IOSR Journal of Computer Engineering (IOSR-JCE)
e-ISSN: 2278-0661, p- ISSN: 2278-8727Volume 15, Issue 1 (Sep. - Oct. 2013), PP 06-11
www.iosrjournals.org

Enhancing Security of Multimodal Biometric Authentication System by Implementing Watermarking Utilizing DWT and DCT

Dr. N. Chaudhary[1], Dr. D. Singh[2], D.Hussain[3]
[1](Professor, Computer Science and Engineering, College of Technology and Engineering, India)
[2](Assistant Professor, Computer Science and Engineering, College of Technology and Engineering, India)
[3](Computer Science and Engineering, College of Technology and Engineering, India)

Abstract : *Conventional personal identification techniques for instance passwords, tokens, ID card and PIN codes are prone to theft or forgery and thus biometrics isa solution thereto. Biometrics is the way of recognizing and scrutinizing the physical traits of a person. Automated biometrics verification caters as a conducive and legitimate method, but there must be an assurance to its cogency. Furthermore, in most of the cases unimodal biometric recognition is not able to meet the performance requirements of the applications. According to recent trends, recognition based on multimodal biometrics is emerging at a greater pace. Multimodal biometrics unifies two or more biometric traits and thus the issues that emerge in unimodal recognition can be mitigated in multimodal biometric systems. But with the rapid ontogenesis of information technology, even the biometric data is not secure. Digital watermarking is one such technique that is implemented to secure the biometric data from inadvertent or premeditated attacks.This paper propounds an approach that is projected in both the directions of improving the performance of biometric identification system by going multimodal and, increasing the security through watermarking. The biometric traits are initially transformed using Discrete Wavelet and Discrete Cosine Transformation and then watermarked using Singular Value Decomposition. Scheme depiction and presented outcomes justifies the effectiveness of the scheme.*

Keywords: *Discrete Cosine Transform (DCT), Discrete Wavelet Transform (DWT), Multimodal biometrics, Singular Value Decomposition, Watermarking*

I. INTRODUCTION

In this era of Information technology and electronic revolution, automatic access of individuals to services is becoming vital. Authenticating the identity of an individual is a prerequisite for completion of all commercial or personal transactions. Forgery and fraud can be prevented only if one establishes its identity with certainty which is unattainable in case of traditional authentication methods that are either token based such as ID Card (that are likely to be lost, forged or stolen), or knowledge based such as passwords (which can be forgotten). This has led in the emergence and formulation of a new technological area known as biometric recognition, or simply stated as biometrics [1]. Biometrics is the science of asserting the identity of an individual through physical assessment for example fingerprints, iris, hand geometry, face recognition etc. or behavioral characteristic that include voice, gait recognition, keystroke scanning, signature-scan. The association of biometric traits with the user is permanent and also these traits are unique for an individual and cannot be easily modified and forged. Thus biometrics is believed to be a more reliable technology. Biometric authentication systems have inherent advantages over traditional personal identification techniques [2]. However, the security of biometrics data is preeminent and must be shielded from external invasion and tampering as they are not endowed with security themselves [1]. It is therefore necessary to provide security to the biometric templates of individuals at all times.

One way of addressing this issue is Encryption [3, 4]. Encryption does not contribute to the much needed mutually integrated security and is ineffective once the data is decrypted after it is being transmitted over the network. Cryptography uses methods of encryption to construct secure information. As cryptography and encryption are not fully capable of providing security throughout the entire life of the work [4], digital watermarking has emerged to fulfill this requirement. In biometric watermarking, a piece of information termed as watermark, is embedded into the host image using a secret key, in such a way that the contents of the host image are not modified to the extent that are perceptible to the Human Visual System (HVS).Further biometric authentication systems based upon only one of the biometric modalities may not fulfill the requirements of demanding applications in terms of universality, uniqueness, performance, acceptability, permanence, collectability and circumvention. These factors paved a way for the development of multimodal biometric authentication system. Multimodal biometric systems use more than one biometric trait in order to identify an individual. These systems provide superior recognition rate in contrast to unimodal systems [5]. The biometric modalities, such as fingerprint, face and iris are one of the most conventional and effective modalities [6].

To enhance the security and performance of multimodal biometrics authentication system this paper targets on watermarking face image with fingerprint image by using a robust watermarking scheme. Then comparing the watermarked image and extracted image with the original images in order to prove that the watermarking and extraction procedure does not affect the recognition capacity of the overall system.

