A Novel Image Encryption Framework Based on Markov Map and Singular Value Decomposition

Gaurav Bhatnagar[1], Q.M. Jonathan Wu[1], and Balasubramanian Raman[2]

[1] University of Windsor, Windsor, ON, Canada N9B 3P4
[2] Indian Institute of Technology Roorkee, Roorkee-247 667, India
{goravb,jwu}@uwindsor.ca,
balarfma@iitr.ernet.in

Abstract. In this paper, a novel yet simple encryption technique is proposed based on toral automorphism, Markov map and singular value decomposition (SVD). The core idea of the proposed scheme is to scramble the pixel positions by the means of toral automorphism and then encrypting the scrambled image using Markov map and SVD. The combination of Markov map and SVD changed the pixels values significantly in order to confuse the relationship among the pixels. Finally, a reliable decryption scheme is proposed to construct original image from encrypted image. Experimental results demonstrate the efficiency and robustness of the proposed scheme.

1 Introduction

With the ripening in the field of communication and internet technology, multimedia transmission over networks and storage on web servers have become a vital part of it. However, this convenience also causes substantial decrease in multimedia security. Cryptography/Encryption techniques are widely used to ensure security but these techniques are developed for textual data and hence inappropriate for direct implementation on multimedia. This is due to the multimedia properties like high redundancy and large volumes which require specific encryption techniques developed with the consideration of structural and statistical properties of multimedia content.

Generally, the process of image encryption is divided into two phases, scrambling the image and then encrypting the scrambled image. Image scrambling cast the image elements into confusion by changing the position of pixel in such a way that the original image is not recognizable. But the original image can be obtained by performing reverse operations. Hence to make process complicated and enhance the security, scrambled image undergoes second phase. This phase essentially changes the pixel values in order to confuse the strong relationship among the pixels. The scrambling is done by various reversible techniques based on magic square transform, chaos system, gray code etc. In second phase, the scrambled image is then passed through some cryptographic algorithm like SCAN based methods [1, 2], chaos based methods [3–8], tree structure based methods [9, 10] and other miscellaneous methods [11, 12].

In this paper, a novel image encryption technique is presented based on the toral automorphism, Markov map and singular value decomposition. The first phase i.e. scrambling of pixels positions is done by toral automorphism. The second phase i.e. changing

M. Kamel and A. Campilho (Eds.): ICIAR 2011, Part II, LNCS 6754, pp. 286–296, 2011.

the pixel values is done by singular value decomposition. For this purpose, singular values of a random matrix, generated from Markov map, is computed via SVD. Hankel matrix is then created using computed singular values and again decomposed into singular values, left and right singular vectors. Now, a secret image is obtained using left and right singular vectors. Using the secret image, encryption process is done and the encrypted image is sent to insecure network channel. From the results, it is observed that the proposed technique significantly reduces the correlation among the pixels by using Markov map and singular value decomposition framework.

This paper is organized as follows: In sections 2 and 3, toral automorphism and singular value decomposition are introduced, followed by the introduction of Markov maps in section 4. The proposed image encryption technique is illustrated in section 5. Section 6, presents experimental results using proposed watermarking scheme and finally the concluding remarks are given in section 7.

2 Toral Automorphism

The toral automorphism [13] is the mapping from torus to torus. In 2D case, the torus say $\mathbb{T}^2$, can be viewed as the square where two points $(x_1,\ y_1)$ and $(x_2,\ y_2)$ are identified by either $x_1 = x_2$, $y_1 = y_2$ or one of the two coordinates is 0 and other is 1. The simplest example of trous is quotient group $\mathbb{R}^2/\mathbb{Z}^2$, where $\mathbb{R}^2$ is a topological group with addition operation and $\mathbb{Z}^2$ is a discrete subgroup of it. More precisely, toral automorphism is given as $\mathbf{r}' = T(\mathbf{r}) = A\mathbf{r}(mod\ 1)$ where $A = \begin{bmatrix} a & b \\ c & d \end{bmatrix}$ with integers $a,\ b,\ c,\ d$ and $det(A) = 1$. This matrix A plays a vital role in the iterated dynamical system formed by T. Mathematically, the dynamical system based on toral automorphism is expressed as $\mathbf{r}(n+1) = A\mathbf{r}(n)(mod\ 1)$ i.e.

