A Review on Secure Key Construction Using Finger Vein Pattern

Dnyaneshwari P.Wagh[1], H. S. Fadewar [2] and G. N. Shinde [3]
[1]Ph.D Scholar, School of Computational Sciences, SRTMU,Nanded.
[2]Assistant Professor, School of Computational Sciences,SRTMU,Nanded.
[3]Pro.Vice Chancellor, SRTMU,Nanded. Maharashtra, India.

Abstract: In modern time security plays an important role in every field. The various types of media carry information like image, audio and video and protecting these from unauthorized access is an important area of active research. To provide strong security we use bio-cryptographic technique. In this paper we taken a review of cryptography key, Steganography key and fusion based key construction using finger vein pattern. Finger vein pattern are difficult to copy because blood flow needed during image capturing. Cryptography plays a very important role in data security. Steganography is the best technique for hiding the data. It is the science or art of embedding private information into the cover media with the alteration to the cover image, which cannot be easily recognized by human eyes. The key of many different sizes can be generated using these methods with minimal amount of time complexity and space complexity.

Keywords *–Cryptography key, biometric, security, finger vein, steganography.*

1. Introduction

Nowadays need of information security and permitting only the authorized users is becoming indispensable. The key like password, pin-code number can be stolen or cracked by hackers or it can be forgotten. The biometric is a technology that uses physiological or behavioral characteristics are used to authentication or used as a key. The biometric techniques like face recognition, finger print, iris, voice, keystroke, Oder. Retina, palm print, finger vein etc. [2][9] The biometric technology has many advantages in comparison to other techniques. The reason for using biometric system is easy to use, privacy, Low cost, enhanced security and accuracy. From all these biometric some have disadvantages like Artificial or simulated samples can be made, stealing of biometric characteristics of people is very difficult but in some cases the body part have been stolen to trick biometric system and in such cases the biometric data cannot be reset or replaced like password. All above disadvantages covered in finger vein biometric technology. The liveliness detection can be performed and a taken presented sample is forming live human beings or not. The vein pattern is present under the skin and cannot be seen by naked eye; therefore damaged skin will not reduce the chance of finding vein behind the skin.

Following are the some advantages of finger vein. 1) Internal nature- vein pattern are inside the skin and cannot be seen by naked eyes, therefore damaged skin will not reduce the chance of finding vein behind the skin. 2) Duplication safety- vein pattern are difficult to copy because blood flow needed during image capturing. 3) Usability- very easy to use. 4) Uniqueness- Finger vein pattern are unique even in identical twins. 5) No Indian culture restriction. 6) Fast processing. 7) Harmless - No one reported any side effect of finger vein system. Some are the disadvantages of finger vein system like light can be affect the system however for external uses there are covers to solve this problem and there are need to guidance for putting the finger correctly inside the reader because misalignment would capture wrong pattern.[9]

The hardware device used for finger vein identification for capturing a vascular network, hemoglobin play an important role by absorbing infrared light and after absorbing infrared light vein pattern are captured.

2. Cryptography

Cryptography plays a very important role in data security when transferring data from sender to receiver. In the cryptography method the original data is encoded by using any key so that it is very complicated for an attacker to understand it.[10] The original data can be obtained by decoding the encoded data using the same key. The privacy is well protected in cryptography. The biometric cryptosystem is a new technique of integrating the features of biometric with cryptography key. The physical biometric characteristics like fingerprint, face, palm print, iris, finger vein etc. from these finger vein based cryptography key gives better results. The finger vein pattern is difficult to copy because blood flow needed during image capturing.

3. Steganography

The main role of steganography is to hide the secret message in to a cover. Steganography is the perform of hideing a file, message, image, or video within another file, message, image, or video. The word steganography combines the Greek words steganos meaning covered or protected, and graphein meaning writing.

The advantage of steganography is that the planned secret message does not attract attention to itself as an object of inquiry. Whereas cryptography is perform of protecting the contents of a message alone, steganography is concerned with concealing the fact that a secret message is being sent as well as concealing the contents of the message.