This paper is formulated in the following manner: the background details related to the technique are stated in Section II. The proposed robust watermarking algorithm for biometric images is described in Section III. In Section IV the results are outlined to assess the significance of the proposed technique on the overall performance of the system. And, conclusions of the scheme are drawn in Section V.

II. BACKGROUND

1. Watermarking

Watermarking [7,8,9] is the technique of embedding data into elements such as an image, video or audio file for authentication purpose. The data which is embedded can later be detected and extracted from, the elements for security reasons. A watermarking algorithm comprises of a watermark structure, an embedding algorithm, and a detection or extraction algorithm. In most of the applications where security is necessary, embedded watermark is required to be robust, invisible and should have a high capacity. Essentially watermarks are used for the purpose of copyright protection i.e. identifying from where the content originated, tracing illegal distribution of copies and undermining unauthorized access to content. The requirements for watermarks in varied scenarios differ. Embedding a single watermark into the content at the source of distribution is sufficient for identification of the origin of content [11]. To trace illegal copies, based on the identity or location of the recipient in the network a unique watermark is required. Non-blind schemes are suitable for both these application as watermark extraction or detection is required only when there is a dispute in context of the ownership of content. Access control, is performed through semi-blind or blind schemes where the watermark should be checked in all authorized consumer devices.

Recently, many watermarking schemes have been developed using the two most popular transforms that are Discrete Cosine Transform (DCT), and Discrete Wavelet Transform (DWT). The generic model of watermark embedding and extraction is shown in Fig. 1.

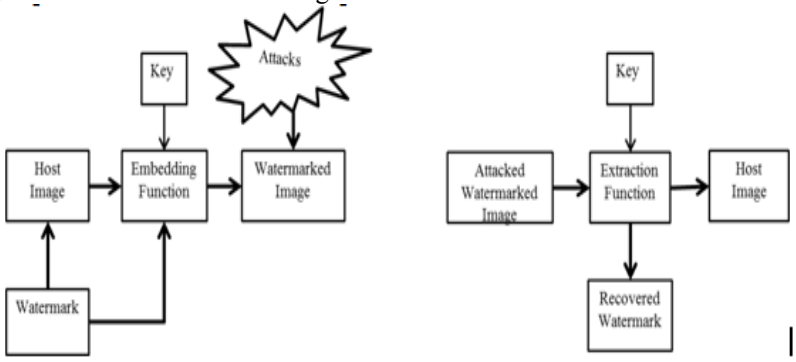

Fig.1: Model for Watermark embedding and extraction

In embedding module the host image is watermarked with the message image using a secret key and embedding function. The watermarked image is stored in the database or transmitted over the network where there is a possibility that it may be attacked. In the extraction module the watermarked image which might have been attacked is fed to the extraction function along with the secret key and the watermark or message image is extracted from it.

Discrete Wavelet Transform

The primary concept of DWT is that a one dimensional signal is divided into two parts one is high frequency band and another is low frequency band. Then the low frequency band is further split into two parts and the same process continues until the desired level is reached. For M*N 2-D images, applying DWT corresponds to processing the image by 2-D filters in each dimension and results in the generation of four M/2*N/2 coefficients. The filters divide the input image into four non-overlapping multi-resolution coefficient sets, (LL1) a lower resolution approximation image as well as (HL1) horizontal high frequency band, (LH1) vertical high frequency band and (HH1) diagonal high frequency band. The information of low frequency band is an image close to the original image. In DWT decomposition, input signal must be a multiple of 2^n. Where, n is equivalent to the number of levels. DWT provides sufficient information to analyze and synthesize the actual signal and also requires less computation time. Fig. 2 shows the two-level DWT decomposition of an image.

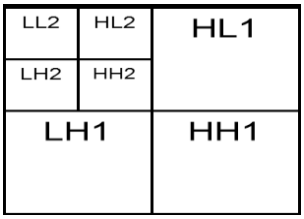

Fig.2: Two level DWT decomposition

Discrete Cosine Transform

In digital signal processing one of the most prevalent linear transformation functions is DCT. It converts spatial or time domain signal to frequency domain and the image is transformed into a form of an even function. In comparison to spatial domain techniques DCT techniques are more robust. Algorithms based on DCT are robust against common image processing operations like adjustment, blurring, brightness, low pass filtering, and contrast and so on. One-dimensional signals like speech waveforms can be processed with one dimensional DCT. For analysis of 2D signals like images, we require 2-D DCT. The two-dimensional DCT of any given matrix gives the frequency coefficients in form of another matrix. The lowest frequency coefficients are represented at the Left topmost corner of the matrix while the highest frequency coefficients are represented at the right bottom most corner of the matrix.

