Volume 4, Issue 8, August 2014 ISSN: 2277 128X
International Journal of Advanced Research in Computer Science and Software Engineering
Research Paper
Available online at: www.ijarcsse.com

Wavelet based image encryption: a Comparative study

A. M. Riad
Department of information system
Mansoura University
Egypt

Reham R. Mostafa
Department of information system
Mansoura University
Egypt

Rasha Elhadary
Department of information system
Mansoura University
Egypt

Abstract— Image encryption is the method through which we can protect the transmission and storage of multimedia data from eavesdroppers. Encryption can achieve this by scrambling the multimedia data so that they can't be understood. The aim is to make the multimedia data not intelligible to any unauthorized entity who might intercept them. In image encryption we don't concentrate only on perceptual security but also concentrate on doing it with achieving a high cryptographic security. This paper presents a comparative study between two wavelet-based image encryption schemes. The first scheme is based on full encryption wavelet transformed image, and the second one based on partial encryption of wavelet transformed image. Results show that full encryption performs better in term of perceptual security, while partial encryption performs better in term of computational time.

Keywords— full encryption, partial encryption, discrete wavelet transform, stream cipher, block cipher

I. INTRODUCTION

Recently, the rapid development of multimedia and communication technologies has resulted in the transmission of large amount of multimedia data, i.e., videos and images. This multimedia data is sensitive in nature and demands confidentiality and integrity.

Cryptographic mechanisms as encryption and digital signature are commonly used for multimedia data protection. They are used to provide confidentiality, integrity and non-repudiation services.

Encryption techniques [1-3] can prevent information leakage by transforming the original information into unintelligible forms with ciphers. It can keep multimedia information away from illegal attacks during the processes of transmission, storage and so on.

Unfortunately, the processing time of encryption and decryption process is a major factor in real-time application. Encryption and decryption algorithms are too slow to handle the tremendous amount of data transmitted. It is not practical to encrypt multimedia data completely with traditional ciphers, such as data encryption standard (DES) or advanced encryption standard (AES), because of high computational cost. Alternatively, partial encryption encrypts only a portion of multimedia data and improves the efficiency.

partial encryption (also called *selective encryption* or *soft encryption*) is a secure encryption technique to save computational complexity or enable interesting new system functionality by only encrypting a part of multimedia data [4] and yet ensuring a secure encryption [5].

There are two basic ways to encrypt digital images: in the spatial domain [6] or in the frequency domain [7, 8]. The term spatial domain refers to the image plane itself, and approaches in this category are based on direct manipulation of pixels in an image. In these algorithms, the encryption procedure usually destroys the correlation among pixels and thus makes the encrypted images incompressible. Frequency domain processing techniques are based on modifying the Frequency transform of an image. The transformation may be done using Discrete Cosine Transform (DCT) [9], Discrete Wavelet Transform (DWT) [10], etc.

The DCT transforms image from spatial domain to frequency domain. It represents an image as a sum of sinusoids of varying magnitudes and frequencies. The DCT has the property that most of the visually significant information about the image is concentrated in just few coefficients of the DCT. For this reason, DCT are used in image compression, for example, DCT is the heart of the JPEG compression standard [11].

The DWT perform a multi-resolution analysis of an image. It represents an image as a sum of wavelet functions with different location and scales. Any decomposition of an image into wavelets involves a pair of waveforms: one to represent the high frequencies corresponding to the detailed parts of an image, and the other for low frequencies or smooth parts of an image. DWT is the heart of the JPEG2000 compression standard [12].

The discrete cosine transform (DCT) and the discrete wavelet transform (DWT) are commonly used for encryption purpose. Several research works employ DWT because it presents a number of advantages over DCT [13, 14]. The wavelet transform is closer to the human visual system (HVS) since it splits the input image into several frequency bands that can be processed independently [15]. It is a multi-resolution transform that permits to locate image features such as smooth areas, edges or textured areas. Some encryption schemes encrypt data in smooth areas where the HVS is high sensitive.

In this paper, we compare the performance between two wavelet based encryption schemes, one based on full encryption and the other based on partial encryption.

The reminder of paper organized as follow: Section 2 introduces the discrete wavelet transform (DWT), and Section 3 details the encryption procedure of full and partial encryption. Experimental results are presented in Section 4. Finally, in Section 5, we draw a brief concluding remarks.

.

II. REVIEW OF DISCRETE WAVELET TRANSFORM (DWT)

An easy way to comply with the conference paper formatting requirements is to use this document as a template and simply type your text into it.

