IJCSC 0973-7391 Volume 8 • Issue 2 March 2017 - Sept 2017 pp. 28-33 available online at www.csjournalss.com

# Enhancing the Security of Biometric System Using DWT Watermarking

Komal[1], Dr.Chander Kant[2]
M.Tech Scholar[1], Assistant Professor[2]
Department of Computer Science and Applications,Kurukshetra University,Kurukshetra, India.

**Abstract:** With the increasing popularity of biometric recognition applications, many security violations have been discovered. Watermarking (WM) has been suggested as a means to resolve some of these problems and can potentially add additional functionalities to biometric systems. The aim of watermarking is to transmit biometric data hidden into host data. Therefore, this acts as a steganographic application scenario, which is based on template embedding. The paper presents 1-level discrete wavelet transform technique for insertion and extraction of watermark in original image. The technique is found to be much simpler and robust than others. The technique is compared with simple LSB method in terms of their merits and demerits over DWT. The proposed framework was implemented using MATLAB software.

**Keywords:** Biometrics, Watermarking, Biometric Watermarking, DWT, LSB, Watermark Embedding and Extraction.

## I. INTRODUCTION

Biometrics is the measurement and statistical analysis of people's physical and behavioural characteristics. The term "biometrics" is derived from the Greek words “bio” meaning life and “metric” meaning to measure. The technology is primarily used for identification and access control, or for identifying individuals that are under observation. Biometric authentication is based on the principle that everyone is unique and an individual can be identified by his or her intrinsic physical or behavioural traits. Biometric applications available today are categorized into 2 sectors;

1) Psychological: Iris, Fingerprints, Hand, Retinal and Face recognition
2) Behavioral: Voice, Typing pattern, Signature

The major building block of any system security comprises of Proper user identification and authentication that comes under access control. For the wide spread utilization of biometric techniques, an increase in the security level of biometric data is necessary [1]. Most common Techniques to achieve this are Encryption and watermarking .But since encryption does not provide security once the data is decrypted, Watermarking is used most commonly as it involves embedding information into the host data to provide greater level of security. A simple block diagram of such an watermarking system in shown below in fig 1.

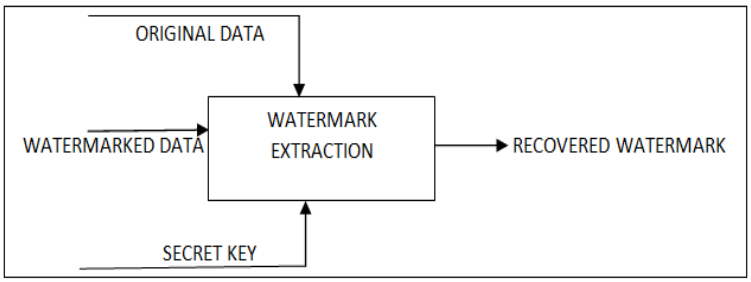


Fig 1: A Simple Diagram of Watermarking System

The biometric watermarking is a technique of embedding biometric templates into cover image using some known algorithm depending upon the requirement to identify the owner of the document [2]. Two commonly used domains for watermarking are spatial domain and transform domain. Spatial domain involves modifying the pixels of an image depending upon perceptual analysis of an image. Whereas in transform domain some frequencies are selected and then are modified from their original values according to certain rules. Also the watermark embedding is found to be more robust in this domain as compared to spatial which leads to its popularity even more. In addition, it also provides more security and imperceptibility [3-5].

The paper discusses the watermarking scheme based on DWT (discrete wavelet transform) which works in transform domain.

### A. PARAMETERS OF BIOMETRIC SYSTEMS:

There are certain factors that make one biometric system to be more secure than the one. The section discusses some of the differences among such systems.

- Liveness testing: Integration of a liveness test makes an attack against the biometric system more difficult. Level of protection varies with the type of liveness tests. It's better to have the combination of multiple liveness tests making the system more secure.
- Tamper resistance: Tamper resistance becomes more important if the biometric system is not under constant human supervision. Without proper supervision the system can be tampered with and forged/replied biometric data can be injected into the system.
- Secure communication: Biometric system can communicate with each other over an external insecure medium or within a secure tamper-resistant box. The communication over an insecure line should be well authenticated and encrypted.
- Security threshold level: Lower the false acceptance rate, higher will be the level of security.
- Fall-back mode: Since biometric authentication is only a necessary part of user authentication therefore proper authentication methods must be used in system as per their needs.

