128-Bit Secured Hybrid Key for Cryptographic Algorithms

S. Sridevi SathyaPriya

Department of ECE, Karunya Institute of Technology and Sciences, Tamilnadu, India

Corresponding author: S. Sridevi SathyaPriya, Email: s.d.s.priya@gmail.com

In this paper a high degree of accuracy coupled with enhanced security 128 bit hybrid cryptographic key is generated. This key is generated by considering more than one bio-metric template. Then to increase the security further, it is fused with an binding key, using the fuzzy commitment scheme. Brute force attack is applied to steal the key which is used for encryption by the hackers. The hybrid key that is generated from the multi-modal bio-metric and further fused with the binding key has high randomness than other generated keys and so it has less possibility of cracking by the brute force attack. The proposed hybrid key is more random when compared to other keys in the frequency test by 5.21%, and the frequency test for blocks by 0.2% and in the overlapping and non overlapping tests by 30%.

Keywords: Biometric key, finger print, IRIS, Cryptography algorithm, AES algorithm.

2021. In Rahul Srivastava & Aditya Kumar Singh Pundir (eds.), *New Frontiers in Communication and Intelligent Systems*, 47–53. Computing & Intelligent Systems, SCRS, India. https://doi.org/10.52458/978-81-95502-00-4-6

1 Introduction

Many online dealings and many internet services are taking place in day to day life. These online dealings and e-commerce applications contain information like bank transactions, some personal information which is has to be kept more secured and confidential data etc. The cryptographic algorithm can be used to protect information during communication. This also gives protection to the information from third parties. This will encipher the information into cipher text. This cipher text will be in an unreadable form. This information can be accessed, only by authenticated persons. These people can decipher the text in order to get the original information with the help of the key. The AES cryptographic algorithm is a symmetric algorithm which encrypts and decrypts data using the same key. The cryptographic standard is used by Centralized/Federal departments and agencies. The authentication of a person is decided by the possession of the key. The protection of the information also depends upon the secrecy of the key. Hence to increase the security of the key, it can be derived from biometrics. Now –a- days in order to provide a high degree of security, many systems use Biometric data for their applications. This is because biometrics is unique to the individual and they cannot be duplicated [1]. Unimodal biometric system, considers single biometric which may not be able to meet the increasing demand of high accuracy [1] in today's applications. The unimodal bio metric system also suffers from problems like noise, non-universality and sensitivity to attack [2]. So in this paper, for cryptographic algorithm 128 bit hybrid key is generated by considering iris and fingerprint biometrics. To increase the protection of the key further, the generated key is combined with the 128 bit random key with help of fuzzy commitment scheme. The biometric key can be used to increase the security of the information since biometrics is unique to every individual [3].

1.1 Related work

Many biometrics can be used to develop the cryptographic key like face, fingerprint, Voice, Iris, and Signature. Bio metrics are compared depending on the availability, uniqueness, and performance like speed, acceptance and durability. The Fingerprint and iris are well suited for the cryptographic algorithm because it has high performance, distinctiveness and permanence throughout the life time of the person [4].The process of generating key by considering single biometric is labelled as the unimodal system. If it considers more than one then it is named as multimodal system. Unimodal biometric systems have to withstand various problems like noisy data, e error rates. It can be overcome by using multimodal biometric [5].

From multimodal biometrics a secured cryptographic key can be generated for cryptographic algorithms. In the multimodal biometric the fusion can be done in three levels, feature level, match level and decision level. Feature level fusion provides feature set which contains rich information of the biometric data [6]. The Multimodal biometrics [14] such as fingerprint and iris features considered for key generation can be combined using fusion algorithm. Cryptographic key is generated from the combined features [7]. All the finger print feature extraction methods are classified under two categories namely Binarized Fingerprint Images, Gray Scale Fingerprint Images [8]. Thinned Binarized method preserves the connectivity of ridge structures [9]. The most identifying feature in the human face is the texture of each eye's iris. The main advantage of iris biometric is the costly to steal over other biometric [10]. This extraction of the iris texture has the following steps segmentation, Normalization and Extraction of Iris Textures. Iris image is localized and isolated from the noise in segmentation step [11]. In Iris localization, in digital eye the Iris region is isolated with the help of iris inner and outer boundary identification. This is done by canny edge detection. The gradient of the image intensity is computed using linear filtering [10]. In normalization process unwrapping of iris is done and it is converted it to polar equivalent [6]. To provide stronger security to the algorithm key, the fuzzy commitment scheme can be used [12],[13].

