Hybrid DCT-DWT Watermarking and IDEA Encryption of Internet Contents

M.A. Mohamed and A.M. El-Mohandes

**Electronics and Communication Engineering, Faculty of Engineering-Mansoura University
Mansoura, Dakhlia, Egypt**

Abstract

Encryption and watermarking are complementary lines of defense in protecting multimedia content. Recent watermarking techniques have therefore been developed independent from encryption techniques. In this paper, we present a hybrid image protection scheme to establish a relation between the data encryption key and the watermark. Prepositioned secret sharing allows the reconstruction of different encryption keys by communicating different activating shares for the same prepositioned information. Each activating share is used by the receivers to generate a fresh content decryption key. In the proposed scheme, the activating share is used to carry copyright or usage rights data. The bit stream that represents this data is also embedded in the content as a visual watermark. When the encryption key needs to change, the data source generates a new activating share, and encrypts the corresponding data with the key constructed from the new activating share. Before transmission, the encrypted data is embedded in a multimedia stream. Each receiver can extract the encrypted data from the host image, and decrypt this data after reconstructing the same key. Our presentation will include the application of the scheme to a test image, and a discussion on the data hiding capacity, watermark transparency, and robustness to common attacks.

Keywords: *discrete cosine transform, discrete wavelet transform, and international data encryption algorithm (IDEA), Bit correct ratio.*

1. Introduction

The advent of the Internet has resulted in many new opportunities for the creation and delivery of content in digital form. Applications include electronic advertising, real-time video and audio delivery, digital repositories and libraries, and Web publishing. An important issue that arises in these applications is the protection of the rights of all participants [1], [2]. It has been recognized for quite some time that current copyright laws are inadequate for dealing with digital data. This has led to an interest towards developing new copy deterrence and protection mechanisms. One such effort that has been attracting increasing interest is based on digital watermarking techniques [3]. Digital watermarking; Fig.1, is the process of embedding information into digital multimedia content such that the information (which we call the watermark) can later be extracted or detected for a variety of purposes including copy prevention and control. Digital watermarking has become an active and important area of research, and development and commercialization of watermarking techniques is being deemed essential to help address some of the challenges faced by the rapid proliferation of digital content [4]. A secure computing environment would not be complete without consideration of encryption technology; Fig.2. The term encryption refers to the practice of obscuring the meaning of a piece of information by encoding it in such a way that it can only be decoded, read and understood by people for whom the information is intended. It is the process of encoding data to prevent unauthorized parties from viewing or modifying it.

The use of simple codes to protect information can be traced back to the fifth century BC. As time has progressed, the methods by which information is protected have become more complex and more secure. Encryption can be used to provide high levels of security to network communication, e-mail, files stored on hard drives or floppy disks, and other information that requires protection. Encryption and watermarking each provide a different line of defense in protecting content. Recent research has therefore followed two different avenues resulting in encryption techniques that are independent from watermarking techniques: (i) Encryption makes the content unintelligible through a reversible mathematical transformation based on a secret key [1], [2]. In secure multimedia content distribution, the audio/visual stream is compressed, packetized and encrypted [3].

One of the most challenging problems in distribution architectures is the delivery of the decryption key, and (ii) Watermarking (data hiding) [4] – [7] is the process of embedding data into a multimedia element such as image, audio or video. This embedded data can later be extracted from, or detected in, the multimedia element for different purposes such as copyright protection, access control, and broadcast monitoring. One possible avenue of research is to establish a relation between the data encryption key and the watermark. A recent method for delivering the keying information in secure multimedia multicast applications suggests the use of a media dependent channel [2]. The rekey messages are embedded in the multimedia stream rather than being sent in a separate channel.

This paper is organized as the following: section (2) introduces the performance measures of: digital watermarking techniques as well as the combined digital watermarking and encryption techniques; (3) discusses the DCT-DWT as a combined digital watermarking technique; (4) presents the basics of encryption and the state of the art of international data encryption algorithm (IDEA) technique; (5) provides the simulation results, and (6) introduces the final conclusion of this paper.

