Enhancement of Biometric Template Security in Multibiometric Systems

Asra Nisar Bhat
Student of Lovely Professional University

Supreet Kaur
Faculty of Lovely Professional University

ABSTRACT

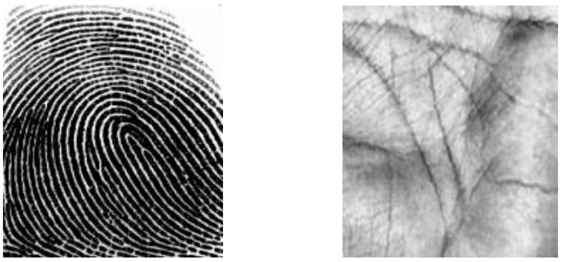
Security is a very important aspect in the biometric systems. Biometric characteristics are unique to an individual hence the compromise of the biometric template is permanent. Attackers mostly attack on template and database of biometric system so securing them is a very crucial issue these days. Moreover the multibiometric systems require storage of multiple biometric templates (e.g., fingerprint, iris, and face) for each user, which results in increased risk to user privacy and system security. In this research paper our focus is on template security in biometrics system and we develop a system to encrypt and decrypt the biometric images. In this work, multi-modal biometric template security for palm print and fingerprint is proposed. At first, the preprocessing steps are applied and subsequently, the features are extracted and combined to simultaneously protect multiple templates. Then different cryptographic techniques are used to encrypt it to make it secure so that even if someone gains access to the encrypted image stored in the database he will not able to reproduce the original image from it and it will be useless for him.

Keywords

Multimodal Biometrics, Fingerprint, Palmprint, Features, Cryptography, Security, Encryption, Decryption.

1. INTRODUCTION

A biometric is a measurement of a biological characteristic of a person. It is a science of determining a person's identity (ID) by measuring his/her physiological characteristics. Biometrics gain increasing interest as a solution to many security issues. New passports include biometric data of the owner and laptops nowadays almost always include a fingerprint reader for login [1]. Biometric template data must be protected to prevent information leakage in case of template compromise. Biometric data is inherently linked to an individual and can reveal private information about that individual [6]. Thus it can be easily prone to abuse in such a way that a person's right to privacy and secrecy is compromised. Hence, strategies to protect biometric template and to ensure an individual's privacy are urgently needed. The stolen template can be replayed to the matcher to gain unauthorized access, and secondly physical spoof can be created from the template to gain unauthorized access to the system. These issues raise a number of ethical, social and security problems that have hindered the uptake of biometrics and must be overcome if biometrics is to gain widespread acceptance [12]. In this research work the two biometric characteristics i.e. fingerprint and palm print has been used which are the commonly used traits for the authentication purpose.



(a) Finger print **(b) Palmprint**

Fig 1: The Fingerprint and Palmprint traits of a person.

Fingerprints have been used for over a century. Fingerprint is the pattern of ridges and valley on the inner surface of a finger or a thumb. The lines that flow in various patterns across fingerprints are called ridges and the spaces between ridges are valleys [1]. It is these ridges that are compared between one fingerprint and another when matching. Palmprint refers to an image acquired of the palm region of the hand. Palmprint inherently implements many of the same matching characteristics that have allowed fingerprint recognition. The main advantage of palm print is the availability of large space for extracting biometric features [1].Usually palmprint images should be normalized and oriented before feature extraction. It contains more information than fingerprints, so they are more distinctive. By combining all features of palm and fingerprint such as ridge and valley features, principal lines and wrinkles, it is possible to build a highly accurate biometric system.

2. PROPERTIES OF TEMPLATE PROTECTION SCHEMES

An ideal biometric template protection scheme should possess the following four properties:

i. Diversity: the secure template must not allow cross matching across databases, thereby ensuring the user's privacy[8]

ii. Revocability: it should be straightforward to revoke a compromised template and reissue a new one based on the same biometric data.

iii. Security: it must be computationally hard to obtain the original biometric template from the secure template. This property prevents an adversary from creating a physical spoof of the biometric trait from a stolen template.[8]

iv. Performance: the biometric template protection scheme should not degrade the recognition performance (FAR and FRR) of the biometric system.

