Edge Based Selective Encryption Scheme for Biometric Data Using Chaotic Theory

[1]Garima Mehta, [1]Malay Kishore Dutta, [2]Carlos M. Travieso-González & [3]Pyung Soo Kim
[1]Amity School of Engineering & Technology, Amity University, Noida, India, [2] University of Las Palmas de Gran Canaria,
Las Palmas de Gran Canaria, Spain, [3]Korea Polytechnic University, Korea
gmehta@amity.edu, mkdutta@amity.edu, carlos.travieso@ulpgc.es, pskim@kpu.ac.kr

***Abstract*— Security of biometric data plays a major concern due to extensive use of biometric systems in many applications. This paper proposes an efficient method for encryption of iris images using edge based encryption algorithm based on chaotic theory. In this proposed technique, the iris image is segmented into significant and non significant blocks to find region of interest (ROI) i.e. to localize iris from complete eye image from which features are extracted to generate biometric template. Selective encryption is used to encrypt the region of interest and it reduces the computational overhead and processing time as compared to full encryption techniques. The experimental results prove that edge based selective encryption significantly reduces the time of encryption of iris images as compared to full encryption method without any compromise in performance. Performance of proposed algorithm has been experimentally analyzed using key sensitivity analysis and the results prove that the encryption algorithm has high key sensitivity and the algorithm is lossless in nature.**

Keywords—Edge Based Selective Encryption, Region of Interest, Arnold Cat Map, Logistic Map

I. Introduction

Traditional methods of user authentication to gain access to secure information systems requires personal identification number, ID cards, passwords, smartcards and so on. These methods are however susceptible to the attacks by an impostors and cannot be implemented for high security systems like financial services, physical access and information security [2] where very high level of confidentiality or security is required. Therefore, in recent years with increase in concern regarding the authentication of data and user identification, biometrics has gained a lot of popularity in public and private sector as fingerprints, palm prints, iris, face, voice provides a unique, permanent and reliable solution for user authentication/identification. Out of all the available biometric traits iris recognition is considered as the most reliable and accurate method available for biometric identification system because of its stability and uniqueness. For example if we are using a fingerprint authentication and the user has a cut or wound, there can be a mismatch, in case of voice, sore throat can give a mismatch during identification.

Biometric traits have also properties like universality, authenticity, convenience [1] but there are still some issues regarding the security and privacy of biometric technology. The most vulnerable point in the biometric technology is the storage of biometric data. Hackers can hack this data and make copies of this biometric data for illegal use. To counter this vulnerability we introduce the concept of combining biometrics with cryptography. The most effective mechanism to counter vulnerability while maintaining the confidentiality is encryption. Standard encryption algorithms like RSA and DSA are not useful as intrauser variability generated different feature set for the same sample scanned multiple times. Another reason why we cannot use standard encryption methods is that the size of the biometric data is very large, thereby increasing the computational complexity and processing time.

To reduce these complexities, we introduce the concept of selective encryption. As the name suggests, we select only some part of data from the complete biometric data that is significant and encrypt that part only. Large part of data that doesn't reveal any significant information left unencrypted as this method reduces the computational complexity and processing time. Now the question arises which part of an eye image comprises the significant part. The most important part of an eye image is the iris region [9] from where unique features are taken out for template generation. To find this iris i.e. significant region we divide the complete eye image into blocks, select significant blocks and encrypt them.

The main contribution of this paper is to propose the selective image encryption algorithm on iris samples in spatial domain. The selective encryption is strategically done in a method so that those portions of an eye image are encrypted from which the features are extracted to generate biometric template. The concept of edge detection is used [7] to find the significant and non significant blocks and encryption is done on significant blocks i.e. iris region which is actually unique for every eye image. Chaotic theory [6, 8] is used to encrypt significant blocks as chaotic theory is highly sensitive to initial conditions and is pseudorandom in nature. In chaotic theory combination of Arnold cat map and logistic map [4] are used for permutation and substitution because they are highly deterministic and robust in nature. Experimental results of proposed algorithm indicates significant reduction in computational overhead and processing time which may be considered as significant contribution in comparison to full encryption.

Rest of the paper is organized as follows: Section II gives an overview of selective encryption. Section III describes the proposed image encryption/decryption algorithm. Section IV shows experimental results and efficiency of proposed algorithm and finally paper is concluded in Section V.