Formula for 2-D DCT:

$$F(m,n) = \sum_{i=0}^{N-1} \sum_{j=0}^{N-1} C(m)C(n)f(i,j)\cos\left[\frac{\pi(2i+1)m}{2N}\right] * \cos\left[\frac{\pi(2j+1)m}{2N}\right]$$

Formula for 2-D inverse DCT:

$$F(i,j) = \sum_{i=0}^{N-1} \sum_{j=0}^{N-1} C(m)C(n)F(m,n)\cos\left[\frac{\pi(2i+1)m}{2N}\right] * \cos\left[\frac{\pi(2j+1)m}{2N}\right]$$

Where,

$$C(m), C(n) = \begin{cases} \sqrt{\frac{1}{N}} & |m,n = 0 \\ \sqrt{\frac{2}{N}} & |m,n = 1\ upto\ N-1 \end{cases}$$

Singular Value Decomposition

Singular Value Decomposition is an effective tool for image transformation and it is based on a theorem from linear algebra which states that a rectangular matrix A can be divided into the product of three matrices; U - an orthogonal matrix, S- a diagonal matrix, and V - the transpose of an orthogonal matrix. The theorem is represented as:

$A_{m*n} = U_{m*m}\ S_{m*n}\ V^T_{n*n}$

Where;

$U^TU = I;\ V^TV = I;$

The columns of U are orthonormal eigenvectors of AA^T,

The columns of V are orthonormal eigenvectors of A^TA, and

S is a diagonal matrix that contains the square roots of eigenvalues from U or V in descending order.

III. THE PROPOSED SCHEME

In the proposed scheme one biometric data is watermarked with another biometric data using SVD based hybrid watermarking scheme. In the proposed scheme face image is used as the cover image or host image which is watermarked using the fingerprint image. This hybrid watermarking technique is depicted schematically as well as algorithmically.

1. Watermark Embedding Algorithm

Initially weinput the Cover image I and DWT is applied on the Cover image I which decomposes image into four sub-bands LL, HL, LH and HH further DCT is applied to all the high frequency bands and SVD is applied to all the high frequency bands to get the matrices SH1_I, SH2_I and SH3_I. Watermark image W is given as input. DWT is applied on the Watermark image W which decomposes into four sub-bands LL1, HL1, LH1 and HH1.DCT is applied to all high frequency bands further SVD is applied to all the higher frequency bands and get the respective matrices.Utilizing the singular values of Watermark image the singular values of

the cover image are modified.Modified SVD matrix is constructed. Inverse DCT is applied to all high frequency bands then inverse DWT is applied to get the final watermarked image.
Fig. 3 shows the watermarking procedure schematically

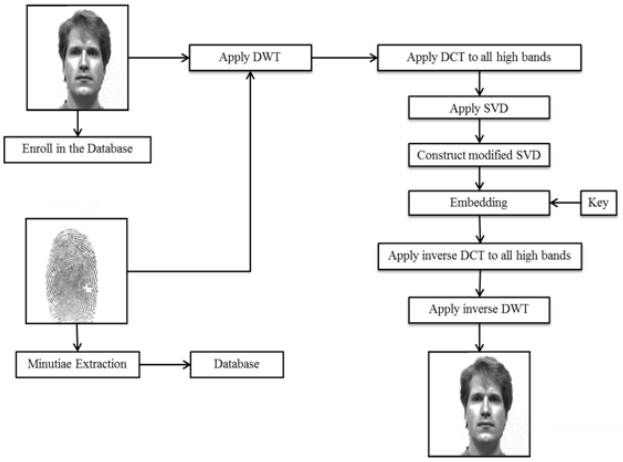

Fig.3: Watermark embedding procedure

2. Watermark Extraction Algorithm

Input Watermarked image W_I.DWT is applied on the Watermarked image W_I; it decomposes image into four sub-bands LL_W, HL_W, LH_W and HH_W. All high frequency bands are selected and DCT is applied to all those bands. Then SVD is applied to all the high frequency bands to get the matrices SH1_WI, SH2_WI and SH3_WI.SH1_WI, SH2_WI and SH3_WI are modified. Modified SVD matrix is constructed.Inverse DCT is applied to all high frequency bands.Inverse DWT is applied to get the final extracted watermark image.

