Secured Multimodal Biometric System

Bedad Fatima, Adjoudj Réda
EEDIS Laboratory, Djillali Liabes University of Sidi Bel Abbes
Algeria
bedad_fatima2006@yahoo.fr
AdjReda@yahoo.fr

**ABSTRACT:** Multimodal biometrics, which consists of combining several biometrics systems. Indeed, it makes it possible to reduce certain unimodal biometric systems limitations, such as the impossibility of acquiring data from certain people or intentional fraud, while improving recognition performance. These benefits of multimodality to unimodal biometric systems are achieved by fusion of several biometric systems.

*In this case, the security is a necessity to have robust and user-friendly biometric systems. In this paper, we proposed a Revocable multi biometric scheme to secured multi biometric data, we focused our attention on BioHashing method which is a recent technique that can address simultaneously the invasion of privacy issue and the Security. An improvement in the level of characteristics has been introduced to obtain very satisfactory results. It combines fingerprint multi sensor features of a single human finger.*

**Keywords:** Multimodal Biometrics, Finger, Feature Fusion, BioHashing, Security

**DOI:** 10.6025/jmpt/2018/9/3/77-87

**Received:** 11 March 2018, Revised 20 April 2018, Accepted 2 May 2018

© 2018 DLINE. All Rights Reserved

1. Introduction

The identification of the user with passwords is not friendly and does not offer a high level of security of user. Biometrics becomes a popular solution to reach this goal. Biometrics refers to an identification and authentication technology that involves transforming a biological, morphological or behavioral characteristic into a digital impression. His goal is to attest to the uniqueness of a person from the measurement of an unchangeable or immeasurable part of his body.

In general, a biometric system is realized in two stages: enrollment and verification. The first is to generate a user’s biometric reference and store it. During the verification, a biometric capture is compared to the biometric reference of the presumed individual for decision. In order to improve the security of user identification, it is generally necessary to combine different factors of identity. This can be achieved by using different biometric data to define a multi-biometric system.
Multimodal biometric systems use two or more biometric resources (e.g., fingerprint, face, iris, etc.) which is the main purpose of this article.

**There are five types of multimodal systems as follows:** Multi-sensors, multi-instances, multi-algorithms, multi-samples and multi-biometrics. These different types of multimodal systems could reduce several problems encountered in single-mode systems.

For multimodal biometric recognition, the crucial point is how to fuse the data of various biometric modalities. Information from different biometric traits can be always fused at three levels, such as the feature level (integrating the features of different biometrics), the score level (combining the genuine and imposter scores), and the decision level (combining the decisions) [14].

Nevertheless, biometric data is sensitive and requires special attention in terms of security and privacy. The protection of biometric data must be realized during the life cycle of data, from storage to manipulation. For an ideal biometric template protection scheme, it must satisfy four criteria, [5], [17] as follow:

- **Unlink ability:** The secure model must not allow cross-compatibility on databases, thus ensuring the privacy of the user.

- **Revocability:** It should be simple to revoke a compromised model and restart a new one based on the same biometric data.

- **Non-invertible:** It must be difficult to obtain calculations of the original biometric template from the secure model. This property prevents an opponent from creating a physical parody of the biometric feature from a flight model.

- **Performance:** The biometric model protection program should not degrade the recognition performance of the biometric system.

Today, we find that there are two field of techniques to protect the privacy of template biometric can be broadly split into two categories [5]:

- Biometric cryptosystems

- Revocable or Feature transformation.

The main contribution of this article is to put the main weaknesses related to biometrics and address the methods of protection of the biometric model and then focus on the protection of multi-biometric data.

The main objective is to present the BioHashing technique as practical solution for biometric data protection and we are trying to study the impact of this technique on multi biometric data.

The paper is organized as follows: In Section 2, we discuss the security biometric. In Section 3, we present the BioHashing technique as a technique of security. In Sections 4 and 5, we detail the proposal system. In section 6, we present the database used and we study the security of our system.

