ISSN (Print) : 0974-6846
Indian Journal of Science and Technology, *Vol 10(7), DOI: 10.17485/ijst/2017/v10i7/111000, February 2017* ISSN (Online) : 0974-5645

Estimation of Modified RSA Cryptosystem with Hyper Image Encryption Algorithm

D. Jagadiswary* and D. Saraswady

Department of Electronics and Communication Engineering, Pondicherry Engineering College, Pillaichavadi - 605014, Puducherry, India; jagadiswary@pec.edu, dsaraswady@pec.edu

Abstract

Generally, security, expediency and outlay are the three crucial factors influencing the espousal of biometrics. Seeing that, a newly scheme is proposed from the fused biometrics specifically fingerprint, finger vein and retina using Modified RSA (MDRSA), a public key cryptosystem used for both numeric and images. But the existing Hyper Image Encryption Algorithm (HIEA) is used only for images. Using MATLAB 2014, the performance is measured through GAR and FAR. Consequently, comparison of simulation results shows that MDRSA gives higher genuine rate of 95.3% and false rate of 0.01% which is reduced in case of HIEA, as it provides genuine rate of 92% and false rate of 0%.

Keywords: Biometric Authentication, Fused Biometrics, MDRSA, HIEA

1. Introduction

Currently, research works were carried in the field of single and multimodal biometric system. Multimodal biometric system has more advantages when compared to traditional single biometrics. Using various fusion algorithms and techniques, features are extracted and fused in case of multimodal biometric systems. Presently researchers proved that fused scores provides better discrimination than entity scores.

Author in[1] discussed fingerprint authentication technique based on minutiae feature extraction. To improve the matching performance, preprocessing and post processing stages were used in this system.

Author in[2] discussed about best accuracy from blood vessel extraction.

Author in+ projected a multibiometric based on feature level fusion followed by fuzzy logic to improve security. The planned algorithm also gives the trade-off between accuracy and security.

Author in[4] developed a technique to extract retina blood vessels using curvelet transform.

To improve the recital of finger vein, a new approach is designed by Author in[5]. Preprocessing is performed for finger vein by image enhancement and feature extraction constructed by Gabor filter.

Author in[6] proposed to bind multiple biometrics with cryptography and fusion at the biometric level. The experiment was conducted on accuracy in terms of FAR and FRR at each model.

Author in[7] clearly explains authentication server attack with its issues and challenges.

Author in[8] anticipated a system to elevate the level of security.

Author in[9] presents an overview of various biometric template which overviews about security and privacy.

Author in[10] shows preventive issues in biometrics.

Author in[11] proves the limitations of feature level fusion in comparison with score level fusion for finger print and voice.

Author in[12] proposed a multimodal based fuzzy vault using iris, retina and finger vein. In this paper, discussion is carried about biometric security using feature level fusion.

2. Proposed Multimodal Biometric System

The courses involved in biometric system are shown in Figure 1.

Feature extraction is performed for the proposed

* *Author for correspondence*

biometrics namely fingerprint, retina and finger vein. These extracted features are encrypted using hyper image encryption algorithm and encrypted images are stored in a database for comparison and matching.

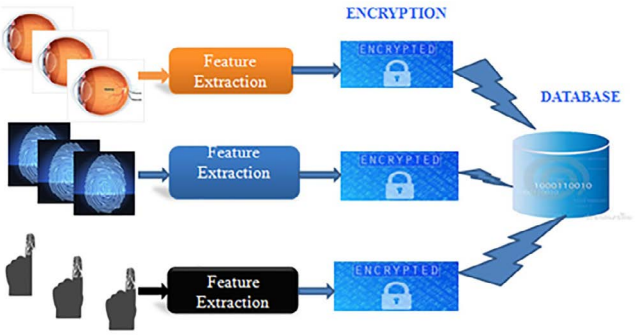

Figure 1. Proposed multimodal biometric system.

2.1 Hyper Image Encryption Algorithm (HIEA)

HIEA is a symmetric cryptographic algorithm which use block cipher instead of stream cipher. Three major steps involved in this algorithm are discussed below:

- Creation of transformation table.
- Encryption process.
- Decryption process.

