Cryptosystem based Multimodal Biometrics Template Security

Ashish P. Palandurkar
Student M.E. WCC, AGPCE,
Nagpur, Maharashtra, India

Pragati N. Patil
Asst. Prof. AGPCE,
Nagpur, Maharashtra, India

Yogesh C. Bhute
Asst. Prof, AGPCE,
Nagpur, Maharashtra, India

ABSTRACT
As we all know that the biometrics system is used everywhere for person identity verfication. So the biometric system identification is based on the modality and that modalities depends on the physical as well as biological behaviour of the person. The physical behaviour like Fingerprint, Iris, face are. physical behaviour of the human being whereas biological behaviour means according to mannerism of human being are signature or DNA testing of human being .If we are using one modality for identification of person it leads to problem as the modality fail for identification so person has to face problems. If modality fails for identification person comes under problem for that purpose multimodal system is the best option. In multimodal system we are using two modalities for person identification. In this paper we have used two modalities i.e. Fingerprint and Iris. If it is compared with other modalities like palm print, Voice, Fingerprint takes comparative little time for scanning and for saving the files of fingerprint images whereas in Iris identification system user should not be should not be present ,so eye template we can get from anywhere, also two Iris image cannot be identical. In Iris system twins Iris are not identical. We propose our work to fuse the vector of Fingerprint and Iris and that fused method provide security. Template security is the main aim of our analysis. The template should be encrypted and by using that encrypted method template should be protected and it must store in database.

Keywords
Cryptosystem, Fusion, Fuzzy commitment, Fuzzy vault, Selective encryption.

1. INTRODUCTION
In biometric system we are using the personal traits for recognizing people. Biometrics provides reliability to retrieve data and get access to that data to only verified user. Recently Biometrics users are huge overall in world. As the new technology is in regular used at the same time we have to face problems. Biometric trait allows authorize user to access by the reliable people. Biometrics system basically use for pattern recognition here in this work, we have physical and biological characteristics. The physical characteristics means the traits that have been collected from the human body where as biological characteristics means it depends on the manner of human being how it behaves in the society. In physical biometrics characteristics categories as fingerprint, face recognition, palm, voice and biological includes gait, keystroke. As we know that the biometrics helpful in recognizing person so the database of biometric traits can be misuse or it can [1] be stolen by any intruder. The biometric templates move by the intruder, so biometric templates came across the security problem. Here we can use different techniques for security purpose of biometric trait. Here we use a technique called Multimodal Biometric System, which uses a combination of more than one biometric trait for identity verification. Multimodal biometrics system assembles more than two traits for recognizing one person. Security provision has been provided in different forms(i)Use different methods for storing templates of different biometric templates.(ii)Use multimodal system. In unimodal system we are using only one modality whereas in multimodal system can give best results in the accuracy level and recognizing the traits with best elapsed time. Unimodal system faces several problems such as noisy data Template security is the main focus of work.

Biometric cryptosystem suffer from various attacks, some of the attacks at various levels are given bellow:

(1) At the sensor level a fake biometric input is given like artificial finger or clone ,

(2) Dishonestly interchanged data is submitted to the system.

(3) Predefined feature data is produced at feature extractor by a program.

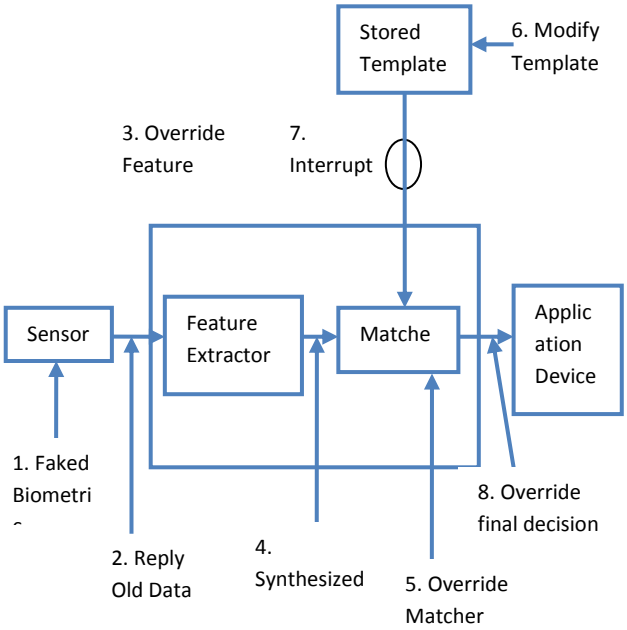

Fig 1: Threats to the Biometric system

To overcome from all these disadvantages of biometric system, we use multibiometric cryptosystem. Multibiometric is combination of more than one biometric, and fusion of multibiometric indicate the improvement in security and reliability of the system. Multibiometric systems fusion is categorized in three levels namely [3]:

1.1 Feature Level Fusion

In feature level fusion new feature vector is constructed with high dimensionality. The newly formed vector is more discriminative than individuals.

