A new cancelable iris Templates protection using Majority vote and TawHas

Research Article

Tawheed Hassan **Alabed**[1*], Faisal Mohammed **Abdallah**[2], Nazim Osman **Bushara**[1], Hassan Abdalla **Ahmed Ali**[1]

1.Department of Computer Science, University of shendi, Shendi, Sudan
2. Department of Computer Science, university of Karary, Khartoum, Sudan

Abstract

With the increasing applied of biometric systems in various applications increased needs a reliable solution to the problem of user authentication. The Identity privacy, unlinkability users at different applications, the integrity and revocability are main requirement to designing biometric system to achieve privacy and security at biometric system. due intra users variability at biometric systems authentication create a challenge of protection the biometric template due that variability in the acquired biometric traits and disclosed sensitive information for bad attacker. This paper proposed a new iris Biometric Templates protection technique using a new TawHas cancelable unique code. it has 0.478 FAR and 0.236 FRR and TSR 99. 8%. Equal Error Rate (EER) 0.242.

Keywords:
Biometric; security; privacy; cancelable; cryptosystem.

1. Introduction

Biometric is composed of two wards bio and metric which means “life” and “to measure” [1]Every biometric system mainly consists of four modules passed two phases proposed at [2]: enrollment and verification are two phases. the modules are registering at the enrollment phase into biometric database system. Second module is feature extraction processes which generate a template from input sample to store it in a database or a smartcard issued to the individual. last module is matching module compares the input with the template to perform identity verification. these physical human biometric and logical known as biometric trait [3] which are differ from one person to another and these traits defined as a unique identification biometric trait [4]Biometric identification taxonomies as physical or behavioral traits like iris, ear, face, hand, finger, and gaits. Also, biometric traits characteristic classified to procedural, technical and inherent [5]. The inherent biometric characteristics proposed at [6] have four characteristics classified as collectability, universality, permanence and universality. Also, the accuracy of the extract biometric feature and matching biometrics are technical characteristics related to the different technical implementations and there are many models using to extract features like Daugman model for iris template. at designing a biometric system, the manner in which the biometric is calculated should also not influence its performance [5]. Adding the procedural characteristics to Lessing circumvention on multi-modal biometric system at many applications [7]. Still many challenges make a failure at biometric system like noisy data caused by defected sensors and defective physical and unfavorable conditions and all that causes incorrectly matched or rejected. in addition, Security and privacy main challenge to protect any biometric system to securing accessing to information at applications used biometric recognition authentication. There are many requirement to achieve this security which are Confidentiality, Renewability, Integrity and revocability. That increasing needs to protection the biometric recognition system. Attacks against stored biometric data on the database. Illegitimate intrusion actions on database biometric systems are classified to: 1) replacing template on database. 2) Changing DB template feature 3) Removed DB template. There are many attacking types which attack the biometric template database in spite of applied different biometric template protection approaches. These attacks are: substitution attack, brute force attack, hill climbing attack, recording multiplicity, correlation, collision attack, and malicious outside and cheating. These attacking make a false reject or false accept or copy features under function creep hacking approach or crossing database.

The rest of the paper organized as follows: Section 2 presents cancelable. In Sections 3 related work and in 4 section new cancelable approaches for iris template protection technique. Lastly concludes the paper at 5.

2. Cancelable Biometrics TEMPLATE PROTECTION APPROACH

In verification biometric system phase, the matching procedure performed using the protected template that to against any attacking. So, if same template is using on the different application, it will need to create different protected template to same trait on different application. Also, a compromised template need to cancelable or renewable template. Cancelable biometric protection introduced in [8], to make different biometric template for different application. It consists of repeatable distortion, an intentional of a biometric trait based on transformation biometric. The implementation of cancelable approach by used a function to generate the protected templates and key is used as a function parameter [9] and the generated template can be cancelled like secret passwords [10]. The main aims of this approach are protect user-specific sensitive data by both intentional and systematic distortion of the extracted biometric features [11] [12] There are two approaches of cancelable non-invertible and salting approaches proposed on [9], which are transform biometric template features to achieve main requirement of security like confidently, revocability and renewability [8].

Main operation on salting cancelable biometric are secured biometric template by transformed function. it has parameters hash value of key s and pseudorandom p, k =H(p +s) [13]. It is difficult for adversary attack to guess key. However, template not longer secure if key compromised. At non-invertible using one way transform function is hard for attacking template to reconstruct original template. However, difficult to designing one way transformation functions.