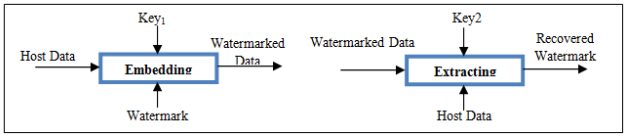

Fig.1 Digital watermarking

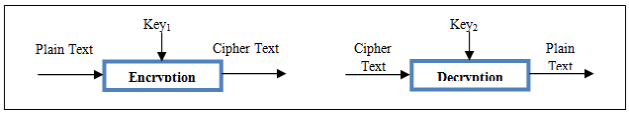

Fig.2 Digital encryption

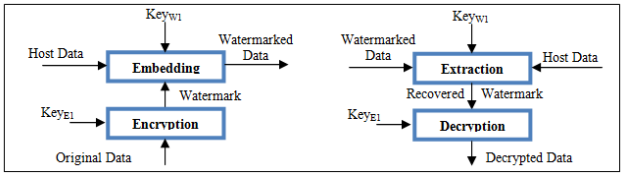

Fig.3 Hybrid technique

2. Performance Measures

How then do we provide metrics for the evaluation of the embedding techniques? Capacity and speed can be easily evaluated using the number of bits per cover size, and computational complexity, respectively. The systems use of keys is more or less by definition, and the statistical imperceptibility by correlation between the original images and recovered counterpart. The more difficult task is providing metrics for perceptibility and robustness.

2.1 Perceptibility Measures

There are five measures used in evaluating the imperceptibility of any embedding system. Assume X is the cover image, and X_W is the watermarked image. Whereas, W is the watermark, and W' is the recovered watermark each of dimensions M×N. It should be noted that these performance measures could be evaluated with respect to: the watermarked data and the host data.

2.1.1 Capacity

$$C = B_w / B_i \tag{1}$$

where B_w is number of watermark bits and Bi is number of host bits.

2.1.2 Minimum Square Error (MSE)

$$MSE = \sum_{i=1}^{M}\sum_{j=1}^{N}\left(W(i,j) - W'(i,j)\right)^2 / (M \cdot N) \tag{2}$$

2.1.3 Peak Signal-to-Noise Ratio (PSNR)

$$PSNR = 20 \times Log\left[\left(2^n - 1\right)/ v\right] \tag{3}$$

where n is the number of bits per pixel.

2.1.4 Correlation Coefficients (R)

$$R = \sum_{i=1}^{N}\left(Xi - \overline{X}\right)\sum_{i=1}^{N}\left(Yi - \overline{Y}\right)\Big/\left(N \bullet \sum_{i=1}^{N}\left(Xi - \overline{X}\right)^2 . \sum_{i=1}^{N}\left(Yi - \overline{Y}\right)^2\right) \tag{4}$$

where N is the number of pixels, Xi is the pixel value of the original image, $\overline{X}$ is the average value of the original image; Y is the pixel value of the modified image and $\overline{Y}$ is the average value of the modified image.

2.1.5 Watermark-to-Document Ratio (WDR)

$$WDR = 10 \times Log\left(\sum_{i=1}^{M}\sum_{j=1}^{N}\left(X(i,j) - X'(i,j)\right)^2 / \sum_{i=1}^{M}\sum_{j=1}^{N}X^2(i,j)\right) \tag{5}$$

2.2 Measuring Robustness

Low level is the bare minimum requirements that a watermark must meet in order to be considered useful. Watermarks at this level should be resistant to common modifications that non-malicious users with inexpensive tools might do to images. As the robustness increases more specialized and expensive tools become required, as well as more intimate knowledge of the watermarking system being used. At the very top of the scale is provable reliability in which it is either computationally or mathematically impossible to remove or disable the mark [8]. Some of the early literature considered a binary robustness metric that only allows for two different states. However, it makes sense to use a metric that allows for different levels of robustness. The use of bit-correct ratio (BCR) has become recently, as it allows for more detailed scale of values; BCR is defined as:

$$BCR = \frac{100}{l}\sum_{n=0}^{l-1}\begin{cases}1 & W_n' = W_n \\ 0 & W_n' \neq W\end{cases} \tag{6}$$

where l is the watermark length, W_n is the nth bit of the embedded watermark and W_n' is the nth bit of the recovered watermark. In this paper, some data processing operations are applied to the watermarked data; these are: (i) JPEG compression; (ii) mean filter; (iii) median filter;

(iv) Gaussian noise; (v) blurring, (vi) histogram equalization; (vii) Gamma correction, and (viii) intensity adjustment.

