International Journal of Computing and Digital Systems
Int. J. Com. Dig. Sys. 11, No.1 (Jan-2022)

https://dx.doi.org/10.12785/ijcds/110128

Studies of the Robustness of a Transformation-Based Multi-Biometric Template Schemes Protection

BEDAD Fatima[1,2], ADJOUDJ Réda [1] and BOUSAHBA Nassima[1,3]

[1]*Evolutionary Engineering and Distributed Information Systems Laboratory, EEDIS Computer Science Department, University of Sidi Bel Abbés, Algeria.*
[2]*Belhadj bouchaib University of Ain Témouchent, Algeria*
[3]*Hassiba Benbouali University of Chlef, Chlef, Algeria*

Received 22 Dec. 2020 , Revised 23 Jun. 2021, Accepted 8 Jul. 2021 , Published 15 Jan. 2022

Abstract: As the number of applications that use multimodal biometrics grows, potential challenges to privacy and protection emerge. New multi-biometric technologies have been suggested in the context of privacy and confidentiality: template protection systems. For the relevant defensive technologies, very current solutions have been presented. Their decision on the optimal strategy is still being considered. This paper provides an evaluation of multi-biometric protection systems according to a transformation proposing some measures and metrics to test its performances and sturdiness faced against attacks. These measures enable evaluating the success of the approach in various scenarios. In this perspective, this article proposes a transformation-based multi-modal biometric protection system that focuses on BioHashing by merging fingerprint modalities. The fingerprint images are classified into three instances and represented by a feature vector using a 2D Log-Gabor filter. A biohashing is applied to its vectors to create Biocode vectors. Following that, a multi-instance score fusion formed by Biocodes of the fingerprints is merged at the matching level. Finally, to get a high score, multi-sample score fusion is used. Furthermore, a transformation-based protection model that focuses on BioHashing demonstrates how specific security and privacy may be validated.

Keywords: Multi-modal biometric systems, multi-biometric templates protection, attack, security, transformation, Performance.

1. Introduction

Security is nowadays an important challenge in various sectors, which led to the introduction of information technology to fight the insecurity problem. Traditional security systems are knowledge-based (password, PIN code, etc.), but these systems are less reliable for many environments due to their common inability to distinguish between a truly authorized person and an imposture. The resolution of these problems has been obtained in authentication technologies based on biometrics. There are several types of biometrics, like fingerprints, iris, voice, face, signature, DNA, etc., that can be applied to authenticate an individual's identity. However, biometrics are not 100% safe, and it is a fact that in case of high protection systems, there is always a constraint.

Multi-modal biometrics are a synthesis of many mono-modal biometric schemes. It also reduces certain limitations of mono-modal recognition, related to recognition performance, acceptability of the authentication process, and deliberate fraud. In many cases, multi-modal biometrics can be used from a particular perspective, either by mixing heterogeneous technologies (e.g., biometrics + badge + coded keypad) or by combining several variations of the same biometric (e.g., several fingerprints of the same individual). This is called "multi-biometrics", i.e. the use of several biometric recognition systems (fingerprint + iris + face). The advantages conferred to "mono-modal" biometric systems by multi-modality are obtained by combining several biometric systems [1].

Data security issues relating to this unique personal data cease its practical use. For example, in some cases, the centralized collection of the biometric information is prohibited or restricted into a specific number of persons. Over the last decade, new biometric solutions have been proposed to solve this problem, centred on the Confidentiality by design." concept. These forms of biometric security defence systems targetabbreviations in the title or headers unless they are unavoidable.

When the information of a multi-biometric user's template is in the hands of harmful persons, they can seriously compromise the multi-biometric system's protection (intrusion threats) and privacy of user (link threats). Therefore, the protection of multi-biometric models is a critical issue

E-mail address: fatima.bedad@univ-sba.dz, adjoudj@univ-sba.dz, nassima.bousahba@univ-sba.dz

that needs to be resolved to improve the acceptance of the public's technology multi biometric.

In view of the recent increase in the number of techniques promoted to protect multi-biometric templates, it is essential to develop a set of measures and metrics to assess these techniques' strength.

