Multimedia Content protection Based on Commutative Watermarking and Cryptographic Technique

B. Rajesh kumar, CH. Sai Murali

Abstract: Watermarking embeds information into a digital signal like images. Watermarking Technologies are being regarded as a vital mean to proffer copyright protection of digital signals. The effectiveness of watermarking and Encryption technique is indicated by the robustness of embedded watermarks against various attacks such as, Rotation, Resizing, etc. In this paper, a novel Commutative Watermarking and Partial Encryption technique using single level 2-Dimension Discrete Wavelet Transform and Multi-Map Orbit Hopping Chaotic System is proposed. In proposed system, the low-low sub-band decomposition is only encrypted. So, it is able to reduce the encryption to one quarter of the image information and the watermark image is embedded into the selected high sub-1bands. The results of the security analysis shows that the proposed algorithm provides a high security level for real time application.

Keywords: Chaos; Partial Encryption; Watermarking; DWT.

I. 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 [1]. Watermarking process embeds copyright information into media content by modifying the media pixels slightly. The embedded information can be detected or extracted from media content and used to verify the ownership. 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 [2, 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]. For the encrypted part to be independent of the watermarked part, the properties of the encryption algorithm and the watermarking algorithm are kept unchanged. However, the disadvantage is that only a part of the media data is encrypted, which causes some loss in security.There are two basic schemes to encrypt or watermarking digital images, in spatial domain or in transform domain. Since wavelet based compression appeared and was adopted in the JPEG2000 standard, suggestions for image encryption and watermarking techniques based in the wavelet domain have been numerous. However, many of these are not secure as they are based solely on random permutations making them susceptible to various attacks [4-6].

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. The characteristics of the chaotic maps have attracted the attention of cryptographers to develop new encryption algorithms with higher security and speed. 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 [7].

Hence, in this paper a new Commutative Watermarking and Partial Encryption (CWPE) algorithm based on Watermarking and Partial Encryption (WPE) algorithm using single level two Dimension Discrete Wavelet Transform (2D DWT) and Multi-Map Orbit Hopping Chaotic Encryption (MMOH-CE) is proposed. In the proposed algorithm, the watermark image is embedded into the selected high pass sub-bands using CDMA Spread Spectrum technique, and then each wavelet sub-band is scrambled with its own Arnold map. Finally, the low-low sub-band is then encrypted using a chaotic scrambled random number pattern which is generated using scrambled multi-chaotic logistic maps.

The proposed system is tested under different signal processing attacks. Security analysis for the proposed system is also performed and presented.

II. PROPOSED COMMUTATIVE PARTIAL ENCRYPTION AND WATERMARKING 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

Revised Manuscript Received on 30 August 2012
*****Correspondence Author(s)

B. Rajesh kumar*, PG Student, (M.Tech), Department of CSE. ASCET, Gudur, India
CH. Sai Murali, Asst. Professor, Department of CSE. ASCET, Gudur, India.

the Secure Key Management (SKM) subsystem. SKM subsystem generates both the control parameters needed for the chaotic scrambling parameters generator and the initial conditions needed for the multi-map orbit hopping chaotic subsystem.The second processing stage is concerned with the watermark embedding and the partial encryption processes. The block diagram of the proposed algorithm is shown in Fig.1.

A. Preprocessing Stage

The CWPE 2D DWT Pre-processing Stage consists of Secure Key Management (SKM) subsystem, Chaotic Scrambling Parameter generator subsystem and Multi-Map Orbit Hopping Chaotic Subsystem (MMOH-CS).

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 (θ), 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 (25×3×9 = 675 bits) [8].

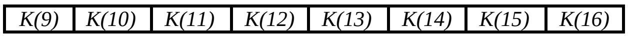
The minutiae data (675-bits) are concatenated with the secret key (256-bits) and interleaved using random interleaver. The output is hashed using SHA-256 to satisfy the diffusion and confusion properties [9]. The ideal diffusion effect for hash value in binary format should be that: any tiny changes 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 x 8) are used to produce the chaotic maps initial conditions for the Multi Map Orbit Hopping Chaotic Subsystem. The last eight sub-keys (64-bits length; 8 x 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.

2) Chaotic Scrambling Parameters Generator Subsystem:

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

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

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.



