Volume 3, Issue 8, August 2013 ISSN: 2277 128X

International Journal of Advanced Research in Computer Science and Software Engineering

Research Paper

Available online at: www.ijarcsse.com

Analysis of Multimodal Biometrics with Security Key

Mr. Rupesh Wagh*
Head, Department Information Technology
Dr. Babasaheb Ambedkar College of Engineering&Research .
Nagpur, India

Ms. Arati P Choudhari
Astt.Professor, Department Computer Technology
Rajiv Gandhi College of Engg. & Research,
Nagpur, India

Abstract— Cryptography is used for security of data. This cryptography we were is used in biometrics system. When we ensure that we are using biometrics, it is basically used for authentication and verification by the person's template. But that template can be misused if it is stolen, by any perpetrate. Focusing on biometric template security is the main discussion of our paper. Multimodal biometrics used two modalities Fingerprint and Iris biometrics characteristics. The significant features are taken from biometric template. That features are stored using feature level fusion and that fused vector is encrypted using different security technologies. Fusion is done using extracting important features of modalities. Here, we discuss regarding how our system is secure when we are using selective encryption method for encrypting the biometric template.

Keywords— Cryptography, Templates, Fusion. Encryption, Biometrics, Multimodal, Fused vector

I. Introduction

. Now a days, biometrics has been using in every area for giving authority to the authorize user of the esteemed organization. Biometrics and cryptography are the significant points of the recognizing the person and providing security to that template. Biometrics gives identification and verification to the template of authorize user where as cryptography gives authentication to that template. So, both the technologies are interconnected based on providing security to the user's essential object. Here, we are using two modalities. Fingerprint and Iris are the two modalities discuss in our paper.

Fingerprint module takes fewer times, in taking the fingerprint template, as its size is smaller it will take reasonable time in taking the Fingerprint template and accepting the template. In Iris system what happens that this system is accepting everywhere, at the time of capturing the eye image no physical interaction is needed with the sensors. So you can capture the image from everywhere and used the template for recognition. Biometrics recognition is done through two distinct methods Evidence Identity, Confirmation of Template.

Evidence Identity: In identity provision the unknown person's template is first checked with the stored database then identity is given to the unrecognized person. The identity is given with the name and the Identification Number and the record is stored successfully.

Confirmation of Template: When the identified person is giving his identity then the sensors should verified the person. In unimodal system we are using only one system as only single Fingerprint System, Iris System or Face Recognition System. Lots of problems has to face ,when we are using unimodal biometrics system. When the trait of biometrics has taken then the sometimes noise enters with the trait, that results in higher the false rejection rate. Also, when we are using the only single system then the database template can be stolen and it can be revoked by any intruder as it contains only one template. If person has been facing difficulty in giving template because of injury or damage of physical part of that person then the he can't use that system.

In this case multimodal system is the best choice for identification of the person without fail. In multimodal biometrics system we are using two modalities for recognition of person. In our paper we discuss the Fingerprint and Iris characteristic. We discuss here how we are fusing the two biometric system and that fused method is storing in the database using encrypting method. Multibiometrics system has lots of advantage as follows:

(i) Its makes better system operation .
(ii) Its accuracy is better as compared to the unibiometric system.
(iii) It prevent from stolen the templates of biometric system as at the time it stores the two characteristics of biometric system in the database.

Here biometric templates have given recognition of person so it can be misuse by the perpetrator so it should provide the security to the templates. Following reasons are encourage as for providing security to the template:

1. Perpetrator can generate false template used as the authorize user.
2. Intruder can also use not earlier data and misused that data.

Lots of reason has there, that the intruder can misused the data. So it should not happen for that reason security of the template is important task.

