International Research Journal of Applied and Basic Sciences
© 2015 Available online at www.irjabs.com
ISSN 2251-838X / Vol, 9 (9): 1627-1635
Science Explorer Publications

IRJABS

Cryptography in social networks using wavelet transform, fractals and chaotic functions

Siavash Sattari[1], Abbas Akkasi[2], Ramin Ahmadi Lari[1], Mohammad Khodaparasti[1]

1. Computer Engineering Department of Islamic Azad University Science and Research Branch, Larestan, Iran.
2. Computer Engineering Department of Islamic Azad University Science and Research Branch, Tehran, Iran.

Corresponding Author email: Siavash.Sattari1@gmail.com

ABSTRACT: In the past two decades, with respect to development of technologies related to the data transmission and social networks, need for secure communications is strongly felt. The proposed encryption method in this paper is based on the combination of chaotic systems, wavelet transform and fractal key. In the first step of cryptography, the approximated image derived by wavelet transform is extracted. The image size will be reduced in the approximated image and consequently the amount of calculation in proposed method will be reduced as well. In the second step of cryptography, the pattern derived by fractals has been used as encryption key. The advantage of this step is separate encryption on each three layers of image, R, G, and B. In the third step of cryptography, the pixels of image which is obtained in second step will be permuted through appropriate scheme based on logistic sequence. Finally in the last step, the pixels of image which is obtained in previous step will be substituted through chaos functions. Results related to the correlation between pixels in encrypted and decrypted images indicate that the correlation between pixels of encrypted image will tend to zero when the chaos function and fractal key are used in cryptography. In the encrypted image, the correlation coefficient between adjacent pixels is close to zero and in the decrypted image, this coefficient is close to one. Using PSNR test, encryption strength can be realized. As the fractals is used for encryption, we can create the encryption key using adjacent pixels. The more pixels used in encryption get the lower PSNR rate.
Keywords: cryptography, wavelet transform, chaotic function, fractals.

INTRODUCTION

Nowadays social network has changed the communication style. Users can simply send various multimedia information through the network. Regarding to convenient access and development of network, the security and reliability of network must be considered as a challenge. The image of users have important information of multimedia communication, thus the data protection is a global issue. Today regarding the development and extension of general communication networks and unauthorized access to private information of individuals or legal has caused the cryptography to be considered more than before. Beside its complication, the Knowledge of encryption has its unique attractiveness and features which themselves are taken from mathematics. In evolvement, with the conversion art into a science of cryptography, a lot of methods have been developed to encrypt and hide the information in form of classical methods which over time and using them in real terms, their characteristics and strengths and weaknesses are analyzed and some classified methods have been proposed to penetrate them. Traditional methods of image encryption such as DES, IDEA and AES due to save images in different formats, is not recommended for image encryption. In recent years numerous approaches have been proposed for image encryption. Diffusion and confusion processes proposed by Shannon in coding are used in cryptography successfully. In diffusion in order to disrupt the high correlation among pixels, the position of pixels will change. In replacement step, the pixel values of image will change. Chaotic mapping is often used to generate pseudorandom sequence and disarrange the pixels. Chaos functions are highly sensitive to initial conditions and by using more than one map chaos, a larger space can be achieved [1].

Other tool used in this paper is wavelet transform. Wavelet analysis is a mathematical tool which is developed in recent decades and employed in various practical fields such as image and speech processing. Wavelet transform has good optimization features in time domain of frequency or space domain. For this reason

the wavelet transform is appropriate for image processing or encryption. According to principles of cryptography, one characteristic of encryption is large enough key space, so in this paper it has been considered.

In second section of this paper the recent proposed algorithms of cryptography have been reviewed. In third section, the encryption tools used in this paper have been described and analyzed and in forth section the proposed method has been investigated. In fifth section, performance of the proposed algorithm will be challenged through simulation and finally in sixth section according to results the conclusion will be introduced.

