Journal of Theoretical and Applied Information Technology
15th April 2017. Vol.95. No 7
© 2005 – ongoing JATIT & LLS

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

JOINT ENCRYPTION AND WATERMARKING TECHNIQUE USING BLOCK CIPHER AND WAVELET

B.SRIDHAR
Professor, Department of ECE,
MLR Institute of Technology, Hyderabad, INDIA
E-mail: sridharbece@gmail.com

ABSTRACT

This paper proposes a joint encryption and watermarking technique based on random block permutation and DWT with the motivation to enhance the security of the multimedia content. The original image is sectioned into the blocks and shuffle the blocks using random permutation, In this technique copyright information is concealed into an encrypted image. Based on the results, permutation of blocks is effective in significantly reducing the correlation thereby reducing the level of perceptual information, whereas the permutation of blocks is good at producing higher level security. Watermarked crypto image is freely distributed to channel with enhanced security, because it combines both encryption as well as watermarking techniques.

Keywords: *Copyright Protection, Encryption, Random Permutation, Watermarking, Wavelet transform*

1. INTRODUCTION

With the fast growing of the computer era, transmission of multimedia content is more, while in transmission the unauthorized person can easily access and modify the information. Hence, the protection of intellectual property becomes more and more attention and important for the society. Due to large data size and real time constrains, algorithms that are good for textual data may not be suitable for multimedia data. Many researchers have been focused on providing solutions to copyright protection and authentication. Since the digital data has no conflict between in the quality of an original and its copy [1- 4]. The technique that can protect the property against the illegal distribution called Watermarking. It provides the owners in asserting their intellectual property rights. Most of the watermarking techniques projected only on the frequency domain because it is more robust, and stable. Image encryption techniques try to convert an image into unperceivable format. Image decryption retrieves the original image from the encrypted one. Proposed block based encryption and decryption algorithm, it will reduce to increasing the entropy value of the encrypted images as well as lower correlation.To design and develop the joint encryption and watermarking techniques that can be used for copyright protection of data and to increase the robustness and minimize the bit error rate of the proposed algorithms are the main objectives of the proposed approach.

2. BACKGROUND

Most of the algorithms specifically designed to encryption and watermarking of digital images are proposed. Regarding encryption two major groups of image encryption algorithms like non-chaos selective methods and Chaos-based selective or non-selective methods. Mitra A *et al.* [6] proposed a random combinational image encryption approach with bit, pixel and block permutations. Zhi-Hong Guan *et al.* [7] explained a new image encryption scheme, in which shuffling the positions and changing the gray values of image pixels is combined to confuse the relationship between the cipher image and the plain image. Shujun Li *et al.* [8] pointed out that all permutations-only image ciphers were insecure against known/chosen-plaintext attacks. In conclusion, they suggested that secret permutations have to be combined with other encryption techniques to design highly secured images.

In the literature survey of watermarking techniques, many algorithms have been reported. Xia *et al.* [9] proposed a watermarking scheme based on the Discrete Wavelet Transform (DWT). The watermark was concealed to the frequency bands of the image. The decoding process involved taking the DWT of a potentially marked image. Sections of the watermark were extracted and correlated with sections of the original watermark. If the cross-correlation was above a threshold, then the watermark was detected. Otherwise, the image was decomposed into finer and finer bands until the entire, extracted watermark was correlated with the entire, original watermark. This technique proved to be more robust than the DCT method when embedded zero-tree wavelet compression and halftoning were performed on the watermarked images.

Yongquiang [10] proposed a novel optimal color image watermarking scheme in the DWT domain to meet watermarking properties such as: security, imperceptibility and robustness. In the scheme, the watermark was a meaningful gray image encrypted with a two-dimensional chaotic stream encryption. Genetic algorithm was used to embed the watermark into the host color image so as to improve the imperceptibility of the watermarked image.

Mehdi Khalili[11] proposed a novel watermarking algorithm which compares to the existing watermarking techniques, this proposed method has combined imperceptibility, security and robustness. This paper shows a wavelet-based watermarking approach for hiding watermark image in color host images is proposed. The experimental results show that the proposed approach provides extra imperceptibility, security and robustness against JPEG compression and different noise attacks such as Gaussian and salt & pepper compared to the similar proposed methods.

