Efficient Watermarking based an Robust Biometric Features

Muzhir Shaban Al-Ani[1]
muzhir@gmail.com
College of Computer - Anbar University – Anbar – Iraq

Khetam Abd Al_Baset[2]
khetam_comp@yohoo.com
College of Computer - Anbar University – Anbar - Iraq

Abstract
Fingerprints are unique biometrics mainly used for the establishment of instant personal identity but they susceptible to accidental/intentional attacks because that must be secure biometric data from any attack by using watermark technique. In this paper biometric image is used for features extraction from fingerprint images and embedded these features in face image at watermarking technique via the calculation of average for all faces images that stored in database. This approach indicates a good result in watermarking and data recovering. This approach may applied in many applications such as could credit card, personal identification card, secure passport … etc.

Key Words: Robust Biometric, Watermarking Security, Biometric Recognition, DWT.

I. Introduction

Biometric is a method for authentication system to identify persons and secure biometric data. Biometric systems should ensure authenticity, integrity, privacy and resistance to attacks and forgery. Biometric algorithms and procedures should conform a system which ensure the identification of the target using biological traits: fingerprint, face image, DNA sequence, voice, walking gaits, …etc. Most of biometric systems require strong security. Therefore, they usually make use of watermarking, cryptography and steganography [1]. Digital watermarking is the process of embedding information into digital multimedia content such that the information after that can be extraction for verifying data. Digital watermarking has become an active and important and development to secure content of any file. *Enrollment* and *authentication* are the two primary processes involved in a biometric security system. During *enrollment*, biometric measurements are captured from a subject and related information from the raw measurements is gleaned by the feature extractor, and this information is stored on the database. During *authentication*, biometric information is detected and compared against the database through pattern recognition techniques that involve a feature extractor and a biometric matcher working in cascade[2]. The computer analyzes your fingerprint to determine who you are and, based on your identity followed by a pass code or pass phrase, allows you different levels of access. Access levels can include the ability to open sensitive files, to use credit card information to make electronic purchases, and so on[3]. This paper deals with the design of robust watermarking approach based on robust biometric. In this paper two level Two dimensional Discrete Wavelet Transform (2D-DWT) approach is used for image compression to reduces the amount of data of fingerprint to hide in face image via LSB technique to implement watermarking.

II. Biometric System

A biometric system is fundamentally a pattern-recognition system that recognizes a individual based on a attribute vector derived from a specific physiological or behavioral characteristic that the person possesses. Biometric security differentiate from the classic security methods because it identifies an individual based on what he is rather than on what he possesses or what he remembers. The advantage of biometric systems over traditional security methods is that they cannot be stolen or shared. Traditional security practices often involve the use of two

authentication methods: possession based and knowledge based. Knowledge based authentication requires that the users remember a user name and password or PIN numbers or answers to security questions. Possession based can use radio frequency IDs, Smart Cards, Interactive Tokens …etc [3].

A simple biometric system as shown in figure (1) consists of four basic components:

1. Sample acquisition first the collection of the biometric data must be done using the appropriate sensor; for example an image capture in the case of iris recognition or a saliva sample for DNA or scanner for fingerprint [19].
2. Feature extraction module where the acquire data is processed to extract feature vectors [5].
3. Matching module where attribute vectors are compared against those in the template [5].
4. Decision-making module in which the user's identity is established or a claimed identity is accepted or rejected [5].

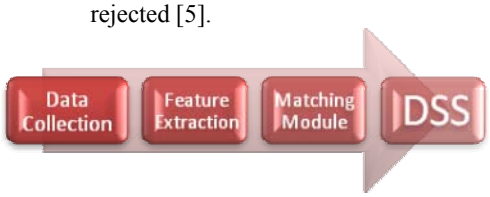


Figure (1) biometric system

III. Watermarking System

A watermark is a secret code or image incorporated into an original image [6]. General digital watermark life-cycle phases as shown in figure (2) with embedding attacking and detection and retrieval functions the information to be embedded in a signal is called a digital watermark, although in some contexts the phrase digital watermark means the difference between the watermarked signal and the cover signal. The signal where the watermark is to be embedded is called the host signal. A watermarking system is usually divided into three distinct steps, embedding, attack, and detection. In embedding, an algorithm accepts the host and the data to be embedded, and produces a watermarked signal. Then the watermarked digital signal is transmitted or stored, usually transmitted to another person. If this person makes a modification, this is called an attack.