Related works

As mentioned in the introduction, due to their close commonalities of the chaotic functions with the concepts of cryptography, they have been known as an appropriate tool for encryption. The most important feature of chaotic systems, which makes them used to encrypt image, are dependence on initial conditions and control parameters. Over the past decade, many encryption methods have been proposed based on chaotic signal. In some of these using a one-dimensional chaotic sequence, the key sequence is generated. Thus the arrangement and the pixel values of the image change based on chaotic key sequence [2-3] and [13-16]. Further category of cryptographic techniques, due to the nature of the two-dimensional image, use two-dimensional key sequence. Most of these methods belong to the category of block encryption [4], [5]. Further category of these methods belong to the category of sequence encryption which is suitable for instantaneous encryption [6]. In [7] and [8] a method has been proposed which generate a random sequence using linear multivalued chaos function at beginning. Then through this sequence, the replacement matrix is generated and through this matrix, the image is encrypted. In [9] using the four-variable hyper-chaos function a method has been introduced such that the output of encryption is dependent on the total pixels in the original image. In [10], fractal images are used as a source of randomness to generate a strong encryption key. In this reference, the proposed algorithm can determine the strength of encryption. This algorithm can encrypt three layer of images separately. In [11] an image encryption method based on chaotic signal has been introduced which uses the Peter de jong attractors. In this method, the image is transformed into the wavelet space then the wavelet coefficients are encrypted appropriately. Due to reduce computation time as well as increasing security of image, the wavelet transform is employed in cryptography [5].

Employed tools

In this section the employed tools in the proposed algorithm will be described briefly.

Wavelet transform

Signal processing using wavelet transform is a new method for signal processing. Most applications of wavelets is to simplify and clean up the signal from the noise. Wavelet transform can detect some aspect of signal which other transforms cannot. Another applications of wavelet transform are compression and removing noise from the signal without perceptible loss. In fact, it's can be said that the wavelet is an inevitable and necessary tool for analysis. Wavelet is a waveform with zero mean, limited time and asymmetric shape. In wavelet analysis, signals are decomposed into shifted signals and scaled signals of original wavelet. The continuous wavelet transform function (CWT) can be defined as Eq.1:

$$C(scale, position) = \int_{-\infty}^{+\infty} f(t)\psi(scale, position, t)dt$$

In above equation, the CWT includes a variety of wavelet coefficients which are depended to scale and position where the $\psi(scale, position, t)$ is shifted and scaled function of original signal.

In most of signals, the main information are located in the low frequencies and in fact this part of signal is the identity of signal.

The details of signal and supplementary information are located in high frequencies. For example consider an image. If the high frequency information of image to be removed, the signal of image will change but yet the image is understood. But if the low frequency information of image to be removed, then the image will be unclear. Through wavelet transform the unnecessary details of image are removed to reduce the amount of computation. Wavelet transform are applied on the images to separate 4 groups HH, LH, HL and LL which represent diagonal features of image, reflect vertical information, correspond to horizontal structures and the coefficients from low-pass filtering in both direction, respectively [5]. The forth group (LL) contains the main information of image and other groups contain the edge information. After applying the wavelet transform on the original signal, a new signal will be generated which used in second step of proposed algorithm.

Fractals

A fractal is a natural phenomenon or a mathematical set that exhibits a repeating pattern that displays at every scale [12]. Whereas the structure of fractals appear irregular, but they have a regularity in themselves. This property can be used to generate the key of encryption. The fractal which is used in this paper is Mandelbrot fractal which describe by Eq.2 as below:

$$P_c : C \to C$$

$$P_c : Z \to Z^2 + c$$

Where C and c are the set of complex numbers and a complex parameter, respectively. For each value of c the behavior of sequence will be as below:

$$\left\{0, P_c(0), P_c\left(P_c(0)\right), P_c\left(P_c\left(P_c(0)\right)\right), ...\right\}$$

Each fractal contains a set of initial parameters which based on these, fractals will be different from each other. The sensitivity of fractals relative to initial parameters is very high. So if one of these parameters change an extremely small amount such as ε, the coordinates of all points in the fractal will change. Therefore the fractals can be used to generate the encryption key.