### 2. Security Biometric

There are mainly two classes for the methods of protection of the biometric model that are

(i) Biometric cryptosystems

(ii) Feature transformation

In *biometric cryptosystems* during registration, an error correction code $\varphi$ is applied to the biometric model $B$ and a key $K$ to extract the set of data $H$ (the set $H$ is called Helper Data). At the time of authentication, an error correction code $\varphi$ is applied to the $H$ data helper and the $Q$ test model to retrieve the $K$ key (Figure 1). Depending on how the data helper is extracted, biometric crypto systems can be divided into two categories: Key-binding and key-generation.

In *Feature transformation*, [11], [10]. The basic idea of feature transformation approaches is to convert an unprotected biometric template to a protected template using a transform function.
Figure 1. Example of template protection by cryptosystem technique [5]

Generally, these approaches work as follows (Figure 2): Suppose that $X$ will be transformed into $T$ coded data during enrolment by the use of a function $F$. For verification, the biometric request $Y$ will be transformed into $T'$ always in using the $F$ function and the authentication will succeed if $T$ is close to $T'$ using some measure of similarity. To ensure the revocability of the system, a random data $S$ in the form of a key is assigned to each user $U$. The key $S$ is then considered as an input parameter of the transformation function $F$. The revocation consists in the direct replacement of this user key.

Feature transformation schemes can be classified into two categories, invertible transformation (known as Salting or Biohashing) and non-invertible transformation.

In the next section, we present the BioHashing method as a chosen solution in our approach.

3. An overview of BioHashing

3.1 Principles
In general, the process of BioHashing [9]. (see Figure 3) has two stages:

In the first stage, the method used is to project the biometric data (normalized) on an orthonormal basis generated from the hazard. The resulting dimension is at most equal to the representation dimension of the biometric data. This phase consists in hiding the biometric data in a part of the space. The use of an orthonormal basis makes it possible to ensure the preservation of
the similarity relations between two projected biometric data, as demonstrated by the Johnson-Lindenstrauss lemma [3].

The second step is to quantify this result using a simple threshold. This step makes it possible to guarantee the non-invertibility of the process (to find the initial biometric data from the BioCode) and to make the process robust (by allowing minor differences in the projected vector inherent in the acquisition of the biometric data).

The secret of BioHashing approach, consisting of three stages [15]:

The Biohashing algorithm transforms the biometric template $T = (T_1, ..., T_n)$ in a binary template $B = (B_1, ..., B_m)$, with $m \leq n$, as following (see Figure 3).

1. $m$ pseudorandom orthonormal vectors $V_1, ..., V_m$ of length $n$ are generated from the random seed (typically with the Gram Schmidt algorithm).

2. For $i = 1, ..., m$, compute the scalar product $x_i = <T_i, V_i>$.

3. Compute the binary template $B = (B_1, ..., B_m)$ with the quantization process:

$$B_i = \begin{cases} 0 & \text{if } x_i < \tau \\ 1 & \text{if } x_i \geq \tau \end{cases}$$

where $\tau$ is a given threshold, generally equal to 0.

The resulting bitstring $B$ named BioHash code is compared by the Hamming distance for a matching score. The security of the process is assured if the BioHash code is non invertible.

3.2 Performance Evaluation

We will describe the performance of BioHashing using the main of the performance of a biometric system is described by its false acceptance rate (FAR) and false rejection rate (FRR). Another index of performance is equal error rate (EER) defined as the point where FAR and FRR are equal. A perfect system would have zero EER.

4. Proposal of System Study

From the previous study, we propose an approach for multi-biometric system security. Application steps and requirements play a major role in the biometric technical scheme.
To do this, we set a set of parameters and methods to ensure security:

- Use of a real database multi biometric;
- Guaranteed the same length the feature vector is advisable;
- The length of the BioHash code is an important point. By increasing this vector, the performance becomes better. The increase of the feature vector is the best alternative to improve this length, made by the merger at the level of features;
- The BioHash codes are always compared using the Hamming distance.

4.1 Steps of the Prototype System
The system will be composed in four steps (see figure 4):

![Figure 4. The proposed system](image)

We use in this new approach the authentication or verification in the multibiometric database. The traditional authentication process consists of a “1 to 1” comparison, in which the system validates the identity of a person by comparing the biometric data entered with the biometric template of that person stored in the system database.

In this section we will describe the steps of our system.