978-1-4799-6629-5/14/$31.00 ©2014 IEEE

II. Edge Based Selective Encryption Method

In selective encryption, edge detection method [3] is used for the segmentation of an image into significant and non significant blocks. We segment an actual iris region i.e. ROI (Region of Interest) [10] from the complete eye image by using the edge detection technique and encryption of significant region helps to distort the unique characteristics of an eye image which are used for the purpose of template matching.

Following are the steps being followed for segmentation of an iris image of size M x M:

1. Apply Edge Detector on iris image to obtain a binary edge detected output.

2. Divide detected output into desired number of blocks.

3. Total number of zeros pixels & its average is calculated by dividing total number of zeros pixels by total number of pixels per block for all the detected blocks.

4. Calculate significant block threshold by multiplying above calculated average with factor Q.

5. From the total number of detected blocks those for which zero pixel average is greater than threshold are termed as Significant Blocks leaving the rest as Non-Significant Blocks.

6. Finally a encryption vector is created where each value is either ‘1’ or ‘0’ suggesting whether a block is significant or non-significant respectively.

III. Proposed Encryption Algorithm

In the proposed algorithm we use the concept of chaotic theory [5] to encrypt the significant blocks of an iris image. Combination of arnold cat map and logistic map [4] is chosen. Arnold cat map is used for image shuffling and logistic map is used as pseudorandom key generator to substitute the pixel values. Both maps provide large key space which makes it difficult for the intruder to make the correct guess about the key structure.

3.1 Encryption Process

1. Convert the encryption vector into a square matrix.

2. Using the 1-D logistic map generate another pseudo random square matrix.

3. Divide this matrix into equal sized blocks as of the biometric data.

4. From encryption vector, check one by one for the significant and non- significant block.

5. If the detected block is significant, perform encryption such that:

- Scramble the detected block using ‘n’ iterations of Arnold Cat Map.
- Bitxor the scrambled output with the respective block of pseudo random matrix block.

6. Re-combine all the significant (encrypted) and non-significant (un-encrypted) blocks together to obtain the encrypted output.

