Watermarking schemebased on Multiple Chaotic Maps

JilaAyubi
University ofSistan and Baluchestan,Zahedan,Iran
jila.ayubi@mail.usb.ac.ir

FarahnazMohanna
University of Sistan and Baluchestan, Zahedan, Iran
f_mohanna@ece.usb.ac.ir

ShahramMohanna
University of Sistan and Baluchestan, Zahedan, Iran
mohana@ece.usb.ac.ir

MehdiRezaei
University Of Sistan and Baluchestan,Zahedan,Iran
mehdi.rezaei@ece.usb.ac.ir

***Abstract*—a watermarking scheme for Grayscale image is proposed based on a family of the chaotic maps and discrete cosine transform. Jacobian Elliptic mapis employed to encrypt of watermarked logo. Piecewise nonlinear chaotic map is also used to determine the location of DCT coefficients for the watermark embedding. The purpose of this algorithm is to improve the shortcoming of watermarking such as small key space and low security. Therefore the size of key space for initial conditions and control parameters is computed about $2^{425}(10^{128})$ and this key space is large enough to resist the attacks. Toevaluate the robustness and effectiveness of proposed method, several attacks are applied to the watermarked image and the best results have been reported.**

***Keywords*-Blind Digital Image Watermarking, Chaos, Discrete Cosine Transform, Multiple Chaotic Maps, JacobianEliptic Map, Piecewise nonlinear chaotic Map**

I. INTRODUCTION

Watermarking technique can be used for protection of multimedia information, content authentication, and so on [1]. Digital Watermarking techniques can be broadly classified into two categories: Spatial [2] and Transform [3] domain methods. These types of watermark generation schemes require initial value and the function seed to recreate the same watermark at a later stage[4]. One of the advantages of these Watermarking methods is the possibility to analyze and control their spectral properties [5]. In most spatial domain schemes, watermark signal is embedded in the LSB (least significant bit) of the pixels in host image in which the robustness against attacks is weak i.e. watermark can be detected easily [6]. Wavelet transform is widely used for digital watermarking, where one of the most well-known methods is Cox's watermark embedding scheme [7].The discrete cosine transform (DCT) is a technique for converting a signal into elementaryfrequency components which was used first time in 1974 [8]. It is widely used in image compression[9].The DCT has special property that most of the visually significant information of the image is concentrated in just a few coefficients of the DCT. It's referred as 'Energy compaction Property' [10].The DCT coefficients can be quantized using visually-weighted quantization values.

Two main requirements for an acceptable watermarking technique are imperceptibility[11] and robustness[12]. Imperceptibility refers to perceptual quality of the data being protected. Robust watermarking embeds information data within the image with an insensible form for human visual system, but in a way that protects from attacks such as common image processing operations.

In authentication watermarking, tamper localization and detection accuracy are two issues performances. However, most of presented methods in the studied literature cannot obtain precise localization. A watermark typically contains information about origin, status, and/or destination of the host data [13], [14].Image scrambling is one of the most prevailing encryption algorithms these years [15], [16], [17]. However, these methods are not so many. The majority of watermarking schemes proposed to date, use watermarks generated from pseudo random number sequences [18].

The first Chaotic system has been discovered by Edward Lorenz in 1963[19]. Other chaotic systemshave been established by many different research areas, such as physics, mathematics, and engineering. The idea of using chaotic signals in different layers of communication systems attracted the attention of researchers [20-25].

This paper chiefly focuses on the application of piecewise nonlinear chaotic map[26] and jacobian elliptic [27] in encryptiontechniques of watermark logo. Piecewise nonlinear chaos and jacobian elliptic chaos began as an attempt to find chaos in the sense of extreme sensitivity to changes in initial conditions.Chaotic functions such as Markov Maps, Bernoulli Maps, Skew Tent Map, and Logistic Map have been widely used to generate watermark sequences [28], [29].

In our previous work, we used the chaos coupled maps and DWT for blind digital watermarking [30]. In that paper the chaotic maps are employed to improve the security of a watermarked image, and an improved mutation operator has been used to encrypt the watermark logo. The upgraded mapping method determines the location of DWT coefficients where the watermark is embedded.

In this paper multiple chaotic maps are employed to enhance of security and the best extraction, and these maps are also used to determine the location of DCT coefficients for the watermark embedding. We also use XOR operator to encrypt the watermark logo.

This paper is organized as; section II describes chaotic maps for scrambling process, and section III presents a Discrete Cosine Transform.The details of watermark embedding and extraction are presented in section IV. Some simulation results are discussed in Section V and the papper is concluded in Section IV.

II. APPLIEDCHAOTIC MAPS

A. Jacobian Elliptic Maps

One-parameter families of jacobian elliptic rational maps[31] of the interval [0,1] with an invariant measure can bedefined as:

$$X_{N+1}=\frac{4\alpha^2 x(1-k^2X_N)(1-X_N)}{(1-k^2X^2{}_n)^2+4(\alpha^2-1)X_N\ (1-k^2X_N)(1-X_N)} \quad (1)$$

Where $X_0 \in [0,1], \alpha \in [0,4], k \in [0,1]$, k (modulus)represents the parameter of the elliptic functions. The3D bifurcationbehavior of System is shown in Fig.1 (a). Fig.2 (a) showsthe pseudo-random generation in 5000 iterations by Eq.(1) andhistogramof the pseudo-random values is shown in Fig.2(b).

