

ROBUST SECURE AND BLIND WATERMARKING BASED ON DWT DCT PARTIAL MULTI MAP CHAOTIC ENCRYPTION

Esam A. Hagra¹, M. S. El-Mahallawy², A. Zein Eldin³, M. W. Fakhr⁴

¹Faculty of Engineering, Alexandria University, Alexandria, Egypt

¹esamhagra_2006@yahoo.com

^{2,3,4}Arab Academy for Science and Technology and Maritime Transport, Egypt.

²mahallawy@ieee.org, ³a3hzein@hotmail.com, ⁴waleedfakhr@yahoo.com

ABSTRACT

In this paper, a novel Commutative Watermarking and Partial Encryption (CWPE) algorithm based on Discrete Wavelet Transform and Discrete Cosine Transform (DWT-DCT) for watermarking and Multi-Map Wavelet Chaotic Encryption (MMW-CE) is proposed. The original host image is first decomposed into four sub-bands using (DWT), each sub-band coefficients are relocated using Arnold transform to create a noise-like version, then apply partial encryption scheme using chaotic scrambled random number pattern bitwise XOR with the scrambled horizontal coefficients only and the shuffled approximation coefficients are divided into non-overlapping and equal sized blocks. Watermark embedding process is based on extracting the (DCT) middle frequencies of the encrypted approximation coefficients blocks. Comparison based threshold of the extracted DCT mid-band coefficients, watermark bits are embedded in the coefficients of the corresponding DCT middle frequencies. The experimental results show that the proposed algorithm is robust against common signal processing attacks. The proposed algorithm is able to reduce encryption to one quarter of the image information. Statistical and differential analyses are performed to estimate the security strength of the proposed algorithm. The results of the security analysis show that the proposed algorithm provides a high security level for real time application.

KEYWORDS

DWT, DCT, Watermarking, Partial Encryption, Chaotic Encryption.

1. INTRODUCTION

The security of multimedia data transmitted over wireless networks is of increased interest. Encryption mechanisms securely transmit multimedia data over insecure networks and protect the confidentiality of media content. Watermarking can be used to protect the copyright of media content. Because media encryption and media watermarking serve different applications, they can be combined to protect both confidentiality and ownership/identity. The concept of Commutative Watermarking and Encryption (CWE) was first reported in [1-3]. It means that multimedia content can either be first watermarked then encrypted or first encrypted then watermarked. Multimedia content first watermarked then encrypted makes use of partial encryption to construct the CWE scheme. In this kind of scheme, the media data is partitioned into two parts, one part of the data is encrypted and the other is watermarked [4].

Digital watermarking techniques can be classified into two categories: spatial domain techniques and transform domain techniques. Spatial domain techniques usually provide simple embedding

schemes with inefficiency and low robustness. By contrast, transform domain watermarking techniques like those based on *DCT* [5-9], *DWT* [10-13] typically provide higher image imperceptibility and are much more robust to image manipulations. In these domains watermark is embedded in perceptually significant coefficients of the image. However, *DWT* has been used more frequently in digital image watermarking due to its time/frequency decomposition characteristics, which resemble to the theoretical models of the human visual system (*HVS*) [14-15]. In order to further performance improvements in *DWT* based digital image watermarking algorithms could be obtained by jointing *DWT* with *DCT* [16-17]. The reason of applying two transform is based on the fact that jointed transform could make up for the disadvantages of each other, so that effective watermarking approaches could acquire.

Chaotic cryptography and watermarking has been attracting more and more attention from the nonlinear system society since the essence of chaos dynamic system matches the very basic criteria of cryptography. Chaos based encryption techniques are considered suitable for practical use as these techniques provide combination of speed, high security, complexity, reasonable computational overheads and computational power [19-20].

Hence, in this paper a new Commutative Watermarking and Partial Encryption (*CWPE*) algorithm based on mixed single level two dimension transform domain (*1L 2D DWT-DCT*) and Multi-Map Orbit Hopping Chaotic System (*MMOH-CS*) is proposed and compared with *PEW* scheme using single level two dimension *DWT* (*PEW 1L 2D DWT*) and Multi-Map Orbit Hopping Chaotic System (*MMOH-CS*). In the proposed algorithm (*CWPE 2D DWT DCT*), first the host image is decomposed into four subbands using *DWT*, each wavelet sub-band is scrambled with its own Arnold map then, the horizontal scrambled coefficients is then encrypted using a chaotic scrambled random number pattern which is generated using scrambled multi chaotic logistic maps. Divided the approximation encrypted coefficients into non-overlapping (8x8) blocks, apply *DCT* to each block and extract the middle frequencies, Comparison based threshold of the extracted *DCT* mid-band coefficients, finally, watermark bits are embedded in the coefficients of the corresponding *DCT* middle frequencies. The proposed system is tested under different signal processing attacks. Security analysis for the proposed system is also performed and presented.