3. Combined Technique

Commonly used frequency-domain transforms include the Discrete Wavelet Transform (DWT), the Discrete Cosine Transform (DCT) and Discrete Fourier Transform (DFT). However, DWT [7] has been used in digital image watermarking more frequently due to its excellent spatial localization and multi-resolution characteristics, which are similar to the theoretical models of the human visual system [8]. Further performance improvements in DWT-based digital image watermarking algorithms could be obtained by combining DWT with DCT [7]. The idea of applying two transforms is based on the fact that combined transforms could compensate for the drawbacks of each other, resulting in effective watermarking.

3.1 The DCT and DWT Transforms

The discrete cosines transform (DCT) and discrete wavelet transform (DWT) transforms have been extensively used in many digital signal processing applications. In this section, we introduce the two transforms briefly, and outline their relevance to the implementation of digital watermarking. The DCT is a technique for converting a signal into elementary frequency components [9]. It represents an image as a sum of sinusoids of varying magnitudes and frequencies. With an input image, x, the DCT coefficients for the transformed output image, y, are computed according to Eq.7 shown below. In the equation, x, is the input image having N x M pixels, x(m, n) is the intensity of the pixel in row m and column n of the image, and y(u, v) is the DCT coefficient in row u and column v of the DCT matrix.

$$y(u,v)=\sqrt{\frac{2}{M}}\sqrt{\frac{2}{N}}\alpha_u\alpha_v\sum_{m=0}^{M-1}\sum_{n=0}^{N-1}(x(m,n)\cos(\frac{(2m+1)u\pi}{2M})\cos(\frac{(2n+1)v\pi}{2N})) \quad (7)$$

where

$$\alpha_u = \begin{cases} 1/\sqrt{2} & u=0 \\ 1 & u=1,2,.....,\ M-1 \end{cases}$$

$$\alpha_v = \begin{cases} 1/\sqrt{2} & v=0 \\ 1 & v=1,2,.....,\ N-1 \end{cases} \quad (8)$$

The image is reconstructed by applying inverse DCT operation according to Eq.9:

$$x(m,n)=\sum_{u=0}^{M-1}\sum_{v=0}^{N-1}(\sqrt{\frac{2}{M}}\sqrt{\frac{2}{N}}\alpha_u\alpha_v y(u,v)\cos(\frac{(2m+1)u\pi}{2M})\cos(\frac{(2n+1)v\pi}{2N})) \quad (9)$$

The popular block-based DCT transform segments image non-overlapping blocks and applies DCT to each block. These results in giving three frequency sub-bands: low frequency sub-band, mid-frequency sub-band and high frequency sub-band. DCT-based watermarking is based on two facts. The first fact is that much of the signal energy lies at low-frequencies sub-band which contains the most important visual parts of the image. The second fact is that high frequency components of the image are usually removed through compression and noise attacks. The watermark is therefore embedded by modifying the coefficients of the middle frequency sub-band so that the visibility of the image will not be affected and the watermark will not be removed by compression.

The DWT transform: Wavelets are special functions which, in a form analogous to sines and cosines in Fourier analysis, are used as basal functions for representing signals [10]. For 2D images, applying DWT corresponds to processing the image by 2D filters in each dimension. The filters divide the input image into four non-overlapping multi-resolution sub-bands LL1, LH1, HL1 and HH1. The sub-band LL1 represents the coarse-scale DWT coefficients while the sub-bands LH1, HL1 and HH1 represent the fine-scale of DWT coefficients. To obtain the next coarser scale of wavelet coefficients, the sub-band LL1 is further processed until some final scale N is reached. When N is reached we will have 3N+1 sub-bands consisting of the multi-resolution sub-bands LLN and LHx, HLx and HHx where x ranges from 1 until N. Due to its excellent patio-frequency localization properties, the DWT is very suitable to identify the areas in the host image where a watermark can be embedded effectively. In particular, this property allows the exploitation of the masking effect of the human visual system such that if a DWT coefficient is modified, only the region corresponding to that coefficient will be modified.

