ISSN (Print) : 2320 – 3765
ISSN (Online): 2278 – 8875

International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 4, April 2015

A Robust Digital Image Watermarking for Biometric Template Protection Applications

S.Usha[1], M.Karthik[2]

Assistant Professor (Sr.G), Dept. of EEE, Kongu Engineering College, Perundurai, Tamilnadu, India [1,2]

ABSTRACT: The scope of Digital Watermarking increases which embeds information to be secured into an image. The proposed work implements a Digital Image Watermarking technique that uses two-level Discrete Wavelet Transform and Least Significant Bit algorithm, which enhances the security of biometric based applications. In the proposed work , the fingerprint image is used as a cover image, the facial and iris templates are used as watermarks. To check the robustness of the proposed method, attacks like channel noises, JPEG compression and geometrical attacks are incorporated in the watermarked image and this image is transmitted through the network. At the receiving end watermarks are recovered using watermark extraction algorithm. The work is simulated using MATLAB R2010b.

KEYWORDS: Fingerprint, Iris, Digital Watermarking, Embedding, Extraction.

I. INTRODUCTION

In Human, vision is the most powerful sense among the five senses. Visual information, conveyed in the form of images gives better impact than textual information. Digital image processing is a technique that uses computer algorithms to perform image processing on digital images. The growth of digital image processing has been fuelled by technological advances in digital imaging, computer processors and mass storage devices. In contemporary era, digital information transformation has a great impact on human life. With this powerful technique, the theft information content can be stored and transmitted with security. Nowadays governments, military, corporations, financial institutions, hospitals, and private businesses collect and store data that is more confidential which may include information about the employees, customers, products, research, and financial status. Most of this information is now collected, processed and stored on electronic computers and transmitted across network to other computers. The confidentiality in information is being maintained by various techniques such as cryptography, stenography and watermarking and the secured access of that information is maintained by personal identification system such as fingerprint, iris, and face recognition.

Biometrics is the study in which humans recognizes automatically by means of inherently unique physical or behavioural characteristics. Multimodal Biometrics is systems that are capable of using more than one physiological or behavioral characteristic for enrollment, verification or identification. For biometric identification to be ultra-secure and provide above average accuracy more than one type must be used as only one form of it may not be accurate enough. One example of this inaccuracy is in the area of fingerprints where at least 10% of people have worn, cut or unrecognizable prints. Hence in the proposed method fingerprint and iris are used for identifying an individual.

II. LITERATURE SURVEY

The idea behind the Controllable secure watermarking CSW is that by altering the host signal in the orthogonal complement of the embedding subspace and makes the watermarked signal have an orthogonally invariant distribution in a higher dimensional subspace including the embedding subspace. A binarization scheme is discussed to transform real valued face templates into binary templates, so that the transformed templates lie in a finite (binary) field that can be protected with a biometric cryptosystem approach.

Feature region selection method based on the idea of simulated attacking and multidimensional knapsack problem(MDKP) optimization techniques, to select a non-overlapping feature region set, which has the greatest robustness against various attacks and preserve image quality as much as possible after watermarked, but the computational time is larger. And two issues of existing feature-based scheme are, avoiding repeated selection of robust regions for watermarking to resist similar attacks, and the difficulty of selecting the most robust and smallest feature region set to be watermarked.

A robust quantization-based image watermarking scheme, called the gradient direction watermarking (GDWM), is based on the uniform quantization of the direction of gradient vectors. This method embeds the watermark bits in the direction (angle) of significant gradient vectors, at multiple wavelet scales. The gradient angle is then quantized by modifying the DWT coefficients that correspond to the gradient vector along with the absolute angle quantization index modulation (AAQIM). The positions of the gradient vectors are scrambled uniformly over the wavelet transform of the image to extract the watermark correctly.

A combined DWT and LSB based biometric watermarking algorithm that securely embeds a face template in a fingerprint image. Watermarking based approaches have been proposed to make the biometric system secure and resilient to deliberate manipulations and attacks . A watermarked fingerprint is created by embedding a template or face image in the fingerprint image using a combination of wavelet and LSB based watermarking techniques. The proposed algorithm synergistically combines the advantages of wavelet and LSB based techniques such that it is robust to both geometric and frequency attacks.Multi-resolution Discrete Wavelet Transform is used for embedding the face image in a fingerprint image. An intelligent learning algorithm based on Support Vector Machine (SVM) is introduced to enhance the quality of the extracted face image. The intelligent learning algorithm is used to train and classify the pixel quality from corresponding locations of extracted multi-resolution face images when subjective attacks.

