I J C T A, 9(15), 2016, pp. 6931-6935

Digital Image Watermarking using Wavelet Packet Transform and Biometric Authentication

Honey Merrin Sam* and D. Saveetha**

ABSTRACT

Nowadays images from different sources are most of the time used and transmitted through the web for different applications, for example, online personal photo collections, social media files, document storage frameworks, medical imaging frameworks, and military imaging databases. These images normally contain private or secret data with the goal that they ought to be shielded from leakageduring transmissions. As of late, numerous techniques have been proposed for securing image transmission, for which two basic methodologies used are image encryption and data hiding.

"Watermarking" is the procedure of concealing computerized data in a carrier signal; the shrouded data ought to, yet does not have to, contain a connection to the carrier signal. Digital watermarks might be utilized to check the authenticity or integrity of the carrier signal or to demonstrate the identity of its proprietors. It is unmistakably utilized for tracing copyright infringement and for banknote authentication.

The majority of the data distribution or redistribution happens on the web. Be that as it may, to assert the ownership and copyright protection, some additional data which can't be removed by intruders, is important to provide security. Such a security is given by Watermarking. In this paper, a robust digital image watermarking algorithm is projected in Wavelet Packet Transform(WPT) domain using biometric authentication. The proposed strategy is more secure and strong to a few attacks such as: Resizing, Median filtering, Row-Column copying, Low pass filtering, JPEG Compression, Rotation, Salt and Pepper Noise, Cropping, Bit Plane Removal, Blurring, Row-Column blanking, Intensity Transformation, and so forth.

Keywords: Watermarking, Biometric authentication, Wavelet Packet Transform

1. INTRODUCTION

Working together on the Internet has turned into an essential plan of action at present time. Since each transmitted information is digitized and can be effectively copied, the issue of the copyright security for business or sensitive information develops to an unavoidable situation for some organizations. Digital watermarking rose as an tool for shielding the multimedia information from copyright infringement. In digital watermarking an imperceptible signal "mark" is implanted into host image, which uniquely identifies the ownership. The main requirements of the watermarking are imperceptibility and robustness to intentional and unintentional attacks.

Random number is used as watermark in Discrete Cosine Transform based embedding scheme. Similar approach can be applied to other transform like the Discrete Wavelet Transform. It is necessary to refer the original image in order to extract the watermark, which is a drawback of this approach. This makes the authentication process difficult. Transform domain methods are more robust than spatial domain methods. It is because,the attacker finds it difficult to read or modify, when image is inverse transformed watermark

* Information Security and Cyber Forensics, Department of information Technology,SRM University, Chennai, India, *Email: honeydrops619@yahoo.com*

** Department of Information Technology, SRM University, Chennai, India

and is distributed irregularly over the image. Because of the use of Human Visual System (HVS) model, wavelet based watermarking methods are gaining more popularity. Another important issue in watermarking is access to original image. In many applications it is difficult to have access to original image, so it is desirable that the watermarks should be extracted without using original image.

Watermarking strategies are additionally characterized into two classifications in light of embedding mechanism. In the principal technique, watermark bits are added straightforwardly to the host information by encoding or modulating. Illustration of this sort of technique is spread spectrum watermarking [4]. In the second technique, single coefficients or group of coefficients are mapped to describe one bit of watermark data. These strategies are free from host interference. Illustration of this method is quantization based watermarking [3], [10].The strategies examined above have not appropriately exploited HVS attributes in embedding the watermark and consequently these techniques are very little robust against deliberate and inadvertent attacks.

Biometric watermarking applications are extensively grouped into two classes. In one situation one biometric is implanted in another, which only goes about as a bearer to secure the previous genuine biometric. In the second situation, two biometrics initial one implanted in the second biometric is further encoded in smart cards to upgrade the security.Smart ID cards frequently provide the protected, helpful and cost-effective ID innovation that stores the selected biometric layout and compares it to the “live” biometric format.