3. RELATED WORKS

Over the years a number of attempts have been made to address the problem of template protection and privacy concerns in biometrics. In this section, we will look at the existing work in light of this security and accuracy provided. The first class of feature transformation approaches known as Salting offers security using a transformation function which is kept by a user specific key. The strength of the approach lies in the strength of the key. Some of the popular salting-based approaches are Biohashing. The second approach is identified as noninvertible transform which applies a trait specific noninvertible function on the biometric template so as to secure it. The parameters of the transformation function are defined by a key which must be available at the time of authentication to transform the query feature set. Some of the popular approaches that fall into this category are robust hashing and cancelable templates [4].

The other forms of protection include Biometric cryptosystems. They try to integrate the advantages of both biometrics and cryptography to enhance the overall security and privacy of an authentication system. A number of template protection techniques under this category include fuzzy commitment, fuzzy vault etc .These can be considered as key binding biometric cryptosystems[7].The fuzzy commitment scheme assumes a binary string representation, where the dissimilarity between template and query is measured in terms of the Hamming distance [10]. The fuzzy vault proposed has become one of the most popular approaches for biometric template protection and its implementations for fingerprint, face, iris and signature modalities.The concepts of secure sketch and fuzzy extractor have also been given[5]. The secure sketch can be considered as helper data that leaks only limited information about the template (measured in terms of entropy loss), but facilitates exact reconstruction of the template when presented with a query that is close to the template[2].The fuzzy extractor is a cryptographic primitive that generates a cryptographic key from the biometric features. According to Jain *et al.* [9], performance degradation usually takes place as the matching is done using error correction schemes. This thus forces the use of sophisticated matchers developed specifically for matching the original biometric template. Biometric cryptosystems, along with salting-based approaches introduce diversity and revocability in them. Brenden Chen et al.[11] analyzed and proposed a new technique for producing secure biometric templates that guarantees security, privacy and cancelability. The person’s biometric feature (F) is passed through a hash like function to produce a transformed copy T (F). Verification is done by comparing in the transformed (T) domain. U. Uludag et al.,[13]have given description and worked about biometric cryptosystem, In traditional cryptosystems, user authentication is based on possession of secret keys, which falls loose if the keys are not kept secret (i.e., shared with non legitimate users). Further, keys can be forgotten, lost, or stolen and, thus, cannot provide non repudiation.

4. PROPOSED TECHNIQUE TO SECURE BIOMETRIC TEMPLATE AND DATABASE

In the proposed system, a technique for template security is implemented for protecting the multiple biometric templates. Multimodal biometric technology uses more than one biometric identifier to compare the identity of a person. The proposed multimodal technique includes combined feature points of the fingerprints and the palm print and there further encryption when they are concatenated after the preprocessing steps as shown in the Figure 2.

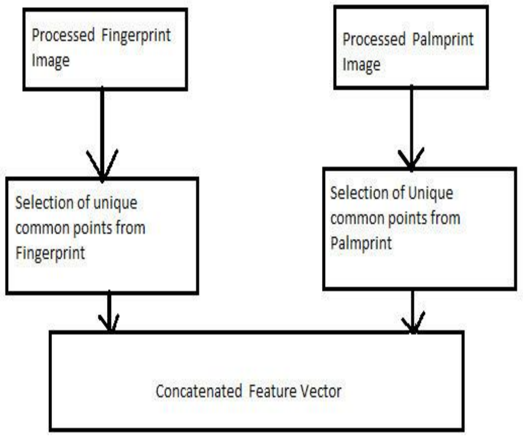

Processed Fingerprint Image
Processed Palmprint Image
Selection of unique common points from Fingerprint
Selection of Unique common points from Palmprint
Concatenated Feature Vector