2 Methodology

The cryptographic 128 bit biometric key is generated from the fingerprint and IRIS. Biometric features are combined with binding key. For combining both the fuzzy commitment scheme is used [12]. This hybrid key is more random than the other biometric keys. Due to this increased randomness, the possibility of getting the brute force attack is reduced. The block diagram for generating the hybrid key is shown in Fig 1.

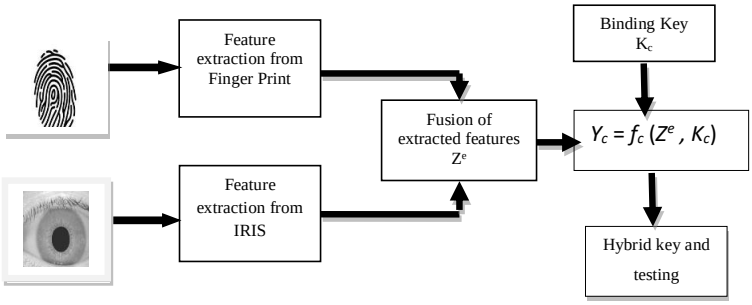

Fig 1. Block diagram for generating Hybrid Key

While generating the hybrid key, feature level fusion is done on the iris and fingerprint. There are some good advantages in multimodal biometrics like improved accuracy etc.

3 Feature Level Fusion of Fingerprint and IRIS Features

The two sets of feature extracted from fingerprint features and from the IRIS features. The extracted features are combined to generate the 128 bit fused key. The extracted features are minutiae points in the fingerprint and each minutiae point is denoted by (x, y) coordinates. Those extracted minutiae points are stored as two different vectorsX1 and X2 are constructed, x co-ordinate value is given by vector X1 and y co-ordinate value is represented by X2.

In the iris, texture properties are extracted using log-Gabor filter and these properties are complex numbers $a + ib$. Like the Finger print, in the iris, the extracted IRIS features are stored as two equivalent vectors. Vector L1 represents the real part and vector L2 represents the imaginary part. The four equivalent vectors namely X1, X2, L1 and L2 are given as inputs to the fusion process. The output of the fusion process is the multimodal biometric template. Shuffling of individual feature vectors, linking of shuffled vectors, Construction of biometric template and key generation steps are applied in feature level fusion.

Individual feature vectors shuffling: The random permutation of the individual feature vectors X1, X2, L1, L2 from the fusion. Shuffling of vectors: This process produces four shuffled vectors S1, S2, S3 and S4. This process includes the following procedure. X1 size a random vector R is generated. After the linking process, J1 and J2 linked vectors are created. Construction of multimodal biometric template: By combining the linked vectors J1 and J2, the multimodal biometric template TB is generated. The multimodal vector TB is generated from the linked vectors J1 and J2.The template vector TB is represented as Equation (1)

$$TB = [t1, t2, t3 \ldots\ldots\ldots td] \qquad (1)$$

Generation of hybrid key**:** The fuzzy commitment scheme can be used for both concealing and binding. In this paper, this scheme is used for generating the Hybrid key by combining the 128 bit

generated key. This is done by using the above mentioned process with the generated multimodal key. This scheme uses the Equation (2)

$$H_c = f_c(Z^e, K_c) \qquad (2)$$

H_c–Hybrid key using fuzzy commitment f_c- Fuzzy commitment functionZ^e-128 bit generated Cryptographic Key K_c-Binding KeyFig2 shows the generation process of the hybrid key from the 128 bit cryptographic key from Finger print and IRIS features with binding keys.