Chaotic systems

As mentioned in part 2, the chaotic systems such as fractals have a regular irregularity in themselves which this regularity has distinguished these systems from random systems. In this paper, Chen chaotic systems have been employed to generate chaotic sequence. The multivalued Chen function will be as below [2]:

$$\begin{cases} \dot{x}_1 = \mathrm{a}\left(x_2 - x_1\right) \\ \dot{x}_2 = -x_1 x_3 + \mathrm{d}x_1 + \mathrm{c}x_2 - x_4 \\ \dot{x}_3 = x_1 x_2 - \mathrm{b}x_3 \\ \dot{x}_4 = x_1 + \mathrm{k} \end{cases}$$

Where a, b, c, d and k are the initial parameters of this system. Therefore according to Eq.4, a chaotic sequence with desired length can be generated to create the encryption key.

Proposed algorithm

In this section the proposed algorithm of this paper is introduced. As depicted in Fig.1, the proposed algorithm has been composed from several parts which used some tools.

As mentioned in previous sections, the wavelet transform, chaotic functions and fractals can be used to encrypt images. Each of these tools has its own advantages and disadvantages which combination of them must be used to minimize their weaknesses and maximize the strength of encryption. The proposed algorithm includes 3 following steps:

Applying the wavelet transform on original image.

Encrypting the image which is derived from step 1 using fractals.

Encrypting the image which is derived from step 2 using chaotic functions.

In proposed method, first by two-dimensional “haar” wavelet transform, the estimated image of original image is derived. Therefore the resulting image size is a quarter of original image size. Since the output values of wavelet transform can be non-integer or negative values, so it is necessary to extract only integer and positive values. Thus three matrices are extracted from estimated image as following:

The matrix corresponding to the integer values which is equal to rounded absolute value of estimated matrix.

Matrix corresponding to the decimal digits.

Matrix corresponding to the sign. If the element sign of estimated matrix was negative, the element value of this matrix will be one, otherwise this will be zero.