7. Encryption vector is stored as a key and is later used for decryption.

3.2 Block Diagram of Proposed Algorithm

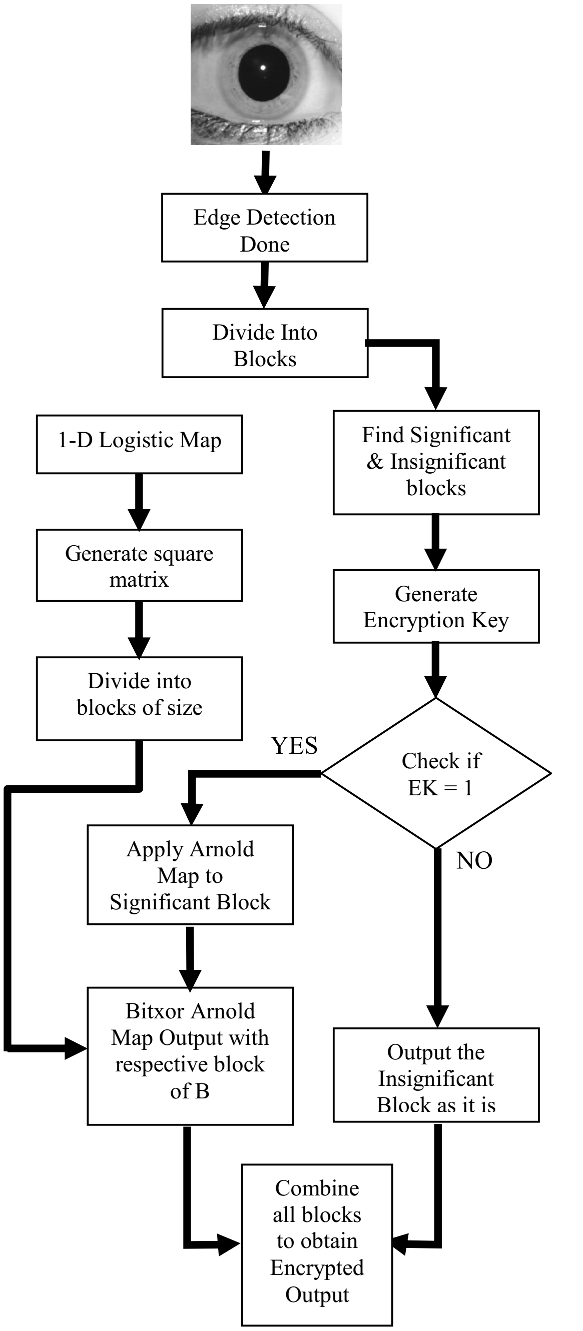

Edge Detection Done
Divide Into Blocks
1-D Logistic Map
Find Significant & Insignificant blocks
Generate square matrix
Generate Encryption Key
Divide into blocks of size
YES
Check if EK = 1
NO
Apply Arnold Map to Significant Block
Bitxor Arnold Map Output with respective block of B
Output the Insignificant Block as it is
Combine all blocks to obtain Encrypted Output

Fig 1. Proposed Encryption Algorithm

Figure 1 shows the block diagram of the proposed encryption algorithm in which encryption of significant blocks is done in spatial domain to secure the biometric data efficiently.

3.3 Decryption Process

During decryption, just the reverse of encryption steps is performed to get back the original iris image. The encryption vector is used for decryption.

1. Read the encrypted data from the stored database.

2. Read the encryption vector.

3. Using the 1-D logistic map generate another pseudo random square matrix.

4. Divide this matrix into equal sized blocks as of the biometric data.

5. Now depending upon the encryption vector, first perform the bit-xoring of the random matrix block with the encrypted image block.

6. Re-shuffle the obtained matrix using the 'p-n' iterations of Arnold Cat Map to obtain the original iris image, where p is the periodicity of the M x M image.

IV. Experimental results and analysis

4.1 Computational Time Analysis:

Experimental analysis is done on different iris samples of size 256*256. The results are presented in Table 1.

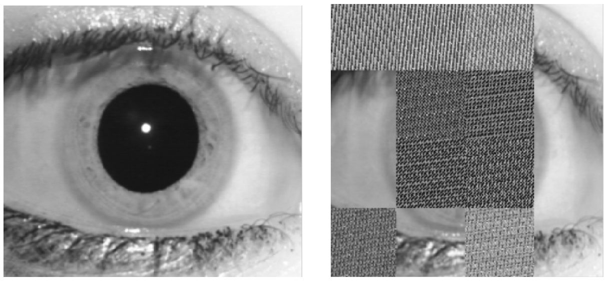
Biometric Sample	Full Image Encryption Time (sec)	Selective Image Encryption Time (sec)
Iris 1	6.95	0.83
Iris 2	6.89	0.80
Iris 3	6.93	0.83
Iris 4	6.90	0.83
Iris 5	7.08	0.80
Iris 6	6.93	0.90
Iris 7	6.10	0.96
Iris 8	6.93	0.81
Iris 9	7.02	0.83
Iris 10	6.99	0.80

Table 1: Time Taken By Full & Edge Based Selective Image Encryption

Table 1 shows significant reduction in computation time of edge based selective image encryption techniques in comparison to full image encryption techniques. The time taken in both cases is only encryption time i.e. time taken in encryption process.

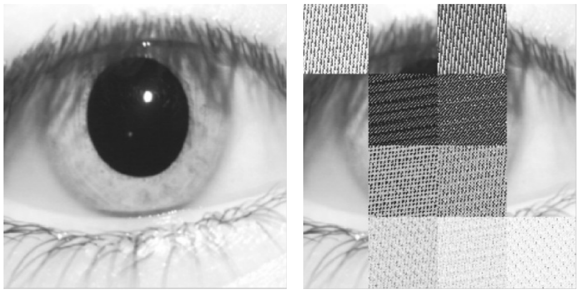
4.2 Secret Key Sensitivity Analysis

The key structure of proposed algorithm should be such that a slight variation in the value of keys of encryption vector results into an incorrect decrypted image since encryption key matrix contains the information regarding the significant blocks and non-significant blocks. Any variation in the encryption key should affect the decryption process.