Jacobianeliptic map is used in this paper as follow:

$$CX^1_{N+1} = \begin{cases} 0 & X_{N+1} \leq 0.5 \\ 1 & X_{N+1} > 0 \end{cases} \quad (2)$$

B. Piecewise nonlinear chaotic Map

We rest present a brief review of one-parameter families of piecewise nonlinear chaotic maps with an invariant measure. These maps can be defined as:

$$X_{n+1} = \frac{\alpha^2 F}{1+(\alpha^2-1)F} \quad (3)$$

Where

$$F = \begin{cases} \dfrac{X_n}{P} & 0 \leq X \leq P \\ \dfrac{X_n - P}{1-P} & P < X \leq 1 \end{cases} \quad (4)$$

Then, the probability parameter of the piecewise nonlinear chaotic maps p is generated by using the results of iteration of the trigonometric map can be defined as:

$$Y_{n+1} = \frac{1}{\beta^2}\tan^2(N \times \arctan(\sqrt{X_n}) \quad (5)$$

Therefore

$$P = \begin{cases} Y_{n+1} & 0 \leq Y_{n+1} \leq 1 \\ \dfrac{1}{Y_{n+1}} & Y_{n+1} > 1 \end{cases} \quad (6)$$

Where $X_0 \in [0,1], \alpha \in [0,4],\ \beta \in [0,4], Y_0 \in [0,1],\ b \in [1,4]\ and\ P \in [0,4]$.

The 3D bifurcation behavior of System is shown in Fig.1 (b).Fig.2(c) shows the pseudo-random generation in 5000iterations by Eq. (3) and histogram of the pseudo-randomvalues is shown in Fig.2 (d).

This map is used for embedding and extraction process asfollow:

$$\begin{cases} CX^2_{N+1} = (X_{N+1} \times 10^{14})\ mod\ M \\ CY^2_{N+1} = (Y_{N+1} \times 10^{14})\ mod\ N \end{cases} \quad (7)$$

C. Eliptic map for watermark logo encryption

The watermark logo encryption proposed in this paper consists of the following major steps:

- The plain logo $W_{m\times n}$is transformed into a one-dimensionalarray $W_{(m\times n)\times 1}$.
- The secret keys, including initial conditions and controlparameters are set, and chaotic map in Eq.(2) are iterated500 times.
- Ciphered values is computed by:

$$C_i = (Cx^1_i\ XOR\ W_i)$$

(Where $C_i$is one dimensional array considered for storing the ciphered value).

- When all the pixels were encrypted, the matrix $C_{(m\times n)\times 1}$ is transformed into $C_{m\times n}$and cipher watermark logo isexported to next step of watermarking algorithm.
- Process of decryption is very similar to the encryption process.Just steps mentioned in the encryption process are repeated.

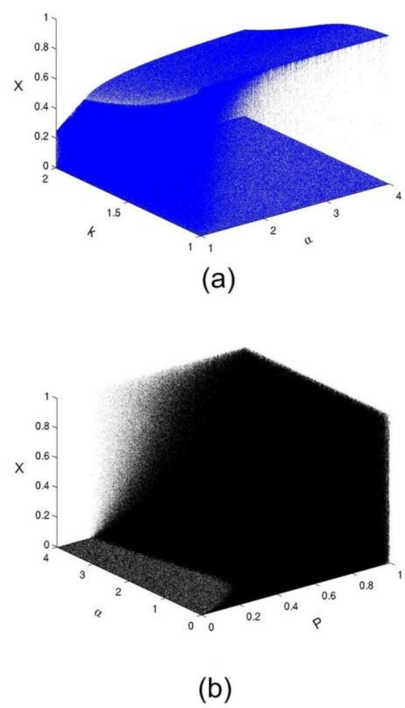


Fig.1. Bifurcation of (a) Jacobian eliptic Map (b) Piecewise nonlinear chaotic Map.

D. Selecting Location embedded by Piecewise nonlinear chaotic Map

Using the coordinate $(i\ ,j)$ position of watermark pixel as theinitial condition and through setting a value for the controlparameter in Eq.(7), chaotic map is iterated after which, theembedding position of the pixels from the watermark imageto host image can be obtained. The watermark pixels will getdifferent embedding positions, so, the embedded watermarkpixels will spread on the host image randomly.

I. DISCRETE COSINE TRANSFORM

Define the orthogonal matrix U of order m by

$$\mathrm{U(i,j)} = \begin{cases} \sqrt{\frac{1}{m}} & i = 1 \\ \sqrt{\frac{2}{m}}\cos\left(\frac{\pi(2j-1)(i-1)}{2m}\right) & 2 \le i \le m \end{cases} \quad (8)$$

The orthogonal matrix V of order n is defined similarly with m replacing n in (8). The discrete cosine transform (DCT) of an image matrix A is defined by

$$X = UAV^T \quad (9)$$

And the inverse discrete cosine transform (IDCT) of X is defined by

$$A = U^T XV \quad (10)$$

In the proposed method, Watermark Logo is inserted in themiddle coefficients. Fig. 3 shows the insertion area.