A novel image-based face recognition algorithm that uses a set of random rectilinear line segments of 2D face image views as the underlying image representation, together with a nearest-neighbour classifier as the line matching scheme . The combination of 1D line segments exploits the inherent coherence in one or more 2D face image views in the viewing sphere. The algorithm achieves high generalization recognition rates for rotations both in and out of the plane, is robust to scaling, and is computationally efficient. In the proposed method, based on literature review to make the process robust and computationally faster, a combination of DWT-LSB based digital watermarking method is suggested.

III. PROPOSED TEMPLATE PROTECTION METHOD

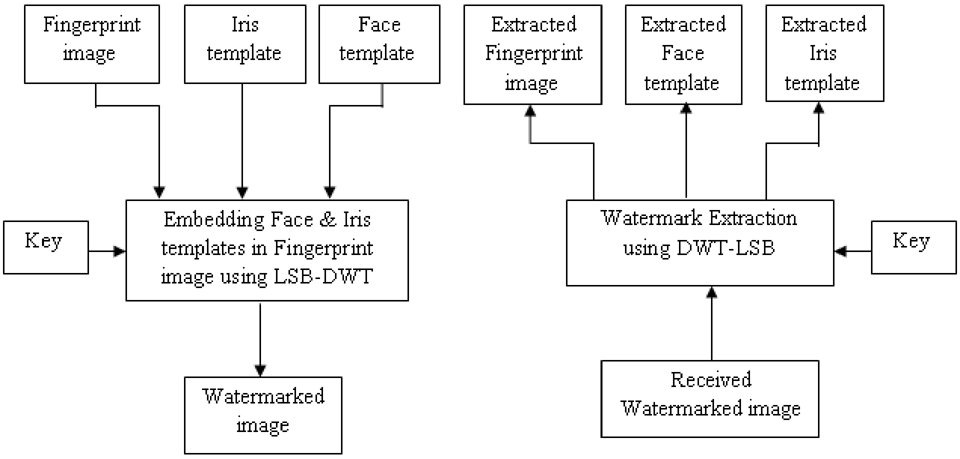
Fingerprint image
Iris template
Face template
Extracted Fingerprint image
Extracted Face template
Extracted Iris template
Key
Embedding Face & Iris templates in Fingerprint image using LSB-DWT
Watermark Extraction using DWT-LSB
Key
Watermarked image
Received Watermarked image

Fig. 1 Block diagram of the proposed work

Biometrics based authentication systems have inherent advantage over the traditional personal identification techniques. However the critical problem is to ensure the security and integrity of biometric data. The block diagram of the proposed work is shown in the Figure 1.

In the proposed digital image watermarking scheme, the watermark is embedded by combining both the discrete wavelet transform and LSB algorithm. The algorithm is composed of two main steps namely, watermark embedding process, and watermark extraction process. In the proposed method fingerprint template is taken as cover image and face and iris templates are taken as watermarks. As per the proposed method the face template is embedded in the Low-High (LH) frequency band and iris template is embedded in the High-Low (HL) frequency band. In the transmission side a key value 'K' is used to strengthen the watermarking algorithm. At the receiving side by using inverse DWT process and the same key value 'K' , the watermarks are recovered.

3.1 Raster Scan Order

Raster scanning is the process of displaying an image by updating each pixel one after the other, rather than all at the same time, with all the pixels on the display updated over the course of one frame. In this proposed work, Raster scanning is applied in the HL1 and LH1 bands of cover image. The HL1 and LH1 bands of size 256x256 are divided into several blocks each of size 16x16. During scanning, all the pixels in the first bock are ordered in the first row and the second block constitutes the second row and so on.

3.2 2D Gabor Filter

A 2D spatial Gabor filter is defined in the radiance domain by,

$$g(x, y) = a(x, y) * c(x, y) \qquad (3.1)$$

Where,

$a(x, y)$ = Gaussian component,

$c(x, y)$ = Sinusoidal component.

Gabor functions are frequently used for feature extraction, especially in texture-based image analysis (e.g., classification, segmentation or edge detection) and more practically in face recognition. In the proposed method the face image is converted into face template that is machine readable format using Gabor filter is shown in the Figure 2.

