ISSN No. 0976-5697

Volume 7, No. 3, May-June 2016

International Journal of Advanced Research in Computer Science

RESEARCH PAPER

Available Online at www.ijarcs.info

Secure Biometric Template Protection Approach using Chaotic Maps

Uma Verma
Research Scholar (M. Tech)
Department of Computer Science and Applications
Kurukshetra University, Kurukshetra, INDIA

Dr. Chander Kant
Assistant Professor
Department of Computer Science and Applications
Kurukshetra University, Kurukshetra, INDIA

Abstract: Dependable user identity administration is most needed these days, with the intention to achieve the heightened security. Finding the exact identity of any person is critical for any biometric system. However, due to the persistent connection between users and their traits(biometric), the disclosure of existing enrolled user's information to attackers can totally compromise the security and privacy of any biometric system. One possible way to tackle the limits of the biometric system approach is to encrypted the template and store decryption key using a smart card or a secure chip, which has to be in the ownership of the designated user. This process is call biometric template protection. To improve template security in biometrics authentication using efficient data encryption technology like watermarking, steganography and chaotic map etc. chaotic map is a technique of bit by bit encryption into the host image to generate authentic image for storing in database instead of original host image. This paper proposes ways to produce protected biometric templates employing present technologies and cancellable biometrics**.**

Keywords: biometric, biometric templates, cancelable biometrics, encryption.

I. INTRODUCTION

Biometrics provides automatic identification or verification of individuality established on behavioral or physical properties". Biometrics validates originality by computing exceptional individual characteristics. The most main spans of biometrics involve fingerprints, eyes and facial characteristics, hand geometry, retina, voice and touch. At the highest level, the wreck modes of a biometric arrangement can be categorized into two classes: intrinsic failure and failure due to an antagonist attack. [1]

A. *Intrinsic failure*

Intrinsic disruption is the protection fault due to an incorrect decision made by the biometric system. A biometric verification arrangement can make two kinds of errors in decision making, namely, false acceptance and false reject. An authentic user could be dishonestly declined by the biometric arrangement due to the huge contrasts in the user's stored template and query biometric feature sets. These intruder variations could be due to incorrect contact by the user alongside the biometric (e.g., adjustments in pose and expression in a face image) or due to the sound gave at the sensor (e.g., residual prints left on a fingerprint sensor). [2] [3]

B. *Adversary attacks*

An adversary's efforts might take the form of attempting to discover secret data, corrupting some of the data in the system. We categorize the antagonist aggressions into three main classes: management attack, non-secure groundwork, and biometric exactness.

1) *Administration attack*

This attack, additionally recognized as the associate attack, mentions to all vulnerabilities gave due to improper management of the biometric system. These contain the integrity of the enrollment procedure amid the antagonist and the arrangement administrator or a legitimate user, and mistreatment of exclusion processing procedures.[4]

a. *Non-secure infrastructure*

The groundwork of a biometric arrangement consists of hardware, multimedia, and the contact channels amid the assorted modules.

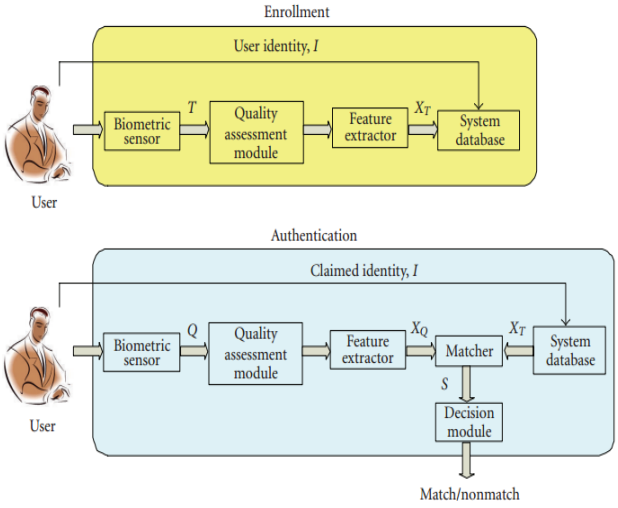

Figure 1. Enrollment and Recognition stage in a biometric system.

b. *Hardware infrastructure*

The groundwork of a biometric arrangement consists of hardware, multimedia, and the contact channels amid the assorted modules. [5]

c. *Biometic adversary attack*

It is probable for an antagonist to covertly buy the biometric characteristics of a genuine user (e.g., fingerprint impressions lifted from a surface) and use them to craft physical artifacts (gummy fingers) of the biometric trait. [6]

2) *Biometric exactness*

It is probable for an antagonist to covertly buy the biometric characteristics of a authenticate user and use them to craft physical artifacts (gummy fingers) of the biometric trait.