Fig 2: Block diagram of the feature extraction process

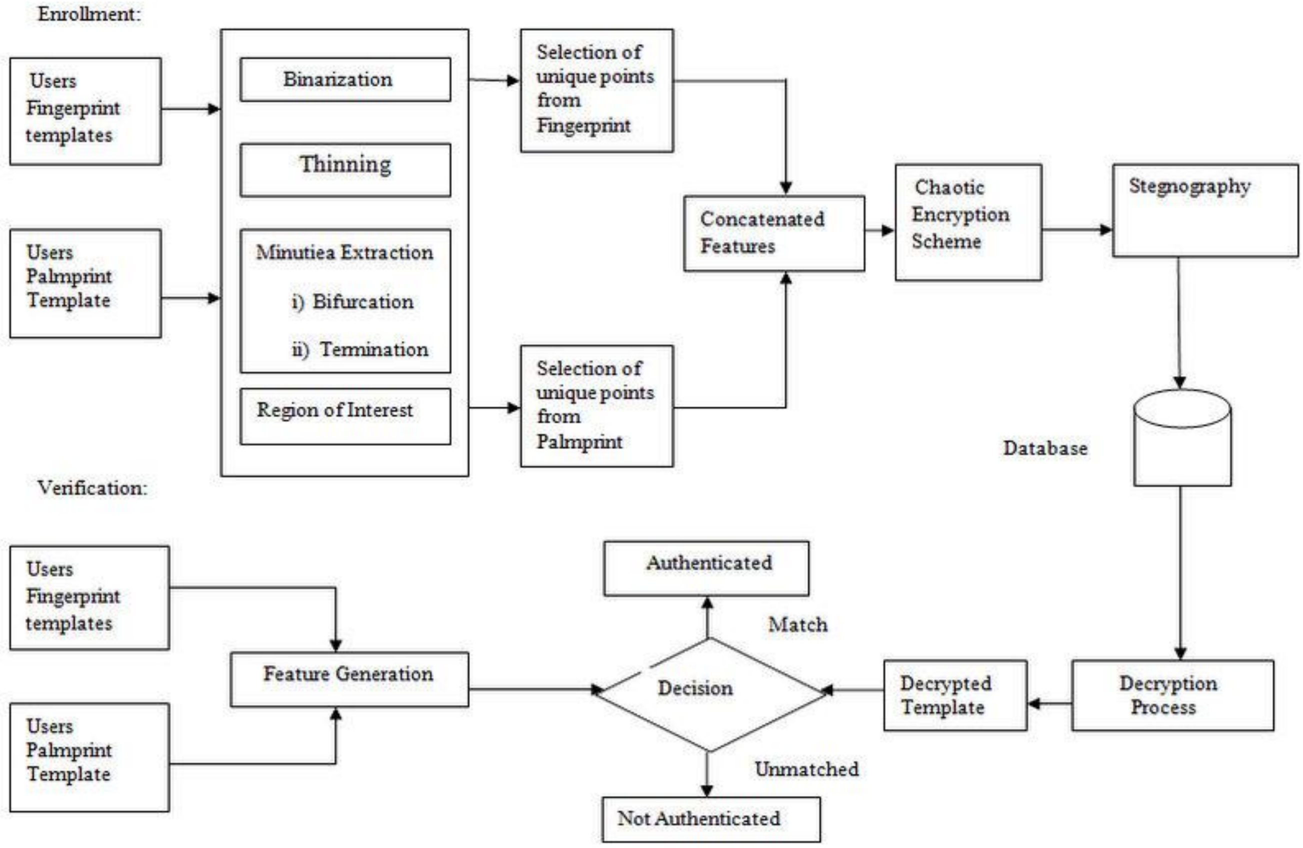


Figure 3: The Block Diagram of the Methodology proposed

Pre-processing: Initially, the enrolled image of the fingerprint and palmprint is pre-processed. The basic and key function of preprocessing is to improve the image such that it increases the chances of success for the other processes. The pre-processing techniques are actually used to enhance the contrast of the image, removal of the noise and isolating the objects of interest in the image. The following are the steps involved in pre- processing:

I. Binarization

II. Thinning

III. Minutiae extraction

- Bifurcation
- Termination

IV. Region of interest (ROI)

I. Binarization: Typically the two colors used for a binary image are black and white though any two colors can be used. The ridges in the fingerprint and palm print images are highlighted with black color while furrows are white. It transforms the 8-bit Gray image into a 1-bit image with 0-value for ridges and 1-value for furrows.

II. Thinning: Thinning is a morphological operation that is used to remove selected foreground pixels from binary images. Thinning is normally only applied to binary images, and produces another binary image as output. Ridge thinning is to eliminate the redundant pixels of ridges till the ridges are just one pixel wide.

III. Minutiae extraction: Everyone is known to have unique, immutable fingerprints. Even the fingerprints of identical twins are different. The image obtained after binarization and thinning is ready to extract the features.