2. PROPOSED CWPE 2D DWT DCT ALGORITHM

The proposed algorithm consists of two stages. The first pre-processing stage is concerned with the preparation of the encryption requirements. In this stage, the biometric features which are considered a secured and authenticated proof of ownership is first generated and combined with a user secret key using the Secure Key Management (*SKM*) subsystem. *SKM* generates both chaotic scrambling parameters and initial conditions for the multi map orbit hopping chaotic system. The second processing stage is concerned with the watermark embedding and partial encryption processes. The block diagram of the proposed algorithm is shown in Fig.1.

2.1 Preprocessing Stage

The *CWPE 2D DWT DCT* Pre-processing Stage consists of Secure Key Management subsystem, Chaotic Scrambling Parameter generator subsystem and Multi-Map Orbit Hopping Chaotic Subsystem.

2.1.1 Secure Key Management Subsystem

The main stages of a typical fingerprint based system; acquisition, representation and feature extraction are implemented to extract the minutiae attributes (x, y, θ) to be used as a biometric key. A post processing step is used to remove spurious detected minutiae. The minutiae data

contain three fields per minutiae: x -coordinate, y -coordinate and orientation for a total of 25 minutiae. Every field of minutia data is converted to 9-bit binary. Hence, the total minutiae bits are represented by $(25 \times 3 \times 9 = 675 \text{ bits})$ [21].

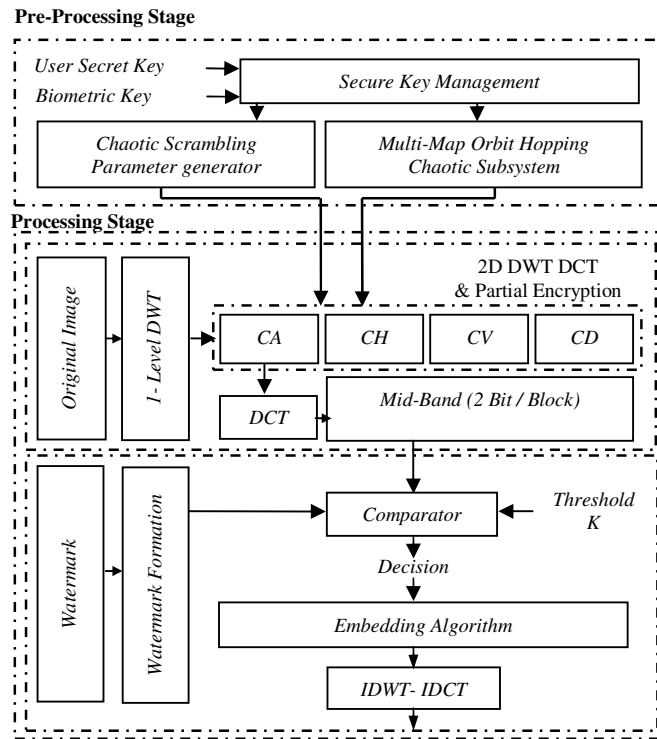


Figure 1. Proposed CWPE 1L 2D DWT DCT scheme

The minutiae data (675 bits) are concatenated with the secret key (256-bits) and interleaved using random interleaver [22]. The output is hashed using the Secure Hash Algorithm-256 (SHA-256) to satisfy the diffusion and confusion properties [23]. The ideal diffusion effect for hash value in binary format should be that: any tiny changes in used secret key leads to 50% changing probability for each bit of the output. The output of SHA-256 is then divided into 16 different length sub-keys to control the behavior of the chaotic maps initial conditions and the Arnold map parameters. The first eight sub-keys (192-bits length; 24×8) are used to produce the chaotic maps initial conditions for the MMOH-CS. The last eight sub-keys (64-bits length; 8×8) are used to produce the Arnold secret control parameters needed for the chaotic scrambling parameter generator subsystem. Fig.2 shows the sub-keys generation process.