Evident from the critical review, it is clear that watermarking and encryption techniques are highly motivated by the copyright owners to secure their rights. In the survey, many more systematic algorithms are needed to enhance the process of encryption and watermarking. This work addresses the encryption and watermarking for improving the security of multimedia content.

3. PROPOSED APPROACH

In this proposed approach the original image is divided into a number of blocks which are shuffled within the image to build a newly cipher image. This perceivable information can be reduced to decreasing the correlation among the image elements using certain transformation techniques. The transformation process refers to the operation of dividing and replacing an arrangement of the original image. Block based encryption and decryption algorithm is based on the combination of image transformation followed by encrypted images and image measurements of correlation entropy. Let us consider the original image of *A*, of 36 blocks it is undergoing the random permutation *A_E*.

$$A = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 7 & 8 & 9 & 10 & 11 & 12 \\ 13 & 14 & 15 & 16 & 17 & 18 \\ 19 & 20 & 21 & 22 & 23 & 24 \\ 25 & 26 & 27 & 28 & 29 & 30 \\ 31 & 32 & 33 & 34 & 35 & 36 \end{pmatrix}$$

$$A_E = \begin{pmatrix} 9 & 17 & 32 & 30 & 34 & 26 \\ 29 & 11 & 8 & 10 & 3 & 33 \\ 2 & 36 & 12 & 24 & 35 & 4 \\ 13 & 16 & 1 & 19 & 14 & 27 \\ 31 & 21 & 28 & 15 & 23 & 5 \\ 6 & 20 & 7 & 22 & 18 & 25 \end{pmatrix}$$

3.1 Discrete Wavelet Transform

A Watermark is concealed into an encrypted image under wavelet domain. Discrete Wavelet Transform can be implemented using digital filters and down samplers. Each level of decomposition produces four bands of data denoted by LL, HL, LH, and HH. The LL sub band can further be decomposed to obtain another level of decomposition. This process is continued until the desired number of levels determined by the application is reached.

Let us consider the encrypted image which undergone the 2 level DWT. Now add the scaled copyright information to the LL band of the encrypted image. Further IDWT is applied and turn back to encrypted image and this image is freely distributed to channel with enhanced security, because it combines both encryption as well as watermarking techniques.

The discrete wavelet coefficients can be acquired by expanding the function *f* (*x*) as a sequence of numbers. By applying the principle of series expansion, the discrete wavelet transform coefficients are defined as,

$$W\varphi(j_0,k) = \frac{1}{\sqrt{M}}\sum_x f(x)\varphi_{j_{0,x}}(x) \qquad (1)$$

$$W\psi(j,k) = \frac{1}{\sqrt{M}}\sum_x f(x)\psi_{j,k}(x) \qquad (2)$$

Figure 1 shows two levels of decomposition of an image. Figure 2 shows an overall view of the proposed approach.

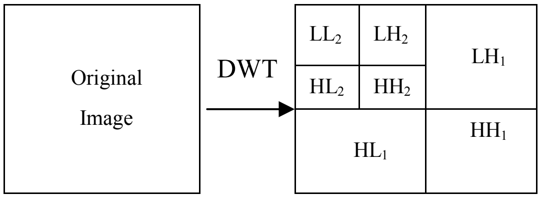


Figure 1: Second level DWT decomposition,

For $j \geq j_0$ and the $W\varphi(j_0,k)$ and $W\psi(j, k)$ are the approximation coefficient and detail coefficient respectively. The parameter M is a power of 2 which ranges from 0 to J-1. The DWT coefficients enable us to reconstruct the signal function $f(x)$ as,

$$f(x) = \frac{1}{\sqrt{M}} \sum\nolimits_k W_\varphi(j_{0,}k)\varphi_{j0,k}(x) + \frac{1}{\sqrt{M}} \sum\nolimits_{j=j0}^{\infty} W_\psi(j,k)\psi_{j,k}(x) \tag{3}$$

Where $1/\sqrt{M}$ is a normalizing factor. The reason that the discrete wavelet transform is a better transform because DWT have a better ability in localizing both time and frequency. This technique employed the two level decomposition in the source image.