In this paper, wavelet packet based watermarking method is used, to embed watermark more robustly by exploiting HVS characteristics. To provide more security the minutiae value is used as key to encrypt the watermark before embedding.We don’t need the original image for watermark extraction; just the secret biometric key is enough. The watermark can only be extracted by providing the same fingerprint that was given during embedding process.

2. PROPOSED SYSTEM

The proposed method creates the biometric key by extracting minutiae value using the user’s fingerprint such that the watermark will be more protected; furthermore, it is shielded from the malicious attackers who may modifyit. During the decryption phase, the fingerprint is provided to revealthe secret watermark image.

2.1. HVS Characteristics

The sensitivity of human eye is affected by many factors like luminance, frequency and texture. The human eye is less sensitive to areas of the image where brightness is high or low. The sensitivity of thehuman eye to noise in thetextured area is less and it is more near the edges. In [8], these observations are exploited for finding weight factors to quantize wavelet coefficients for image compression. With some modification, Barni et al. [2], used these weight factor in embedding the watermark. With some modifications, a method for exploiting HVS characteristics in wavelet packet domain was presented.

A 4-level transformed image on the basis of wavelet packet is described above in figure 1. The images are processed using Db1 or Haar wavelet.

For $N \in N$, a Daubechies wavelet of class D-2*N* is a function $\Psi = N\Psi \in L^2(R)$ defined by

$$\psi(x) := \sqrt{2}\sum_{k=0}^{2n-1}(-1)^k h_{2N-1-k}\phi(2x-k) \tag{1}$$

Where $h_0,\ldots,h_{2N-1} \in \mathbf{R}$ are the constant filter coefficients satisfying the following conditions as mentioned below:

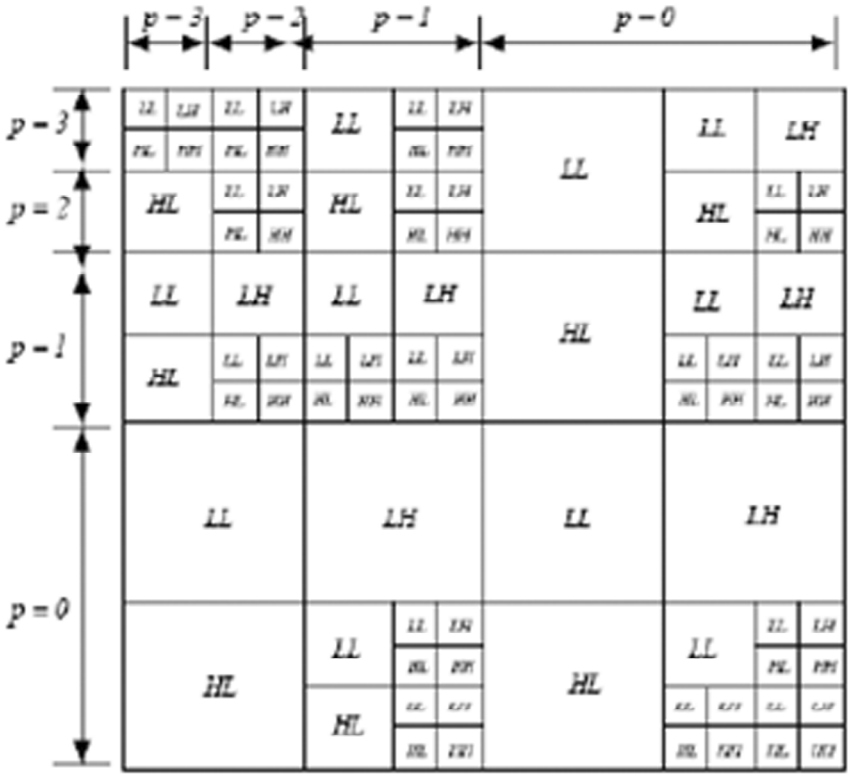

Figure 1: 4-level wavelet packet basis representation.

