Available online at http://www.journalcra.com

International Journal of Current Research
Vol. 8, Issue, 08, pp.37043-37047, August, 2016

INTERNATIONAL JOURNAL OF CURRENT RESEARCH

ISSN: 0975-833X

RESEARCH ARTICLE

ENHANCING THE PERFORMANCE OF MULTIMODAL BIOMETRIC AUTHENTICATION SYSTEM

[1,*]Monika Mittal and [2]Dr. Maitreyee Dutta

[1]Department of Computer Science and Engineering, National Institute of Technical Teachers Training and Research, Chandigarh

[2]Department of Electronics and Communication Engineering, National Institute of Technical Teachers Training and Research, Chandigarh

ARTICLE INFO

Article History:
Received 22nd May, 2016
Received in revised form
10th June, 2016
Accepted 07th July, 2016
Published online 31st August, 2016

Key words:

Multibiometric, Unimodal, Encryption, Multimodal, Security.

ABSTRACT

The term Biometric has the relation with "life measurement" however the tenure is commonly interconnected by means of exclusive physiological personality to recognize an individual. A uni-modal biometric system has a diversity of problems such as noisy data, nonuniversality, spoof attacks and undesirable error rate. These limitations can be solved by deploying multimodal biometric system. Multimodal biometric authentication system makes use of two or more individual modalities, like face, iris, retina and fingerprint etc. Here we have anticipated fingerprint and iris traits at feature level extraction. Pre-processing of images of iris and fingerprint is done and features are extracted from them. Our work composed of two foremost sections: Feature extraction of both traits and fusing them before matching and appliance of an encryption technique to boost the security of the fused template and lastly matching stage to authenticate a person.

Citation: Monika Mittal and Dr. Maitreyee Dutta, 2016. "Enhancing the performance of multimodal biometric authentication system", *International Journal of Current Research*, 8, (08), 37043-37047.

INTRODUCTION

Each and every biometric attribute has its own robustness and limitations and the miscellany generally rely on the purpose. The improved biometric attribute has basically few merits namely strength, uniqueness, availability, ease of access and suitability. Fingerprints are unmatched and it is the trait that is generally employed to recognize the individual. It has high matching accuracy (Nandakumar, 2008). The supreme element of the eye in individual body is Iris (Biometric template encryption, 2010). Iris technology basically offers enhanced unique recognition. According to the overall features of iris and fingerprint they are engaged to build up the planned system. A Multibiometric scheme basically clubs the features from dissimilar biometric traits. A reliable and flourishing multimodal biometric system needs an proficient fusion scheme to combine biometric features derived from one or modalities. It also improves the template security by combining the feature sets from unlike biometric sources using appropriate fusion scheme. In this paper we proposed a framework for multimodal biometric fusion for the purpose of improving the performance of individual biometrics at feature extraction level and then fuses them together before matching. The template which is accumulated in the database will not be safe as there is a possibility of numeral attacks like alteration of template etc. Template database is encrypted using cryptography for achieving security.

Related study

Neha Singh *et al.* in (2014) introduced the concept of biometric template security. When we are using biometrics we ensure that, it is specially used for authenticating and verifying the person's template. This template can be misrepresented if it is stolen by any non-authenticate person. Rupesh Wagh *et al.* in (2013) discussed regarding how our system is secure when we are using selective encryption method for encrypting the biometric template. Lahane *et al.* in (2012) discussed that basic endeavor of a biometric scheme is involuntarily differentiate between topic as well as guard information. Multimodal biometric identification system based on iris & fingerprint trait is proposed. The Euclidean-distance matching algorithm helps in the comparison of data base template and the input data. Maheswari *et al.* in (2012) discussed that Multimodal Biometric identification system aims to fuse two or more physical or behavioral traits to provide optimal False

Corresponding author: Monika Mittal,
Department of Computer Science and Engineering, National Institute of Technical Teachers Training and Research, Chandigarh