II. RELATED WORK

Kenta, Takahashi, and Shinji Hirata et. al. (2011) [7] In this paper, protecting biometric information is a critical issue in biometric systems, since physical characteristics such as fingerprints, irises, face and vein patterns, cannot be changed or revoked like passwords. To address this issue, an authentication scheme called cancelable biometrics has been studied, in which the biometric features are transformed by a kind of encryption or one-way function and matched without restoring the original features.

Patrick, Lacharme, Estelle Cherrier et. al. (2013) [8] In this paper, biometric recognition is more and more employed in authentication and access control of various applications. Biometric data are strongly linked with the user and do not allow revocability nor diversity, without an adapted post-processing. Cancelable biometrics, including the very popular algorithm BioHashing, is used to cope with the underlying privacy and security issues.

Anne Magaly, de Paula Canuto, et. al. (2014) [9] In this paper, the concept of cancellable biometrics has been introduced as a way to overcome privacy concerns surrounding the management of biometric data.. In this study, the authors specifically investigate the use of ensemble systems and cancellable transformations for the multi-biometric context, and the authors use as examples two different biometric modalities (fingerprint and handwritten signature) separately and in the multi-modal context (multi-biometric).

C., Divya, and E. Surya et. al. (2012) [10] In this paper, in many applications, Palm print data hiding can be viewed as a trade-off between capacity, robustness (against attacks), and embedding induced distortion. They derived a mathematical expression for the security of our algorithm, using which we show that the security can be increased independent of capacity, robustness, and embedding induced distortion

Tzuo-Yau, Fan, Bin-Chang Chieu et. al. (2012) [11] In this paper, a robust copyright scheme for image protection based on visual secret sharing (VSS) and Bose–Chaudhuri–Hocquenghem (BCH) code techniques is proposed. This scheme not only maintains the quality of a host image without the change of any pixel value but also generates a meaningful ownership share to improve the management of image copyright. In addition, no codebook is required to store, and the watermark size is independent of the host image.

Xi, Chen, Xiangwei Bai et. al. (2012) [12] In this paper, we propose a novel finger vein based cancelable biometric key generation scheme. Three main steps are involved in the proposed scheme:

(i) Finger vein feature is extracted by maximum margin locality preserving projection (MMLPP);
(ii) Chaotic random projection was used for cancelable biometric template generation;
(iii) Construct a fuzzy commitment based key generation system. Experiment and analysis show our proposed scheme is a secure and efficient key generation scheme.

III. PROPOSED WORK

Numerous template protection methods have been counseled in the works alongside the goal of safeguarding non-invariability, revocability, and non- linkability lacking compromising on the credit performance. In the counseled way a non-invertible or one-way key purpose is requested to the biometric template (x). As the transformed template is stored in the database. Across authentication, the key makes it probable to apply alike makeover purpose to the biometric query and reconstruct Template that is contrasted to the stored Template. Thus, the biometric matching sizes locale undeviatingly in the transformed domain. This can form a cancelable biometrics and robust key are a little of the well-known schemes that can be gathered below feature transformation. Methods that can produce non-invertible templates lacking the demand for each secrets are from time to time denoted to as keyless biometric template protection schemes. Such schemes can be functional in requests whereas it could not be feasible or desirable to permit user-specific supplementary data.

In biometric cryptosystems, the auxiliary data is frequently denoted to as a safe guard key, that is a normally derived employing encryption technique. As the safeguard key in itself is insufficient to reconstruct the early template, it does encompass adequate data to recoup the early template in the attendance of one more biometric example that closely matches alongside the enrollment sample.

The safeguard draft is whichever obtained as the syndrome of an error correction program requested to the biometric template or by attaching the biometric template alongside a encryption scheme that is indexed by a cryptographic key. A cryptographic hash of the early template or the key utilized to index the error correction. Matching in a biometric cryptosystem is gave indirectly by endeavoring to recoup the early template (x) employing the safeguard key. The strength of biometric cryptosystems is the potential of bounds on the data leaked by the safeguard draft if we accept that the biometric data allocation is recognized.

The strength of biometric cryptosystems is the potential of bounds on the data leaked by the safeguard draft if we accept that the biometric data allocation is recognized.

