I.J. Image, Graphics and Signal Processing, **2020, 5, 28-36**
Published Online October 2020 in MECS (http://www.mecs-press.org/)
DOI: 10.5815/ijigsp.2020.05.03

A Fingerprint Template Protection Scheme Using Arnold Transform and Bio-hashing

Olufade F. W. Onifade
Department of Computer Science, University of Ibadan, Oyo State Nigeria
Email: fadowilly@yahoo.com

Kabirat B. Olayemi and Folasade O. Isinkaye
Department of Computer Science, University of Ibadan, Oyo State, Nigeria
Department of Computer Science, Ekiti State University, Ado-Ekiti, Nigeria
Email :{kabiratolayemi@gmail.com, folasade.isinkaye@eksu.edu.ng}

Received: 01 February 2020; Accepted: 05 August 2020; Published: 08 October 2020

Abstract: Fingerprint biometric is popularly used for protecting digital devices and applications. They are better and more reliable for authentication in comparison to the usual security tokens or password, which make them to be at the forefront of identity management systems. Though, they have several security benefits, there are several weaknesses of the fingerprint biometric recognition system. The greatest challenge of the fingerprint biometric system is theft or leakage of the template information. Also, each individual has limited and unique fingerprint which is permanent throughout their lifespan, hence, the compromise of the fingerprint biometric will cause a lifetime threat to the security and privacy of such an individual. Security and privacy risk of fingerprint biometric have previously been studied in the context of cryptosystem and cancelable biometric generation. However, these approaches do not obviously address the issue of revocability, diversity and irreversibility of fingerprint features to guard against the wrong use or theft of fingerprint biometric information. In this paper, we proposed a model that harnesses the strength of Arnold transform and Bio-hashing on fingerprint biometric features to overcome the limitations commonly encountered in sole fingerprint biometric approaches. In the experimental analysis, the result of irreversibility showed 0% False Acceptance Rate (FAR), performance showed maximum of 0.2% FAR and maximum of 0.8% False Rejection Rate (FRR) at different threshold values. Also, the result of renewability/revocability at SMDKAB SMKADKB and SMKBDKA showed that the protection did not match each other. Therefore, the performance of the proposed model was notable and the techniques could be efficiently and reliably used to enforce protection on biometric templates in establishments/organizations so that their information and processes could be secured.

Index Terms: Biometric Templates, Cancelable biometrics, Biometric cryptosystem Arnold Transformation, Bio-hashing, Fingerprint.

1. Introduction

The appearance of biometric verification systems has necessitated the protection of biometric templates taken from individuals. Biometric template represents the digital version of the biometric features that are extracted from images of diverse biometric modalities with the aid of different algorithms [1]. The fact that biometrics features of a person cannot be transformed or interchanged when leaked, calls for the need to strongly safeguard biometric templates to prevent counterfeit biometric templates from being used to circumvent a biometric matcher [2]. Also, the usual methods of verification such as passwords and PINs [3] have been employed to protect digital content but their capability are insufficient to protect biometric templates hence the introduction of other template techniques such as encryption of templates, biometric cryptosystem and template transformation. Encryption entails encoding templates with individual information, for example, date of birth, security codes or identity number [4]. Most of these encryption techniques can be predicted by invaders. Biometric cryptosystem usually bind digital key to biometric, though it is tolerant to intra-user variation, generating key with high stability and entropy is challenging [5]. In template transformation, biometric templates extracted from user's original biometric sample is transformed by a non-invertible transformation or user-specific invertible transformation [6]. Also, some attempts have been made to secure biometric template using Unimodal and multimodal techniques. Unimodal systems use single biometric feature [7,8] while multimodal systems use multiple features [6,9] for template protection. Unimodal biometric systems are cheaper and simple to execute but without a unique method for securing their templates information. Multimodal systems on the other hand reduces error rate but they could be costly to implement. Hence, the main goal of a good protection template are not achieved.

In this research, we propose a new approach that provides revocability, irreversibility while preserving performance. To achieve that, we consider harnessing the strength of Arnold transform and Bio-hashing on fingerprint biometric features.

In our proposed model, there are two components: Arnold transformation and Bio-hashing. The Arnold Transformation seeks to apply a scrambling method on the extracted biometric feature. This aims to change the position of the fingerprint minutiae to address the issue of compromised unsecured user key and biometric feature in the bio-hashing phase. The resultant features are then passed into a method based on bio-hashing presented by [10].

