SIRIS – Secure IRIS Authentication System

Priyanka Loya
Student of Master of Technology
Department of Computer Science & Engineering
National Institute of Technology Karnataka
Mobile no.:7204857117
priyanka.loya3@gmail.com

Alwyn Roshan Pais
Assistant Professor
Department of Computer Science & Engineering
National Institute of Technology Karnataka
Telephone number:(0824)2474000 extn:3407
alwyn@nitk.ac.in

ABSTRACT
As the password based authentication systems are not able to meet the performance because they can be stolen, forgotten, cracked, sniffed and tampered with. Lateral thinking to this problem evolved the use of biometrics to authenticate the person uniquely. Since, the templates are stored in a centralized database there is possibility of tampering of templates. The objective of this paper is to combine cryptography with biometrics by apply minor changes to the iris templates to transform them and store in a database, and hence forth even the system is compromised, the template is safe from the wrong hands thus to improve the security of the system in a network. For determining the performance of the system digitized grayscale eye images from CASIA 1.0[3] iris image set is used. This authentication system consists of an automatic recognition of iris template using the password provided by the user. The system performance is tested using different key sizes 128 bit, 256 bit and 512 bit keys. We used Hamming distance for classification of iris templates, and templates are accepted to match if the statistical independence was failed. Experimental results showed that the system performed with perfect recognition on a set of 756 images and resulted in an accuracy rate of 96%.

Categories and Subject Descriptors
E.3 [Data Encryption]

C.2.0 [Security and Protection]

H.2.7 [Security, Integrity, Protection]

1. INTRODUCTION
In the early days, authentication is provided by password based authentication systems, or one- time password generating systems. Due to tremendous enhancement in the architecture of the systems, the processing power and the storage capacity of the systems have enormously increased. So, a strong mechanism to improve the security for data has to be introduced. Smart cards, intelligent data storage devices, are becoming a method to perform identification and authentication for the users.

The inherent problem with smart card/ device is the possibility of loss or theft of the smart card. This loss or theft can make an unauthorized person use the resources and therefore it is not considered as a secure mechanism to authentication. The problems with password based authentication can be solved by Biometrics which is a promising area in this regard.

SIN'12, October 25-27, 2012, Jaipur, Rajastan, India

Biometrics is derived from the Greek words "bios" and "metrics", which means "life" and "measurement" respectively. Biometric technologies are, hence, technologies developed to use statistical analysis of an individual's biological traits to determine his identity. The objective of all biometric recognition systems is to automate the authentication process, which would bring greater security, efficiency, and convenience to our lives. Biometric traits suitable for automatic recognition systems are classified into two categories (1) anatomical (2) behavioral. Anatomical biometrics includes fingerprints, iris prints, facial features, etc., which are inherent physical characteristics of an individual, while behavioral biometrics includes gait, signature, speech patterns, etc., which are usually characteristics acquired naturally during an individual's life time, and Esoteric biometrics includes facial thermographs, DNA, odour, palm vein, etc, which are presence of life in the individual. Anatomical or behavioral or esoteric traits that qualify for biometric systems are composed of seven characteristics as listed in the below Table 1:

Table 1: Biometrics Characteristics

Characteristic	Description
Universality	does everybody has it,
Uniqueness	The trait should be unique and can distinguish between users
Permanence	is this trait stable over a long time,
measurability	can this trait be quantitatively measured for identification,
performance	how accurate and fast can identification be performed
acceptability	is it acceptable by the public to be used for everyday access,
circumvention	how easy is it to "fool" the system.

The popularity of use of these biometric traits according to their seven characteristics discussed in Table 2.

The primary motivation for this paper is to develop secure template database in iris based biometric recognition systems, so as to ensure the revocability, privacy and security of the templates while maintaining the performance of already existing iris-based authentication systems. The work in this paper focuses on the template security of iris recognition systems that use binary Iris Codes for authentication. We explore how security can be incorporated into iris based biometric authentication systems. We develop an algorithm for iris template security and test this algorithm using varying key sizes (128, 256, 512-bit) on same iris database. And the system is tested for the four main objectives

revocability, privacy, security without compromising the performance of the iris based biometric authentication system.