*Feature Extraction*: Feature extraction is the first step of every biometric system. In our system the extraction consists of the LBP filter (Local Binary Pattern): this filter has shown great efficiency for preprocessing and is more suitable for our approach since it gives result vectors code equal in size. This operator, as proposed by Ojala and al [4], consists of three steps (see Figure 5):

1. Threshold of each neighborhood $3 \times 3$ considering the intensity value of the pixel central as the value of the threshold. A value of 1 is assigned to each pixel in the intensity is greater than or equal to the threshold, 0 otherwise. An 8-bit binary string is then deduced.

2. The binary string is converted, by weighting, into a decimal number which is assigned to the central pixel. There are 256
possible values to represent the different possible micro-patterns. An example of these micro-patterns is shown in Figure 6.

3. A histogram of 256 values counts the number of occurrences of each micro-pattern for all pixels in the image. The fingerprint is represented by this histogram.

The LBP approach codifies and collects, in a histogram, the occurrences of the different micro-patterns representing the texture of the local neighborhood.

• **Fusion:** In multimodal systems the information can be merged at different levels. In our approach we have chosen fusion at the characteristic level this operation requires the concatenation of the information that represents the characteristics extracted from different modalities (result of the step of feature extraction).

• **Biohashing:** Generate the biocode, this step is dedicated to the transformation to a binary vector using the biohashing algorithm.

• **Matching:** It’s the verification step. The matching is processed using hamming distance to compare two biocodes.

5. Databases, Experimental Results

We present in this section some experimental results on images from the SDUMLA-HMT database [20] fingerprint benchmark database.

At present, fingerprint recognition is the most widely used biometric method. The most extensive database of fingerprints was used, the SDUMLA-HMT database. This database includes 106 individuals. Each fingerprint image is saved under a 256 gray level « Bmp » format. The capture was made for the six fingers with 5 different types of sensors. The multi-sensor fingerprint
database contain $6 \times 5 \times 8 \times 10^6 = 25,440$ fingerprint images in total.

Figure 7 shows some images for different sensors.

![Figure 7. Some images for different sensors](image)

In order to form our multi-biometric databases, we took count the first fingerprints of sensor FT-2BU and the second fingerprints of sensor AES2501, so our multi-sensor multi instance fingerprint database contains $2 \times 8 \times 10^6 = 1696$ fingerprint images in total.

In order to evaluate the performance of the proposed method, we use the following methodology. We use the first sample of each user as a model reference. The rest of the images from the user and those from other users are used to test the proposed schema. In total we have learning database $2 \times 2 \times 10^6 = 424$ fingerprint images and test database $2 \times 6 \times 10^6 = 1272$ fingerprint images.

In feature extraction, we used the LBP model of size $n = 256$, so we got a vector matrix of size $= 1696 \times 256$, after in the step of fusion we use the concatenation between two vectors, the first one is obtained from the sensor FT-2BU and the second from the sensor AES2501, we got a vector matrix of size $= 848 \times 512$.

For the secret path, we use this last matrix data to calculate the Reference BioCode. We have found the same size of matrix $(848 \times 512)$ of 0 and 1. (the result of biohashing).

The performances are reported in the form of Receiver Operating Characteristic (ROC) curves as a plot of the false rejection rate (FRR) against the false acceptance rates (FAR). For this, we set an acceptance threshold between 0% and 100%: the more the threshold goes to 0%, the more the false ones acceptances will be many, the more the threshold goes to 100% the more false rejects will be numerous. The performance is evaluated in EER.

Figure 8 presents the Receiver Operating Curve (ROC) curve of the initial system multibiometric using only the fingercode (without any BioHashing) on this database. We obtain an EER value of 36%.

But when the BioHashing technique is applied in our system multi biometric, the EER reduces to 0%. This is shown in Figure 9.