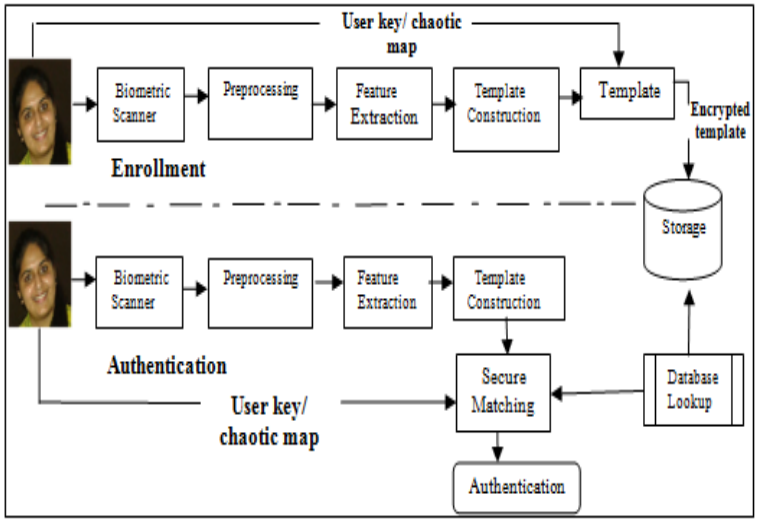

Figure 2. Proposed Biometric Template Protection Approach

A. Algorithm

Input: Images I and keys K

1*) Steps for Enrollment*

For j = 1 to Subjects
Step 1: Read biometric image I, from scanner.
Step 2 : Preprocess image to remove any abnormalities, noise and perform color correction, Rotation and displacement alignment is also performed here.
Step3 :From preprocessed I_p image necessary features are extracted (e.g., minutiae) which generates the fingerprint template I_{tj}.
Step4 : From extracted region I_r , template I_{tj} are constructed by applying encryption Algorithm RSA(I_{tj}).
Step5: Then encrypted Template I_{enc} stored into database.

2*) Steps for Authentication*

Input: Image I and key K
Step 1: Read biometric image I, from scanner.
Step 2 : Preprocess image to remove any abnormalities, noise and perform color correction, Rotation and displacement alignment is also performed here.
Step3 :From preprocessed I_p image necessary features are extracted (e.g., minutiae) which generates the fingerprint template I_{tj}.
Step4 :From extracted region I_r , template I_{tj} are constructed by applying encryption Algorithm RSA(I_{tj}).
Step5: Then encrypted Template I_{enc} stored inta database.
Step 6: Try MATCH with Stored Encrypted Template I_{enc} using Secure Matching Algorithm. if match successfully done then :

user are authorized.

Else

User are unauthorized

B. Template Protection using Chaotic MAPs

For the template protection stage, we introduce the chaotic Chebyshev map to diffusion each pixel of the original biometric image. Chebyshev map can be defined as follows:

$$x_{n+1} = \cos(\beta \arccos(x_n)), x_n \in [-1, 1]$$

where β and initial value x_0 are the secret key, the system is chaotic with $\beta \geq 2$.

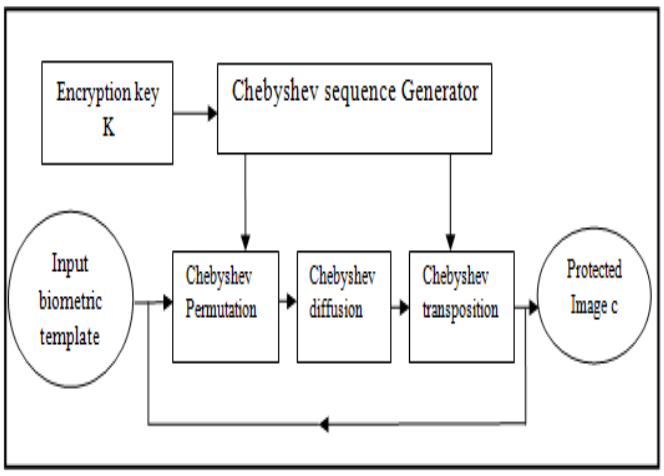

Figure 3. Chaotic Map scheme

However, the range of β should be restricted to a particular interval of 2π to prevent Chebyshev map from producing periodic orbits. The detailed diffusion process is stated as follows:

Step 1

Iterate map for s+t times and discard the first s bits to avoid the harmful effect of map. Then, get a chaotic sequence X = $\{x_1, x_2, \ldots, x_t\}$, where s and t are constant.

Step 2

Get a new chaotic sequence: Y = $\{y_1, y_2, \ldots, y_t\}$ in ascending order by y = sort(x), where Y is a permutation of X.

Step 3

Transform each pixel value G(x, y) into 8 bits binary sequence B = $\{b_1, b_2, \ldots, b_8\}$, then, Let T = $\{t_1, t_2, \ldots, t_8\}$ denote the permutation vector of X, such that Y=X(T). Then rearrange each bit of the binary sequence according to T, that is, move the first bit to t_1th position, the second bit to t_2th position,…, the last bit to t_8th position. Therefore, we get a new binary sequence B' = $\{b'_1, b'_2 \ldots b'_8\}$.