## 2. RELATED WORK:

Alpha blending technique by using DCT domain was proposed by Bo Shen ,Ihwar k. Sethi and Vasudev Bhaskaran [6]. AkhilPratap Singh and Agya Mishra [7] proposed DWT domain watermarking by using alpha domain technique and then compared the PSNR values of recovered image with original image.

Mathivadhaniet. al. [8] compared the other biometric watermarking techniques of Zebbiche et al. [9] and Vasta et al. [10], both of which are based on Discrete Wavelet Transformation (DWT). They found that, both provide adequate security to the data without degradation of visual quality.

RajlaxmiChouhan et al., [11] proposed Fingerprint Authentication by Wavelet-based Digital Watermarking. The DWT technique has been found to give better robustness against noises, geometrical distortions, filtering and JPEG compression attack than other frequency domain watermarking techniques. Moreover the proposed method is compared with DCT based and hybrid DWT- DCT watermarking techniques, but as a resultant the performance of the proposed technique is better than the other compared techniques.

NilanjanDey et al.,[12] proposes a DWT based Steganographic technique. He decomposed the Cover into four sub bands using DWT. After that Encoded Secret image using spiral scanning is hidden by alpha blending technique in HH sub bands. Encoded secret images are extracted to recover the original secret image. In this approach the generated stego image is imperceptible and security is high.

## 3. DISCRETE WAVELET TRANSFORM (DWT):

DWT involves a multi-resolution decomposition of a signal. Discrete Wavelet Transform is used for mapping an image into a set of coefficients by hierarchically decomposing an image. Also it can be used to provide frequency and spatial domain of an image by capturing its the frequency and location information. Decoding is carried out in low resolution to high resolution manner. .High and low frequency parts are obtained on decomposing an image by dwt. While the information about edge components are contained in high frequency parts, low frequency parts again get decomposed into another set of low and high frequency parts forming an image that is further divided into four multiresolution sub-bands LL, LH, HL and HH using DWT as shown in fig 3.

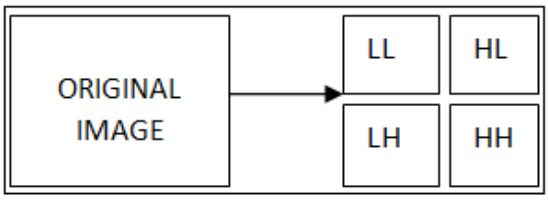


Fig 3: 1 Level Discrete Wavelet Decomposition

LH, HL, HH sub-bands represents the fine-scale DWT coefficients while LL represents the coarse-scale DWT coefficients as shown in fig above. LL sub-band can further be decomposed into four multiresolution sub-bands

as in fig 4 giving next coarser wavelet coefficients. Depending upon the application the process can be repeated as per needs.

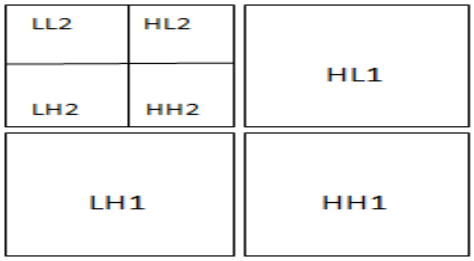


Fig 4: Sketch Map of Image Decomposed

**ALPHA BLENDING:**

The process of combining an image with a background to create the appearance of partial or full transparency is named as Alpha blending. It is done by blending each pixel from the first source image with the corresponding pixel in the second source image in image processing. In accordance to the formula of alpha blending, the watermarked image is given by WM1=k*LL + q*WM (1) where, WM1= Low frequency component of watermarked image, LL= low frequency component of cover image, WM= low frequency component of watermark, k and q= scaling factors for cover image and watermark respectively. Similarly, the recovered image is given by RW = (WMI-k*LL) (2) where, RW=Low frequency component of recovered watermark, WMI=Low frequency component of watermarked image, k=scaling factor for cover image.

