



Biometric Security based on Reversible Data Hiding with RZL Code and Elliptic Curve Cryptography

Dr.M.Gobi¹, Mrs.R.Sridevi²

¹Department of Computer Science, Chikkanna Government Arts College
Tiruppur, Tamil Nadu, India

²Department of Computer Science, PSG College of Arts & Science
Coimbatore, Tamil Nadu, India

Abstract: Cryptography and Steganography are the two prevalent tactics for protecting the data over the network traffic. Proposed is a system of combining together these approaches to improve data privacy. Elliptic Curve Cryptography is used for encrypting the personal information before applying RZL Coding so as to increase the PSNR. A histogram pair based image reversible hiding is used for RZL coding so as to embed the encrypted secret information into the biometric image such as thumb impression. Zhang et al. proved that the method using RZL is better increasing the performance of data hiding than the method without using it. With a popular Elliptic Curve Cryptography rational to the secret data before RZL for image hiding will improve the privacy of secret data to an extent.

Keywords: Elliptic Curve Cryptography, Reversible Data Hiding, PSNR (Peak Signal to Noise Ratio), RZL, Privacy

I. Introduction

Over last two decades, due to conflicts of environment over the internet the concerns about confidentiality of information have increased at outstanding rate. Therefore preventing unauthorized information access has been a key consideration for growing use of steganography techniques for applications like copyright protection, feature tagging and secret communication [1].

As is renowned, cryptography is a conventional way that has a long history for secure communication. The main idea of cryptography can be illustrated as the following: The information-sender uses a key to translate the secret information (the plaintext) into a meaningless bit stream (the cipher text) and transmits it to the recipient by means of an un secure communication channel, and the intended recipient would decrypt the cipher into the plaintext with a secret key that has been exchanged in advance. The benefit of cryptography is that involuntary recipients can't interpret the cipher text without the secret key even when they get the whole cipher text. But on the other hand, because the cipher text is an irregular bit stream, which flags the fact that some sensitive information is being transmitted, the communication would attract illegal parties' attention and request a danger of being decrypted or even being destroyed.

Steganography, a branch of information hiding techniques, is another way for safe communication. The main idea of steganography is to embed the secret information into a dissimilar plain digital media, such as an image, a piece of video or audio, and transmit this slightly reformed digital media to the intended recipient without attracting illegal observers' attention, so that the recipient can get the sensitive information secretly. Superficially, the advantage of steganography is that it successfully covers the fact that some sensitive information is being transmitted, so that this method can avoid attracting attackers' attention. This method not only is simple but also maintains good visual or aural quality.

Steganography also outsides a risk that the secret information might be extract illegitimately by a third party when he knows the very steganography protocol. In view of the respective advantages and disadvantages of steganography and cryptography, we can naturally get an idea that combining them in practice, then the new method would concurrently hold the advantages of steganography and cryptography while avoid the respective defects. And there have been a lot of works applying this idea and one may refer to [2-8], they encrypt the secret information firstly and then hide them in the digital media. But the common thing is that they all do the encryption and hiding separately [9].

II. Preliminaries

A. Elliptic Curve Cryptography

1) *Key Generation*: Key generation is an important part where we have to generate both public key and private key. Here, Elliptic curve cryptography algorithm is used to generate both of these keys. The sender will encrypt the message with receiver's public key and the receiver will decrypt it using his own private key. For this key generation, select a number 'd' within the range of 'n', which is the random number representing the maximum limit. Using the following equation, the public key, Q can be generated.

$$Q = d * P \quad (1)$$

d = the random number that we have selected within the range of (1 to n-1).

P = is the point on the curve.

'Q' is the public key and 'd' is the private key.

2) *Image Encryption*: Assume the original image is in uncompressed format and each pixel with gray value falling into [0, 255] is represented by 8 bits. Denote the bits of a pixel as $pb_{i,j,0}, pb_{i,j,1}, pb_{i,j,2}, \dots, pb_{i,j,7}$, where (i,j) indicates the pixel position, and the gray value as $p_{i,j}$. Thus

$$pb_{i,j,k} = \left\lfloor \frac{p_{i,j} \bmod 2^k}{2^k} \right\rfloor, \quad k = 0, 1, 2, \dots, 7 \quad (2)$$

and
7

$$p_{i,j} = \sum_{u=0}^7 pb_{i,j,u} \cdot 2^u \quad (3)$$

In encryption phase, the exclusive OR results of the original bits and key bits are calculated.

$$PB_{i,j,k} = pb_{i,j,k} \oplus PU_{i,j,k} \quad (4)$$

Where $PU_{i,j,k}$ are the public keys generated using Elliptic Curve Cryptography. Then, $PB_{i,j,k}$ are concatenated in order as the encrypted data. A secure asymmetric block cipher is used here to ensure that anyone without the key pair, such as a potential attacker or the data hider, cannot obtain any information about original content from the encrypted data.