$$\begin{bmatrix} x(n+1) \\ y(n+1) \end{bmatrix} = A \begin{bmatrix} x(n) \\ y(n) \end{bmatrix} (mod\ 1), \quad n = 0, 1, 2, ... \tag{1}$$

If $a = 1,\ b = 1,\ c = 1$ and $d = 2$ then toral automorphism is reduced to cat map. Hence, cat-map is a special case of toral automorphism. The working procedure of toral automorphism is depicted in figure 1. It essentially, stretches the unit square by transformation and then folds it into square by unit modulo operation. Hence, toral automorphism is area preserving. Toral automorphism can be easily be extended from unit square to a square of length N by stretching the square of length N via transformation and then folding it into square by N modulo operation. Hence, the generalized toral automorphism is expressed as $\mathbf{r}(n+1) = A\mathbf{r}(n)(mod\ N)$ i.e.

$$\begin{bmatrix} x(n+1) \\ y(n+1) \end{bmatrix} = A \begin{bmatrix} x(n) \\ y(n) \end{bmatrix} (mod\ N) \tag{2}$$

Toral automorphism is a special class of Anosov Diffeomorphisms which are extreme chaotic systems obeying local instability, ergodicity with mixing and decay of correlation and periodic. Due to periodicity, the original square will reappear after some large number of iterations.

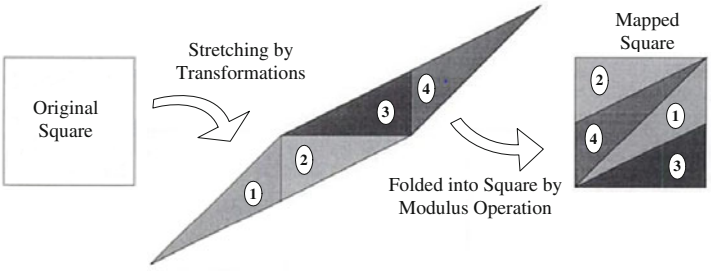

Fig. 1. Working Process for Toral Automorphism

3 Singular Value Decomposition

In linear algebra, the singular value decomposition(SVD) [14] is an important factorization of a rectangular real or complex matrix with many applications in signal/image processing and statistics. The SVD for square matrices was discovered independently by Beltrami in 1873 and Jordan in 1874, and extended to rectangular matrices by Eckart and Young in the 1930s. Let A be a general real(complex) matrix of order $m \times n$. The singular value decomposition (SVD) of X is the factorization

$$X = U * S * V^T \tag{3}$$

where U and V are *orthogonal(unitary)* and $S = diag(\sigma_1, \sigma_2, ..., \sigma_r)$, where σ_i, $i = 1(1)r$ are the singular values of the matrix X with $r = min(m, n)$ and satisfying $\sigma_1 \geq \sigma_2 \geq ... \geq \sigma_r$. The first r columns of V are the *right singular vectors* and the first r columns of U are the *left singular vectors*.

Use of SVD in digital image processing has some advantages. First, the size of the matrices for SVD transformation is not fixed. It can be a square or rectangle. Secondly, singular values in a digital image are less affected if general image processing is performed. Finally, singular values contain stable intrinsic algebraic image properties such that large difference in singular values does not occur whenever a small perturbation is added to the matrix.

