Australian Journal of Basic and Applied Sciences, 7(3): 46-50, 2013
ISSN 1991-8178

A New Hybrid Embedding Method in Iris Biometric System

[1]Zaheera Zainal Abidin, [2]Mazani Manaf, [1]Abdul Samad Shibghatullah, [3]Kamaruzaman Jusoff, [1]Rabiah Ahmad, [1]Zakiah Ayop, [1]Syarulnaziah Anawar, [4]Azizah Shaaban and [5]Mariana Yusoff

[1]Faculty of Information and Communication Technology, Universiti Teknikal Malaysia Melaka (UTeM), Hang Tuah Jaya, 76100 Durian Tunggal, Melaka, Malaysia
[2]Faculty of Computer and Mathematical Sciences, Universiti Teknologi MARA (UiTM), 40450 Shah Alam, Selangor, Malaysia
[3]Department of Forest Production, Faculty of Forestry, Universiti Putra Malaysia, 43400 UPM Serdang, Selangor, Malaysia
[4]Faculty of Manufacturing Engineering, Universiti Teknikal Malaysia Melaka (UTeM), Hang Tuah Jaya, 76100 Durian Tunggal, Melaka, Malaysia
[5]Centre for Languages and Human Development, Universiti Teknikal Malaysia Melaka (UTeM), Hang Tuah Jaya, 76100 Durian Tunggal, Melaka, Malaysia

Abstract: The challenging part in achieving high security biometrics data is viewed from the engineering perspective which includes security, accuracy, speeds and application size. The objective of this paper is to increase the accuracy through an embedding technique. A combination of modified pixel value differencing and wavelet decomposition techniques were used in this study. The pixels were scanned in a new direction embedded with the wavelet difference matrix. The system is developed using both eyes and each eye is enrolled with 10 snaps. The embedding process creates the embedded iris feature and the reverse process of embedding is known as de-embedding. Two thousands iris from CASIA database are used. The application is developed using MATLAB and executed for 5-20 iterations. The new hybrid system shows better performance in accuracy in terms of False Acceptance Rate (FAR), embedding capacity and Peak Signal to Noise Ratio (PSNR) values as benchmarked with the existing method. The finding shows that the output of the embedding capacity is 743801 and 41.10dB of PSNR. The good PSNR value is between 40-50 dB. The implication of this study contributes to a higher accuracy in iris biometric security. Future work should focus on the genetic algorithm to recognize human iris in biometric system.

Key words: Pixel value differencing, Wavelet decomposition, Iris steganographic, Biometric security, Hybrid system

INTRODUCTION

Human identification has been a major challenge in the first generation of biometric system for more than a decade ago. On the other hand, the second generation faces new issues in two perspectives: engineering and social. The engineering part concerns security, accuracy, speed, ergonomics and application size, while the social perspective focuses on values issues in privacy policies, ethical and health concerns, and cultural biases (Jain, A.K. and A. Kumar, 2010).

There are various methods used to improve accuracy in the iris security system. All methods have its advantages and disadvantages depending on the acceptability, usability, modality, permanence, and user friendly (Ross, A., S. Prabhakar and A.K. Jain, 2004). Research in iris biometrics had covered issues mostly on Cryptography, Wavelet and Information hiding. Only a handful studies issues on steganography in Iris due to its authenticity, security, accuracy, robustness and feature classification. In fact, measuring accuracy in Iris system is complex (Jain, A.K. and A. Kumar, 2010; Ross, A., S. Prabhakar and A.K. Jain, 2004) and it needs to be designed in a systematic way. Therefore, there is a need to explore further the steganography issue and find ways of to improve accuracy for iris system.

The existing biometric system uses a strong encrypted iris codes, however, the cryptographic system has been attacked. The hacker gets the original iris codes to generate the iris feature through reverse process of segmentation and normalization (Storm, D. 2012). In fact, 40% of original iris codes can be easily obtained and the success rate of attacking is more than 50%. The secret keys are easily guess in asymmetric encryption with the authentication protocol although it is running over public network and provide nonrepudiable identity verification (Upmanyu, M. *et al*., 2010). The study shows the encryption key generated gives an additional layer of security but private and public keys create curiosity and intention for cracker to hack the system. There are number of attacks have been launched to the biometrics encryption (BE) system. The important attacks are hill