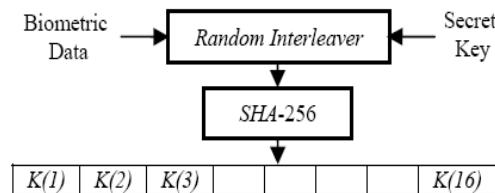


Figure 2. SKM sub-keys generation process

2.1.2 Chaotic Scrambling Parameter Generator Subsystem

The DWT scrambling process is based on Arnold Cat Map which is 2-D chaotic map described by [7]:

$$\begin{bmatrix} x_{n+1} \\ y_{n+1} \end{bmatrix} = \begin{bmatrix} 1 & a \\ b & a \cdot b + 1 \end{bmatrix} \begin{bmatrix} x_n \\ y_n \end{bmatrix} \text{mod}(255) \quad (1)$$

Where, (x_n, y_n) is the pixel position in each 2D DWT sub bands (CA, CH, CV, CD), (x_{n+1}, y_{n+1}) is the transform position after scrambling and $a, b \in 255$ are the secret control parameters. Fig. 3 shows Arnold Cat Maps parameter generation process.

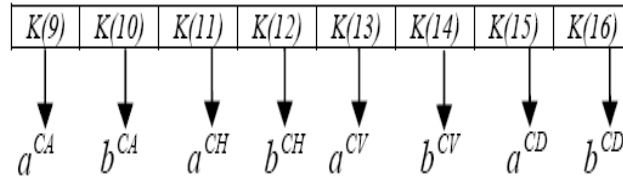


Figure 3. Arnold Cat Maps parameter generation process

2.1.3 Multi-Map Orbit Hopping Chaotic system

The proposed MMOH-CS uses four chaotic logistic maps as shown in Fig. 4. The multiple chaotic logistic maps are used to generate chaotic orbits hopping patterns for the single level 2D DWT partial encryption algorithm, the multiple logistic maps are given by:

$$x_{n+1}^j = r \cdot x_n^j \cdot (1 - x_n^j), \quad r \in (3.9, 4], x_n \in (0, 1) \quad (2)$$

Where, x_n and r are the system variable and parameter respectively, n is the number of chaotic orbit and J is the logistic map index.

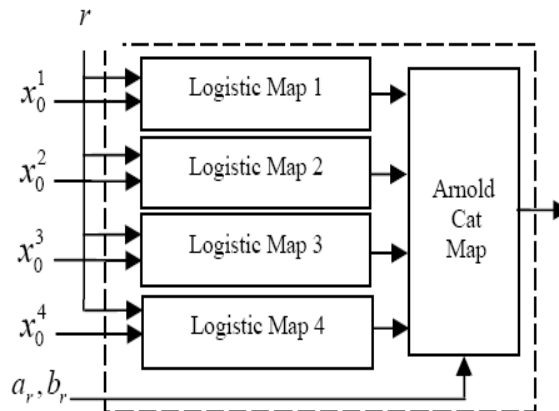


Figure 5. Multi-Map Orbit Hopping Chaotic Subsystem

The initial values for each logistic map are generated as shown in Fig. 5. The initial values are calculated using the following steps:

- Convert the first 24-bit in the four sub-keys to its decimal values.
- Make the number 6 digits. If the original number is shorter than 6 digits, add zeros at the end. If the original number is longer than 6 digits, chop off the extra digits from the left side.
- Multiply the generated 6 digits number by 10^{-7} .

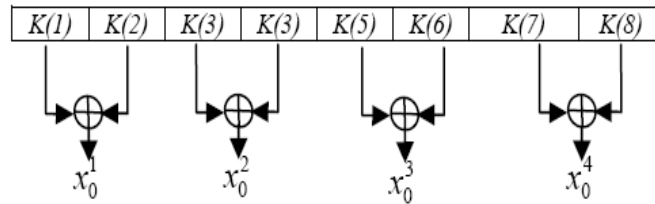


Figure 6. Logistic Maps initial condition generation process

The four chaotic logistic maps are used to generate 128×128 chaotic orbit points concatenated together. Arnold Cat Map is used to scramble all orbit points. The Arnold Cat Map Parameters (a_r, b_r) generation process is illustrated in Fig. 6.