3.2 Watermark Embedding Technique

From the encrypted image *(A_E)*, compute 2 levels of DWT to obtain eight sub-bands of each frame *(LL_1,LH_1, HL_1, HH_1, LL_2, LH_2, HL_2&HH_2)*. LL_2 sub band is taken for embedding. Consider the watermark image which are multiplied by the scaling factor and the scaled watermark image is added to the subband which are chosen

$$[A_E]_{mxn} \xrightarrow{2-DWT} \begin{bmatrix} A_E^{LL2} & A_E^{LH2} \\ A_E^{HL2} & A_E^{HH2} \end{bmatrix}_{mxn} \tag{4}$$

$$[Y]_{mxn} = [A_E^{LL2}]_{\frac{m}{2}x\frac{n}{2}} + \alpha * [W]_{\frac{m}{2}x\frac{n}{2}} \tag{5}$$

$$\begin{bmatrix} Y & A_E^{LH2} \\ A_E^{HL2} & A_E^{HH2} \end{bmatrix}_{mxn} \xrightarrow{2-IDWT} [A_E^{'}]_{mxn} \tag{6}$$

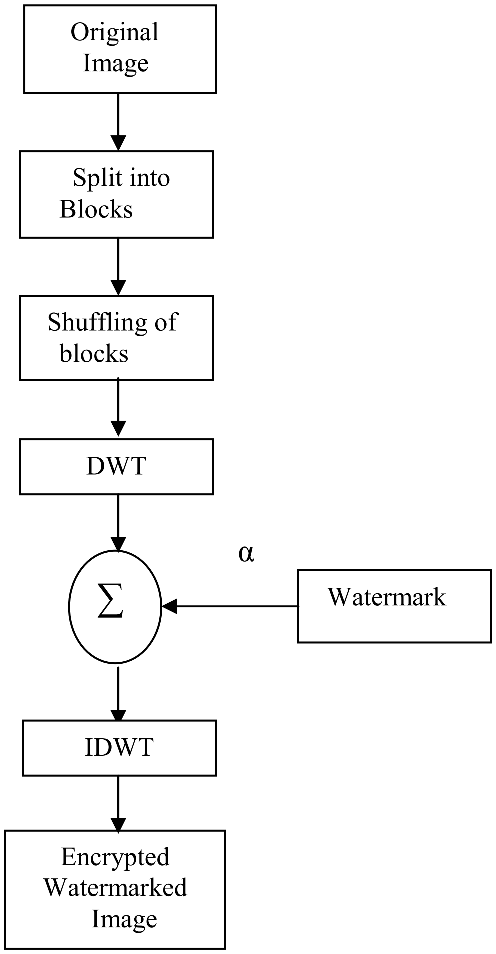


Figure 2: Overall view of proposed approach

3.3 Watermark Extraction technique

In order to extract the copyright information from the encrypted image for proving the authentication the following steps are carried out.

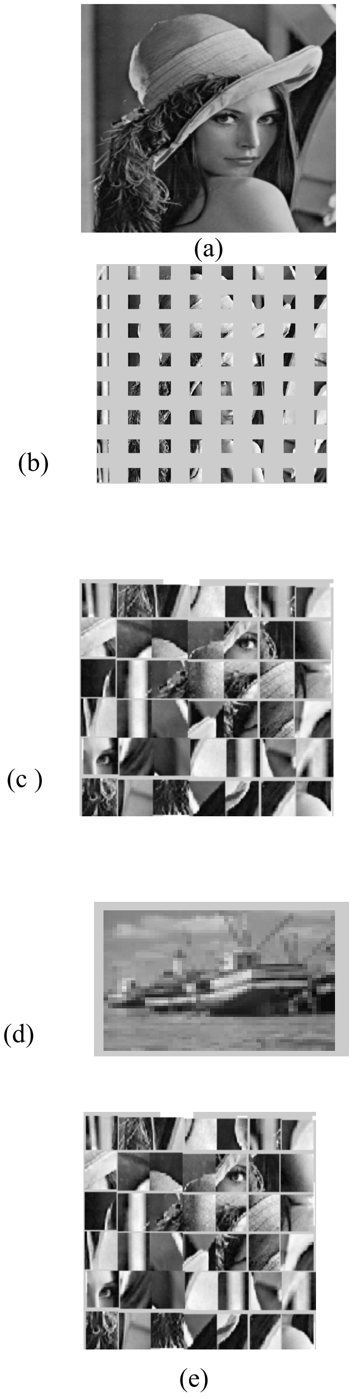
$$[A_E^{'}]_{mxn} \xrightarrow{2-IDWT} \begin{bmatrix} Y & A_E^{LH2} \\ A_E^{HL2} & A_E^{HH2} \end{bmatrix}_{mxn} \tag{7}$$

$$[W]_{\frac{m}{2}x\frac{n}{2}} = \frac{[Y]_{mxn} - [A_E^{LL2}]_{\frac{m}{2}x\frac{n}{2}}}{\alpha} \tag{8}$$

