Framework for Secured Biometric System

F.S. Omotosho, R.S. Babatunde, K. A. Gbolagade

Abstract— Biometrics provides higher accuracy of personal recognition in real identity management system than traditional methods because of its properties. However, the security of biometric systems can be undermined, if the template derived from the biometrics traits such as fingerprint is compromised. If a biometric template is compromised, it leads to serious security and privacy threats. Unlike passwords, it is impossible for a legitimate user to revoke his/her biometric traits and switch to another set of uncompromised identifiers.

One methodology for biometric template protection is the template transformation approach, where the template, consisting of the features extracted from the biometric trait, is transformed using parameters derived from a user specific password or key, through transformation algorithm and only the transformed template is stored in the database.

This study develops a framework that uses a generated random key without user specific password or key during enrollment / verification and it will be used to secure medical records that uses biometric authentication. Collection of fingerprint images will be carried-out through Fingerprint Live Scan Device (SecuGen 7.1).

The outcomes of this study will incorporate the property of revocability or cancelability with Biometric system without degrading the performance and efficiency of the system.

Index Terms: Biometrics, Security, Template, Traits, Revocability, Cancelability, Transformation, Authentication.

1 INTRODUCTION

Biometrics are our most unique physiological traits such as fingerprint, face, iris, hand geometry, voice that can be practically sensed by devices and interpreted by computers so that they may be used as proxies of our physical selves in the digital realm [1]. In this way we can bond digital data to our identity with permanency, consistency, and unambiguity, and retrieve that data using computers in a rapid and automated ways [2].

1.1 Fingerprint Recognition

Fingerprint identification is one of the most well-known and publicized biometrics [4]. Fingerprint identification is popular because of the ease in acquisition, the numerous sources ten fingers available for collection per individual [5].

1.2 What is a Template?

A template is a set of features extracted from the biometric trait. A template is stored in the biometric system database and is used for matching with the input biometric during an authentication attempt [3].

1.3 Biometric systems modes

Biometric systems can be used in two different modes enrollment and identification modes [6].

With the widespread deployment of biometric systems in various applications, the focus now is on biometric template security which is an important issue because, unlike passwords and tokens, compromised biometric templates cannot be revoked and reissued [7]. Protecting the template post a great challenge [2], [13]. Therefore, storing biometric templates, which is unique to individual user, entails significant security risks [8].

One of the most potentially damaging attacks on a biometric system is against the biometric templates stored in the system database. Attacks on the template can lead to the following three vulnerabilities:

(i) A template can be replaced by an impostor’s template to gain unauthorized access.

(ii) A physical spoof can be created from the template to gain unauthorized access to the system, also to other systems which use the same biometric trait.

(iii) The stolen template can be replayed to the matcher to gain unauthorized access [2].

This work addresses this problem by proposing a framework for securing biometric system through fingerprint template

•Segun F. Omotosho obtained B.Sc., M.Sc. in Computer Science. He is currently pursuing Ph.D. degree program in Computer Science at the Department of Computer Science, College of Information and Communication Technology, Kwara State University, Malete. Nigeria. His research interests includes Biometric authentication, Pattern recognition, E-health and Residue Number System. funshosegun@yahoo.com

•Ronke S. Babatunde has a Ph.D in Computer Science, currently a Lecturer in the Department of Computer Science, College of Information and Communication Technology, Kwara State University, Malete. Nigeria. Her research interest includes: Soft Computing, Machine Learning, Deep Learning, Big Data and Computational Intelligence. ronke.babatunde@kwasu.edu.ng

•Kazeem A. Gbolagade is a Professor of Computer Science, in the Department of Computer Science, College of Information and Communication Technology, Kwara State University, Malete. Nigeria. His research interest includes: Residue Number System, VHDL, Parallel Processing, and building High Speed Microprocessor. kazeem.gbolagade@kwasu.edu.ng

transformation approach that uses a generated random key as parameter for the transformation rather than user supply password or key. This work focuses on achieving a secure biometric system and flexibility of use by the user without the needs to remember special password or key. It does not address the security of the system database itself but securing the fingerprint template from being compromised.
Section II provides a critical analysis of related work while Section III gives detailed explanation of our proposed framework. Evaluation of the framework is discussed in Section IV with Section V concludes the paper by summarizing our contribution.

2 RELATEDWORK

2.1 Securing Biometric System

Passwords and PIN have the property that if they are compromised, the system administrator can issue a new one to the user. It is desirable to have the same property embedded in biometric system [10].