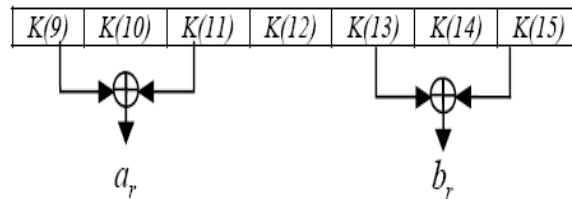


Figure 7. Arnold Cat Map Parameters generation process

2.2 Processing Stage

In this stage, multiple domain watermarking and Partial Multi Map Chaotic Encryption (PMMCE) is applied. The proposed algorithm processing stage is illustrated below.

2.2.1 Watermark Embedding and PMMCE process

- Apply *DWT* to the host image and computes the approximation coefficient matrix *CA* and details coefficients matrices (*CH*, *CV* and *CD*).
- Scramble each sub-band using its own Arnold map.
- Apply partial encryption scheme using chaotic scrambled random number pattern bitwise XOR with the scrambled wavelet decomposition *CH* sub-band only.
- Divide encrypted *CA* into (8×8) blocks, apply *DCT* and extract the middle frequencies.
- For watermark embedding, two locations are chosen from mid band region for comparison, when the two differences in magnitude between the two locations being compared does not exceed the threshold; they coefficients are scaled such that they meet this requirement.

2.2.2 Watermark extraction Process and decryption

- Apply de-scrambling and partial decryption scheme.
- Repeat comparison based threshold for the extracted mid band frequencies for each block and revert back the watermark image.

3. SECURITY ANALYSIS

In this paper, the strength of the proposed encryption algorithm is tested using visual analysis and evaluating the most important security analysis tests, statistical analysis, and differential analysis as illustrated below.

3.1 Visual Testing

In order to demonstrate the effectiveness of the proposed algorithm, the Peak Signal to Noise Ratio (*PSNR*) is used to measure the invisibility of the encrypted watermarked image. *PSNR* is defined [21] and the results are shown in Table 1. The *1L 2D DWT DCT* encrypted Peppers based on the user secret key and the biometric key is shown in Fig. 7.

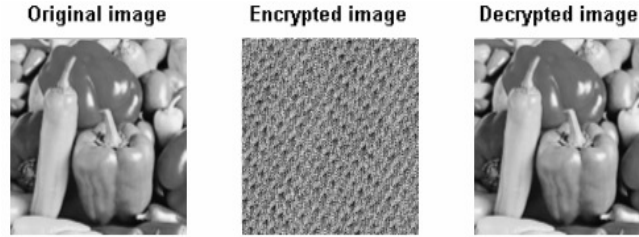


Figure 8. 1L 2D DWT DCT-based encrypted and decrypted Peppers

3.2 Statistical analysis

Statistical analysis has been performed on the proposed algorithm demonstrating its superior confusion and diffusion properties, which strongly resist statistical attacks. This is shown by a test on the correlations of adjacent pixels in the ciphered image. To test the correlation between two vertically adjacent pixels, the correlation coefficient in plain image /cipher image, respectively is calculated using the following two formulas:

$$Cov(x, y) = \frac{1}{N} \sum_{i=1}^N (x_i - E(x))(y_i - E(y)) \quad (3)$$

$$r_{x,y} = Cov(x, y) / \sqrt{D(x) \cdot D(y)} \quad (4)$$

Where, x and y are grey scale values of two adjacent pixels in the image. In numerical computation, the following discrete were used:

$$E(x) = \frac{1}{N} \sum_{i=1}^N x_i \quad (5)$$

$$D(x) = \frac{1}{N} \sum_{i=1}^N (x_i - E(x))^2 \quad (6)$$

3.3 Differential Analysis

In general, the opponent may make a slight change such as modifying only one pixel of the encrypted image, and then observes the change of the result. In this way, he may be able to find out a meaningful relationship between the plain image and the cipher image. If one minor change in the plain image can cause a significant change in the cipher image, with respect to diffusion and confusion, then this differential attack would become very inefficient and practically useless. To test the influence of one-pixel change on the whole image encrypted by the proposed algorithm, two common measures were used; number of pixels change rate (*NPCR*) and unified average changing intensity (*UACI*) [10]. Denote two cipher-images, whose corresponding plain-images have only one-pixel difference, by C_1 and C_2 , respectively. Label the grey-scale values of the pixels at grid (i, j) of C_1 and C_2 by $C_1(i, j)$ and $C_2(i, j)$ respectively. Define a bipolar array D with the same size as image C_1 or C_2 , then $D(i, j)$ is determined by $C_1(i, j)$ and $C_2(i, j)$. Namely if $C_1(i, j) = C_2(i, j)$ then $D(i, j) = 1$, otherwise $D(i, j) = 0$. The *NPCR* and *UACI* are defined as:

$$NPCR = \frac{\sum_{i,j} D(i, j)}{N} \times 100 \% \quad (7)$$

$$UACI = \frac{1}{N} \left[\sum_{i,j} \frac{|C_1(i, j) - C_2(i, j)|}{255} \right] \times 100 \% \quad (8)$$