In essence, we investigate the following research issues: (1) whether we can develop a fingerprint template which is revocable and irreversible (2) how can we ensure that the performance of the system is not lost. We evaluate this model on real world data to demonstrate the effectiveness of the model. Our result demonstrates that our model was able to achieve a non-invertible transformation that meets the requirement of revocability, irreversibility and diversity.

The rest of the paper is organized as follows. Section II covers a brief review of existing techniques. Section III presented the proposed framework, Section IV described the experiments, results and discussion. Finally section V presented the conclusions and future work.

2. Related Works

Biometric is currently employed in the real world applications [11] and has raised a lot of security and privacy concerns. Biometric templates are very important and hence, there is need to keep them from all forms of attacks which can cause corruption or abuse [12]. Biometric template protection ensures the security of biometric templates at both network and database levels [13] and it therefore important to discuss some of the significant efforts that have been expended on the capability of BioHashing and Arnold transform schemes for protecting and securing biometric templates.

In an attempt to secure a biometric template, [14] proposed a two-stage effective and lossless fingerprint encryption algorithm based on Henon Map and Arnold Transformation. Their protection scheme offered the capability to encrypt and secure templates from illegal users. Also, in a bid to reduce the computational complexity and increase the security of biometric templates, [15] proposed an approach that implemented encryption using the concept of multiple 1-D chaos and 2-D Arnold chaotic map. The proposed scheme was able to provide a large key space and a high order of resistance against several attacks. For the purpose of discovering any alteration of watermarked biometric images and ensure high quality of watermarked biometric images, [16] proposed a fragile watermarking scheme based singular value decomposition (SVD) and Arnold transform. They demonstrated that the proposed fragile watermarking scheme can be applied to the integrity authentication systems based on biometric image. Also, [17] suggested a secure image encryption without size limitation using Arnold Transform and Random Strategies in order to alleviate the problem of security and inadequacy of Arnold Transform to handle images of any size.

[18] proposed a BioHashing technique for fingerprint verification based on minutiae information. They used the spectral minutiae representation of a fingerprint minutiae set to generate a fixed-length bit string by randomly projecting spectral minutiae feature vectors. They reported that their approach showed a promise of fast and secure verification. [19] suggested a transformation-based biometric template protection scheme as an improvement of the BioHashing algorithm where the projection matrix was created by integrating the secret and the biometric data. Experiment conducted on two biometric modalities showed that the proposed technique is efficient. [20] in an attempt to overcome some of the weaknesses of biohashing technique, soft biometrics of the same person was used to improve the discrimination between the genuine and the impostor populations. The technique was evaluated using receiving operating characteristic (ROC) curve and the equal error rate (EER). The performance of the new system was better. [21], in a bid to address the security difficulty of speech perception hash authentication, the application scope of speech authentication algorithm, and improve the robustness, discrimination and real-time authentication in the process of authentication proposed a multi-format speech BioHashing algorithm based on spectrogram. They reported that their work showed very high real-time performance. [22] examined the technical performance of biometric template protection schemes using biohashing technique. They reported that fingerprints easily achieve a very low EER with only some random bits, since only five random bits in the auxiliary data are adequate to alter experimental results considerably. The authors suggested that the security analysis of biometric systems should be founded on irreversibility and unlinkability criteria.

Though, Arnold transformation is very useful in image scramble due to its periodicity. However, a lot of time is wasted during the time of using its periodicity to get the anti-Arnold transformation algorithm, particularly when it employed in the picture with large degree. Likewise, despite the fact that biohashing technique is simple and can be implemented on any biometric modality, the performance degrades whenever a legitimate token is stolen and used by an impostor to claim as an authentic user. Therefore, in this work, we proposed a model that harnesses the strength of Arnold transform and Bio-hashing on fingerprint biometric features to overcome their limitations.

3. Proposed Framework

Our proposed framework aims to concurrently improve performance and ensures irreversibility, revocability and diversity. The framework (illustrated in figure 1) consists of two major components, 1) Arnold Transformation, and 2) Biohashing. The Arnold Transformation F_A aims to scramble each position of the extracted features. The Biohashing F_B phase seeks to generate a vector of bits starting from the biometric feature set and a seed which represents the "Hash key" by utilizing the scrambled F_A as its input value.