The following section provides a detailed description of the approaches that have been proposed for securing biometric templates:

The template protection schemes proposed in the literature can be broadly classified into two categories, namely, (i) feature transformation approach and (ii) biometric cryptosystem [2]. As seen in figure 1.

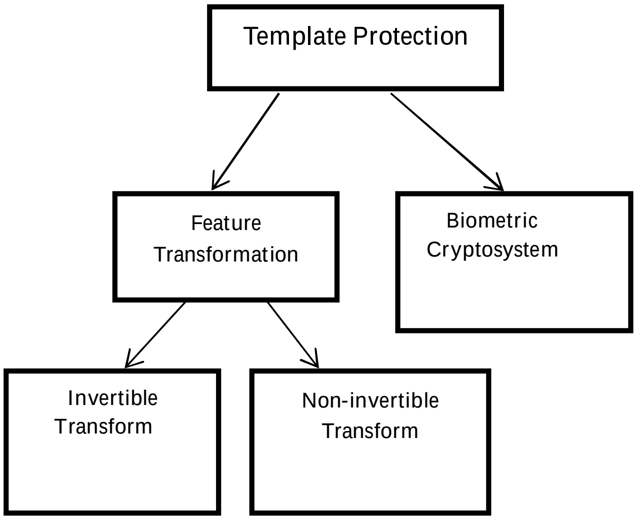

Figure 1: Categorization of template protection schemes

2.2 Feature transformation approaches

In the feature transform approach, a transformation function (F) is applied to the biometric template (T) and only the transformed template (F (T; K)) is stored in the database. The parameters of the transformation function are typically derived from user specific key (K) or password. The same transformation function is applied to query features (Q) and the transformed query (F (Q; K)) is directly matched against the transformed template (F (T; K)). The feature transform schemes can be further categorized as (i) Invertible and (ii) Non-invertible transforms [9], [11].

2.2.1 Invertible (Salting) transform

This is a template protection approach in which the biometric features are transformed using a function defined by a user-specific key or password. Since the transformation is invertible to a large extent, the key needs to be securely stored or remembered by the user and presented during authentication. The limitation in this approach is that there is need for additional information in the form of special password or key which increases user's inconveniences [11, 9]. Also, if the user-specific key is compromised, the template is no longer secure.

2.2.2 Non-invertible transforms

In this approach, the biometric template is secured by applying a noninvertible transformation function to it. Noninvertible transform refers to a one-way function, F, that is "easy to compute" (in polynomial time) but "hard to invert" (given F (x), the probability of finding x in polynomial time is small) [9], [8]. The parameters of the transformation function are defined by a key which must be available at the time of authentication to transform the query feature set. The main drawback of this approach is the trade of between discriminability and noninvertibility of the transformation function. The transformation function does not preserve the discriminability (similarity structure) of the feature set, that is, features from the same user should have high similarity in the transformed space, and features from diferent users should be quite dissimilar after transformation [2]. Also, given a transformed feature set, an adversary can still obtain a close approximation of the original feature set of it. The user must remember the special key which increases the user inconveniences [6}, [7].
This paper proposes a fingerprint transformation method that does not require user to supply a secrete key during enrollment or verification, yet secure the template and preserve the similarity structure of the feature set.

3 ARCHITECTURAL FRAMEWORK

Our framework consists mainly of two phases:
The Enrollment Phase
The Verification Phase
The model works towards the design of fingerprint transformation approach which employs some existing algorithms for feature extraction see figure 2.