- **Bifurcation:** The ridge pixels with three ridge pixel neighbors are identified as ridge bifurcations.
- **Termination:** The ridge pixels with two ridge pixel neighbors are identified as ridge termination.

IV. Region of Interest: A false minutia affects the accuracy of matching. So, removing false minutiae are essential to keep the system effective .Therefore Region of Interest (ROI) is useful. The image area without effective ridges and furrows is first discarded because it only holds background information.

Feature extraction: Transforming the input data into the set of features is called feature extraction. After the pre-processing step, both the images of fingerprint and palmprint are feature extracted. The feature vector obtained from both the fingerprint and palmprint is subsequently concatenated and further encryption steps are applied to secure it.

The chaotic key based encryption is used and further stegnography is applied to secure the key. At the time of matching the templates, the key would be decrypted and the decrypted key would further decrypt the encrypted image, which will be compared with the new template.

5. RESULTS AND DISCUSSION

The proposed technique is implemented in MATLAB on a system having 3 GB RAM and 2.13 GHz Intel(R) Pentium processor. Here, the error rates are measured in order to determine the accuracy of the proposed technique.

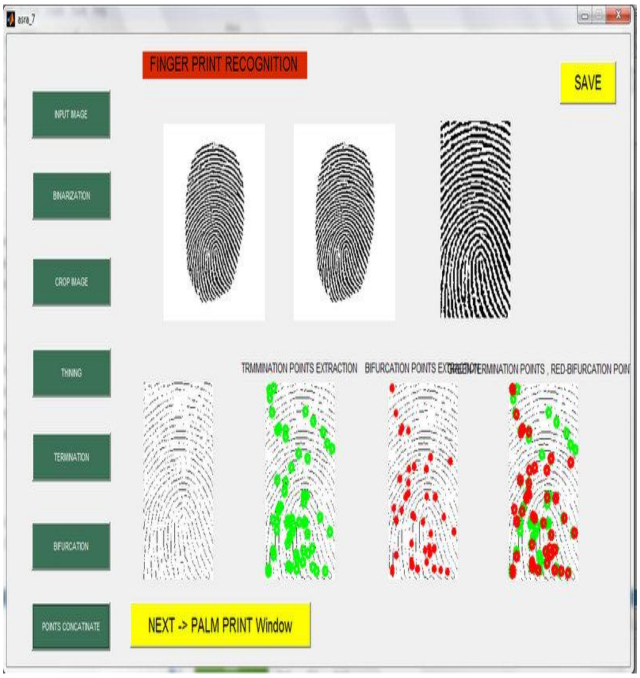

asra_7
FINGER PRINT RECOGNITION
SAVE
INPUT IMAGE
BINARIZATION
CROP IMAGE
THINING
TERMINATION
BIFURCATION
POINTS CONCATINATE
TRMMINATION POINTS EXTRACTION
BIFURCATION POINTS EXTRACTION
GREEN-TERMINATION POINTS , RED-BIFURCATION POIN
NEXT -> PALM PRINT Window

Fig 4: The fingerprint image undergoes Binarization, Thinning and then the features are extracted

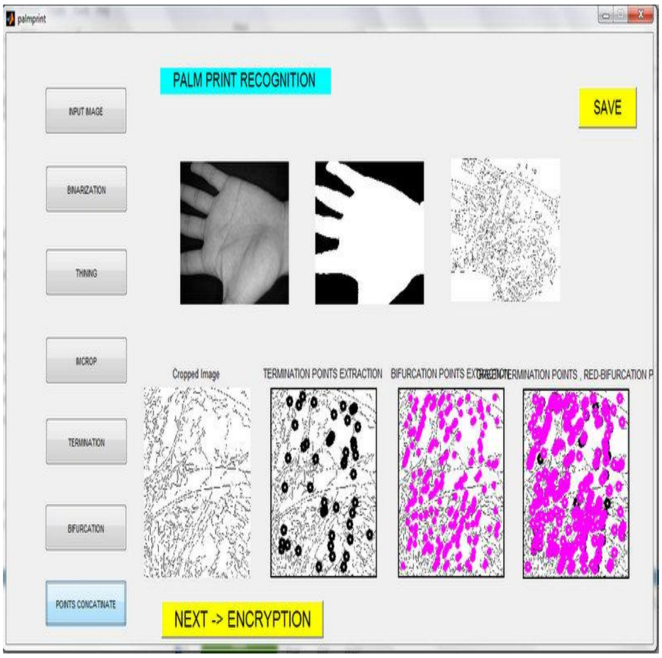


Fig 5: The Palmprint image undergoes Binarization, Thinning and then the features are extracted.