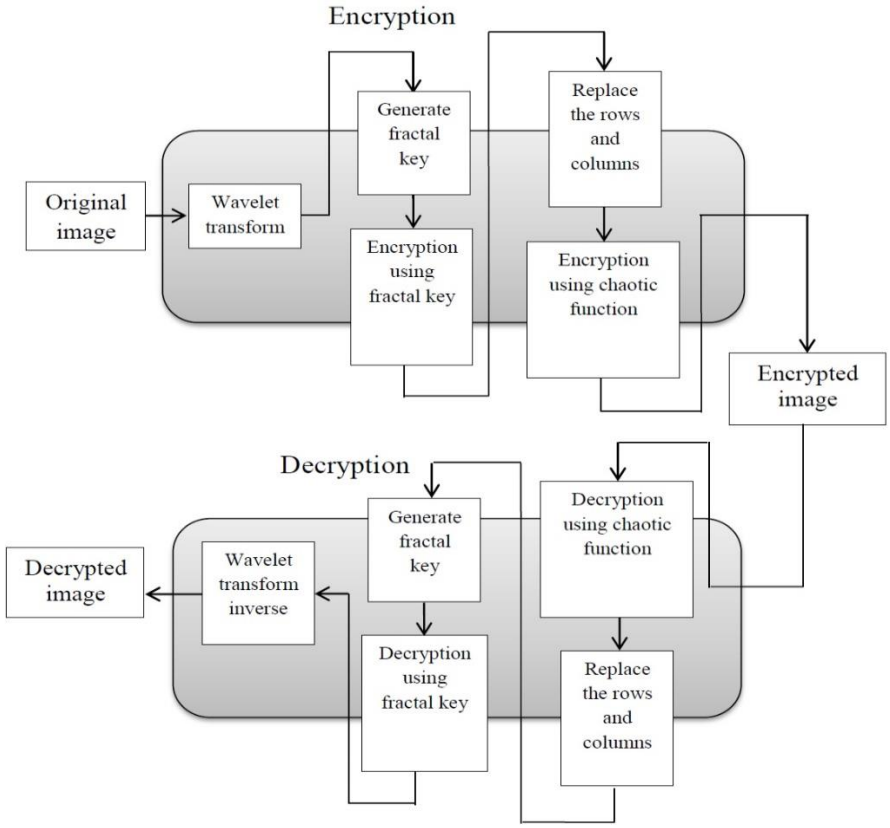


Figure1. the proposed algorithm

In second step of proposed method, the matrix derived in previous step is used as input image for encryption through fractals. If the size of estimated image is considered with m×n, the size of each layers of that image would be m×n. Also the layers of fractal matrix which encryption key is extracted through those, are shown with R_{key}, G_{key} and B_{key}, respectively. Also the size of fractal matrix must to be m×n. the first part of second step of proposed algorithm will be as following [12]:

$$\forall D \in R_{key}, G_{key}, B_{key}$$

$$\exists D' : \forall i \in [1,m],\ j \in [1,n]$$

$$d'_{ij} = \sum_{k=1}^{k_{\max}} \left(\sum_{l=1}^{l_{\max}} r(i,j,k,l) \times d_{K,L} \right)$$

Where:

$$k_{\max} = \left\lfloor \frac{i-1}{\delta+1} \right\rfloor + \left\lfloor \frac{m-1}{\delta+1} \right\rfloor + 1$$

$$l_{\max} = \left\lfloor \frac{j-1}{\delta+1} \right\rfloor + \left\lfloor \frac{n-1}{\delta+1} \right\rfloor + 1$$

$$K = i - \left\lfloor \frac{i-1}{\delta+1} \right\rfloor \times (\delta+1) + (k-1) \times (\delta+1)$$

$$L = j - \left\lfloor \frac{j-1}{\delta+1} \right\rfloor \times (\delta+1) + (l-1) \times (\delta+1)$$

$$r(i,j,k,l) = \sqrt{[K-i]^2 + [L-j]^2}$$

For each pixels of image, a grid with spatial parameter δ is created. The smaller the δ gets a grid with further pixels and better encryption. The weight coefficient *r*(*i,j,k,l*) is used to be difference among d'_{ij} values. Thus, despite the weight coefficient the encryption would be better. The matrix elements of D' will be distinct from each other and this indicates strength of the encryption. Fig.2 has been depicted how to generate the encryption key using δ.

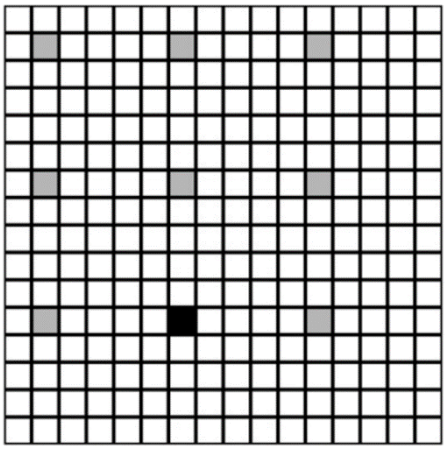


Figure 2. Encryption using fractal key. This indicates the grid of one of 3 layers of fractal image which is used for encryption with spatial parameter δ = 4. The black cell is the pixel which based on this the key matrix D' would be generated. The gray cells are the effective pixels on the encryption of black cell [12].