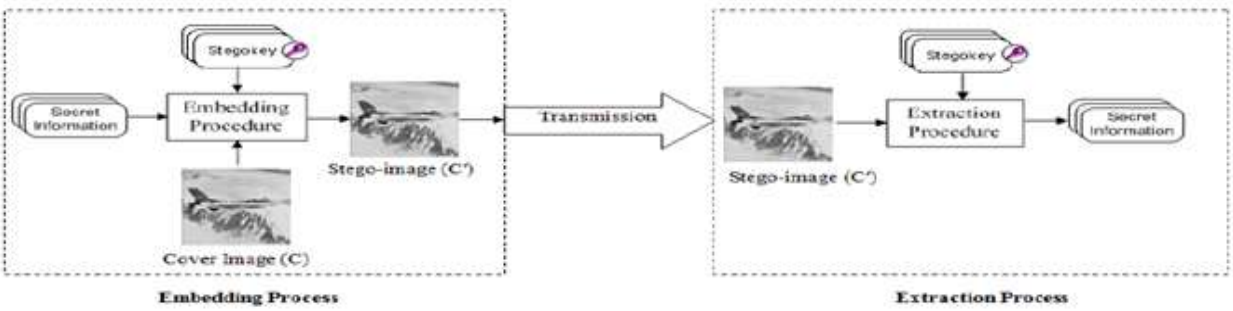

Figure 1. steganographic key structure

4. Literature Survey

Fusion based key generation

In 2010, A. Jagadeesan et.al. [2] introduced a multimodal biometric cryptographic key construction using fingerprint and Iris to provide better security. The features, minutiae points and texture properties are take out from fingerprint and Iris images respectively. The extracted features are fused together and construct a 256-bit secure cryptographic key. The experimental results gives effectiveness of the proposed approach.

In 2011, P.Balakumar et.al. [8] introduced the implementation if fingerprint and iris biometrics to secure the system. The features obtained from these two biometrics are combined using fusion technique. From that create a key which is more secure than other methods. The experimental results show better security than the existing techniques.

In 2012, Shanthini, B. et.al. [12] introduced Traditional security mechanisms are not sufficient for the appliances so biometric security is a very promising technology; challenges are slowing its development and deployment. Fingerprint images and face images are chosen due to their unique physiological traits. Multimodal biometrics can be used for several security services and this is proved in health care systems and ATM transactions.

In 2014, Minakshi Kumari et.al. [3] introduced the palm and Iris based strong protection on secret project. The gabor wavelet based Iris recognition system and wavelet packet based system is used for authentication.

In 2015, Saad Abuguba et.al. [14] Proposed an efficient approach to cryptographic key construction from face feature and Iris feature. They generate 256-bit cryptographic key.

In 2016, Saritha Reddy Venna et.al. [9] introduced a new bio-cryptography key. The cryptography key generation method uses dual finger vein pattern images. Both patterns are subjected to pre processing and then the features are extracted. The feature vector of both the images are fused to create a 256-bit length cryptography key is used in the encryption and decryption for secure transmission of data.

Steganography + cryptography key

In 2010, Madhumita Kathuria [11] proposed a technique for integrating together cryptography and steganography through image processing. she present a system able to perform steganography and cryptography at the same time using images as cover objects for steganography and as keys for cryptography using vein biometric characteristics.

In 2016, Manjari Benhar Peethala ei.al. [4] introduced the biometric system can be securing the ecommerce transaction in future. They focuses on two level protection i.e. biometric cryptography followed by steganography. The complexity of this algorithm is less as compare to other multimodal biometric system.

In 2016, Anjana Yadav ei.al. [1] proposed integrates elliptical cryptography with RSA and biometric steganography for high security. This method result is reduction in size of key.

Cryptography based key

In 2015, M. Gobi et.al. [5] proposed Elliptic curve cryptography and Hyper Elliptic curve cryptography based biometric authentication system. They implement key and compared the results.

In 2015, J. Chavez-Galaviz et.al. [13] introduced a cryptosystem based on finger vein authentication. The tinned vein pattern could be obtained in preprocessing and segmentation process. The DES algorithm is applied for data encryption and decryption key.

In 2016, G. Kanimozhi et al. [7] introduced a cryptosystem based on finger vein confirmation. They assemble a device to get infrared figures where the finger vein appears as a dark network. To remove background of finger and finger vein enhancement was implemented and after segmented and a tinned vein pattern could be obtained. The vein crossing point and angle between the branches at those point where calculated to get the pattern. The DES step used for encryption and decryption and they construct a finger vein based cryptography key.