The challenges in developing such a mechanism for securing iris templates lies in trying to maintain seperability between different users or inter-user variability, as well as, the fuzziness of the templates of the same user, or intra-user variability. Maintaining those two variability's while providing revocability, preventing cross-matching and not affecting the performance of the biometric authentication system is not an easy task. Another major challenge is developing algorithms that can be appended to existing biometric recognition systems using binary iris codes.

Table 2: Comparison of Various Biometric Traits

Biometric	Universality	Uniqueness	Permanence	Collectability	Performance	Acceptability	circumvention
Face	H	L	M	H	L	H	L
Fingerprint	M	H	H	M	H	M	H
Hand geometry	M	M	M	H	M	M	M
keystroke	L	L	L	M	L	M	M
Palm vein	M	M	M	M	M	M	H
Iris	H	H	H	M	H	L	H
Signature	L	L	L	H	L	H	L
DNA	H	H	H	L	H	L	L
Voice	M	L	L	M	L	H	L
Facial thermograph	H	H	L	M	H	H	H

This paper is organized into 5 sections:

Introduction, gives the motivation and challenges encountered in this project. Literature Survey, gives the survey on iris recognition systems, previous works and challenges posed to security and research work. Methodology, discusses how a solution to the problem is achieved and the architecture of the system is discussed. Results presents the various results obtained during the experimentation of our system and the last section draws the conclusion and suggestions for the future work.

2. LITERATURE SUREVEY

Besides the practical limitations and attacks on the biometric systems, they also face challenges which are not seen in traditional security systems, like lack of secrecy[16]. For example, finger prints are left on objects, faces are captured on cameras etc, and the non-replace ability i.e., unlike passwords, tokens, and smart cards biometric data cannot be "reissued" once compromised [1][2][6].

We now provide a detailed survey of research on iris recognition systems. The first iris recognition system was developed by Daugman which is accepted worldwide and is being used till today. Iris recognition is the process of recognizing a person by analyzing the random pattern of the iris[4][7]. In [13], the authors proposed a mechanism that corresponds to the recognition of iris for authentication, and the infrastructure needed to deploy iris based authentication, and its advantages. [12] discusses combining cryptography into biometrics, and the challenges encountered in that process. He discusses using AES encryption/decryption on the templates at the database level to provide the security to the database templates. In [14], the authors proposed a key binding algorithm for fingerprint matching system. The user finger print image is bind with the cryptography key during the time of enrollment and the key will be retrieved only if it is a successful authentication. Key generation from voice based biometric trait is also introduced by Fuzzy Commitment Scheme [8]. In [5], the authors also proposed a key regeneration scheme on iris biometric by combining Hadamard Code and Reed Solomon Error Correction Code (ECC) [15] but the system is not as secured because of its key length and limitation on the number of errors to be present in the generated template.

Hence, in order to improve the security and increase the total success rate of the system, we propose a secure iris template scheme that uses both user specific key as well as the iris biometric. In our approach, we use a non-invertible feature transform that not only provides revocability to the template but also preserves privacy, security for the individual. The basic template is generated using Libor Masek's [9] implementation.

3. METHODOLOGY

The proposed systems consists of two phases: (i) Enrollment Phase (ii) Verification phase. Enrollment process flowchart is shown in Figure 1 and the Verification process flowchart is shown in Figure 2.

Algorithm for Enrollment is described below.

Algorithm: Enrollment

Step 1: User enrolls to the system by providing his eye image which is any picture format available (.bmp/.jpeg/.png etc.).

Step 2: Along with the image, the user also specifies his password, which is used as a key in later section.

Step 3: Iris is located in the picture using segmentation process.

Step 4: Follows normalization and feature extraction process to generate the iris template and to produce the iris binary code which is of 2048-bit length.

Step 5: Once the password as well as the iris code is available, the actual process of the system will start.

Step 6: Using the user specific password, a key is generated which is of 512-bit length(128-bit, 256-bit lengths are also provided if necessary).

Step 7: Iris shuffling algorithm is carried out on the generated iris template using the key generated.

Step 8: The generated shuffled iris template is stored into the database.

Algorithm for Verification is described below.