Regarding to computational complexity, the second part of second step of proposed method is much simpler from the first part and uses only a sum operation as following [12]:

$$\forall E \in R, G, B$$

$$\exists E'_{m\times n} : \forall i \in [1, m],\ j \in [1, n]$$

$$e'_{ij} = \left(e_{ij} + d'_{ij}\right) \bmod (256)$$

Note that the above process for each layer of image should be implemented. After applying second step, the image which is extracted from previous step must be encrypted through chaotic functions which includes two part. The first part is related to replacement the rows and columns of derived image from previous step according to following logistic function [2]:

$$x_{n+1} = 4x_n\left(1 - x_n\right)$$

In Eq.7, the sequence is begun through an initial x_0. The above sequence is repeated for several times until a new x_0 achieved such that it satisfies the following equation:

$$l = \bmod(x_0 \times 10^{14}, M)$$

In above equation, M can be the number of rows or columns of image matrix. Note that the value of *l* must be limited in range [0 , M-1] and distinct from each other. Thus the rows and columns of the matrix of encrypted image in the previous stage, will be replaced by the vector *l* such that the number which is located in *i*'th index of vector *l* will be the new number of *i*'th row or column of encrypted image.

In second part of this step, a chaotic system is employed to encrypt the derived image from previous part and for this purpose, the Chen chaotic system has been used. After generating the chaotic sequences of Chen system, each sequence is preprocessed as following:

$$x_i = \bmod\left(\left(\left|x_i\right| - \left\lfloor \left|x_i\right| \right\rfloor\right) \times 10^{14}, 256\right)$$

Now through Eq.10, the table 1 is created which used for encryption:

$$\bar{x}_1 = \bmod\left(x_1, 4\right)$$

Table.1 the serial numbers have been created by one of chaotic sequences such as x_1.

Corresponding mode	Serial number
(x_1, x_2, x_3)	0
(x_1, x_2, x_4)	1
(x_1, x_3, x_4)	2
(x_2, x_3, x_4)	3

As shown in Table 1, the serial number is corresponded to $\bar{x}_1$ values and according to table 1, the value of $\bar{x}_1$ defines the corresponding mode. The corresponding combination of $\bar{x}_1$ do XOR with image pixels according to Eq.11 and the obtained values are token place in encrypted image matrix as encrypted pixel values and the image is encrypted. Note that for using the Eq.11 at the beginning, the matrix of image must to be reshaped as a vector which the size of this vector is product of row number and column number of image matrix.

$$\begin{cases} C_{3\times(i-1)+1} = P_{3\times(i-1)+1} \oplus B_{x_1} \\ C_{3\times(i-1)+2} = P_{3\times(i-1)+2} \oplus B_{x_2} \\ C_{3\times(i-1)+3} = P_{3\times(i-1)+3} \oplus B_{x_3} \end{cases}$$

Where P and C are the pixels of image and pixels of encrypted image, respectively. So the image is encrypted by chaotic functions.

Decryption

Now assume that the encrypted image has been received in receiver. For decryption, the inverse of above steps must to be done. For this purpose, it is necessary to create the Table.1 in receiver. Then according to following and using the XOR operation, the received image is decrypted from chaotic functions.

$$\begin{cases} P_{3\times(i-1)+1} = C_{3\times(i-1)+1} \oplus B_{x_1} \\ P_{3\times(i-1)+2} = C_{3\times(i-1)+2} \oplus B_{x_2} \\ P_{3\times(i-1)+3} = C_{3\times(i-1)+3} \oplus B_{x_3} \end{cases}$$

Then the derived vector in Eq.12 must to be reshaped into matrix form. After this, the rows and columns of matrix must to be return to their initial position. After this step, the fractals are used to decrypt the derived image from previous step. The first part of this step is exactly similar to first part of encryption using fractals. So the matrix D' must to be generated. There is little difference between second part of this step and second part of encryption using fractals such that in this part the subtraction operation is used instead of summation operation as following:

$$\forall E' \in R', G', B'$$

$$\exists E_{m\times n} : \forall i \in [1, m],\ j \in [1, n]$$

$$e_{ij} = \left(e'_{ij} - d'_{ij}\right) \bmod (256)$$

In last step of decryption using the inverse of wavelet transform, the original image will be reconstructed. In next section the results will be simulated and analyzed.

