A chaos-based digital image encryption scheme with an improved diffusion strategy

Chong Fu,[1,*] Jun-jie Chen,[2] Hao Zou,[2] Wei-hong Meng,[3] Yong-feng Zhan,[3] and Ya-wen Yu[1]

[1]*School of Information Science and Engineering, Northeastern University, Shenyang 110004, China*
[2]*Software College, Northeastern University, Shenyang 110004, China*
[3]*Northern Hospital, Shenyang 110016, China*
[*]*fuchong@ise.neu.edu.cn*

Abstract: Chaos-based image cipher has been widely investigated over the last decade or so to meet the increasing demand for real-time secure image transmission over public networks. In this paper, an improved diffusion strategy is proposed to promote the efficiency of the most widely investigated permutation-diffusion type image cipher. By using the novel bidirectional diffusion strategy, the spreading process is significantly accelerated and hence the same level of security can be achieved with fewer overall encryption rounds. Moreover, to further enhance the security of the cryptosystem, a plain-text related chaotic orbit turbulence mechanism is introduced in diffusion procedure by perturbing the control parameter of the employed chaotic system according to the cipher-pixel. Extensive cryptanalysis has been performed on the proposed scheme using differential analysis, key space analysis, various statistical analyses and key sensitivity analysis. Results of our analyses indicate that the new scheme has a satisfactory security level with a low computational complexity, which renders it a good candidate for real-time secure image transmission applications.

OCIS codes: (100.2000) Digital image processing; (110.1758) Computational imaging; (100.2960) Image analysis.

References and links

1. J. Fridrich, "Symmetric ciphers based on two-dimensional chaotic maps," Int. J. Bifurcat. Chaos **8**(6), 1259–1284 (1998).
2. G. R. Chen, Y. B. Mao, and C. K. Chui, "A symmetric image encryption scheme based on 3D chaotic cat maps," Chaos Solitons Fractals **21**(3), 749–761 (2004).
3. Y. B. Mao, G. R. Chen, and S. G. Lian, "A novel fast image encryption scheme based on 3D chaotic baker maps," Int. J. Bifurcat. Chaos **14**(10), 3613–3624 (2004).
4. F. Belkhouche, I. Gokcen, and U. Qidwai, "Chaotic gray-level image transformation," J. Electron. Imaging **14**(4), 043001 (2005).
5. N. K. Pareek, V. Patidar, and K. K. Sud, "Image encryption using chaotic logistic map," Image Vis. Comput. **24**(9), 926–934 (2006).
6. H. S. Kwok and W. K. S. Tang, "A fast image encryption system based on chaotic maps with finite precision representation," Chaos Solitons Fractals **32**(4), 1518–1529 (2007).
7. 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 **366**(4-5), 391–396 (2007).
8. S. Behnia, A. Akhshani, H. Mahmodi, and A. Akhavan, "A novel algorithm for image encryption based on mixture of chaotic maps," Chaos Solitons Fractals **35**(2), 408–419 (2008).
9. T. G. Gao and Z. Q. Chen, "A new image encryption algorithm based on hyper-chaos," Phys. Lett. A **372**(4), 394–400 (2008).
10. X. J. Tong and M. G. Cui, "Image encryption scheme based on 3D baker with dynamical compound chaotic sequence cipher generator," Signal Process. **89**(4), 480–491 (2009).
11. V. Patidar, N. K. Pareek, and K. K. Sud, "A new substitution-diffusion based image cipher using chaotic standard and logistic maps," Commun. Nonlinear Sci. Numer. Simul. **14**(7), 3056–3075 (2009).
12. R. Rhouma, S. Meherzi, and S. Belghith, "OCML-based colour image encryption," Chaos Solitons Fractals **40**(1), 309–318 (2009).