In general most of the image energy is concentrated at the lower frequency sub-bands LLx and therefore embedding watermarks in these sub-bands may degrade the image significantly. Embedding in the low frequency sub-bands, however, could increase robustness significantly. On the other hand, the high frequency sub-bands HHx include the edges and textures of the image and the human eye is not generally sensitive to changes in such sub-bands. This allows the watermark to be embedded without being perceived by the human eye. The compromise adopted by many DWT-based watermarking algorithm, is to embed the watermark in the middle frequency sub-bands LHx and HLx where acceptable performance of imperceptibility and robustness could be achieved.

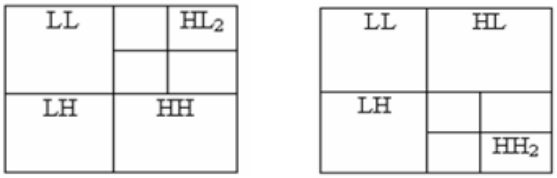

Fig.4 DWT decomposition levels

3.2 The Combined DCT-DWT Algorithm

The watermark embedding procedure is depicted in Fig.5 followed by a detailed explanation [11-14]:

Step-1: Apply DWT to decompose the cover host image into four non-overlapping multi-resolution sub-bands: LL1, HL1, LH1, and HH1.

Step-2: Apply DWT again to sub-band HL1 to get four smaller sub-bands and choose the HL2 sub-band as shown in Fig.4a. Or, apply DWT to sub-band HH1 to get four smaller sub-bands and choose the HH2 sub-band as shown in Fig.4b.

Step-3: Divide the sub-band HL2 (or HH2) into 8 x 8 blocks.

Step-4: Apply DCT to each block in the chosen sub-band (HL2 or HH2).

Step-5: Re-formulate the grey-scale watermark image into a vector of zeros and ones.

Step-6: Generate two uncorrelated pseudorandom sequences. One sequence is used to embed the watermark bit 0 (PN_0) and the other sequence is sued to embed the watermark bit 1 (PN_1). Number of elements in each of the two pseudorandom sequences must be equal to the number of mid-band elements of the DCT-transformed DWT sub-bands.

Step-7: Embed the two pseudorandom sequences, PN_0 and PN_1, with a gain factor α, in the DCT transformed 8x8 blocks of the selected DWT sub-bands of the host image. Embedding is not applied to all coefficients of the DCT block, but only to the mid-band DCT coefficients. If we donate $\boldsymbol{X}$ as the matrix of the mid-band coefficients of the DCT transformed block, then embedding is done as follows: If the watermark bit is 0 then:

$$X' = X + (\alpha \times PN\_0) \quad (10)$$

Otherwise, if the watermark bit is 1 then,

$$X' = X + (\alpha \times PN\_1) \quad (11)$$

Step-8: Apply inverse DCT (IDCT) to each block after its mid-band coefficients have been modified to embed the watermark bits as described in the previous step.

Step 9: Apply the inverse DWT (IDWT) on the DWT transformed image, including the modified sub-band, to produce the watermarked host image.

The watermark *extraction* procedure is depicted in Fig.6, and described in details in the following steps. The combined DWT-DCT algorithm is a blind watermarking algorithm, and thus the original host image is not required to extract the watermark:

Step-1: Apply DWT to decompose the watermarked image into four non-overlapping multi-resolution subbands: LL1, HL1, LH1, and HH1.

Step-2: Apply DWT to HL1 to get four smaller subbands, and choose the sub-band HL2, as shown in Fig. 4a. Or, apply DWT to the HH1 sub-band to get four smaller sub-bands, and choose the HH2 sub-band, as shown in Fig. 4b.

Step-3: Divide the sub-band HL2 (or HH2) into 8 x 8 blocks.

Step-4: Apply DCT to each block in the chosen sub-band (HL2 or HH2), and extract the mid-band coefficients of each DCT transformed block.

Step-5: Regenerate the two pseudorandom sequences (PN_0 and PN_1) using the same seed used in the watermark embedding procedure.

Step-6: For each block in the sub-band HL2 (or HH2), calculate the correlation between the mid-band coefficients and the two generated pseudorandom sequences (PN_0 and PN_1). If the correlation with the PN_0 was higher than the correlation with PN_1, then the extracted watermark bit is considered 0, otherwise the extracted watermark is considered 1.