4. RESULTS AND DISCUSSION

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

This proposed method is strong resistant against the attacks also gives just comparable results in terms of the PSNR. To demonstrate the effectiveness of the proposed algorithm, MATLAB simulations are given in this section. Figure 3 shows the simulation results of this proposed approach.


(a)
(b)
(c)
(d)
(e)

(f)

Figure 3: (a) Original Image, (b) Sectioned blocks of an image, (c) Encrypted image, (d) Watermark image, (e) Watermarked Encrypted image, (f) Recovered an Image after decryption.

Dividing the image into a larger number of blocks made the performance even better. The results showed that the correlation was minimized even further and the entropy was increased as the number of blocks is increased.

4.1 Invisibility test

The Mean Square Error (MSE) between the original image O(x, y) and the decrypted image E(x, y) is given by X and Y represents the size of the Image. Average MSE for all the watermarked Image is 0.1874. Peak signal to noise ratio (PSNR) is used to measure the quality of the Image. It measures the signal to noise ratio of the watermarked Image;

$$MSE = \left(1/_{XY}\right)\sum_{x,y}\left(O(x,y)-E(x,y)\right) \qquad (9)$$

$$PSNR = 10\log_{10}(255/MSE) \qquad (10)$$

$$CC = \frac{\sum_{x}\sum_{y}(O_{xy}-\bar{O})(E_{xy}-\bar{E})}{\sqrt{\left(\sum_{x}\sum_{y}(O_{xy}-\bar{O})^2\right)\left(\sum_{x}\sum_{y}(E_{xy}-\bar{E})^2\right)}} \qquad (11)$$

In this technique PSNR yields 45.7623dB. Comparison between extracted and original watermark can be evaluated by Correlation Coefficient (CC). This method achieves the Correlation Coefficient of the overall watermarked frame is 0.9996.

4.2 Attacks in Image watermarking

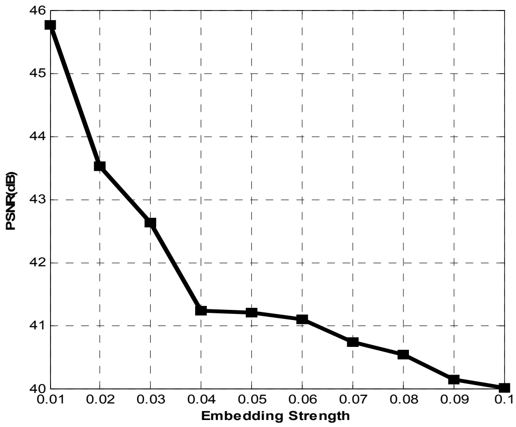
Generally attackers are trying to remove the copyright information inside the encrypted image for claim the ownership of an image. Noise and geometrical attacks are the most common attacks on watermarking system. Noise attacks like Salt &Pepper, Speckle, Gaussian and Median filtering attacks. In order to measure the robustness, we perform some noise attacks and filtering attacks to the encrypted image.

In Frame rotation attacks the watermarked Image is subject to angle of rotation (5° degrees) and test the quality of the rotated frame and extracted watermark Image. Frame cropping involves removing a part of the image from the watermarked frame and retrieving the watermark from the cropped part. Take the embedded image and cropped it into the size of 200x200 and extract the watermark in the cropped region and estimate the PSNR values. Performance of PSNR and Correlation coefficient of Decrypted and watermarked image under various attacks is listed in Table 1.

