Journal of mathematics and computer science 13 (2014), 311-320

Contents list available at JMCS

Journal of Mathematics and Computer Science

Journal Homepage: www.tjmcs.com

A Chaotic Blind Digital Image Watermarking Based On Singular Value Decomposition in Spatial Domain

Niaz Khorrami*, Peyman Ayubi**, Sohrab Behnia, Jila Ayubi

Department of Mathematics, Salams Branch, Islamic Azad University, Salmas, Iran.

Department of Computer Engineering, Urmia Branch, Islamic Azad University, Urmia, Iran.

Department of Physics, Urmia University Of Technology, Urmia, Iran.

Department of Electrical Engineering, Meraj Inistitue, Salmas, Iran.

**n.khorrami@iausalmas.ac.ir*
***p.ayubi@iaurmia.ac.ir*

Article history:
Received August 2014
Accepted October 2014
Available online October 2014

Abstract

In this letter a new watermarking scheme for Gray scale image is proposed based on a family of the chaotic maps and Singular Value Decomposition. Jacobian elliptic map is used to encrypt the watermark logo to improve the security of watermarked image. Quantum map is also used to determine the location of image's block for the watermark embedding. To test the robustness and effectiveness of our proposed method, several attacks are applied to the watermarked image and the best results have been reported. The purpose of this algorithm is to improve the shortcoming of watermarking such as small key space and low security. The experimental results demonstrate that the key space is large enough to resist the attack and the distribution of grey values of the encrypted image has a random-like behavior, which makes it a potential candidate for encryption of multimedia data such as images, audios and even videos.

Keywords: Blind Digital Image Watermarking, Chaos, Singular Value Decomposition, Chaotic Map.

1 Introduction

Watermarking technique is one of the active research fields in recent years, which can be used for protection of multimedia information, content authentication, and so on [1, 2]. A watermark typically contains information about origin, status, and/or destination of the host data [3], [4].

Image scrambling is one of the most prevailing encryption algorithms these years [5-7]. However, these methods are not so many. The majority of watermarking schemes proposed to date, use watermarks generated from pseudo random number sequences [8].

Chaotic systems have been studied for more than 50 years. In 1963, Edward Lorenz discovered the first chaotic system and has been established by many different research areas, such as physics, mathematics, and engineering [9]. This paper chiefly focuses on the application of quantum chaos and Jacobian elliptic in encryption techniques of watermark logo. Quantum chaos and Jacobian elliptic chaos began as an attempt to find chaos in the sense of extreme sensitivity to changes in initial conditions. It was found however, that in quantum mechanics, it is the sensitivity of quantum trajectories with respect to changes in control parameters that is likely to define quantum chaos [10]. Chaotic functions such as Markov Maps, Bernoulli Maps, Skew Tent Map, and Logistic Map have been widely used to generate watermark sequences [11-12].

Singular Value Decomposition (SVD) is said to be a significant topic in linear algebra by many renowned mathematicians. The SVD was introduced by Eckart and Young [13] and has become one of the most widely used techniques of computational algebra and multivariate statistical analysis applied for data approximation, reduction and visualization. The use of singular value decomposition (SVD) in digital image watermarking has been widely studied [14-15].

The chaotic maps are employed to improve the security of a watermarked image, and an improved SVD embedding and extraction procedure has been used to encrypt the watermark logo. The upgraded mapping method determines the location of image's block where the watermark is embedded. The proposed method increases the security of watermarking and also it enables to hide more information in the watermarked image. The robustness of the proposed method has been evaluated against various attacks including common signal processing methods and geometric transformations.

2 CHAOTIC MAPS

2.1 Jacobian Elliptic Maps

One-parameter families of Jacobian elliptic rational maps [16] of the interval [0,1] with an invariant measure can be defined as:

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

Where $X_0 \in [0,1]$, $\alpha \in [0,4]$ and $\in [0,1]$, k (modulus) represent the parameter of the elliptic functions. Jacobian elliptic map is used in this paper as follow:

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

2.2 Quantum Map

The quantum rotators model has been widely used to study the dynamics of classically chaotic quantum systems [17] and is specified in a simple form by:

$$X_{N+1}^{1} = r(X_N - X_N^2)Cos^k(-\lambda \frac{e^{-mb}}{b}) \qquad (3)$$

Where $X_0 \in [0,1]$,$r \in [3.6,4]$, $\lambda \in [0,1]$, $\in [1,4]$, $b \in [1,4]$ and $k \in [2,10]$.