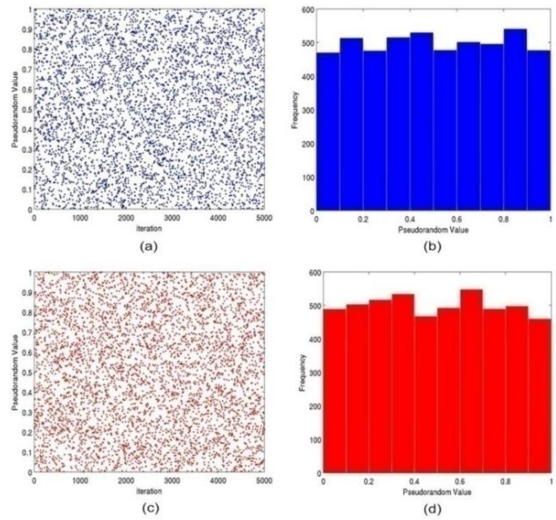
II. WATERMARK EMBEDDING AND EXTRACTION

Block diagram of proposed embedding and extraction processare shown in Fig.(4).

A. Watermark embedding

Theembedding process proposed in this paper consists of thefollowing major parts:

- Encryption process is applied to input watermark logo.
- Original image using 2D discrete Cosine transform are decomposed into coefficients as Fig. 3.
- In this step, embedding location of watermark logo is obtained by Eq. (2).



- **Figure 2. (a) The pseudo-random generation in 5000 iterations by Eq. (1) (b) Histogram of the pseudo-random values for 5000 iterations by Eq. (1) (c) The pseudo-random generation in 5000 iterations by Eq. (3) (d) Histogram of the pseudo-random values for 5000 iterations by Eq. (3)**
-

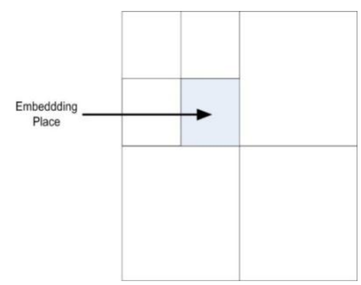


Fig.2. Embedding location in DCT coefficients

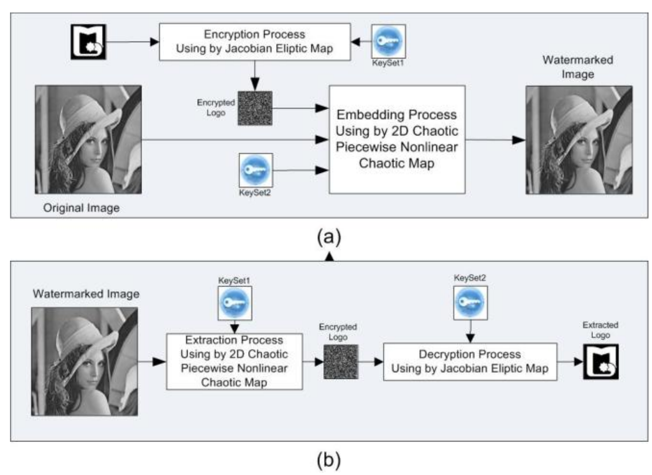


Fig.3. Block Diagram of (a) embedding process (b) extraction process

- Neighborhoods of central coefficient are determined (See Fig.5).In this paper, neighborhood type in Fig.5 (a) is usedin embedding and extraction process.
- Calculate Minimum and maximum of coefficients inFig.5. (a) and store in MAX,MINvariables.
- If pixel value of watermark logo equal to 1 , central coefficient is replaced by $MAX + t$, else pixel value of watermark logo equal to 0 ,central coefficient is replaced by $MIN - t$(t is threshold value).
- When all pixels were embedded into coefficients, 2Dinverse discrete cosine transform is applied and finalwatermarked image is obtained.

Flowchart of embedding process is shown in Fig.6.

B. *Watermark extraction*

Watermark extraction process which is very similar to the embeddingprocess consists of the following majorparts:

- Watermarked image using 2D discrete Cosine transformare decomposed into DCT coefficients.
- Extraction location of watermark logo is obtained byEq.(5).
- Neighborhoods of central coefficient is determined (SeeFig.5.(a)).
- Calculate median of coefficients in Fig.5.(a) and store inMed variable.
- If central coefficient is greater thanMed, watermark pixelvalue is 1 , else watermark pixel value is 0;
- When all pixels were extracted from coefficients, Watermarklogo decryption is applied and final watermark logois obtained.

Flowchart of extraction process is shown in Fig.7.

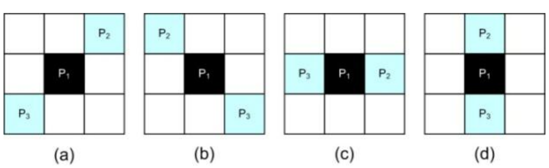


Fig.4. Types of Neighborhood in the DCT Coefficients.

I. EXPERIMENTAL RESULTS

This section will present and discuss the experimental results of our proposed scheme. Digital watermarking techniques must satisfy the following properties.