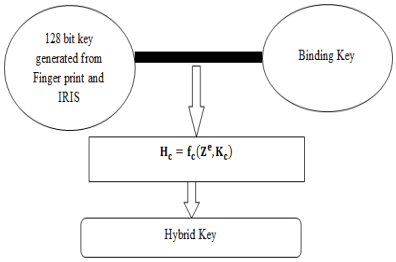

Fig 2. Hybrid key generation process

The 128 bit biometric key is generated by fusing Finger print and IRIS feature and is then combined with the 128 bit Binding key. For combining the binding key with the Generated Biometric key, the fuzzy commitment Scheme is used.

4 Extraction of Feature from Finger Print

In this paper, the 128 bit hybrid key is generated by combining the binding key with the 128 bit cryptographic key, generated from fingerprint and iris images. The iris images are then taken from the CASIA data set [18] and fingerprints are taken from National Institute of Standards (NIST) fingerprint data set [19]. The Hybrid key is generated using the MATLAB in the Windows 7 operating system. The experimental result for the fingerprint feature extraction is shown in Fig 3.

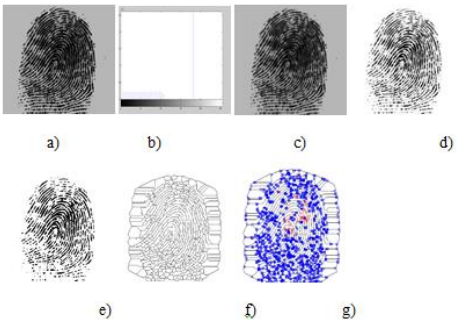

Fig 3. a) Original image b) Histogram Equalized Image c) Filtered Image d) Normalized Image e) Binary image f) Thinned Image g) Minutiae Extraction

In the pre-processing process, the Histogram equalization is used to increase the contrast of images. It also converts image range from 0 to 255 which is used to enhance visualization effect of an image. The Wiener filtering is then used to improve the legibility of the fingerprint image without affecting its ridge structures [17]. In Fig3 c) the Weiner filtered image is shown. Normalization: Each image is normalised to a predetermined level before proceeding on to the

subsequent enhancement stages. Fig3 d) shows the results of normalised fingerprint image and it has a desired mean of zero and a variance of one.

5 Extraction of Feature from IRIS

The results obtained for the IRIS feature extraction is shown in Fig 4. In the iris feature extraction, initially the segmentation process is done on the input iris image which is shown in Fig4 a). Segmentation: In this process, the centre point of the image is identified which will be useful for extracting the features from iris image and it is shown in Fig 4 b).Estimation of Iris Boundary: An extensive range of edges in images are identified by using the estimation of the iris boundary process. Fig4 c) shows the resultant image after the canny Edge detection process and Fig4 d) and also shows image after the Hough transform. Radial Suppression: The Radial Edge detection is an important tool in image segmentation. It is used to segment the iris more effectively and accurately[17] and it is illustrated in Fig4 e).Iris Localization and Normalization:Themaximum radius is defined as the space from pupil midpoint to boundaries of the right or left search region in iris localization process and this is shown in Fig4 f). In the Normalization process, the iris templates are shifted and compared in n different directions to compensate for the rotational effects and this is shown in Fig4 g).