There are three main solutions for the security of biometric prototypes. In the initial, crypto-systems with biometrics, such as the ones described by [2] and [3], use cryptography. Secondly, secure approaches for computing seek to calculate the relationship of an unreliable part between two biometric models, like those presented by [3]. Finally, [4] discuss feature transformation methods protection of models.

The BioHashing algorithm remains yet the well-known method, which is focused on biometric data revocable. It has been designed for various biometric templates [5], [6].

The approach applied in this paper is built on the application of the BioHashing algorithm. BioHashing algorithms based on multi-biometric transformation schemes are also proposed for the security of multi-biometric template. The second contribution of the article is the application of the number of metrics. Metrics are the main element of an evaluation process. In this framework, a metric is used to produce values that compare the different schemes against the criteria to be assessed to test the robustness and analyse the safety of multi-biometric transformation schemes.

The rest of the article is as below: Section 2 describes the context of the transformation-based protection scheme template. The properties of these biometric system templates are also defined. Section 3 is dedicated to the related work. Section 4 introduces the Robustness of BioHashing. Section 5 is dedicated to the proposed methodology, while Section 6 presents the evaluation of the transformation-based protection schemes template. Section 7 terminates the study and provides several perspectives.

2. Background

This section focuses on model security schemes using transformation (Figure 1), because some vulnerabilities were identified in the previous method [7]. A feature transformation or cancellable system is a function f that is applied to a biometric template b using a key K (usually a seed at random or password). The transformed $f(b, K)$ templates are stored in a personal Computer or database. Apply the same transformation to the template of the questionnaire b' with the same K key during the authentication step, and a comparison of $f(b', K)$ and $f(b, K)$.

In general, it is assumed that the original model b (or a similar approximation) as provided by [8]. Provided the transformed data $f(b, K)$ and the primary K are given, it can be retrieved. Thus, this key must be stored securely, even if the original template's reconstruction is highly dependent on the biometric modality used, cancellable systems must satisfy various properties, some of which are stated and presented by [9]:

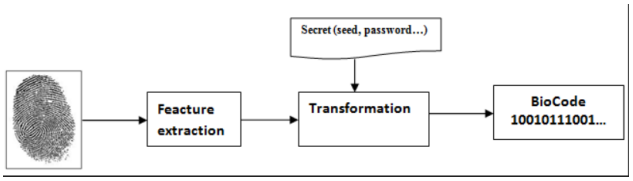

Figure 1. General Model of Fingerprint security concept based in transformation

A. Revocability|Renewability

A model of biometrics must be removed, and a new one should be created using the original template. Using the biometric prototype provided by user z, it should be able to calculate a BioCode $f(bz , Kz^1)$ with the Kz^1 parameters provided by a biometric method with a cancellable transformation revocation by calculating $f (bz , Kz^2)$ with another Kz^2 parameters. Revocability can be achieved conveniently because it only stores the reference BioCode.

B. Performance

The security of the models does not negatively impact the effectiveness of the initial scheme of biometrics. Since effectiveness is linked to the reliability in the method of authentication (e.g., by reducing the amount of false acceptances), a system of cancellable biometric should be as effective as possible. The seed (contained for user z in Kz) could be used like a detail a priori (or secret key) for transformation-based cancellable template biometric systems. For this reason, efficiency or performance is required [4] .

C. Non-inevitability or Irreversibility

It would not be necessary to extract from the converted data adequate information about the original biometric data to stop any attack that might consist of copying a stolen biometric system; this is essential in the security interest An impostor can offer information for any attack to have authentication as the legitimate user [10].

D. Diversity or Unsinkability:

Various BioCodes for different applications should be produced, and neither detail ought to be inferred from comparing or combining different implementations. This property is important for privacy schemes since it removes the risk of identifying a person building on authentication details. $Bz = f (bz , K z^1),..., f (bz , Kz^Q)$ is a variety of BioCodes generated by Q concerning user z and Kz^i the number of parameters for revocation by user z, an indiscriminate subsample of $(0; 1)^Q$ must be used. Also this property avoids the connection attack using the various BioCodes of a user to anticipate an appropriate BioCode; this is linked to an intrusion that consists of listening to the different BioCodes realizations for the same person impostor [4].

