International Journal of Management, IT & Engineering
(ISSN: 2249-0558)

CONTENTS

Title

AN INTEGRATED CRYPTOGRAPHIC ALGORITHM BASED ON BIOMETRIC FEATURES

Author(s)

S. Sathyavathi

Research Scholar,

Karpagam University,

Coimbatore, India

P. Krishnakumari

Associate Professor,

Department of Computer Science,

Sri Ramakrishna College of Arts and Science for women,

Coimbatore. India.

Abstract:

Biometric cryptography is a technique using biometric features to encrypt the data which can improve the security of the encrypted data and can overcome the shortcomings of the traditional cryptography. Biometric features are integrated with the cryptographic techniques for better security and authentication. The proposed work concentrates on the integration of the retinal biometric features with the cryptographic techniques. Reed-Solomon (RS) error correcting algorithm is employed directly to encrypt and decrypt the data. The encrypted data generated using RS code is added to the retinal feature to obtain more secured encrypted data. To decrypt the data, the encrypted data is subtracted from retinal features to get the original data. The performance of the proposed approach is compared with the existing Iris features and the experimental results shows that FAR (False Acceptance Ratio) and FRR (False Rejection Ratio) of the proposed system has been very much reduced. In future, Multimodal Biometrics can be implemented and their performance measures like Failure to Enroll, System throughput and fraud prevention level can be estimated.

Keywords— Biometric features, Feature Extraction, RS Codes, FAR (False Acceptance Rate), FRR (False Rejection Rate).

INTRODUCTION:

In the traditional cryptographic techniques the original data is encoded by using any key so that it is not in understandable format for the attacker. The original data can be obtained by decoding the encoded data using the key. To improve the security and authentication, the biometric features are integrated with the cryptographic algorithms. Recently biometric features play a vital role in personal authentication as they are automated methods of recognizing a person based on a physiological or behavioral characteristic. Some of the features are face, fingerprint, hand geometry, iris, retina, signatures and voice. Retinal features are extracted [5] and integrated with the cryptographic techniques.

In this proposed work, the FAR and FRR values are compared between the two biometric techniques namely Iris [3] and Retina. Further fingerprint [6] is also compared with Iris. Experimental results shows that Retinal features are more secure than the Iris features.

RELATED STUDY:

Hao et al., [1] presented a technique for combining crypto with biometrics effectively. The author proposed a practical and secure way to incorporate the iris biometric into cryptographic applications. The author proposed a two-layer error correction approach that merges Hadamard and Reed-Solomon codes for deliberating on the error patterns within iris codes.

Dutta et al., [2] put forth a network security using biometric and cryptography. The author presented a biometrics based Encryption/Decryption method, in which unique key is generated using partial portion of combined sender's and receiver's fingerprints. A random sequence is produced from this unique key, which is used as an asymmetric key for both Encryption and Decryption

Zhaofeng He et al., [3] presented iris segmentation is an essential module in iris recognition because it defines the effective image region used for subsequent processing such as feature extraction. Traditional iris segmentation methods often involve an exhaustive search of a large parameter space, which is time consuming and sensitive to noise. To address these problems, this paper presents a novel algorithm for accurate and fast iris segmentation.

Cancellable biometrics gives a better performance of security as it facilitates with more than one template for the same biometric data. Ang et al., [6] proposed the measurement of the success of a particular transformation and matching algorithm for fingerprints. A key-dependent cancellable template for the fingerprint was produced by employing a key dependant geometric transform on the obtained fingerprint features.

EXISTING WORK:

The existing algorithm [4] works with Iris as its biometric technology. Encryption and Decryption process works as follows,

A. Encryption Process

The message to be encrypted is undergone a RS Encoding and then the Biometric Feature is added to the encrypted message.

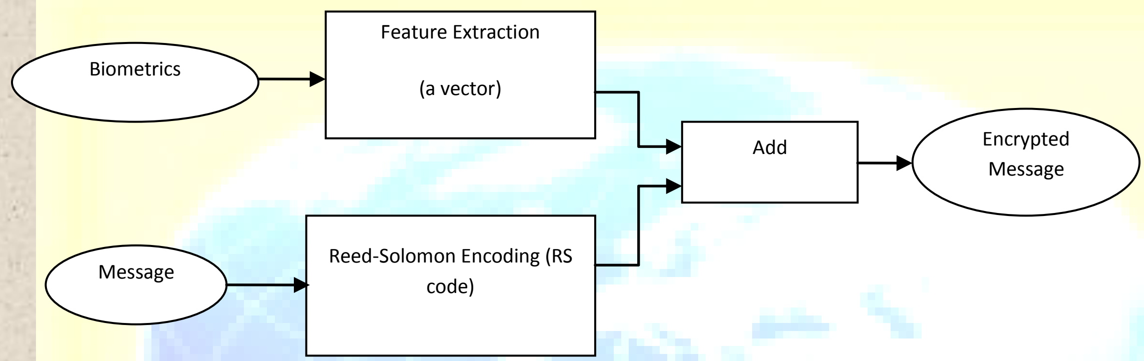

Figure 1: Encryption process

Algorithm 1 : Algorithm for Encryption

Step 1: Extract the feature vector (FV) by inputting the Iris..