4 1-D Chaotic Map: Linear Markov Maps

A one dimensional map $\mathcal{M} : U \rightarrow U,\ U \subset \mathbb{R}$, U usually taken to be [0,1] or [-1,1] is defined by the difference relation

$$x(i+1) = \mathcal{M}(x(i)), \quad i = 0, 1, 2, ... \tag{4}$$

where $\mathcal{M}(\cdot)$ is a continuous and differentiable function which defines the map and $x(0)$ is called the initial condition. Iterating this function with newly obtained value as initial condition, one can get the sequence of desired length associated with the map i.e. $x(0),\ x(1) = \mathcal{M}(x(0)),\ x(2) = \mathcal{M}(x(1)), ...$ Further, the different values of $x(0)$ are resulted in different sequences. The obtained sequence is called the orbit of the map associated with $x(0)$. In order to check the chaoticity of a map, Lyapunov exponent(LE) and Invariant measure (IM) are considered [15]. The mathematical definition of these measures are given as

– Lyapunov Exponent (LE): The LE of the map shows the divergence rate between nearby orbits. It is defined as:

$$\lambda = \lim_{L\to\infty} \frac{1}{L} \sum_{l=0}^{L-1} \ln |\mathcal{M}'(x(l))| \tag{5}$$

– Invariant Measure (IM): Invariant measure $\rho(x)$ determines the density of the map which further shows the uniformity of map and defined as

$$\rho(x) = \lim_{L\to\infty} \frac{1}{L} \sum_{l=0}^{L} \delta|x - \mathcal{M}(x(l))| \tag{6}$$

If $\rho(x)$ does not depend on initial condition $x(0)$, the map uniformly covers the interval U and the system is ergodic.

The map $\mathcal{M}$ is said to be a linear Markov map [16] if it satisfies the following conditions

1. The map is a piecewise linear one, that is, there exist a set of points $0 = \mu_1 < \mu_2 < \cdots < \mu_M = 1$ and coined as the partition points.
2. The map satisfies the Markov property i.e the partition points are mapped to partition points:

$$\forall i \in [0, M],\ \exists j \in [0, M] : \mathcal{M}(\mu_i) = \mu_j \tag{7}$$

3. The map is eventually expanding i.e. there exist an integer $r > 0$ such that

$$\inf_{x\in[0,1]} \left| \frac{d}{dx} \mathcal{M}^r(x) \right| > 1 \tag{8}$$

For brevity, any map satisfying the above definition will be referred to Markov maps. Any sequence obtained by Markov map are having exponential autocorrelation function and uniform distribution. Another main property, which make Markov maps better than others is that their spectral characteristics are completely controlled by the parameters of the map (μ). An example of Markov map with very interesting properties is the skew tent map which is illustrated in figure 2(I) and can be expressed as

$$\mathcal{M}(x) = \begin{cases} \dfrac{x}{\mu}, & x \in [0,\ \mu] \\ \dfrac{x}{\mu - 1} + \dfrac{1}{\mu - 1}, & x \in (\mu,\ 1] \end{cases} \tag{9}$$

The above described skew tent map is further modified in order to get more better properties. The extended/generalized skew tent map is illustrated in figure 2(II) and given by

$$\widetilde{\mathcal{M}}(x) = \begin{cases} \dfrac{2x}{\mu + 1} + \dfrac{1 - \mu}{1 + \mu}, & x \in [-1,\ \mu] \\ \dfrac{2x}{\mu - 1} + \dfrac{\mu + 1}{\mu - 1}, & x \in (\mu,\ 1] \end{cases} \tag{10}$$