Simulation and results

The used image for simulation of proposed algorithm is famous image of Lena with size 512×512 which is depicted in Fig.3. For simulation the proposed algorithm, it is required to initialize the chaotic function and fractal. In order to create a fractal from Mandelbrot set, the center of this fractal is coordinated on (-0.5, 0) and also its range set on 1.1. With these assumptions and 15 iterations, the fractal is created which is depicted in Fig.4. Note that the image size of fractal must to be equal with original image size. In order to create the key, the δ value is considered to be 20. Also the initial parameters of Chen chaotic system including a, b, c, d and k are considered to be 36, 3, 28, -16 and 0.2, respectively. The encrypted image has been depicted in Fig.5. After decryption in receiver, the decrypted image has been depicted in Fig.6.

Figure 3. Original image

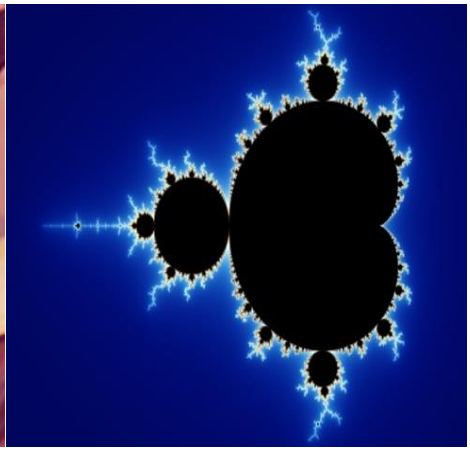


Figure 4. The Mandelbrot fractal

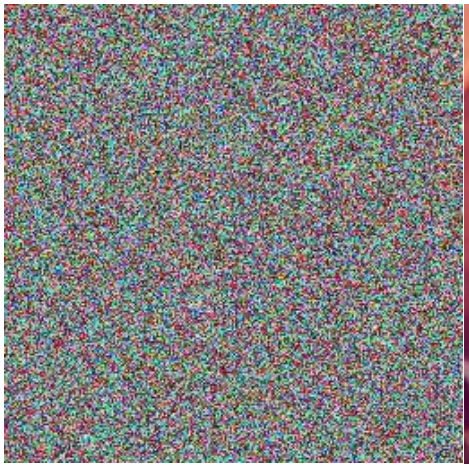


Figure 5. The encrypted image

Figure 6. The decrypted image

PSNR test

As mentioned in above, one of the parameters which is used in encryption using fractals, is the spatial parameter which is shown as δ. The smaller values of δ get the stronger encryption. Through PSNR test the strength of encryption can be defined. Eq.14 shows how to compute the PSNR as following:

$$PSNR = 10\log\left(\frac{MAX^2}{MSE}\right)$$

Where MAX is the maximum gray level of pixels which is usually equal to 255 and MSE also is calculated by Eq.15 as below:

$$MSE = \frac{1}{3mn}\sum_{R,G,B}\sum_{j=1}^{m}\sum_{k=1}^{n}\left(E(j,k)-D(j,k)\right)^2$$

m, n, E, D are the row number of image, column number of image, matrix of encrypted image and matrix of decrypted image, respectively. PSNR test is used to determine the encryption strength and the smaller PSNR indicates the stronger encryption. As mentioned in above, in this algorithm the strength of algorithm is greatly dependent on the value of δ. Therefore it is expected that the lower δ gets the lower PSNR, too. As shown in Fig.7, the PSNR value has been obtained toward various δ.

Correlation between adjacent pixels

To investigate the correlation between adjacent pixels in the horizontal, vertical and diagonal modes in the original images and encrypted image, 10000 pair of adjacent pixels in image is selected, then the correlation coefficient for each pair is calculated as following:

$$E(x)=\frac{1}{2}\sum_{i=1}^{2}x_i$$

$$D(x)=\frac{1}{2}\sum_{i=1}^{2}\left(x_i-E(x)\right)^2$$

$$\mathrm{cov}(x,y)=\frac{1}{2}\sum_{i=1}^{2}\left(x_i-E(x)\right)\left(y_i-E(y)\right)$$

$$r_{x,y}=\frac{\mathrm{cov}(x,y)}{\sqrt{D(x)}\sqrt{D(y)}}$$

Where x and y are the gray level values of two adjacent pixels. In Table.2 the correlation coefficient values for adjacent pixels in the original image and the encrypted image can be seen.

