A New Model of Securing Iris Authentication Using Steganography

Zaheera Zainal Abidin[1], Mazani Manaf[2], and Abdul Samad Shibghatullah[3]

[1] Faculty of Information and Communication Technology,
Universiti Teknikal Malaysia Melaka, Hang Tuah Jaya, 76100 Durian Tunggal, Melaka
[2] Faculty of Computer & Mathematical Sciences, UiTM, Shah Alam, 40450, Selangor
[3] Faculty of Information and Communication Technology,
Universiti Teknikal Malaysia Melaka, Hang Tuah Jaya, 76100 Durian Tunggal, Melaka
zaheera@utem.edu.my, mazani@tmsk.uitm.edu.my,
samad@utem.edu.my

Abstract. The integration of steganography in biometric system is a solution for enhancing security in iris. The process of biometric enrollment and verification is not highly secure due to hacking activities at the biometric point system such as overriding *iris template* in database. In this paper, we proposed an enhancement of temporal-spatial domain algorithm which involves the scheme of Least Significant Bits (LSB) as the new model which converts iris images to binary stream and hides into a proper lower bit plane. Here, the *stego key*, *n*, will be inserted into the binary values from the plane which concealed the information; where *n* is the input parameter in binary values which inserted to the *iris codes, m*. These values produce the output which is the new *iris stego* image after binary conversion. Theoretically, the proposed model is promising a high security performance implementation in the future.

Keywords: LSB, PSNR, FAR, stego key, coverimage, message and stegosystem.

1 Introduction

Biometric utilize physical traits (gait and voice recognition) or behavioral characteristics (iris, retina, thumbprint and face) for a reliable identity of authentication. The usage of iris biometric technology and application has increased tremendously for its user friendliness, performance, permanence, accuracy and uniqueness. There are many systems and machines use biometric in daily activities for instance, attendance system, withdrawing money from ATM and thumbprint to switch on laptop. In fact, in biometric, human is the key to access systems. Biometrics data is powerful [1] and useful to the system [2][3]; however, they have no keys [4]. The biometric data is easy to steal [4] or leading to identity theft and not secured [5]. The more a biometric data is used, the less secret it would be [2].

Due to these problems, steganography has been rediscovered and expanding the security performances in iris biometric systems. Steganography is the art and science

J.M. Zain et al. (Eds.): ICSECS 2011, Part I, CCIS 179, pp. 547–554, 2011.

of hiding information in a cover document such as digital images in a way that conceals the existence of hidden data. The word steganography in Greek means "covered writing" (Greek words "stegos" meaning "cover" and "grafia" meaning "writing"). The main objective of steganography is to hide the true message which is not visible to the observer and securing the database and transmission channel. The intruder should not be able to distinguish in any sense between cover-image and iris stego. Therefore, the iris stego should not diverge much from original cover-image.

Steganography conceals encrypted message from intruders; hiding the information with information to camouflage the observer who unable to comprehend the message.

It differs with watermarking. The technique of watermarking is just to hide the image with another image, with no key. The cryptography itself is insufficient to secure the iris image since it scrambles the message with the encryption algorithm. The encrypted message creates curiosity to the intruders or observers to decrypt the intended message and gives a success to hacker who able to hack the biometric system. Cryptography protects the contents of a message while steganography is to protect both messages and communicating channel. There are cases which, the iris image can be fooled and easily cracked by the hacker.

In [6][7][8][9][10], Discrete Wavelet Transform (DWT) is distinctive and widely used for embedding the iris image which improving the recognition accuracy from tampering. Meanwhile, [6][8] [11][12][13] used the LSB as the embedding scheme. Most of the researchers combine the algorithms to sustain a better security performance. On the other hand, use a single scheme with a different or other property, for instance Haar transformation is used to create the water sign to the respective image [10]. The [11] use the blind extraction with LSB to prevent unauthorized use, and inappropriate user to the system. According to [6], LSB is better scheme comparing with DWT. This is because the PSNR for LSB is 48 while DWT is 9.2.

However, most of the researches are in biometric data watermarking and information hiding. In [11], the iris steganography implementation is only for iris recognition process. The algorithms have been improved [12] however the stego key is not inserted into the binary stream. In this study, we propose a modification to the temporal spatial domain by enhancing the algorithm with the insertion of stego key into the iris codes for both enrollment and verification processes.