Acceptance Rate (FAR) and False Rejection Rate (FRR). Mamta Ahlawat *et al.* in (2015) proposed the multimodal biometric system based on eye, ear and face color and proved its efficiency over existing multimodal techniques. The combination of face, ear and eye color increases the performance of biometric system. Vincenzo Conti *et al.* in (2010) introduced an innovative multimodal biometric identification system based on iris and fingerprint. The paper is a state-of-the-art advancement of multibiometrics, offering an innovative perspective on features fusion. Geetha and Radhakrishnan (2014) discussed various issues related to multimodal biometric system. Using the various Biometric traits in conjunction improves the system performance. Fingerprints and palm prints are used here. Features are extracted from them and then they are fused together. Classification of the fused features are done using support vector machine (SVM). David Marius Daniel *et al.* in (2014) introduced analyzes the performance obtained by a multimodal biometric system that combines the feature extraction level and the score level fusion of iris and fingerprint unimodal biometric systems in order to take advantage of both fusion techniques.

Proposed Multibiometric system

In this paper we had proposed an innovative multimodal biometric system for enhancing the performance of the Multimodal Biometric Authentication System. Iris and fingerprint images are taken as the inputs. Features are extracted from both of them using various techniques i.e minutia point extraction for fingerprint and hough transform for iris. Fusion is applied at this stage which is known as feature level fusion.

After the fusion, selective encryption technique is applied to the fused template for better security. To achieve security, encryption is done on the fused template. Figure 1 and Figure 2 represents the planned multimodal biometric authentication scheme. Templates are stored in the Template database. For matching process template is decrypted and matched with the fused template. If the matching score of both the templates is more than 90% then person is authenticated otherwise not.

The proposed methodology can be explained using following stepladder:

Step 1: Iris and fingerprint biometric traits will be registered using dissimilar sensors.
Step 2: From both the biometrics features will be extracted independently.
Step 3: Fusion of extracted features of iris and fingerprint will be done (i.e fusion at the feature extraction level)
Step 4: Template generated by the fusion of Iris and Fingerprint are accumulated in the template database.
Step 5: Accumulated pattern in the template database will be protected by encrypting the template using cryptography.
Step 6: Matching will be performed.