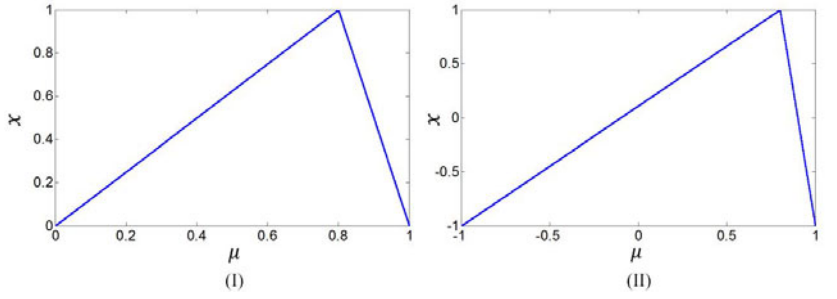

Fig. 2. I) Skew-tent Map II) Generalized Skew-tent Map

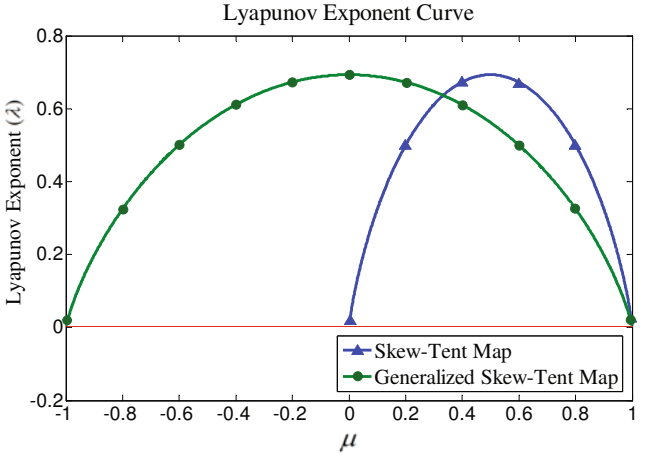

Fig. 3. Lypunov Exponent Curve for Skew-tent map (Eqn. 9) and its generalized version (Eqn. 10)

Unlike skew-tent map, the generalized skew-tent map mapped (-1,1) to (-1,1) with $\mu \in (-1, 1)$. Therefore, the domain and range for the generalized map is twice with more possible values of μ, when compare to traditional skew-tent map. Using Eqn. 5, one can verify that the LE of skew-tent map and its generalized version are

$$\begin{aligned} \lambda_{\mathcal{M}} &= -\mu \ln(\mu) + (1-\mu) \ln\left(\frac{1}{1-\mu}\right) > 0 \\ \lambda_{\widetilde{\mathcal{M}}} &= \frac{\mu+1}{2} \ln(\frac{2}{\mu+1}) + \frac{1-\mu}{2} \ln(\frac{2}{1-\mu}) > 0 \end{aligned} \tag{11}$$

The positive value of LE for all μ (Eqn. 11) shows the chaoticity of the maps. The Lypunov exponent curve for both the maps are depicted in figure 3 which again shows the chaotic nature of the maps in whole domain. Similarly, using Eqn. 6, one can obtain the IM for the skew-tent map and its generalized version and are given by

$$\rho_{\mathcal{M}} = 1 \text{ and } \rho_{\widetilde{\mathcal{M}}} = \frac{1}{2} \tag{12}$$

From Eqn. 12 it is clear that IM is independent of initial guess. Hence, the map uniformly covers the interval U and the system is ergodic. In the present work, we have used generalized skew-tent map due to its merit over skew-tent map i.e. bigger range for x and μ.

5 Proposed Technique

In this section, the motivating factors in the design of proposed image encryption framework are discussed. The proposed technique uses an image and gives an encrypted image which can be decrypted later for various purposes. Without loss of generality, assume that F represents the original image of size $M \times N$ $(M < N)$. The proposed technique can be described as follows:

5.1 Encryption Process

1. *First Phase:* Scramble image pixel positions using toral automorphism by iterating it l times with selected $a,\ b,\ c$ and d. The values of $a,\ b,\ c,\ d$ and l are secret and used as the keys. Let us denote l times scrambled image by F_s^l.
2. By adopting k_0 and μ as the keys, iterate generalized skew-tent map (Eqn. 10) to generate $M \times N$ values $\{k_i :\ i = 1, 2, ..., M \times N\}$.
3. Map the obtained chaotic sequence k into an integer sequence z as follows

$$\text{if } \frac{j}{M \times N} \leq k_i < \frac{j+1}{M \times N}, \text{ then } z_i = j \tag{13}$$

   where $j = 1, 2, 3, ..., M \times N$.
4. Arrange integer sequence z into a random matrix (Z) of size $M \times N$ followed by SVD on it.