2 A General Process of Steganography

The concept of securing the information is almost similar between steganography and cryptography. Cryptography encrypts the information to unreadable codes however; steganography is not only encrypts but hide the information at the same time. Major differences between them are in terms of techniques, applications and technologies.

Three basic techniques used by [15] for steganography are injection, substitution and generation. The first technique of injection is to hides the data (in the form of text, image video or audio) with a cover file (in the form of text, image, video or audio). The second technique is to apply the substitution into the (data+cover file). Here, the Least Significant Bits (LSB) mechanism is useful for embedding information. The least significant bit means the 8th bit of the message is changed to a bit of secret message as in Figure 2. It determines a meaningful content with least distortion. The third technique is generation, which is generating a cover file for solely hiding the information, producing a stego file.

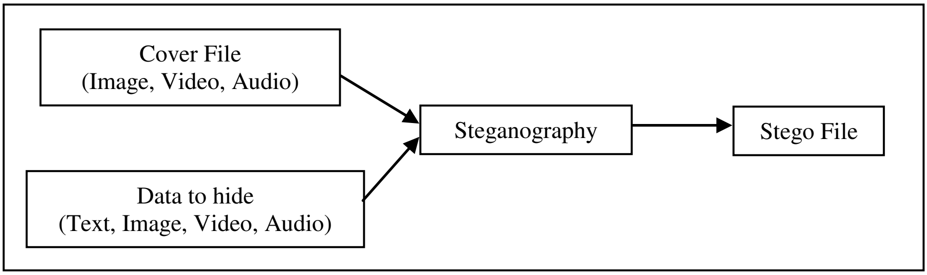
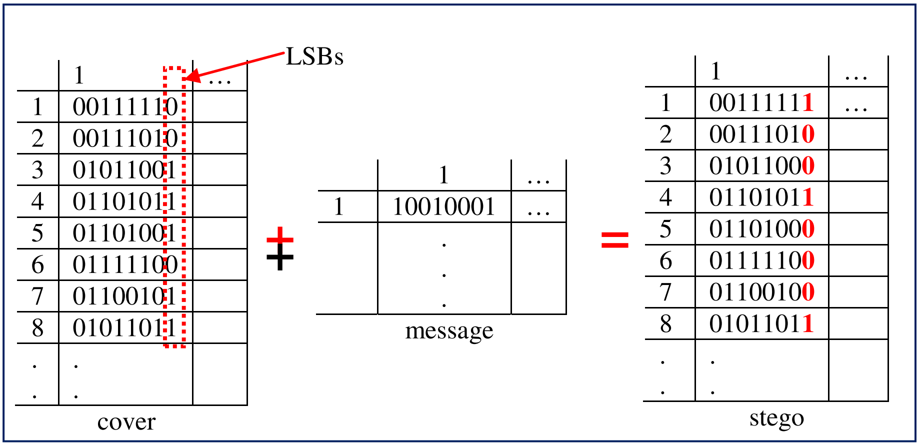


Fig. 1. General process of hiding data [15]



cover

	1	…
1	00111110	
2	00111010	
3	01011001	
4	01101011	
5	01101001	
6	01111100	
7	01100101	
8	01011011	
. .	. .	

message

	1	…
1	10010001	…
	. . .	

stego

	1	…
1	00111111	…
2	00111010	
3	01011000	
4	01101011	
5	01101000	
6	01111100	
7	01100100	
8	01011011	
. .	. .	

Fig. 2. LSB insertion at the 8th bits

Studies show that there is no established framework of implementing steganography into biometric images. The propose model of securing iris using steganography is explained in section 3.

3 A Propose Model of Iris Steganography

Biometric consists of two general processes which is the enrollment and verification. The enrollment process collects the biometric images, which is the iris image using extraction algorithms. Meanwhile, the verification stage involves matching and detraction algorithms. The integration of the steganography properties is implemented into the biometric enrollment and verification processes, as in Figure 3 and 4; in section 3.1 and 3.2. Steganography has three properties which are:

- key generation algorithm (SK) : takes as input parameter n and outputs a bit string sk, called the stego key.
- steganographic encoding algorithm (SE) : takes as inputs the security parameter n, the stego key (sk) and a message (m), {0, 1} l, to be embedded and outputs an element c of the coverimage space C, which is called iris stego. The algorithm may access the coverimage distribution C.
- steganographic decoding algorithm (SD) : takes as inputs the security parameter n, the stego key (sk), and an element c of the coverimage space C and outputs either a message m {0, 1} l or a special symbol ?. An output value of indicates a decoding error, for example, when SD has determined that no message is embedded in c.

