IRIS BIOMETRICS STEGANOGRAPHIC METHOD WITH PIXEL VALUE DIFFERENCING AND HOUGH TRANSFORM FOR HIGHER SECURITY SYSTEM

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

[1]Faculty of Information and Communication Technology, Universiti Teknikal Malaysia Melaka, Hang Tuah Jaya, 76100, Durian Tunggal, Melaka.
[2]Faculty of Computer & Mathematical Sciences, Universiti Teknologi MARA, Shah Alam, 40450, Selangor.
[3] Faculty of Information and Communication Technology, Universiti Teknikal Malaysia Melaka, Hang Tuah Jaya, 76100, Durian Tunggal, Melaka.

[a]zaheera@utem.edu.my, [b]mazani@tmsk.uitm.edu.my and [c]samad@utem.edu.my

Keywords: steganography, pixel value differencing (PVD), least significant bits (LSB) and wavelet decomposition.

Abstract. In biometric security, steganography has become one of the techniques used in defending biometrics data and system. This is due to fraud to the biometric data and illegal activites occured at the biometrics point of system. The biometric data, which in this study, iris, is preprocessed using Hough Transform in producing the iris feature. The pixel values of iris feature is formed, in order to embed the iris feature with the stego key which gained from the cover image (thumbprint from the same trained sample). Studies showed that various techniques of embedding such as least significant bits and pixel value differencing are among popular researches. However, none has been designed for iris implementation in biometrics system. Therefore, a new technique is presented in this paper which integrates pixel value differencing with Hough method in the iris biometrics system. The proposed method modified the pixels values by modifying the most conservative pixels of the block. The theoritical estimation and results produce a scheme which provide a better embedding. The new simulation method provides an embedding capacity, human visual quality and PSNR value is 39.34 dB which is better than the previous methods.

Introduction

More than a decade ago, biometric technology was widely used for attendance system, access control, country border control and airport system. It is a convenient since human uses their own physical traits and behavior rather than using keys and IDs to enter the systems [1]. However, as the use of biometrics arising, the issues of security in biometric data and at the points of system exist. It contributes to the use of fake biometric data and attacks to the databases. The attacks come from various forms, for instance people (imposter, trespasser and manipulator) and software or firmware (software cracker, replay, DoS and crypto attack) [2]. The other factor of tendency to launch attacks is to identify the weaknesses in the biometric system. The weaknesses or vulnerabilities of the biometric systems give an opportunity to the trespasser to bypass at the access level and obtaining the crucial data [3]. Every points of vulnerability in the biometrics system consists of specific defend techniques to prevent the misidentification of the real person. In biometrics security system, steganography has been one of the techniques which are used to defend and reduce the number of attacks to the system itself. There are other techniques such as live detection, cryptography, cancellable template and many more. Steganography is divided into two techniques of embedding which are the least significant bits (LSB) and pixel value differencing (PVD). The embedding methods in steganography are summarized in Figure 1. The LSB is the

536

most popular technique in data hiding field and data embedding. This method embeds the fixed-length secret bits in the same fixed-length LSBs of pixels. PVD works marvelous by providing a high quality stego image besides the high capacity of concealed information [4].
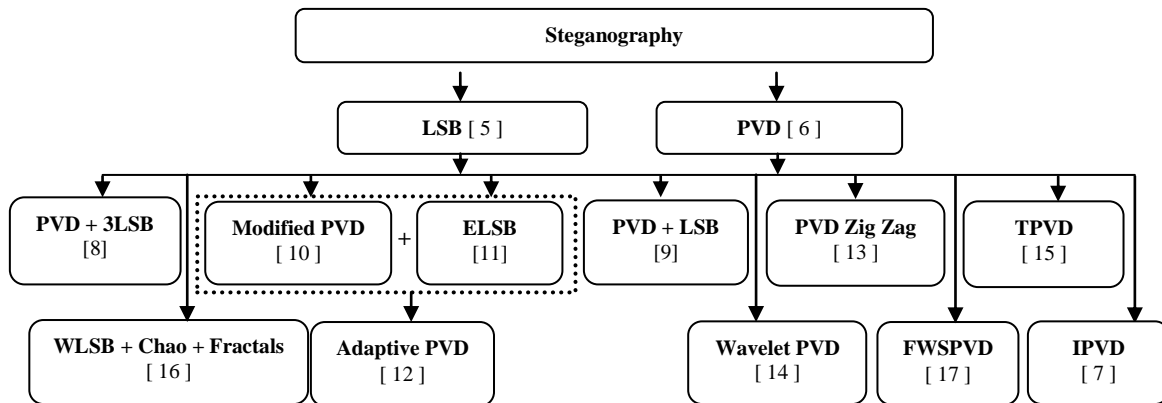

Figure 1.0: The Embedding Methods in Steganography

The proposed embedding and de-embedding method.

