Cyber Digital Forensics: A Novel Spiking of Multimodal Biometric Based on DWT

7

Dr. Najran Nasser Hamood Aldawla

Assistant professor of computer science and IT, College of Science, Sana'a University

الطب الشرعي الرقمي السيبراني : تصاعد جديد للقياسات الحيوية متعددة الوسائط استناداً إلى التحول الموجي المنفصل

١ -د. نجران ناصر حمود الدولة - استاذ علوم الحاسوب وتقنية المعلومات المساعد كلية العلوم -جامعة صنعاء

٢ -د/ محمد حسن الصغير أستاذ المالية والمصرفية المساعد بالجامعة الوطنية

٣ -أ/أمل علي السري -ماجستير نظم معلومات –كلية العلوم – جامعة صنعاء

الملخص — أدت سرعة تقنيات إخفاء المعلومات في البيانات للوسائط المتعددة إلى تحسين موثوقية البيانات الرقمية ونقلها ومعالجتها وصناعة إنتاج غير قانوني وإعادة التوزيع للوسائط الرقمية أمرًا سهلاً وغير قابل للكشف. بحيث تم الطرح في هذا البحث ، تكاملًا جديدًا لمقاييس حيوية هجينة متعددة الوسائط لإيجاد حلول لتعزيز أمن إخفاء المعلومات استنادًا إلى حماية البيانات من حيث التعرف على القزحية والوجه. لقد اقترحنا طريقة لخوارزمية إخفاء المعلومات، والتي يتم تحديد صورة الوجه لتكون الصورة المضيفة. وفي الوقت نفسه ، يتم اختيار ميزة القزحية للعين لتكون بمثابة بيانات سرية مخفية في مضمون صورة الوجه. النظام المقترح هو شكل لتصميم الاخفاء في البيانات الممتد من الأمن والمتانة الذي تم تنفيذه باستخدام خوارزميات التحول المويجي المنفصل. تظهر النتائج التجريبية فعالية وكفاءة القياسات الحيوية الثنائية النسق (الوجه والقزحية) التي توفر التحسين في دقة أداء النظام.

الكلمات المفتاحية:

الامن ، والحماية ، إخفاء المعلومات ، القياسات الحيوية الثنائية ، التحول الموجي المنفصل.

Cyber Digital Forensics: A Novel Spiking of Multimodal Biometric Based on DWT

Dr. Najran N. H.
Al_Dawla
Faculty Member,
Dept. of Mathematics &
Computer
Sana'a University, Yemen

Dr. Mohammed Alsaquir
Faculty Member,
National University,
Sana'a, Yemen

Mrs. Amel Ali Alserry
Dept. of Mathematics &
Computer
Science Faculty
Sana'a University, Yemen

Abstract:

The rapidly information hiding in multimedia data has improved the reliability, transfer and processing of digital data and making the illegal production and redistribution of digital media easy and undetectable. In this paper we present a novel integration of a hybrid multimodal biometric to find a solution for enhancing steganography security based on Iris and face recognitions and protecting data. We proposed a steganography algorithm approach, which face image is selected to be the host image. Meanwhile, iris feature is chosen to be as secret data hidden in the host of the face image. The proposed scheme is an extended generalized form of security and robustness which based the Discrete Wavelet Transform DWT. An experimental results show the effectiveness and efficiency the bimodal biometrics (Face and iris) that provides the improvement in the accuracy performance of the system.

Keywords-Steganography:, Bimodal biometric, DWT, security

I. INTRODUCTION

The rapidly development of digital technology and escalation use of multimedia across, internet, telecommunication networks and other transmission has greatly expanding a way to deliver services around the world. The easy copy and distribution of digital content on the internet has explored a large number of pirated digital media content and can be reproduced without losing the quality. It has explored means of new business, economic, social opportunities, scientific and culture that seriously injured. So the incorporate of digital steganography and biometrics are developed the fascinating scientific area of digital content copyright protection and security technology with the wider use of digital technology to prevent the illegal copying of a digital content and provides security digital content contribution [1, 2].