#154920 - $15.00 USD Received 20 Sep 2011; revised 13 Jan 2012; accepted 13 Jan 2012; published 19 Jan 2012

13. F. Y. Sun, S. T. Liu, Z. Q. Li, and Z. W. Lü, "A novel image encryption scheme based on spatial chaos map," Chaos Solitons Fractals **38**(3), 631–640 (2008).
14. C. K. Huang and H. H. Nien, "Multi chaotic systems based pixel shuffle for image encryption," Opt. Commun. **282**(11), 2123–2127 (2009).
15. S. Mazloom and A. M. Eftekhari-Moghadam, "Color image encryption based on coupled nonlinear chaotic map," Chaos Solitons Fractals **42**(3), 1745–1754 (2009).
16. Y. Wang, K. W. Wong, X. F. Liao, T. Xiang, and G. R. Chen, "A chaos-based image encryption algorithm with variable control parameters," Chaos Solitons Fractals **41**(4), 1773–1783 (2009).
17. I. F. Elashry, O. S. F. Allah, A. M. Abbas, S. El-Rabaie, and F. E. A. El-Samie, "Homomorphic image encryption," J. Electron. Imaging **18**(3), 033002 (2009).
18. S. E. Borujeni and M. Eshghi, "Chaotic image encryption design using Tompkins-Paige algorithm," Math. Probl. Eng. **2009**, 762652 (2009).
19. X. Ma, C. Fu, W. M. Lei, and S. Li, "A novel chaos-based image encryption scheme with an improved permutation process," Int. J. Adv. Comput. Technol. **3**(5), 223–233 (2011).
20. S. G. Lian, J. S. Sun, and Z. Q. Wang, "A block cipher based on a suitable use of the chaotic standard map," Chaos Solitons Fractals **26**(1), 117–129 (2005).
21. T. Xiang, K. W. Wong, and X. F. Liao, "Selective image encryption using a spatiotemporal chaotic system," Chaos **17**(2), 023115 (2007).
22. K. W. Wong, B. S. H. Kwok, and W. S. Law, "A fast image encryption scheme based on chaotic standard map," Phys. Lett. A **372**(15), 2645–2652 (2008).
23. K. W. Wong, B. S. H. Kwok, and C. H. Yuen, "An efficient diffusion approach for chaos-based image encryption," Chaos Solitons Fractals **41**(5), 2652–2663 (2009).
24. F. Rannou, "Numerical study of discrete plane area-preserving map," Astron. Astrophys. **31**, 289–301 (1974).
25. A. J. Litchenberg and M. A. Lieberman, *Regular and Stochastic Motion* (Springer, 1983).
26. IEEE Computer Society, "IEEE standard for binary floating-point arithmetic," ANSI/IEEE Std. 754–1985 (1985).
27. G. Alvarez and S. Li, "Some basic cryptographic requirements for chaos-based cryptosystems," Int. J. Bifurcat. Chaos **16**(8), 2129–2151 (2006).

1. Introduction

Since 1990s, many researchers have noticed that there exists close relationship between chaos and cryptography. With the desirable properties of extreme sensitivity to initial condition and parameters, ergodicity, pseudo-randomness, chaotic maps have demonstrated great potential for information especially multimedia encryption. Ever since Fridrich proposed the chaotic image encryption scheme in 1998 [1], there have been increasing researches on chaos-based image cipher. The major core of these systems consists of one or several chaotic maps serving the purpose of either just encrypting the image or shuffling the image and subsequently encrypting the resulting shuffled image [1–23]. Compared with conventional block ciphers such as DES, AES and IDEA, chaos-based algorithms have shown their superior performance in aspect of complexity, speed, computing power and security.

Recently, a number of improvements have been made to chaos-based image encryption techniques and a short summary of these achievements is given hereafter.

(a) Security improvements

In [2, 3], 3D chaotic Cat map and Baker map were employed in permutation stage, respectively. With a larger leading Lyapunov characteristic exponent than that of their 2D version, a better confusion performance is achieved. In [4], Belkhouche et al. proposed a chaotic sequence sorting algorithm based permutation scheme, which can effectively avoid the periodicity of permutation caused by discretization of area-preserving chaotic maps. In [6], Kwok et al. proposed a novel chaos-based pseudo-random keystream generator, which is cascade of a number generator using one-dimensional chaotic map and a mixer based on high-dimensional Cat map. Verified by the National Institute of Standards and Technology (NIST) statistical test suite, it is found the randomness of keystream is enhanced even under finite precision implementation and thus the security of the cryptosystem is improved. In [7], the parameter of nonlinear piecewise chaotic maps was changed by attaching it to the additional trigonometric chaotic maps with the purpose of enhancing the unpredictability of the cryptosystem. In [8, 9, 12], high-dimensional chaotic systems were employed for image encryption in order to overcome the drawbacks of small key space and weak security in widely used one-dimensional chaotic system. In [13, 15], spatial chaos system or coupled nonlinear chaotic map were used for the same purpose. In [16], Wang et al. proposed a chaos-