While the modification may not be malicious, the term attack arises from copyright protection application, where pirates attempt to remove the digital watermark through modification. There are many possible modifications, for example, lossy compression of the data (in which resolution is diminished), cropping an image or video or intentionally adding noise. Detection (often called extraction) is an algorithm which is applied to the attacked signal to attempt to extract the watermark from it. In robust digital watermarking applications, the extraction algorithm should be able to produce the watermark correctly, even if the modifications were strong. In fragile digital watermarking, the extraction algorithm should fail if any change is made to the signal [7].

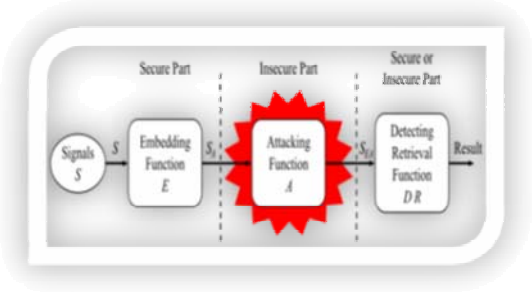


Figure (2) watermark phases

IV. Literature Reviews

There are several systems that implemented for biometric image and watermark technique during previous years.

Anil K. jain, et al. **(2002)** implemented hiding the face image biometric in a fingerprint image by computing the ROC(Receiver Operating Characteristic) curves for all image in database and apply minutiae on fingerprint image to hide features [12].

Mayank Vasta, et al. **(2004)** implemented a multimodal biometric system using watermarking algorithms with two levels of security for simultaneously verifying an individual and protecting the biometric template (Iris is Watermarked in face),In biometric applied ID log Gabor algorithm on the iris image and using MCBA(Modified Correlation based algorithm) and M2DCT(Modified 2D Discrete Cosine Transform based algorithm) for watermark face image [13].

Mayank Vast, et al. **(2006)** implemented a combined DWT and LSB based biometric watermarking algorithm that securely embeds a face template in fingerprint image. The proposed algorithm is robust to geometric and frequency attacks and protects the integrity of both the face template and the fingerprint image [14].

Nick Bartlow, et al. **(2007)** implemented the encodes voice feature descriptors in raw iris images thereby offering an example of a secure biometric system. The contributions of this work are as follows: application of biometric watermarking to iris images in order to provide an added level of authentication; a mechanism to validate the originating source of iris images; understanding levels in which watermarks can be compromised in a biometric system; and implementation of an asymmetric watermarking framework [15].

Aboul Ella Hassanien, et al. **(2009)** introduces an efficient approach to protect the ownership by hiding the iris data into a digital image for authentication purposes. The idea is to secretly embed an iris code data into the content of the image, which identifies the owner. Algorithms based on Biologically inspired Spiking Neural Networks, called Pulse Coupled Neural Network (PCNN) are first applied to increase the contrast of the human iris image and adjust the intensity with the median filter [16].

Meenakshi Arya1, et al. **(2011)** applied two technique, one for biometric (lifting wavelet transform technique) on signature image ,second for watermarking (SVD) to reduce a dataset containing a large number of value to a dataset containing significantly fewer values but which still contains large fraction of the variability present in the original data [17].

Bin Ma, et al. **(2011)** implemented a robust watermarking method to enhance the security of multimodal biometric authentication system, use face image for biometric to extraction features for employed as watermark and embedded into fingerprint image with a blind SS_QIM scheme [18].

Rajlaxmi Chouhan, et al**. (2011)** using fingerprint image watermarking by applied DWT. The embedding/extraction for all image in the database has been achieved successfully and the watermarking scheme is found to give equally good results for all fingerprint in the database [19].

Sengul Dogan, et al. **(2011)** recommend a biometric color images hiding approach An Watermarking System based on Discrete Cosine Transform (DCT), which is used to protect the security and integrity of transmitted biometric color images [20].

Sandip Dutta, et al. **(2012)** ,in which unique key is generated using partial portion of combined sender's and receiver's fingerprints. From this unique key a random sequence is generated, which is used as an asymmetric key for both Encryption and Decryption [21].

V. Implemented System Design

The proposed system can be summarized in the four steps as shown in the figure (3).