With respect to *NPCR* and *UACI* estimations for different standard gray scale images, the experimental results in Table I. show that the proposed algorithm is secure against differential attacks and has very low correlation coefficients (r_{xy}) for different standard gray scale encrypted images.

TABLE I. ENCRYPTED WATERMARKED IMAGE SECURITY ANALYSIS

Algorithm		CWPE 2D DWT DCT				CWPE 2D DWT Only			
No Attack		PSNR	NPCR	UACI	r_{xy}	PSNR	NPCR	UACI	r_{xy}
Test Images	Peppers	10.38	99.45	24.51	0.000048	10.40	99.46	24.46	- 0.0051
	Lena	11.82	99.37	20.76	-0.0017	11.87	99.39	20.62	- 0.0037
	Mandrill	12.92	99.35	18.19	0.0017	13.01	99.30	18.01	0.0024
	Pirate	11.40	99.39	21.86	-0.0059	11.45	99.43	21.75	- 0.0016
	Fishing Boat	11.57	99.20	20.27	0.0012	11.63	99.14	19.96	- 0.0018

4. SIGNAL PROCESSING ATTACKS (SPA) ANALYSIS

The proposed secure chaotic watermarking algorithm (*CWPE 2D DWT DCT*) is tested under common signal processing attacks such as Salt & Pepper noise, Gaussian noise, Wiener filter, Median filter, and JPEG compression, Resizing, Rotation and Cropping. Standard grayscale Peppers image (512x512) pixels and the embedded watermark binary image (12x9) pixels are used. The decrypted watermarked Peppers image has PSNR value of 35.07 dB under no signal processing attacks on the other hand the secure chaotic watermarking algorithm (*CWPE 2D DWT*), the decrypted watermarked Peppers image has PSNR value of 30.98 dB under no signal processing attacks. Security analysis for Peppers image under different signal processing attacks is shown in table II. Table II demonstrates the security strength of the encrypted watermarked image is still high under different signal processing attacks.

Table III-V show the quality of the extracted watermark image after the different signal processing attacks using the PSNR measure (measured between the original watermark and the extracted watermark) and the Normalized Cross Correlation (NCC) measure is given by:

$$NCC = \frac{\sum_i \sum_j w(i, j)w'(i, j)}{\sum_i \sum_j [w(i, j)]^2} \tag{9}$$

$$PSNR = 10 \cdot \log_{10} \frac{225^2 \cdot (M \cdot N)^2}{\sum_{i=1}^M \sum_{j=1}^N ((w(i, j) - w'(i, j))^2)} \tag{10}$$

Where, $w(i, j)$ is the original watermark pixel value $w'(i, j)$ is the extracted watermark pixel value and $M.N$ is the image size [8].