Step-7: Reconstruct the watermark using the extracted watermark bits, and compute the similarity between the original and extracted watermarks.

4. Encryption

Encryption is said to occur when data is passed through a series of mathematical operations that generate an alternate form of that data; the sequence of these operations is called an algorithm. To help distinguish between the two forms of data, the unencrypted data is referred to as the plaintext and the encrypted data as ciphertext [1, 15]. The security of encryption lies in the ability of an algorithm to generate ciphertext that is not easily reverted to the original plaintext. Encryption is generally used because of its benefits such as ease –of– use, reliability, and security. Encryption divided into many categories: (i) according to key; we have two types (Symmetric key and Asymmetric key algorithm); (ii) according to the way of encryption; we have two types (Stream ciphering and Block ciphering), and (iii) according to the type of operation; we have two types (Substitution and Transposition) [2].

4.1 Why we use Encryption?

There are many reasons of using encryption: (i) Reliability means that the cipher text will always be recoverable and the recovered data will be the same as to the original plaintext; (ii) Security means that the encryption system will in fact keep the information hidden from all but those persons intended to see it, and (iii) An encryption system which is easy to use should allow keyboard entry of a string from 10 to 60 characters Ease-of-use is easy to understand.

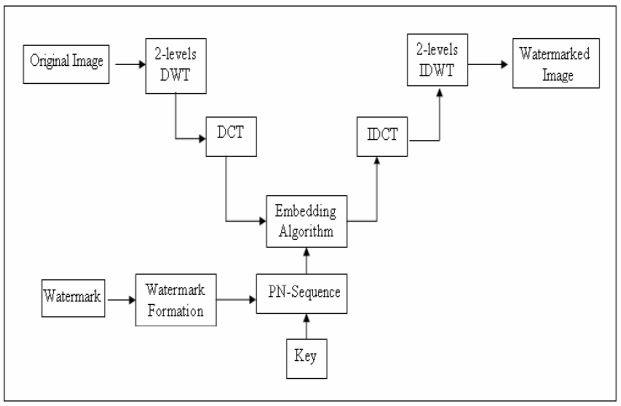

Fig.5 Embedding in DCT-DWT technique

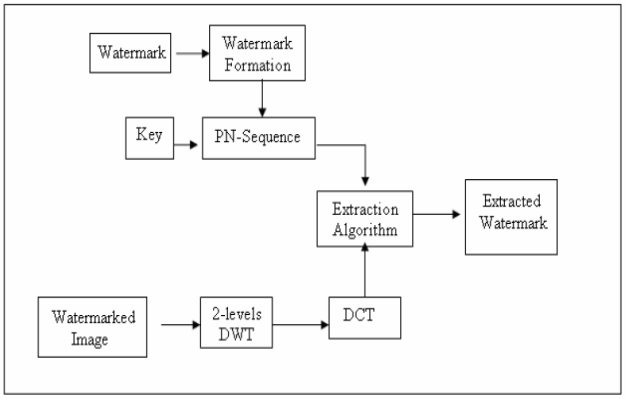

Fig.6 Extraction in DCT-DWT technique

4.2 Advantages & Disadvantages of Encryption

Encryption can play a very important role in your day-to-day computing and communicating: (i) Encryption can protect information stored on your computer from unauthorized access - even from people who otherwise have access to your computer system; (ii) Encryption can protect information while it is in transit from one computer system to another, and (iii) Encryption can be used to deter and detect accidental or intentional alterations in your data. Despite these advantages, encryption has its limits: (i) Encryption can't prevent an attacker from deleting your data altogether; (ii) An attacker might find a previously unknown and relatively easy way to decode messages encrypted with the algorithm you are using, and (iii) An attacker could access your file before it is encrypted or after it is decrypted [15-20].

4.3 Encryption Benefits

In addition to the advantages of encryption; it has the following benefits: (i) data confidentiality-protects the privacy and safety of business and personal information; (ii) Access control–allows data access only to authorized users, and (iii) key management–provides key generation, distribution, and storage.