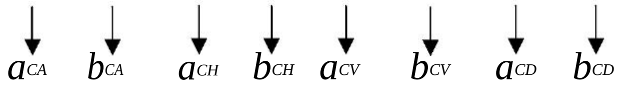


Figure 3. Arnold Cat Maps parameter generation process

3) Multi-Map Orbit Hopping Chaotic Subsystem: 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:

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

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.

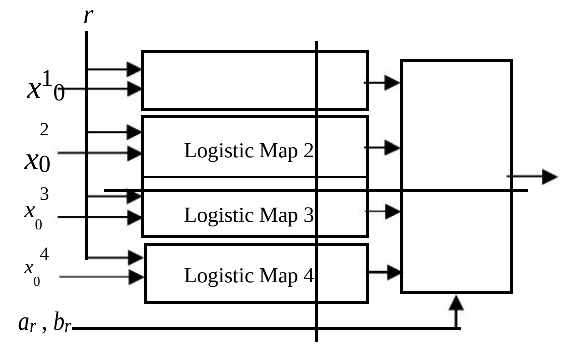


Figure 4. Multi-Map Orbit Hopping Chaotic Subsystem

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 by10^{-7} .

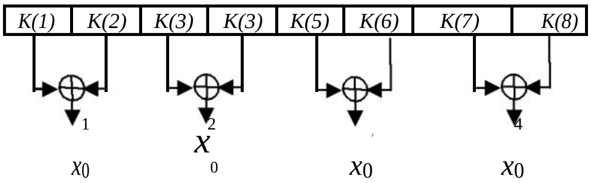


Figure 5. Logistic Maps initial condition generation process

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.

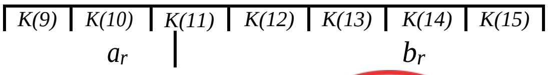


Figure 6. Arnold Cat Map Parameters generation process

B. Processing Stage

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

1) *Watermark Embedding and PMMCE process:*

- □ Apply DWT to the cover image and computes the approximation coefficient matrix CA and details coefficients matrices CH, CV, and CD (horizontal, vertical, and diagonal).
- □ Set the embedding strength factor *k* .
- □ Add PN sequence to CH and CV components based on watermark bit value.
- □ 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 low-low sub-band only.

2) *Watermark extraction Process and decryption:*

- □ Apply de-scrambling and partial decryption scheme.
- □ Find correlation in CH and CV components of the watermarked image.
- □ Compare the correlation with mean correlation.
- □ Revert back the watermark image.

III. SECURITY ANALYSIS

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

A. 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 as follows:

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

The 1L 2D DWT encrypted Lena based on the user secret key and the biometric key is shown in Fig. 7.

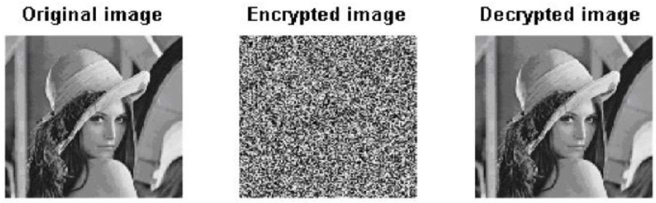


Figure 7. 1L 2D DWT-based enecrypted and decrypted Lena

B. 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:

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

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

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

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

$$D(x) = \frac{1}{N}\sum(x_i - E(x))^2 \qquad (6)$$

Table I shows the very low correlation coefficients (r_{xy}) for different standard gray scale encrypted images.

TABLE I. ENCRYPTED WATERMARKED IMAGE SECURITY ANALYSIS

	No Attack	PSNR	NPCR	UACI	r_{xy}
Test Images	*Lena*	*11.49*	*99.37*	*20.45*	-0.0030
	Pirate	*11.50*	*99.39*	*21.62*	-0.0019
	Mandrill	*13.02*	*99.26*	*17.98*	0.0032
	Peppers	*10.44*	*99.47*	*24.35*	-0.0046
	Fishing Boat	*11.68*	*99.13*	*19.79*	-0.0019

C. 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:

$$\sum^{N} D(i, j) \qquad (7)$$

Published By:
Blue Eyes Intelligence Engineering
and Sciences Publication (BEIESP)
© Copyright: All rights reserved.

$$NPCR = \frac{{}_{i,j}}{N} \cdot 100\ \%$$

$$UACI = \frac{1}{N} \sum_{i,\ j}^{N} \frac{|C_1(i,j) - C_2(i,j)|}{255} \cdot 100\ \% \qquad (8)$$

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.