The overview of embedding procedure:

- key generation algorithm (sk) : takes as input parameter n and outputs a bit string sk, called the stego key, in M x N dimension of matrix.
- steganographic embedding algorithm (se) : takes as inputs the security parameter n, the stego key (sk) in M x N and a iris feature (i) in M x N, {0, 1} l, to be embedded and outputs an element c of the coverimage space C in M x N, which is called iris stego. The algorithm may access the coverimage distribution C.
- steganographic de-embedding 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 '#'. 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 i {0, 1} l, the probability that sd (1n,*sk*,se(1n, *sk*, i)) 6 = i, must be negligible in n. The probability of de-embedding algorithm that 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 iris feature itself. The number of insertion bits depending on whether the pixel is an edge area or smooth area. The pixels information is larger at the edge area rather than the pixels at the smooth area [18].

The embedding algorithm

The embedding procedure firstly selects the maximum and the minimum values among the four pixel values that have finished the embedding process. The gray value difference of maximum and minimum, *d* is calculated as:

$$d = g_{max} - g_{min} \qquad (1)$$

where,

$$g_{max} = \max \ (g(x-1,y-1), \quad g(x-1,y), \quad g(x-1,y+1), \quad g(x,y-1))$$

and

$$g_{min} = \min \ (g(x-1,y-1), \quad g(x-1,y), \quad g(x-1,y+1), \quad g(x,y-1))$$

Based on equation (1), we assume the pixel is at the smooth area. The embedding capacity of pixel depends on the value of d. Let n be the number of bits which can be embedded in the pixel P_x. The value n is calculated by:

$$n = \begin{cases} 1, & \text{if } 0 \leq d \leq 1 \\ \log_2 d, & \text{if } d > 1 \end{cases} \qquad (2)$$

The image quality of stego-image degraded as n > 6. If n > 6, we set $n \equiv 6$. A sub-stream with n bits in the embedding data is extracted and converted to integer b. The new value of g_x is generated as:

$$g_x' = g_x - g_x \bmod 2^n + b$$

$$(3)$$

where b is the data to be hidden. The embedding error between pixels in the host-image and stego-image is limited to $0 \leq |\hat{g}_x - g_x| \leq 2^{n-1}$ thus the quality of the stego-image is enhanced.

The de-embedding algorithm:

The secret data is obtained from the stego-image by pixels located in the first row and the first column abandoned. Given the target pixel Px* with gray value g(x-1,y-1)*, g(x-1,y)*g(x,y-1)*, be the gray values of its left PL* pixel, upper Pv* pixel and upper-left Pul* pixel respectively. The gray value difference d* is defined as:

$$d^* = gmax^* - gmin^* (x)$$

Where $\qquad\qquad g_{max^*} = max^* (g(x-1,y-1)^*, \quad g(x-1,y)^*, \quad g(x-1,y+1)^*, \quad g(x,y-1)^*)$
and $\qquad\qquad\quad g_{min^*} = min^* (g(x-1,y-1)^*, \quad g(x-1,y)^*, \quad g(x-1,y+1)^*, \quad g(x,y-1)^*)$

Let n* be the number of bits which can be de-embedded from the input pixel Px*. The value n* is calculated by

$$n^* = \begin{cases} 1, & \text{if } 0 \leq d^* \leq 1 \\ \log_2 d^*, & \text{if } d^* > 1 \end{cases}$$

If n* > 6, we set $n^* \equiv 6$, the value b is calculated by $b = g_x^{*} \bmod 2^{n^*}$. Finally, n* bits secret data can be obtained by converting the value of b to binary string. Figure 2 shows the overall process.
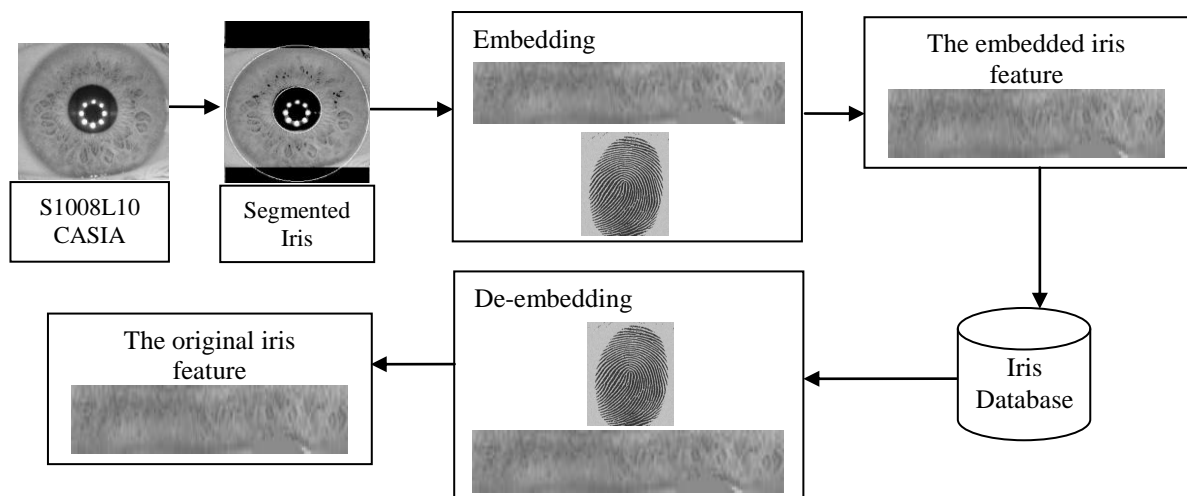