Security today has become an important issue during the storing andtransmission of digital data that relies on cryptography that focuses on concealing the contents of data by using the most prominent of which is the key management and the use of physiological characteristics of the users and the steganography techniques.[4]

Digital Steganography describe techniques that are used to imperceptibly convey information by hide secrets into the cover-data such as an image, document, audio, video file, so that no other people can detect or extract the existence of the secrets. A steganographic method consists of an embedding algorithm and an extraction algorithm. The embedding algorithm describes how to hide a message into the cover object and the extraction algorithm illustrates how to extract the message from the stego object. On the other hand, Biometric [4, 5].In the current years, biometric-based systems are becoming very popular because of their ability to identify and verify the physiological or behavioral characteristics of person and differentiate between a legitimate user and an unlawful user [3]. Biometric techniques have inherent advantages over traditional personal identification techniques, but the problem of security and privacy of biometric data is extremely critical. If a person’s biometric data is stolen, it is not possible to replace it. Furthermore, it has problems such as, the secrecy is weak, cannot be reproducing and non-canceling which make it necessary and difficult to protect while biometric data can provide uniqueness, it is not a secret. In order to promote widespread utilization of biometric recognition, an increase of biometric security level is necessary. Cryptography and steganography are possible techniques to achieve this. The steganography embedded in the biometric data provides another line of defense against illegal utilization of the biometric data. Meanwhile, it should be as a means to eliminate some of attacks to biometric system [4]. A comprehensive details discussion on information hiding can be found in [26-29]. This paper is arranged as follows. In section 2, we discuss related research a brief introduction to digital steganography, DWT, biometrics generating data. Embedding and extracting strategies is proposed and describes in section 3, Experimental result and conclusion are given in section 4 and 5 respectively.

II. RELATED RESEACH

This section describes the brief introduction to digital steganography, DWT, biometrics. In this proposed work we are focusing on biometric data hiding that involve the use of face and iris images. With the wide spread of biometric authentication technology in various applications, it often gives the case that “the biometric features need to be transmitted through non-secure communication channel”. In such a case, the issue to secure and protect the biometric features to be transmitted is raised. In addition, to increase the security and authentication accuracy, it is required to combine more than two biometric. So the technology of combining biometrics and steganography algorithm has been proposed [18, 19]. Anjali et al. proposed a dwt steganography method using biometrics [4]. A. E. Hassanien describes a method of hiding Iris code for authentication based on wavelet scheme [9]. Ratha et al. shows the method of data hiding that applicable to wavelet compressed fingerprint images [15]. N. Komninos et al. describe the way for protecting biometrics templates with image hiding techniques [20]. A. K. Jain et al. have shown the scheme of hiding fourteen Eigen face coefficients in fingerprint images based on digital watermarking technique to protect the biometric features such as face and increase the security and authentication accuracy by both face and fingerprint recognition [23**]**. Najran et al. describe the Enhancement of Steganography that used a wavelet transform technique to combine the text and image, fingercode .that show the roubustness and effective of the proposed scheme. [24, 25]. T. Hoang et al. [21] proposed the authentication system of the priority watermarking based on multimodal biometric (fingerprint and face features). Proposed scheme not only overcome drawbacks and problems of previous schemes, but also provide a stronger and more secure authentication of over insecure network. A. E. Hassanien et al. proposed a spiking biometrics date to be hidden as iris that based on neural network and wavelets techniques in digital images [16]. Z.Z. Abidin et al. [22] shows an enhancement of new model iris security for authentication based on steganography techniques.

III. HIDING IRIS CODE DATA

In this section, the process of concealing biometric data such as iris into face images includes four main steps: (Generating iris code, embedding, extracting and authentication). We use iris features as secret information embedded to the face images, after image recognition is completed, we extract the embedded stego image (Iris code features) and compute the similarity between the extract iris features and the enrolled one. This is not only a robust and effective authentication method, but it can make the stego image of embedded data more secure. The methods description of embedding and extracting biometrics generating data, are shown in figure 1.

A. Biometrics generating data

The general processes for generating biometrics data are consist of two processes enrollment and verification, where the enrollment collects the biometric images, which is the iris image using extraction algorithms and verification step involves matching and detraction algorithms. The combination of the steganography properties is implemented into both processes of biometric enrollment and verification. The iris image analysis works when the eye image acquired by a digital camera. Then, by utilizing the eye image, the iris image is segmented to show the boundary between the pupil and the iris is detected after the position of the eye in the given image is normalized to be localized. After extraction the center and the radius of the pupil, the both sides right and the left radius of the iris are searched based on these data to produces an iris template. By calculated the centre of iris and radius then, we set the polar coordinate system where the feature of the iris is extracted. This step produces iris code.