TABLES 2. ENCRYPTED WATERMARKED IMAGE SPA

Algorithm		CWPE 2D DWT DCT				CWPE 2D DWT Only					
Attack Style		PSNR	NPCR	UACI	r_{xy}	PSNR	NPCR	UACI	r_{xy}		
Noise	S&P	10.19	99.45	25.02	0.000085	10.21	99.47	24.97	-0.0041		
	Speckle	10.15	99.48	25.16	0.000054	10.61	99.48	25.15	-0.0056		
	Gaussian	9.70	99.54	26.55	0.000036	9.71	99.53	26.54	-0.0041		
Filtering	Winner	S&P	[3 3]	11.87	99.43	20.81	0.000082	11.57	99.44	21.51	-0.0040
			[5 5]	12.62	99.42	19.34	0.0079	12.44	99.44	19.71	-0.0050
			[3 3]	11.87	99.42	20.80	0.0061	11.57	99.47	21.51	-0.0042
			[5 5]	12.61	99.44	19.37	0.0018	12.45	99.43	19.67	-0.0066
			[3 3]	11.74	99.38	21.02	0.0080	11.39	99.42	21.89	-0.0031
			[5 5]	12.36	99.39	19.70	0.0070	12.18	99.40	20.15	-0.0031
	Median	S&P	[3 3]	11.77	99.40	20.95	0.0076	11.47	99.45	21.71	0.0001
			[5 5]	12.43	99.43	19.61	0.0068	12.32	99.43	19.90	-0.0063
			[3 3]	12.50	99.46	19.55	0.0014	11.63	99.43	21.35	-0.0067
		Gaussian	[3 3]	13.03	99.47	18.69	0.0027	12.99	99.48	18.76	-0.0133
			[5 5]	10.60	99.47	23.88	0.000037	10.65	99.45	23.76	-0.0052
			[3 3]	10.33	99.49	24.64	-0.000013	10.46	99.46	24.32	-0.0051
Resizing	50%	8.67	99.59	30.75	0.1168	8.67	99.61	30.77	0.1118		
	75%	6.51	99.72	39.78	-0.1111	6.51	99.70	39.73	-0.1142		
JPEG Comp.	10%	11.40	99.42	21.77	-0.0100	11.19	99.45	22.32	-0.0156		
	25%	11.01	99.45	22.59	-0.0396	10.82	99.45	23.13	-0.0432		
Cropping	2°										
	5°										
Rotation	2°										
	5°										

TABLE 3. NOISE EFFECTS

Algorithm	CWPE 2D DWT DCT			CWPE 2D DWT Only		
	Noise (Intensity =0.02)					
Attack	S&P	Speckle	Gaussian	S&P	Speckle	Gaussian
Extracted Watermark						
PSNR	68.46	Inf	63.69	Inf	Inf	Inf
NCC	0.9932	1	0.9795	1	1	1

TABLE 4. WINNER FILTERING EFFECTS

Algorithm	CWPE 2D DWT DCT		CWPE 2D DWT Only	
	S&P	Gaussian	S&P	Gaussian
Winner Filtering	[3 3], 0.02	[3 3], 0.02	[3 3], 0.02	[3 3], 0.02
Extracted Watermark				
PSNR	Inf	63.69	Inf	65.45
NCC	1	0.9795	1	0.9863

TABLE 5. MEDIAN FILTERING EFFECTS





Algorithm	CWPE 2D DWT DCT		CWPE 2D DWT Only	
	S&P	Gaussian	S&P	Gaussian
Median Filtering	[3 3], 0.02	[3 3], 0.02	[3 3], 0.02	[3 3], 0.02
Extracted Watermark				
PSNR	63.69	63.69	55.45	55.91
NCC	0.9796	0.9798	0.8547	0.8704

TABLE 6. RESIZING & JPEG COMPRESSION EFFECTS

















Algorithm	CWPE 2D DWT DCT				CWPE 2D DWT Only			
	Resizing & JPEG Compression							
	Resizing		JPEG Compression		Resizing		JPEG Compression	
Attack	50%	75%	10%	25%	50%	75%	10%	25%
Extracted Watermark								
PSNR	Inf	60.86	Inf	Inf	Inf	54.31	57.67	62.44
NCC	1	0.9587	1	1	1	0.8077	0.9154	0.9725

TABLE 7. CROPPING & ROTATION EFFECTS

Algorithm	CWPE 2D DWT DCT				CWPE 2D DWT Only			
	Cropping %		Rotation °		Cropping %		Rotation °	
	25%	50%	2°	5°	25%	50%	2°	5°
Extracted Watermark								
PSNR	Inf	Inf	65.45	59.43	Inf	Inf	Inf	Inf
NCC	1	1	0.9864	0.9452	1	1	1	1

5. CONCLUSIONS

In this paper, a new Commutative Watermarking and Partial Encryption (CWPE) algorithm based on mixed single level two dimension transform domain (1L 2D DWT-DCT) and Multi-Map Orbit Hopping Chaotic System (MMOH-CS) is proposed and compared with PEW scheme using single level two dimension DWT (PEW 1L 2D DWT) and Multi-Map Orbit Hopping Chaotic System (MMOH-CS). In the proposed algorithm, the horizontal coefficients sub-band decomposition is only encrypted so; it is able to reduce the encryption to one quarter of the image information. Divided the approximation encrypted coefficients into non-overlapping (8x8) blocks, apply DCT to each block and extract the middle frequencies, Comparison based threshold of the extracted DCT mid-band coefficients, finally, watermark bits are embedded in the coefficients of the corresponding DCT middle frequencies. The proposed system is tested under different signal processing attacks. Security analysis for the proposed system is also performed and presented. Simulated results confirmed the robustness of the proposed system against common signal processing attacks especially median filtering and JPEG compression. Also the proposed algorithm has been securely analyzed using various security measures. The proposed algorithm provides a high security levels for real time application.