Step 2: Compute the (N, K, T) RS codes of the original message, where N, K and T are the length of the RS code, the length of the message and the number of the errors this code can correct, respectively. According to Reed-Solomon algorithm, these three parameters should satisfy $K = N - 2T$.

Step 3: Add the RS codes to the feature vector to get the encrypted message.

B. **Decryption Process**

The Decryption is performed by subtracting the encrypted message from the Biometric Feature. Then RS decoding is performed to get back the original message.

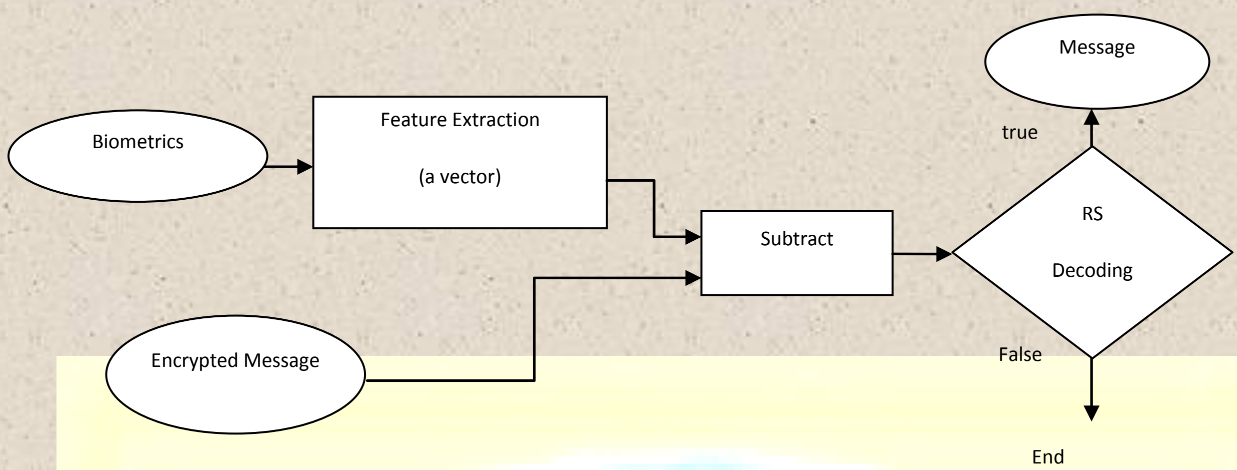

Figure 2 : Decryption Process

Algorithm 2 : Algorithm for Decryption

Step 1: Extract the feature vector (FV') by inputting the Iris.

Step 2: Subtract the feature vector from the encrypted message to get the noisy RS Code.

Step 3: Correct the error in the noisy RS Code using the standard Reed- Solomon.

II. PROPOSED WORK

In the proposed work the Iris is replaced with the Retinal feature. The proposed algorithm also has two processes namely encryption and decryption process and works as follows,

Algorithm 3 : Algorithm for Encryption

Step 1: Extract the feature vector (FV) by inputting the Retina.

Step 2: Compute the (N, K, T) RS codes of the original message, where N, K and T are the length of the RS code, the length of the message and the number of the errors this code can correct, respectively. According to Reed-Solomon algorithm, these three parameters should satisfy $K = N - 2T$.

Step 3: Add the RS codes to the feature vector to get the encrypted message.

Algorithm 4 : Algorithm for Decryption

Step 1: Extract the feature vector (FV’) by inputting the Retina.

Step 2: Subtract the feature vector from the encrypted message to get the noisy RS Code.

Step 3: Correct the error in the noisy RS Code using the standard Reed- Solomon.

Thus the proposed algorithm works with Retinal features to enhance the degree of security. The degree of security is measured using the factors like FAR (False Acceptance Ratio) and FRR (False Rejection Ratio)

III. EXPERIMENTAL RESULTS

The proposed retinal feature is experimented using two datasets namely,

- Real Time Retinal data set [http://www.sinobiometrics.com]
- DRIVE dataset. [http://www.isi.uu.nl]

The results are measured using two measures like FAR (False Acceptance Ratio) and FRR (False Rejection Ratio)

A. **Real Time Retinal data set:**

100 persons retinal images are sampled and the following FAR and FRR results are obtained.

Table 1 show the resulted False Rejection Rate (FRR) for the various biometric techniques.

TABLE 1

False Rejection Rate (FRR) (%) Comparison for Real Time Retinal data set

User	Fingerprint	Iris	Retina
1-10	9.5	6.2	4.1
11-20	9.1	7.5	3.4
21-30	8.9	6.2	3.5
31-40	8.2	7.1	3.24
41-50	8.4	7.3	3.45
51-60	8.21	6.6	3.1
61-70	9.6	7.6	3.64
71-80	8.5	6.1	3.28
81-90	9.2	6.12	3.3
91-100	8.31	6.34	3.8

Table 2 shows the resulted False Acceptance Rate (FAR) for the various biometric techniques.