B. Embedding scheme

The embedding process in our proposed method is shown in fig.1, In the embedded process, we first decompose face image into several bands with a pyramid structure and then pseudorandom sequence is added to the huge coefficients, which are not located in the lowest resolution. The host image and digital steganography are represented as:

$$f = \{f(i,j), 0 \leq i \leq M_{1,} 0 \leq j < M_2 \qquad (1)$$

$$s_I = \{s(i,j), 0 \leq i \leq N_{1,} 0 \leq j < N_2 \qquad (2)$$

Where $f(i,j) \in \{0,1,\ldots,2^L - 1\}$ is the intensity (i,j) and L is the number of bits used in each pixel, $s(i,j) \in \{0, 1\}$. The perceptually significant wavelet coefficients can be found for each sub-band, according to the decomposition level the threshold value is calculated. For example, in the 3-level decomposition, the largest coefficients C1 for 1-level sub-bands (LH_1, HL_1, HH_1) is selected and the threshold T_1 is calculated by Eq. (3). The same process of T_2 and T_3 for the subsequent levels can be calculated respectively [9].

$$T_i = 2^{\log 2 \text{ Ci}-1} \qquad (3)$$

Where i is the decomposition level and represents the largest integer which is not greater than X. DWT embedded algorithm is contained of four parts: cover image; multi-level thresholds calculation for selecting perceptually significant coefficients; iris code insertion process; and inverse wavelet decomposition (IWT) of the coefficients with iris code.

C. Extracting scheme

The extraction process is to estimate and obtain the reliability of the original image from the stego image. The extraction process can be carried out by reversing the embedding procedures that is generate the similar random permutations of each embedding subchannel as the encoding by using the same shared key and given the correlation coefficient between the given and extracted one to get the output as the original image and the iris code.

D. iris Biometric Authentication

We use the iris feature extracted. Then we calculate the correlation value between the extracted features of iris and the registered features of iris. User’s authentication is successful when the computed correlation value is greater than predefined threshold. If the correlation value is smaller than the threshold, then the user’s authentication is regarded to be unsuccessful.

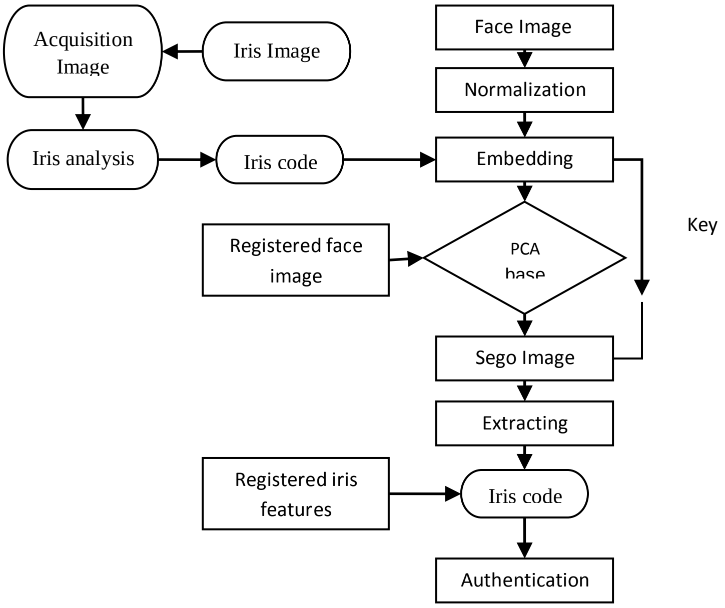


Fig.1. hiding iris code into a face image scheme.

IV. EXPERIMENTAL RESULT AND DISSCUSION

To authenticate the performance and the efficiency of the embedding methods, executive tests have taken place. We perform simulation on four face biometric images each with parameter size 256 x 256 and an embedded iris code data which describe how the iris image is converted. The resulting parameters from the proposed methods of four tested face biometric images are show in the tab.