For all sk output by SK(1n) and for all m {0, 1} l, the probability that SD (1n,*sk*,SE(1n, *sk*, m)) 6 = m, must be negligible in n. The syntax of a stegosystem as defined above is equivalent to that of a (symmetric-key) cryptosystem, except for the presence of the coverimage distribution. The probability that the decoding algorithm outputs the correct embedded message is called the reliability of a stegosystem. Indeed, it has no public or private key to be hacked; the key is embedded in the template itself.

The steganographic decoding algorithm is done at the verification process, Figure 4. The verification is a 1:1 matching process, where the user claims an identity and the system verifies whether the user is genuine or vice versa. If the iris code of the claimed identity has a high degree of similarity with the database, then the claim is accepted as “genuine” or else, the claim is rejected and the user is considered as “fraud”. The evaluation testing is going to be implemented to the proposed model. This is for achieving the security performance which is based on the performance parameter, by taking the percentage of False Acceptance Rate (FAR) and the value of Peak-Signal-to-Noise Ratio (PSNR).

In biometric system, FAR measures the percentage of invalid inputs which are incorrectly accepted which it is used to identify between the imposter and genuine user of the system. Meanwhile, in steganography, the performance measurement for image distortion is known as PSNR. The performance of PSNR is in decibels (dB), which providing system’s robustness and the accuracy that benchmarking to the new proposed system. It is expected that the larger PSNR values indicates the higher performance. On the other hand, a smaller PSNR means there is huge distortion between the cover-image and the iris stego. We assume that LSB is better from DWT, since [6] showed in their study, the value of PSNR for LSB is greater than DWT. Therefore, in calculating the value of peak–signal-to-noise-ration (PSNR), which is used for measuring the invisibility of the watermark and normalized correlation (NC).

The definition of PSNR and NC is as follows:

$$PSNR = 10 \text{ X } (\log(255^2/MSE)) \tag{1}$$
$$\text{Where } MSE = \sum_{x=0}^{N-1} \sum_{y=0}^{N-1} (f(x,y) - g(x,y))^2 / N^2$$

where f(x,y) and g(x,y) stand for the pixel values of the original iris image and the iris image with secret information.

$$NC(W.W^*) = \frac{\sum_{i=1}^{N} Wi \,.\, Wi^{\,*}}{\sqrt{\sum_{i=1}^{N} Wi}^{\;2} \,.\, \sqrt{\sum_{i=1}^{N} Wi*^{2}}} \tag{2}$$

Where W is the original iris code and W* is the extracted iris code. NC is in the range of [0,1], which represents the similarities between W and W*.

The temporal spatial domain is enhanced by inserting the stego key into the binary stream and focus on the BMP format type. [14] provides the formula of brightness : **I = 0.3R + 0.59G + 0.11B**, which define the colour component of green, red and blue. Each colour pixel can be concealed by another data. The effect of brightness is **2^0 x 0.59 = 0.59**. If it is the red colour component, the effect of brightness is **2^0 x 0.3 = 0.3**. If the fisrt 2 bits of the blue component are altered, the effect on the brightness is **(2^0 + 2^1) x 0.11 = 0.33**. Therefore, all of the effects are not greater than the maximum change in brightness in LSB which is 0.59. This means an increase in hiding efficiency about 17% [12]. The stego key is inserted into the binary stream in providing the impact to hiding result.