**3. PROPOSED FRAMEWORK:**

Watermarking is used to secure templates, but the aim of watermarking is to;

1) detect any kind of tampering occurring with the original template
2) using one mode of template to watermark another template providing multimodal authentication, as well as, template protection.

Recently for enhancing the security of multimedia content, biometrics is merged with watermarking technology. Biometric watermarking is a special case of digital watermarking in which the watermark content is biometric data. Both digital watermarking as well as by biometric authentication can be used to verify an access control or authenticity of legitimate user as shown in fig5.

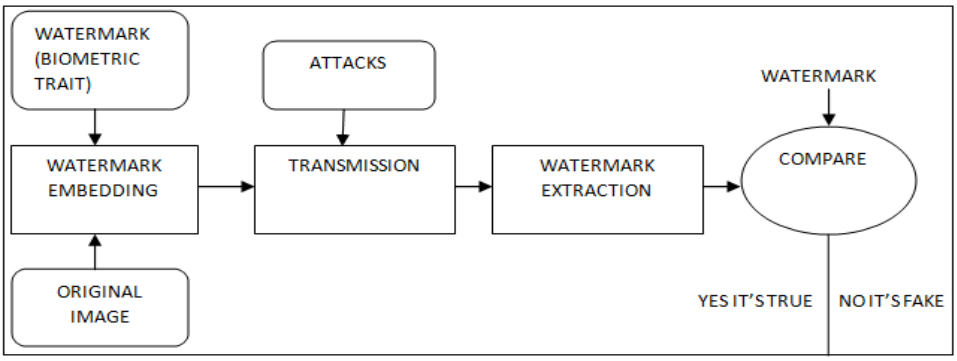


Fig 5: Biometric Watermarking System

Biometrics technology has the ability to differentiate well between an authorized person and malicious users who fraudulently acquires the access privilege of an authorized person is one of the main reasons for its popularity. In this paper DWT is used to combine watermarking with biometric features to develop more secured and confidential watermarking techniques for providing authenticity of multimedia content since biometric features are unique for each and every individual.

Firstly the cover image is taken and decomposed into four components i.e. low frequency approximation, high frequency diagonal, low frequency horizontal, low frequency vertical components using 2D DWT as in fig 6. LL1 gives lower resolution approximation coefficient and LH1, HL1; HH1 gives the detailed components of an image.

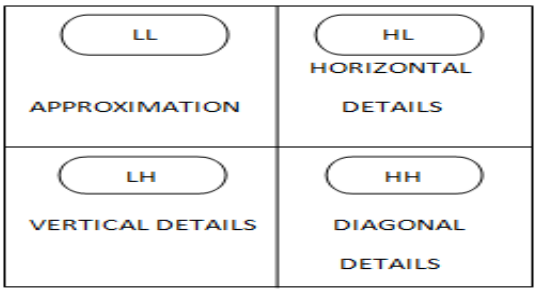


Fig 6: Frequency Bands in DWT

Exactly the same procedure is repeated on the watermark image i.e. the fingerprint that is to be embedded into cover image. After that alpha blending technique is used for inserting a watermark in cover image. The watermark cannot be directly embedded into cover image wavelet coefficients reason being that approximation wavelet coefficients contain more information of original watermark image so it is advisable to embed wavelet coefficients of watermark image into cover image. Since the watermark needs to be visible in nature, so watermark is embedded in low frequency approximation component of cover image. To extract the watermark back, alpha blending formula is applied to recover the watermark image from watermarked image. Here low frequency approximation component of cover image is first multiplied by a particular scaling factor and then subtracted from watermarked image coefficient.

**PROPOSED DIAGRAM:**

The diagrams for the proposed framework are shown below. Fig 7.1and 7.2 explains the process for watermarking embedding and extraction respectively.