The 2D quantum map can be defined as:

$$\begin{cases} X_{N+1}^{1} = r_1(X_N - X_N^2)Cos_1^k(-\lambda_1 \frac{e^{-m_1 b_1}}{b_1}) \\ Y_{N+1}^{1} = r_2(Y_N - Y_N^2)Cos_2^k(-\lambda_2 \frac{e^{-m_2 b_2}}{b_2}) \end{cases} \qquad (4)$$

This map is used for embedding and extraction process as follow:

$$\begin{cases} X_{N+1}^{1} = (X_{N+1} \times 10^{14}) \ mod \ M \\ Y_{N+1}^{1} = (Y_{N+1} \times 10^{14}) \ mod \ N \end{cases} \qquad (5)$$

Where M, N denote the number of rows and columns in the blocked image, respectively.

2.3 Elliptic 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-dimensional array$W_{(m\times n)\times 1}$.
- The secret keys, including initial conditions and control parameters are set, and chaotic map in Eq.(2) are iterated 500 times.
- Ciphered values are computed by:

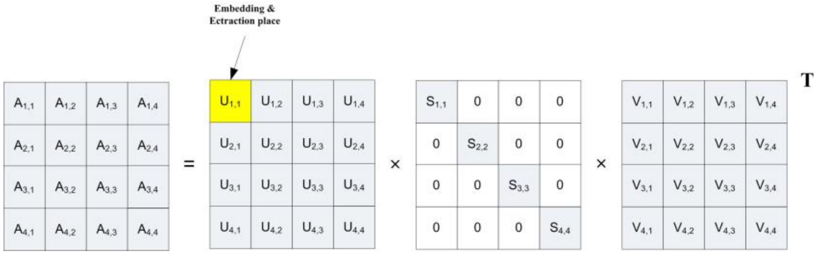
  $$C_i = (cx_i^1 \ \oplus \ W_i) \qquad (6)$$
- Where C_i is one dimensional array considered for storing process in the ciphered value.
- When all the pixels were encrypted, the matrix $C_{(m\times n)\times 1}$ is transformed into $C_{m\times n}$ and cipher watermark logo is exported to next step of watermarking algorithm.

Process of decryption is very similar to the encryption process. Just steps mentioned in the encryption process are repeated.

2.4 Selecting Location embedded by Quantum Map

Using the coordinate i , j position of watermark pixel as the initial condition and through setting a value for the control parameter in Eq.(5), chaotic map is iterated after which, the embedding position of the pixels from the watermark image to host image can be obtained. The watermark pixels will get different embedding positions, so, the embedded watermark pixels will spread on the host image randomly.

Fig. 1. Singular value decomposition of 4×4 block of digital image.



3 Singular Value Decomposition

An $m \times n$ matrix A can be factorized as:

$$A = USV^{\mathrm{T}} \qquad (7)$$

Or

$$A = \sum u_i\, s_i {v_i}^T = u_1 s_1 {v_1}^T + u_2 s_2 {v_2}^T + \cdots + u_r s_r {v_r}^T \qquad (8)$$

Where U is an $m \times m$ orthogonal matrix, V is an $n \times n$ orthogonal matrix, S is an $m \times n$ diagonal matrix with non-negative entries as follows

$$S_{m\times n} = \begin{bmatrix} D & O_1 \\ O_2 & O_3 \end{bmatrix} \qquad (9)$$