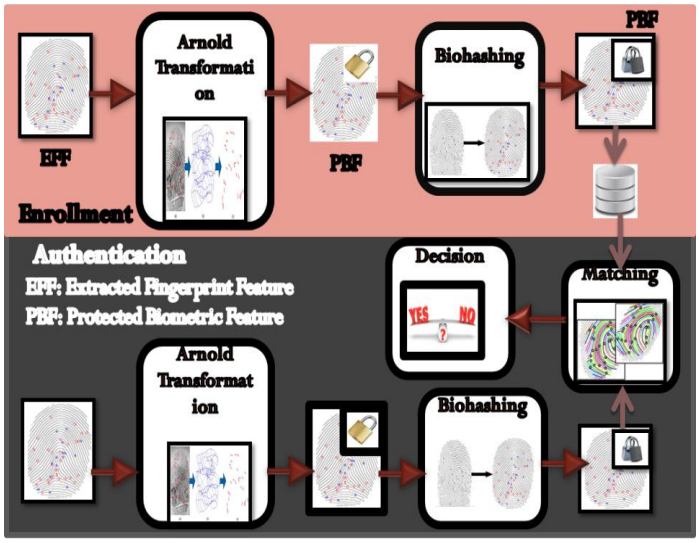

Fig. 1. The architecture of the proposed model

A. Arnold Transformation

Arnold Cat Mat transformation approach was adopted in this work to scramble the biometric feature before passing it into the Biohashing phase. The aim is to address the issue of compromised unsecured user key and biometric feature in the Biohashing proposed by [10]. Arnold transformation is a spatial domain transformation [23] which has security quality factor of zero. Similarly, the Cat Map represents a one-to-one mapping where each point in matrix can be distinctively transformed to another point. This means the intensity distribution remains the same as in the in scrambled images. Also, the histogram of original image as well as that of the scrambled image is identical. In addition, images scrambled using Arnold transformation has a good correlation coefficient. A 2-D Arnold transformation which converts the coordinate (x, y) to (x', y') can be defined as (1):

$$\begin{bmatrix} x' \\ y' \end{bmatrix} = \begin{bmatrix} 1 & 1 \\ 1 & 2 \end{bmatrix} \times \begin{bmatrix} x \\ y \end{bmatrix} \ mod\ n \quad (1)$$

Algorithm 1 was used to find our scrambled fingerprint minutiae. Coarsely speaking, in each iteration, it keeps swapping the position of the minutiae.

Algorithm 1: Arnold Transformation Algorithm

Input: gray fingerprint image;
Output: encrypted image;

1. Define the number of iteration;
2. j=1;
3. do, until the j is greater than number of iteration
4. for x = 1 to n
5. for y = 1 to n
6. x1 = mod ((1*x+1*y),n);
7. y1 = mod ((1*x+2*y), n);
8. temp = image(x,y);
9. image(x,y) = image(x1,y1);
10. image(x1, y1) = temp
11. J = j + 1;
12. End do

B. Reformulated Bio-Hash

In this section, we propose a new Biohashing model. The proposed model is shown in Figure 2. Inspired by the success of Biohashing in [10], we choose Biohashing over other methods. The model generates a vector of bits starting from the biometric feature set and a seed which represents the "Hash key". The ideas behind Biohashing are:

(i) Biometric feature is extracted from the fingerprint as input. The biometric feature is represented as a fixed-length vector, $\Gamma \in R^n$, with n being the length of Γ.
(ii) Random number $\{r_i \in R^n | i = 1 \ldots m\}$, is generated using a user-specific key.
(iii) Orthonormal pseudo-random vectors are generated using Gram-Schmidt algorithm from the random number. $\{\boldsymbol{r} \perp i \in R^n | i = 1 \ldots m\}$ and $m \leq n$.
(iv) Compute inner product of user key and biometric feature via $\{<\Gamma | \boldsymbol{r} \perp i> | i = 1 \ldots m\}$.
(v) Binary discretisation to compute an m bit BioHash template, $b = \{b_i | i = 1, \ldots, m\}$ from (2) as:

$$\boldsymbol{b_i} = \begin{cases} \boldsymbol{0\ if} \ < \Gamma \,||\boldsymbol{r} \perp i > \leq \tau \\ 1 \text{ if } < \Gamma||\boldsymbol{r} \perp i > \geq \tau \end{cases} \tag{2}$$

with τ being an empirically determined threshold.