2.1.1 Transformation Table

Creation of transformation table as in Figure 2.

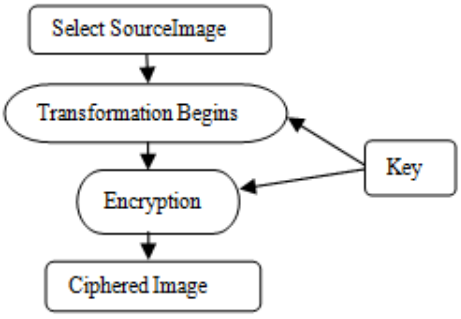

Figure 2. Clear representation of transformation table.

2.1.2 Encryption Algorithm

Feistal structure of HIEA in encryption process is shown in Figure 3.

This is block based combination of permutation and followed by encryption algorithm and the encrypted data is stored in database. When user's comes under verification, key will generate. This key is used for both encryption and decryption process.

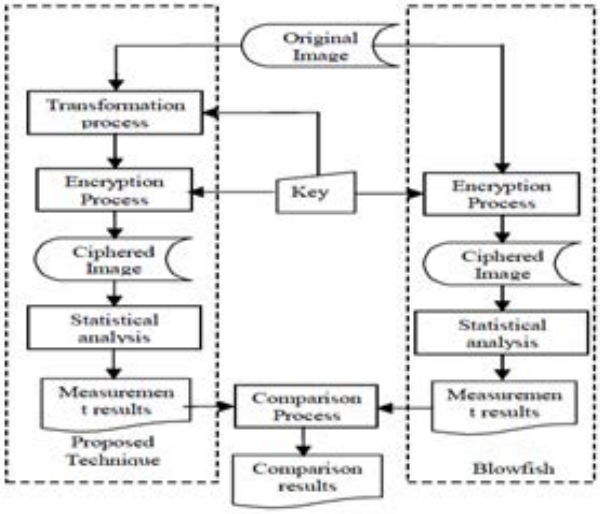

Figure 3. Steps involved in encryption.

2.2 Modified RSA (MDRSA)

RSA is a public key cryptography where public key was used to encrypt and private key for decrypt the fused biometric images. In order to acquire fine eminence of the decrypted image, the amendment was made in decryption in RSA using symmetry properties of an algorithm.

MDRSA (Modified Rivest, Shamir and Adleman) was explained by the steps shown below:

2.2.1 Key Making

Figure 4 shows the key generation process in MDRSA.

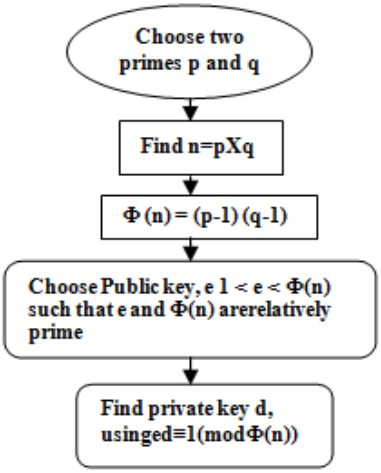

Figure 4. Key generation in MDRSA.

2.2.2 Encryption

Given message 'm' is converted to ciphertext 'C' using the equation as shown in Figure 5.

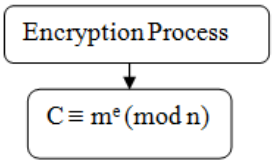

Figure 5. MDRSA encryption.

2.2.3 Decryption

Ciphertext(C) is converted to plaintext(m) using public key 'e' and private key 'd'. The steps involved in MDRSA decryption is shown in Figure 6.

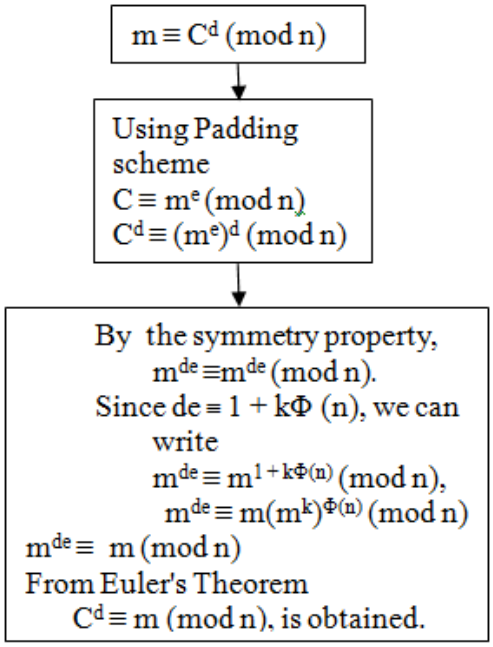

Figure 6. MDRSA decryption.