Algorithm: Verification

Step 1: During verification process, a tested iris image is extracted using iris segmentation, normalization and feature extraction to obtain the iris binary code and the iris template of the testing iris image.

Step 2: Along with the image, the user also specifies his password, which is used as a key in later section.

Step 3: The generated iris template is shuffled based on the shuffling algorithm using the key generated from the password given by the user.

Step 4: Then the user is selected from the database whose username matches with the database.

Step 5: Both iris shuffled templates undergo the template matching process using Hamming distance as the metric.

Step 6: If the iris template is found to match, the user will be authenticated otherwise the system exits.

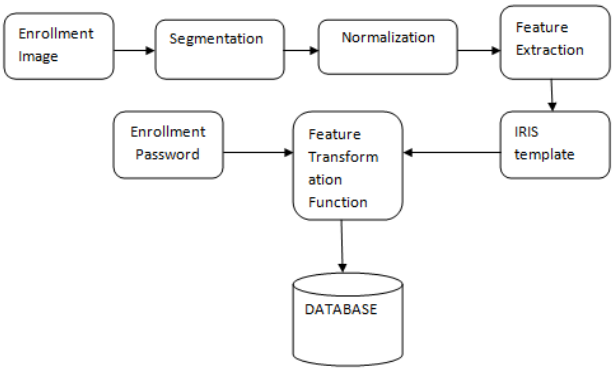

Figure 1: Enrollment Process

The feature transformation[10][11] used in our project is "Iris Shuffling" which is invertible in nature. This feature is used to introduce revocability to binary iris templates. We used varying key sizes to compare the algorithm we implemented and evaluated them using the same database and recognition algorithm as a benchmark for comparing the different key sizes. This enables to understand the nature of iris templates and how the bits in the iris templates are correlated. It also enables to compare the transforms in terms of how they affect the performance of the iris based recognition system.

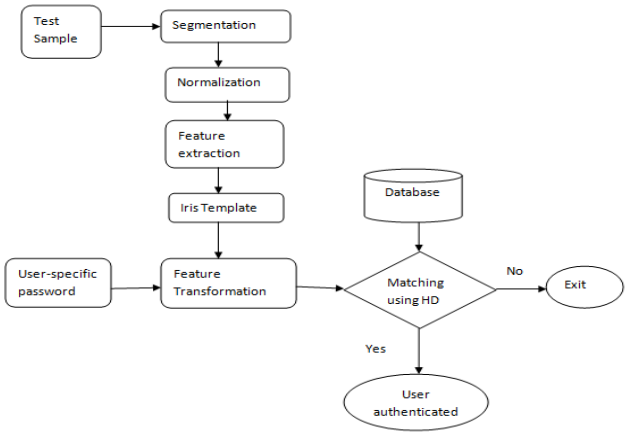

Figure 2: Verification Process

IRIS Shuffling Algorithm:

Step 1: The input is takes as a vector of 16 x 128 matrix.

Step 2: Converted into a one dimensional array.

Step 3: Divide the array into equal number of chunks based on the key size i.e., if the key is of K-bits length then the input array is divided into k number of equal parts.

Step 4: If the bit at a particular position r, is 0 then the corresponding block is shifted to the end of the array else it is unaltered.

Step 5: Return the transformed template to the database.

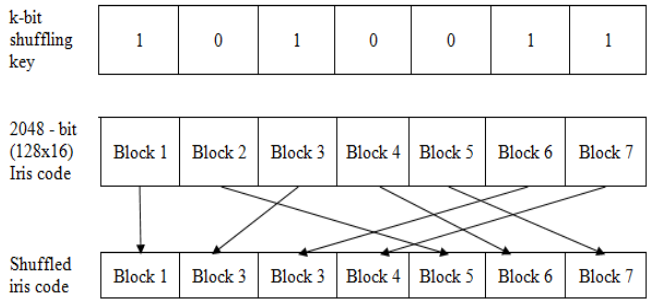

Figure 3: Iris Shuffling Algorithm

In our project, we provide two way authentication procedure, where the user has to give the password and according to the user-specific key, the iris template produced is shuffled according to it. And nowhere in the system, the "real" template is stored. The hash of the password given by the user is used as the key to transform the original template. We produce a hash of 512 bits using SHA-512. If the key is of 512 bits then the template is divided into 512 chunks. Depending on the bit at each position the template is shuffled i.e. if the bit at 1st position is "1" then the block is not shifted or left in place. Else if the bit at 1st position is "0" then the block is shifted to the end of the string.