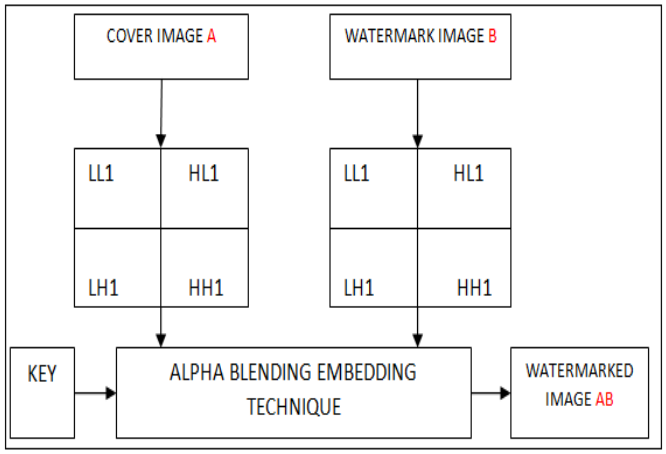


Fig 7.1: Watermark Embedding Technique

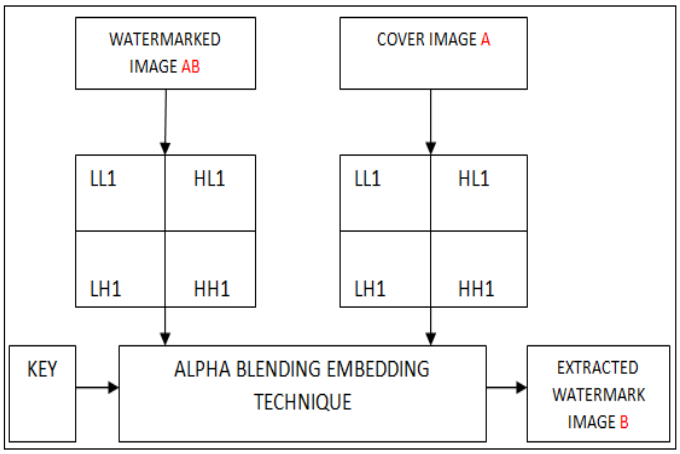


Fig 7.2: Watermark Extraction Technique

**RESULTS:**

Fig 8.1: Cover Image

Fig 8.2: Watermark Image

Fig 8.3: DWT2 of Cover ImageFig

8.4: DWT2 of Watermark Image

Fig 8.5: Watermarked Image

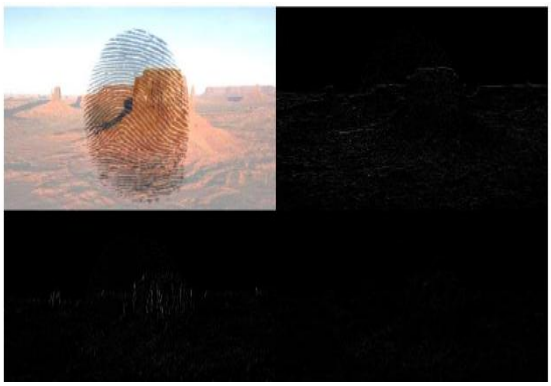

Fig 8.6: DWT2 of Watermarked Image

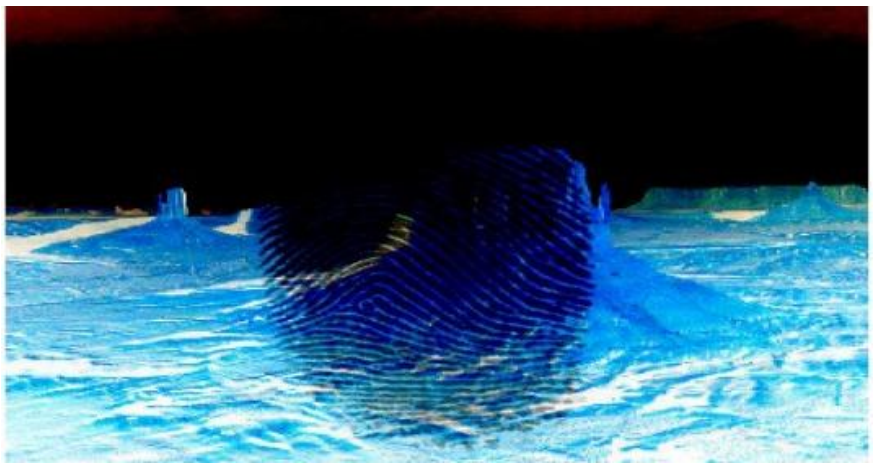

Fig 8.7: Extracted Watermark.