Õ = N^{Õ} : R → R is the (Daubechies) scaling function (sometimes also "scalet" or "father wavelet"), given by the recursion equation

$$\phi(x) = \sqrt{2} \sum_{k=0}^{2N-1} h_k \phi(2x - k) \tag{2}$$

And obeying

$$\phi(x) = 0 \qquad \text{for } x \in \mathbf{R} \backslash [0, 2N-1] \tag{3}$$

2.1.1. Haar wavelet (D2 wavelet)

Here N = 1 and $h_0 = 1/\sqrt{2},\ h_1 = 1/\sqrt{2}.$ Then the function with the initial values $\phi(0) = 1$, $\phi(k) = 0$, for $k \in Z$, $k \neq 0$; This determines the unique scaling function.

Õ and Ψ turn out to be simply the step functions

$$\phi(x) = \begin{cases} 1 & if\ 0 \le x \le 1, \\ 0 & otherwise \end{cases} \qquad \psi(x) = \begin{cases} 1 if\ 0 \le x < \frac{1}{2} \\ -1 if\ \frac{1}{2} \le x < 1 \\ 0 \qquad otherwise \end{cases} \tag{4}$$

2.2. Watermark Embedding and Extraction

This is thesecond phase of our approach which will embed the watermark after it is being encrypted by the fingerprint minutiae value. We have used N level wavelet decomposition on both the host and watermark

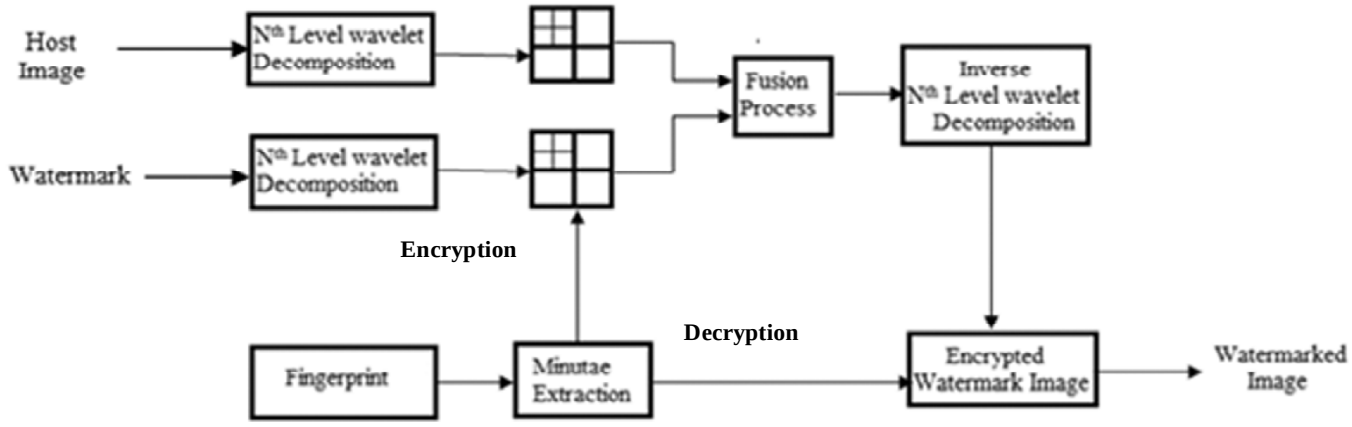

Figure 2: Biometric authenticated watermarking model

image. First, we have generated the key from fingerprint and then performed the encryption followed by the embedding process. Results of this phase are encrypted watermark image.

2.3. Minutiae Extraction

There are totally five modules used in this section which is listed as below. Each module has aspecific usage in the project and its description is given below. A fingerprint is made of a series of ridges and furrows on the surface of a finger. Uniqueness can be determined by the pattern of ridges and furrows as well as the minutiae points.

2.3.1. Finger Image Preprocessing

The performance of a minutiaeextraction algorithm relies heavily on the quality of the input fingerprint images

Before extracting the proposed ridge features, we need to perform some preprocessing additional procedures for quality estimation.

2.3.2. Binarize

We binarize the image. This operation gives us the fingerprint, where ridges are black in color and furrows are white. It transforms the image from 256-level image to a 2-level image that gives the same information.