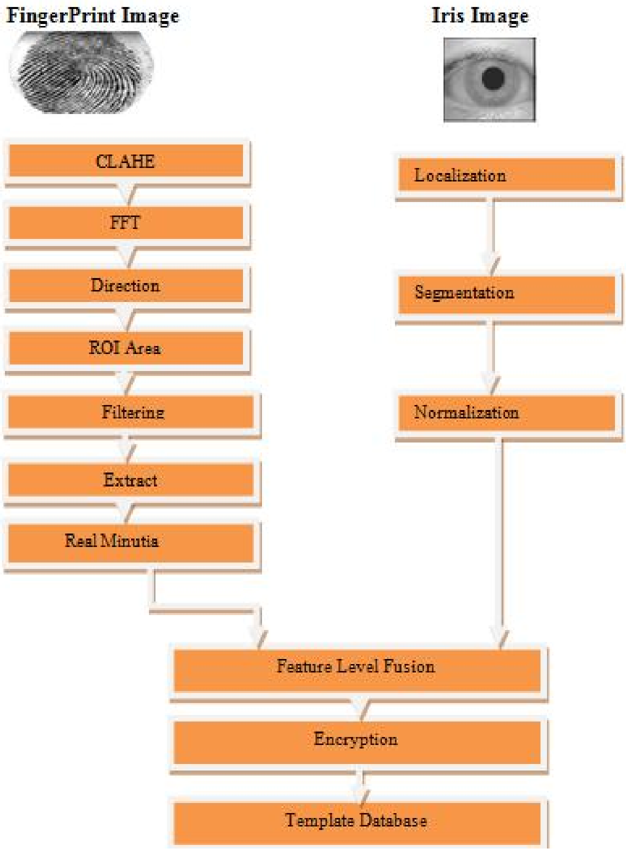


Fig. 1. Enrollment Module

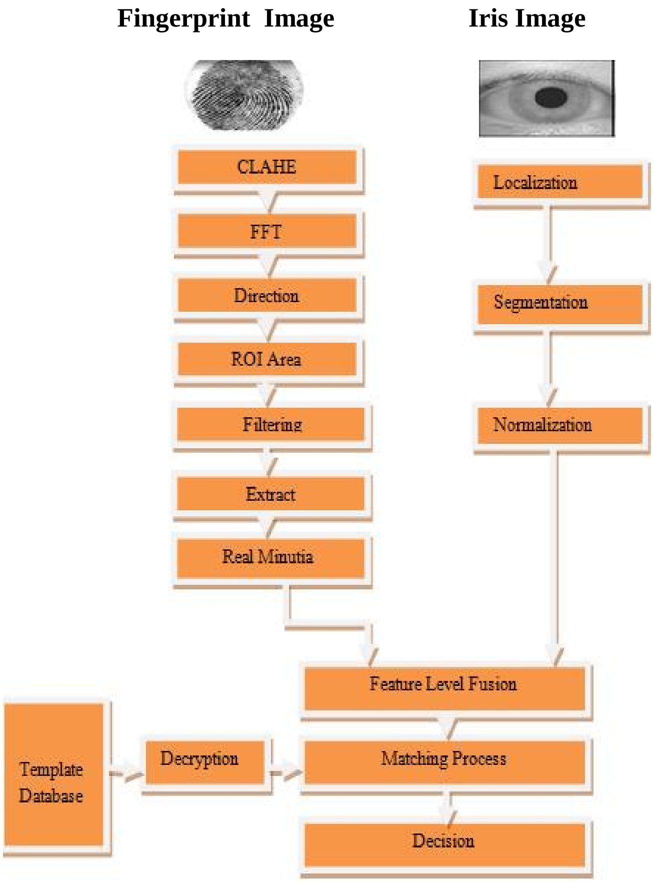


Fig. 2. Identification Module

The used unimodal biometric systems

1) Iris Identification System

Iris identification is measured to be one of the most precise biometric technologies when compare it to other technologies commercially in use these days. This is because of the reason that the false match and false no match error rate are extremely minute, which results in a very high precision. Various stages that are incorporated in Iris identification system are iris analysis, feature extraction, encoding and recognition stage. In order to establish the matching process, the distinctive parts of Iris should be encoded. This is required for producing the Iris code. In our planned scheme, binary string, segmented iris, noise removal are the functions which are employed for extracting the features from the iris images. Lastly matching will be done by employing the intended Hamming distance (HD). The computation of dissimilar bits among the two iris codes is referred to as hamming distance.

2) Fingerprint identification System

A fingerprint is collection of many ridges and furrows. For the fingerprint image preprocessing stage, we are using Histogram Equalization and Fourier Transform to do image enhancement. Region of Interest extraction is done.

- Clahe is used to improve the image's contrast.
- For segmenting the image block wise FFT is used.
- Segmentation is done so that we can separate the actual fingerprint from the background area.
- Ridge Orientation estimation is done to estimate the orientation of the fingerprint image.
- Ridge frequency estimation is done to approximate the ridge frequency for fingerprint image by isolating it into blocks of 8x8 pixels.
- Filtering is done to remove the noise and preserve ridge structure.
- Minutiae Extraction is done as minutia points are the most exclusive points of the fingerprints.

RESULTS AND DISCUSSION

For showing fingerprint enhancement we had taken two fingerprint images of the same person one is the perfect image and second is the noisy image. Enhancement techniques are applied on both the images. Finally the matching of both the images is done to show the enhancement. Clahe (contrast limited adaptive histogram equilization) is used for enhancing the contrast of both the fingerprint images as shown in the figure below. It eliminates the falsely induced boundaries.