TAB.1.SIMILARITY MEASURES FOR THE “FACE1”, “FACE2”, “FACE3”, “FACE4” IMAGES .

Image	Face1	Face2	Face3	Face4
PSNR	31.9313	80.7933	47.0799	34.536
MSE	41.682	5.42E-04	1.2738	22.8814
NC	-0.1849	-0.0685	-0.0539	-0.1833

Here we have used the similarity measures for the various images such as Peak Signal to Noise Ratio (PSNR), is adopted to estimate the dissimilarity between the original and the stego images and can be defined via Mean Square Error (MSE) in the unit of logarithmic decibel (dB) as follows:

$$PSNR = 10log\frac{(2^{n}-1)^2}{MSE} = 10log\frac{255^2}{MSE} \qquad (4)$$

$$MSE = \frac{1}{\mathrm{MN}}\sum_{j=1}^{M}\sum_{k=1}^{N}\left(x_{j,k}-x'_{j,k}\right)^2 \qquad (3)$$

A higher PSNR indicates that the watermarked host image is closer to the original one from the perspective of host contents. The host fidelity is acceptable for any PSNR greater than 30 dB.

We have used average difference and Maximum Difference measures for the various images to differentiate between the original image and stego image as follows:

$$NC = \sum_{j=1}^{M}\sum_{k=1}^{N} xj,k\,.x'j,k \qquad (4)$$

Fig.2. shows the face host face image and the stego image respectively and it shows the iris code date and we see that the host face image is not distinguishable from the stego image.

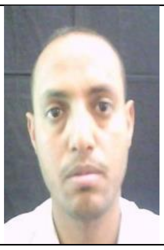
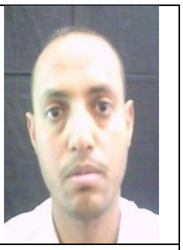
	011110010001000 101111111001011 110101010101110 1100	
Face Original Image	Iris code	Stego Image

Fig.2. Result of the proposed algorithm

V. CON LUSION

In steganography the emerging techniques in the field of transform domain such as DWT are not an easy target for attaches, especially when the concealed messages are small.We have proposed a new framework for enhancing security biometrics authentication system .in which a new digital steganography method based on DWT shows the effectiveness and robustness of the proposed system. A new metric that measures the objective quality of the image based on the extracted stego image bit is introduced in our proposed method. The face image after extracting the embedding finger features is nearly the same with the original face image before embedding in aspect of recognition result.

In future work, we are considering the use of multimodal biometrics features in various multimedia as reference points to recover from any various attaches and distortions.

VI. References

[1] Saraju P. Mohanty "Digital Watermarking: A Tutorial Review," Dept of Comp Sci and Eng. Unversity of South Florida Tampa, FL 33620 1999.

[2] S. Katzenbeisser, A.P Fabien. Petitcolas "Information hiding techniques forSteganography and digital watermarking" editors. p. cm. (Artech House Computing library) 2000.

[3] A. K. Jain, and U. Uludag, "Hiding biometric data", IEEE Transactions Pattern Analysis and Machine Intelligence,
2003, Vol.25, No.11, pp.1494-1498.

[4] Anjali A. Shejul, U. L. Kulkarni,
"A DWT Based Approach for Steganography Using Biometrics,"
IEEE Internatioal Conferece On Data Storage And Data Engineering,
2010.

[5] Wenbo Mao, Modern Biometric: Theory and Practice, , Prentice Hall PTR, , Prentice-HallInc., 2004

[6] William Stallings, Biometric and Network security: principles and Practice, Prentice HallInternational Inc.; 2002

[7] Jae K. Shim, Anique A. Qureshi and Joel G. Siegel, The International Hand book of Computer Security, Glenlake Publishing Company, Ltd., 2000.

[8] Sekhar R. Sarukkai and David D. Zhang, *Biometric Solutions for Authentication in an E-World* (Springer,2002).

[9] A. E. Hassanien,**“**Hiding Iris Data for Authentication of Digital Images Using Wavelet Theory” Pattern Recognition and Image Analysis, Vol. 16, No. 4, pp. 637–643, 2006.