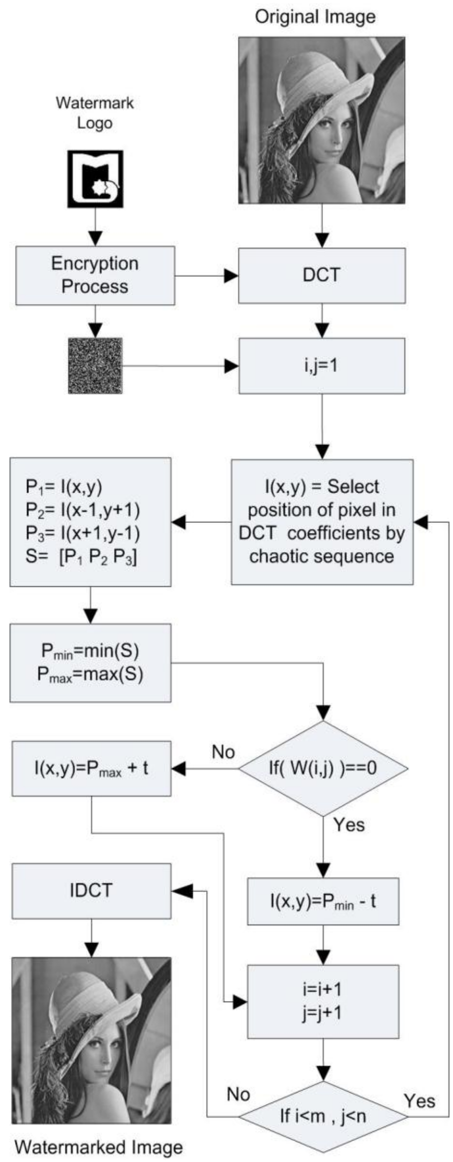


Fig.5. Flowchart of embedding process

A. *Evaluation of the effectiveness*

To demonstrate the effectiveness of the proposed algorithm,MATLAB simulations are performed by using 512×512 pixel gray level "LENA" image and 64 ×64 pixel binary watermark logo "USB". Fig. 5 demonstrates the invisibility of watermark. Figs. 8(a-b) show the original host image and watermark logo, respectively. Figs. 8 (c-e) show the watermarked image, the extracted watermark logo by correct keys and the extracted watermark logo by incorrect keys, respectively. The watermark embedding process is said to be imperceptible if the original data and watermarked data cannot be distinguished.

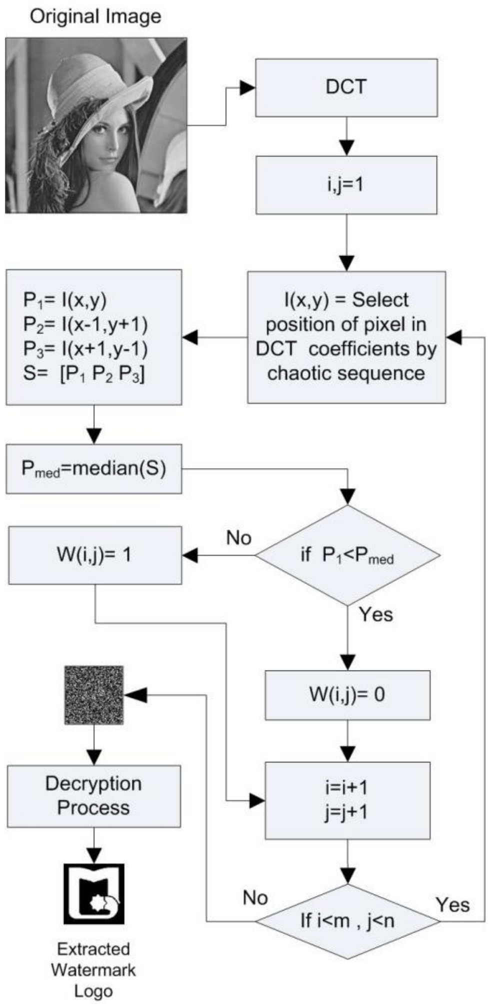


Fig.6. Flowchart of extraction process

To quantitatively evaluate the performance of the proposed scheme, the peak signal-to-noise ratio (PSNR) was adopted to measure the image qualityof a watermarkedimage which is given by:

$$\text{PSNR}=10\times log_{10}\frac{255^2}{MSE}\,(\text{dB}) \qquad (11)$$

According to the definitions in statistics, the mean squared error (MSE) between the original and watermarked images is defined by

$$MSE = \frac{1}{M\times N}\sum_{i=1}^{M}\sum_{j=1}^{N}(H_{i,j} - \acute{H}_{i,j})^2 \qquad (12)$$

Where $H_{i,j}$ and $\acute{H}_{i,j}$ indicate the pixel values in the location (i, j) of the original host image and the watermarked image, respectively, while M ×N is the image size. In this study, reliability was measured as the bit error rate (BER) of extracted watermark through this formula:

$$BER = \frac{B}{M\times N}\times 100 \qquad (13)$$

Where, B is the number of erroneously detected bits, and MN is the extracted watermark image dimensions. The PSNRfor the watermarked image is 40.51 dB, and the BER of theextracted watermark is zero. Therefore, there is no obviousperceptual distortion between watermarked image and original one; the embedded watermark does not degrade the quality of original host image.

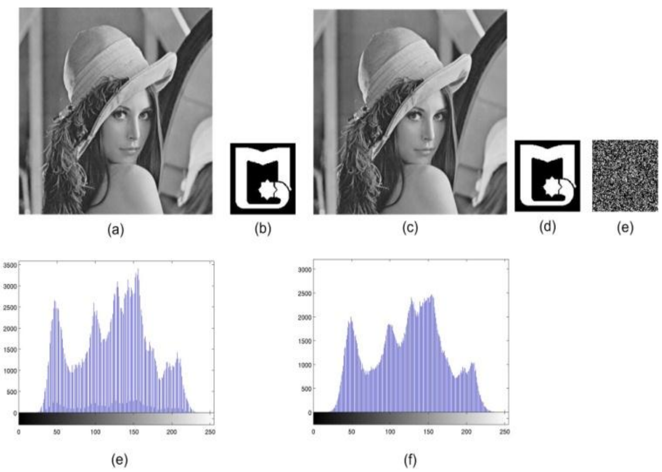


Fig.7. (a) Original Image, (b) Watermark Logo (c) Watermarked Image (d)Extracted Logo by correct password, (e) Extracted Logo by incorrect password (f) Histogram of Original image (g) Histogram of Watermarked image.