#154920 - $15.00 USD Received 20 Sep 2011; revised 13 Jan 2012; accepted 13 Jan 2012; published 19 Jan 2012

based image encryption algorithm with variable control parameters with the purpose of avoiding the periodicity of permutation and improving the ability against known/chosen plaintext attack. In [19], a bit-level permutation method was proposed to improve the security of the easy broken confusion module. Since the pixel value mixing effect is contributed by both diffusion module and the improved confusion module, the overall security of the cryptosystem is significantly enhanced.

(b) Efficiency improvements

In [20], a sine table was introduced in permutation procedure in order to reduce the computational complexity of standard map. In [21], Xiang et al. proposed a selective image encryption scheme which only encrypting 50% of the whole image data while the security is acceptable. Therefore, the encryption time is substantially reduced. In [22], Kwok et al. introduced certain diffusion effect in the confusion stage so as to reduce the workload of the time-consuming diffusion module. As a result, the encryption speed is effectively accelerated. In [23], a light-weight table lookup and swapping techniques was proposed to address the efficiency problem encountered by substitution-diffusion type chaos-based image cryptosystems.

As can be seen from above discussion, most of these achievements are focus on security improvements, while only a few are dealing with efficiency issues. For the most widely investigated permutation-diffusion type image cipher, the diffusion is the highest cost of the whole cryptosystem. This is because a considerable amount of computation load is devoted to the real number arithmetic operation and the subsequent quantization required by the key stream generation in the diffusion stage. Therefore, the key problem of design an efficient image cryptosystem is how to either reduce the computational complexity or improve the diffusion effect of the diffusion module. In this paper, we propose a novel bidirectional diffusion strategy which can significantly accelerate the spreading process so as to promote the efficiency of chaos-based image cipher. Moreover, to further enhance the security of the cryptosystem, a plain-text related chaotic orbit turbulence mechanism is introduced in diffusion procedure by perturbing the control parameter of the employed chaotic system according to the cipher-pixel. Experimental results indicate that a satisfactory security level can be obtained with only one cipher cycle by using the new scheme. The remainder of this paper is organized as follows. Section 2 discusses the image shuffling algorithm by using Chirikov standard map. Then the proposed diffusion algorithm is described in Section 3. In Section 4, we analyze the security of the proposed image cipher through various statistical analysis, key space analysis, key sensitivity analysis, etc. Finally, conclusions are drawn in the last section.

2. Image permutation based on Chirikov standard map

Image data have strong correlations among adjacent pixels. Statistical analysis on large amounts of images shows that averagely adjacent 8 to 16 pixels are correlative in horizontal, vertical, and also diagonal directions for both natural and computer-graphical images. In order to decorrelate the strong relationship among adjacent pixels, Chirikov standard map is employed to shuffle the pixel positions of the plain image. The so-called Chirikov standard map is an invertible area-preserving chaotic map from a square with side 2π onto itself [24, 25]. It is defined by

$$\begin{cases} a_{i+1} = (a_i + b_i) \mod 2\pi, \\ b_{i+1} = (b_i + k\sin(a_i + b_i)) \mod 2\pi, \end{cases} \tag{1}$$

where k is the control parameter satisfying $k > 0$, and the ith states a_i and b_i both take real values in $[0, 2\pi)$ for all i.

For $k = 0$, the map is linear and only periodic and quasiperiodic orbit exist. Nonlinearity of the map increases with k, and with it the possibility to observe chaotic dynamics for appropriate initial conditions. Figure 1 illustrates a collection of different orbits (each orbit

#154920 - $15.00 USD Received 20 Sep 2011; revised 13 Jan 2012; accepted 13 Jan 2012; published 19 Jan 2012

starts from a different initial condition) exhibited by the Chirikov standard map for various value of $k > 0$.