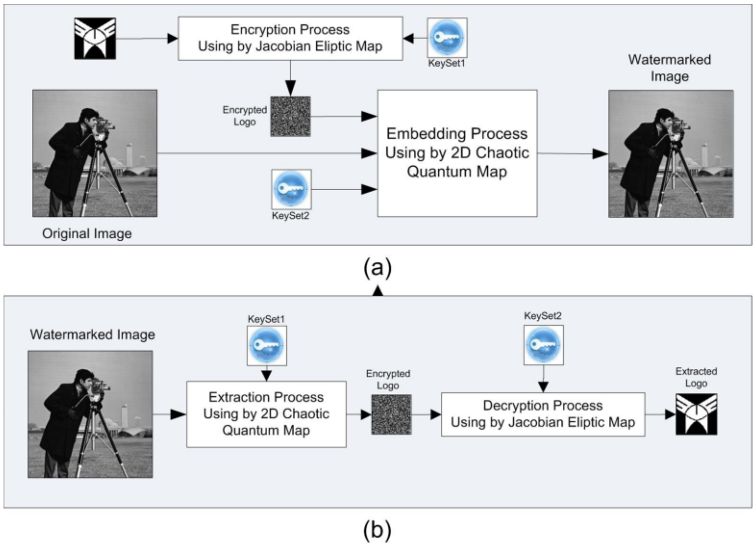
Where O_1, O_2, O_3 are zero matrices and D is a diagonal matrix whose diagonal entries Σ have nonzero singular values of A:

$$D = \begin{bmatrix} S_1 & 0 & \dots & 0 & 0 \\ 0 & & & & 0 \\ \vdots & & \ddots & & \vdots \\ 0 & & & & 0 \\ 0 & 0 & \dots & 0 & S_r \end{bmatrix}, S_1 \geq S_2 \geq \cdots \geq S_r \geq 0 \qquad (10)$$

Where r is the rank of A.

The factorization in (1) is called the singular value decomposition of A.For a matrix with more rows than columns, in an alternate definition of the singular value decomposition, the matrix U is $m \times n$ with orthogonal columns, and S is a $m \times m$ diagonal matrix with nonnegative entries. Likewise, for a matrix with more columns than rows, the singular value decomposition can be defined above but with the matrix V being $n \times m$ with orthogonal columns, and S is a $m \times m$ diagonal with nonnegative entries. Given an $m \times n$ matrix A, a rank-k approximation of A is a matrix A_k of the same size and of rank at most k that minimizes that difference with A.A rank-k approximation to A is obtained by taking the first k terms of the SVD:

$$A_k = \sum_{i=1}^{k} u_i\, \sigma_i {v_i}^T \qquad (11)$$



(a)

(b)

Fig. 2. Block Diagram of (a) embedding process (b) extraction process.

In general, low-rank approximations of data matrices serve two proposes: they reduce space requirements and often provide a more transparent representation. Fig.1 is shown singular value decomposition for 4×4 block in digital image.

4 Watermark Embedding and Extraction

Block diagram of proposed embedding and extraction process are shown in Fig.2

4.1 Watermark embedding

In this section the algorithm of embedding are discussed. The embedding process proposed in this paper consists of the following major parts:

Step 1: Encryption process is applied to input watermark logo.

Step 2: Position of block in original image is selected by quantum map and pixel values in block are stored in $Block_{4\times4}$.

Step 3: The SVD coefficients are computed as follow:

$$[U\,,S\,,V] = SVD(Block_{4\times4})$$

Where U, S, V has values in 4×4 arrays (See Fig.1) and $SVD(.)$ denotes the singular value decomposition computational function.

Step 4: U_{11} coefficient is updated as follow:

$$\begin{Bmatrix} U_{11} = Sign(U_{11}) \times (U_{21} + T) & if\ W_{ij} = 1 \\ U_{11} = Sign(U_{11}) \times (U_{21} - T) & if\ W_{ij} = 0 \end{Bmatrix}$$

Where W_{ij} denotes the binary pixel value of watermark logo in location $(\,i\,,j\,)$ and T is threshold value (T=0.02).