Table 1 present different point of strings, weakness and operation of salting and non-invertible approaches.

Table 1. Cancelable approach: Types, operation, strength and weakness.

Approach	Operation	Strength	Weakness
Salting cancelable	Biometric features secured by transformed function with parameters hash value of key s and pseudorandom p k =H(p +s)	Difficult to guess key for adversary attack.	Template not longer secure if key compromised.
Non-invertible	Using non invertible transformation function	Hard to reconstruct original template.	Difficult to design one way transformation function

3. Related work

Many technique take cancelable concept to implement a protection iris technique such as Bio Encoding salting methods for iris in [14] which implemented on CASIA-V1 iris database evaluated as 1.3 EER. The challenge is save key because if key is compromised, system opens for attacker. In addition to that, the non-invertible cancelable approach implement for iris in [15] by applied Block remapping images warping on CASIA-V3 evaluated as 0.02 EER. On [16] too implemented non-invertible approach for iris by implemented Rectangular and polar block remapping, mesh wrapping method on CASIA-V3 evaluated as 2.0% EER. At [17] adaptive bloom filter applied on CASIA-V3 too, which evaluated as 1.14 EER. Mixing iris codes adaptive bloom filter evaluated as 0.5% EER. Difficulties appeared in designing a transformation functions that satisfy both the discriminability and non-invertibility conditions simultaneously. Moreover, transformation function depends on biometric features to be used in specific applications. But False Accept Attack maybe happen if attacker having appropriate knowledge of transformation algorithm and parameters uses some publicly available benchmark databases to masquerade the system. the attacker subjects the biometric samples of a public database to transformation algorithm using known parameters in order to generate a wide set of transformed templates. Also, Attacks via Record Multiplicity the attacker gets access to more than one copy of transformed templates obtained from the same instance and attempts to link that to find original template. At brute Force Attack secret information about the original template or the transformation keys isn't necessary because tries all possible permutations and combinations to generate a transformed template and make a successful attempt.

4. New Cancelable Technique using Tawhas linear transformation algorithm

It considered as a new technique used cancelable concept to protect iris template against threats. It consists of four main steps. The first step is generating iris template using Daugman model. The second step is preparation before implement TH. Step three is the TawHas new cancelable approach. Here the iris pattern will be secured as a new size. Step four is the matching phase, where two iris codes will be compared and a similarity score is computed. These steps are shown schematically in Figure 2.

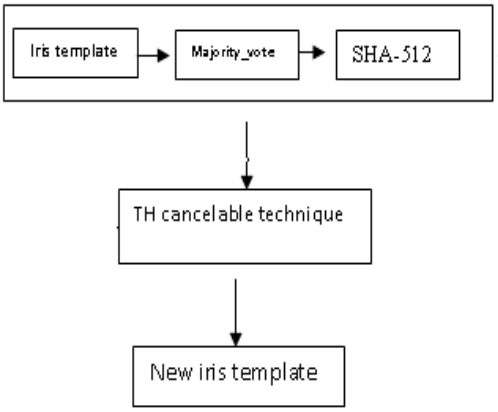


Figure1: TawHas cancelable iris template protection technique.

4.1 Iris template generation

Depending on Daugman model to generate iris template many steps constructed this model [18] begin with segmentation, normalization and encoding features which shown on figure 2 to generate 9600 bit. At this paper we implement model on cassia v1 [19] which contains 756 grayscale eye images with 108 unique eyes or classes and 7 different images of each unique eye.

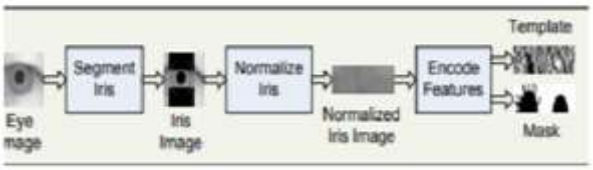


Figure2 Iris template generation process.

4.2 First Preparing encoding phase for TawHas cancelable technique

At this phase two steps implement to give input value to TawHas technique. we implement majority vote technique on iris template to construct a unique iris code [20]. Majority vote is function used to find a prototype code or a representative iris feature code [21] by counting the elements of a 1D array and outputs the value with the most occurrences which produced a unique code. The unique 1D code passed to 512 hashes [22].