In step one Data collection from students in computer college at 100 sample for 100 students we take 10 fingerprint image by using scanner(Canon, 1410 mf, 300 dp, color photo) and 10 face image by using came with (14.1) resolution for each student and save this images in two database (fingerprint image, face image) that fingerprint image and face image are related for same person.

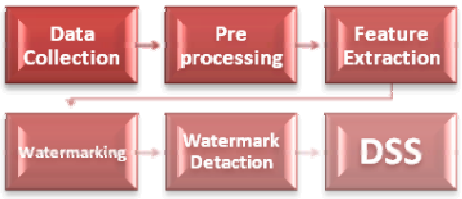
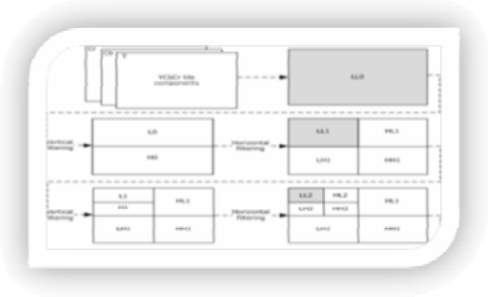


Figure (3) The block diagram of the biometric and watermarking

each fingerprint image enter to pre processing phase to applied many step to enhance fingerprint image (read rgb image, resize images, convert to gray scale, segmentation, edge detection).

Feature extraction phase is implemented via DWT, and it is mathematical tool for hierarchically decomposing of an image is implemented. DWT provides both frequency and spatial description of an image, After the first level of decomposition, 4 sub-bands are obtained: LL1, LH1, HL1, and HH1. For each successive level of decomposition, the LL sub band of the previous level is used as the input. To perform second level decomposition, the DWT is applied to LL1 band which decomposes the LL1 band into the four sub-bands LL2, LH2, HL2, and HH2. DWT is currently used in a wide variety of signal processing applications, such as in audio and video and image compression [8].



Figure(4) two level of 2DWT

The statistical calculation of features are[9]:

1. Max (maximum value in image).
2. Min (minimum value in image).
3. Mode.
4. STD (standard deviation).

$$S^2=\sum_{i=1}^{n}\frac{(Xi-\bar{X})2}{n-2} \quad \text{...……(1)}$$

5. Median value .
6. TSS (Total Sum of Square)

$$TSS=\sum(k-\bar{X})^2 \text{……...(2)}$$

7. Variance.

$$var(x)=\sum_{i=1}^{n}\frac{(Xi-\bar{X})2}{n-2} \text{.....(3)}$$

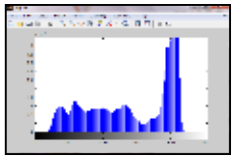
8. Mean.

$$\bar{X}=\left(\sum_{i=1}^{n}\frac{[Xi)}{n}\right] \text{…...……(4)}$$

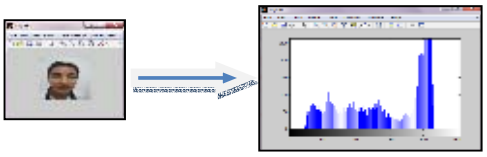
We applied DWT for two level for fingerprint image and using (LL) sub band for feature extraction, after that beginning to hide this feature for fingerprint image into face image by calculate the average for all face images and using LSB technique for hide features in different color of image, Least Significant Bit (LSB) which replaces the least significant bits of pixels selected to hide the information [10]. In fourth phase authentication of features by back the same watermark method to back features and matching with base feature saving in database, where the matching successfully the watermark for hide data is good.

VI. Analysis and Result

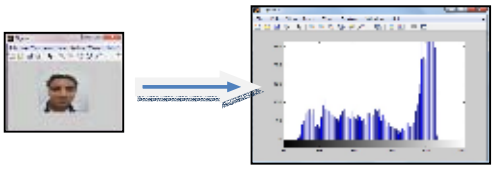
The proposed method has been simulated using the Matlab programming language. All the images fingerprint resize 256*256 for biometric and resize face images to 128*128 for watermarking .five fingerprint and five face images person are used for training and the rest of the five fingerprint and five face images for testing. In this paper embedded the feature of biometric fingerprint image into face watermark image. The feature extract by two way, one way used 2DWT with two level of LL sub band, second way take features without DWT, when compeer between two way, two robustness methods of watermarking are implemented, and these methods are greatly affected but with DWT faster implementation for run time program. In figure(5)-a shows the histogram of face image before watermarking,(b) show histogram of face image after watermarking without DWT,(c) histogram of face image after watermarking with DWT.