B. Robustness to attacks

To test the robustness of our proposed method, we applied several attacks to the watermarked image. In the experiments, both geometric and non geometric attacks are considered. Non geometric attacks include:

- JPEG compression: JPEG is the first international image compression standard for continuous-tone still images both grayscale and color images [32], [33].
- Median filtering: In median filtering the input pixel is replaced by the median of the pixels contained in the neighborhood [34].

Fig.8. Watermarked Image under different attacks : (a) JPEG compression, (b) Salt & pepper noise 10%, (c) Gaussian noise [0,0.01] (d) Histogram Equalization, (e) Median filter [3×3], (f) low-pass filter [5×5], (g) Gamma correction 0.6 (h) motion blur 45^o, (i) Rotation (1^o), (j) Cropping (25%).

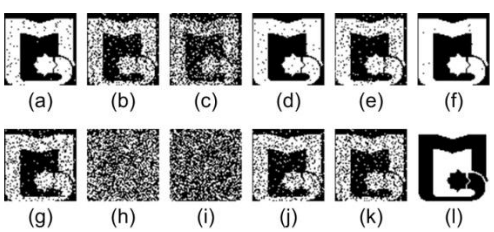


Fig.9. Extracted watermark logo under different attacks (a) JPEG compression, (b) Salt & pepper noise 10%, (c) Gaussian noise [0,0.01] (d) Histogram Equalization, (e) Median filter [3×3], (f) low-pass filter [5×5], (g) Gamma correction 0.6 (h) motion blur 45^o, (i) Rotation (2^o), (j) Cropping (25%).

- Low-pass filtering: Low-pass filtering attenuates the high frequency components in
  the signal and is essentially equivalent to integrating the signal. Low-pass filtering ofan image is a spatial averaging operation. It produces an output image, which is a smooth version of the original image, devoid of the high spatial frequency components that may be present in the image [35].
- Gamma correction: Gamma correction, gamma nonlinearity, gamma encoding, or often simply gamma, is the name of a nonlinear operation used to code and decode luminance or tristimulus values in video or still image systems.
- Blurring: Blurring is used in preprocessing steps, such as removal of small details from an image prior to (large) object extraction, and bridging of small gaps in lines or curves. Noise reduction can be accomplished by blurring with a linear filter and also by nonlinear filtering [35].
- Sharpening: The principal objective of sharpening is to highlight fine detail in an image or to enhance detail that has been blurred, either in error or as a natural effect of a particular method of image acquisition.
- Histogram equalization: Histogram equalization is a technique which consists of adjusting the gray scale of the image so that the gray level histogram of the input image is mapped onto a uniform histogram [35], [36], [37].

And the geometric attacks include:

- Rotation: Rotation of an input image about an arbitrary pivot point can be accomplished by translating the origin of the image to thepivot point, performing the rotation, and then translating back by the first translation offset [35].
- Gaussian noise: Gaussian noise is a statistical noise that has a probability density function of the normal distribution. In other words, the values that the noise can take are Gaussian-distributed. It is most commonly used as additive white noise to yield additive white Gaussian noise [35], [36], [37].
- Salt &Pepper noise: Salt and pepper noise is a form of noise typically seen on images. It represents itself as randomly occurring white and black pixels [35], [36], [37].
- Cropping: Cropping refers to the removal of the outer parts of an image to improve framing, accentuate subject matter or change aspect ratio [38], [39], [40].

Fig. 9 showsan example of a watermarked image, LENA, which is attacked by the listed attacks. The corresponding best extracted watermarks are shown in Fig. 10. The test results for “LENA” image are shown in Table 1 and Table 2.

C. Key Space

The key is the fundamental aspect of every cryptosystem. An algorithm is as secure as its key. No matter how strong and well designed the algorithm might be, if the key is poorly chosen or the key space is small enough, the cryptosystem will be broken. The size of the key space is the number of encryption/decryption key pairs that are available in the cipher system.

In the proposed scheme, the secret key includes nineteen control and initial conditions parameter of the four chaotic maps. The sensitivity to these initial parameters is shown as follows:

- JacobianElliptic Map: $X_0 \in [0,1], \alpha \in [0,4], k \in [0,1]$.
- Piecewise Nonlinear Chaotic Map: $X_0 \in [0,1], \alpha \in [0,4],\ \beta \in [0,4], Y_0 \in [0,1],\ b \in [1,4]\ and\ P \in [0,4]$.

If the precision is 10^{-16} for each of 8 parameters, the size of key space for initial conditions and control parameters is$2^{425}((10^{16})^8 = 10^{128})$. The key space is large enough to resist all kinds of brute-force attacks [41].