FFT (fast fourier transform) is used to segment both the finger print images block wise. FFT improves the image by relating some falsely broken on the ridges and it also removes some false associations between the ridges

Figures 4.3 show the steps for the enhancing fingerprint images. Fig 3 shows the improved contrast of the input image using CLAHE. Fig 4 shows the application of FFT on the input image which segments it into blocks and Fig 5 shows the extracted minutia points by eliminating false minutia points.

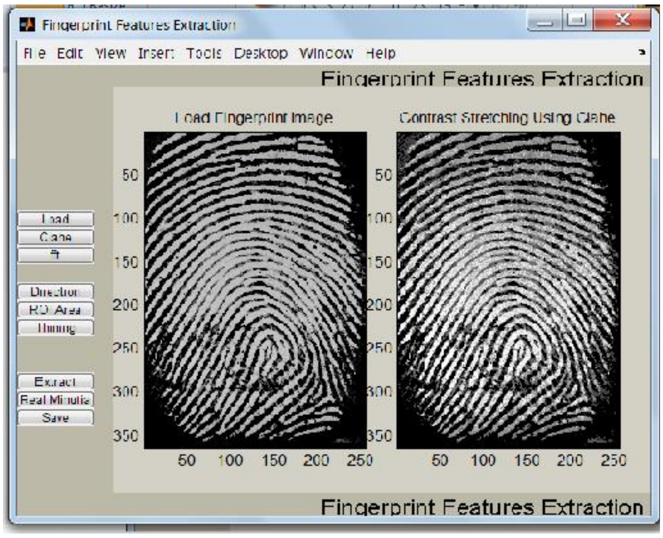

Fingerprint Features Extraction
File Edit View Insert Tools Desktop Window Help
Fingerprint Features Extraction
Load Fingerprint Image
Contrast Stretching Using Clahe
Load
Clahe
fft
Direction
ROI Area
Thinning
Extract
Real Minutia
Save
50
100
150
200
250
300
350
50 100 150 200 250
Fingerprint Features Extraction

Fig. 3. Contrast Stretching using CLAHE

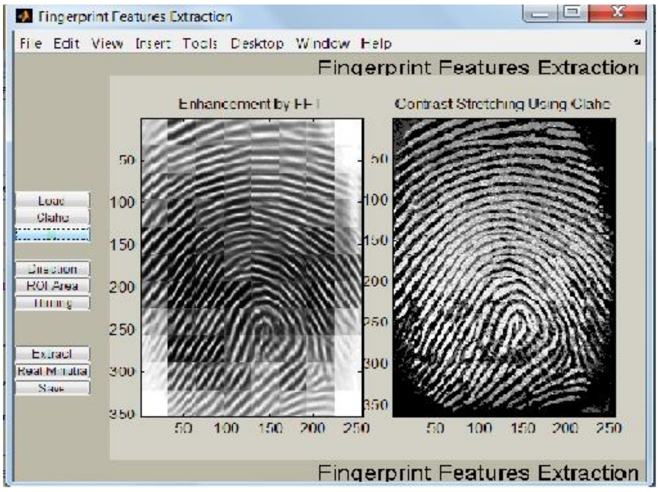

Fingerprint Features Extraction
File Edit View Insert Tools Desktop Window Help
Fingerprint Features Extraction
Enhancement by FFT
Contrast Stretching Using Clahe
Load
Clahe
Direction
ROI Area
Thinning
Extract
Real Minutia
Save
50
100
150
200
250
300
350
50 100 150 200 250
Fingerprint Features Extraction