The similar procedure is followed with keys of sizes 128-bit and 256-bit as well.

The transformation algorithm, used the first key to determine the shifts in each row, and the second key i.e., hash is used to randomly permutate the order of blocks. While matching, both the transformed template along with its mask is shifted 8 bits left-right to match perfectly in case if the templates produced are different due to noise present while taking the sample.

4. EXPERIMENTAL RESULTS

Performance test for any system is to find the stamina of the system at critical situations. It also serves to measure, scalability and reliability of the system under workload. We carried out different performance tests on the system we build which include frequency test, originality test, hamming distance for genuine and imposter templates to measure, False Acceptance Ratio (FAR), False Reject Ratio (FRR) of the system.

*4.1 Frequency Test:*The frequency test is used to test the randomness of a sequence of zeroes and ones. The test is based on the proportion of zeroes and ones. Specifically, it tests the closeness of the proportion of ones to 0.5. In the transformed IRIS Templates, we checked for the 0's and 1's frequencies which always resulted in a random number and the proportion varies from 45-53%.

*4.2 Originality Test:*All the transformed templates are matched with the original templates in order to find any similarities. Each transformed template of 512 bit key, 256 bit key, 128 bit key are mapped with the original template. The number of comparisons made are 17,14,608. And none of the template matched with the original one or the imposter templates. Hence we deduced that all the transformed templates are random and did not cause any discrepancy.

4.3 Hamming Distance Metric: Hamming distance for genuine templates as well as imposter templates is calculated and the graphs are presented in the report for the three different keys, 128-bit, 256-bit and 512 bit respectively. They produced equivalent graphs, but the cumulative graph suggests that, the count for each hamming distance unit is different for varying keys. So, from this we can deduce that the transformations produced with different keys are creating a change in hamming distance for the same template.

For genuine template testing we have used 2,42,676 samples for testing and for imposter template matching we have used 17,14,608 samples for testing.

The FAR, FRR, TSR of the system are calculated using the following formulae:

The False Acceptance Rate (FAR) measures the number of individual being wrongly identified as another individual.

$$FAR = \frac{Number\ of\ False\ Acceptance}{Number\ of\ Imposter\ Verification}$$

The False Rejection Rate (FRR) measure the number of enrolled individuals that cannot access the system, because the system do not identify the individual.

$$FRR = \frac{Number\ of\ False\ Reject}{Number\ of\ Enrollee}$$

Total Success Rate is obtained from FAR, FRR of the system, represents the security rate of the overall cryptosystem.

$$TSR = (1- \frac{No.of\ False\ Accept + No.of\ False\ Reject}{Total\ no.of\ accessess}) * 100\%$$

Table 3: Comparison with different Keys

Keys Sizes	128-bit key	256-bit key	512-bit key
FRR	0.094	0.081	0.060
FAR	0.1	0.0	0.0
TSR	91.1%	93.7%	96%

Table 3 shows the FAR, FRR, TSR for different key sizes 128-bit, 256-bit, 512-bit keys. The TSR for 512 bit key is 96% but the transformed template is too much distorted when compared to the original template. The below chart represents the hamming distance versus no. of templates using a 128- bit key.

5. CONCLUSION & FUTURE WORK

This thesis has explored a way of securing templates in iris based biometric authentication systems. Compromising the templates database poses two major risks: first, it enables attackers to create spoofs from the template, which in turn enables them to access other biometric based authentication systems using the same biometric trait. Second, compromised templates enable the cross-referencing between databases using the same trait without user's consent. All the results of implementation are testes using the same database CASIA V1. From the experimental results of the evaluation of the proposed system, the following results are drawn:

- Building an iris template security for already existing binary iris templates is possible and the results are promising.
- Using one way transformations are the secure way to store iris templates. Because it is difficult to generate non-invertible iris templates with uniqueness and inter-user variability.
- Overall performance of the system is acceptable. And the system also provides revocability of the trait used
- Combining cryptography with biometrics although increases the complexity of the system, it significantly increases the security, privacy of the iris templates while offering performance rates that are suitable for large scale high security applications, like airport checking and border crossing.