1.2 Score Level Fusion

In this level matching scores are collected from every individual and then combine together.

1.3 Decision Level Fusion

In decision level fusion final results are combined together. We use feature level fusion for multibiometric cryptosystem. Unlike passwords and tokens, compromised multibiometric templates are not recoverable. Because of this, multibiometric template security is very necessary thing. In this paper, we propose a scheme to protect all the templates of user in multibiometric system.

2. BACKGROUND

To secure biometric templates many techniques are there. These techniques are categorized into two classes:

2.1 Template Transformation

These techniques modify the biometric template with a user specific key so that it is complicated to recover the original template from the transformed template. Throughout authentication, the same transformation is applied to the biometric query and the matching is performed in the transformed domain to evade exposure of the original biometric template. Generally the secure template should satisfy the properties like:

(i) Noninvertibility—specified a secure template, it must be computationally not easy to find a biometric feature set that will match with the particular template.

(ii)Revocability— specified two secure templates generated from the same biometric data, it must be computationally tough to identify that they are consequent from the same data or obtain the original biometric data.

2.2 Biometric Cryptosystems

In this technique secure sketch is obtained from given biometric template and stored in database as an alternative of original template. The helper data is usually obtained by binding a key with the template. So such techniques are also known as key binding biometric cryptosystems. To handle intra-user variations error correction coding techniques are typically used.

Fuzzy vault [4] is well known example of biometric cryptosystem. And which is very useful in protecting point-set-based features. It is design to secure multibiometric features which are represented as a point set. Main advantage of fuzzy vault is, it has ability to secure fingerprint details.

Fuzzy Commitment is a biometric cryptosystem which is used to secure biometrics traits represented in binary vector. Main advantage of this technique is its compact size of the sketch. Assume that the enrolled biometric template is an -bit binary string. In fuzzy commitment, a uniformly random key of length l bits is generated and used to exclusively index an n-bit codeword of suitable error correcting code. The sketch is then extracted from the template. At the end sketch is stored in the database.

3. PREVIOUS RESEARCH

A number of attempts have been made to enlarge the secure biometric recognition framework to integrate multiple biometric traits [6]. It joint faces and fingerprint templates that are both altered into binary strings. These binary strings are concatenated and then used as the input to a fuzzy commitment scheme. Fu et al. Hypothetically analyzed the template security and recognition accuracy imparted by a multibiometric cryptosystem, which is operated in 4 different ways: no-split, MN-split, package,and biometric model. The first three models keep up a correspondence to decision-level fusion, where the biometric templates are secured separately. The biometric model is based on feature-level fusion of standardized templates. However, no system implementation was reported.

Nandakumar and Jain [7] wished-for a multibiometric cryptosystem in which biometric templates based on binary strings and point-sets are united. The binary string is separated into a number of segments and each segment is independently secured using a fuzzy commitment scheme. The keys related with these segment-wise fuzzy commitment schemes are then used as supplementary points in the fuzzy vault constructed using the point-set-based features.

Fu and Yang [6] bind multiple biometrics to cryptography, and form multibiometric cryptosystem. Abandoning the unambiguous integration techniques of different biometrics, the impacts of fusion at biometric and cryptographic levels on the biometric security, privacy and accuracy are trying to increase.

In this paper, we propose the design of a multibiometric cryptosystem with various templates and try to provide security with biometric cryptosystem techniques.

4. PROPOSED WORK

Multimodal biometrics refers to the use of combinations of two or more biometric modalities in an identification system. Identification based on multiple biometrics represents an emerging trend. The most compelling reason to combine different modalities is to improve the recognition rate. This can be done when biometric features of different biometrics are statistically independent. There are other reasons to combine two or more biometrics. Another reason is simply customer preference. The fusion of Iris and Fingerprint at feature level is using a unique technique. The features of Iris and Fingerprint are extracted after the processing of normalized image & histogram equalization accordingly. A key is applied to perform encryption and fusion of these two feature vectors are combine. The query image feature vectors are fused and then compared with the fused feature vectors stored in the database. The final decision that if the user is genuine or imposter is taken with the help of Hamming distance matcher method.