Figure 2.0: The overall process of embedding and de-embedding in the new method

The Results and Analysis

Cover (256x256)	Iris Feature	PVD (Wu and Tsai)		Proposed PVD Zaheera and Mazani	
		Capacity (byte)	PSNR (dB)	Capacity (byte)	PSNR (dB)
	S1**008**L10 – Left Iris	14,055	37.56	14,001	39.34
	S1**008**R08 – Right Iris	13,863	36.49	13,860	38.54

Capacity means number of bits which can be embedded into cover-image and column labeled 'PSNR' is the peak signal to noise ratio of the stego-image. The results are the average value of embedding 130 sets of irises from the CASIA database. The Hough Transform is used in this study since its error correction scheme reduces error in iris image.

Conclusion

In this paper, we presented a novel method to gain stego key from the cover image and embed it into the iris feature using pixel value differencing with pixel modifications to improve the iris security and quality in biometric system. Experimental results shows the PSNR value and the embedding capacity of our method are better than previous scheme.

References

[1]   R.J. Anderson, *Security Engineering: A Guide to Building Dependable Distributed Systems*. New York: Wiley, 2001.

[2]   F. Hao, R. Anderson and J. Daugman. Combining Crypto with Biometrics Effectively. *IEEE, Transactions on Computers*, Vol. 55(9), 2006, pp. 1081-1088.

[3]   N.K. Ratha, J.H. Connell, R.M. Bolle. Enhancing Security and Privacy in Biometrics-Based Authentication System. *IBM System Journal (3)*, 2001.

[4]   R.Amirtharajan, R. Akila, P. Deepikachowdavarapu. A Comparative Analysis of Image Steganography. International Journal of Computer Applications, Vol 2, No 3, 2012, pp. 41-47.

[5]   R-Z Wang, C-F Lin and J-C Lin. Hiding data in images by optimal moderately significant-bit replacement. IEEE Electron. Vol 36 . No 25, 2000, pp. 2069-2070.

[6]   D.-C Wu, W-H Tsai. A steganographic method for images by pixel-value differencing. Pattern Recognition. 2003, pp. 1613-1626.

[7]   X. Zhang and S. Wang. Vulnerability of pixel-value differencing steganography to histogram analysis and modification for enhanced security. Pattern Recognition, Vol 25, Issue 3, 2004. pp. 331 – 339.

[8]   H.C. Wu, N.I. Wu, C.S. Tsai and M.S. Hwang. Image Steganographic scheme based on pixel-value differencing and LSB replacement methods. VISP(152), No. 5, October 2005.

[9]   C.-H. Yang, S.-J. Wang and C.-Y. Weng. Analyses of Pixel-Value-Differencing Schemes with LSB Replacement in Steganography. Intelligent Information Hiding and Multimedia Signal Processing, Vol. 1, 2007, pp. 445 – 448.

[10]   C. Bui, H. Lee, J. Joo and H. Lee. Steganalysis method defeating the modified pixel-value differencing steganography. ICIC, 2009, pp. 3193-3203.

[11]   M. Padmaa and Dr. Y. Venkataramani. Zig-Zag PVD – A Nontraditional Approach. International Journal of Computer Applications. Vol. 5, No. 7, 2010, pp. 5-10.

[12]   W. Luo, F. Huang and J. Huang, A more secure steganography based on adaptive pixel-value differencing scheme. Multimedia Tool Application, Springer, 2010.

[13]   M. Padman and Dr. Y. Venkataramani steganographic method based on differences of pixel difference histogram. Multimedia Tool Application, Springer, 2012.

[14]   A.K. Al-Asmari, M.A. Al-Qodah, A.S. Salama. Wavelet-Pixel Value Differencing Technique for Digital Images Data Hiding. International Conference on System Engineering and Technology, 2011, pp. 45-48.

[15]   N. Zaker and A. Hamzeh. A novel steganalysis for TPVD steganographic method based on differences of pixel difference histogram. Multimedia Tools Application, Springer, 2011.

[16]   Y. Wu and J.P. Noonan. Image Steganography Scheme using Chaos and Fractals with the Wavelet Transform. International Journal of Innovation, Management and Technology, Vol.3, No. 3, 2012, pp. 285-289.

[17]   S. Maruthuperumal, Dr. V. Vijakumar and B. Vijayakumar. Sorted Pixel Value Difference on Fuzzy Watermaking Scheme. Global Journal on Computer Science and Technology, Vol 12 No. 4, 2012.

[18]   C.C. Thien and J.C. Lin. A simple and high-hiding capacity method for hiding digit-by-digit data in images based on modulus function. Pattern Recognition, Vol 36. No. 11, 2003, pp. 2875-2881.