Table 1: Performance values of the approach

Attacks	Decrypted Image		Watermark Image	
	PSNR (dB)	CC	PSNR (dB)	CC
No Attacks	45.7623	0.9996	31.3962	0.9879
Salt & Pepper	28.6134	0.8987	21.2612	0.8683
Speckle	31.3407	0.9546	26.3908	0.9052
Gaussian	25.5331	0.8498	23.6124	0.7992
Median filtering	40.0912	0.9904	30.2671	0.9543
Frame Rotation	23.1349	0.6393	175612	0.6211
Frame cropping	22.6142	0.6112	17.8124	0.6001

In this proposed method we set the embedding strength (α) is 0.01. If raising the scaling factor performance of the system are reduced or if we decrease the scaling factor less than 0.01 the bit rate change is more hence the size of the watermarked image is extremely high. Hence we set an optimum value of the scaling factor.
Figure 4 shows the performance curve between the embedding strength (α) and the PSNR values.



Encryption and watermarking technique can guard the information and communication from unauthorized revelation and access of information. While coming to the advantages degree of security level is enhanced in the weakness point of view, a strongly encrypted, authentic, and digitally signed information can be difficult to access even for a legitimate user at a crucial time of decision-making. By comparing the proposed method with existing method, we find that the proposed method yields the PSNR is 45.7623 dB. Which is greater than the PSNR reported by Chandraprased *et al.* [12] is 43 dB.

5. CONCLUSION

A joint encryption and watermarking techniques is proposed. Results show the security level of testing image is enhanced. Results illustrate that we can achieve a reasonable value of PSNR with lower MSE of testing images. This method shows the degree of invisibility is high in noise and geometrical attacks. Further the enhancement of this algorithm and the property of real time have been emphasized in this ongoing work.

REFRENCES:

[1] C.Busch, W.Funk, and S.Wolthusen, "Digital watermarking: From concepts to real-time Image applications," IEEE Trans. Comput.Graphics Applicat., vol.19, no.1,1999, pp. 25–35.

[2] C. I. Podilchuk and E. J. Delp, "Digital watermarking: Algorithms and applications," IEEE Signal Process. Mag., vol.18, no.4, Jul. 2001, pp. 33–46.

[3] C.T.Hsu and J.L.Wu, “Hidden digital watermarks in images,” IEEE Trans. Image Process., vol. 8, no. 1, Jan. 1999, pp. 58–68.

[4] H. Y. Huang, C. H. Fan, and W. H. Hsu, “An effective watermark embedding algorithm for high JPEG compression,” in Proc. Machine Vision Applications, 2007, pp. 256–259.

[5] I. Cox, J. Kilian, F. T. Leighton, and T. Shamoon, “Secure spread spectrum watermarking for multimedia,” IEEE Trans. Image Process., vol.6, no. 12, pp. 1673–1687, Dec. 1997.

[6] A. Mitra, , Y V. Subba Rao, and S. R. M. Prasnna, "A new image encryption approach using combinational permutation techniques," Journal of computer Science,vol. 1, no. 1, p.127, 2006,

[7] G. Zhi-Hong, H. Fangjun, and G.Wenjie, "Chaos - based image encryption algorithm, "Department of Electrical and computer Engineering,University of Waterloo, ON N2L 3G1, Canada. Published by: Elsevier, 2005, pp. 153-157.

[8] Li. Shujun, Li. Chengqing, C. Guanrong, Dan Zhang., and Nikolaos, G., Bourbakis, "A general cryptanalysis of permutation-only multimedia encryption algorithms," 2004, http://eprint.iacr. Org/2004/374.pdf

[9] X. Xia, C. Boncelet, and G. Arce, “A Multiresolution Watermark for Digital Images,” Proc. IEEE Int. Conf. on Image Processing, Oct. 1997, vol. I, pp. 548-551

[10] Chen Yongquiang, Zhang Yangqing, Peng Lisen, “A Novel Optimal Color Image Watermarking Scheme”, 3rd International Conference on Genetic and Evolutionary Computing”, 2009.

[11] Mehdi Khalili, “A Novel Secure, Imperceptible and Robust CDMA Digital Image Watermarking In Jpeg-Ycbcr Channel Using DWT2”, International Journal of Enterprise Computing and Business Systems Vol. 1 Issue 2 July 2011.

[12] V.Chandra Prasad and S.Maheswari, “Robust Watermarking of AES Encrypted Images For DRM Systems” In Proceedings: IEEE International Conference on Emerging Trends in Computing, Communication and Nanotechnology (ICECCN 2013), 2013, pp.189-193