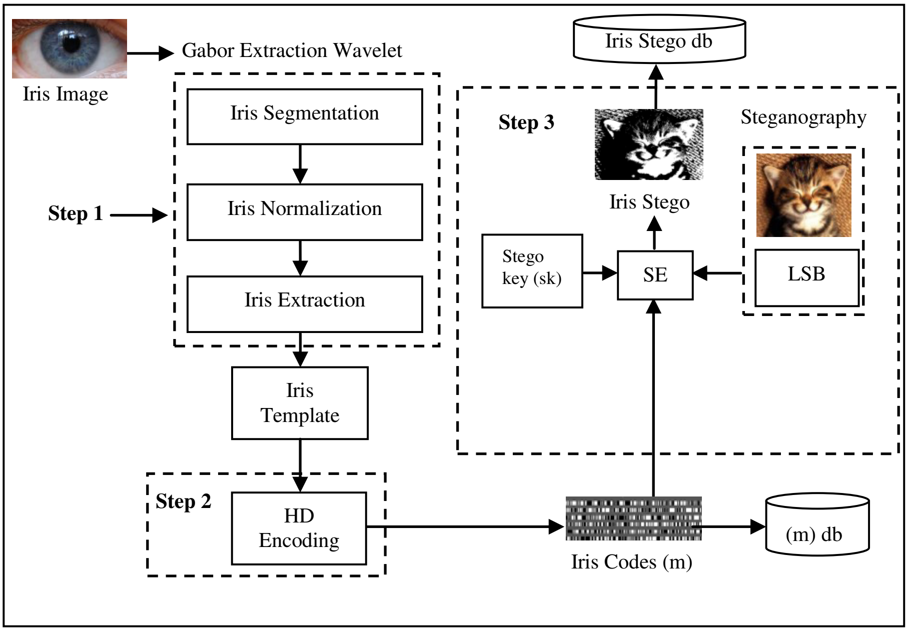


Fig. 3. Iris Enrollment Process

3.1 Iris Enrollment Process

Step 1: The iris image is segmented, normalized and extracted using Gabor Extraction Wavelet. This step produces an iris template.

Step 2: The iris template is encoded with Hamming Distance Algorithm, HD to determine between imposter and genuine. This step produces iris codes.

Step 3: The iris codes is converted in binary before moving to the embedding process. During this step, the cover image (binary) and stego key (binary) is inserted using the LSB algorithm. The value of this combination, gives iris stego in binary.

3.2 Iris Verification Process

Step 1: In de-embedding phase, SD, the iris stego is de-embedded with stego key insertion and LSB algorithm. This process produces iris codes.

Step 2: The iris codes is decoded using Hamming Distance. The decoded iris codes are converted to be iris template.

Step 3: The iris template is extracted using Gabor Wavelet and produce the iris image.

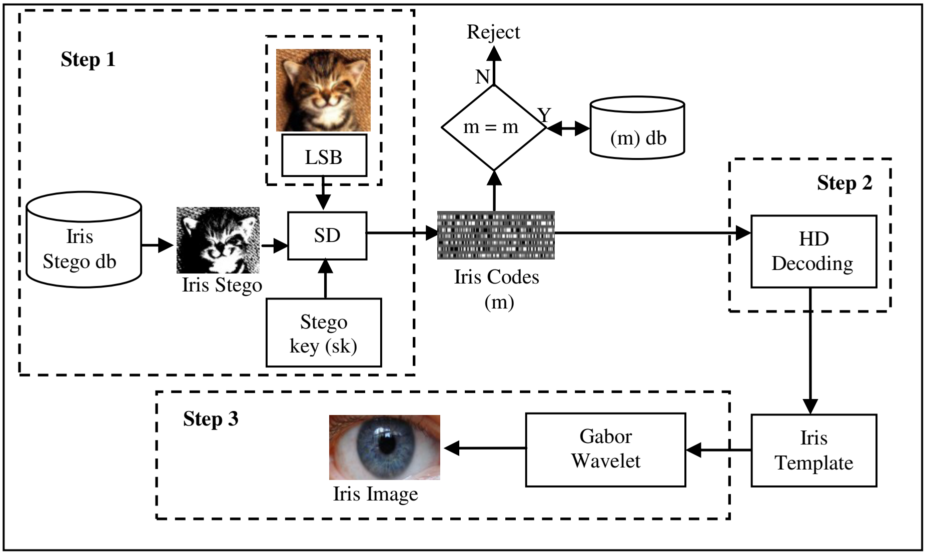


Fig. 4. Iris Verification Process

4 Discussion

How secure is the biometric iris authentication against attacks? Biometric data is easy to steal and has no key. Fake contact lenses with both eyes image on it and use it for illegal activities is one of the trend to attack the system. The biometric threats give different attack at different points in biometric authentication system. The attack launched at the sensor, seize the channel, modify the template and override the biometric templates. Is cryptography process in not sufficient enough to secure the biometric templates, where it has public and private keys to protect the iris template? The encrypted iris code creates a curiosity to the hacker to decrypt the secret keys and most of hackers understand how to do cryptography. Here, we propose the implementation of steganography into the biometric systems which is the new model of temporal-spatial domain algorithm enhancement. A stego-key, coverimage and value of n have been applied to the system during embedment in producing the iris stego. Without the valid key, it is difficult for a hacker to understand the embedded message. However there is a limitation and issues need to be explored in the implementation of LSB on iris images for example the processing time for verifying the genuine. If a longer time takes for a matching process, this gives opportunities for hacker to attack the existing system.