REFERENCES

- [1] Mohamed S. El-Mahallawy, Esam A. Hagra, Ahmed Zein Eldin, Mohamed Waleed Fakhr, " Robust Blind and Secure Biometric Watermarking Based on Partial Multi-Map Chaotic Encryption", 4th IFIP International Conference on New Technologies, Mobility and Security (NTMS), 7-14 Feb., 2011, Paris, France, 2011.
- [2] Shiguo Lian, Multimedia content Encryption, CRC Press, Taylor & Francis Group, 2009.
- [3] S. Lian, Z. Liu, Z. Ren, and H. Wang, "Commutative watermarking and encryption for media data," International Journal of Optical Engineering 45(8): pp. 5101–5103, 2006.
- [4] S. Lian, Z. Liu, Z. Ren, and H. Wang, "Commutative encryption and watermarking in compressed video data," IEEE Circuits and Systems for Video Technology 17(6): pp. 774–778, 2007.
- [5] A. J. Ahumada and H. A. Peterson, "Luminance- model-based DCT quantization for color image compression," Proc.SPIE:Human Vision, Visual Processing, and Digital Display III (SPIE'92), SPIE press, Aug.1992, pp.365-374, doi:10.1117/12.135982.
- [6] C. J. Zhang and M. Y. Fu, "Infrared Image De-noising Based on Discrete Stationary Wavelet Transform," Optical technique, vol. 29, Feb.2003, pp. 250-256.
- [7] N. Li, X. S. Zheng, Y.I. Zhao, H.M. Wu and S.F. Li, "Robust Algorithm of Digital Image Watermarking Based on Discrete Wavelet Transform," Proc. IEEE Symp. Electronic Commerce and Security, IEEE press, Aug. 2008, pp.942-945, doi: 10.1109/ISECS.2008.140.
- [8] J. X.. Liu and Z. M. Lu. "DWT and DCT Combined Robust Watermarking Algorithm Based on Vector Quantization with Labeled Codewords," Proc. IEEE Conf, Anti-counterfeiting, Security, and Identification in Communication (ASID'08), IEEE press, Nov. 2008, pp.51- 54, doi: 10.1109/IWASID.2008.4688335.
- [9] J. Liu, F. Gao and H. Zhang, "A Blind Watermark Algorithm in Mixed Transform Domain Based on Chaotic Sequence Locating," Proc. IEEE Conf. Innovative Computing Information and Control(ICICIC'08), IEEE press, Jun. 2008, pp.23-27, doi: 10.1109/ICICIC.2008.9.
- [10] A. F. Hu and N. Chen, "A Blind Watermarking Algorithm for Color Image Based on Wavelet Transform and Fourier Transform," Proc.IEEE Conf, Young Computer Scientists(ICYCS'08), IEEE press, Jun.2008, pp.1453 -1458, doi: 10.1109/ICYCS.2008.100.
- [11] J. F. Delaigle, C. De Vleeschouwer and B. Macq, "Watermarking algorithm based on a human visual model", Signal Processing, vol. 66, May 1998, pp.319-335, doi: 10.1016/S0165-1684(98)00013-9.
- [12] Y. Z. Li, H. Zhu, R. Q. Yu, G. Yang, and J. Xu, "An Adaptive Blind Watermarking Algorithm Based on DCT and Modified Watson's Visual Model," Proc. IEEE Symp. Electronic Commerce and Security, IEEE Press, Aug. 2008, pp.904- 907, doi: 10.1109/ISECS.2008.83.
- [13] X. F. Zhao, "Digital image scrambling based on baker's transformation," Journal of Northwest Normal University (Nature science), Northwest Normal University, 2003, pp. 26-29.
- [14] I. J. Cox, J. Kilian, F. T. Leighton and T. Shamoan, "Secure spread spectrum watermarking for multimedia," IEEE Trans. Image processing, vol. 6, Dec. 1997, pp.1673-1687, doi: 10.1109/83.650120.
- [15] S. Voloshynovskiy, S. Pereira, V. Iquise and T. Pun, "Attack Modelling: Towards a second generation watermarking benchmark," Signal Processing, Special Issue on Information Theoretic Issues in Digital Watermarking, vol. 81, Elsevier, Jun. 2001, pp.1177-1214, doi: 10.1016/S0165-1684(01)00039-1.
- [16] K. Janthawongwilai and T. Amornraksa, "Improved Performance of Amplitude Modulation Based Digital Watermarking," Proc. IEEE Symp. International Symposium Communications and Information Technology(ISCIT'04), IEEE press, Oct. 2004, pp.318-323, doi: 10.1109/ISCIT.2004.1412861.
- [17] M. W. Zhao and Y. Z. Dang, "Color Image Copyright Protection Digital Watermarking Algorithm Based on DWT&DCT," Proc.IEEE Conf, Wireless Communications, Networking and Mobile Computing (WiCOM'08), IEEE press, Oct. 2008, pp.1-4, doi: 10.1109/WiCom.2008.2913.
- [18] Said E. El-Khamy, M. A. El-Nasr, and Amina H. El-Zein, "A Partial image encryption scheme based on ELKINZ chaotic stream cipher," MASAUM Journal of basic and applied sciences, Vol. 1, No. 3, pp. 389-394,October 2009.