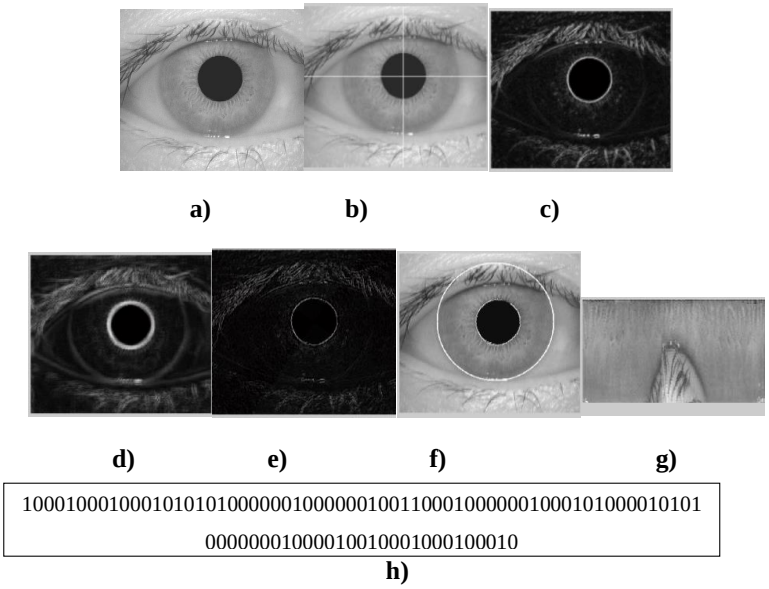

Fig 4 a) Input Iris Image, b) Centre point of image, c) Canny Edge Detection d) Hough Transform, e) Radial Suppressed Image f) Localized image, g) Normalized image h Biometric key generated from Fingerprint and iris feature

6 Generation of Hybrid Key

A 128 bit Hybrid key is generated by combining the 128 bit biometric key generated from fingerprint and iris features with binding key using the fuzzy commitment scheme.. The Mixed and Blended keys are now generated by considering a single biometric template, to increase the security furthermore. Therefore, the multimodal biometric is considered in this research work and a hybrid key is generated. The generated hybrid key using the fuzzy commitment scheme.

7 Randomness Test

In this paper, Hybrid keys are generated from the biometric template and the generated keys' randomness is tested, using a statistical test which is then, all the randomness is compared. Table 1 shows the statistical test P value for all generated keys. Various statistical tests are applied to the sequence in order to evaluate the randomness of the sequence [15]. The test is used to calculate a P-value and, each P-value states the randomness of the generated sequence. If a Randomness test P value is equal to 1, then the sequence is fully random. P-value of 0 specifies that the sequence is fully non random.

Table 1. Randomness test for all the generated keys

	Finger print Key[16]	**IRIS Based Key[17]**	**Mixed key[16]**	**Blended Key[17]**	**Hybrid key**
Cumulative sums test	0.5	0.8413	0.84	0.8413	0.8413
Frequency test	0.241	0.3329	0.859	0.317	0.8547
Frequency within a block	0.923	0.7599	1	0.8056	1
Non overlapping test	0.9989	0.99	0.9993	0.9993	0.9993
overlapping test	0.9975	0.9652	0.8994	0.938	0.9826

Table 1 is constructed from the randomness analysis. From the results, it is observed that the generated Hybrid key gives a high P-Value when compared to the other keys. This clearly depicts that this proposed method is increasing the randomness. For the Cumulative sum test, the P-Value for the generated Hybrid key is 0.8413 and in the frequency test also P-value is 0.8547 This is almost larger than the other keys. But for all the other tests, the P-Value of the generated key is greater than 0.9. In the frequency within a block test, the P-Value is equal to one, so it is completely random.

8 Conclusion

This paper a 128 bit hybrid key is generated and its randomness is tested and compared with the other keys. The Hybrid key is generated using fingerprint features and iris patterns, these biometrics are unchanging throughout the lifetime of a person. Its inter-class variability for a person is also very large. The 128 bit key is generated by combining features of fingerprint and IRIS. 128-bit hybrid key is generated by combining generated key and binding key using fuzzy commitment scheme. Thus the randomness of key is increased. So it is less prone to brute force attack. The proposed hybrid key increases the randomness when compared to the fusion key in the frequency test by 5.21%, and the frequency test for blocks by 0.2% and in the overlapping and non overlapping tests by 30%. The special scanners are needed for real time biometric images. This work can be extended by considering other biometric by generation of key for increasing security of the key.

References

[1] Gayathri, R. Ramamoorthy, "Fingerprint and Palmprint Recognition Approach based on Multiple Feature extraction", *Eur. J. Sci. Res.*, vol. 76, no. 4, pp. 514-526, 2012.