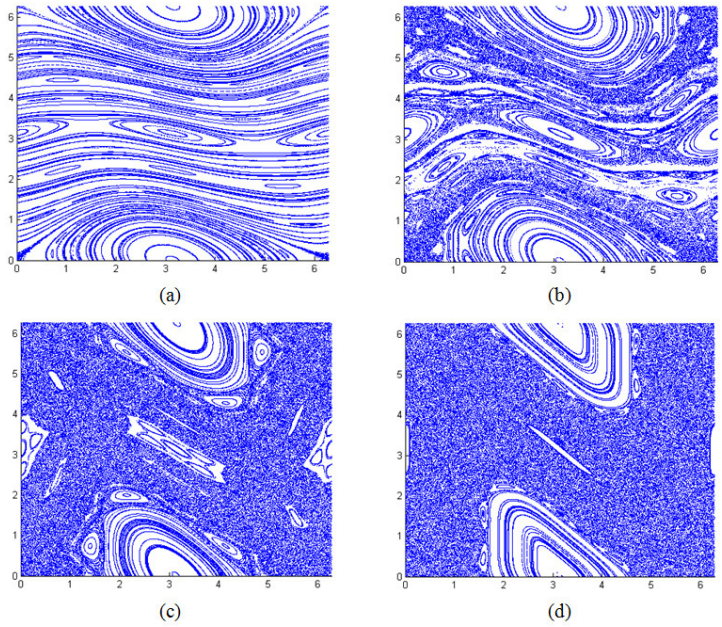


Fig. 1. Chaotic orbits of Chirikov standard map for various k. (a) $k = 0.5$. (b) $k = 1.0$. (c) k=1.5. (d) k=2.0.

For $k = 0.5$, one can see the primary period-1 and period-2 orbits very closely, only local stochasticity near the seperatrix occurs. For $k = 1.0$, the KAM curve between the period-1 and period-2 islands has been destroyed and the chaos is global now, only the islands of stability remain. As the value of k increases, the size of the islands of stability decreases. Therefore, a larger k is much preferred to achieve a satisfactory permutation performance.

In order to incorporate Chirikov standard map into image encryption that operated on a finite set, it has to be discretized. The discretized version Chirikov standard map can be obtained by changing the range of (x, y) from the square $[0, 2\pi)\times[0, 2\pi)$ to the discrete lattice $N\times N$.

$$\begin{cases} x_{i+1} = (x_i + y_i) \mod N, \\ y_{i+1} = (y_i + K \sin \dfrac{2\pi x_{i+1}}{N}) \mod N, \end{cases} \tag{2}$$

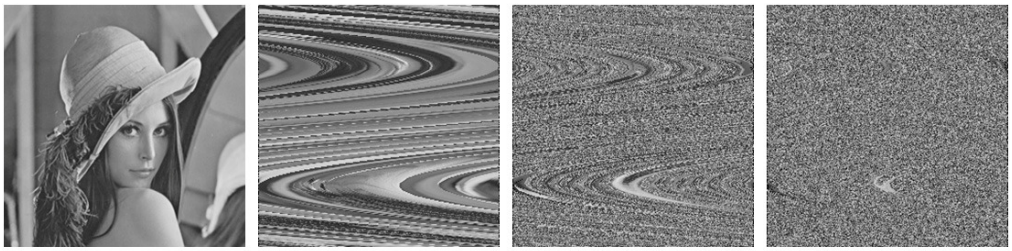
where N is the width or length of a square image, and K is a positive integer which can be used as the permutation key. Although the properties of the discretized map may not be as good as that of the continuous one, most of the useful features are inherited such as the mixing property and the sensitivity to initial conditions and parameters. Since there only exist simple mathematical operations, it is very efficient to shuffle the pixel positions by using the Chirikov standard map.

The inverse transform for deciphering is easily found to be given by

$$\begin{cases} x_{i+1} = (x_i - y_i + K \sin \dfrac{2\pi x_i}{N}) \mod N, \\ y_{i+1} = (y_i - K \sin \dfrac{2\pi x_i}{N}) \mod N. \end{cases} \tag{3}$$

#154920 - $15.00 USD Received 20 Sep 2011; revised 13 Jan 2012; accepted 13 Jan 2012; published 19 Jan 2012

The application of the Chirikov standard map to a grayscale test image with 256 × 256 size is demonstrated in Fig. 2. Figure 2(a) shows the plain image, and Figs. 2(b)-2(d) show the results of applying the discretized Chirikov standard map once, two, and five times, respectively. The ciphering key is K=512.