Corresponding Author: Zaheera Zainal Abidin, Faculty of Information and Communication Technology, Universiti Teknikal Malaysia Melaka (UTeM), Hang Tuah Jaya, 76100, Durian Tunggal, Melaka, Malaysia.
Tel: +606-3316571, E-mail: zaheera@utem.edu.my

climbing, nearest imposters, running the error correcting code, Error Correction Code (ECC) histogram, re-usability and blended substitution attack (Stoianov, A., *et al*., 2009). The attacker collects the biometric database and mitigated using private and public keys, which typically controlled by user's password. The River-Shamir-Adelman (RSA) algorithm is used in securing a multimodal biometrics of iris and fingerprint. A number of researchers reported that the iris and fingerprint have been attacked although many encryption algorithms and schemes are used such as RSA, AES with ECC and hash function (Lakshmi, A.J and I.R. Babu, 2012; Bendre, M.R and S.A. Shivarkar, 2012; Seetharaman, K and R. Ragupathy, 2012; Revenkar, P.S., *et al*., 2010; Alvarez, F.H and Encinas, L.H., 2009). In fact, the fuzzy cryptographic scheme is vulnerable to attacks (Juels, A and M. Sudan, 2006; Poon, H.T and A. Miri, 2009; Kholmatov, A and B. Yanikoglu, 2008; Reddy, E.S and I.R. Babu, 2008; Thiyaneswaran, B and S. Padma, 2012). The trend of securing iris template has evolved from cryptographic to other method using various techniques for instance information hiding and wavelet families.

The information hiding later comes into picture when the watermarking is introduced to hide the important information in iris (Xueyi, Y.E., *et al*., 2008). The Set Partitioning In Hierarchical Trees (SPHIT) algorithm (based on EZW) is suitable for encoding the iris features (Hsieh, L., *et al*., 2010). The proposed technique achieves 0% error and good recognition rate of 99%. In reversible steganography or lossless steganography has successfully been conducted in the spatial domain for hiding information in digital image through secure communication channel (Hassan, M., *et al*., 2012). In their research, the Most Frequent Pixel (MFP) is applied in the compression technique to obtain greater quality of image. Later, two studies proposed an iris steganography consists of secret keys and cover which are embedded together with the iris feature (Na, W., *et al*., 2010; Abidin, Z.Z., *et al*., 2011). In fact, a combination of watermarking and steganography, known as 'hardening', is used to strengthen the security of iris (Kamaldeep., 2011). The integration of zero crossing of dyadic wavelet is transformed into the iris recognition system (S-Avila, C., *et al*., 2002). The iris signature, as an input signal, is measured with finite resolution that gives finer scale resolution, smaller coefficients, reduces computational operation, and produces higher security in iris template. To enhance the security in iris template, DCT coefficient is used (Chhikara, R and S. Kumar, 2012) while DWT is integrated with LSB techniques (Fouad, M., A.E. Saddik and E. Petriu, 2010).

A web-based architecture on iris biometrics has reduced the number of credit card frauds over the Internet (Rahimi, A., *et al*., 2010). The iris is preprocessed using 2D Haar techniques to get the iris codes. Then, the iris codes are encrypted using Henon and Logistic maps. The encrypted iris codes are embedded into the cover image using DWT through web-based architecture in biometric authentication.

Methods:

The proposed method of iris steganographic in biometric security model is anticipated to increase the security of iris feature in the biometrics system. The modification of the pixel value differencing uses basic mathematical operation of add (+), minus (-), multiplication (*) and division (/). In steganography, the secret key is embedded together with the iris feature and can be saved into the database. In this stage, the proposed algorithm integrates the pixel value differencing and wavelet decomposition for higher accuracy. Furthermore, the method is further detailed in the proposed algorithm.