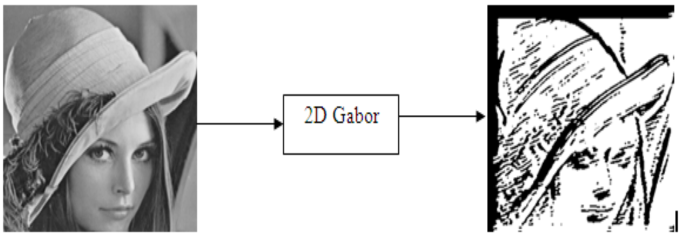

Fig. 2 Face Image and Face Template Image

In a two-dimensional case, the absolute square of a correlation between an image and the two-dimensional Gabor function provides a local spectral energy density concentrated around a given position and frequency in a certain direction. A two-dimensional convolution with a circular (non-elliptical) Gabor function is separable to series of one-dimensional ones. Thus, image analysis by the Gabor wavelets is similar to perception in the human visual system. In Image processing algorithm, Gabor wavelet is applied at the point of interest and this point can be detected using Gabor functions.

3.3 Embedding Process

The Two-level Discrete Wavelet Transform (DWT) is applied on the original fingerprint image. The coefficients in the approximation band of the DWT image contain significant details of the fingerprint image. Hence the approximation band should not be modified during embedding or extraction.

The detailed sub-bands (HL1 & LH1) are divided into blocks I1, I2 ...Ir of size M x N and the coefficients in each block are numbered in raster scan order. From each block, the first wavelet coefficient that has a positive phase and whose value is less than threshold is selected.

3.4 Message Block Formation

To obtain watermarked image, the face and iris template bits are embedded in the fingerprint image. In which the position of embedding can be obtained from message block formation. The following procedure is used to embed the face and iris templates.

(i) For each block Ir, a message block MBr is formed by selecting high order bit from each pixel of Ir. A key K is appended to message block MBr. The value K is sufficiently large to prevent an attacker.

(ii) The key of K is used to compute the message block

$$Hr = (MBr)K \qquad (3.2)$$

Where,
Hr=indicates the pixel position to embed the watermark bits,
MBr=message block, K=key.

(iii) The value of [Hr mod (M x N)] gives the pixel position for embedding the iris template and the modulus of resulted values with thresholding factor gives the pixel position for embedding the face template. After embedding all the bits of the face and iris templates, Inverse Discrete Wavelet Transformation (IDWT) is applied on the watermarked fingerprint coefficients to generate the final secure watermarked fingerprint image.

3.5 Extraction Process

The watermarked image, obtained from embedding process is divided into sub-bands using DWT. Two level DWT is applied to the watermarked image and the watermark images are extracted from the mid-frequency bands of watermarked image. IDWT is performed to generate final watermark extracted image. The PSNR value is calculated to measure the imperceptibility of the watermarking scheme. Various attacks can be applied to the watermarked image to check the robustness. The extracted bits are arranged to form the facial and iris templates, then IDWT is applied to the remaining bits for extracting the original fingerprint image. So that the extracted face, iris and fingerprint image can be recovered at the receiving side in secured transmission.

IV. SIMULATION RESULTS AND ANALYSIS

The experiment is carried at using 250 real-time face, fingerprint and iris images respectively. The face image and fingerprints are collected from male and female of age group 18-50. The iris image is collected from and MMU2 public database.

The fingerprint image of size 1024x1024 is taken as a cover image, the face and iris templates are used as a watermark images. The face template of size 256x256 is generated using 2D Gabor filter and the iris template of size 16x10 bits is generated using Gabor Transform .

4.1 Face Image to Face Template

The standard Lena image of size 256x256 has been convolved with 2D gabor filter to obtain the Lena template image. Gabor functions produce optimal resolution in both the time (spatial) and frequency domains. Figure 3 shows the watermark image and the watermark template image obtained through Gabor filtering.

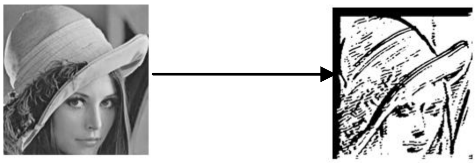

Fig. 3 Face Image and Face Template

4.2 Eye Image to Iris Template

Iris is segmented from the image, which has been carried out using three process namely image pre-processing, pupil boundary detection and iris boundary detection. The segmented iris image is normalized for the feature extraction process. The normalized image is enhanced and Gabor Transform is applied to generate the iris code. The size of the iris code is resized to 16x10 bits.

5.3 Two Level DWT On Cover Image

The original cover image of size 1024x1024 is taken and the two level DWT is applied for the first level the image is divided into four sub-bands, each band having the size of 512x512 and for the second level LL band is again divided into four sub-bands namely, LL1, LH1, HL1 and HH1each of size 256x256. Then the HL1 & LH1 bands are used as a cover image to embed the watermark images.