5 Conclusion

Biometric usage is rising and widely accessible in most countries. In fact, the biometric providers have delivered biometric authentication for mobile transactions and client/server based applications. Sustained improvements in the technology will increase performance at a lower cost. However, biometric templates leave traces and traits along the human movements. A new innovation on securing the iris authentication model needs to produce. Therefore, a new model of securing iris is designed with the integration of steganography into the biometric system. The importance of steganography has been apprehended against cryptography and information hiding due to capabilities, security services and performance. Steganography is emphasis on avoiding detection and possibilities of largest hidden massage meanwhile watermarking is robust, emphasis on avoiding distortion of cover file and a small amount of hidden message. The comparison of previous implementations and future model promise a successful achievement. Finally, our contribution of this study is to design and develop iris model for protecting the biometric system against imposter attack, making the iris biometric system more secure with the implementation of steganography.

References

1. Bhargav, A., Squicciarini, A., Bertino, E., Kong, X., Zhang, W.: Biometrics-Based Identifiers for Digital Identity Management. In: ACM International Conference Proceeding Series, Proceedings of the 9th Symposium on Identity and Trust on the Internet, pp. 84–96 (2010)
2. Anderson, R.J.: Security Engineering: A Guide to Building Dependable Distributed Systems. Wiley, New York (2001)
3. Jain, A.K., Ross, A., Prabhakar, S.: An Introduction to Biometric Recognition. IEEE Trans. on Circuits and Systems for Video Technology 14(1), 4–19 (2004)
4. Schneier, B.: The Uses and Abuses of Biometrics. Communications of The ACM 42(8), 136 (1999)
5. Hao, F., Anderson, R., Daugman, J.: Combining Crypto with Biometrics Effectively. IEEE, Transactions on Computers 55(9), 1081–1088 (2006)
6. Xiao, M.-m., Yu, L.-X., Liu, C.-J.: A comparative Research of Robustness for Image Watermarking. IEEE, Computer Science and Software Engineering 6(12-14), 700–703 (2008)

7. VijayKumar, Dinesh: Performance Evaluation of DWT Based Image Steganography. In: IEEE, 2nd International Advance Computing, pp. 223–228 (2010)
8. Fouad, M., Saddik, A.E., Petriu, E.: Combining DWT and LSB Watermarking to Secure Revocable Iris Templates. In: International Conference on Information Science, Signal Processing and their Applications, pp. 25–28 (2010)
9. Zebbiche, K., Khelifi, F., Bouridane, A.: An Efficient Watermarking Technique for the Protection of Fingerprint Images. Journal of Information Security, 20 (2008)
10. Varbanov, G., Blagoev, P.: An Improving Model Watermarking with Iris Biometric Code. In: ACM, International Conference on Computer Systems and Technologies, pp. 5-1 – 5-6 (2007)
11. Das, S., Bandyopadhyay, P., Paul, S., Ray, A.S., Banerjee, M.: A New Introduction Towards Invisible Image Watermarking on Color Image. In: IEEE, International Advance Computing Conference, pp. 1224–1229 (2009)
12. Deng, H., Xie, M., Zhang, L., Yao, Z.: An Improved LSB Information Hiding Algorithm and Its Realization by C#. In: IEEE, International Forum on Information Technology and Application, pp. 759–763 (2009)
13. He, H., Zhang, J., Chen, F.: Block-wise Fragile Watermarking Scheme Based on Scramble Encryption, pp. 216–220 (2007)
14. Lu, H., Wan, B.: Information Hiding Algorithm using BMP Image. Journal of Wuhan University of Technology 28(6), 96–98 (2006)
15. Mehboob, B., Faruqui, R.A.: A Steganography Implementation. IEEE, Los Alamitos (2008)