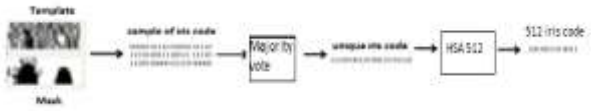


Figure3: Majority vote and HSA512 first preparing encoding step.

4.3 Iris template protection using TawHas technique

To illustrate protection for biometric, we provide TawHas new cancellable iris template protection shown on figure.5

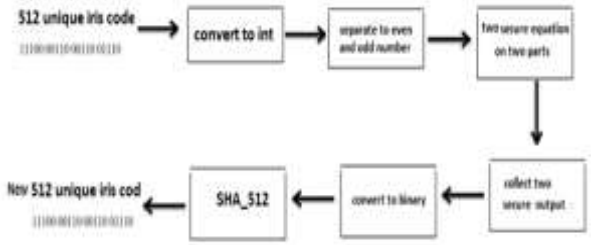


Figure4: Building TawHas cancellable iris template

The alignment challenge on salting or cancellable, using mathematic nature of numbers known here as TawHas cancellable technique. The TawHas cancellable technique was new security algorithm which has input and output. The 512 hash consider as input to TawHas to separate the unique hash iris using two different equations on the two parts by get an even part which known here as first part and odd part known also as a second part. The securing executed by implement two different security equations, each one for one part and then collecting two transforms parts by adding two outputs. After that, compute hashing-512 to get a secure iris code.

4.4 Matching

The matching procedure is evaluation the similarity of two iris representations. At this paper we implement Hamming distance [23]. At this paper we construct distance score matrix between training sample and testing for exactly person.

With the CASIA V1' data set 1296 unique inter-class comparisons are possible. In other words 1296 Hamming distance values are calculated. Also, construct distance score matrix between training sample and testing for different person. With the CASIA V1' data set 756 unique intra-class comparisons are possible. In other words 756 Hamming distance values are calculated.

4.5. EXPERIMENTAL ANALYSIS

The performance of proposed TawHas technique has been tested on CASIA V1 iris datasets. Performance comparison is done using FAR (false acceptance rate), FRR (false rejection rate) and computed EER(equal error rate). According to statistical theory, the mean Hamming distance for comparisons between inter-class iris templates will be 0.5. This is because, if truly independent, the bits in each template can be thought of as being randomly set, so there is a 50% chance of being set to 0 and a 50% chance of being set to 1. Therefore, half of the bits will agree between two templates, and half will disagree, resulting in a Hamming distance of 0.5 [24]. Due to this, the mean Hamming distance for inter-class template comparisons will be slightly lower than 0.5, since the lowest Hamming distance out of several comparisons between shifted templates is taken. As the number of shifts increases, the mean Hamming distance for inter-class comparisons will decrease accordingly. After that, Compute false accepts rate and compute false reject rate. In addition, we decided to take 4 samples in class for training and 3 samples for testing. Suitable threshold value is 0.4 because it has 0.478 FAR and 0.236 FRR and TSR 99. 8%. Equal Error Rate (EER) 0.242.

The output from my iris template protection security technique is 512 bit which is from SHA512. This hash function is one way known as message summary or compression function takes the enter variable length and converts it into a binary sequence of a fixed length. If we want to analyze it , breaking the hash algorithm is equivalent to finding a collision in the hash algorithm. We just need to find an output of the hash function that is equal to the hash of a valid password (thus "collision"). Finding a collision using a birthday attack takes O(2^(n/2)) time, where n is the output length of the hash function in bits. Also, SHA-2 has an output size of 512 bits, so finding a collision would take O(2^256) time. Given there are no clever attacks on the algorithm itself. The 2^256 actually computations which would take

2^240 * 2^-2 = 2^238 ~ 10^72s ~ 3,17 * 10^64 years Even calling this millions of years is improbably.

5. Conclusion

Biometric template protection using cancelable approach phase a challenge of designing one way function that hard for attacking database. The attacking Illegitimate intrusion actions on database biometric systems are classified to: 1) replacing template on database. 2) Changing DB template feature 3) Removed DB template. There are many attacking types which attack the biometric template are: substitution attack, brute force attack, hill climbing attack, recording multiplicity, correlation, collision attack. This new cancelable technique used two linear transformation equations to achieved one way transformation function. Also, it against recording multiplicity and correlation attack hard and take long time for hill climbing and brute force attack and it hard to reconstruct original template. To achieved It applied on CASIA v1 and achieved security requirement.