D) Key sensitivity test.

In order to demonstrate the sensitivity of the proposed algorithm to the cipher keys, a typical key sensitivity test has been performed by modifying the least significant bit (case-1), the middle significant bit (case-2), and the most significant bit (case-3), of the secret key used.

It is not easy to compare the encrypted images visually. Hence, the correlation and the NPCR between the corresponding pixels of the mentioned three cases are calculated. The Correlations values of single level 2D DWT in the three cases using Lena image (512x512) embedded with binary image watermark (12x9) are 0.0027, 0.0031 and 0.0035 respectively. Also, The NPCR values of single level 2D DWT for the three cases of Lena image (size 512x512) embedded with binary image watermark (size of 12x9) are 99.64, 99.57 and 99.51 respectively. It is obvious that when a key is used to encrypt an image while another trivially modified key is used to decrypt the ciphered image, the decryption also completely fails.

IV. SIGNAL PROCESSING ATTACKS ANALYSIS

The proposed secure chaotic watermarking algorithm is tested under common signal processing attacks such as Salt & Pepper noise, Gaussian noise, Wiener filter, JPEG compression, Resizing and Cropping. Standard grayscale Lena image (512x512) pixels and the embedded watermark binary image (12x9) pixels are used. The decrypted watermarked Lena image has PSNR value of 30.98 dB under no signal processing attacks.

Security analysis for Lena 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 II. ENCRYPTED WATERMARKED IMAGE SIGNAL PROCESSING ANALYSIS

Attack Style			PSNR	NPCR	UACI	r_{xy}
Noise	Salt & Pepper	Noise = Intensity0.02	11.66	99.39	21.05	-0.0025
	Speckle		11.59	99.40	21.28	-0.0039
	Gaussian		17.10	99.46	23.19	-0.0020
Wiener Filtering [3 3]			13.25	99.32	17.65	-0.0033
Resizing		50%	13.95	99.24	16.37	-0.0056
		75%	13.32	99.31	17.50	-0.0051
JPEG Compression		10%	12.21	99.37	19.75	-0.0022
		25%	12.00	99.38	20.29	-0.0030
Cropping		25%	9.12	99.52	27.99	-0.0207
		50%	7.21	99.68	36.54	-0.1279
Rotation		10°	11.94	99.39	20.11	0.0215
		20°	11.35	99.37	21.42	0.0438

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,

$$NCC = \frac{\sum_i \sum_j w(\mathrm{i},\mathrm{j})w'(i,j)}{\sum_{ij} \sum [w(i,j)]^2} \qquad (9)$$

where, $w(i,j)$ is the original watermark pixel and $w'(i,j)$ is the extracted watermark pixel [8].

V. CONCLUSIONS

In this paper, a new DWT-based commutative watermarking and encryption algorithm based on partial encryption and multi-map orbit hopping chaotic system is proposed. The multi-chaotic logistic maps used ‘‘Arnold map" to generate hopping pattern of random numbers used in the encryption process. In the proposed algorithm, the low-low sub-band decomposition is only encrypted. So, it is able to reduce the encryption to one quarter of the image information and the watermark image is embedded into the selected high sub -1bands. Experimental results confirmed the robustness of the proposed system against common signal processing attacks. 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. Shiguo Lian, Multimedia content Encryption, CRC Press, Taylor & Francis Group, 2009.
2. 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.
3. 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.
4. 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.
5. Ke Lue, Xiaolin Tian, “A New Robust Watermarking Scheme based on Wavelet Transform,” Congress on Image Processing vol 2 .pp. 312-316, 2008.
6. P.Ramman, Munage.V.N.K.Prasad, D.Sreenivasa Rao, 2'Robust Digital Watermarking of Images using Wavelets,” International Journal of Computer and Electrical Engineering, Vol.1, No.2, pp. 111-116, June 2009.
7. 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.
8. 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.
9. W. Stallings, *Cryptography and network security*, Prentice Hall, New Jersey, 2006.
10. Howard Chi Ho Cheng, Partial encryption for image and video communication, Master’s thesis, Department of Computing Science, University of Alberta, Edmonton, Alberta, Canada, 1998.