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 map cube (all public data). If he/she does not know the role of the map cube, the number of possibilities is similar to the previous scenario. Otherwise, if he/she knows the role of a map cube, the number of possibilities is $(m^2 \times z)^n$ (i.e., z is the number of identities), since he/she does not know that the projection vectors are stored spirally in the cube and there is no evidence in the database or public data to determine the storage manner. We have found that even in the worst case scenario where the adversary has all the public data and the template protected, the security 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 reach the security of the system. A rigorous analysis of security of these methods, like [17], is necessary, and will be the objective of future work.

4 Experimental results

In this Section, we present our experimental results using the YALE and UMIST face databases (Fig. 5). The YALE face database consists of 165 face images of 15 distinct persons. Images are characterized by variations in facial expressions and lighting conditions. The UMIST face database consists of 550 face images of 20 distinct persons. Faces in the database cover a wide range of poses from profile (90°) to frontal (0°) views.

Fig. 5. Examples from UMIST database (top) and YALE database (down)

The biometric system used in our experimentation is based on an efficient feature extraction method LST [15] followed by a multi-class dimensionality reduction approach SVDA [16] for feature selection, and a KNN classifier for classification [18]. For the YALE database, each person is presented with five images. Thus, the training

database contains 75 templates while the test database contains 90 images. For the UMIST database, each person is presented with six images and the *leave-one-out* approach is used for testing on 120 training images [18]. According to the leave-one-out approach, the algorithms are run N times. In each round, N-1 samples are used for training and the remaining sample is used for testing. If the test sample is correctly predicted, the test accuracy of the round is 100%, otherwise it is 0%. The overall test accuracy is the mean accuracy of all the N predictions. Figure 6 shows a comparison between the unprotected system and the protected system using the two databases.

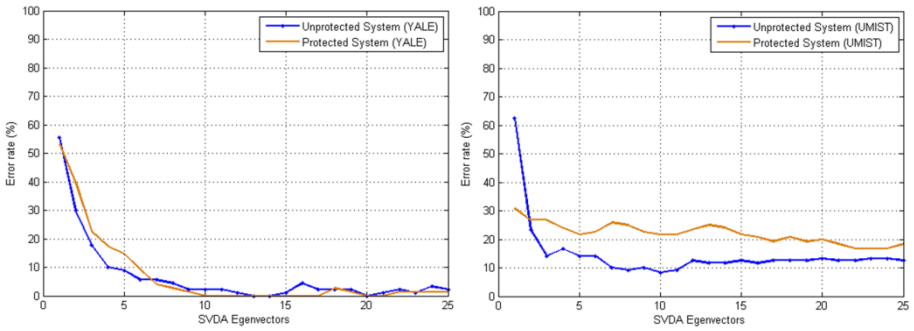

Fig. 6. Comparison of performance between protected systems and unprotected systems

In the case of the YALE database, the performance of the unprotected system is very high because the feature extraction (i.e., LST) and selection (i.e., SVDA) techniques are very efficient. On the other hand, the variation in facial expressions and lighting conditions do not degrade the performance significantly. In the case of the protected system, we can notice a small improvement compared to the unprotected system.

In the case of the UMIST database, the performance of the unprotected system is average because each person is presented with six images (one image per view class). Knowing the principle of the leave-one-out, in each test round, the view class of the test image is not present in the training database, which presents a very complex test situation. Knowing also that the major challenge in designing a template protection approach is the presence of intra-subject variations (the multi-view in our case), we believe that the observed decrease in performance by 3.34% is quite acceptable

Our results show the ability of our technique to increase the performance of protected system in ideal test conditions and to preserve it in non-ideal test conditions.

5 Conclusions and perspectives

In this paper, we proposed a new approach for biometric template protection. We used the logistic map vector to generate the vectors of projection. We have stored these vectors in a spiral cube, which is used to generate the matrix of protections and depends on the template to be protected. Our approach meets revocability, diversity and security, required in an ideal method for template protection. In addition, it does not only preserve recognition performance but increases it; due to using a dynamic projection matrix for each identity. Thus, it manages better the intra-subject variations. In

future work, we will test other biometric modalities such as fingerprints. As for the security analysis, we plan to use the analytical equations presented in [17].

Acknowledgments. Dr. George Bebis is a Visiting Professor in the Department of Computer Science at King Saud University, Riyadh, Saudi Arabia. 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, R. M. Bolle. *An analysis of minutiae matching strength*. Third International Conference on Audio- and Video-Based Biometric Person Authentication, 2001.
2. A. K. Jain, K. Nandakumar, A. Nagar. *Biometric Template Security*. EURASIP Journal on Advances in Signal Processing, 2008.
3. P. Syverson. *A taxonomy of replay attacks*. the Computer Security Foundations Workshop. 1994.
4. A. Adler. *Vulnerabilities in Biometric Encryption Systems*. International Conference on Audio- and Video-Based Biometric Person Authentication, 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, R. M. Bolle. *Enhancing security and privacy in biometrics-based authentication system*. IBM Systems Journal, 2004.
7. J. Breebaart, B. Yang, I. B.-Dulman, C. Busch. *Biometric Template Protection: The need for open standards*. Privacy and Data Security journal, 2009.
8. K. Lam, T. Beth. *Timely authentication in distributed systems*. The European Symposium on Research in Computer Security, 1992.
9. R. M. Bolle, J. H. Connell, N. K. Ratha. *Biometric perils and patches*. Pattern Recognition, 2002.
10. A. B. J. Teoh, K.-A. Toh, W. K. Yip. 2^N *discretisation of BioPhasor in cancellable biometrics*. International Conference on Biometrics, 2007.
11. B.Yang, D. Hartung, K. Simoens, C. Busch. *Dynamic Random Projection for Biometric Template Protection*. the 7th Framework Programme of the European Union, Project TURBINE (ICT-2007-216339), 2010.
12. N. Goel, G. Bebis, A. Nefian. *Face Recognition Experiments with Random Projection*. SPIE Defense and Security Symposium (Biometric Technology for Human Identification). Orlando, FL, March 28 - April 1, 2005.
13. Y. Wang K.N. Plataniotis. *Face Based Biometric Authentication with Changeable and Privacy Preservable templates*. Biometrics Symposium, 2007.
14. D. Achlioptas. *Database-friendly random projections*. ACM Symposium on the Principles of Database Systems, pp. 274.281, 2001.
15. S. Gu, Y. Tan, X. He. *Laplacian Smoothing Transform for Face Recognition*. Science in China Series F-Information Sciences, 2009.
16. S. Gu, Y. Tan, Xi. He. *Discriminant Analysis via Support Vectors*. Neurocomputing, 2009.
17. A. Nagar, K. Nandakumar, A. K. Jain. *Biometric Template Transformation: A Security Analysis*. SPIE digital library, 2010.
18. C. Moujahdi, S. Ghouzali, M. Mikram, D. Aboutajdine. *Multi-View Face Recognition*. Journal of Communications and Computer Engineering, Volume 2, Issue 1, 2012, Pages 46:50.