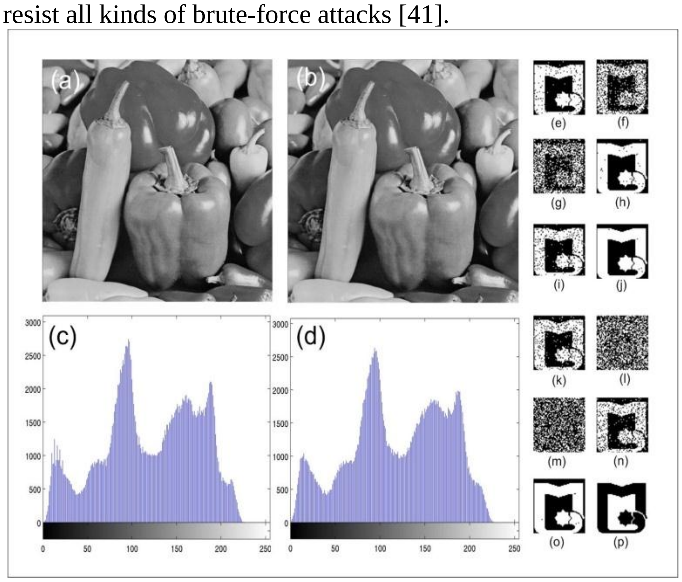


Fig. 11.(a) Original Peppers image (b) watermarked Peppers (c) histogram of original image (d) histogram of watermarked image. Extracted watermarks under different attacks include : (e) JPEG compression (f) Salt &pepper noise 10% (g) Gaussian noise [0,0.01] (h) Histogram Equalization (i) Median filter [3×3] (j) low-pass filter [5×5] (k) Gamma correction 0.6 (l) motion blur 45^o (m) Rotation (1^o) (n) Cropping (25%) (o) Sharpening (p) complement.

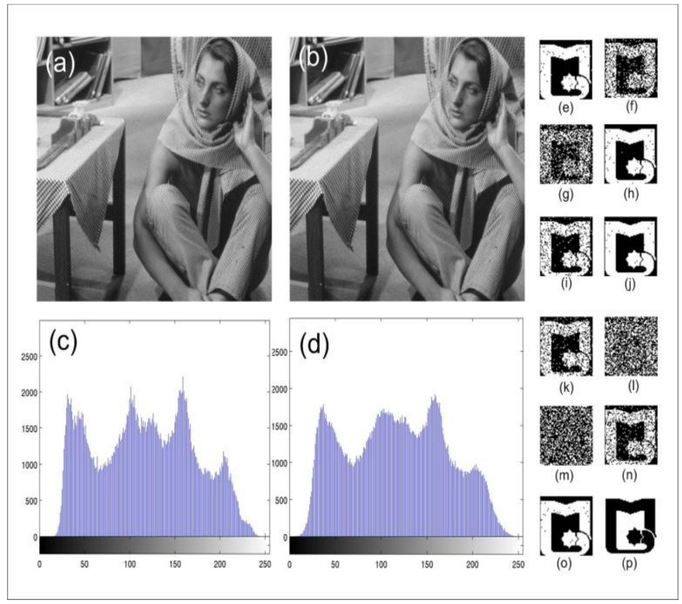


Fig.10. (a) Original Barbara image (b) watermarked Barbara (c) histogram of original image (d) histogram of watermarked image. Extracted watermarks under different attacks include : (e) JPEG compression (f) Salt &pepper noise 10% (g) Gaussian noise [0,0.01] (h) Histogram Equalization (i) Median filter [3×3] (j) low-pass filter [5×5] (k) Gamma correction 0.6 (l) motion blur 45^o (m) Rotation (1^o) (n) Cropping (25%) (o) Sharpening (p) complement.

Table 1
SIMULATION RESULTS OF PSNR UNDER DIFFERENT ATTACKS

Attack	Lena	Peppers	Barbara
Without Attacks	40.21	43.29	36.18
JPEG compression (75%)	37.63	38.03	34.58
Salt & Pepper noise 10%	27.61	41.88	35.87
Gaussian noise (0,0.1)	31.42	31.50	31.35
Histogram Equalization	27.87	29.71	30.63
Median Filtering[3×3]	37.99	38.56	33.41
Low pass filter	40.15	41.18	34.87
Gamma Correction 0.6	27.61	27.22	26.93
Motion Blur 15°	32.49	32.65	30.76
Rotation 1°	31.98	32.14	30.06
Cropping (25%)	27.51	27.65	27.30
Sharpening	39.43	29.83	28.76
Complement	27.43	27.50	27.94

Table 2

SIMULATION RESULTS OF BER UNDER DIFFERENT ATTACKS

Attack	Lena	Peppers	Barbara
Without Attacks	0.00	0.00	0.00
JPEG compression (75%)	1.92	3.36	1.14
Salt & Pepper noise 10%	14.96	18.60	10.52
Gaussian noise (0,0.1)	26.90	32.00	20.92
Histogram Equalization	1.39	0.7	0.95
Median Filtering[3×3]	7.08	6.78	9.54
Low pass filter	0.24	0.12	0.43
Gamma Correction 0.6	11.96	8.91	13.89
Motion Blur 15°	45.55	44.53	44.45
Rotation 1°	51.39	51.70	22.00
Cropping (25%)	13.57	11.20	15.45
Sharpening	0.24	0.12	0.61
Complement	100.00	100.00	100.00

Statistical Test	Ellipticjacobian		Piecewise nonlinear	
	p-value	Result	p-value	Result
Frequency	0.4067	success	0.1901	succes
Block Frequency (m=128)	0.4900	success	0.1827	succes
Cusum-Forward	0.6577	success	0.1252	succes
Cusum-Reverse	0.2771	success	0.2412	succes
Runs	0.3384	success	0.9551	succes
Long Runs of Ones	0.9998	success	0.5069	succes
Rank	0.6861	success	0.4391	succes
Spectral DFT	0.5146	success	0.7242	succes
Non-overlapping Templates(m=9, B=0.000000001)	0.5542	success	0.2271	succes
Overlapping Template (m=9)	0.1390	success	0.9092	succes
Universal	0.0445	success	0.4420	succes
Approximate Entropy (m=10)	0.4419	success	0.0468	succes
Random excursions (x=+1)	0.8814	success	0.3551	succes
Random excursions Variant (x=-1)	0.5356	success	0.4264	succes
Linear Complexity (M=500)	0.8302	success	0.0395	succes
Serial (m=16,$\nabla\psi_m^2$)	0.3680	success	0.2009	succes