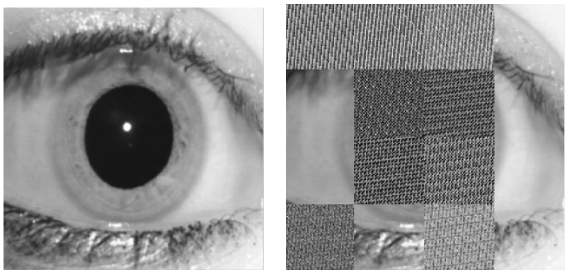
(a) (b)

Fig 2. (a) Original Image (b) Encrypted Image



(a) (b)

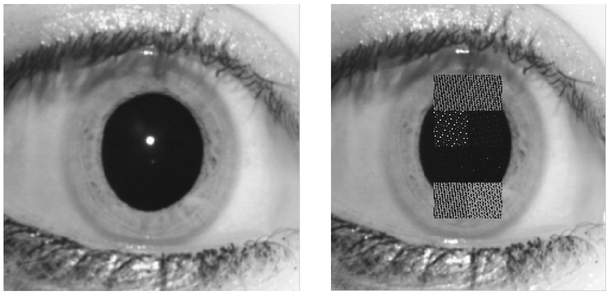
Fig 3. (a) Original Image (b) Encrypted Image



(a) (b)

Fig 4. (a) Original Image (b) Encrypted Image

Fig. 2(a), 3(a), 4(a) shows the original eye image samples and Fig 2(b), 3(b), 4(b) shows the edge based encrypted output of test eye images of size 256*256.



(a) (b)

Fig 5. (a) Decrypted Image with Correct EK
(b) Decrypted Image with Incorrect EK

Fig. 5(a) shows the decrypted image with correct key values of encryption key and Fig. 5(b) shows the decrypted image with incorrect key values of encryption key. Experimental analysis proves that proposed algorithm is highly sensitive to keys.

V. Conclusion

This paper proposes an edge based selective encryption scheme based on chaotic theory for the secure transmission of iris images over insecure network channels or storage in database. Selective encryption enhances the overall performance by encrypting only the ROI (Region of Interest) from where features are extracted to generate biometric template which overall reduces the computational time. Further key sensitivity analysis shows that to decrypt the image accurately the correct combination of encryption keys is required. This algorithm works well for color iris images and this can be extended further for other biometric traits.

References

1. Anil K. Jain, Arun Ross, Sharath Pankanti "Biometrics: A tool for Information Security", IEEE Transactions on Information Forensics and Security, vol. 1, No.2, June 2006.
2. Anil K. Jain, Karthik Nandakumar, Abhishek Nagar, "Biometric template security", EURASIP J.Adv. Signal Process. 2008.
3. Osama A.Khashan, Abdullah M. ZIN, Elankovan A. SUNDRARAJAN,"Performance Study of selective in comparison to full encryption for still visual images", Journal of Zhejiang University Science C, pp. 435-444, 2014.
4. M. K. Sabery,M.Yaghoobi , "A New approach for the image encryption using chaotic logistic map," in Proc IEEE, Phuket, pp. 585-590, 2009.
5. Y. Wang, Anqing Normal Coll., Anqing,Guangyong Ren,Julang Jiang , Jian Zhang , "Image encryption method based on chaotic map", Industrial Electronics and Applications, 2007.
6. G.Mehta, M.K.Dutta, Jan Karasek, Pyung Soo Kim, "An efficient and lossless fingerprint encryption algorithm using Henon map & Arnold transformation", Int.Conference on Control, Communication and Computing", pp. 485-489, 2013.
7. N.Taneja, Balasubramanian Raman, Indra Gupta, "Combinational domain encryption for still visual data", Multimedia Tools and Applications, pp.775-793, 2012.
8. Osama A. Khashan, Abdullah Mohd Zin, "An efficient adaptive of transparent spatial digital image encryption"Int.Conference on Electrical Engineering and Informatics, pp.288-297, 2013.
9. Muhammad H Dashtban, Parham Moradi, "A Novel and Robust Approach for Iris Segmentation", IJCA, pp.63-70, 2011.
10. Yan Li, Wen Li, Yide Ma, "Accurate Iris Location Based on Region of interest", International Conference on Biomedical Engineering and Biotechnology, pp.704-707, 2012.