(a) Original image



(b) watermarking image without DWT



(c) watermarking image with DWT

Figure (5) histogram implementation before DWT(a) before watermarking (b) after watermarking without DWT (c) watermarking image with DWT

In Table(1) calculation many error for five images in first column the number original image, second columns error rate for original images, third columns error rate for watermarking images without DWT. The error is very little when compeer between original image and watermarking image.

Table (1) error rate for image after watermarking without DWT

	Original image error		**Watermarking without DWT error**	
No. of image	MSE	PSNR	MSE	PSNR
Imag 1	**2.4992e +004**	**4.1528**	**2.4984e+ 004**	**4.1542**
Imag 2	**2.8204e +004**	**3.627**	**2.8156e+ 004**	**3.6352**
Imag (3)	**3.0498e +004**	**3.2881**	**3.0470e+ 004**	**3.2921**
Imag 4	**2.3850e +004**	**4.3559**	**2.3828e+ 004**	**4.3599**
Imag 5	**2.7052e +004**	**3.8089**	**2.6967e+ 004**	**3.8225**

In Table(2) calculation many error for five images in first column the number original image, second columns error rate for original images, third columns error rate for

watermarking images with DWT. The error is very little when compeer between original image and watermarking image.

Table (2) error rate for image after watermarking with DWT

	Original image error		**Watermarking with DWT error**	
No. of image	MSE	PSNR	MSE	PSNR
Imag1	**2.4992e +004**	**4.1528**	**2.4984e +004**	**4.1542**
Imag2	**2.8204e +004**	**3.627**	**2.8156e +004**	**3.6351**
Imag3	**3.0498e +004**	**3.2881**	**3.0470e +004**	**3.2921**
Imag4	**2.3850e +004**	**4.3559**	**2.3828e +004**	**4.3599**
Imag5	**2.7052e +004**	**3.8089**	**2.6967e +004**	**3.8225**

VII. Conclusion

Computer vision and imaging sciences are closely related to biometrics. Old biometric systems which relied on human visual verification are being displaced by the superior analyzing capabilities of computers. Using biometric features in security become very important information in many applications in our life. In this paper, we use biometric features with watermarking to be more security of biometric data. In addition this paper verify secure personal data from attackers or hackers.

References

[1] Ms.Yamini S.Bute, Prof. R.W. Jasutkar, "Implementation of Discrete Wavelet Transform Processor For Image Compression", International Journal of Computer Science and Network (IJCSN), Volume 1, Issue 3, June 2012 www.ijcsn.org ISSN 2277-5420.

[2] Mary Lourde R, and Dushyant Khosla, "Fingerprint Identification in Biometric Security Systems", International Journal of Computer and Electrical Engineering, Vol. 2, No. 5, October, 2010.

[3] Adrian POCOVNICU, "Biometric Security for Cell Phones", Information Economic vol. 13, no. 1/2009.

[4] IPTS – JRC, " Biometrics at the Frontiers: Assessing the impact on Society", Institute for Prospective Technological Studies in Europe, 2009.

[5] Ion Marqués and Manuel Graña, "Image security and biometrics: A review", Computational Intelligence Group, University of the Basque Country, HAIS'2012, Salamanca, Spain.2012.

[6] Ismael A. Jannoud ,Mohammed A. F., Al-Husainy, "Digital Watermarking Technique for Hiding Text Into Image", Damascus Univ. Journal Vol. (22)-No. (2)2006.

[7] Sahil Anand, Swati Mehla, Samiksha Arya, Piyush Kapoor, " Digital Watermarking", International Journal of Engineering and Innovative Technology (IJEIT) Volume 2, Issue 2, August 2012.

[8] Nikita Kashyap, G. R. SINHA, "Image Watermarking Using 3-Level Discrete Wavelet Transform (DWT)", I.J. Modern Education and Computer Science, 2012, 3, 50-56.

[9] Lindsay I Smith," A tutorial on Principal Components Analysis", February 26, 2002.

[10] Juan José Roque, Jesús María Minguet, " SLSB: Improving the Steganographic Algorithm LSB ", Universidad Nacional de Educación a Distancia (Spain) ,2009.