Implementation of the biometric technology is the very challenging task for our system. Apart, of using biometric template we have implemented fused of two biometric templates and that template also used with the algorithm for encryption technique. The interconnection of this technique is very useful for reproducing the accuracy and security of the biometric template. Now a day we have deployment of biometric system in every industries, companies and colleges. As we are all having knowledge regarding the biometric

system that biometric system is used for recognition of person. But when we have analyzed different biometric system they have to face problems in using biometric system if user template fails to detect the template at the time of matching[8].

To improve the performance, accuracy of the system and reduce the complexity of database we have proposed multibiometric system with cryptography key. The main objective of our work is to give security to the biometric template. The proposed approach is to use two modalities i. e. Fingerprint biometric trait and Iris Biometric trait. The biometric system is basically is used for pattern recognition so here also we are recognizing the patterns of biometric system as an features format and that features are fused with principal component analysis. Implementation of fused image is used for encryption. The encrypted image is stored in database as a record.

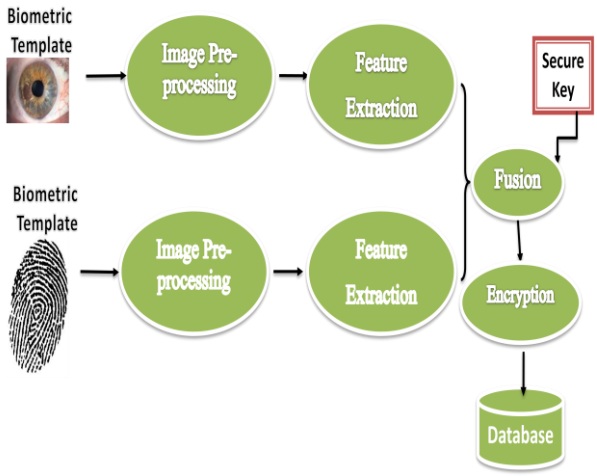

Fig 2. Implementation of Template Security with Cryptography Key

The above figure is the implementation of our multimodal biometric system. Working scheme of our system is, first step consists of performing the image acquisition of various biometric templates. The next step involves the feature extraction from the biometric traits. The extracted features are stored in the database that template have to be compared with the template stored in the database. Result is obtained as a matching score of that template.

4.1 Advantages of Proposed System

1. Compared to uni-biometric systems that rely on a single biometric trait, multi-biometric systems can provide higher recognition accuracy and larger population coverage.
2. Consequently, multi-biometric systems are being widely adopted in many large-scale identification systems.

4.2 Different Modules to be implemented

- Fingerprint feature Extraction.
- Iris feature Extraction.
- Feature-Level Fusion.
- Preserves the template with Security.
- Template matching.

4.2.1 Fingerprint Feature Module

In this module, Fingerprint minutiae are extracted obtain the binary string representation from the minutiae set. First the user has to upload and select the fingerprint images from the sample database. Then the Finger print feature are loaded into the system. Then this module, extracts the fingerprint features[1].

4.2.2 Iris Feature Module

In this module, the binary Iris Code features are extracted. The user has to upload and select the IRIS images from the sample database. Then the IRIS feature are loaded into the system. In order to reduce the dimensionality of the iris code and remove the redundancy present in the code, LDA is applied to the IRIS code features. Then the binary IRIS code features are extracted [2].

4.2.3 Feature-Level Fusion Module

We propose a feature-level fusion framework to simultaneously secure multiple templates of a user using biometric cryptosystems[3]. To demonstrate the viability of this framework, we propose simple algorithms for the following three tasks:

1) Converting different biometric representations into a common representation space using various embedding algorithms: (a) binary strings to point-sets, (b) point-sets to binary strings, and (c) fixed-length real-valued vectors to binary strings.

2) Fusing different features into a single multi-biometric template that can be secured using an appropriate biometric cryptosystem such as fuzzy vault and fuzzy commitment; efficient decoding strategies for these biometric cryptosystems are also proposed.

3) Incorporating a minimum matching constraint for each trait, in order to counter the possibility of an attacker gaining illegitimate access to the secure system by simply guessing/knowing only a subset of the biometric traits.

4.2.4 Preserves the Template with Security

In this module, the fused template in encoded by using some encryption algorithm and the new template is generated. Here we also applied the secure key to the fusion output vector, to generate the key we use some algorithm for random key generation. Then the new encrypted template is created i.e. is stored in database for person identification at the time of verification process.