Fig. 4. Application of FFT

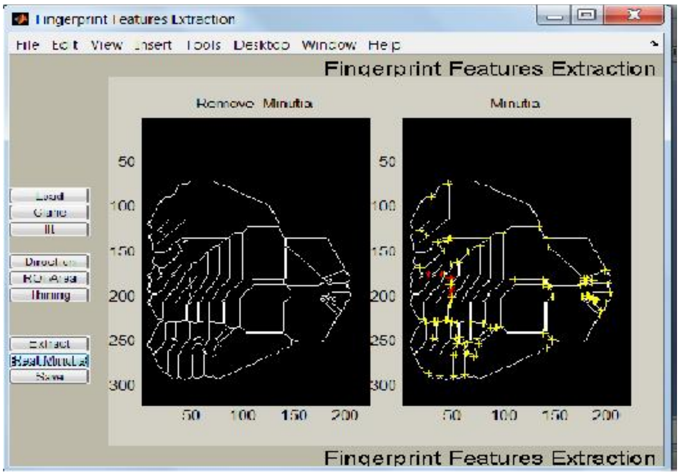

Fingerprint Features Extraction
File Edit View Insert Tools Desktop Window Help
Fingerprint Features Extraction
Remove Minutia
Minutia
Load
Clahe
fft
Direction
ROI Area
Thinning
Extract
Real Minutia
Save
50
100
150
200
250
300
50 100 150 200
Fingerprint Features Extraction

Fig. 5. False minutia points removal

Hough Transform is used for Iris enhancement. To show the iris enhancement two iris images of the same person is used. To show the enhancement hamming distance matching is done on the segmented images.

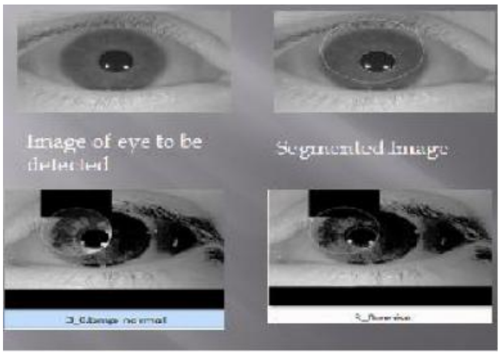


Fig. 6. Iris enhancement

Fig 6 shows the input image of eye on which the feature extraction is to be performed and the segmented image is obtained .4th level of quantization is used which results in the removal of polar noise which also shown in figure above.

Fusion of the two biometric behaviour is shown in the figure above. Fusion of the characteristics of iris and fingerprints is done into a solitary multi-biometric template that is tenable using fuzzy vault and fuzzy commitment. The fuzzy vault is basically is used for fingerprint modality where as for Iris modality fuzzy commitment is used. After fusion the encryption of the multimodal biometric modality is done. Here have used selective encryption technique which gives helpful results for the data to be secured. The fused template is determined using the encryption algorithm and a new template is obtained. On the fused output security key is applied. And so, a new template is created which is saved in the database for the person's identification at the time of verification process. To identify a person fused image of the person is decrypted from the template database and matched with the given input. And comparison is done with the fused image of the various persons as shown in the table. If the matching percentage is greater than 90% only then the person is authenticated otherwise not.