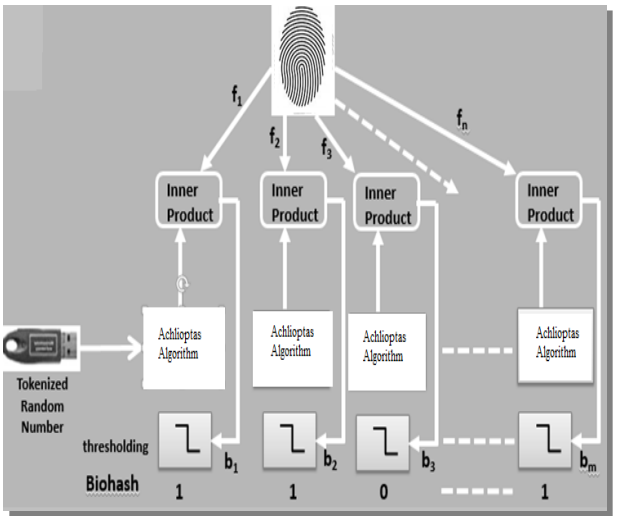

Fig. 2. The Proposed Bio-hashing Progression.

Through an experimental study, some weaknesses of the base Bio-Hashing technique were identified which include:

i. Compromised of unsecured user key and biometric feature
ii. The execution speed is slow due to the method used in obtaining the orthogonal matrix.

In order to boost the performance of Bio-Hashing technique, our Algorithm1 put the following points into consideration.

i. We improve the security of the system by first applying a scrambling method on the biometric feature
ii. The execution speed was improved by applying Achilioptas algorithm to generate orthogonal matrix.

4. Experimental Evaluation

A. Experimental Setup

The proposed methodology was evaluated on images taken from FVC 2000, 2002 and 2004 (Set B), which is available on their website for download. All the FVC (Set B) provided four different fingerprint databases: DB1, DB2 and DB3 which are acquired by various sensors, low cost and high quality, optical and capacitive whereas the fourth; DB4 contains synthetically generated images. The procedure used for feature extraction by [24] was adopted in this work.

B. Evaluation Criteria

In order to evaluate the proposed approach, three template protection requirements were employed, they are: Irreversibility, Renewability/Revocability and Performance/Diversity. They are discussed as follows:

i. ***Irreversibility****:* In the proposed method, irreversibility is ensured in that if an impostor is able to break through the Bio-hashing stage, he will only obtain the scramble minutiae which will not match with the original fingerprint minutiae. Table 1 shows the result obtained from matching the original minutiae with a compromised minutia after breaking through the Bio-hashing stage. There was exaggerated displacement while matching all the dataset in FVC2000 DB4, eight (8), five (5) and nine (9) in FVC2004 DB1, DB3 and DB4 respectively.

ii. ***Renewability/Revocability:*** To measure the degree of difference between transformed minutiae, different user keys were used to transform same biometric feature and then compared. To achieve this, three (3) approaches were used:

- The matching of the same minutiae, same key at Bio-hashing stage but different keys at Arnold transformation stage (SMKBDKA);
- The matching of the same minutiae, and same key during Arnold transformation stage but different keys at Biohashing stage (SMKADKB); and
- The matching of the same minutiae but different keys during Arnold transformation stage and Biohashing stage (SMDKAB).

Tables 2, 3 and 4 show the results of the evaluation approaches respectively.

iiii ***Performance/Diversity:*** Tables 5 shows the distribution when each user has different key while table 6 shows the distribution when each user has the same key. In both cases, the proposed method showed better performance.

C. Results and Discussion

i. ***Ensuring Irreversibility:*** in order to ensure this, it should be computationally hard to construct the original biometric template from stored reference data. It should at the same time easy to generate the protected biometric template. The proposed method gave a result of no match (0% FAR) in Table 1 when the compromised protected fingerprint template was matched with the original protected fingerprint template.

ii. ***Ensuring Renewability/Revocability:*** Figure.3 shows the three distributions when same minutiae were matched against different keys at both levels of protection (SMDKAB) and at individual level of protection (SMKADKB AND SMKBDKA). It was found that at the three levels, the protected fingerprint templates did not match with each other hence; ensuring that if a minutia is compromised, other keys can be used to protect the fingerprint template.

iii. ***Ensuring high performance:*** the proposed method ensured high performance level in that different keys were used to test for the false acceptance rate (FAR) and the false rejection rate (FRR). We achieved a maximum of 0.2% FAR and a maximum of 0.8% FRR after varying the threshold values as shown in Figure 4.