TABLE 2

False Acceptance Rate (FAR) (%) Comparison for Real Time Retinal data set

User	Fingerprint	Iris	Retina
1-10	0.26	0.16	0.02
11-20	0.25	0.18	0.01
21-30	0.21	0.15	0.02
31-40	0.24	0.16	0.04
41-50	0.23	0.14	0.05
51-60	0.29	0.13	0.02
61-70	0.25	0.18	0.03
71-80	0.22	0.15	0.02
81-90	0.23	0.14	0.01
91-100	0.21	0.16	0.02

B. DRIVE data set

The Retinal images taken from the DRIVE data base are resized to the standard 256 x 256 format. 40 retinal samples are collected and is maintained in the database for various research works. Table 3 shows the comparison of FAR with various biometric techniques like fingerprint, iris and retina.

TABLE 3

False Acceptance Rate (FAR) (%) Comparison for DRIVE data set

Samples	Fingerprint	Iris	Retina
1-10	4.6	2.3	0.9
11-20	4.4	2.4	0.92
21-30	4.3	2.3	0.88
31-40	4.3	2.5	0.87

Table 4 shows the False Rejection Rate (FRR) comparison for the biometrics features like fingerprint, iris and retina.

TABLE 4

False Rejection Rate (FRR) (%) Comparison for DRIVE data set

Samples	**Fingerprint**	**Iris**	**Retina**
1-10	6.45	4.95	1.25
11-20	6.43	4.92	1.22
21-30	6.5	4.93	1.35
31-40	6.48	4.9	1.28

Table 5 shows the overall average FAR and FRR comparison of the biometric techniques for DRIVE dataset.

TABLE 5

Overall average FAR and FRR Comparison

Evaluation Measures	**Fingerprint**	**Iris**	**Retina**
FAR	4.2	2.4	0.9
FRR	6.4	4.9	1.2

From the figure 3, it is clearly observed that, the FAR of the proposed retinal cryptographic technique is 0.9%. But the FAR for the existing fingerprint and iris techniques are 4.2% and 2.4%.Similarly, FRR for the retinal cryptographic technique is 1.2% and the FAR for the existing fingerprint and iris techniques are 6.4% and 4.9%

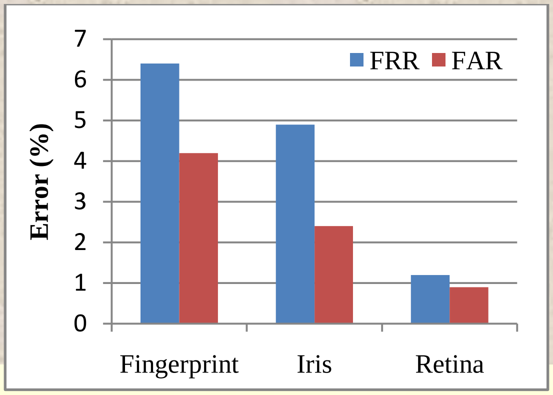

Figure 3 : Comparison of FAR and FRR of the Biometric Techniques

From the result, it can be observed that the cryptographic algorithm technique based on retinal features results in lesser FAR and FRR for all the persons, whereas the other biometric techniques like fingerprint and iris results in higher percentage of FAR and FRR.

The percentage of improvement of the proposed approach in terms of FAR and FRR is 1.5 and 3.7 compared to Iris.

TABLE 6

Percentage of Improvement

Evaluation Measures	**Retina Improvement %**
FAR	1.5
FRR	3.7

CONCLUSION:

This work mainly overcomes the drawbacks of the traditional cryptographic algorithm which uses only the cryptographic keys for the encryption and decryption process. The existing work uses Iris as the biometric measure to enhance the degree of security. In the proposed approach Retina replaces the Iris features and experimental results shows that the security of the message is increased when compared to the existing work. Such approach is used in highly secured system.

REFERENCES:

- F. Hao, R. Anderson, and J. Daugman, “Combining crypto with biometrics effectively," IEEE Transactions on Computers, Vol. 55, Pp. 1081-1088, 2006.
- Sandip Dutta, Avijit Kar, N. C. Mahanti, and B. N. Chatterji, “Network Security Using Biometric and Cryptography,” Proceedings of the 10th International Conference on Advanced Concepts for Intelligent Vision Systems, Pp. 38-44, 2008.
- Zhaofeng He, Tieniu Tan, Zhenan Sun and Xianchao Qiu, “Toward Accurate and Fast Iris Segmentation for Iris Biometrics,” IEEE Transactions on Pattern Analysis and Machine Intelligence, Vol. 31, No. 9, Pp. 1670 – 1684, 2009.
- Xiukun Li, Xiangqian Wu, Ning Qi, Kuanquan Wang, “A Novel Cryptographic Algorithm based on Iris Feature” International Conference on Computational Intelligence and Security, pp. 463-466, 2008
- K. Saraswathi, B. Jayaram and Dr. R. Balasubramanian, “Retinal Biometrics based Authentication and Key Exchange System”, International Journal of Computer Applications (0975 – 8887), Volume 19– No.1, April 2011.
- R. Ang, R. Safavi-Naini, L. McAven, “Cancellable key-based fingerprint templates," ACISP 2005, Pp. 242-252.