Now, we study the robustness of the our system multi biometric based on BioHashing when it is attacked.
Figure 8. Performance of the multi biometric system based on the fingercode without BioHashing

Figure 9. Performance of the multi biometric system based on the BioHashing

Figure 10. Performance of the multi biometric system based on the BioHashing when the impostor has the biometric reference but not the seed value
Table 1. Comparison between different approaches to secure data multimodal

| Author          | Year | Principle                                                                 | Modality                  | Method                                      |
|-----------------|------|---------------------------------------------------------------------------|---------------------------|---------------------------------------------|
| Jeong & al [6]  | 2006 | Combine two methods of extracting different characteristics to obtain a revocable biometry. (PCA and ICA). | Face                      | revocable biometry                          |
| Teoh & al [18]  | 2008 | The quantized random projection set based on the Johnson-Lindenstrauss lemma is used to establish the mathematical underpinnings of BioHashing. Based on this model. | Fingerprint + plamprint + face | The BioHashing EER = 21.53%                 |
| Maiorana & al [7] | 2011 | Biometrics is secured by applying a set of non-invertible transformations, thus generating modified models from which the retrieval of the original information is as difficult as to guess it. | Online signature (database MCYT) | Non-invertible transformations              |
| Paul & al [8]   | 2012 | Present a new solution for revocable biometrics in the multimodal system.   | Face and hear             | The random projection + a transformation based on the extraction and the selection of characteristics |
| Canuto & al [2] | 2013 | Specifically study the performance of different fusion approaches in the context of recognizing revocable multibiometry. | Voice + iris              | revocable transformations                     |
| Rathgeb & al [12] | 2014 | Fusion at the feature level, then they apply the transformation.            | Irises are obtained from both eyes (database IISD) | Irreversible transformation (based on Bloom filter) EER<0,5 % |
| Sushma & al [16] | 2015 | Two methods were used to extract the characteristics of the image, namely: 1) Gabor filter and 2) random projection techniques (RP). | Iris                      | Non irreversible transformation (Bloom filter) |
| Rathgeb & al [13] | 2015 | Fusion at the level of the characteristics of different biometric data to a single protected model. | Face + iris               | Non irreversible transformation (Bloom filter) |
| Stokkenes & al [15] | 2016 | The fusion at the score level is applied to increase the accuracy of the recognition. | Face + of the two peri-ocular regions | Bloom Filters + Binarized Statistical Image Features (BSIF) FAR= 0,01 % |
| Yildiz & al [19] | 2017 | Constructs a multi-biometric model by superimposing several biometric data of a user, so that it is difficult to separate the individual layers. | Voice + fingerprint       | Revocable biometry EER = 2,1 %               |
| Bringer & al [1] | 2017 | One approach develops the approach of [12]. they analyze the non-capacity on protected models from two different iris codes from the same iris. | Two iris                  | Bloom filter                                |

Figure 10 present the performance when the impostor has the biometric reference but not the seed value.

In this case, the EER value is 0%. We can observe that the impostor cannot be authenticated. So the use of BioHashing enhances the performance of the initial multi biometric system because the seed value can be considered as additional information for the authentication of an individual.

To conclude on the evaluations carried out, the table 1 gives an idea of the importance of the work provided. It presents a
comparison between different approaches to secure data multimodal using Revocable or Feature transformation methods.

After this comparaison, the Results show that by using the biohashing algorithm, obtain a lower EER. The proposed algorithm satisfies the requirements of the cancelable biometrics like cited in section 1 (introduction).

6. Conclusion

The uses of biometric recognition system offer an alternative to perform personal recognition.

In this paper, we proposed a Revocable multi biometric scheme. Revocable biometrics is used to diversify and secure data biometric, so as not to directly use the original data and protect thus the privacy of people. We focused our attention on BioHashing which is a recent technique that can address simultaneously the invasion of privacy issue and the Security.

We have proposed a fingerprint multi sensor features of a single human finger. In this case, we have chose the feature fusion and use the biohashing to get an biocode, the identification can be improve by the comparison of two biocodes using hamming distance and obtain a lower EER.

The proposed biohashing approach could be useful for securing any type of multi biometric data.

In future work, we intend to combine other types multimodal systems.

References

[1] Bringer, J., Morel, C., Rathgeb, C. (2017). Security analysis and improvement of some biometric protected templates based on Bloom filters. *Image and Vision Computing*, 58. 239-253.

[2] Canuto, A. M., Pintro, F., Xavier-Junior, J. C. (2013). Investigating fusion approaches in multi-biometric cancellable recognition, *Expert Systems with Applications*, 40 (6) 1971-1980.

[3] Dasgupta, S., Gupta, A. An elementary proof of the Johnson-Lindenstrauss Lemma, 1999. UTechnical Report TR-99-006, *International Computer Science Institute*, Berkeley, CA.