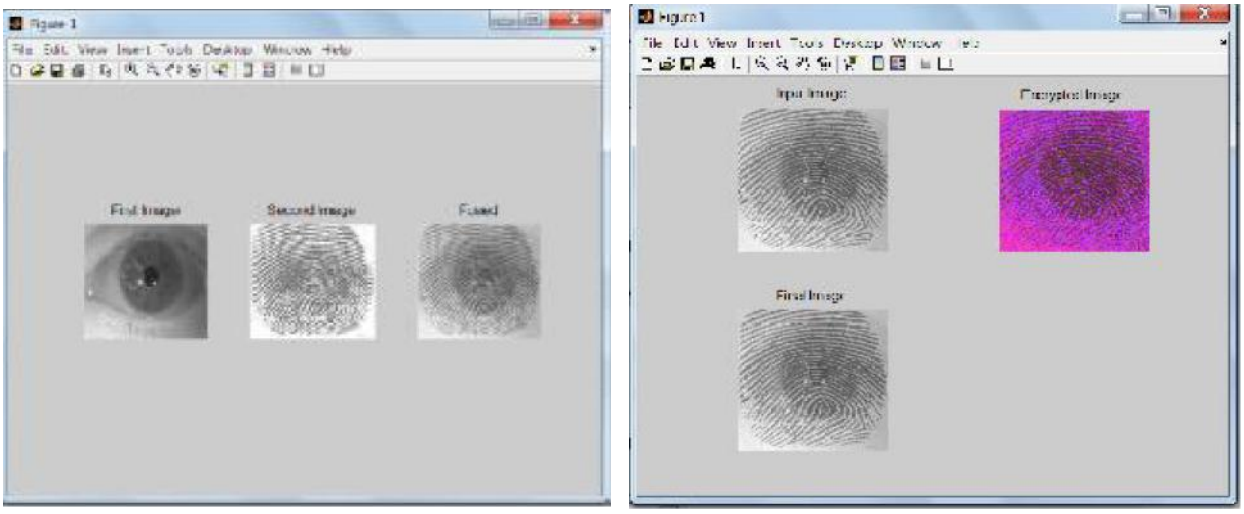


Figure 1
File Edit View Insert Tools Desktop Window Help
First Image
Second Image
Fused
Figure 1
File Edit View Insert Tools Desktop Window Help
Input Image
Encrypted Image
Final Image

Fig. 7. Fusion and Encryption of the Fingerprint and iris traits

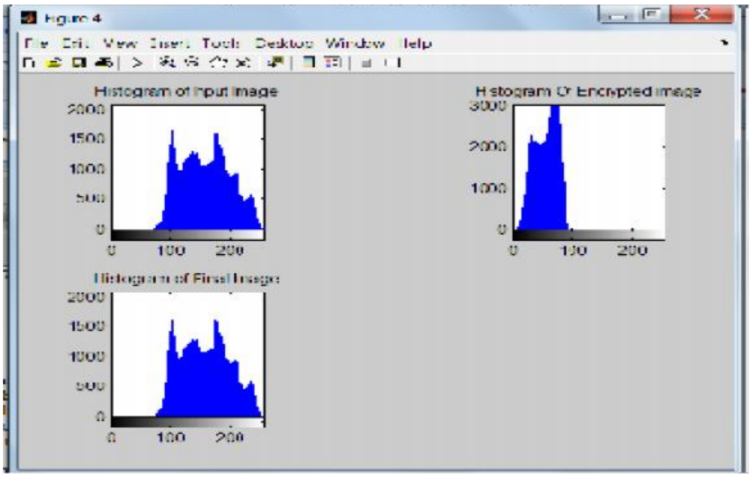
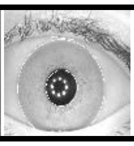


Fig. 8. Histogram of Encrypted Image

S.No	Finger image	Iris segmented image	Fused color	Encrypted image	Decrypted Image	Matcing score	Matching Score with person2	Matching Score with person3	Matcing Score with person4	Matching Score with person5
1						100%	66%	63%	71%	68%

Conclusion & Future scope

Multimodal biometrics systems provide a additional secure environment and improved accuracy. Features are extracted from both the biometric traits and then the fusion is performed at this stage which is also called as feature level fusion. The proposed technique is based on improving the performance of individual biometrics at feature extraction level and then fuses them together before matching. This is believed to be a better approach as compared to the one that involves fusion after matching. Further the security of the template database is done with the help of encryption. The proposed model is effective for segmentation of iris with less loss of features. This technique can be further enhanced in the future for iris image capture from the moving face.

REFERENCES

"Biometric template encryption" by A.K.Mohapatra, Madhvi Sandhu IGIT,GGSIP University, Kashmere GateDelhi Published in *International Journal of Advanced Engineering & Application*, Jan.2010.

Geetha, K. and V. Radhakrishnan, "Multimodal biometric system: A feature level fusion approach," IJCA, David Marius Daniel, "Combining Feature Extraction Level and Score Level Fusion in a Multimodal Biometric System", ISETC, Timisoara, pp.1-4, Nov 2014.

Jagadeesan, A. 2010. "Secured Cryptographic Key Generation From Multimodal Biometrics: Feature Level Fusion ofFingerprint and Iris", *(IJCSIS) International Journal of Computer Science and Information Security*, Vol. 7, No. 1.