D. The study of the performance of the new algorithm

To evaluate the performance of the new algorithms the PSNR and BER has been computed and compared with some famous benchmarks. Figs.(11-12) show the implementation of the new algorithm on Peppers and Barbara, respectively. The histogram and the extracted logos using different attacks also are presented in these figures. Additionally Table 1 and Table 2 show the comparison of PSNR and BER for the benchmarks. The results conclude of this new watermarking scheme improves the quality of the watermarking as well as increasing the security of images.

E. A Statistical test suit for pesudo random generation for cryptography

The need for random and pseudorandom numbers arises in many cryptographic applications. For example, common cryptosystems employ keys that must be generated in a random fashion. Many cryptographic protocols also require random or pseudorandom inputs at various points.In this paper , we have applied the NIST (National Institute of Standards and Technology) statistical test suites to investigate the randomness of cryptographic random generator numbers. These statistical tests are listed in Table 3. The P-value shows the probability of the randomness of the statistical test suite. If the P-value is very close to one the generated random number passes the test. Therefore the randomness of the generated sequences is accepted. P-value in the range of [0.001,0.01] shows a failure test.

Table 3

Result of Statistical test suites for pseudo random generators in applied chaotic maps

II. CONCLUDING REMARKS

A new watermarking scheme for blind digital image watermarking based on multiple chaotic maps and DCT transform was proposed. Chaotic Quantom map and Jacobian elliptic map were applied to design the selection scheme for watermark embedding. We have used multiple chaotic maps to increase both the number of keys (control parameters) and complexities involved in the algorithm. The size of key space for initial conditions and control parameters were computed about 10^{128} (2^{425}). Therefore the resistance of the method is the highest in comparison with our previous work.

Furthermore, in this work the maximum amount of data to be stored was 128*128. Finally, according applied multiple chaotic maps, the extracted watermark logo results were much better than our previous work.

REFERENCES

[1] Cox IJ, Matthew LM, Jeffrey AB, et al. Digital Watermarking and Steganography. Second edition, Burlington, MA: Morgan Kaufmann Publishers (Elsevier); 2007.

[2] A.G. Bors, I. Pitas, Image watermarking using DCT domain constraints, Proceedings of IEEE International Conference on Image Processing, vol. 3, 1996, pp. 231–234.

[3] D. Kundur, D. Hatzinakos, Towards robust logo watermarking using multiresolution image fusion, IEEE Transcations on Multimedia 6 (2004) 185–197.

[4] A. Mooney and J. G. Keating, \The impact of the theoretical properties of the logistic function on the generation of optically detectable watermarks," proceeding of SPIE, Technology for Optical Countermeasures 5615,pp.120_129,2004.

[5] S.Behnia, S.Teshnelab, P.Ayubi, Multiple-watermarking scheme based on improved chaotic maps Communications in Nonlinear Science and Numerical Simulation Volume 15,Issue 9, September 2010, Pages 2469-2478

[6] X.Wu,Z.Hong Guan, Z.Wu ‘A Chaos Based Robust Spatial Domain Watermarking alghorithm’ Advances in Neural Networks_ISNN 2007, Lecture Notes in Computer Science,2007, Volume 4492/2007, 113-119

[7]Cox and M.L. Miliier, A review of watermarking and the importance of perceptual modeling, Proc. of SPIE 3016 (1997), pp. 9299.

[8] R. Reeves, and K. Kubik, “Benefits of Hybrid DCT Domain Image Matching. International Archives of Photogrammetric and Remote Sensing”, Vol. 33, Part B3. Amsterdam 2000, pp. 771-778.

[9] A. K. Bhandari, A. Kumar and P. K. PadhyEnhancement of Low Contrast Satellite Images using Discrete Cosine Transform and Singular Value Decomposition, World Academy of Science, Engineering and Technology ISSUE 55 july 2011

[10] B L. Gunjal, R.R. Manthalkar An overview of transform domain robust digital image watermarking algorithms, Volume 2 No. 1 ISSN 2079-8407 Journal of Emerging Trends in Computing and Information Sciences ©2010-11 CIS Journal

[11] H.Peng, J.Wang, W.Wang, Image watermarking method in multiwavelet domain based on support vector machines' journal of Systems and software, volume 83, Issue 8, Agust 2010,Pages 1470-1477

[12] Ramani K.; Prasad E.V, Varadarajan S.; Subramanyam A,"A Robust Watermarking Scheme for Information Hiding", Advanced Computing and Communications, 16th International Conference, 14-17 Dec. 2008 pp:58 – 64.

[13] C.H. Huang, J.L. Wua, Fidelity-guaranteed robustness enhancement of blind-detection watermarking schemes, Information Sciences 179 (2009) 791-808.

[14] Y. Liu, J. Zhao, A new video watermarking algorithm based on 1-D DFT and Radon transform, Signal Processing, 90 (2010) 626-639.

[15] H. Wei, M. Yuan, J. Zhao, Z. Kou, Research and Realization of Digital Watermark for Picture Protecting, First International Workshop on Education Technology and Computer Science, IEEE, Vol. 1, 2009, pp.968-970.