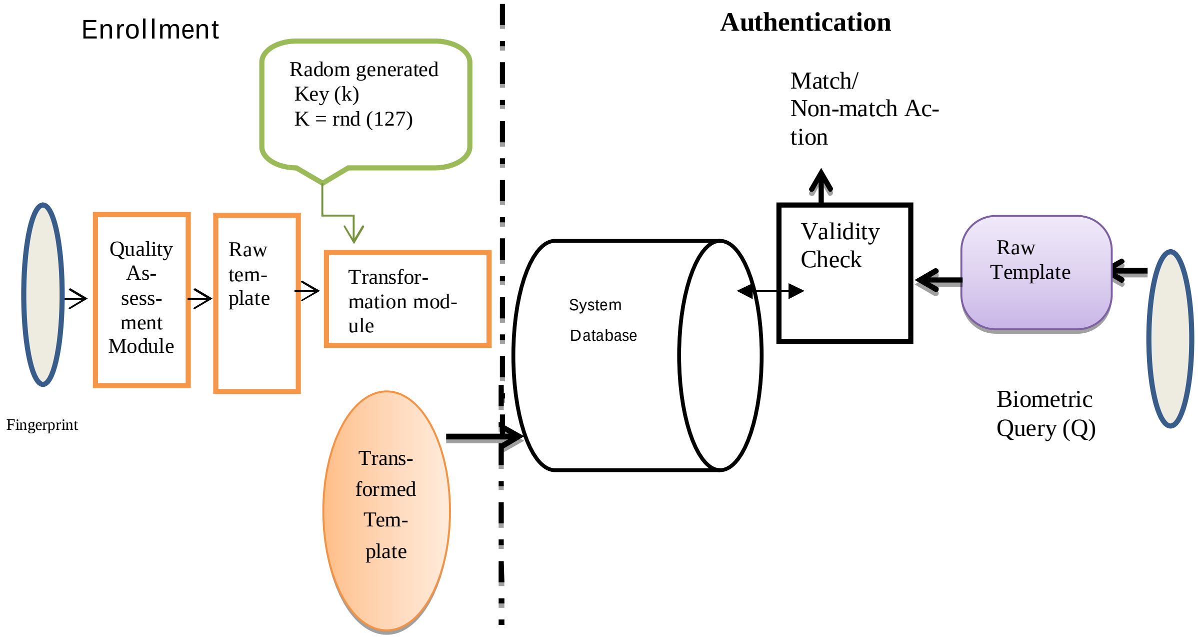

Figure 2: Framework of the proposed Fingerprint template transformation

3.1 The enrollment Phase

The sensor which represents a fingerprint scanner attached toa system on which the application runs will accept the fingerprint of the user. The quality assessment module determines whether the scanned biometric trait (fingerprint) is of sufficient quality for further processing. Feature extraction module processes the scanned biometric data to extract the salient information (feature set) that is useful in distinguishing between different users. Two image samples will be captured per fingerprint for a higher degree of accuracy. The minutiae data from each image sample will then be compared against each other (i.e. matched) to confirm the quality of the registered fingerprints. This comparison is analogous to a password confirmation routine that is commonly required for entering a new password. Then the feature data (minutiae) is extracted from the image into a template. The template transformation algorithm which is the main work of this research takes the extracted feature (template (t), random generated key (k), fixed indexed and computed indexed to generate a new transform template (tr) which will be stored in the database, indexed by the user's identity see figure 3 & 4.

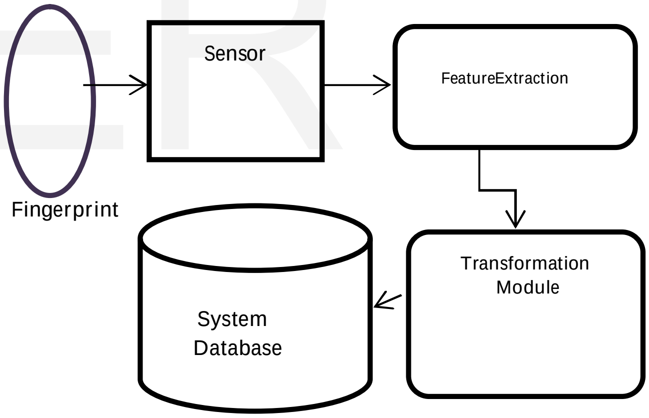

Figure 3: Fearture transformation Module

.

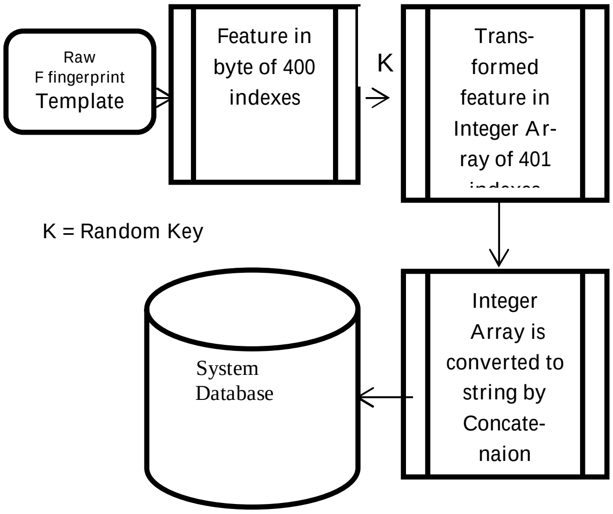
Raw
F fingerprint
Template
Feature in byte of 400 indexes
K
Trans- formed feature in Integer Ar- ray of 401 indexes
K = Random Key
System Database
Integer Array is converted to string by Concate- naion