The wavelet decomposition is used to spot the eye image (cover) in two dimensional ways. Hence, the eye image is partitioned into two dimensional blocks of lower bound (LL and LH) and upper bound (HL and HH). The LL means low band in lower bound and LH is high band in lower bound. In the other hand, the HL is low band in upper bound and HH gives high band in upperbound. The lower bound provides higher frequency while upper bound gives higher frequency using wavelet decomposition symbol, known as, Ψ, of the signal at level N. The cutoff frequency of signal is 2, 4 and 8. The signal of N is divided by 8 in fulfilling the threshold in two dimensional wavelets. The boundary consists of lower bound and upper bound for embedding and de-embedding processes:

The embedding process:

For lower bound boundary; [0 8 16 32 64 128] (1)

$$yh[n] = x[2n+0] * g[3]z4 + x[2n+1] * g[2]z3 + x[2n+2] * g[1]z2 + x[2n+3] * g[0]z1 \quad (2)$$

For upper bound boundary; [7 15 31 63 127 255] (3)

$$yl[n] = x[2n+0] * h[3]z4 + x[2n+1] * h[2]z3 + x[2n+2] * h[1]z2 + x[2n+3] * h[0]z1 \quad (4)$$

The function of y[n] is the cover matrix with dimension of [40 x 35]. From the formula (2) and (4) show that the function x times with function z1, z2, z3 and z4 for embedding process. Furthermore, the lower bound and the upper bound matrix is continued with pixel value differencing technique. The function of y is added with the function i, where, function i, is the matrix of iris feature where, the P(i,x) and P(i,y) is the dimensions

of rows and columns of $F_i = (P_{(i,x)}, P_{(i,y)})$. The difference of pixels values are calculated and illustrated by $d_i = P_{(i,y)} - P_{(i,x)}$. For upper band, u_j and lower band, l_j, the difference values, d_i, is formulated as $d_i' = \{ u_j + t_i$ for $d \geq 0$ and $-(l_j + t_i)$ for $d < 0 \}$. Thus, $m = d' - d$ in obtaining the secret key from the iris feature. The matrix m[10 x 10], is added with the iris feature matrix [20 x 240], which produce the *embedded iris feature = m + iris + random.*

For the de embedding process, the reverse operation is done at this stage. The embedded iris is decomposition using Haar and Morlet in four bands, LL, LH, HL and HH. Then, the pixel value differencing technique is applied to restore the hidden data. The value of original iris feature is compared with the iris feature from database in matching process. The embedded iris feature is read where the *original iris feature = embedded iris feature – m – iris – random* as shown as:

The de-embedding process:

For lowerbound boundary; [0 8 16 32 64 128] (5)

$$x[2n] = y1[n-1]/z4 * h[1] + yl[n]/z2 * h[3] + yh[n-1]/z2 * g[1] + yh[n]/z1 * g[3] \quad (6)$$

For upperbound boundary; [7 15 31 63 127 255] (7)

$$x[2n+1] = yl[n-1]/z1 * h[0] + yl[n]/z3 * h[2] + yh[n-1]/z1 * g[0] + yh[n]/z3 * g[2] \quad (8)$$

The de embedding process involves the division operation where the function y divides the function z1, z2, z3 and z4 for both upperbound and lowerbound. The lower bound consists of the highest frequency in the iris feature.

RESULTS AND DISCUSSION

The wavelet decomposition is applied to detect the highest frequency area in the iris feature, whereby the iris feature is divided into lower and higher frequency bands. As the lower band is spotted, a matrix is generated and multiplies with matrix cover. The pixels are scanned in new directions by subtracting the second element with the first and followed to the rest of the block. The accuracy of what is further discussed based on previous methods and the proposed scheme. Based on the experiment conducted, the iris feature ran well on the wavelet decomposition technique. However there are problems such as conflict in matrix dimension and data overflow as applying the iris feature in pixel value differencing technique. Pixel value differencing technique is good when scanning the pixel information with the same dimension of matrix or called as square matrix, such as, 512 x 512, 256 x 256 and 128 x 128.

On the other hand, when comes to iris feature, another layer of noise is created if the process of determining the matrix dimension of inverting is not well done. The segmentation and normalization in iris feature do not give the square matrix but gave dimension as 20 x 240. All information in iris feature are significant and one of a kind, thus, we cannot just discard them. It is unwise to generate iris codes since the iris code has been hacked in getting the original iris feature. The solution of this problem is to resize the cover image (eye) to be 40 x 35 and the cover of eye in 320 x 280. The process of subtracting the element then continued using modification of direction in pixel value differencing method, which then creating a new matrix with dimension. The new matrix is then embedded with secret keys through adding the vectors. Once the embedded iris feature is obtained, it is saved into the database. The reverse process is done and called as de-embedding of iris feature.