2.3 Fused Biometric Techniques

2.3.1 Finger Print Recognition

Most widely used biometric technology is fingerprint[13,14] recognition technology as given in Figure 7.

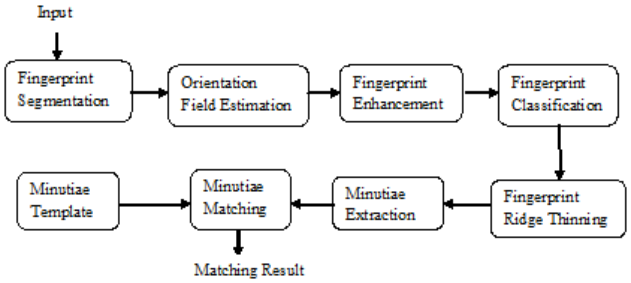

Figure 7. Fingerprint recognition process.

2.3.2 Retina Recognition

Steps involved in retina recognition[15–17] are explained as below:

- **Preprocessing** is the process which makes the input image suitable for further processing by image enhancement techniques.
- **Computation of Block Directions** determines the blood vessels area.
- Blood vessels in retina are extracted using **Segmentation**
- Extraction of blood vessels in finger vein is done using **Ridge Extraction.**
- **Minutia Extraction** determines the location and orientation of vessel bifurcation and vessel termination.
- **Post processing** is the process which eliminates extraneous minutia.

2.3.3 Finger Vein Recognition

Finger vein[18,19] recognition in biometric recognition has excellent advantages like stability, uniqueness, immunity to counterfeiting, highly accurate etc. In proposed technique, pixels are identified using line-tracking scheme. The static position of the pixel is referred as current tracking point. The maximum curvature means locates the positions that acquire the maximum curvature from the image profile, and the profiles are acquired in different direction, while all points are extracted, they are connected and combined according to the rules. Hence vein pattern is obtained by connecting the positions with each other. The resulting binary mask is used to segment the ROI from the original finger vein image samples.

3. Simulation Results

The projected multimodal biometric scheme offers better performance in terms of GAR and FAR as discussed from the below results using MATLAB 2014. For instance, GAR and FAR for fused biometric gives better result when compared with single biometric. Designed fused biometric are trained with MDRSA and HIEA and similarly without MDRSA and HIEA.

Based on identical minutiae points in fingerprint, performance was deliberated for an identity using FAR of 10% and GAR of 72%.

For retina, 78% GAR and 6.74% FAR were measured.

The extracted finger vein gives genuine rate of 80% and false rate of 5.02% as in Figure 8.

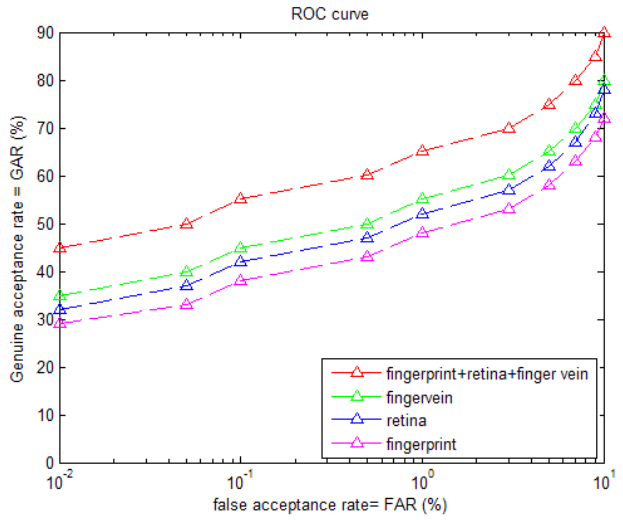

Figure 8. GAR and FAR without MDRSA and HIEA.