Transformation systems can be split into two categories invertible transformation (also called BioHashing) and non-reversible transformation. This work focuses on the BioHashing process, a recent methodology capable of solving the problem of privacy and protection reversal.

The BioHashing algorithm is used for biometric models, de ned through a true-valued of the xed-long vector (A Euclidean distance referred for the determination of the similarity in the midst of the two biometric templates), and then produces binary length templates less than or the same length as the longitude of the original (The Hamming distance for assessing similarity of the two transformed templates) [4].This algorithm was rst introduced by [7].

The ngerprints attributes are rst converted into a xed real vector to produce the biometric system for face and ngerprints. In a second step, the BioHashing algorithm applies to the biometric template, and a binary BioCode is generated. The biometric template is rejected at the end of the enrolment phase, and BioCode is only stored. The BioHashing algorthim can be hired to any biometric modality, represented by a xed- length vector of real values. It converts the biometric template $= (b1,\ldots bw)$ into a binary model $B= (B1,\ldots Bz)$ withm as n as de ned in Algorithm 1[4].

BioHashing Algorithm

1: Inputs
2: $b=(b^1,\ldots,b^w)$:biometric template
3: K: seed value
4: Output $B=(B^1,\ldots,B^z)$: Biocode
5: Generation with K of z pseudo-random vectors V_1 , $\ldots V_z$ of length w,
6: Orthogonalize vectors with the Gram Schmidt algorithm,
7: for j=1,...,z do compute $x_j =< b; V_j >$
8: end for
9: Compute Biocode:

$$B^i = \begin{cases} 0 = x_j \geq r \\ 1 = x_j < r; \end{cases}$$

The r generally have a de ned threshold equivalent to 0 scalar products with orthonormal vectors, ensure the success of this algorithm. The last steps quanti cation process guarantees a non-inevitability of the data (even if $z > w$ since every input b coordinate is a real number, while the output B coordinates are a single bit). The last step, the random seed ensures the properties of revocability and diversity.

3. Related Work

As mentioned in the preceding section, the limited protection of multi-modal systems, the biometric template drawbacks of security techniques, and the impracticality of the identi cation algorithms used in these cases have encouraged searchers to explore the chances to successfully combine these two areas. From the scienti c viewpoint, the protection of a multi-biometric template has multiple aspects [6].

Simultaneously, the industrial actions try to develop a frame that can be used selectively to understand the problems and progress in the eld whereas assessing applications; necessities. In any case, the relationship between the biometrics and protection technics presents emerging challenges and illustrates the potential of additional scenarios that could promise better overall system accuracy [11], [12].

Several studies or experimental approaches that focus on the most widely used biometric data (ngerprint, iris, ,face) and goal to reduce mistakes provinding increased protection [9],[13],[14]. Table 1 summarizes the most remarkable work, according to current methods, aimed at securing the multi-biometric model[6] .

4. Study of the biohashing robustness

Multi biometric system acts, by de nition, on data sensitive personal of individuals. These data must be protected to prevent theft, modi cation, or torture. A general revocable transformation presented by [4], or the potential criteria to be evaluated can be categorized as follows:

A. Security criteria

The risk of intrusion.

Revocability and renewal.

Con dentiality control: this criterion can be likened to the two criteria of irreversibility and partial disclosure of information biometric.

B. Criteria for the preservation of privacy

Irreversibility.

Partial disclosure of biometric information (privacy leakage).

Intractability.

Diversity.

These criteria are now de ned more formally within the framework of the revocable transformation.

C. Evaluation Metrics:

We suggest a set of metrics $A_i \in [0, 1]$, i = 1, ... , 6 [27].

The determination of these metrics is evaluated through di erent attacks. To all those attacks, we employ one or more biometric pattern to produce b z argument from user z. Centered on every theory of attack, we produce a lot of false attempts A_z by the genuine user.