4.2.5 Template Matching

Here we verified the person by verifying that the template i.e. generated at the time of user login will be same as the stored biometric trait in database [4]. To do this we use the hamming distance matching algorithm, which find score of matching of two traits.

5. PROPOSED APPROACH FOR CRYPTOGRAPHY

5.1 Encryption using Chaotic Map

In this paper we use an algorithmm using chaotic map.There are two steps for [2] encryption, in first step we introduces a chaotic map using henon map.

$a(x+1)=1-ka(x)^2+g(x)$

$g(x+1)=sa(x)$

where k=1.4 s=0.3 to illustrate chaotic manner.

5.2 Encryption using Feature Level Fusion of Biometrics Cryptography

Multimodal biometrics is more dependable as compared to unimodal biometrics. In unimodal system n user uses only one modality i.e. Fingerprint, Iris whereas in multimodal biometrics we can use two modalities i.e. Fingerprint and Iris. Here they have been used cryptography in four Steps.

As an input they have been taken feature vector of Iris and Fingerprint. From fingerprint they have been generalized two vectors as an x-coordinate, and y –coordinate, and from iris they have generated two vectors because here feature vector generated in complex format because of gabor filter.

Step 1:Mixing of Individual feature Vectors: Here, Mixing of individual vector is done with random vector generation.

Step2:Merging Of Feature vector is done. Here, Merge vector is stored in the third vector.

Step 3:Assembling of feature vector is encrypted using secret Key.

5.3 Encryption using Multimodal Biometrics with Cryptography

Here, we have been worked on feature level fusion. In Feature level fusion Features are extracted from different modalities in Ht and stored in the third vector J K In this paper author discuss that for security they have been using fuzzy vault and fuzzy commitment..In fuzzy Vault is used for point-based where as fuzzy commitment is used for binary sets. In fuzzy Vault set of r points randomly generated and that points are added with the feature vector and that assembled points stored as a vault for security. The fuzzy vault is basically is used for fingerprint modality where as for Iris modality fuzzy commitment is used. In fuzzy commitment feature vector is generated and key which is used for encryption that key is assembled using error correcting code method. After assembling this it is stored in the database. When user authenticating through this random points are disappeared and thet user is verified.

5.4 Encryption Method using Selective Method

Selective encryption method is basically used of media applications. In media applications we are consist of audio, video, text, images data. Researchers implemented this method because this method takes less time for encryption and decryption. Here features of modalities has taken and after that security key is taken from the user. when we have taken the key operation has performed on the key and that random points vector is bitxor with the key generation operation. After assembling all this encryption of key is done.

For decrypting the same image we have to enter the same key which is entered at the time of encryption. Here, for assembling of points they have used different channels. The channels are represented with different colors. For x they represented data with red channel, Y used Green channel, Z used Blue channel. When we are encrypting data they are represented as per plotting of points. For key generation they have used following key generation equation:

key1=3.925, key2=3.925; key3=0.2,key4=0.3

a=key0=key1*key0*(1-key0)

b=key3=key2*key3*(1-key3)

c=key4=key2*key4*(1-key4)

6. EXPERIMENTAL RESULTS

We evaluate the trade-off between recognition accuracy and security of the proposed multibiometric cryptosystems. To validate the constrained multibiometric cryptosystem, we implemented a system consisting of iris and fingerprint modalities, where minimum matching constraints are imposed for the fingerprint modality. We further assume that the adversary has knowledge about the iris biometric, i.e., he has access to some iris image of the enrolled user.