Step 5: Inverse of singular value decomposition is computed to obtain block pixels as follow:

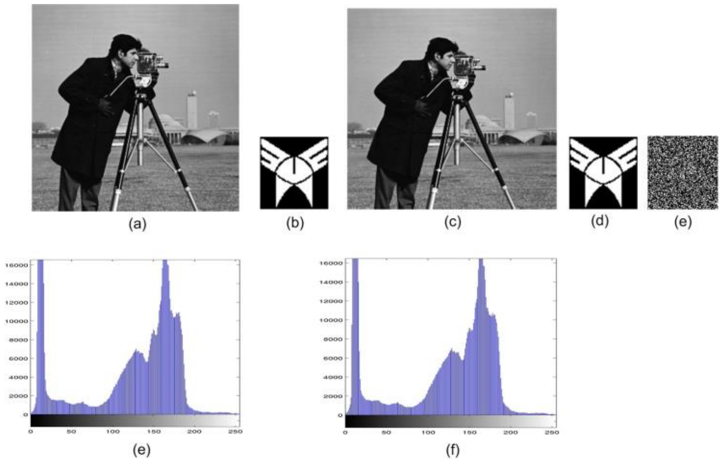


Fig. 3,4 (a) Original Image, (b) Watermark Logo (c) Watermarked Image (d)Extracted Logo by correct password, (e) Extracted Logo by incorrect password (f) Histogram of Original image (g) Histogram of Watermarked image

$$Block_{4\times4} = U \times S \times V^T$$

Where (.) ^{T} is transpose operation.

Step 6: step 2 to 5 is iterated, when all pixels in watermark logo are embedded to original image and final watermarked image is obtained.

4.2 Watermark extraction

Watermark extraction process is very similar to the embedding process. This process consists of the following major parts:

Step 1: Position of block in watermarked image is selected by quantum map and pixel values in block are stored in Block$_{4\times4}$.

Step 2: The SVD coefficients are computed as follow:

$$[U\ ,S\ ,V] = SVD(Block_{4\times4})$$

Where U, S, V has values in 4×4 arrays (See Fig.1) and $SVD(.)$ denotes the singular value decomposition computational function.

Step 4:W_{ij} is extracted as follow:

$$\begin{Bmatrix} W_{ij} = 1 & if\ ABS(U_{11}) > ABS(U_{21}) \\ W_{ij} = 0 & if\ ABS(U_{11}) \le ABS(U_{21}) \end{Bmatrix}$$

Where W_{ij} denotes the binary pixel value of watermark logo in location $(\ i\ ,j\ )$ and $ABS(.)$ denotes the absolute function in mathematics.

Step 5: Step 1 to 4 is iterated, when all pixels in watermark logo are extracted from watermarked image and encrypted watermark logo is obtained

Step 6: Decryption process is applied to obtained watermark logo in Step 5.