Fig. 4 shows the watermark extraction procedure schematically

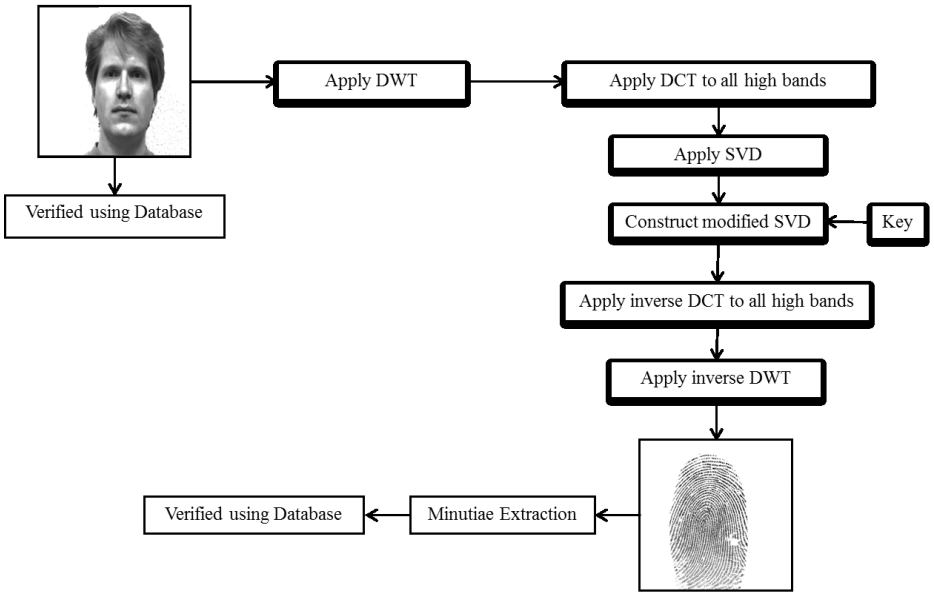

Fig. 4: Watermark extraction procedure

IV. IMPLEMENTATION AND RESULTS

Broadly, a watermarking algorithm can be assessed based on two parameters: imperceptibility and robustness. The similarity or correlation between the original watermark and the Extracted watermark is quantitatively measured by utilizing Normalized Cross-Correlation (NCC) [12].

The formula for Normalized Cross-Correlation (NCC) is

$$NCC = \sum_i \sum_j \frac{w(i,j)w'(i,j)}{\sum_i \sum_j |w(i,j)|^2}$$

The value of Normalized Cross-Correlation lies between [-1, 1]. And greater NCC value means the watermark is more robust [13,14]. Peak Signal to Noise Ratio (PSNR) is used in quantitatively analyzing the concealing capacity of the algorithm. Peak Signal to Noise Ratio (PSNR) is defined as:

$$PSNR = 10 \log_{10} \left(\frac{255^2}{MSE} \right)$$

The unit is decibels (dB). The larger the value of PSNR is, the better the imperceptibility of watermark.Performance of the algorithm is tested by simulating the experiment on MATLAB 2012a. 256x256 pixels of gray-level host image and watermark image are chosen for the purpose of simulation of the algorithm. The original cover image, watermarked image and the extracted watermark images are shown in Fig.5.

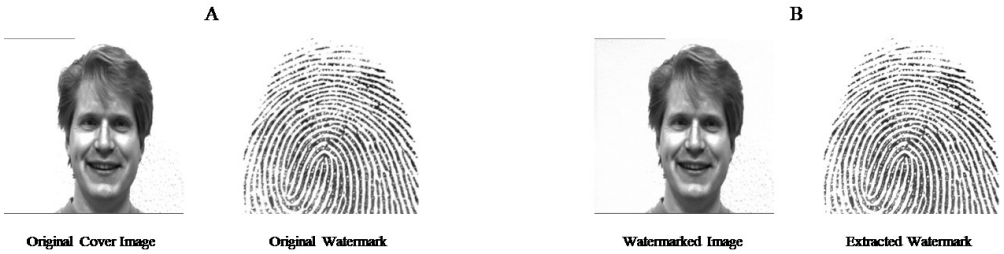

Fig. 5: [A] Original cover and Watermark image [B] Watermarked image and Extracted watermark

The watermarked image resembles the original image in vision impression to a large extent. To the Human Visual System there is no clearly visible difference between the two images. Thus, this algorithm hides watermark very well. The PSNR of the original cover image and watermarked image is 46.041 dB, which is considered a quite good value. Along with that, the NCC of the original watermark image and extracted watermark is 0.9727, which shows that the two images are strongly correlated.