Zero e ort attack (A_1): The impostor tries to usurp the real identity of user z by representing their own

TABLE I. COMPARISON BETWEEN PREVIOUS STUDIES [6]

Authors	Year	Methods	Evaluation (%) FRR FAR EER
Jeong and al [15].	2006	Uses two methods PCA and ICA for feature extraction, and compare them with each other and then use a transformation of BioHashing uses Face template	/
Maiorana and al [8].	2011	Non-invertible transformations use signature template	/
Paul and al [16].	2012	Hybridation of random projection and transformation use Face and Ear template's	/
canuto and al [17].	2013	Revocable multi biometrics Fusion level recognition use iris and Voice data template's	/
Rathgeb and al [18].	2014	Multi biometrics transformation with bloom of lters use iris template	EER= 0,5 %
Rathgeb and al [19].	2015	Multi-biometric transformation with Bloom lters and fusion in level features use Face and iris template's .	EER=0.4 %
Damasceno and al[20].	2015	Interpolation ,BioHashing ,BioConvolving and DoubleSum use Touch Analytics	EER= 28,6 %
Stokkenes and al[10] .	2016	Bloom lter use Face and two peri-ocular regions	/
Yildiz and al[21].	2017	Superimposing various biometric data a fusion of multi-biometric templates of Fingerprint	EER= 2,1 %
Bringer and al[22].	2017	Bloom of lters of Iris	/
Jegede and al[23].	2018	multi-biometric transformation with Matrix transformation of Face and Iris template's	FRR=7.8 % FAR=2.74%
Bedad and Adjoudj [1].	2018	fusion in feature level and BioHashing of Fingerprint	EER= 0 %
Gomez-Barrero and al[24]	2018	Multi-Biometric Template Protection-based on Bloom Filters of face , ngerprint ,Fingervein and iris template's	EER= 0.1 %
Yang and al[25].	2018	cancelable biometric system, feature level fusion and fusion of dtabases (MD-A , MD-B),Fingerprint and Finger-vein template's	EER= 0.12 %
Dwivedi and al[26].	2019	transformation multi-modal biometric with fusion in score and decision stage of Iris and Fingerprint template's	EER= 0.13 %

biometric data b'y with unknown parameters Ky. We will then have Az = f (b'y, Ky)

Brute force attack (A2): The impostor determines to subvert the security module via submitting a model ready to be compared by the comparison module. He randomly estimates dierent values of A so that: Az= A.

Stolen token attack (A3): The impostor manages to get the Kz parameters from user z and attempts to produce various values b to building: Az = f (b, Kz).

Stolen biometric data attack (A4): The impostor gets b'z (Right or after doing the calculation from a compromised biometric sample like a ngerprint trace, for example). He tries dierent values of K to building: AZ = f (b'z, K).

Listening attacks (A5, A6): The impostor should not extract information from any other BioCodes issued by the same user. We assume that an intruder has intercepted N BioCodes distinct from the same user b1, ..,bN . Based on these Q listening, we then generate a BioCode whose bits are set to the value (0 or 1).

The following procedure checks such attacks:

User z produce Q BioCodes:
$Bz = f(bz, Kz^1), .., f(bz, Kz^Q)$
Predicting a potential BioCode by calculating the all likely value of any bit given Bz

Calculation the formula Ai = P(DT (f (bz , Kz),Az EERT)value A5 for Q= 3 and A6 for Q = 11.

5. Proposed Methodology

Multimodal biometric systems are based on several modalities (information sources). We present the most used architecture in a multimodal system. This architecture determines the order of acquisition and the order of data processing as shown in Figure 2.

Researches in the eld of multi-modal biometrics are relatively recent. There have been a lot of researches conducted combining dierent modalities, varying the biometric data fusion level, and testing several fusion strategies.

Figure 2. Architecture of a biometric system

There are four dierent stages of fusion: at the level of data, at the stage of derived characteristics, at the score level resulting from the process of comparison, or in the stage of decision. Figure 3 shows a description of the proposed solution.