$$Z = U_Z\ S_Z\ V_Z^T \tag{14}$$

5. Obtain a Hankel Matrix with the help of singular values of Z i.e. $S_Z = \{\sigma_p |\ p = 1, 2, ..., r(= min(M, N))\}$, denoted by H_Z and given by

$$H_Z = \begin{pmatrix} \sigma_1 & \sigma_2 & \sigma_3 & \cdots & \sigma_{r-1} & \sigma_r \\ \sigma_2 & \sigma_3 & \sigma_4 & \cdots & \sigma_r & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ \sigma_{r-1} & \sigma_r & 0 & \cdots & 0 & 0 \\ \sigma_r & 0 & 0 & \cdots & 0 & 0 \end{pmatrix} \tag{15}$$

6. Perform SVD on obtained Hankel matrix.

$$H_Z = U_{H_Z}\ S_{H_Z}\ V_{H_Z}^T \tag{16}$$

7. Obtain the matrix key ($\mathcal{K}$) by U_{H_Z} and V_{H_Z} as

$$\mathcal{K} = U_{H_Z} V_{H_Z}^T \tag{17}$$

where the matrix key $\mathcal{K}$ is an orthogonal matrix i.e. $\mathcal{K}\mathcal{K}^T = I$. Since, it is the multiplication of two orthogonal matrices.

8. *Second Phase:* Change the pixel values of scrambled image using matrix key $\mathcal{K}$ to get encrypted image F^e as

$$F^e = \mathcal{K} F_s^l \tag{18}$$

5.2 Decryption Process

The decryption process consists of the following steps:

1. By adopting keys k_0 and μ, **step 2** to **step 7** of encryption process are performed to get matrix key $\mathcal{K}$.
2. Obtain the decrypted scrambled image from F^e with the help of matrix key i.e.

$$\widetilde{F}_s^l = inv(K) F^e = K^T F^e \tag{19}$$

3. Scramble pixels of $\widetilde{F}_s^l$, $P - l$ times to get decrypted image (F^d), where P is the period of toral automorphism for the original image F.

6 Experiments and Security Analysis

The performance of proposed encryption technique is demonstrated using MATLAB platform. A number of experiments are performed on different gray scale images namely Barbara, Lena and Cameraman, which are used as original image having size 256×256. Due to page restriction the visual results are given only for Barbara image whereas numerical results are given for all images. In the proposed technique, seven parameters are used as the keys, these parameters are $a,\ b,\ c,\ d,\ l,\ \mu$ and k_0. The first five keys are used as the parameters for toral automorphism and are taken as $a = 8$, $b = 5$, $c = 3$, $d = 2$ and $l = 150$. For making matrix key, $\mu = -0.3456$ and $k_0 = 0.8$ are used as the initial parameters for the Markov map. The encrypted and decrypted images using above mentioned keys are shown in figures 4(II, III).

Security is a major issue of encryption techniques. A good encryption technique should be robust against all kinds of cryptanalytic, statistical and brute-force attacks. In this section, a complete investigation is made on the security of the proposed encryption technique such as sensitivity analysis, statistical analysis, numeric analysis etc to prove that the proposed encryption technique is secure against the most common attacks. The detailed analysis are given as follows.

6.1 Key Sensitivity Analysis

According to the principle, the slight change in the keys never gives the perfect decryption for a good security. And for this purpose, the key sensitivity of the proposed technique is validated. In the proposed technique, seven keys ($a,\ b,\ c,\ d,\ l,\ \mu$ and k_0) are used. Keys $a,\ b,\ c,\ d$ are used in the toral automorphism to form the matrix A. First