In order to test the robustness of the algorithm, it is tested under different types of attacks. The images on which attacks have been applied are shown in Fig.7. The Extracted Watermark images along with their NCC values are shown in Fig.6

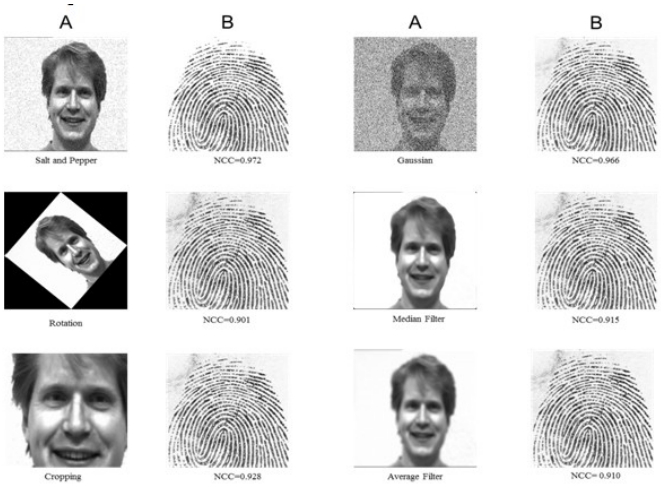

Fig. 6: [A] watermarked images that are attacked [B] Extracted watermark with normalized cross correlation

The simulation results show that the watermark image can be extracted well even after the watermarked image is attacked. Simulation results indicate that this watermarking algorithm is robust against many common attacks like adding salt noise, filter, image compression, sharp enhancing, image cutting and rotation.

V. CONCLUSION

This paper proposed a discrete wavelet transform (DWT) and discrete cosine transform (DCT) based watermarking algorithm for biometric data. By using Singular Value Decomposition, watermarking signals are embedded in the high frequency bands of wavelet transformation domain. And before the embedding procedure is followed the watermark image is also transformed using both DWT and DCT. The simulation results prove that this watermarking algorithm not only keeps the image quality well, but is also robust against many image processing operations. This algorithm is very efficient in embedding signals and also anti-attack.

REFERENCES

[1] A. K. Jain, U. Uludag, Hiding Biometric Data,*IEEE Trans. Pattern Analysis and Machine Intelligence, 25(11),* Nov. 2003, 1494 – 1498.

[2] A. K. Jain, A. Ross, and S. Prabhakar, An introduction to biometric recognition,*IEEE Transactions on Circuits and Systems for Video Technology,14(1),*200,4-20.

[3] U. Uludag, S. Pankanti, S. Prabhakar, and A.K. Jain, Biometric cryptosystems: issues and challenges, *Proceedings of IEEE, 92(6),*2004, 948-960.

[4] Y. Dodis, L. Reyzin, and A. Smith, Fuzzy extractors: how to generate strong keys from biometrics and other noisy data, *Eurocrypt*2004, 523-540.

[5] A.Nagar, K.Nandakumar, A. K.Jain, Multibiometric Cryptosystems Based on Feature-Level Fusion, *IEEETrans. Inf. Forensics Security, 7(1),* Feb. 2012, 255 – 268

[6] Z. huiming, Z.Huile, A technology of hiding fingerprint minutiae in image,*Research & progress of solid state electronics, 26(2),*2006, 197-200.

[7] C. I. Podilchuk and E. J. Delp, Digital Watermarking: Algorithms and Applications, IEEE *Signal Processing Magazine,* July 2001, 33-46.

[8] I. J. Cox, M. L. Miller, and J. A. Bloom, *Digital Watermarking* (Morgan Kaufmann Publishers, 2002).

[9] E. T. Lin, A. M. Eskicioglu, R. L. Lagendijk and E. J. Delp, Advances in Digital Video Content Protection, *Proceedings of the IEEE, Special Issue on Advances in Video Coding and Delivery, 2004*.

[10] G.C. Langelaar, I. Setyawan, R.I. Lagendijik, Watermarking digital image and video data, *IEEE Signal Processing Magazine 17 (5) 2000, 20–46.*

[11] N.F. Johnson, Z. Duric and S. Jajodia, *Information Hiding, Steganography and Watermarking-Attacks and Counter Measures*, Kluwer academic publisher, 2003, 15-29.

[12] M. Nageshkumar , P.K. Mahesh , M. N. ShanmukhaSwamy, An Efficient Secure Multimodal Biometric Fusion Using Palmprint and Face Image,*IJCSI International Journal of Computer Science Issues*, *2*, Aug. 2009,49-53.

[13] J Jiang, A. Armstrong, Data hiding approach for efficient image indexing, *Electronics letters. 7th, 38(23),*2002, 1424- 1425.

[14] I.J .Cox, J.G. Linnartz, Some general methods for tampering with watermarks, *IEEE Journal on Selected Areas in Communications,16(4),*1998, 587-593.