[11] Prashant Kawale, "Seminar Report On Digital Watermarking", 2009, http://csis.bitspilani.ac.in/faculty/murali/netsec09/seminar/refs/prashantkrep.pdf.

[12] Anil K.jain, Umut Uludag and Rein-Lien Hsu, "Hiding a Face in a Fingerprint Image", Computer Science and Engineering Department, Michigan State University, USA, 2002.

[13] Mayank Vasta, Richa Singh, P.Mitra ,Afzel Noore, "Digital Watermarking based Secure Multimodal Biometric System", IEEE International Conference on System, Man and Cybernetics 2004.

[14] MayankVast , Richa Singh, Afzel Noore, Max M.Houck, and Keith Morris, " Robust Biometric image watermarking for fingerprint and face template protection", IEICE Electronics, Vol.3, No.2, 23-28, 2006.

[15] Nick Bartlow, Nathan Kalka, Bojan Cukic, and Arun Ross, "Protecting Iris Images through Asymmetric Digital Watermarking", Appeared in Proc.of 5th IEEE Workshop on Automatic Identification Advanced Technologies (AutoID), (Alghero, Itaiy), PP, 191_197, June 2007.

[16] Aboul Ella Hassanien · Ajith Abraham · Crina Grosan, " Spiking neural network and wavelets for hiding iris data in digital images", Springer-Verlag 2008 ,2009.

[17] Meenakshi Arya, and Rajesh Siddavatam, "A Novel Biometric Watermarking Approach Using LWT- SVD", V.V. Das, G. Thomas, and F. Lumban Gaol (Eds.): AIM 2011, CCIS 147, pp. 123–131, 2011. Springer-Verlag Berlin Heidelberg 2011.

[18] Bin Ma1, Chunlei Li1,2, Zhaoxiang Zhang1, and Yunhong Wang1, "Sparse Reconstruction Based Watermarking for Secure Biometric Authentication", Z. Sun et al. (Eds.): CCBR 2011, LNCS 7098, pp. 244–251, 2011. c_ Springer-Verlag Berlin Heidelberg 2011.

[19] Rajlaxmi Chouhan, Agya Mishra, and Pritee Khanna, "Wavelet-based Robust Digital Watermarking Scheme for Fingerprint Authentication", Rajlaxmi Chouhan is a Master student in Electronics & Communication, Engineering at Indian Institute of Information Technology, Design & Manufacturing Jabalpur 482 005 India, 2011.

[20] Sengul Dogan & Turker Tuncer & Engin Avci," A New Watermarking System Based on Discrete Cosine Transform (DCT) in Color Biometric Images", Received: 22 February 2011 / Accepted: 6 April 2011, Springer Science +Business Media, LLC 2011.

[21] Sandip Dutta, Avijit Kar, N.C. Mahanti, and B.N. Chatterji, "a biometrics based(fingerprint) Encryption / Decryption Scheme", 2012.

[22] Khattab M. Ali Alheeti, "Biometric Iris Recognition Based on Hybrid Technique", International Journal on Soft Computing (IJSC) Vol.2, No.4, November 2011.

Authors

[1]Muzhir Shaban Al-Ani has received Ph. D. in Computer & Communication Engineering Technology, ETSII, Valladolid University, Spain, 1994. Assistant of Dean at Al-Anbar Technical Institute (1985). Head of Electrical Department at Al-Anbar Technical Institute, Iraq (1985-1988), Head of Computer and Software Engineering Department at Al-Mustansyria University, Iraq (1997-2001), Dean of Computer Science (CS) & Information System (IS) faculty at University of Technology, Iraq (2001-2003). He joined in 15 September 2003 Electrical and Computer Engineering Department, College of Engineering, Applied Science University, Amman, Jordan, as Associated Professor. He joined in 15 September 2005 Management Information System Department, Amman Arab University, Amman, Jordan, as Associated Professor, then he joined computer science department in 15 September 2008 at the same university. He joined in August 2009 Computer Science Department, Anbar University, Anbar, Iraq, as Professor.

[2]Khetam Abd Al_Baset Al_Heety has received B.Sc. in Computer Science, Al-Anbar University, Iraq, (2005-2009). M.Sc student (2012- tell now) in Computer Science Department, Al - Anbar University. Fields of interest: Adapting of Biometric image and watermark technique. He taught many subjects such as steganography system, computer vision, image processing.