The suggested system consists of six consecutive phases:

A. Registration phase

The users, during the enrolment process, must provide their ngerprints on the sensor to generate the reference models. Several examples of instances are stored and replicated in the same kind of biometric characteristic describing this characteristic's variation during this step. We choose the ngerprint method for many causes:

1) The identi cation of the ngerprint is the rst biometric method.
2) It's one of the really popular approaches. Its usefulness for both law enforcement as well as for criminology has been con rmed.
3) Today, con dent biometric methods, such as ngerprint identi cation, are needed wherever to authenticate persons and, therefore, they can be used for programs of very high protection.
4) They are easy to acquire and accepted by the public. The existing database of real ngerprints

B. Feature extraction phase

This phase is at the center of the multi-biometric identi- cation system. The data are removed from the image and saved in the database to retrieve the biometric characteristics for later use in di erent algorithms. It is necessary, however, to discover algorithms in which the feature vectors' values are of constant size since the BioHashing algorithm is used to the biometric data. The result is a xed-length vector of the real value.

They're many recent approaches, commonly used in computer vision problems, such as, LBP (Local Binary Pattern), the Gabor lters. In this analysis, the 2D Log-Gabor lter was used.

Gabor lter was applied in various approaches like enhancement of image, contour detection, extraction of features, and pattern recognition image denotation [28].

Using a 2D Log-Gabor lter to obtain characteristic patterns in two dimensions. Because the lter built a precise frequency and built a precise orientation. The orientation part is a function of Gaussian distance according to the polar coordinate angle. The following equation determines this lter:

$$G(f;\ ) = \exp\left(\frac{\log\frac{f}{f_o}^{2}}{2\log\frac{f}{f_o}}\right)\exp\left(\frac{(\quad_0)^2}{2\ ^2}\right) \quad (1)$$

with:

fo : The frequency at the centre lter;

f : The frequency parameter wide,

o : The filter orientation angle,

: The orientation parameter wide,

The lter applies to the image through a convolution between the lter and the image. The 2D Log-Gabor multiresolution lter G(fs, o) is a 2D Log-Gabor lter applied in various scale(s) and orientation (o) [29].

In our system, we applied this lter on the ngerprints with parameters that gave us a better result, its parameters are scale= 4, orientation= 6, and for the f/ fo ratio, we chose 0.65, for the scale factor, we took 1.3.

2D Log-Gabor lter is used in this work to choose the best possible parameters. A feature vector whose size is 552 features for each image is the result of this extraction process.

C. BioHashing phase

BioHashing principle is to create a BioCode. The BioCode is a binary vector equivalent to the original implemented vector dimension. Results of the algorithm are a feature vector. The size of this vector is 552 features for each picture containing a binary code (0 or 1).

D. Matching phase

Matching between the image request's BioCode and the searched database image's BioCode.

Various distance, like Manhattan, Mahalanobis, Range chi-square, etc.... In this approach, the distance Euclidean was considered.

E. Fusion phase

Fusion examines multi-biometric data security applications between multi-biometric architectures and security algorithms that occur by fusion levels. This research focuses on coupling at two levels: multi -biometric and BioHashing. BioHashing is used in the fusion point. Score-stage fusion,

Figure 3. Overview of the proposed method

therefore, o ers the best balance between the abundance of knowledge and the facility of implementation.

Both fusion methods are used: multi-sample score fusion (that considers the variable exposure and the quality of the acquired image) and multi instance score fusion of three ngers of the left hand are added for better protection and reduced error rate. In the analysis, two scores of the two patterns of a single instance are combined, resulting in an overall score and using a speci c approach by adding three instances. This approach is the weighted sum, which represents a balanced weight equal to one. This method allows a di erent weight to be assigned for each individual system according to its eciency or bene t in the multi-modal approaches [30]. Used methods include the sum rule, the decision tree, and the linear discriminant analysis [5].

F. Decision phase

The decision re ects a similarity matrix's insertion with all combined scores; the system must approve the application if it has a high score (point of interest high number couple).

6. ExperimentalResults

The ngerprint sub-database SDUMLA-HMT [31] is used for experimental tests. This database includes ngerprint images of 106 persons which have been acquired by ve di erent sensors for each person. Six instances (thumb, index, and middle nger of each hand) are recorded, with eight samples of each instance.

The sensors AES2501 and FT-2BU areused in this study, which allow a good analysis of a ngerprint's texture. This database is used for ngerprint veri cation. For each person in a dataset, the rst and the third sample is used as a reference template. The others are used to evaluating the proposed system.