Juels A. and M. Sudan, "A fuzzy vault scheme," in Proceedings of the IEEE International Symposium on Information Theory, p. 408, Piscataway, NJ, USA, June-July 2002.

Kankrale, R. N. "Template Level Concatenation of Iris and Fingerprint in Multimodal Biometric Identification Systems", 1st International Conference on Recent Trends in Engineering & Technology, Mar-2012,Special Issue of International Journal of electronics, Communication & Soft Computing Science & Engineering, ISSN: 2277-947.

Karthik Nandakumar, "Multibiometric Cryptosystems based on Feature Level Fusion".

Kevin W. Bowyer, K. I. Chang, P. Yan, P. J. Flynn, E. Hansley, S. Sarkar, "Multi-Modal Biometrics: An Overview"

Lahane, P.U., Prof. S.R.Ganorkar, "Fusion of Iris & Fingerprint Biometric for Security Purpose", *International Journal of Scientific & Engineering Research*, Vol. 3, Issue 8, August-2012 1 ISSN 2229-5518.

Maheswari M A.P, Ancy S and EbenPraisyDevanesam. K, "Biometric identification system for features fusion of iris and fingerprint", *Recent Research in Science and Technology*, 2012, 4(6): 01-04 ISSN: 2076-5061.

Mamta Ahlawat, "A Multimodal Approach to Enhance the Performance of Biometric System", *International Journal of Innovations & Advancement in Computer Science IJIACS*, Volume 4, Issue 6, June 2015, ISSN 2347 – 8616.

Mhaske, V. D. "Multimodal biometrics by integrating fingerprint and Palmprint for security", 2013 IEEE International Conference on Computational Intelligence and Computing Research.

Nalini K. Ratha, "Generating Cancelable Fingerprint Templates, IEEE Transactions On Pattern Analysis And Machine Intelligence, Vol. 29, No. 4, April 2007.

Nandakumar, K. 2008. "Multibiometric systems: Fusion strategies and template security". Ph.D.Thesis, Department of Computer Science and Engineering, Michigan State University.

Neha Singh, "Review Paper Optimizing Security of Multimodal Biometric System", *International Journal of Advanced Research in Computer Science and Software Engineering*, Vol. 4, Issue 7, July 2014 ISSN: 2277 128X.

Pooja Choudhari, "Fusion of Iris and Fingerprint Images for Multimodal Biometrics Identification", IOSR Journal of Engineering (IOSRJEN), ISSN (e): 2250-3021, ISSN (p): 2278-8719 Vol. 04, Issue 08 (August. 2014), ||V2|| PP 01-04.

Rupesh Wagh, 2013. "Analysis of Multimodal Biometrics with Security Key", International Journal of Advanced Research in Computer Science and Software Engineering, Vol. 3, Issue 8, ISSN: 2277 128X.

Sheetal Chaudhary, " A New Multimodal Biometric Recognition System Integrating Iris, Face and Voice", *International Journal of Advanced Research in Computer Science and Software Engineering*, Volume 5, Issue 4, April 2015, ISSN: 2277 128X

Ujwalla Gawande, "Fingerprint-Iris Fusion Based Multimodal Biometric System Using Single Hamming Distance Matcher", *International Journal of Engineering Inventions*, e-ISSN: 2278-7461, p-ISSN: 2319-6491 Volume 2, Issue 4 (February 2013) PP: 54-61.

Vincenzo Conti, "A Frequency-based Approach for Features Fusion in Fingerprint and Iris Multimodal Biometric Identification Systems", IEEE Transactions on systems, Man, And Cybernetics—Part C: Applications And Reviews, Vol. 40, No. 4, July 2010.

Vincenzo Conti, "A Frequency-based Approach for Features Fusion in Fingerprint and Iris Multimodal Biometric Identification Systems", IEEE Transactions on systems, Man, And Cybernetics—Part C: Applications And Reviews, Vol. 40, No. 4, July 2010.

****