5.4 Watermarked Image

The Watermark bits are embedded using LSB algorithm in the mid frequency sub bands (HL1 & LH1) of cover image and IDWT is taken for each blocks. The embedded blocks are concatenated and the watermarked image is obtained. Table 1 shows the PSNR, similarity and UQI values of 250 real-time images.

Table 1 PSNR, SIM, and UQI Value of Watermarked Images

S.No.	Image metrics	Watermarked image
1.	PSNR	61.5691
2.	SIM	0.9091
3.	UQI	0.7777

5.5 Watermark Recovery

In this process, the two level DWT is applied to the watermarked image and the Watermark bits are extracted in the mid frequency sub bands (HL & LH1) based on the pixel position obtained from key and message block using LSB algorithm. The obtained recovered watermark images are taken IDWT to recover the cover image. The recovered watermark face template and the recovered fingerprint image are shown in Figure 4.

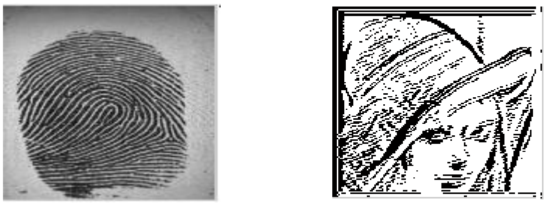

Fig. 4 Recovered Cover Image and Watermark Face Template

Table 2 shows the similarity, universal quality index and hamming distance values of 250 real-time images.

Table 2 SIM, UQI and HD Value for Recovered Face, Iris and Fingerprint Image

ATTACKS	**FINGERPRINT IMAGE**		**FACE TEMPLATE**		**IRIS TEMPLATE**	
	SIM	**UQI**	**SIM**	**UQI**	**SIM**	**HD**
No attacks	0.9818	0.9997	0.9973	0.9955	1	0
Salt & pepper(0.01)	0.9646	0.9915	0.7637	0.5504	0.9625	0.0375
Gaussian(0.01)	0.9415	0.9902	0.2892	0.1814	0.6813	0.3187
Speckle(0.01)	0.9664	0.9690	0.4957	0.3648	0.7250	0.2750
Poisson	0.9727	0.9412	0.5723	0.4061	0.7375	0.2625
JPEG Compression(1)	0.8867	0.8284	0.9677	0.9916	0.9125	0.0875

From the Table 2, it is found that the similarity, UQI and hamming distance of the proposed method yields better results for channel noises and JPEG compression attacks.

V. CONCLUSION

The proposed work enhances the security of biometric based applications by combining the LSB and DWT algorithms in Digital image watermarking, by considering three modalities, i.e., fingerprint, face and iris template. The effectiveness of this method is observed by the PSNR, UQI, similarity values. The performance analysis of the proposed method gives better results for channel noises and JPEG compression attacks.

REFERENCES

[1] Daugman, J., “How iris recognition works”, IEEE Transactions on Circuits and Systems for Video Technology, Vol.14, No.1, pp.21-30, 2004.

[2] Cao, J., and Huang, J., “Controllable secure watermarking technique for trade off between robustness and security”, IEEE Transactions on Information Forensics and Security, Vol.7, No.2, pp. 821-826, 2012.

[3] Feng, Y.C., and Yuen, P.C., “Binary discriminant analysis for generating binary face template”, IEEE Transactions on Information Forensics and Security, Vol.7, No.2, pp. 613-624, 2012.

[4] Tsai, J.S., Huang, W.B., and Kuo, Y.H., “On the selection of optimal feature region set for robust digital image watermarking”, IEEE Transactions on Image Processing, Vol.20, No.3, pp. 735-743, 2011.

[5] Nezhadarya, E., Wang, Z.J., and Ward, R.K., “Robust image watermarking based on multiscale gradient direction quantization”, IEEE Transactions on Information Forensics and Security, Vol.6, No.4, pp.1200-1213, 2011.

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

[7] Vatsa, M., Singh, R., and Noore, A., “Improving biometric recognition accuracy and robustness using DWT and SVM watermarking”, IEICE Electronic Express, Vol.2, No.12, pp. 362-367, 2005.

[8] De Vel, O., and Aebehard, S., “Line-based face recognition under varying pose”, IEEE Transactions on Pattern Analysis and Machine Intelligence, Vol.21, No.10, pp. 1081-1088, 1999.

[9] Fouad , M., El sadik, A., and Petriu, E.M.., “Combining DWT and LSB watermarking to secure revocable iris templates”, Proceedings of IEEE International Conference on Information Sciences Signal Processing and their Applications, pp. 25-28, 2010.