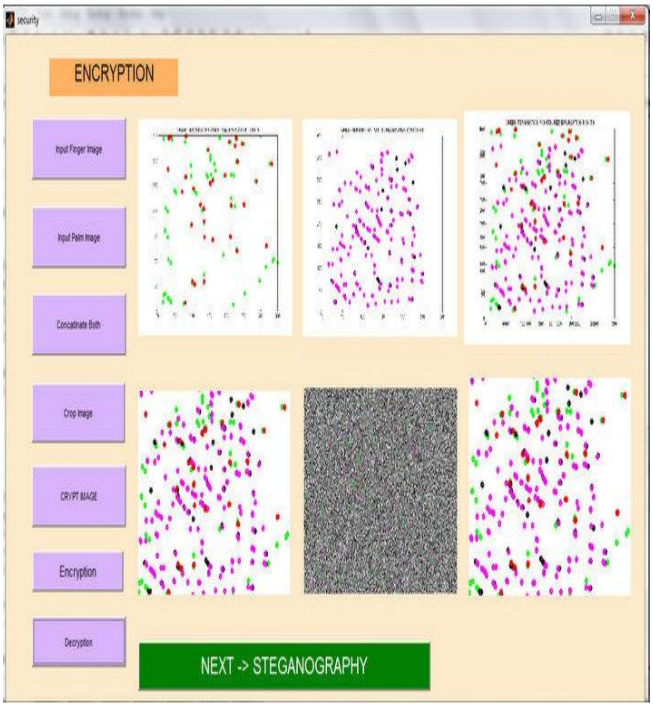
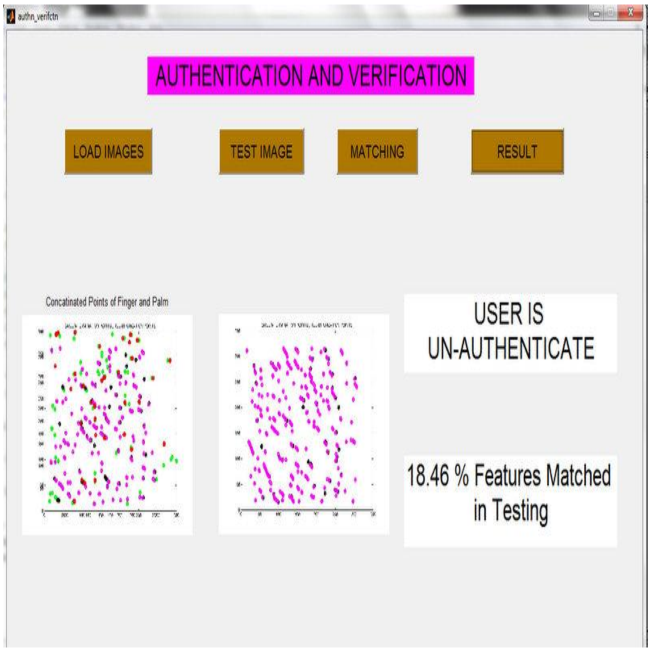


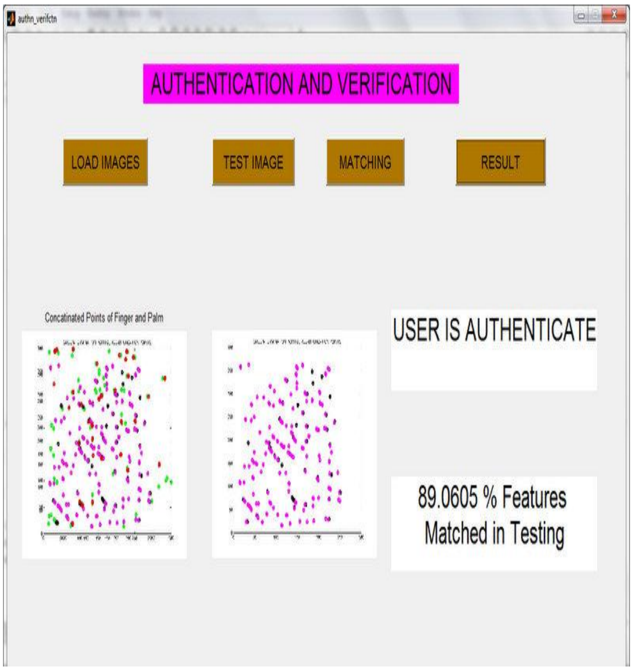
Fig 6:The Concatenated features of fingerprint and palmprint is encrypted and decrypted.