In 2017, A. Rubba et.al. [10] used the finger print can derive the information from the key, the key formed by using fingerprint is more advantage and can be applied in PC access and internet security, Physical area security, Employee record check, mobile phone and mobile financial transaction.

5. Conclusion

In this paper we have studied different key construction techniques i.e. cryptographic key, steganographic key and fusion based key using finger vein. We selected finger vein based key construction technique because it gives better result as compare to other physiological biometric methods. Different authors proposed different techniques and also measure the performance of the techniques using parameters. The key can be used in the consecutive process of encrypting and decrypting the information for individual communication in the network.

References

[1] Anjana Yadav and Pankaj Rakheja , " Integration of Elliptical Cryptography with RSA and Steganography using Biometric Authentication", International Journal of Computer Applications (0975-8887) Volume 144 – No.4, June 2016.
[2] A. Jagadeesan, T.Thillaikkarasi, Dr.K.Duraiswamy, "Cryptographic Key Generation from Multiple Biometric Modalities: Fusing Minutiae with Iris Feature", International Journal of Computer Applications (0975 – 8887) Volume 2 – No.6, June 2010.
[3] Minakshi Kumari, Somesh Kumar Dewangan, "High Security System Provided By Steganographic Technique Using Palm and Iris Scan", International Journal Of Engineering And Computer Science ISSN:2319-7242 Volume 3 Issue 11 November, 2014 Page No. 9270-9272.
[4] Manjari Benhar Peethala and Sujata Kulkarni, "Integrating Biometric Cryptosystem with Steganography for Authentication", 2016 IEEE International WIE Conference on Electrical and Computer Engineering (WIECON-ECE) 19-21 December 2016, AISSMS, Pune, India

[5] M. Gobi and D. Kannan, "A Secured Public Key Cryptosystem for Biometric Encryption," IJCSNS International Journal of Computer Science and Network Security, VOL.15 No.1, January 2015.

[6] Yuo-Jen Chang, Wende Zhung, and Tsiihun Chen, "BIOMETRICS-BASED CRYPTOGRAPHIC KEY GENERATION", 2004 IEEE International Conference on Multimedia and Expo (ICME).

[7] G.Kanimozhi, A. Shaik Abdul Khadir, " Cryptosystem Based On Finger Vein Patterns Using Vas Algorithm" , International Journal Of Scientific & Technology Research Volume 5, Issue 05, May 2016 Issn 2277-8616.
[8] P.Balakumar[1] and R.Venkatesan, "Secure Biometric Key Generation Scheme for Cryptography using Combined Biometric Features of Fingerprint and Iris", IJCSI International Journal of Computer Science Issues, Vol. 8, Issue 5, No 2, September 2011 ISSN (Online): 1694-0814.
[9] Saritha Reddy Venna, Ramesh Babu Inampudi, "A Novel Method for Cryptographic Key Generation Fusing Dual Finger Vein Images" , (IJCSIT) International Journal of Computer Science and Information Technologies, Vol. 7 (6) , 2016, 2569-2573.
[10] A. Rubba, G.Rajkumar, K.Parimala, " Biometric based Cryptographic key generation using Finger Print" , International Journal of Computer Engineering in Research Trends, Volume 4, issue 6, June- 2017, pp.259-262.
[11] Madhumita Kathuria, "Performance Enhancement of Identification System using Vein Biometric with Modified Run Length Encoding, Stegnography and Cryptography", International Journal of Computer Applications (0975 – 8887) Volume 12– No.8, December 2010.
[12] Shanthini, B. and S. Swamynathan, "Multimodal Biometric-based Secured Authentication System using Steganography" , Journal of Computer Science 8 (7): 1012-1021, 2012. ISSN 1549-3636.
[13] J. Chavez-Galaviz, A. Garcia-Gonzalez," Embedded Biometric Cryptosystem Based on Finger Vein Patterns", 12th International Conference on Electrical Engineering, Computing Science and Automatic Control (CCE) Mexico City, Mexico October 28-30, 2015.
[14] Saad Abuguba, Milan M. Milosavljevic and NemanjaMacek, " An efficient Approach to generate Cryptographic keys from face and Iris Biometrics Fused at the feature level", International Journal of Computer Science and Network security, VOL.15 No.6, June 2015.