FUTURE WORK

A need for identity management and protection is growing drastically and becoming more complicated day by day. Biometric authentication offers a very promising method to ensure security as well as convenience. But they also face many challenges that can limit their use on a large scale. One of the most important vulnerabilities is the biometric template database itself. If the database is compromised, cannot be revoked and can be used for cross-referencing among different databases using the same biometric trait. Although research is been undertaken, many points have to be addressed yet to improve the security:

- The time taken to generate each template is pretty high, measures should be taken to reduce the time to produce the transformed template by using parallel processing.
- The possibility of implementing iris recognition and iris template security algorithms on hardware to enable faster real time implementations.

Table 4:Summary of Iris Shuffling a template protection scheme

Feature Transform / Measure	IRIS Shuffling Scheme
Inter user variability	Templates are matched accurately
Data Storage	Transformed template & Key
Security	Password Security, Non-invertible

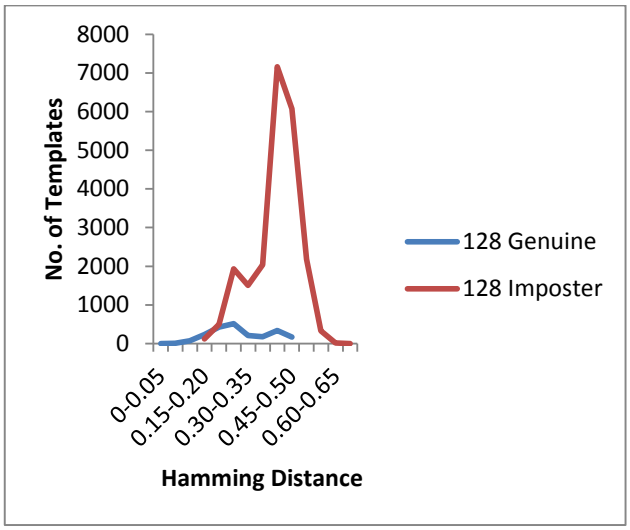

Figure 4: Genuine, Imposter HD for 128-bit Key size

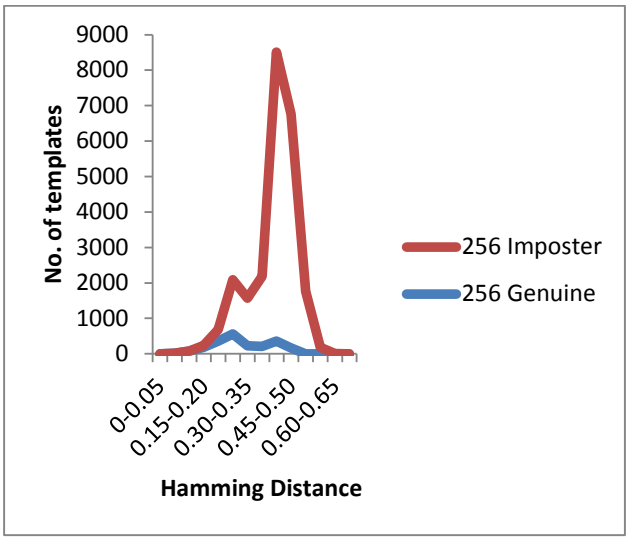

Figure 5: Genuine and Imposter HD for 256-bit Key size

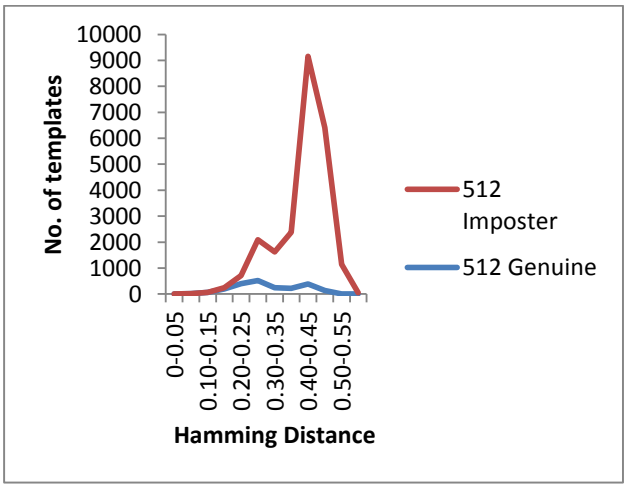

Figure 6: Genuine and Imposter HD for 512-bit Key size

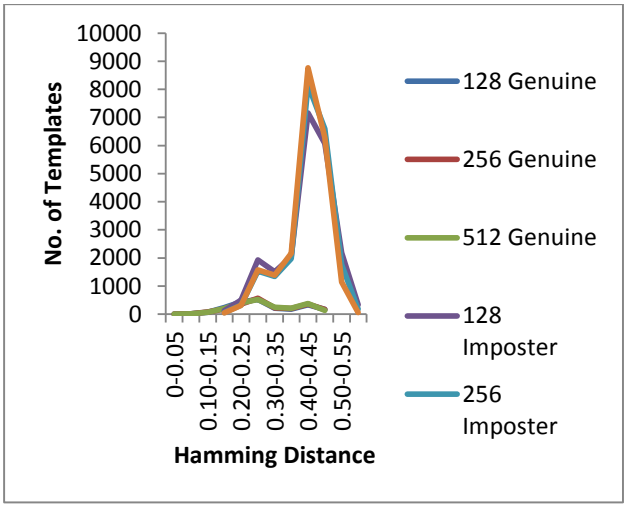

Figure 7:Genuine and Imposter HD Comparison with different key sizes

REFERENCES

[1] 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.

[2] B.Schneier, (1999) "The uses and abuses of biometrics", Communications of the ACM, 42(8):136.

[3] CASIA Iris Database of The Chinese Academy of Science, http://www.cbsr.ia.ac.cn/IrisDatabase.htm (accessed November 2011).