4.4 IDEA Algorithm

International data encryption algorithm (IDEA) is patented by the Swiss firm of Ascom. They have, however, been generous in allowing, with permission, free noncommercial use of their algorithm, with the result that IDEA is best known as the block cipher algorithm used within the popular encryption program PGP. The IDEA algorithm is interesting in its own right. It includes some steps which, at first, make it appear that it might be a non-invertible hash function instead of a block cipher [1], [2]. Also, it is interesting in that it entirely avoids the use of any lookup tables or S-boxes. IDEA uses 52 subkeys, each 16 bits long. Two are used during each round proper, and four are used before every round and after the last round. It has eight rounds; Fig.7 and 8.

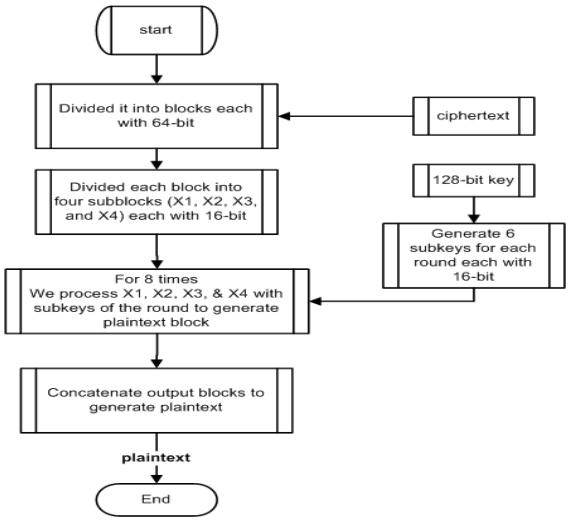

Fig.7The encryption process of IDEA

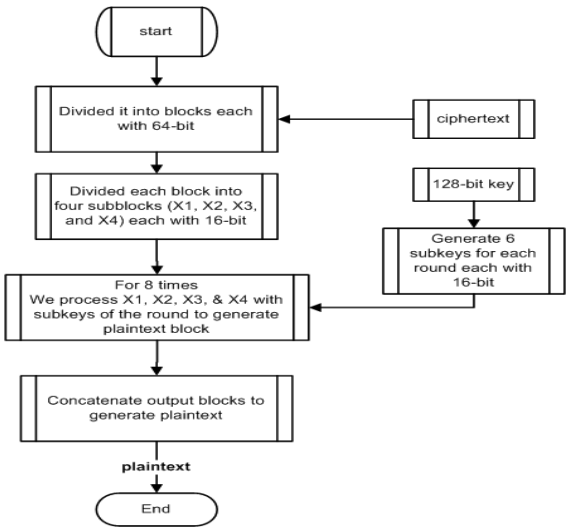

Fig.8The decryption process of IDEA

The plaintext block in IDEA is divided into four quarters, each 16 bits long. Three operations are used in IDEA to combine two 16 bit values to produce a 16 bit result, addition, XOR, and multiplication. Addition is normal addition with carries, modulo 65,536. Multiplication, as used in IDEA, requires some explanation. Multiplication by zero always produces zero, and is not invertible. Multiplication modulo n is also not invertible whenever it is by a number which is not relatively prime to n. The way multiplication is used in IDEA, it is necessary that it be always invertible. This is true of multiplication IDEA style. The number 65,537, which is $2^{16}+1$, is a prime number. (Incidentally, 2^8+1, or 257, is also prime, and so is 2^4+1, or 17, but $2^{32}+1$ is not prime, so IDEA cannot be trivially scaled up to a 128-bit block size.) Thus, if one forms a multiplication table for the numbers from 1 through 65,536, each row and column will contain every number once only, forming a Latin square, and providing an invertible operation. The numbers that 16 bits normally represent are from 0 to 65,535 (or, perhaps even more commonly, from -32,768 to 32,767). In IDEA, for purposes of multiplication, a 16 bit word containing all zeroes is considered to represent the number 65,536; other numbers are represented in conventional unsigned notation, and multiplication is modulo the prime number 65,537.

5. Results and Discussions

The performance of two combined digital watermarking techniques: (i) DCT-DWT and (ii) modified DCT-DWT; with and without encryption was tested and evaluated. The simulation process was performed using MATLAB-2009a using Intel Core2 Duo 2.66 GHz, 4 GB RAM on Microsoft Windows Service Pack-3. The host image was chosen as a grayscale image of size 256×256, uncompressed, and of 8 bits per pixel depth. The watermark data was simulated as a black and white image of size 32×128 containing text information. The results provided in Tables 1 introduce the objective evaluation parameters: (i) capacity; (ii) MSE; (iii) $PSNR_{dB}$; (iv) WDR_{dB}, and (v) R.