Figure 4: Flowchart of Template transformation module

3.2 The verification phase

Here, unlike the enrollment phase the sensor accept input of a single fingerprint from an individual who had previously enrolled, extract its features and then present the template to the validity module. The validity module performed validity check on the presented template by comparing it with stored transformed template in the system database. If the template is found it will perform a match action, if not it will performed a non-match action.

3.3 Application of Our Proposed Scheme to Medical Record:

The framework will be applied by implementing an application based on the proposed framework using Medical Record Biometric System [14] as shuwn in figure 5.

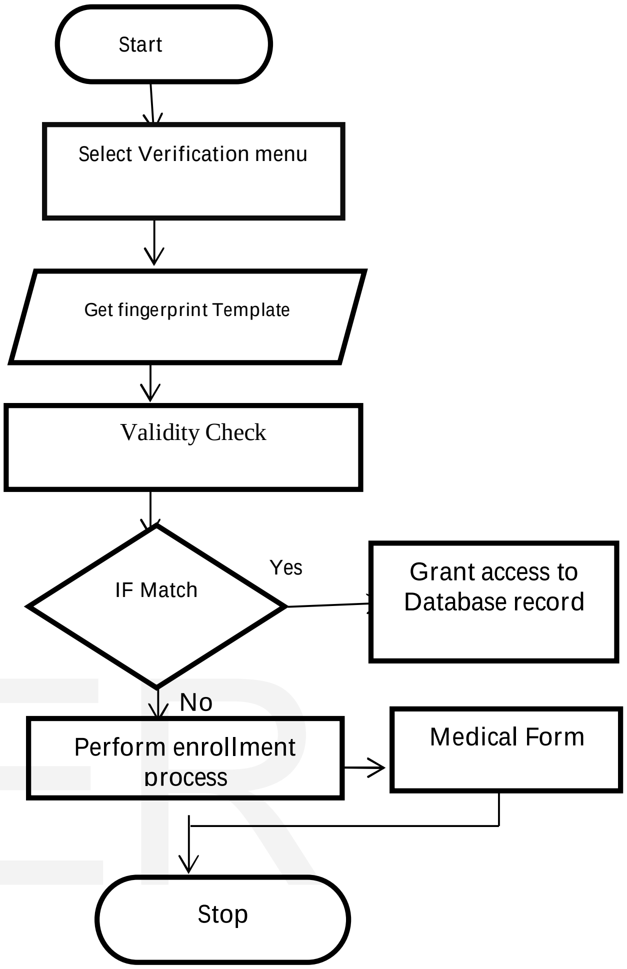

Figure 5: Prototype Program Flowchart

4. PERFORMANCE EVALUATION

The prototype of the framework will be evaluated based on users' assessment in terms of system reliability and effectiveness, system ease of usage and efficiency of the system. We intend to carry out an initial pilot study where the experimental procedure and guideline will be properly mapped out through hardware performances, software management and how easy and productive user find it through user testing [13].

4.1 Evaluation indexes for fingerprint recognition.

Two indexes are well accepted to determine the performance of a fingerprint authentication system: One is FRR (false rejection rate) and the other is FAR (false acceptance rate) [12].

FAR- describes the number of times, someone is inaccurately positively matched.

FRR- describes the number of times someone who should be identified positively is instead rejected [11].

Table 1: Evaluation Indexes

FAR	FRR
(%) FAR = (FA/N) * 100 FA = number of incidents of false acceptance N = total number of samples	(%) FRR = (FR/N) * 100 FR = number of incidents of false rejections. N = total number of samples.

5. CONCLUSION

The success of biometric system cannot be affirmed without a critical examination of security of template stored in the system database. The main idea of this approach is to store the transformed template instead of storing the original template in its raw form. In case the stored template is stolen or lost, it is computationally hard to reconstruct the original raw biometric data from this template.

In this research work, we proposed a fingerprint transformation method that does not require user to supply a secrete key during enrollment.