The multimodal biometric was trained based on fused matrix values using correlation and it's GAR of 92% and FAR of 0%. The performance of finger print using HIEA has a GAR of 78% and FAR of 5.67%. Similarly the performance of Retina using HIEA has a GAR of 83% and FAR of 3.33%.

The performance of finger vein using HIEA has a GAR of 85% and FAR of 0.78% which was shown in Figure 9.

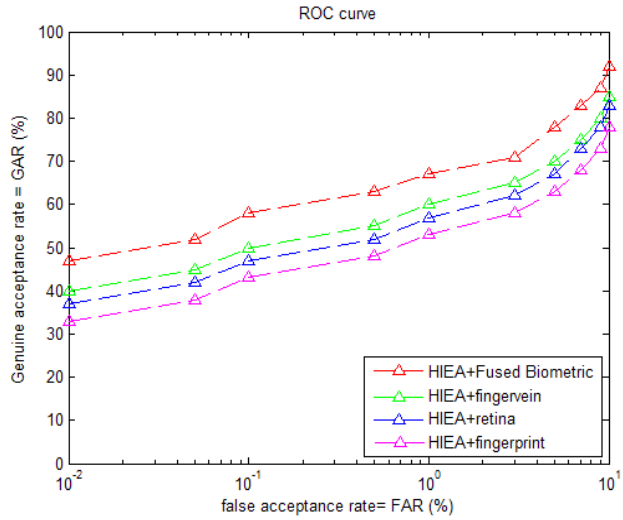

Figure 9. HIEA in terms of GAR and FAR.

The fused matrix values of fingerprint using MDRSA gives 80% GAR and 3.25% FAR whereas for Retina, MDRSA gives GAR of 84.2% and FAR of 2.2%. The performance of finger vein using MDRSA has a GAR of 87.6% and FAR of 0.52%. as in Figure 10.

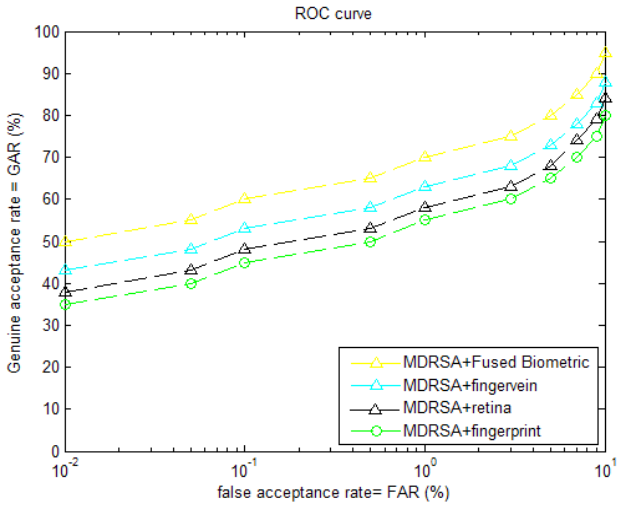

Figure 10. GAR and FAR in MDRSA.

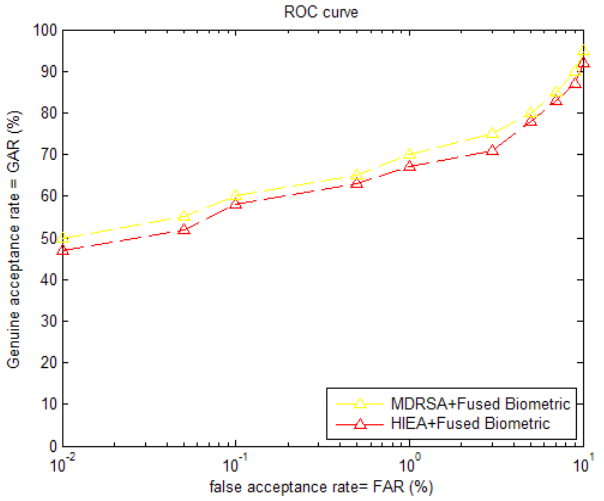

Figure 11. Performance analysis of MDRSA with HIEA.