[4] Daugman J, (2004) "How Iris recognition works", IEEE Trans. Circuits and Systems for Video Technology, 14: 21-30.
[5] Feng Hao, Ross Anderson, John Daugman (2007) "Combining Cryptography with biometrics effectively", University of Cambridge, Proc. IEEE.

[6] I. Buhan , P. Hartel (2005) "The state of the art in abuse of biometric", Center of Telematics and Information Technology, University of Twente, Technical Report, TR-CTIT-05-41.

[7] J. Daugman (1993), "High Confidence Visual Recognition by a Test of Statistical Independence", IEEE Trans. Pattern Analysis and Machine Intelligence, Vol. 15, No.11, pp.1148-1161.

[8] Juels A., Wattenberg M.,(1999) "A Fuzzy Commitment Scheme", in Proceedings of Sixth ACM Conference on Computer and Communications Security, Singapore, pp. 28-36.

[9] Libor Masek,(2003) "Recognition of human iris patterns for Biometric Identification", Univeristy of Western Australia.

[10] N. Ratha, J. Connell (2000)"Cancelable Biometrics", presented at Biometric consortium 2000 Conference, Sept. 13-14.

[11] N. K. Ratha, J. H. Connell, and R. M. Bolle (2001) "Enhancing Security and Privacy in Biometric-based authentication system", IBM Systems Journal, 40(3): 614-634.

[12] Sim Hiew Moi et. al.(2009), "Iris Biometric Cryptography for Identity Document", 2009 International Conference of Soft Computing and Pattern Recognition, IEEE Computer Society Conference, pp. 736-741.

[13] S.Mohammadi, A.Kaldi, K.N.Toosi, (2008) "Adoption of Iris based authentication", University of Technology, IEEE.

[14] Souter C., et. al.(1998), "Biometric Encryption using image processing", in Proceeding SPIE, Optical Security and Counterfeit Deterrence Techniques II, Vol 3314, pp. 178-188.

[15] S. S. Agaian (1985) "Hadamard Matrix and their applications", LNM, Springer Verlag.

[16] S V Sheela, P.A.Vijaya (2010) "Iris Recognition Methods-Survey", International Journal of Computer Applications(0975-8887), Volume 3-No.4.