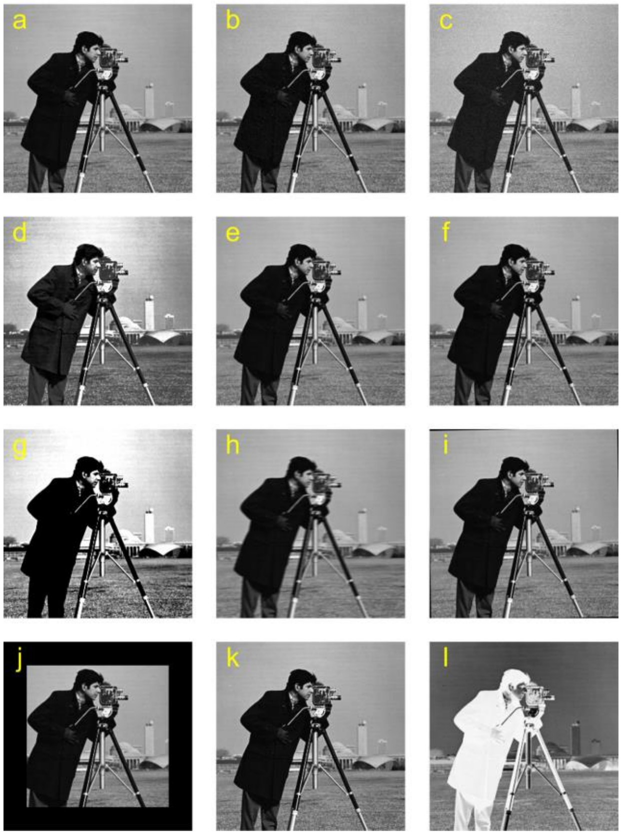


Fig. 5 Watermarked image under different attacks. (a) JPEG compression (70%), (b) Salt & pepper noise (10%), (c) Gaussian noise (0,0.01), (d)Histogram Equalization, (e) Median filter [3×3], (f) Low-pass filter [5×5], (g) Gamma correction (0.6^o) (h) Motion blur (45^o) (i) Rotation (1^o), (j) Cropping (25%) (k) Sharpening (l) Complement.

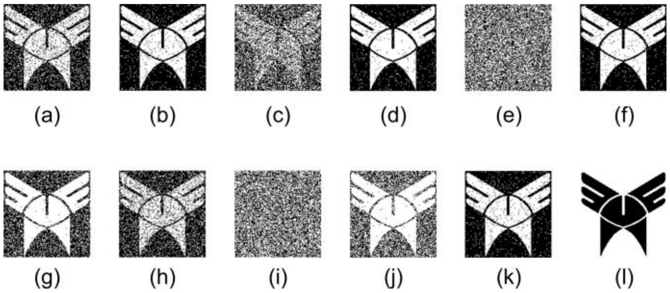


Fig. 6. The Extracted Watermark logo under different attacks. (a) JPEG compression (70%), (b) Salt & pepper noise (10%), (c) Gaussian noise (0,0.01), (d)Histogram Equalization, (e) Median filter [3×3], (f) low-pass filter [5×5], (g) Gamma correction (0.6^o) (h) motion blur (45^o) (i) Rotation (1^o), (j) Cropping (25%) (k) sharpening (l) complement.

5 Experimental Result

Table 1. Simulation results of PSNR(dB) in standard images

Attack	Cameraman	Peppers	Boat
Without Attacks	46.44	46.99	45.93
JPEG compression (75%)	43.34	42.62	41.85
Salt & Pepper noise 10%	42.24	42.39	41.88
Gaussian noise (0,0.1)	31.68	31.47	31.44
Histogram Equalization	29.43	29.66	29.96
Median Filtering[3×3]	48.00	45.30	43.12
Low pass filter	45.55	45.44	44.38
Gamma Correction 0.6^0	29.32	27.21	29.64
Motion Blur 15°	35.48	35.52	33.64
Rotation 1°	32.76	32.26	31.01
One quarter cropped	27.62	27.66	27.63
Sharpening	36.09	34.10	33.08
Complement	26.59	27.50	26.01

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

5.1 Evaluation of the effectiveness

To demonstrate the effectiveness of the proposed algorithm, MATLAB simulations are performed by using 512× 512 pixel gray level "Cameraman" image and 128 ×128 pixel binary watermark logo "IAU". Fig. 3 demonstrates the invisibility of watermark. Figs.3 (a) and Fig.3 (b) show the original host image and watermark logo, respectively. Figs.3(c-e) shows 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. To quantitatively evaluate the performance of the proposed scheme, the peak signal-to-noise ratio (PSNR) was adopted to measure the image quality of a watermarked image which is given by:

$$PSNR = 10 \times log_{10} \frac{255^2}{MSE} \ (dB) \qquad (12)$$

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

Table 2. Simulation result of BER(%) in standard images

Attack	Cameraman	Peppers	Boat
Without Attacks	0	0	0
JPEG compression (75%)	14.22	10.66	9.61
Salt & Pepper noise 10%	4.22	3.69	3.80
Gaussian noise (0,0.1)	35.03	35.29	32.90
Histogram Equalization	2.88	2.16	1.86
Median Filtering[3×3]	47.28	48.66	49.54
Low pass filter	2.52	2.22	1.90
Gamma Correction 0.6^{0}	15.58	15.96	11.09
Motion Blur 15°	17.90	15.02	18.54
Rotation 1°	49.81	50.61	49.69
One quarter cropped	26.53	26.34	26.34
Sharpening	3.57	3.42	3.44
Complement	100	100	100

$$MSE = \frac{1}{M\times N}\sum_{i=1}^{M}\sum_{j=1}^{N}(H_{i,j} - \acute{H}_{\iota,J})^{2} \qquad (13)$$