2.3.3. Ridge Thinning

This process is carried to eliminate unwanted pixels of the ridge, till they are just one pixel wide. This helps to get a clear view of the ridges and bifurcations

2.3.4. Minutiae Feature Extraction

In this method, two different types of minutiae like ridge and bifurcation points are identified. If a minutia is an end point, there is only one ridge belonging to the minutia. If a minutia is a bifurcation, there are three ridges connected to the minutiae.

2.3.5. Eliminating False Minutiae

The preprocessing stage does not usually fix the fingerprint image in total. Forexample, false ridge breaks due to aninsufficient amount of ink and ridge cross-connectionsdue to over inking are not totally eliminated. As there are lots of spurious minutiae, the false ones are removed from the fingerprint image, as they will

significantly affect the accuracy of matching. False minutiae are determined depending on a predefined distance between any two of the minutiae points. They are processed between two ridges or two bifurcations or between a ridge and bifurcation.

2.3.6. Matching/Recognition

We need an adaptive matching algorithm for the minutia patterns. It is because the strict match requires that all parameters (x, y, θ) are thesame for two identical minutiae.When using biometric-based matching, it is impossible to go for strict matching.

Therefore, we have to set a threshold value for matching in the form of a ratio. The match ratio for two fingerprints is the number of totalmatched pairs divided by the number of theminutia of the template fingerprint.The score is 100*ratio. It ranges from 0 to 100. Thetwo fingerprints are from the samefinger, if the score is larger than apre-specified threshold (typically 80%).

3. RESULTS AND CONCLUSION

In this paper, we have proposed a 3-level Wavelet Packet Transform for the image watermarking. The proposed method of watermarking is perceptually invisible. Perceptually invisiblemeans that modification of pixels cannot be noticed when the watermark is embedded in an image. We have also mentioned how minutiae is used as the secret biometric key in brief. To gain more security in images is conveniently explained in this proposed method.

REFERENCES

[1] A. Geetha, B. Vijay Kumari, C. Nagavani, T.Pandiselvi, *Digital image Watermarking Based on wavelet Packet*, International Journal of Computer Science, November 2011.

[2] M. Barni, F. Bartolini,and A. Piva. Improved Wavelet-based Watermarking through Pixel-wise Masking.IEEE Transaction on Image Processing, May 2001.

[3] L.H. Chen and J.J. Lin. Mean Quantization based Image Watermarking. Image and Vision Computing, vol. 21, Aug. 2003.

[4] I.J. Cox, J. Kilian, F.T Leighton and T.Shamoon. Secured Spread Spectrum Watermarking for Multimedia. IEEE Tran. on Image Processing, Dec 1997.

[5] Nagar Abhishek, Nandakumar Karthik, Jain Anil K, *Biometric Template Transformation: A Security Analysis*, SPIE, The International Society for Optical Engineering, 2010.

[6] S. Pankanti and M.M.Yeung, *Verification on Fingerprint recognition and Retrieval*," Proc. SPIE, vol. 3657, pp. 66-78, 1999.William Stallings, *Cryptography, and Network Security*, Pearson Education Inc publishing as Prentice Hall.

[7] M.J.Tsai, K.Y.Yu,and Y.Z.Chen. Wavelet Packet and Adaptive Spatial Transformation of Watermark for Digital Image Authentication. IEEE Int. Conf. On Image Processing, Sep 2000.

[8] M.J.Tsai, K.Y.Yu,and Y.Z. Chen. Wavelet Packet and Adaptive Spatial Transformation of Watermark for Digital Image Authentication. IEEE Int. Conf. On Image Processing, vol. 1. pp 450-453, Sep 2000.

[9] S.H. Wang and Y.P. Lin. Wavelet Tree Quantization for Copyright Protection Watermarking. IEEE Tran. on Image Processing, vol.13, pp 154-165, Feb 2004.

[10] J.L. Vehel and A. Manoury. Wavelet Packet-based Digital Watermarking. Int. Conf. on Pattern Recognition, Barcelona, Spain**,** pp 413-416, Sep 2000.