During the experiments, the performance is also evaluated, based on:

1) FAR (False Acceptance Rate)
2) FRR (False Rejection Rate).
3) ROC curve (Receiver Operating Characteristic) show the FRR according to the FAR protection.

Before analysing the multi-biometric protection systems performance based on a transformation, it is important to establish the unprotected multi-modal systems performance to validate the proposed method.

First, we test the proposed system39;s performance without applying the transformation (The BioHashing algorithm). The system is proposed with the application of the

TABLE II. Comparison with the proposed system

Authors	Year	Authors	Evaluation (%) FRR FAR EER
Studies of the robustness of a transformation-based multi-biometric template schemes protection	2021	Multi biometrics transformation with BioHashing and two fusion methods are used: multi-sample score fusion and multi instance score fusion use Fingerprint template's .	FAR=100% EER=0%

Figure 4. ROC curves of the multi-modal approch transformation

transformation (The BioHashing algorithm) without attack, by analysing their curves ROC. We present the values of the six metrics Ai, i=1: 6 for the BioHashing algorithm.

We start by the ROC curve (Receiver Operating Characteristics). Ideally, a successful approach should have low false acceptance rates (FARs) and a high veri cation rates.

In the proposed system for the protected multi-modal system with the application of the transformation, the FAR = 100 % as shown in the Figure 4, versus 81 % for the unprotected multi-modal system without any transformation.

TABLE III. EVALUATION OF EER BY DIFFERENT METRICS

Metrics	A1	A2	A3	A4	A5	A6
EER	0%	50%	47%	47%	51%	51%

The results display that the proposed system without transformation performance is given EER=32%. Figure 4 clearly shows that the EER=0% after application of transformation by the BioHashing algorithm; this is because the BioHashing algorithm made the EER rate private and protected multi-biometric data. We see that these results are better and that using transformations for the security of multi-biometric systems is known to improve results.

On the basis of the studies carried out in section 3 on related works, we used the same pairs from table 1.Table 2 shows the proposed system as well as the evaluation rate.

Now, if we look at the attacks, we begin by re ecting on metrics A1 to A6 relating to an attack. Figure 05 presents these curves for the metrics A1 to A6 : A1 (Zero cost attack), A2(Brute force attack),A3(Stolen token attack), A4(Stolen biometric data attack), A5 (Listening attacks Q = 3),A6(Listening attacks Q = 11).

According to the di erent attacks, we start by setting the value of the EER of the transformation of a multi-biometric protection system. Table 2 summarizes the values of the di erent EERs according to the metrics A1,.. . , A6.

From this representative table of the EER rate according to metrics A1,. . . , A6 (The attacks), we present here an Overview of conducted attacks and their ectiveness:

With the metric A1, it can be observed that this attack is inoperative with an EER=0%. With other attacks, the EER values show that an intruder has a good chance of being accepted through the system without knowing which user he impersonates. From A2 ... A6, we are getting an operational attack.

The proposed system with the application of the transformation is reasonably resilient to attacks (in the worst scenarios); this is due to the use of the estimation of the projection matrix of details relevant to the biometric data. The advantage of the transformation is that it does not directly use the original data for all calculations.

Figure 6 presents the histogram of the distribution of legitimate impostor scores of the proposed approach. It can be noticed that the two pseudo-legitimate distributions are well separated from the legitimate ones39; distribution in the proposed approach. Recall that a histogram is a tool for the statistical representation of a series of N data xi. In abscissa, we represent the classes, that is to say, the intervals $[a_j; a_j + 1]$ within which we will count the data.

This distribution presents an evaluation factor for the models registered in a multi-biometric system. Considered classes are registered individuals. Each class groups together several models of the information of the individual concerned:

1) The legitimate class (intra-class) represents a rate of change or dissimilarity between models of the same individual (representative of the same class).
2) The impostor class (inter-class) represents a rate of change or dissimilarity between the models of dif-

Figure 5. ROC curves for the metrics A1 to A6

ferent individuals (di erent classes of the database). smaller the inter-class class is the greater the FAR's risk.