Where $H_{i,j}$ and $\acute{H}_{\iota,J}$ 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:

$$BER = \frac{B}{M\times N}\times 100 \qquad (14)$$

Where, B is the number of erroneously detected bits, and $M \times N$ is the extracted watermark image dimensions. The PSNR for the watermarked image is 46.44 dB, and the BER of the extracted watermark is zero. Therefore, there is no obvious perceptual distortion between watermarked image and original one; the embedded watermark does not degrade the quality of original host image.

5.2 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.

Fig. 4 shows an example of a watermarked image attacked with the listed attacks. The corresponding best extracted watermarks for denoted attacks are shown in Figs. 5.

The test results, BER and PSNR computed for standard images are shown in Table 1 and 2.

6 Concluding Remarks

Our proposed method is a novel watermarking scheme for image authentication based on multiple chaotic systems. The scheme is specially designed for image, thus, enabling various network multimedia applications. Quantum chaos is applied to design the selection scheme for watermark embedding and Jacobian elliptic map is used to encryption of watermark logo. This algorithm tries to address the shortcoming of watermarking such as small key space, watermarking speed and level of security.

Without the correct initial condition, the watermark cannot be successfully detected. In general, the method is suitable for image authentication with application in law, commerce, defense, medical databases and journalism. The security of watermarking is greatly improved when chaos is administered. The goal is to realize a watermarking method with a private code. Further studies must be started to develop watermarking methods with a public key.

References

1. Cox IJ, Matthew LM, Jeffrey AB, et al. Digital Watermarking and Steganography. Second edition, Burlington, MA: Morgan Kaufmann Publishers (Elsevier); 2007.
2. S.Amirgholipour,A.Naghsh-Nilchi, , et al. ,Application of Unsharp Mask in Augmenting the Quality of Extracted Watermark in Spatial Domain Watermarking, The journal of Mathematics and Computer Science, 11 (2014) 137-146.
3. C.H. Huang, J.L. Wua, Fidelity-guaranteed robustness enhancement of blind-detection watermarking schemes, Information Sciences 179 (2009) 791-808.
4. Y. Liu, J. Zhao, A new video watermarking algorithm based on 1-D DFT and Radon transform, Signal Processing, 90 (2010) 626-639.
5. 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.
6. 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 .
7. 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.
8. M. Barni, F. Bartolini, A. Piva, Improved wavelet based watermarking through pixel-wise masking, IEEE Trans Image Process 10 (2001) 783- 791.
9. J. Vahidi, M. Gorji , The Confusion-Diffusion Image Encryption Algorithm with Dynamical Compound Chaos, 9 (2014) 451-457.
10. A. Peres, Quantum Theory: Concepts and Methods 24.
11. 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.
12. 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.
13. C. Eckart, G. Young, The approximation of one matrix another of lower rank, Psycometrika 1 (1936) 211218.
14. Ray-Shine Run, Shi-Jinn Horng, Jui-Lin Lai, Tzong-Wang Kao, Rong-Jian Chen, An improved SVD-based watermarking technique for copyright protection, Expert Systems with Applications, In Press, Uncorrected Proof, Available online 28 July 2011, ISSN 0957-4174, DOI: 10.1016/j.eswa.2011.07.059.
15. Chih-Chin Lai, An improved SVD-based watermarking scheme using human visual characteristics, Optics Communications, Volume 284, Issue 4, 15 February 2011, Pages 938-944, ISSN 0030-4018, DOI: 10.1016/j.optcom.2010.10.047.
16. R.L. Devancy, An Introduction to Chaotic Dynamical Systems. Addison Wesley, 1982.
17. Behnia, S.; Ayubi, P.; Soltanpoor, W., "Image encryption based on quantum chaotic map and FSM transforms," Telecommunications Network Strategy and Planning Symposium (NETWORKS), 2012 XVth International , vol., no., pp.1,6, 15-18 Oct. 2012.