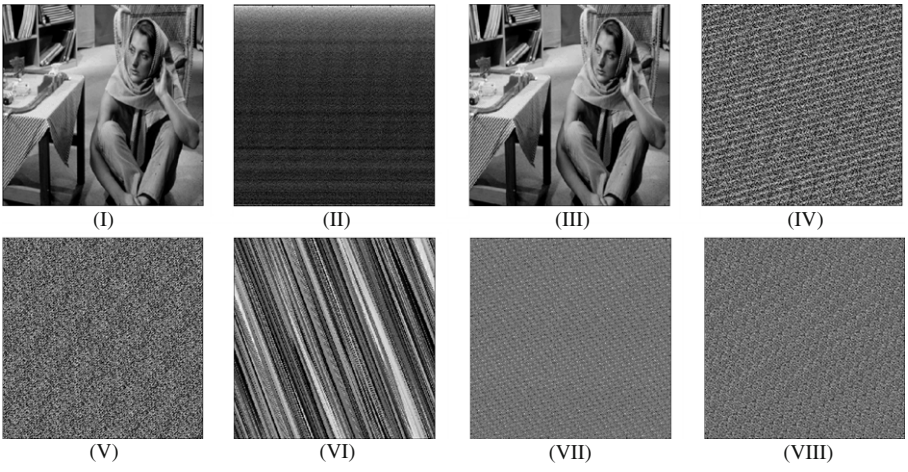

Fig. 4. I) Original Image II) Encrypted Image; Decrypted Image III) with all correct keys IV) with swapped values of a and d V) with wrong $a,\ b,\ c$ and d ($a = 12,\ b = 7,\ c = 5,\ d = 3$) VI) with wrong l ($l = 151$) VII) with wrong k_0 ($k_0 = 0.7999$) VIII) with wrong μ ($\mu = 0.3455$)

check these keys sensitivity, for this the values of the leading diagonal are swapped (i.e. swap a and d) and all other keys remain un-altered. The respective result is shown in figure 4(IV). It is clear that after swapping only two values one cannot get the correct decrypted image. Hence, the proposed technique is highly sensitive to $a,\ b,\ c,\ d$. Figure 4(V) shows the decrypted image when all of $a,\ b,\ c,\ d$ ($a = 12,\ b = 7,\ c = 5,\ d = 3$) are changed. Figures 4 (VI-VIII) show the decrypted images when l, k_0 and μ are wrong respectively. Since, l represents the number of iteration of toral automorphism which is always an integer. Hence, for slight change, either l is decreased or increased by 1. Figure 4(VI) shows the result when l is increased by 1. Similarly, figure 4(VII, VIII) show the results of change in k_0 and μ. The changes are made in the way such that older values ($k_0 = 0.8, \mu = 3.8$) and newer values ($k_0 = 0.7999, \mu = -0.3455$) are approximately same. Hence, the proposed technique is highly sensitive to the keys.

6.2 Statistical Analysis: Histogram and Correlation Analysis

Another method to evaluate encryption technique is statistical analysis. This analysis is composed of two terms viz. 1) Histogram analysis 2) Correlation analysis. According to first term, for a good encryption technique, there is uniform change in the image histogram after encryption. Figure 5(I, II) show the histograms of both original and encrypted images. From figures, it is clear that after encryption histogram becomes uniform. The second term says that a good encryption technique must break the correlation among the adjacent pixels of the image. For this purpose, the correlation between two adjacent pixels are calculated and it is said to be good encryption if correlation come to be as far as from 1. First, randomly select $\mathcal{P}$ pairs of adjacent pixels (either in horizontally or vertically or diagonally) and then calculate their correlation as

$$r_{x,y} = \frac{E(x - E(x))(y - E(y))}{\sqrt{E(x^2) - (E(x))^2}\ \sqrt{E(y^2) - (E(y))^2}} \tag{20}$$

where x and y are the gray levels of two adjacent pixels in the image and $E()$ denotes the expected (mean) value. Figures 5(III, IV) show the correlation distribution of two horizontally adjacent pixels in the original and encrypted image. The correlation coefficients in all directions are shown in table 1, which are far apart. Hence, proposed technique is able to break the high correlation among the pixels.