These results show a great improvement in the performance of the combined watermarking technique when assigned with encryption. In addition the use of hybrid system of digital watermarking and encryption resist different types of attacks in a very good manner as shown in the BCR values presented in Table 2. These results showed that the proposed technique provided a great improvement in resisting: (i) histogram equalization; (ii) gamma correction; (iii) intensity adjustment; (iv) blurring; (v) JPEG compression; (vi) cropping; (vii) median filtering, and (viii) mean filtering. These improvements are illustrated in the set of figures from Fig.9 to Fig.22. Fig.9 shows the watermark information; Fig.10 shows the host image; Fig.11 shows the watermarked image without encryption; Fig.12 illustrates the recovered watermark; Fig.13 provides the encrypted watermark; Fig.14 illustrates the watermarked data with encryption; Fig.15 shows the recovered encrypted watermark from Fig.14; Fig.16 gives the recovered decrypted watermark of Fig.15; Fig.17 watermarked data with modified technique without encryption; Fig.18 recovered watermark from Fig.17; Fig.19 encrypted original watermark; Fig.20 shows the watermarked data using modified watermarking technique with encryption; Fig.21 recovered encrypted watermark from Fig.20, and Fig.22 shows the decrypted watermark of Fig.21.

6. Conclusion

From our results we can easily see that our modified watermarking with encryption technique improves the imperceptibility measures (PSNR, WDR, R, Capacity, and MSE), and also improves the robustness against attacks that depend on filtering the data. Although we can see that our modified technique makes the robustness against JPEG compression attacks, histogram equalization attacks, etc. worst than watermarking without encryption.

Table.1 Results of imperceptibility measures

Parameter	Watermark Only		Watermark with Encryption	
	DCT-DWT	Modified DCT-DWT	DCT-DWT	Modified DCT-DWT
Capacity	0.0037	0.0037	0.0037	0.0037
MSE	228.0360	2.2903	157.1601	1.5755
PSNR(dB)	24.6707	45.5215	26.2804	46.5283
WDR(dB)	-24.5934	-38.1551	-26.2123	-39.1618
R	0.9533	0.9995	0.9671	0.9997

Table.2 Results of robustness measures; BCR

Attacks	Watermark Only		Watermark with Encryption	
	DCT-DWT	Modified DCT-DWT	DCT-DWT	Modified DCT-DWT
Histogram Equalization	49.5493	51.8126	71.2354	96.2840
Gamma Correction [0.5]	49.9968	63.9981	73.5863	98.4241
Intensity Adjustment	25.5869	60.0973	51.1154	98.3722
Blurring [16*16]	22.9604	48.0739	52.9086	49.7147
JPEG Compression [2:1]	50.2367	50.4086	80.1621	98.5765
Cropping [50:40]	25.5869	60.0973	53.1154	98.3722
Mean Filter [16*16]	22.9767	48.1388	52.6005	49.6920
Median Filter [16*16]	23.1582	48.2685	53.1809	50.4248

References

[1] S. Lian, "Multimedia content encryption: techniques and applications," CRC Press, 2009, ISBN: 0-8493-8214-9.

[2] B. Schneier, "Applied cryptography", John Wiley & Sons, Inc, 1996, ISBN 0-471-12845-7.

[3] M.Y. Rhee, "Internet security cryptographic principles, algorithms and protocols," Wiley Press, 2003, ISBN-13: 978-0470852859.

[4] J. Seitz, "Digital watermarking for digital media," Information Science Publishing, 2005, ISBN-10: 159140519X.

[5] Y.O. Shi, "Transactions on Data Hiding and Multimedia Security III," Springer, ISBN: 3540690166, 2008.

[6] B. Furht and D. Kiroviski, "Multimedia Security Handbook Internet & Communications," CRC press, 2004, ISBN-10: 0849327733.

[7] A. Haj, "Combined DWT-DCT digital image watermarking," Journal of Computer Science, Vol. 3, No. 9, pp: 740-746, 2007.

[8] F.A. Petitcolas, "Watermarking Schemes Evaluation," IEEE Signal Processing Magazine, Vol.17, pp: 58-64, September 2000.