authn_verifctn
AUTHENTICATION AND VERIFICATION
LOAD IMAGES
TEST IMAGE
MATCHING
RESULT
Concatinated Points of Finger and Palm

USER IS UN-AUTHENTICATE

18.46 % Features Matched in Testing

Fig 7: The user is not authenticated as feature don’t match.


authn_verifctn
AUTHENTICATION AND VERIFICATION
LOAD IMAGES
TEST IMAGE
MATCHING
RESULT
Concatinated Points of Finger and Palm

USER IS AUTHENTICATE

89.0605 % Features Matched in Testing

Fig8: The user is authenticated as the features match.

The CASIA database is used. A receiver operating characteristic (ROC) is drawn which illustrates the performance of a system as its threshold is varied**.** We will be thus varying the threshold and plot a graph between the FAR and FRR.

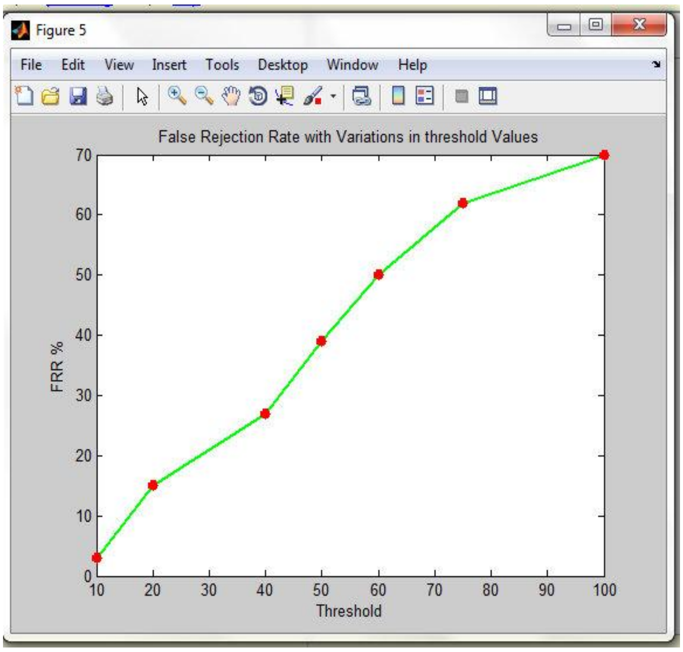


Fig 9: A Graph between FRR and Threshold

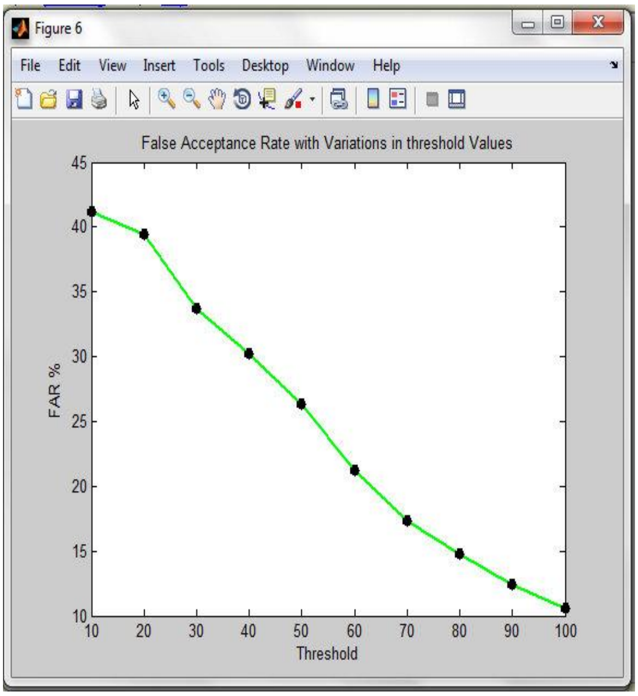


Fig 10: A Graph between FAR and Threshold

6. CONCLUSION AND FUTURE WORK

6.1 Conclusion

This research work presents a method of Biometric Template Security with, its characteristics, design issues and applications. It presents a template protection scheme of the multibiometric traits of a user which are concatenated and further secured. Images are encrypted and decrypted in this thesis and results have been shown. In this work, we mainly focused on protecting Fingerprint and Palmprint templates and have also given a new idea to secure user authentication by combining both features of same user. The proposed work is an attempt to overcome some weakness regarding security concern of the system.

6.2 Future work

The Proposed technique can give an extra edge to biometric systems credibility; it will reduce the attacks on the system and provide a better approach to safeguard the system and user‘s privacy. In this work fingerprint template and palmprint templates are used and they are pre-processed to acquire the bifurcation and termination points. Further the points obtained are concatenated and secured by using suitable encryption techniques. So combination of these two attribute give more security. This can be further extended if three or more biometric templates are used to secure the data. This means a encryption and decryption technique developed for secure the biometric templates and database by the help of feature vectors of three or more templates to provide more authentic and secure solutions.