Discrete Wavelet transform (DWT) [10] is a mathematical tool for hierarchically decomposing an image. It is useful for processing of non-stationary signals. The transform is based on small waves, called wavelets, of varying frequency and limited duration. Wavelet transform provides both frequency and spatial description of an image. Unlike conventional Fourier transform, temporal information is retained in this transformation process. Wavelets are created by translations and dilations of a fixed function called mother wavelet.

DWT is the multi-resolution description of an image the decoding can be processed sequentially from a low resolution to the higher resolution. The DWT splits the signal into high and low frequency parts. The high frequency part contains information about the edge components, while the low frequency part is split again into high and low frequency parts. The high frequency components are usually used for watermarking since the human eye is less sensitive to changes in edges.

In two dimensional applications, for each level of decomposition, we first perform the DWT in the vertical direction, followed by the DWT in the horizontal direction. After the first level of decomposition, there are 4 sub-bands: LL1, LH1, HL1, and HH1. For each successive level of decomposition, the LL subband of the previous level is used as the input. To perform second level decomposition, the DWT is applied to LL1 band which decomposes the LL1 band into the four sub- bands LL2, LH2, HL2, and HH2. To perform third level decomposition, the DWT is applied to LL2 band which decompose this band into the four subbands – LL3, LH3, HL3, HH3. This results in 10 sub-bands per component. LH1, HL1, and HH1 contain the highest frequency bands present in the image tile, while LL3 contains the lowest frequency band. The three-level DWT decomposition is shown in Fig. 1. The human visual system (HVS) is more sensitive to low-frequency coefficients, and less sensitive to high frequency coefficients.

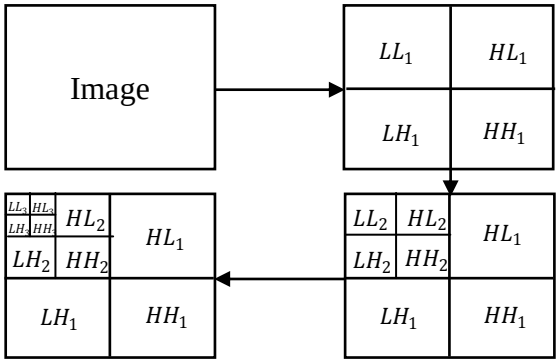


Fig. 1 Flow of DWT process (3-level discrete wavelet decomposition)

DWT is currently used in a wide variety of signal processing applications, such as in audio and video compression, removal of noise in audio, and the simulation of wireless antenna distribution. Wavelets have their energy concentrated in time and are well suited for the analysis of transient, time-varying signals. Since most of the real life signals encountered are time varying in nature, the Wavelet Transform suits many applications very well.

III. WAVELET BASED ENCRYPTION SCHEMES

The encryption procedure consists of two steps. In the first step, the wavelet decomposition is applied to the original image and resulted subbands image are encrypted using stream cipher or block cipher.

A. Full Encryption

In this approach all subbands resulted from wavelet decomposition are encrypted using cipher as shown in Fig. 2.

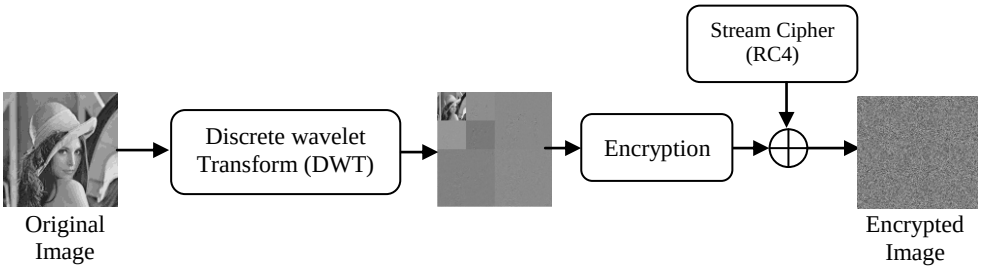


Fig. 2 Steps of full encryption procedure

B. Partial Encryption

In this approach, only one or more of the wavelet subbands are selected to be encrypted using cipher as shown in Fig.3. Next wavelet subbands images are collected to form the encrypted. The main idea of this scheme is to reduce computational time. The time factor is very important for encryption in real-time application.

The low frequency subbands are the most important because it achieves a high perceptual security as most of the image energy is concentrating in the low frequency subband. Moreover, human eyes are more sensitive to the low frequency subbands.