The results for biometric watermarking using DWT are shown above fig 8.1-8.7. Here we have used lowest bands (LL) of DWT because the magnitude of DWT coefficients is larger in LL bands as compared to other bands. Also the results for the quality of the watermarked image and the recovered watermark clearly depend upon scaling factor alpha and will vary with varying values of alpha. DWT method provides the advantage of high privacy and hides secret image very well.

**COMPARISION BETWEEN LSB AND DWT:**

The paper proposes the commonly used steganography techniques i.e. DWT. LSB substitution is also used for the same. Each of the method has its own merits and demerits.

- DWT changes the image composition by decomposing the image to uncorrelated data. This operation affects the entire image and hence the reconstructed image is smaller in size. On the other hand, LSB embeds about 60% of data bits giving the same size image as only the pixels values were altered.
- Discrete wavelet transform provides high compression ratio with good quality of reconstruction. While in comparison,Least Significant Bit substitution popularly known to increase capacity by reducing the quality of image.
- DWT method gives highest image quality for any light toned image while LSB Substitution is known to be suitable for dark cover image and secret image, where the bits substituted can be hardly visible to a human eye.

**CONCLUSION:**

The paper studies the method of biometric watermarking using DWT technique and its comparison with LSB technique. The reason behind using the Wavelet domain watermarking is its capability to reduce the risk of any distortions such as compression and low pass filtering that changes the high frequency components of an image but it is impossible for it to resist attacks that destroy the whole watermarked image such as cropping. More deep investigation can be carried out in the same to deal with this kind of attacks.

**REFERENCES:**

[1]. R. **M.** Bok, J. H. Connell, S. Pankanti, N. K. Ratha, A. W. Senior, "Guide to Biometrics", Springer Verlag, 2004

[2]. R. **M.** Bok, J. H. Connell, S. Pankanti, N. K. Ratha, A. W. Senior, "Guide to Biometrics", Springer Verlag, 2004

[3]. Nikita Kashyap, Sinha G.R,"Image Watermarking Using 2-Level DWT", Advances in Computational Research, Vol.4, Issue 1, 2012.

[4]. Kamran Hameed, AdeelMumtaz, S.A.M.Gilani,"Digital Image Watermarking in the Wavelet Transform Domain",World Academy of Science, Engineering and Technology 13, 2008.

[5]. Mohammad Reza Soheili,"A Robust Digital Image Watermarking Scheme Based on DWT, Journal of Computer Engineering 1, 2009.

[6]. Shen, Iihwar K. Sethi and VasudevBhaskaran (1998),"DCT Domain Alpha Blending", IEEE,

[7]. AkhilPratapSingh,"WaveletBased Watermarking on Digital Image

[8]. D. Mathivadhani, and C. Meena, A Comparative Study on Fingerprint Protection Using Watermarking Techniques, pg 98-102, Global Journal of Computer Science and Technology Vol. 9 Issue 5 (Ver 2.0), 2010.

[9]. K. Zebbiche, and F. Khelifi, Region-Based Watermarking of Biometric Images: Case Study in Fingerprint Images, International Journal of Digital Multimedia Broadcasting, Article ID 492942, Pp. 1-13, 2009.

[10]. M. Vatsa, R. Singh, A. Noore, M. M. Houck, and K. Morris, Robust biometric image watermarking for fingerprint and face template protection, IEICE Electronics Express, Vol. 3, No.2, Pp. 23-28, 2006.

[11]. RajlaxmiChouhan, A. M. (2012). Fingerprint Authentication by Wavelet-based Digital Watermarking. International Journal of Electrical and Computer Engineering,Vol.2, No.4 , 523-528.

[12]. NilanjanDey, S. S. (2011). A Novel Approach of Image Encoding and Hiding using Spiral Scanning and Wavelet Based Alpha- Blending Technique. IJCTA, Vol 2 (6) , 1970-1974.