- [19] TianKai Sun, XiaoGen Shao, XingYuan Wang, "A Novel Binary Image Digital Watermarking Algorithm Based on DWT and Chaotic Encryption," The 9th International Conference for Young Computer Scientists, pp 2797-2802, 2008.
- [20] Ke Lue, Xiaolin Tian, "A New Robust Watermarking Scheme based on Wavelet Transform," Congress on Image Processing vol 2 .pp. 312-316, 2008.
- [21] Khalil Zebbiche, Lahouari Ghouti, Fouad Khelifi and Ahmed Bouridane, "Protecting Fingerprint Data using Watermarking," Proceedings of the First NASA/ESA Conference on Adaptive Hardware and Systems (AHS'06) 4/06, 2006.
- [22] Sun J., Takeshita O., "Interleavers for Turbo Codes Using Permutation Polynomial Over Integers Rings" IEEE Transactions on Information Theory, vol.51, no.1, pp. 101-119, 2005.
- [23] W. Stallings, Cryptography and network security, Prentice Hall, New Jersey, 2006.

Esam A. A. HAGRAS received the B.S. degrees in Electrical Engineering from faculty of engineering, Alexandria Univ., Egypt, in 1994, M.S. degrees in Electrical Engineering from Mansoura Univ., Egypt, in 2001, respectively. During 2005-2007, he was on in Dept., of Electrical Engineering, faculty of engineering, Alexandria Univ. In Dec. 2007, he gets the PhD degree in information security in communications. His research interests in the field of information and multimedia security, chaotic cryptography, Hardware implementation of encryption algorithms on FPGA ,data compression, digital image watermarking, communication and wireless sensor network security. He has published more than ten papers on security and communications.



Mohamed S. El-Mahallawy finished his Ph.D. at the Cairo University, Egypt, 2008 in the field of image processing and pattern recognition. Dr. El-Mahallawy finished his BSc and Msc. at the Electronics and Communications Department, Faculty of Engineering, Arab Academy for Science and Technology and Maritime Transport, Egypt, at 1998, 2002, respectively, in the field of speech processing. Dr. El-Mahallawy is now an Assistant Professor at Electronics and Communications Department, Faculty of Engineering, Arab Academy for Science and Technology and Maritime Transport, Egypt. He interests in the field of pattern recognition signal processing, digital watermarking.



Ahmed A. A. Zein He is born in Mansoura at 1976 and received the B.S. degrees in Electrical Engineering from faculty of engineering, Alexandria Univ., Egypt, in 1994. During 2008-2010, he was on in Dept., Electronics and Communications Department, faculty of engineering, Arab Academy for Science and Technology and Maritime Transport, Egypt,. His research interests in the field of information and multimedia security, chaotic cryptography, data compression, digital image watermarking.



Mohamed Waleed Fakhr finished his Ph.D. at the Waterloo univ., Canada, 1993 in the field of neural networks and pattern recognition. Dr. Waleed joined NORTEL, Montreal research lab from 1994-1999, where he was working in the field of speech recognition, where he had 2 patents with NORTEL. Dr. Waleed has joined the Arab academy for science and technology (AAST) since 1999, where he is conducting research in the areas of pattern recognition, signal processing, digital watermarking and time series forecasting.