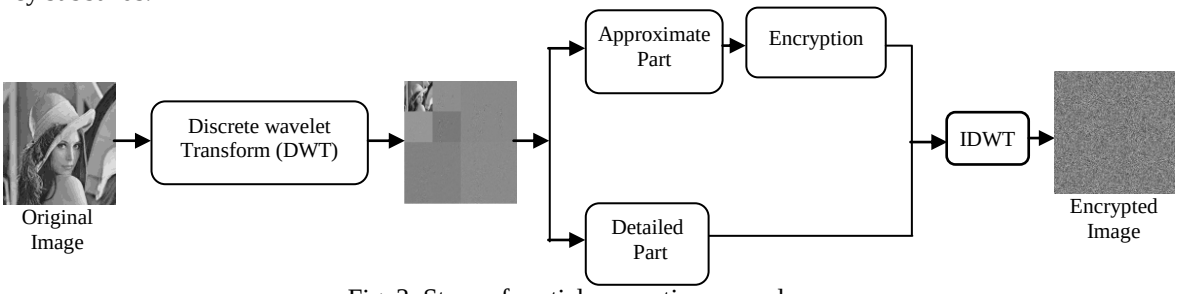


Fig. 3 Steps of partial encryption procedure

IV. EXPERIMENTAL RESULTS

For a comprehensive comparison between two wavelet-based image encryption schemes: full and partial encryption, the experiments are conducted to evaluate both perceptual security and cryptographic security. Perceptual security refers to the cipher-image's intelligibility, while cryptographic security refers to the ability to resist attacks.

A. Perceptual Security

In image encryption, it is important to keep the encrypted image unintelligible. It is called perceptual security. In order to evaluate perceptual security, PSNR measure is used:

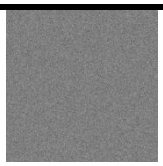
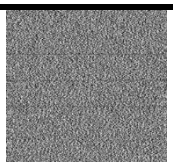
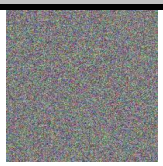
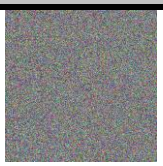
- Peak signal to noise ratio (PSNR)

The peak signal-to-noise ratio (PSNR) is used as a quality measurement between the original and an encrypted image by equation (1). The lower the PSNR mean that the lower the intelligibility of the encrypted image and the higher the perceptual security. The result of full and partial encryption schemes are shown in Table 1, in which it can be seen that the corresponding PSNR are all smaller than 15 and the encrypted image are unintelligible. Moreover the PSNR of the full encryption is the lowest

$$PSNR = 10 \times log\,10\,(255^2/MSE) \quad (1)$$

where MSE denotes the mean square error between the original image and the encrypted.

Table I
Encryption Results Of Different Wavelet Based Encryption Procedure

Original image (Airplane) 512×512		**Full Encryption**	**Partial Encryption**		
			LL3	**LL3 + HH3**	**All subbands in level 3**
					
Stream Cipher (RC4)	**PSNR**	6.052	11.894	8.763	6.226
	Time	20.09 sec	4.22 sec	4.97 sec	5.32 sec
Block Cipher (AES)	**PSNR**	5.971	11.022	10.097	6.258
	Time	50.89 sec	18.06 sec	20.22 sec	23.98 sec

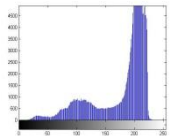
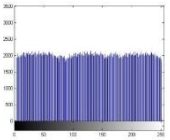
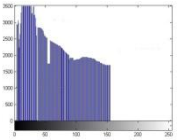
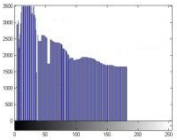
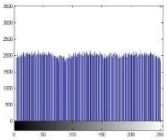
B. Cryptographic Security

In order to evaluate perceptual security, two measures are used:

- Histogram Analysis

Table 2 shows the histogram of original image and the histogram of encrypted image in different encryption schemes. It is clearly visible that histogram of encrypted image is flat or uniformly distributed and it does not leak any amount of information about the original image. Therefore, all the encryption schemes are secure from frequency analysis attack.

Table 2
histogram of the original image and encrypted image in different schemes

Histogram of original image	Full Encryption	Partial Encryption		
		LL3	LL3 + HH3	All subbands in level 3
				

- **Information Entropy**

The information entropy is defined to express the degree of uncertainties in the system; it ideally should be 8 bits for gray level images. If an encryption scheme generates an output encrypted image whose entropy is less than 8 bits, then there would be a possibility of predictability, which may threaten its security [20]. Information entropy is calculated by the following equation.

$$H(m) = \sum_{i=0}^{2^{N}-1} p(m_i) \times \log_2 \frac{1}{p(m_i)}, \tag{2}$$

where $p(m_i)$ represent the probability of occurrence of the symbol m_i . Simulation results for entropy analysis are shown in Table 3. Entropy analysis shows that the different encryption schemes have entropy that close to ideal entropy (8), so the schemes are secure against the entropy attack. Moreover, the full encryption achieves entropy value that is closest to the ideal value than partial encryption.