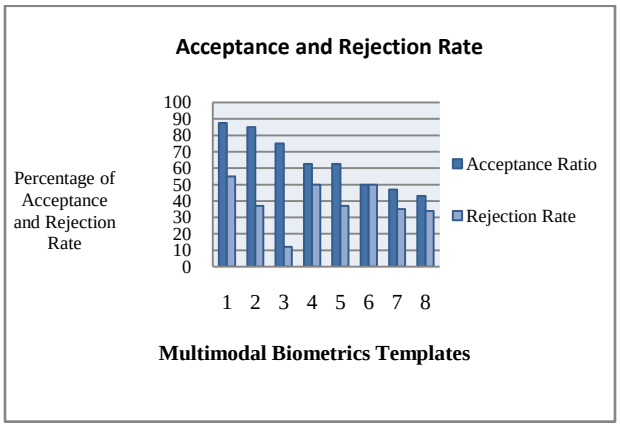

Fig. 3: Acceptance Ratios and Rejection Ratio

In above diagram we have seen the acceptance and rejection ration .We have tested the acceptance and rejection ratio on 800 subjects. Here the subjects are divided into the range of 1-100 for 1 database according to this range the result is tested for 8 databases. On y axis we have percent of matching acceptance and rejection rate matching whereas on x-axis we have been taken the subjects samples. When we have calculated the biometric system with 101_1 and102_2 the percent of matching between the two images then we have obtained result as the total_matched_percentage = 7.5049 and get the message, Hence the pictures have not been matched, Different Pictures, when we have matched with the same image then we get the result as an 100% matching and get the message same image. When we have compared two Iris image i. e. Eye1 and Eye2 image then we get the percent of matching as the 1.0741 and when we have evaluated with the same image then we get the result as the matching is 100% and get the message same image.

6.1 Comparison with the Unimodal and Multimodal System

Table_1: Elapsed Time between Unimodal biometrics system and Multimodal system.

Sr. No	Fingerprint	Iris	Cryptosystem
1	0.555220	0.415847	0.95797
2	0.439939	0.477761	0.676297
3	0.537351	9.374624	0.631027
4	0.500591	13.510012	0.646848
5	0.499712	12.579513	0.652246
6	0.482172	15.154365	0.776297
7	0.436021	10.260830	0.576297
8	0.476388	0.650242	0.526354
9	0.460306	8.469078	0.65522
10	0.449348	9.499048	0.631029

The above result is the elapsed time between two modalities system. In order to get the overall results in first step we have computed the time unimodal system of fingerprint then computed the Iris system and after that cryptosystem based system's evaluation is done. Here in Table 1 we have observed that elapsed time required for Iris system is huge as compared to the fingerprint and Cryptosystem based system. We have shown that as compared to unimodal system Fingerprint and Iris the Cryptosystem based system requires average time. Therefore we our system represents results with best outcomes.

7. CONCLUSION

Thus, we have studied different methods of encryption. But multimodal biometrics gives best accuracy and flexibility as compared to the unibiometric system. In unimodal biometric system we are using only any modality which can be hacked by the intruder where as in multimodal system we are storing the template or biometric feature of modalities and that is stored simultaneously in third vector .So, it is very difficult for the intruder to hacked this data. In experimental results multimodal system gives best results as compared to the unimodal system. Here we can give review that multimodal system provides best results as compared to the unimodal system. Here we have point out that multimodal system is little bit complex and time consuming processing as compared to the unimodal system.

8. REFERENCES

[1] P. S. Sanjekar and J. B. Patil, An Overview Of Multimodal Biometrics Department of Computer Engineering, RCPIT, Shirpur ,Signal & Image Processing : An International Journal (SIPIJ) Vol.4, No.1, February 2013,DOI :

[2] Kulwinder Singh, Kiranbir Kaur, Ashok Sardana,Gulzar Group of Institutes, Khanna, Punjab, India Global Institute of Engineering and Technology, Punjab, India IET Bhaddal, Ropar, Punjab, India,"Fingerprint Feature Extraction", IJCST Vol. 2, Issue 3, September 2011

[3] Abhishek Nagar, Student Member, IEEE, Karthik Nandakumar, Member, IEEE, and AnilK. Jain, Fellow, IEEE, Multibiometric Cryptosystems Based on Feature-Level Fusion, IEEE Transactions On Information Forensics And Security, Vol. 7, No. 1, February 2012,Page No255

[4] R.N. Kankrale, Prof. S. D. Sapkal. Template Level Fusion of Iris and Fingerprint in Multimodal Biometric Identification Systems, Department of Information Technology SRES

[5] A. Jagadeesan, Dr. K. Duraiswamy. Secured Cryptographic Key Generation From Multimodal Biometrics: Feature Level Fusion Of Fingerprint And Iris, (IJCSIS) International Journal of Computer Science and Information Security,Vol. 7, No. 2, February 2010

[6] Ai-hong Zhu ,Lian Li. Improving for Chaotic Image Encryption Algorithm Based on Logistic Map ,2nd Conference on Environmental Science and Information Application Technology ,2010,Page No:211 -214

[7] Sangram Bana1 and Dr. Davinder Kaur2.Fingerprint Recognition using Image Segmentation, Sangram Bana, et al. / (Ijaest) International Journal Of Advanced Engineering Sciences And Technologies Vol No. 5, Issue No. 1, 012 – 023

[8] S. Arun Vivek, J. Aravinth, S. Valarmathy Professor "Feature Extraction for Multimodal Biometric and Study of Fusion Using Gaussian Mixture Model".