Step 4

Repeat step 3 M × N times, where M and N is the length and width of biometric image, respectively. It should be noted that in each permutation, X, Y generated in Step 2 are different. In decryption process, same permutation vector is generated using the same keys. Then the original biometric can be obtained by moving back the positions according to the permutation vector. we can set $\beta = \pi$, $x_0 = 0.123456$, s= 500, t= 9500, M= N = 512. The result of applying the above diffusion algorithm with these parameters on standard test biometric image.

IV. CONCLUSION & FUTURE SCOPE

Biometric arrangements themselves are vulnerable to a number of attacks. In this paper, we have summarized assorted aspects of biometric arrangement protection and debated methods to counter these threats. Finally, specific implementations of these ways on a public fingerprint database were given to illuminate the subjects encompassed in requesting template security. In exercise, an antagonist could be able to exploit the non-uniform nature of biometric features to raise an attack that could need considerably less endeavors to compromise the arrangement security.

As we have pointed out a little of the vulnerabilities in specific schemes such as furry vault, a rigorous scrutiny of the cryptographic strength of the template protection schemes comparable to those obtainable in the cryptanalysis works has not been grasped out till date. A solitary template protection way could not be adequate to encounter all the request requirements. Hence, hybrid schemes that make use of the gains of the disparate template protection ways have to be developed. For instance, a scheme that secures a “salted” template employing a biometric cryptosystem could have the gains of both salting (which provides elevated diversity and revocability) and biometric cryptosystem (which provides elevated security) approaches.

Finally, alongside the producing attention in multibiometric and multifactor authentication arrangements,

schemes that simultaneously safeguard multibiometric templates and several authentication factors (biometrics, passwords, etc.) demand to be industrialized.

V. REFERENCES

[1] Arun, Ross, and Asem Othman. "Visual cryptography for biometric privacy." IEEE transactions on information forensics and security 6, no. 1 (2011): 70-81.

[2] Sowmya, Suryadevara, Rohaila Naaz, Shuchita Kapoor, and Anand Sharma. "Visual cryptography improvises the security of tongue as a biometric in banking system." In Computer and Communication Technology (ICCCT), 2011 2nd International Conference on, pp. 412-415. IEEE, 2011.

[3] Hua-hong, Zhu, Qian-hua He, and Yan-xiong Li. "A two-step hybrid approach for voiceprint-biometric template protection." In Machine Learning and Cybernetics (ICMLC), 2012 International Conference on, vol. 2, pp. 560-565. IEEE, 2012.

[4] R., Sinduja, R. D. Sathiya, and V. Vaithiyanathan. "Sheltered iris attestation by means of visual cryptography (sia-vc)." In Advances in Engineering, Science and Management (ICAESM), 2012 International Conference on, pp. 650-655. IEEE, 2012.

[5] Koen, Simoens, Bian Yang, Xuebing Zhou, Filipe Beato, Christoph Busch, Elaine M. Newton, and Bart Preneel. "Criteria towards metrics for benchmarking template protection algorithms." In Biometrics (ICB), 2012 5th IAPR International Conference on, pp. 498-505. IEEE, 2012.

[6] Hengjian, Li, and Lianhai Wang. "Chaos-based cancelable palmprint authentication system." Procedia Engineering 29 (2012): 1239-1245.

[7] Kenta, Takahashi, and Shinji Hirata. "Parameter management schemes for cancelable biometrics." In Computational Intelligence in Biometrics and Identity Management (CIBIM), 2011 IEEE Workshop on, pp. 145-151. IEEE, 2011.

[8] Patrick, Lacharme, Estelle Cherrier, and Christophe Rosenberger. "Preimage attack on biohashing." In Security and Cryptography (SECRYPT), 2013 International Conference on, pp. 1-8. IEEE, 2013.

[9] Anne Magaly, de Paula Canuto, Michael C. Fairhurst, and Fernando Pintro. "Ensemble systems and cancellable transformations for multibiometric-based identification." Biometrics, IET 3, no. 1 (2014): 29-40.

[10] Divya, and E. Surya. "Visual cryptography using palm print based on dct algorithm." International Journal of Emerging Technology and Advanced Engineering 2, no. 12 (2012): 2250-2459.

[11] Tzuo-Yau, Fan, Bin-Chang Chieu, and Her-Chang Chao. "Robust copyright-protection scheme based on visual secret sharing and Bose–Chaudhuri–Hocquenghem code techniques." Journal of Electronic Imaging 21, no. 4 (2012): 043018-043018.

[12] Xi, Chen, Xiangwei Bai, Xie Tao, and Xiaolu Pan. "Chaotic random projection for cancelable biometric key generation." In Intelligent Science and Intelligent Data Engineering, pp. 605-612. Springer Berlin Heidelberg, 2012.