Table 2. The correlation coefficient between the pixels

Adjacent pixels	Original image	Encrypted image
Horizontal mode	0.9366	0.0170
Vertical mode	0.9563	-0.0198
Diagonal mode	0.9090	-0.0107

As seen in Table.2, in encrypted image the correlation coefficients are nearly close to zero. This indicates that through proposed algorithm any correlation between pixels which may help the hackers to decrypt the image in social networks vanish completely. In Fig.8 the correlation between pixels in original image and decrypted image has been depicted.

Sensitivity of encryption key

In order to test the sensitivity of encryption key in receiver side, assume that only one of the initial parameters of fractal change extremely small amount. For this purpose in encryption mode, considered that the center of fractal on x axis be equal to -0.5. To test the sensitivity of encryption key of proposed method in decryption mode, considered that the center of fractal on x axis be equal to -0.500001 and according to initial parameters of fractal, image be decrypted based on proposed algorithm. The decrypted image has been depicted in Fig.9:

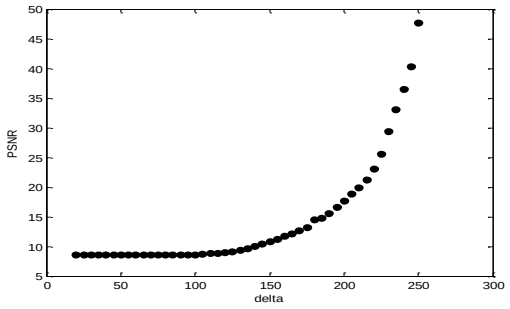
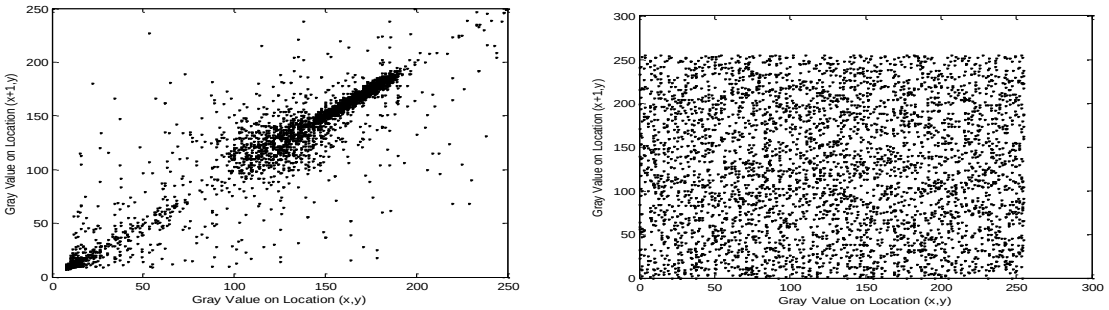


Figure 7. PSNR changes based on δ changes.



a) original image b) encrypted image

Figure 8. the correlation between adjacent pixels

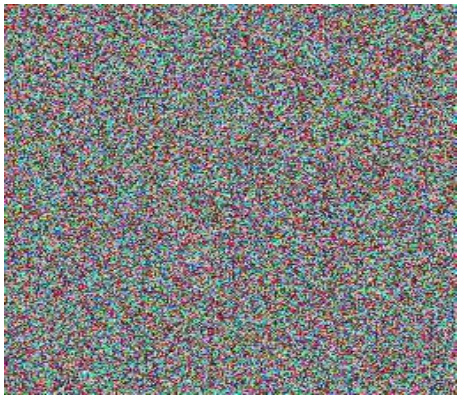


Figure 9. decrypted image through wrong key.