[10] Huang Daren, L. Jiufen, H.Jiwu and L.Hongmei “A DWT-Based image watermarking algorithm,” IEEE Int Conf on Multimedia and Expo.

[11] HONG CAI, M.S. “Wavelet Structure Based Transform: Information Extraction and Analysis,” University Of Texas, Dissertation, December 2007.

[12] Ali Al-Ataby and Fawzi Al-Naima “A Modified High Capacity Image SteganographyTechnique Based on Wavelet Transform,”The International Arab Journal of Information Technology, Vol. 7, No. 4, October 2010.

[13] XuJianyun, A. H. Sung, P. Shi, Liu Qingzhong “JPEG Compression Immune Steganography Using Wavelet Transform,” IEEE International Conference on Information Technology,Vol.2, pp.704 – 708,2004.

[14] H.W. Sun, K. Lam, M. Gu, and J. Sun “An Efficient Algorithm for Fingercode-Based Biometric Identification,” Springer OTM Workshops 2006.

[15] N. K. Ratha, J.H. Connel, and R. M. Bolle, “Secure Data Hiding in Wavelet Compressed Fingerprint Images”, Proc. ACM Multimedia, Oct. 2000, pp.127-130.

[16] A. E. Hassanien, Ajith Abraham, Crina Grosan **“**Spiking neural network and wavelets for hiding iris data in digital images” Springer-Verlag, Vol. 13, pp. 401–416, 2008.

[17] Gui Feng, and Qiwei Lin, “Iris feature based watermarking algorithm for personal identification”, Proc. of SPIE, 2007, Vol.6790, pp.679045.

[18] H. Lin, and K. J. Anil., “Integrating Faces and Fingerprints for Personal Identification”, IEEE Trans. on Pattern Analysis and Machine Intelligence, 1998, Vol.20, No.12,

[19] D. S. Wang, J. P. Li, Y. Tang at el., “Authentication Scheme of Remote Users by Using Multimodal Biometric and Smart Cards”, International

Conference 2007 on Information Computing and Automation, Chengdu, Sichuan, China, Dec. 2007, Vol.1, pp.98-101.

[20] N. Komninos and T. Dimitiou,. "Protecting biometrics templates with image watermarking techniques," springer- verlag Berlin Heidelberg, ICB, 2007, pp.114-123.

[21] M. Minerva, and P. Sharath, “Verification Watermarks on Fingerprint Recognition and Retrieval”, Proc. of SPIE Conference on Security and Watermarking of Multimedia Contents, 1999, Vol. 3657.

[22] Z.Z. Abidin, M. Manaf, and A.S. Shibghatullah,. "A new Model of Securing Iris Authentication Using Steganography," Springer, ICSECS, pp.547-554. 2011.

[23] A. K. Jain, U. Uludag, and R. L. Hsu, “Hiding a Face in a Fingerprint Image”, Proc. of Int. Conf. on Pattern Recognition, 2002, Vol. 3, pp. 756-759.

[24] Najran N. H. Aldawla, M. M. Kazi, K. V. Kale, “Steganography Enhancement by combining text and image through Wavelet Technique ,” in International Journal of computer & Applications (IJCA), Vol.51 No.21, pp. 0975 – 8887, August 2012.

[25] Najran N. H. Aldawla, M. M. Kazi, K. V. Kale, “Steganography Enhancement By Hiding Fingercode-Biometric Into Digital Image Through Wavelet Technique,” in International Journal of Systems , Algorithms & Applications (IJSAA), Vol.2, PP. 119-121, May 2012. ISSN: 2277-2677.

[26] Petitcolas FAP, Anderson RJ, Kuhn MG ,"Information hiding: a survey", Proc IEEE, special issue on protection of multimedia content, No. 87(7):pp.1062–1078, (1995).

[27] X.Zhang, S. Wang, "Steganography usingmultiple-base notational system and human vision sensitivity", IEEE Signal Process Lett, No 12: pp.67–70,(2005).

[28] F. Hartung, M. Kutter, "Multimediawatermarking techniques", Proc IEEE, No. 87: pp.1079–1107,(1999).

[29] V.M. Potdar, S. Han, E. Chang, "A survey of digital image watermarking techniques", In: Proceedings of IEEE third international conference on industrial informatics, INDIN05, pp 709–16, (2005).□