TABLE 3
IMAGE ENTROPY

Image	Encryption	Entropy Value
Airplane (stream cipher RC4)	Full	7.9995
	LL3	7.9453
	LL3 + HH3	7.9874
	All subbands in level 3	7.9993
Airplane (block cipher RC4)	Full	7.9997
	LL3	7.9653
	LL3 + HH3	7.9794
	All subbands in level 3F	7.9997

V. CONCLUSIONS

From the experimental results, we can see that:

- The PSNR value between the original image and encrypted image is less than 11 dB. This indicates that the encryption schemes achieve a high perpetual security. The less PSRR value leads to the best encryption. Full encryption achieves a lower PSNR than partial encryption.
- The entropy value of the encrypted image is nearby equal to the ideal value (8) , which mean that the encrypted image does not leak any information about the original image and can resist entropy attack.
- The histogram of encrypted image is uniformly distributed and it does not leak any amount of information about the original image. Therefore the encryption schemes are secure from frequency analysis attack.
- As the amount of the encrypted part is decreased in partial encryption, the execution time is decreased. So that execution time of partial encryption is lower than the execution time of full encryption.

REFERENCES

[1] S. S. Maniccam and G. B. Nikolaos, "Image and video encryption usingv CAN patterns," *Pattern Recognit.*, vol. 37, no. 4, pp. 725–737, 2004.

[2] E. I. Lin, A. M. Eskicioglu, R. L. Lagendijk, and E. J. Delp, "Advances in digital video content protection," *Proc. IEEE*, vol. 93, no. 1, pp. 171–183, Jan. 2005.

[3] C. Wu and C. C. J. Kuo, "Efficient multimedia encryption via entropy codec design," in *Proc. SPIE Int. Symp. Electronic Imaging 2001*, Jan. 2001, vol. 4314, pp. 128–138.

[4] L. Krikor, S. Baba, T. Arif, and Z. Shaaban, "Image Encryption Using DCT and Stream Cipher", *European Journal of Scientific Research*, Vol.32, No.1, pp.47-57, 2009.

[5] M. Van Droogenbroeck, and R. Benedett, "Techniques for a Selective Encryption of Uncompressed and Compressed Images", *in Proceedings of Advanced Concepts for Intelligent Vision Systems (ACIVS)*, Ghent, Belgium, 2002.

[6] S. K. Panigrahy, B. Acharya, and D. Jena, "Image Encryption Using Self-Invertible Key Matrix of Hill Cipher Algorithm," *1st International Conference on Advances in Computing*, Chikhli, India, 21-22 February 2008

[7] S. R. M. Prasanna, Y. V. Subba Rao and A. Mitra, "An Image Encryption Method with Magnitude and Phase Manipulation using Carrier Images," *International Journal of Computer Science*, Vol. 1, February 20, 2006

[8] W. Zeng and S. Lei, "Efficient Frequency Domain Selective Scrambling of Digital Video," *IEEE Trans. Multimedia*, 2002.

[9] B. Andrew, "Image Compression Using the Discrete Cosine Transform", *Mathematica Journal*, vol. 4, 1994, p. 81-88.

[10] N. Kashyap, and G. R. SINHA, "Image Watermarking Using 3-Level Discrete Wavelet Transform (DWT)," *I.J.Modern Education and Computer Science*, vol. 3, pp. 50-56, 2012.

[11] JTC 1/SC 29, ISO/IEC 10918-1:1994 Information technology – Digital compression and coding of continuous-tone still images: Requirements and guidelines, ISO/IEC Std., 1994.

[12] JTC 1/SC 29/WG 1, ISO/IEC 15444-1:2004 Information technology – JPEG 2000 image coding system: Core coding system, ISO/IEC Std., 2004.

[13] Z. Yang, S. Xie-hua, "A Semi-fragile Watermarking Algorithm Based on HVS Model and DWT," *csse, 2008 International Conference on Computer Science and Software Engineering*, vol. 3, 2008, pp.638-641.

[14] X.-Y. Wang and H. Zhao, "A novel synchronization invariant audio watermarking scheme based on DWT and DCT," *IEEE Transactions on Signal Processing*, vol. 54, no. 12, 2006, pp. 4835–4840.

[15] Y. Zhang. "Blind watermark algorithm based on HVS and RBF neural network in DWT domain", *Wseas transactions on computers*, 2009, vol. 1, pp.174-183.