B. Data Embedding using RZL Coding

Uniformly distributed binary random original data m can be transferred to RZL code c, in which the number of "1" will be less than that in original data, but c has length increasing. That is: $S1 < S0$ with $L1 > L0$, where $S0$ and $S1$ are the number of "1" in original data m and in the RZL code c, respectively. And $L0$ and $L1$ are the length of original data m and that of the RZL code c respectively. Both parameters σ and λ are adopted to describe the function of RZL, where $\sigma = S1/S0$ is the decrement rate of the number of "1" and $\lambda = L1/L0$ is the increment rate of length. Above all, we know there are two factors of RZL coding:

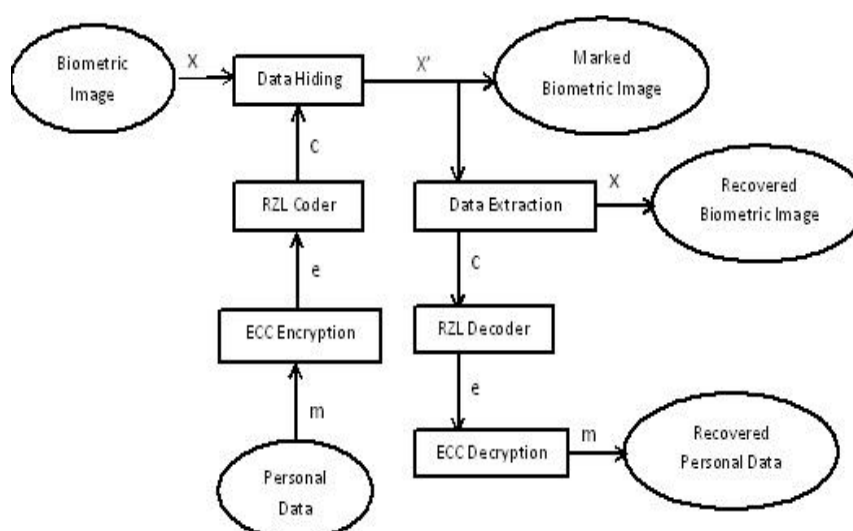
- Decrease the rate of 1, this factor is useful to raise the PSNR for Histogram-pair based Image Reversible Data Hiding,
- Increase the length of data, this factor is disadvantage to reduce the PSNR for Histogram-pair based Image Reversible Data Hiding.

Whether raising or reducing PSNR by RZL depends on payload and image [10].

III. Proposed System

Fig. 1 shows the Biometric Cryptosystem of histogram-pair based reversible data hiding with the RZL coding and ECC encryption, where x is original image, x' is the marked image. A person's personal secret information 'm', which is to be stored in a secure manner is encrypted using an efficient Asymmetric Cryptosystem, Elliptic Curve Cryptography which uses private and public key to enable the secure data to be encrypted to get the cipher text. The encrypted data 'e' is being embedded within the persons biometric data like fingerprints, iris or even in face image using RZL Coder which in turn uses histogram pair based image hiding technique. This cover biometric image after embedding is stored in a public server, which is eminent for various types of threats. The person for his authenticity initially extracts his encrypted personal information from his biometric image using RZL Decoder to recover the original biometric image and the encrypted data. Then the data is decrypted using ECC Decryption to get back the original information which is very private to that person. This method uses a very effective asymmetric cryptosystem ECC to keep the information very private from the hacker.

Fig. 1 Biometric Cryptosystem based on reversible data hiding with RZL Code and ECC Encryption



IV. Conclusion

The capability of biometrics-based personal identification techniques to differentiate between an authorized person and an impostor who deceptively acquires the access privilege of an authorized person is one of the main reasons for their popularity compared to outdated identification techniques. However, the security and integrity of the biometric data itself are important issues. Encryption, watermarking, and steganography are possible techniques to secure biometric data. In this paper, two applications of cryptography and steganography to secure that data are presented. In addition to image hiding, encryption can also be used to further increase the security of biometric data. The first application is related to increasing the security of biometric data exchange, which is based on steganography. In the second application, we embed thumb impression in fingerprint images. In this application, the data is hidden in such a way that the features that are used in fingerprint matching are not significantly changed during encoding/decoding. As a consequence, the verification accuracy based on decoded/embedded images is very similar to that with original images. We are currently working on increasing the data hiding capacity of the host images.

V. References

- [1] Souvik Bhattacharyya, Indradip Banerjee and Gautam Sanyal, A Novel Approach of Secure Text Based Steganography Model using Word Mapping Method (WMM), International Journal of Computer and Information Engineering Issue 4, Volume 2, 2010.
- [2] T. Sharp. An implementation of key-based digital signal steganography, *Proceedings of 4th Information Hiding Workshop*, LNCS, Vol.2, pp.137, Berlin: Springer-Verilog, 2001, pp. 13–26.
- [3] R.Z. Wang, C.F. Lin, J.C. Lin. Image hiding by optimal LSB substitution and genetic algorithm. *Pattern Recognition*. Vol.34 (3), 2001, pp. 671–683.
- [4] X.L. Li, B. Yang, D.F. Cheng, T.Y. Zeng. A Generalization of LSB Matching. *Signal Processing Letters, IEEE*, Vol. 16(2), pp. 69-72, 2009.
- [5] C.K. Chan, L.M. Chen. Hiding data in images by simple LSB substitution, *Pattern Recognition*. Vol.37 (3), 2004, pp. 469–474.
- [6] K. Bhowal, A.J. Pal, G.S. Tomar, P.P. Sarkar, Audio Steganography Using GA. *Computational Intelligence and Communication Networks (CICN)*, 2010 International Conference on 2010, pp.449-453.
- [7] J.K. Mandal, M. Sengupta, Steganographic Technique Based on Minimum Deviation of Fidelity (ST MDF). *Emerging Applications of Information Technology (EAIT)*, 2011 Second International Conference on. 2011, pp. 298-301.
- [8] I.C. Lin, Y.B. Lin, C.M. Wang. Hiding data in spatial domain images with distortion tolerance, *Comput. Stand. Inter.* Vol.31 (2), 2009, pp.458–464.
- [9] ZHANG Xin-peng; WANG Shuo-zhong. Steganography using multiple-base notational system and human vision sensitivity, *Signal Processing Letters, IEEE*, 2005. Vol.12(1), pp.67 - 70.
- [10] Xuefeng Tong, Guorong Xuan, Guangce Shen, Xiaoli Huan, Yun Q. Shi, Using RZL Coding to Enhance Histogram-pair Based Image Reversible Data Hiding, 2013.