Table 1. Correlation coefficients of two adjacent pixels in original and encrypted image

Direction	Correlation coefficients in					
	Original Image			Encrypted image		
Image	Barbara	Lena	Cameraman	Barbara	Lena	Cameraman
Horizontal	0.9682	0.9826	0.9862	-0.1107	0.0914	-0.0716
Vertical	0.9257	0.9551	0.9675	-0.1123	-0.0029	-0.0156
Diagonal	0.9514	0.9753	0.9539	0.0083	0.0601	0.0831

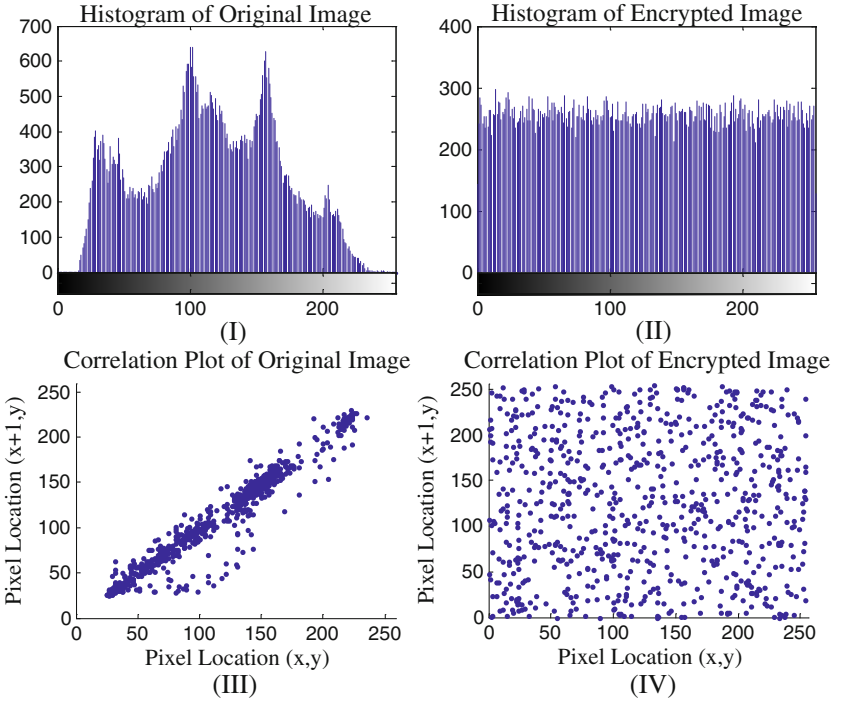

Fig. 5. Histogram of I) Original Image II) Encrypted Image; Correlation plot of two horizontal adjacent pixels in III) Original Image IV) Encrypted image

6.3 Numerical Analysis

Finally numerical analysis is done to evaluate the proposed framework. Numerical analysis includes the values of the objective metrics. A metric which provides more efficient test methods and is suitable for computer simulations is called objective metrics. Peak signal to noise ration (PSNR), spectral distortion (SD), normalized singular value similarity (NSvS) [17] and Universal Image Quality Index (UIQ) [18] are used as the objective metrics to evaluate proposed technique. Table 2 shows the values of objective metrics between original-encrypted and original-decrypted images with correct keys, for all experimental images. From the table, it is clear that for encryption/decryption the values of objective metrics is higher/lower according to their definition mentioned above. Therefore, the proposed technique is able to perfectly encrypt and decrypt the images.

Table 2. Numerical analysis of proposed technique

Metric	Values b/w Original Image and					
	Encrypted Image			Decrypted Image		
Image	Barbara	Lena	Cameraman	Barbara	Lena	Cameraman
PSNR	10.3969	9.7845	10.3575	235.7433	231.7721	237.0556
SD	60.1270	57.7603	62.5469	0.0469	0.0344	0.0952
NSvS	120.9058	129.5549	121.8048	2.1419×10^{-3}	5.8935×10^{-3}	2.0451×10^{-3}
UIQ	2.2958×10^{-4}	4.8305×10^{-4}	1.2363×10^{-4}	1	0.9994	0.9959