Reference

1. Ashok, J., V. Shivashankar, and P. Mudiraj, *An overview of biometrics.* International Journal on Computer Science and Engineering, 2010. **2**(7): p. 2402-2408.
2. Ambalakat, P. *Security of biometric authentication systems*. in *21st Computer Science Seminar*. 2005. Citeseer.
3. Jain, A.K., A. Ross, and S. Prabhakar, *An introduction to biometric recognition.* IEEE Transactions on circuits and systems for video technology, 2004. **14**(1): p. 4-20.
4. Le, C. and R. Jain, *A survey of biometrics security systems.* EEUU. Washington University in St. Louis, 2009.
5. van de Haar, H., D. van Greunen, and D. Pottas. *The characteristics of a biometric*. in *2013 Information Security for South Africa*. 2013. IEEE.
6. Gokulkumari, G. and A. Lakshmi, *Study of effects and perceptual analysis in implementing biometric authentication.* European Journal of Scientific Research, 2011. **61**(2): p. 242-254.
7. Manivannan, S. and E. Padma, *Comparative and analysis of biometric systems.* International Journal on Computer Science and Engineering, 2011. **3**(5): p. 2156-2162.
8. Ratha, N.K., J.H. Connell, and R.M. Bolle, *Enhancing security and privacy in biometrics-based authentication systems.* IBM systems Journal, 2001. **40**(3): p. 614-634.

9. Patel, V.M., N.K. Ratha, and R. Chellappa, *Cancelable biometrics: A review.* IEEE Signal Processing Magazine, 2015. **32**(5): p. 54-65.
10. Kaur, H. and P. Khanna, *Biometric template protection using cancelable biometrics and visual cryptography techniques.* Multimedia Tools and Applications, 2016. **75**(23): p. 16333-16361.
11. Rathgeb, C. and A. Uhl, *A survey on biometric cryptosystems and cancelable biometrics.* EURASIP journal on information security, 2011. **2011**(1): p. 1-25.
12. Belguechi, R., et al., *An overview on privacy preserving biometrics.* Recent Application in Biometrics, 2011: p. 65-84.
13. Ratha, N.K., et al., *Generating cancelable fingerprint templates.* IEEE Transactions on pattern analysis and machine intelligence, 2007. **29**(4): p. 561-572.
14. Ouda, O., N. Tsumura, and T. Nakaguchi, *Bioencoding: A reliable tokenless cancelable biometrics scheme for protecting iriscodes.* IEICE TRANSACTIONS on Information and Systems, 2010. **93**(7): p. 1878-1888.
15. Hämmerle-Uhl, J., E. Pschernig, and A. Uhl. *Cancelable iris biometrics using block re-mapping and image warping*. in *International conference on information security*. 2009. Springer.
16. Färberböck, P., et al. *Transforming rectangular and polar iris images to enable cancelable biometrics*. in *International Conference Image Analysis and Recognition*. 2010. Springer.
17. Rathgeb, C., et al., *On application of bloom filters to iris biometrics.* IET Biometrics, 2014. **3**(4): p. 207-218.
18. J. Daugman, *How iris recognition works,.* IEEE Trans. Circuits Syst. Video Technol.
, 2004. **14**
(1).
19. Sciences, C.A.o., *CASIA Iris Image Database (version 1.0)* http://www.sinobiometrics.com: Institute of Automation (IA).
20. Seetharaman, K.a.R.R., *LDPC and SHA Based Iris Recognition for Smart Card Security.* . Proceedings of International Conference on Advances in Computing. Springer., 2013. .
21. VIRIRI, S.T., Jules. , *Iris pattern recognition based on cumulative sums and majority vote methods.* International Journal of Advanced Robotic Systems,, 2017, . **14.3** (1729881417703931.).
22. N.I.o.S.a., *Secure hash standard.* . Federal Information Processing Standards Publications FIPS PUB. , 2001. . **180**(2).
23. RAI, H.Y., Anamika., *Iris recognition using combined support vector machine and Hamming distance approach.* Expert systems with applications., 2014. **41**(2): p. 588-593..
24. Masek, L., *Recognition of human iris patterns for biometric identification.* . 2003, University of Western Australia.