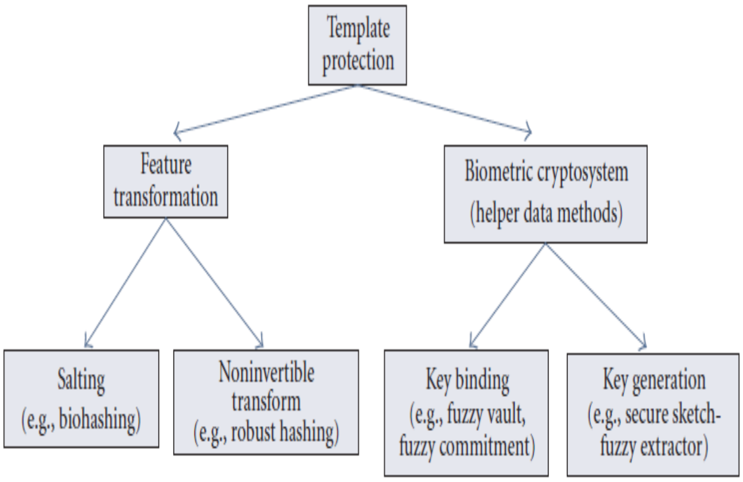
Template protection
Feature transformation
Biometric cryptosystem (helper data methods)
Salting (e.g., biohashing)
Noninvertible transform (e.g., robust hashing)
Key binding (e.g., fuzzy vault, fuzzy commitment)
Key generation (e.g., secure sketch-fuzzy extractor)

Fig. 1 Different Techniques of Securing Biometric Templates

We have different template security techniques:

Template Protection is done through different techniques Feature Conversion and providing Cryptography to the biometric template.In Feature Conversion features are converted using security key and stored in the database.

Using security key we can encrypt our biometric template and stored in the database, whereas in biometric cryptosystem the features of biometric template are extracted and it is wrapped with the key and stored in the database.

II . Related Work

Cryptographic key method we are using for encryption of fused template. There are two methods of encryption with the key, symmetric key and asymmetric key. In symmetric key, one key is used for encryption and decryption i.e. sender and receiver has to know only information about one key, whereas in asymmetric key sender use different key for encryption and for decryption receiver use different key. In asymmetric key one key is used for encryption called as public key and key is used for decryption called as private key. Public key can be disclosed but private key cannot be known to anyone. Here we are using digital image processing with cryptography i.e. two technologies are combined.

III. PROPOSED WORK

The work has been divided into three parts,
1. Feature extraction of biometric template
2. Fusion Module
3. The template stored in the database with Security.

In first module we are using two templates as discussed in above i.e . extraction of features of Fingerprint in form of minutia points where as in Iris modality we are extracting the features in form of texture or Iris code template.

(i) Fingerprint Recognition System

- Image Acquisition: In image acquisition the captured image form the database is load in our system.
- Image Enhancement:
  Enhancement of template is done for making image clear for further operations .Histogram Equalization used for Image Enhancement.
- Binarization: Fingerprint binarization converts 8 bit gray level image into 1 bit gray level image with 0-value for ridges and 1-value for bifurcation.
- Ridges comes in black color and bifurcation comes in white color.
- Segmentation
- Segmentation is done for removing the ridges and bifurcations those having less importance.
- Region of Interest(ROI) is used for segmentation. ROI is used in two steps direction map and morphological operation.

III. EXPERIMENT SETUP

Here we took the biometrics samples tested from two database i.e. Virtual database and Real database. Virtual database means the database we are generated from doing the operation where as the real database is the database for testing of the biometric system.

IV. CONCLUSION

Multimodal biometrics gives accuracy in providing results as compared to unimodal system. By experimental results it will prove that accuracy of multimodal system is improved than fingerprint and Iris unimodal system

REFERENCES

[1] Anil K. Jain, Karthik Nandakumar, and Abhishek Nagar, Review Article Biometric Template Security**,** Department of Computer Science and Engineering, Michigan State University, 3115 Engineering Building, East Lansing, MI 48824, USA

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

[3] 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*

[4] 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

[5] Ajay Kumar, Senior Member, IEEE, Vivek Kanhangad, Student Member, IEEE, and David Zhang, Fellow, **IEEE "A New Framework for Adaptive Multimodal Biometrics Management",** *Transactions on information forensics*