The FAR is the percentage of identification instances in which false acceptance occurs. It is defined as:

$$FAR = \frac{no\ of\ false\ acceptance}{total\ number\ of\ trials} \times 100$$

While FRR is the percentage of identification instances in which false rejection occurs. It is defined as:

$$FRR = \frac{no\ of\ false\ rejection}{total\ number\ of\ trials} \times\ 100$$

Table 1. Test for Irreversibility using original minutiae against compromised minutiae.

	Data Set(Number of false match for each 80 fingerprints)			
	DB1	DB2	DB3	DB4
FVC2000	0/80	0/80	0/80	Exaggerated displacement
FVC2002	0/80	0/80	0/80	0/80
FVC2004	0/72	0/80	0/75	0/71

Table 2. Test for renewability/revocability using same minutiae and key during Bio-hashing but different key during Arnold transform.

	Data Set(Number of false match for each 80 fingerprints)			
	DB1	DB2	DB3	DB4
FVC2000	0/80	0/80	0/80	Exaggerated displacement
FVC2002	0/80	0/80	0/80	0/80
FVC2004	0/80	0/80	0/80	0/80

Table 3. Test for renewability/revocability using same minutiae and key during Arnold transform but different key during Bio-hashing.

	Data Set(Number of false match for each 80 fingerprints)			
	DB1	DB2	DB3	DB4
FVC2000	0/80	0/80	0/80	Exaggerated displacement
FVC2002	0/80	0/80	0/80	0/80
FVC2004	0/80	0/80	0/80	0/80

Table 4. Test for performance/diversity (False Acceptance Rate)

	Data Set(Number of false match for each 80 fingerprints)			
	DB1	DB2	DB3	DB4
FVC2000	0/80	0/80	0/80	Exaggerated displacement
FVC2002	10/80	0/80	4/80	0/80
FVC2004	8/80	1/80	0/80	0/80

Table 5. Test for performance/diversity (False Rejection Rate)

	Data Set(Number of false match for each 80 fingerprints)			
	DB1	DB2	DB3	DB4
FVC2000	0/80	0/80	0/80	Exaggerated displacement
FVC2002	6/80	0/80	0/80	2/80
FVC2004	3/80	0/80	0/80	4/80

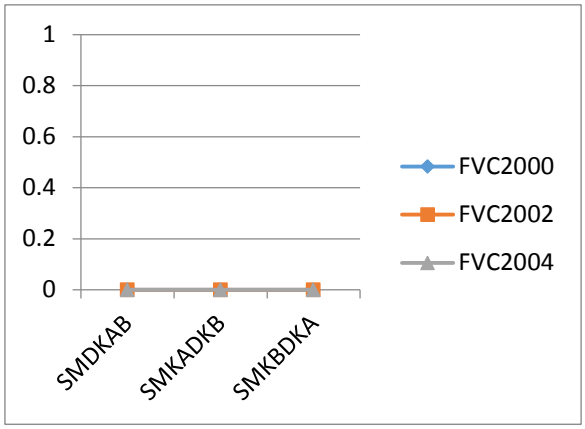

Fig.3. Match rate for or renewability/revocability.

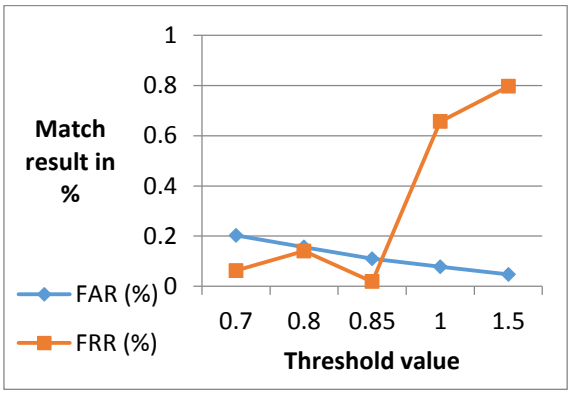

Fig.4. Result for FAR/FRR test

We integrated the Arnold transform and Bio-hashing approaches together in order to overcome the limitations commonly encountered in sole fingerprint biometric approaches. We used different evaluation criteria namely, irreversibility, renewability/revocability and performance/diversity to evaluate our model and the results as discussed above showed very good performance.