[9] J.R. Hernández, M. Amado, and F. Pérez-González," DCT-domain watermarking techniques for still images: detector performance analysis and a new structure," IEEE Trans. on Image Processing, Vol. 9, No.1, pp: 55-68, January 2000.

[10] S. Vural, H. Tomii, and H. Yamauchi, "DWT based robust watermarking embed using CRC-32 techniques," World Academy of Science, Engineering and Technology, Vol. 5, pp: 106-109, 2005.

[11] A. Reddy and B. Chatterji, "A New Wavelet Based Logo-watermarking Scheme," Pattern Recognition Letters, Vol. 26, No. 7, pp: 1019-1027, 2005.

[12] W. Chu, "DCT-based image watermarking using subsampling," IEEE Trans. Multimedia, Vol. 5, No.1, pp: 34-38, 2003.

[13] M. Sharkas, D. ElShafie, and N. Hamdy, "A Dual Digital-Image Watermarking Technique," World Academy of Science, Engineering and Technology, Vol. 5, pp: 136-139, 2005.

[14] S.A. Kasmani and A. Naghsh-Nilchi, "A New Robust Digital Image Watermarking Technique Based on Joint DWT-DCT Transformation," Convergence and Hybrid Information Technology. Third International Conference on ICCIT '08, pp: 539 – 544, 2008.

[15] A.J. Menezes, P.C. Van Oorschot, S.A. Vanstone, "Handbook of applied cryptography, 1996, ISBN: 0-8493-8523-7.

[16] M. Salleh, S. Ibrahim & I.F. Isnin, "Image encryption algorithm based on chaotic mapping," *Jurnal Teknologi*, Vol.39, No. D, pp:1–12, 2003.

[17] G. Jakimoski and L. Kocarev."Chaos and cryptography: block encryption ciphers based on chaotic maps". IEEE Trans. on Circuits And Systems, Vol. 48, No.2, pp:163-169, 2001.

[18] S. Li, et. al. "Chaotic encryption scheme for real-time digital video". Proc.of SPI,E Vol. 4666: pp: 149-160, Real-Time Imaging VI, Nasser Kehtarnavaz; Ed., 2002.

[19] P. Junod and S. Vaudenay, "FOX: A new family of block ciphers," in *Proceedings of the SAC 2004 workshop*, 2004, pp. 114–129.

[20] J. Wolkerstorfer, E. Oswald, and M. Lamberger, "An ASIC implementation of the AES SBoxes," in *Proceedings of CT-RSA*, 2002, pp. 67–78.

Dr. Mohamed Abdel-Azim received the PhD degree in Electronics and Communications Engineering from the Faculty of Engineering-Mansoura University-Egypt by 2006. After that he worked as an assistant professor at the electronics & communications engineering department until now.

He has 27 publications in various international journal and conferences. His current research interests are in multimedia processing, wireless communication systems, and field programmable gate array (FPGA) applications.

I am a teaching Assistant at the Department of Electronics and communications Engineering, Faculty of Engineering, Mansoura University, Egypt. I got the B. Sc in electronics and communications Engineering 2008; excellent with honor, Faculty of Engineering-Mansoura University.

My areas of interest are security systems and multimedia encryption techniques for cellular communications systems and internet content. I hope to join a research team in one of foreign universities in order to complete my research in this area.

Fig.9 The watermark data

Fig.10 The host image

Fig.11 Watermarked data without encryption

Fig.12 Recovered watermark from Fig.11 encryption

Fig.13 Encrypted original watermark

Fig.14 Watermarked data with encryption

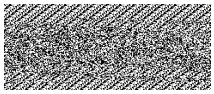

Fig.15 Recovered encrypted watermark

Fig.16 Decryption of original watermark

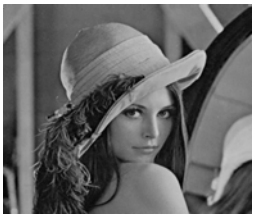

Fig.17 Modified watermark without encryption

Fig.18 Recovered watermark data

Fig.19 Encrypted original watermark

Fig.20 Modified watermark with encryption

Fig.21 Recovered encrypted watermark data

Fig.22 Decrypted data of Fig.21