Security breaches have been usually traced to the in-house people like developers, administrators, users and so on due to having some constant values in the encrypting algorithms, this research takes an extra effort to having fixed and computed indexes. Computed indexes are determined internally by the algorithm at runtime which makes it impossible for these people to predetermine or guess indexes that will be encrypted.

Passwords and PIN have the property that if they are compromised, the user can change it; it is desirable to have the same property of revocability or cancelability with biometric templates.

The outcomes of this study will incorporate the property of revocability or cancelability with Biometric system without degrading the performance and efficiency of the system.

Acknowledgment

The authors wish to thanks all the researchers that have done great work in this research area.

References

[1] J. Wayman, et al, (2005), "Biometric Systems Technology, Design and Performance Evaluation" (London: Springer). W.-K. Chen, *Linear Networks and Systems.* Belmont, Calif.: Wadsworth, pp. 123-135, 1993. (Book style)

[2] A. K. Jain, N.Nandakumar, and A.Nagar, (2008), "Biometric template security," EURASIP Journal on Advances in Signal Processing 2008, 1–17 K. Elissa, "An Overview of Decision Theory," unpublished. (Unplublished manuscript)

[3] Maltoni, Davide, Maio, Jain, and Prabhakar, (2005), "Handbook of Fingerprint Recognition" (Springer: New York).

[4] A. K. Jain, A. Ross, and S. Pankanti, (2006), "Biometrics: a tool for information security," IEEE Transactions on Information Forensics and Security, vol. 1, no. 2, pp. 125–143, D.S. Coming and O.G. Staadt, "Velocity-Aligned Discrete Oriented Polytopes for Dynamic Collision Detection," IEEE Trans. Visualization and Computer Graphics, vol. 14, no. 1, pp. 1-12, Jan/Feb 2008, doi:10.1109/TVCG.2007.70405. (IEEE Transactions)

[5] F. Farooq, R. Bolle,T. Jea, and N. Ratha,, (2007), "Anonymous and revocable fingerprint recognition," in [Proc. IEEE Computer Vision and Pattern Recognition]. H. Goto, Y. Hasegawa, and M. Tanaka, "Efficient Scheduling Focusing on the Duality of MPL Representation," Proc. IEEE Symp. Computational Intelligence in Scheduling (SCIS '07), pp. 57-64, Apr. 2007, doi:10.1109/SCIS.2007.367670. (Conference proceedings)

[6] A. Vetro and N. Memon, (2007), "Biometric system security," in Proceedings of the 2nd International Conference on Biometrics, Seoul, South Korea.

[7] N. K. Ratha, J. H. Connell, and R. M. Bolle, (2001), "Enhancing security and privacy in biometrics-based authentication systems," IBM Systems Journal, vol. 40.

[8] A. K. Jain, A. Ross, and U. Uludag, (2005), "Biometric template security: challenges and solutions," in Proceedings of the European Signal Processing Conference (EUSIPCO '05), Antalya, Turkey.R.J. Vidmar, "On the Use of Atmospheric Plasmas as Electromagnetic Reflectors," IEEE Trans. Plasma Science, vol. 21, no. 3, pp. 876-880, available at http://www.halcyon.com/pub/journals/21ps03-vidmar, Aug. 1992. (URL for Transaction, journal, or magzine)

[9] K. Kamal, A.Ghany, A.Hesham. A. E.Hassanien, I. Ghali., (2012), "A Hybrid approach for biometric template security". IEEE/ACM International Conference on Advances in Social Networks Analysis and Mining.

[10] P. Campisi, (2013), "Security and privacy in biometrics: towards a holistic approach", Security and Privacy in Biometrics, pp. 1–23: London, Springer.

[11] A. Ross, J. Shah, and A. K. Jain, (2007), "From template to image: reconstructing fingerprints from minutiae points," IEEE Transactions on Pattern Analysis and Machine Intelligence, vol. 29.

[12] N.Radha and S.Karthikeyan, (2011), " An evaluation of fingerprint security using Noninvertible Biohash" International Journal of Network Security & its Applications (INSA).

[13] A. Adler, (2005), "Vulnerabilities in biometric encryption systems," in Proceedings of the 5th International Conference on Audio- and Video-Based Biometric Person Authentication (AVBPA, 05), Hilton Rye Town, NY, USA.

[14] S. Krawczyk and A. k. Jain, (2007),"Securing Electronic Medical Records using Biometric Authentication ".