The genuine rate of MDRSA is raised to 95.3% and lowered to 0.01% whereas GAR was 92% and FAR was 0% in HIEA as shown in Figure 11.

4. Conclusion

The primary benefit of feature level fusion is the detection of correlated feature values, generated by fused biometric which improves the recognition accuracy in terms of genuine rate and false rate. From the performance analysis of MDRSA in fused biometric, it is proved that GAR is increased to 95.3% and reduced FAR of 0.01%.

5. References

1. Jain AL. Latent fingerprint matching. IEEE Transactions on pattern analysis and machine intelligence. 2011 Feb; 33(1):88–100. PMid:2108832. Available from: Croosref
2. Marín D, Aquino A, Gegundez-Arias ME, Bravo JM. A new supervised method for blood vessel segmentation in retinal images by using gray-level and moment invariants-based features. IEEE Transactions on Medical Imaging. 2011 Jan; 30(1):146–58. PMid:20699207. Available from: Crossref
3. Nagar A, Nandakumar K, Jain AK, Hu D. Multibiometric cryptosystems based on feature-level fusion. IEEE Transactions on Information Forensics and Security. 2012; 7(1):255–68. Available from: Crossref
4. Kalaivani M, Jeyalakshmi MS, Aparna V. Extraction of retinal blood vessels using curvelet transform and Kirsch's templates. International Journal of Emerging Technology and Advanced Engineering. 2012 Nov; 2(1):360–3.
5. Kumar A, Zhou Y. Human identification using finger images. IEEE Transactions on Image Processing. 2012 Apr; 21(4):2228–44. PMid:21997267. Available from: Crossref
6. Fu B, Yang SX, Li J, Hu D. Multibiometric cryptosystem: Model structure and performance analysis. IEEE Transactions on Information Forensics and Security. 2009 Dec; 4(4):867–82. Available from: Crossref
7. Simoens K, Bringer J, Chabanne H, Seys S. A framework for analyzing template security and privacy in biometric authentication systems. IEEE Transactions on Information Forensics and Security. 2012 Apr; 7(2):833–41. Available from: Crossref
8. Kumar A, Kanhangad V, Zhang D. A new framework for adaptive multimodal biometrics management. IEEE Transactions on Information Forensics and Security. 2010 Mar; 5(1):92–102. Available from: Crossref
9. Sim T, Zhang S, Janakiraman R, Kumar S. Continuous verification using multimodal biometrics. IEEE Transactions on Pattern Analysis and Machine Intelligence. 2007 Apr; 29(4):687–700. PMid:17299225. Available from: Crossref
10. Rathod H, Sisodia MS, Sharma SK. Design and implementation of image encryption algorithm by using block based symmetric transformation algorithm. IJCTEE. 2012 Oct; 1(3):7–13.
11. Jain AK, Nandakumar K, Nagar A. Biometric template security. EURASIP Journal on Advances in Signal Processing. 2008 Dec; 1–17.
12. Jani R, Agrawal N. A proposed framework for enhancing security in fingerprint and finger-vein multimodal biometric recognition. IEEE International Conference on Machine Intelligence Research and Advancement. 2013 Dec; 440–4. Available from: Crossref
13. Elmir Y, Elberrichi Z, Adjoudj R. Score level fusion based multimodal biometric identification (fingerprint and voice). IEEE 6th International Conference on Sciences of Electronics, Technologies of Information and Telecommunications (SETIT); 2012 Mar. p. 146–50.
14. Geetika, MK. Multimodal based fuzzy vault using iris retina and fingervein. 4th International Conference on Computing, Communications and Networking Technologies (ICCCNT); 2013 Jul. p. 1–5. Available from: Crossref
15. Maltoni D, Maio D, Jain AK, Prabhakar S. Hand book of finger print recognition. 6th ed. London: Springer-Verlag Publication; 2009.
16. Fingerprint Identification. Available from: Crossref
17. Upmanyu M, Namboodiri AM, Srinathan K, Jawahar CV. Blind authentication: A secure crypto-biometric verification protocol. IEEE Transactions on Information Forensics and Security. 2010 Jun; 5(2):225–68. Available from: Crossref
18. Iris Recognition vs Retina Scanning. Available from: Crossref
19. Finger vein reader. Available from: Crossref