SUMMERY AND CONCLUSION

In this paper, in order to protect private images in social network against hacker attacks, an algorithm has been proposed to encrypt images. In the first step of this algorithm the wavelet transform is used to reduce the computational complexity. In second and third step of this algorithm the fractal key and chaotic functions are used to encrypt the image and increase the strength of encryption, respectively. Through PSNR test, the strength of encryption has been evaluated and also to prevent the decrypting of image by hackers, the correlation between pixels will be tended to zero. This algorithm has a high sensitivity to initial parameters such that with an extremely small amount change in parameter values, the image is not decrypted correctly.

REFERENCES

A novel image fusion encryption algorithm based on DNA sequence operation and hyper-chaotic system. Zhang Q, et al. s.l.: Optik - Int. J. Light Electron Opt, 2013.

A simple, sensitive and secure image encryption algorithm based on hyper-chaotic system with only one round diffusion process. B. Norouzi, S. Mirzakuchaki, S. M. Seyedzadeh, M. R. Mosavi. s.l.: Multimed Tools Appl, Springer, 2012.

A symmetric image encryption scheme based on combination of nonlinear chaotic maps. Akhavan A. et al, Journal of the Franklin Institute, vol 348, 2011. pp. 1797–1813.

An image encryption algorithm based on hyper-chaos and DNA sequence. Huang X, Ye G. s.l.: Multimed Tools Appl, Springer, 2012.

An Improved Chaos-Based Image Encryption Scheme. Fu, Ch., Zhang, Z., Chen, Z., Wang, X. s.l.: ICCS, 2007.

An Improved Image Encryption Algorithm Based on Chaotic Maps. Fu, Ch., Zhang, Z., Cao, Y. s.l.: ICNC, 2007.

Chaos synchronization using sporadic driving. U. Parlitz, L. Kocarev, T. Stojanov, and L. Junge. s.l.: Phys. D., 1997, Vol. 109, pp. 139-152.

Hossam A, Hamdy K, Osama A. 2007.An Efficient Chaos-Based Feedback Stream Cipher (ECBFSC) for Image Encryption and Decryption. Hossam, A., Hamdy, K., Osama. s.l.: Informatica, 2007, Vol. 31.

Image Encryption Based on Chaotic Modulation of Wavelet Coefficients. Xiping He, Qionghua Zhang. s.l.: Congress on Image and Signal Processing, 2008.

Implementation of gray image encryption with pixel shuffling and gray-level encryption by single chaotic system. Huang C.K., Liao C.W., Hsu S.L., Jeng Y.C. s.l.: Telecommunication Systems, 2013, Vol. 52, pp. 563–571.

Implementation of gray image encryption with pixel shuffling and gray-level encryption by single chaotic system. Huang C.K., Liao C.W., Hsu S.L., Jeng Y.C. s.l.: Telecommunication Systems, 2013, Vol. 52, pp. 563–571.

Improvement of an image encryption algorithm based on hyper-chaos. Hermassi H, Rhouma R, BelghithS. s.l.: Telecommunication SystemsSpringer, 2013, Vol. 52, pp. 539–549.

Improving Chaos Image Encryption Speed. Jiri Giesl, Ladislav Behal, Karel Vlcek. 3, s.l.: International Journal of Future Generation Communication and Networking, September 2009, Vol. 2.

Modulo image encryption with fractal keys. Valerij Rozouvan, Optics and Lasersin Engineering, Vol. 47, pp. 1-6, 2009.

Practical Bifurcation and Stability Analysis from Equilibrium to Chaos Second Edition. Seydel, R. s.l.: New York: Springer-Verlag, 1994.

Symmetric Ciphers Based on Two-dimensional Chaotic Maps. Fridrich, J. 0218-1274, s.l.: International Journal of Bifurcation and Chaos, 1998, Vol. 9, pp. 1259-1284.