7. REFERENCES

[1] A.K. Jain, A. Ross and U. Uludag, “Biometric template security: Challenges and solutions”, Proceedings of 13th European Signal Processing Conference (EUSIPCO), 2005.

[2] F. Hao, R. Anderson, and J. Daugman, "Combining crypto with biometrics effectively," IEEE Transactions on Computers, vol. 55, pp. 1081-1088, 2006.

[3] Feng YC, Yuen PC, Protecting face biometric data on smartcard with reed-solomon code. In Proceedings of Computer Vision and Pattern Recognition Workshop, New York, USA 29, 2006.

[4] A. K. Jain, P. Flynn, and A. A. Ross, Eds., Handbook of Biometrics New York: Springer,2007.Anil K. Jain, Karthik Nandakumar, and Abhishek Nagar" Review Article Biometric Template Security",Hindawi Publishing Corporation EURASIP Journal on Advances in Signal Processing Volume 2008.

[5] Dodis Y, Ostrovsky R, Reyzin L, and Smith A, Fuzzy extractors: how to generate strong keys from biometrics and other noisy data. SIAM journal on computing 38: 97-139, 2008.

[6] Mrs. D. Shanmugapriya , Dept. of Information Technology and Dr. G. Padmavathi , Dept. of Computer Science(IJCSIS) ," A Survey of Biometric keystroke Dynamics Approaches, Security and Challenges" International Journal of Computer Science and Information Security,Vol. 5, No. 1, 2009.

[7] Daesung Moon, Woo-Yong Choi and Kiyoung Moon "Fuzzy Fingerprint Vault using Multiple Polynomials" World Academy of Science, Engineering and Technology 59 , 2009.

[8] Manvjeet Kaur, Dr. Sanjeev Sofat and Deepak Saraswat,"Template and Database Security in Biometrics Systems: A Challenging Task", International Journal of Computer Applications, July 2010.

[9] Kocher Niinuma, Unsang Park, and Anil K. Jain, "Soft Biometric Traits for Continuous User Authentication "IEEE TRANSACTIONS ON INFORMATION FORENSICS AND SECURITY, VOL. 5, NO. 4, DECEMBER 2010.

[10] E. Maiorana and P. Campisi, "Fuzzy commitment for function based signature template Protection," IEEE Signal Process. Lett, vol. 17, no.3, pp. 249–252, Mar. 2010.

[11] Brenden Chen and Vinod Chandran, "Biometric Template Security Using Higher Order Spectra", ICASSP,2010.

[12] K. Niinuma and A. K. Jain, "Continuous user authentication using temporal information," in Proc. SPIE, vol. 7667, p. 76670L,2010.

[13] U. Uludag, S. Pankanti, S. Prabhakar, and A. K. Jain, "Biometric Cryptosystems: Issues and Challenges", vol. 92, no. 6, pp. 948–960, June 2004.