[4] Harwood, D., Ojala, T., Pietikeinen, M. (1996). A comparative study of texture measures with classification based on feature distributions. *Pattern Recognition*, 29. 51–59.

[5] Jain, A. K., Nandakumar, K., Nagar, A. (2008). Biometric template security. *EURASIP Journal on Advances in Signal Processing*.

[6] Jeong, M., Lee, C., Kim, J., Choi, J. Y., Toh, K. A., Kim, J. (2006). Changeable biometrics for appearance based face recognition. In Biometric Consortium Conference, 2006 Biometrics Symposium: Special Session on Research at the p. 1-5. IEEE.

[7] Maiorana, E., Campisi, P., Neri, A. (2011). Cancellable biometrics for on-line signature recognition. In New Technologies for Digital Crime and Forensics: Devices, Applications, and Software IGI Global.

[8] Paul, P. P., Gavrilova, M. (2012). Multimodal cancelable biometrics. In: Cognitive Informatics and Cognitive Computing (ICCICC), 2012 IEEE 11th International Conference on. IEEE. (August).

[9] Pillai, J. K., Patel, V. M., Chellappa, R., Ratha, N. K. (2010). Sected Random Projections for Cancelable Iris Biometrics. In: *Acoustics Speech and Signal Processing (ICASSP)*, 2010 IEEE International Conference on, p. 1838–1841.

[10] Ratha, N. K., Connell, J. H. et Bolle, R. M., Chikkerur, S. (2006). *Cancelable Biometrics : A Case Study in Fingerprints*. In: Pattern Recognition, 2006. ICPR 2006. In: 18th International Conference on, V 4, p. 370–373.

[11] Ratha, N. K., Connell, J. H. et Bolle, R. M. (2001). Enhancing security and privacy in biometrics-based authentication systems. *IBM Systems Journal*, 40 (3) 614–634.

[12] Rathgeb, C., Busch, C. (2014). Cancelable multi-biometrics: Mixing iris-codes based on adaptive bloom filters. *Computers and Security*, 42, 1-12.

[13] Rathgeb, C., Gomez-Barrero, M., Busch, C., Galbally, J., Fierrez, J. (2015, March). Towards cancelable multi-biometrics based on bloom filters: a case study on feature level fusion of face and iris. In: Biometrics and Forensics (IWBF), 2015 International
[14] Ross, A., Jain, A., Qian, J. Z. (2001). Information fusion in biometrics. Pattern Recogn Lett 24. 2115–2125 S. Dasgupta and A. Gupta. An elementary proof of the Johnson-Lindenstrauss Lemma, 1999. UTechnical Report TR-99-006, International Computer Science Institute, Berkeley, CA.

[15] Stokkenes, M., Ramachandra, R., Siggaard, M. K., Raja, K., Gomez-Barrero, M., Busch, C. (2016). Multi-biometric template protection—A security analysis of binarized statistical features for bloom filters on smartphones. In: Image Processing Theory Tools and Applications (IPTA), 2016 6th International Conference on IEEE. (December).

[16] Sushma, H. R., Sandeep, R. (2015). Multi Biometric Template Protection using Random Projection and Adaptive Bloom Filter. International Journal of Research in Electronics and Computer Engineering (IJRECE), 3(2).

[17] Teoh, A. B., Goh, A., Ngo, D. C. (2006). Random multospace quantization as an analytic mechanism for biohashing of biometric and random identity inputs. IEEE Transactions on Pattern Analysis and Machine Intelligence, 28 (12) 1892-1901.

[18] Teoh, A. B., Kuan, Y. W., Lee, S. (2008). Cancellable biometrics and annotations on biohash. Pattern recognition, 41 (6) 2034-2044.

[19] Yildiz, M., Yanikoglu, B., Kholmatov, A., Kanak, A., Uludağ, U., and Erdoğan, H. (2017). Biometric layering with fingerprints: template security and privacy through multi-biometric template fusion. The Computer Journal, 60 (4) 573-587.

[20] Yilong Yin et al. (2011). SDUMLA-HMT: A Multimodal Biometric Database, Springer-Verlag Berlin Heidelberg 2011.