[16] X. Li, A New Measure of Image Scrambling Degree Based on Grey Level Difference and Information Entropy, 2008 International Conference on Computational Intelligence and Security, Vol. 1, 2008, pp.350-354 .

[17] Z.W.Shen, W.W. Liao, Y.N.Shen, Blind watermarking algorithm based on henon chaos system and lifting scheme wavelet, Proceedings of the 2009 International Conference on Wavelet Analysis and Pattern Recognition, Baoding, 2009, pp.308-313.

[18] M. Barni, F. Bartolini, A. Piva, Improved wavelet based watermarking through pixel-wise masking, IEEE Trans Image Process 10 (2001) 783- 791.

[19] JA.Logan, JC.Allen' Nonelinear Dynamics and chaos in insect population, Annual Review of Entomology (1992) Volume: 37, Issue: 1, Pages: 455-477

[20] Singh, N., Sinha, A. Digital image watermarking using gyrator transform and chaotic maps ,Optik, 121 (15), pp. 1427-1437 (2010).

[21] Ma, N., Zhang, Q., Wei, X. Novel image watermarking algorithm based on DWT and chaos theory , Journal of Information and Computational Science, 7 (7), pp. 1613-1620 (2010).

[22] Wei, Y., Li, Y. Multipurpose digital watermark algorithm for color images , HuazhongKejiDaxueXuebao (ZiranKexue Ban)/Journal of Huazhong University of Science and Technology (Natural Science Edition), 38 (2), pp. 109-112 (2010).

[23] Eisencraft, M., Kato, D.M., Monteiro, L.H.A. Spectral properties of chaotic signals generated by the skew tent map , Signal Processing, 90 (1), pp. 385-390.(2010).

[24] Zhang, X.-C., Zhang, C.-J., Jia, J. Digital image watermarking by double encryption with chaos and Arnold , GuangdianGongcheng/Opto-Electronic Engineering, 36 (8), pp. 116-122(2009).

[25] Peng, H., Jiang, T. Application of chaotic map in the color image watermarking , Wuhan LigongDaxueXuebao (JiaotongKexue Yu Gongcheng Ban)/Journal of Wuhan University of Technology (Transportation Science and Engineering), 33 (4), pp. 776-778(2009)

[26] S. Behnia, A. Akhshani, S. Ahadpour, H. Mahmodi, and A. Akhavan, “A fast chaotic encryption scheme based on piecewise nonlinear chaotic maps,” Phys. Lett. A vol. 366, pp.391-396, 2007.

[27] M.jaefarizadeh, S.Behnia, Hierarchy of one- and many-parameter families of elliptic chaotic maps of cn and Sn types, Physics Letters A 310, P. 168, 2003.

[28] A. Tefas, A. Nikolaidis, N. Nikolaidis, V. Solachidis S. sekeridou, I. Pitas, Markov chaotic sequences for correlation based watermarking schemes, chaos, solitons& fractals 17 (2003) 567-573.

[29] S. Nikolaidis, I. Pitas, Comparison of different chaotic maps with application to image watermarking, In: Proceedings of IEEE international symposium on circuits and systems, Geneva, (2002) 509-512.

[30] J.Ayubi,Sh.Mohanna, F.Mohanna, M.Rezaei, A Chaos Based Blind Digital Image Watermarking in The Wavelet Transform Domain, International Journal of Computer Science Issues,Volume 8, Issue 4, July 2011.

[31] A.Jafarizadeh, S.Behnia, Hierarchy of random deterministic chaotic maps with an invariant measure, J. Math. Phys. **44**, 5386 (2003); doi:10.1063/1.1610240 (*15 pages,* volume 44, issue11

[32] W.B. Pennebaker and J. L. Mitchell, JPEG Still Image Data Compression Staadard. Chapman & Hall, New York, 1993.

[33] T. Acharya and P. Tsai, JPEG2000 Standard for Image Compression: Concepts, Algorithms and VLSI Architectures, Wiley, Hoboken, NJ,2004.

[34] T.S. Huang, G. I.Yang, and G. Y .Tang, A Fast Two-Dimensional Median Filtering Algorithm, IEEE Trans. Acoustics, Speech, and Signal processing, ASSP-27, 1, 1979, pp.13-18.

[35] R. C. Gonzalez, R. E. Woods, Digital Image Processin,g, Addisonwesley, Reading, MA, 1992.

[36] W.K. Pratt, Digital Image Processing, 2nd ed., Wiley, New York, 1991.

[37] A. Rosenfeld, A. C. Kak, Digital Picture Processing, 2nd ed., Vol. 1, Academic Press, 1982.

[38] P. Lee, Yi Chenb, S. Pei, Y. Chena, Reply to the comment Keystream cryptanalysis of a chaotic cryptographic method, Computer Physics Communications 160 (2004) 208.

[39] M. Falcioni, L. Palatella, S. Pigolotti, Properties making a chaotic system a good pseudo random number generator, Phys. Rev. E 72 (2005)
016220-10. IMAGE ENCRYPTION BASED ON JACOBIAN ELLIPTIC MAPS 7

[40] C.M. Gonzaleza, H.A. Larrondoa, O.A. Rosso, Intensive statistical complexity measure of pseudorandom number generators, PhysicaA 354 (2005) 133-138.

[41] Z.Hong Guan, F.Huang, W.Gua, ‘Chaos-based image encryption algorithm’ Physics letters A,volume 346, issue 1-3, 10 Octobr 2005, pages 153-157