5. Conclusion

In this paper, we proposed a new technique for protecting fingerprint templates using Arnold Transform and Bio-hashing. This approach has significant advantages over the use of token or solely biometrics. In our experimental analysis, the result of irreversibility showed 0% FAR, performance showed maximum of 0.2% FAR and maximum of 0.8% FRR at different threshold values. Also, the result of renewability/revocability at SMDKAB SMKADKB and SMKBDKA showed that the protection did not match each other. This implied that the performance was ideal when there was no match in two templates from the same fingerprint and different keys were used and when different fingerprints but same keys were used thereby clearly separating genuine user from an impostor. Our approach can be considered highly secured in that, during the one-way transformation used to generate the token, the token could not be recovered. Also, if the protected template is compromised, a new protected template can simply be generated using different keys during Arnold Transform and Bio-hashing. Therefore, the techniques could be efficiently and reliably used to enforce protection to biometric templates in establishments/organizations so that their information and processes could be secured. However, the proposed method was implemented only on fingerprint biometric where the features are not of high dimensional space. We hope to apply the new technique to other biometric features where the features extracted belong to an intrinsically high dimensional space.

References

[1] V.K. Gunjan, P.S. Prasad, and S. Mukherjee, “Biometric template protection scheme-cancelable biometrics.” In *ICCCE 2019* (pp. 405-411). Springer, Singapore

[2] M. Arjunwadkar, R. V. Kulkarni and C. Shahu, “Biometric Device Assistant Tool: Intelligent Agent for Intrusion Detection at Biometric Device using JESS,” *International Journal of Computer Science Issues*, 2012, Vol. 9, no. 6, pp. 366-370.

[3] N. K. Ratha, J. H. Connell, R. M. Bolle, “Enhancing security and privacy in biometrics-based authentication systems.” *IBM systems Journal*, 2001, Vol.40, no. 3, pp. 614-634.

[4] M. Kaur, S. Sofat and D. Saraswat, "Template and Database Security in Biometric Systems: A Challenging Task," *International Journal of Computer Applications*, 2010, Vol. 4, no. 5, pp.1-5.
[5] P. Poongodi, and P. Betty, "A Study on Biometric Template Protection Techniques." *International Journal of Engineering Trends and Technology (IJETT)*, 2014, Vol.7, no. 4, pp. 202-204.
[6] M. Butt, O. Henniger, A. Nouak, A. and Kuijper, "Privacy protection of biometric templates," In *International Conference on Human-Computer Interaction*, 2014, (pp. 153-158). Springer, Cham.
[7] V. Sujitha and D. Chitra, "Highly secure palmprint based biometric template using fuzzy vault." *Concurrency and Computation: Practice and Experience*, 2019, Vol. 31, no. 12, e4513.
[8] R. Mehmood, and A. Selwal, "Fingerprint biometric template security schemes: attacks and countermeasures." In *Proceedings of ICRIC 2019* (pp. 455-467). Springer, Cham.
[9] A. Selwal, and S.K Gupta, "Template security analysis of multimodal biometric frameworks based on fingerprint and hand geometry." *Perspectives in Science*, Vol. 8, pp. 705-708.
[10] F. O. Isinkaye, J. Soyemi, and O. I. Arowosegbe, (2020). An Android-based Face Recognition System for Class Attendance and Malpractice Control. *International Journal of Computer Science and Information Security (IJCSIS)*, 2020, Vol. 18, no.1, pp.78-83.
[11] O. F. Onifade, P. Akinde, and F. O. Isinkaye, Circular Gabor wavelet algorithm for fingerprint liveness detection. *Journal of Advanced Computer Science & Technology*, 2020, Vol. 9 no.1, pp.1-5.
[12] N. M.Surse, and P. Vinayakray-Jani, "Finger-vein template protection using compressed sensing." In *Innovations in Computer Science and Engineering*, 2019, (pp. 299-307). Springer, Singapore.
[13] G. Mehta, M. K. Dutta, J. Karasek, and P. S. Kim, "An efficient and lossless fingerprint encryption algorithm using Henon map & Arnold transformation." In *2013 International Conference on Control Communication and Computing (ICCC)*, 2013, (pp. 485-489). IEEE.
[14] G. Mehta, M. K. Dutta, and P. S. Kim, "A secure encryption method for biometric templates based on chaotic theory." In *Transactions on Computational Science XXVII*, 2016, (pp. 120-140). Springer, Berlin, Heidelberg.
[15] D. S Wang, J. P. Li, D. K. Hu, and Y. H. Yan, "A novel biometric image integrity authentication using fragile watermarking and Arnold transform." In *Information Computing and Automation, 2008, (In 3 Volumes)* (pp. 799-802).
[16] Z. Tang, and X. Zhang, "Secure image encryption without size limitation using Arnold transform and random strategies." *Journal of multimedia*, 2011, Vol. 6, no. 2, pp. 202.
[17] B. Topcu, H. Erdogan, C. Karabat, and B. Yanikoglu, "Biohashing with fingerprint spectral minutiae". In *2013 International Conference of the BIOSIG Special Interest Group (BIOSIG)*, 2013, (pp. 1-12). IEEE.
[18] K. Atighehchi, L. Ghammam, M. Barbier, and C. Rosenberger, "GREYC-Hashing: Combining biometrics and secret for enhancing the security of protected templates". *Future Generation Computer Systems*, 2019, Vol. 101, pp. 819-830.
[19] N. Saini, and A. Sinha, "Soft biometrics in conjunction with optics based biohashing." *Optics communications*, 2011, Vol. 284, no. 3, pp. 756-763.
[20] Y. B. Huang, Y. Wang, Q. Y. Zhang, W. Z. Zhang, and M. H. Fan, (2020). "Multi-format speech BioHashing based on spectrogram." *Multimedia Tools and Applications*, 2020, pp. 1-21.
[21] P. Lacharme, "Revisiting the accuracy of the biohashing algorithm on fingerprints." *IET biometrics*, 2013, Vol. 2, no. 3, pp. 130-133.
[22] S. K. A. Khalid, M. M. Deris and K. M. Mohamad, "A robust digital image watermarking against salt and pepper using Sudoku," In *The Second International Conference on Informatics Engineering & Information Science (ICIEIS2013)*, 2013, (pp. 96-106). The Society of Digital Information and Wireless Communication.
[23] A. T. B. Jin, D. N. C. Ling and O. T. Song, "An efficient fingerprint verification system using integrated wavelet and Fourier–Mellin invariant transform," *Image and Vision Computing*, 2004, Vol. 22, no. 6, pp. 503-513.
[24] P. N. Gakare, A. M. Patel, J. R. Vaghela and R. N. Awale, "Real time feature extraction of ECG signal on android platform," In *2012 international conference on communication, information & computing technology (ICCICT)*, 2012, (pp. 1-5). IEEE.