[2] H. Benaliouche and M. Touahria, "Comparative Study of Multimodal Biometric Recognition by Fusion of Iris and Fingerprint", *Scientific World J.*, vol. 2014, Id 829369, pp. 1-13, 2014.

[3] M. M. H. Ali, V. H. Mahale, P. Yannawar and A. T. Gaikwad, "Overview of fingerprint recognition system", in *Int.Conf. on electrical, electronics, and optimization techniques,* 2016, pp. 1334-1338.
[4] U. Uludag, S. Pankanti, S. Prabhakar and A. K. Jain, "Biometric Cryptosystems: Issues and Challenges", *Proceedings of the IEEE*, vol. 92, no. 6, pp. 948-960, 2004.
[5] A. K. Jain, A. Ross and S. Prabhakar, "An Introduction to Biometric Recognition", *J. IEEE Tran. on Circuits and Systems for Video Tech.*, vol. 14, no. 1, pp. 4-20, 2004.
[6] A. Jagadeesan and K. Duraiswamy, "Secured Cryptographic Key Generation from Multimodal Biometrics Feature Level Fusion of Fingerprint and Iris", *Int. J. Comp. Sci. Inf. Security*, vol. 7, no. 2, pp. 28–37, 2010.
[7] P. Balakumar and R. Venkatesan, "Secure Biometric Key Generation Scheme for Cryptography using Combined Biometric Features of Fingerprint and Iris", *Int. J. Comp. Sci. Issues,* vol. 8, no. 5, pp. 349-356, 2011.
[8] R. Bansal, P. Sehgal and P. Bedi, "Minutiae Extraction from Fingerprint Images - a Review", *Int. J. Comp. Sci. Issues*, vol. 8, no. 5, pp. 74-85, 2011.
[9] B. R. Rao et al., "Finger Print Parameter Based Cryptographic Key Generation", *Int. J. Eng. Res. Appl.*, vol. 2, no. 6, pp. 1598-1604, 2012.
[10] F. Hao, R. Anderson and J. Daugman, "Combining Crypto with Biometrics Effectively", *IEEE Tran. on Comp.*, vol. 55, no. 9, pp. 1081 – 1088, 2006.
[11] A. Boukhari, S. Chitroub and I. Bouraoui, "Biometric Signature of Private Key by Reliable Iris Recognition Based on Flexible-ICA Algorithm", *Int. J. on Comm. Network Sys. Sci.,* vol. 4, pp. 778-789, 2011.
[12] A. Juels and M. Sudan, "A fuzzy vault scheme", in *Proceedings of IEEE International Symposium on Information Theory,* IEEE Press, Lausanne, Switzerland, 408, 2002.
[13] A. Juels and M. Wattenberg, "A fuzzy commitment scheme", in *Proceedings of the 6th ACM Conf. on Comp. and Comm. Security*, 1999, pp. 28–36.
[14] W. Dahea and H. S. Fadewar, "Multimodal biometric system: A review", *Int. J. Eng. Tech.,* vol. 4, no. 1, pp. 25-31, 2018.
[15] A. Rukhin et al., "A Statistical Test Suite For Random And Pseudorandom Number Generators For Cryptographic Applications", *NIST Special Publication,* vol. 800, no. 22, 2002.
[16] S. S. S. Priya, P. Karthigaikumar and N. M. S. Mangai, "Mixed Random 128 Bit Key Using Finger Print Features and Binding Key for AES Algorithm", in *Int. Conf. on Contemp. Comput. Inform.,*. 2014, pp. 1226-1230.
[17] S. S. S. Priya, P. Karthigaikumar and N. M. S. Mangai, "GENERATION OF 128-BIT BLENDED KEY FOR AES ALGORITHM", in *Emerging ICT for Bridging the Future - Proceedings of the 49th Annual Convention of the Computer Society of India CSI,* 2015, vol. *2, pp. 431-439.*
[18] http://english.ia.cas.cn/db/201610/t20161026_169399.html
[19] http://english.ia.cas.cn/db/201611/t20161101_169922.html