Table 1 shows the results of embedding techniques for iris steganographic in biometric system. The left iris embedding capacity value shows higher in bytes according to each technique. On the other hand, the value of PSNR is smaller compared to the right iris. A good PSNR value is between 40 to 50 dB and the results are within the range. The values may vary with other human iris since the data is authentic and unique. The results shows by combining different techniques give better performance as in Figure 1. The x-axes refer to rows and the y-axes refer to columns of the iris feature. The stem plots of the same vector matrices prove that the proposed scheme give additional information compared to the existing method since the circle reaches more than 250 at y-axes. The existing method shows that the circle is less than 250 at the y-axes. This means that there is extra information or secret keys embedded in the iris feature in the new scheme.

Table 1: The Performance of Embedding Technique

Iris Feature (20 x 240)	Wavelet 2d Decomposition		PVD		Propose Scheme	
	Embedding Capacity	PSNR	Embedding Capacity	PSNR	Embedding Capacity	PSNR
Left (S1001R01)	735838 bytes	36.25	695679	36.20	743801	41.10
Right (S1001R01)	735701 bytes	45.30	694363	45.00	735005	46.15

S1001R01 - Original S1001R01 – Propose Scheme

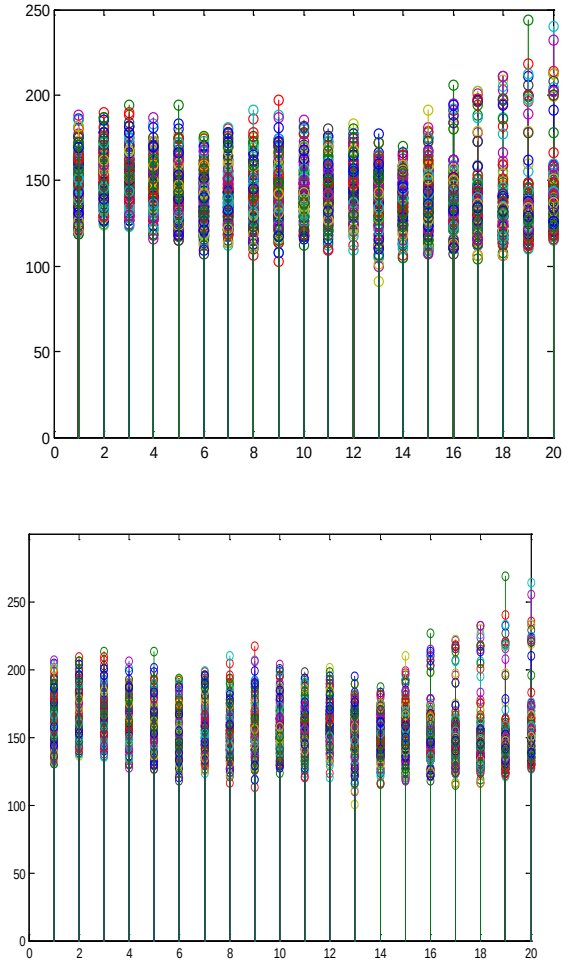

Fig. 1: A comparison of pixel's information in iris feature

Conclusion:

An integration of different techniques in embedding process is proposed and applied to iris steganographic in the biometric security system. The proposed scheme produces 46.15 dB for the right eye compared to 45 dB in PSNR value in existing method. The results have shown that the proposed scheme produces higher embedding capacity and PSNR values. Therefore, the next generation of biometric system requires a lightweight system, cost effective and high security. The implication of this study contributes to a higher accuracy in iris biometric security. Future work should explore the application genetic algorithm to recognize human iris in biometric system.

REFERENCES

Jain, A.K. and A. Kumar, 2010. Biometrics of next generation: An overview. In: E. Mordini & D. Tzovaras (Eds.), Second generation biometrics. Heidelberg, Germany: Springer.

Ross, A., S. Prabhakar and A.K. Jain, 2004. An Introduction to Biometric Recognition, IEEE Trans. on Circuits and Systems for Video Technology, 4(1): 4-19.

Storm, D. Black Hat: Hacking iris recognition systems, Computerworld Inc, Retrieved 2012: from http:// blogs.computerworld.com/security/20704/black-hat-hacking-iris-recognition-systems.

Upmanyu, M. Namboodiri., A.M.K. Srinathan and C.V. Jawahar, 2010. Blind Authentication: A Secure Crypto-Biometric Verification Protocol, IEEE, Journal of Information Forensics and Security, 5(2): 255-268.