Authors' Profiles

Olufade F.W. Onifade received his PhD in Computer Science from University of Ibadan, Oyo State, Nigeria. He is currently an Associate Professor at the Department of Computer Science, University of Ibadan, Oyo State, Nigeria. His areas of specialization include Data and information quality, Risk Management in Economic Intelligent processes using Soft Computing Methodology with deep bias for Fuzzy. Biometrics Applications, Algorithm Development and Web Intelligence. He was a visiting scholar at Massachusetts Institute of Technology and he is currently a visiting Professor at Campbellsville University, School of Business Education & Technology, Campbellsville, KY.

Kabirat B. Olayemi is a PhD research student at Federal University, Oye Ekit, Ekiti State. She has a B.Sc degree in Computer Science from Adekunle Ajasin University, Akungba Akoko, Ondo State, Nigeria. She received her M.Sc degree in computer science from University of Ibadan, Oyo State, Nigeria. Her research interest includes Biometric security, Natural Language Processing (NLP), Machine learning and Internet security. She is a member of Data Science Nigeria.

Folasade O. Isinkaye received her PhD in Computer Science from the University of Ibadan, Oyo State, Nigeria. She is a Senior Lecturer in the Department of Computer Science, Ekiti State University, Ado-Ekiti, Nigeria. Her research interests include Recommender systems, data mining, machine learning and Information security. She is a member of professional bodies which include, Computer Professionals (Registration Council of Nigeria (CPN)) and Association for Computing Machinery (ACM). She was a visiting PhD scholar at the Laboratory for Knowledge Management, Politecnico di Bari, Italy.

How to cite this paper: Olufade F. W. Onifade, Kabirat B. Olayemi, Folasade O. Isinkaye, " A Fingerprint Template Protection Scheme Using Arnold Transform and Bio-hashing", International Journal of Image, Graphics and Signal Processing(IJIGSP), Vol.12, No.5, pp. 28-36, 2020.DOI: 10.5815/ijigsp.2020.05.03