7 Conclusions

This paper proposes a simple yet efficient image encryption technique that encrypts the image using toral automorphism, Markov map and singular value decomposition. Toral automorphism is used for scrambling of pixels whereas Markov map and singular value decomposition is used for changing the pixel value. Some security analysis is also given to demonstrate that the right combination of keys is important to reveal the original image. The security analysis proves the efficiency and robustness of the proposed technique. The algorithm is suitable for any kind of gray scale image with which can be further extended for color images. This extension can be easily done by either employing proposed technique separately to all color channels or converting original image to some independent space (like YCbCr) and applying the proposed technique.

Acknowledgement

This work is supported by the Canada Research Chair program, the NSERC Discovery Grant. One of the authors, Dr. B. Raman acknowledges DST for the collaboration of CVSS Lab, University of Windsor during his BOYSCAST fellowship tenure awarded by DST, India.

References

1. Maniccam, S.S., Bourbakis, N.G.: Image and Video Encryption using Scan Patterns. Pattern Recognition 37, 725–737 (2004)
2. Bourbakis, N.: Image Data Compression Encryption using G-SCAN Patterns. In: Proceedings of IEEE Conference on SMC, Orlando, FL, pp. 1117–1120 (1997)
3. Guan, Z.H., Huang, F., Guan, W.: Chaos-based Image Encryption Algorithm. Physics Letters A 346, 153–157 (2005)
4. Gao, H., Zhang, Y., Liang, S., Li, D.: A New Chaotic Algorithm for Image Encryption. Chaos, Solitons and Fractals 29(2), 393–399 (2005)
5. Tong, X., Cui, M.: Image encryption scheme based on 3D baker with dynamical compound chaotic sequence cipher generator. Signal Processing 89(4), 480–491 (2009)
6. Gaoa, T., Chen, Z.: A new image encryption algorithm based on hyper-chaos. Physics Letters A 372(4), 394–400 (2008)
7. Gao, H., Zhang, Y., Liang, S., Li, D.: A new chaotic algorithm for image encryption. Chaos, Solitons and Fractals 29(2), 393–399 (2006)
8. Gao, T.G., Chen, Z.Q.: Image encryption based on a new total shuffling algorithm. Chaos, Solitons and Fractals 38(1), 213–220 (2008)
9. Chang, L.: Large Encrypting of Binary Images with Higher Security. Pattern Recognition Letters 19(5), 461–468 (1998)
10. Li, X.: Image Compression and Encryption using Tree Structures. Pattern Recognition Letters 18(11), 1253–1259 (1997)
11. Chuang, T., Lin, J.: New Approach to Image Encryption. Journal of Electronic Imaging 7(2), 350–356 (1998)
12. Chuang, T., Lin, J.: A New Multiresolution Approach to Still Image Encryption. Pattern Recognition and Image Analysis 9(3), 431–436 (1999)
13. Pollicott, M., Yuri, M.: Dynamical systems and ergodic theory, Cambridge. London Mathematical Society Student Text Series (1998)
14. Golub, G.H., Reinsch, C.: Singular value decomposition and least squares solutions. Numerische Mathematik 14(5), 403–420 (1970)
15. Schuster, H.G., Just, W.: Deterministic Chaos. Wiley-VCH (2005)
16. Tefas, A., Nikolaidis, A., Nikolaidis, N., Solachidis, V., Tsekeridou, S., Pitas, I.: Performance analysis of correlation-based watermarking schemes employing markov chaotic sequences. IEEE Transactions on Signal Processing 51(7), 1979–1994 (2003)
17. Bhatnagar, G., Raman, B.: Distributed multiresolution discrete Fourier transform and its application to watermarking. International Journal of Wavelets, Multiresolution and Information Processing 8(2), 225–241 (2010)
18. Wang, Z., Bovik, A.C.: A Universal Image Quality Index. IEEE Signal Processing Letters 9(3), 81–84 (2002)