The multi-biometric system must be based on methods 7. Conclusion and Perspectives
that take these two classes into account to ensure better Multi-biometric data protection is a key development in
discrimination. The larger the intra-class class is, the greater information protection, as it is becoming a classic authenti-
the risk of an increase in the FRR. In the other side, the cation method. This paper proposes an evaluation methodol-

Figure 6. The histogram of the distribution of legitimate/impostor scores of the proposed approach

ogy to protect multi-biometric data with the transformation that focuses on BioHashing, proposing some measures and metrics to test their performance and robustness faced against attacks. The advantage of this solution is that it does not directly use the original data,in addition to guaranteeing the protection of users' privacy.

Several measures are proposed to test the performance between the protected and the unprotected multi-modal system. After the evaluation, a FAR of 100% is achieved on the protected multi-modal system, versus 81% for the unprotected multi-modal system without any transformation. Using this methodology,it is possible to demonstrate the usefulness of the proposed solution, which is also very important for protected multi-modal biometric systems.

On the basis of these obtained results in this study, perspectives for future work are based on biometric transformation and other methods in the literature. The use of transformation represents an effective means of protecting raw multi-biometric data. Furthermore, the authors suggest developing their transformation by reducing the proposed algorithms, running the system in real-time, using deep learning, and executing an HPC machine.

Acknowledgment

The authors are grateful to the anonymous referees for their valuable and helpful comments. This research has been carried out within the PRFU project (Grant: C00L07UN220120180002) of the Department of computer science, University Djillali Liabes of Sidi Bel-Abbes. The authors thank the staff of EEDIS laboratory for helpful comments and suggestions.

References

[1] B. Fatima and A. Peda, "Secured multimodal biometric system," 2018.

[2] A. Juels and M. Wattenberg, "A fuzzy commitment scheme," in Proceedings of the 6th ACM conference on Computer and communications security, 1999, pp. 28–36.

[3] J. Bringer, H. Chabanne, M. Favre, A. Patey, T. Schneider, and M. Zohner, "Gshade: Faster privacy-preserving distance computation and biometric identification," in Proceedings of the 2nd ACM workshop on Information hiding and multimedia security, 2014, pp. 187–198.

[4] C. Rosenberger, "Evaluation of biometric template protection schemes based on a transformation," in ICISSP, 2018, pp. 216–224.

[5] V. Conti, S. Vitabile, L. Agnello, and F. Sorbello, "Fingerprint and iris based authentication in inter-cooperative emerging e-infrastructures," in Internet of Things and Inter-cooperative Computational Technologies for Collective Intelligence. Springer, 2013, pp. 433–462.

[6] F. Bedad and R. Adjoudj, "Multi-biometric template protection: an overview," in International Conference in Artificial Intelligence in Renewable Energetic Systems. Springer, 2018, pp. 70–79.

[7] A. T. B. Jin, D. N. C. Ling, and A. Goh, "Biohashing: two factor authentication featuring fingerprint data and tokenised random number," Pattern recognition, vol. 37, no. 11, pp. 2245–2255, 2004.

[8] P. C. E. Maiorana and A. Neri, "Cancellable biometrics for online signature recognition. in new technologies for digital crime and forensics: Devices, applications, and software," IGI Global, pp. 290–315, 2011.

[9] L. Lu and J. Peng, "Finger multi-biometric cryptosystem using feature-level fusion," International Journal of Signal Processing, Image Processing and Pattern Recognition, vol. 7, no. 3, pp. 223–236, 2014.

[10] M. Stokkenes, R. Ramachandra, M. K. Sigaard, K. Raja, M. Gomez-Barrero, and C. Busch, "Multi-biometric template protection—a security analysis of binarized statistical features for bloom filters on smartphones," in 2016 Sixth International Conference on Image Processing Theory, Tools and Applications (IPTA). IEEE, 2016, pp. 1–6.

[11] R. Connaughton, K. W. Bowyer, and P. J. Flynn, "Fusion of face and iris biometrics," in Handbook of iris recognition. Springer, 2016, pp. 397–415.

[12] C. Rathgeb and A. Uhl, "A survey on biometric cryptosystems and cancelable biometrics," EURASIP Journal on Information Security, vol. 2011, no. 1, pp. 1–25, 2011.