Stoianov, A., T. Kevenaar and M.V.D, Veen, 2009. Security Issues of Biometric Encryption, IEEE, pp.34-39.

Lakshmi, A.J and I.R. Babu, 2012. PKI Generation using Multimodal Biometrics Fusion of Fingerprint and Iris, Journal of Engineering Science & Advanced Technology, 2(2): 285-290.

Bendre, M.R and S.A. Shivarkar, 2012. An Improved Approach for Iris Authentication System using Daugman's Rubber Sheet Model, Segmentation, Normalization and RSA Security Algorithm, Journal of Computer Technology and Electronics Engineering, 1(3): 102-107.

Seetharaman, K and R. Ragupathy, 2012. A Novel Biometric Crytosystem using LDPC and SHA based Iris Recognition, Journal of Computer Technology and Electronics Engineering, 4(1): 41-47.

Revenkar, P.S., A. Arjum and W.Z. Gandhare, 2010. Secure Iris Authentication using Visual Cryptography, Journal of Computer Science and Information Security, 7(3): 1-11.

Alvarez, F.H and Encinas, L.H., 2009. Security Efficiency Analysis of a Biometric Fuzzy Extrator for Iris Templates, Journal of Advances in Intelligent and Soft Computing, 63: 163-170.

Juels, A and M. Sudan, 2006. A Fuzzy Vault Scheme, Journal of Design, Codes and Cryptography, 38(2): 237-257.

Poon, H.T and A. Miri, 2009. A Collusion Attack on the Fuzzy Vault Scheme", Journal of Information Security, 1(1): 27-34.

Kholmatov, A and B. Yanikoglu, 2008. Realization of Correlation Attack Against Fuzzy Vault Scheme, Proceedings of Security, Forensics, Steganography and Watermarking of Multimedia Contents.

Reddy, E.S and I.R. Babu, 2008. Performance of Iris Based Hard Fuzzy Vault, International Conference on Computer and Information Technology Workshop, IEEE, pp: 248-253.

Thiyaneswaran, B and S. Padma, 2012. Iris Recognition using Left and Right Iris Feature of the Human Eye for Biometric Security System, Journal of Computer Applications, 50(12): 37-41.

Xueyi, Y.E., H.E. Zhiwei and Z. Wencong, 2008. A Data Hiding Method for Improving the Self-security of Iris Recognition, IEEE, International Conference on Communications, Circuits and Systems, pp: 762-766.

Hsieh, L., W-S. Chen and T-H. Li, 2010. Personal Authentication using Human Iris Recognition Based on Embedded Zerotree Wavelet Coding, International Multi-Conference on Computing in the Global Information Technology, IEEE, pp: 99-103.

Hassan, M., K.M. Nur and T. Noor, 2012. A Novel Compressed Domain Technique of Reversible Steganography", Journal of Advanced Research in Computer Science and Software Engineering, 2(3): 251-256.

Na, W., Chiya, Z. L. Xia and W. Yunjin, 2010. Enhancing Iris-Feature Security with Steganography, Conference on Industrial Electronics and Applicationsis, IEEE, pp: 2233-2237.

Abidin, Z.Z., M. Manaf and A.S. Shibghatullah, 2011. A New Model of Securing Iris Authentication using Steganography, Springer-Verlag, International Conference on Software Engineering and Computer Systems, Part I, CCIS 179, pp: 547-554.

Kamaldeep., 2011. A Review of Various Attacks on Biometrics System and Their Known Solutions, International Journal of Computer Technology and Application, 2(6): 1980-1992.

S-Avila, C., R. S-Reillo and D.de. M-Roche, 2002. Iris-Based Biometric Recognition using Dyadic Wavelet Transform, IEEE-AESS Systems Magazine, pp: 1-4.

Chhikara, R and S. Kumar, 2012. Concealing Encrypted iris Templates in Images using Quantized DCT Coefficients, Journal of Engineering, 2(5): 1007-1012.

Fouad, M., A.E. Saddik and E. Petriu, 2010. Combining DWT and LSB Watermarking To Secure Revocable Iris Templates, Information Sciences Signal Processing and their Applications, pp: 25-28.

Rahimi, A., S. Mohammadi and R. Rahimi, 2010. A New Web-based Architecture Based on Iris Biometrics Technique to Decrease Credit Cards Frauds over Internet, Journal of Digital Society, 1(2): 86-93.