(a) (b) (c) (d)

Fig. 2. The application of the Chirikov standard map. (a) The test grayscale image with 256 × 256 size. (b) The test image after applying the Chirikov standard map once. (c) The test image after applying the Chirikov standard map three times. (d) The test image after applying the Chirikov standard map five times.

As can be seen from Fig. 2, after five rounds iterations, the correlation among the adjacent pixels is completely disturbed and the image is completely unrecognizable. Unfortunately, the histogram of the shuffled image is the same as that of the plain-image since the permutation operation only shuffles the pixels positions without changing its value. Therefore, the shuffled image is weak against statistical attack and known plain-text attack. As a remedy, we employ a diffusion procedure next to improve the security.

3. Improved image diffusion based on Chebyshev map

In diffusion stage, the pixel values are modified sequentially to confuse the relationship between cipher image and plain image. Chaotic map is used as generation of key stream for diffusion. Usually, the modification made to a particular pixel not only depends on the corresponding key stream element, but also the accumulated effect of all the previous pixel values, as described by

$$c(n) = k(n) \oplus \{[p(n) + k(n)] \bmod N\} \oplus c(n-1), \tag{4}$$

where $p(n)$, $k(n)$, $c(n)$ are the currently operated pixel, key stream element and output cipher-pixel, respectively, and $c(n\text{-}1)$ is the previous cipher-pixel.

Such diffusion strategy makes the cryptosystem secure against differential attack. In general, an opponent may make a slight change, usually one pixel, in the plain image and compare the cipher images (corresponding to very similar plain images and obtained by the same key) to find out some meaningful relationship between plain image and cipher image, which further facilitates in determining the secretary key. If one minor change in the plain image can be effectively diffused to the whole ciphered image, then such differential analysis may become inefficient and practically useless. The diffusion process of conventional chaos-based image cipher is illustrated in Fig. 3.

#154920 - $15.00 USD Received 20 Sep 2011; revised 13 Jan 2012; accepted 13 Jan 2012; published 19 Jan 2012

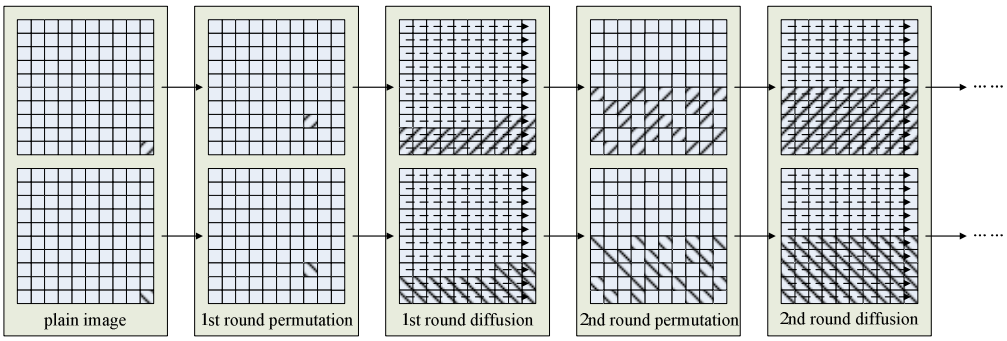


Fig. 3. Diffusion process of conventional chaos-based image cipher.

We assume a worst case that two plain images have only one pixel difference at the lower right corner (M, N). In first round permutation, the pixel at (M, N) is shuffled to (M', N'). Then in first round diffusion process, the pixel values are modified sequentially left to right, top to bottom and the difference is spread out to all pixels subsequent to (M', N'). The diffused pixels are scattered to a wider range of the cipher image in second round permutation and the difference scale is further enlarged in second round diffusion. According to above encryption process, this small difference can be spread out to the whole cipher image with several overall rounds encryption.

As mentioned above, the diffusion operation is a time-consuming procedure. While for conventional chaos-based image cipher, 3-4 overall rounds are usually needed to achieve a satisfactory diffusion performance. Such computational complexity greatly downgrades its advantage in practical large image encryption. To improve the efficiency of the chaos-based image cryptosystem, this paper proposes a bidirectional diffusion scheme which can significantly accelerate the spreading process, as shown in Fig. 4.

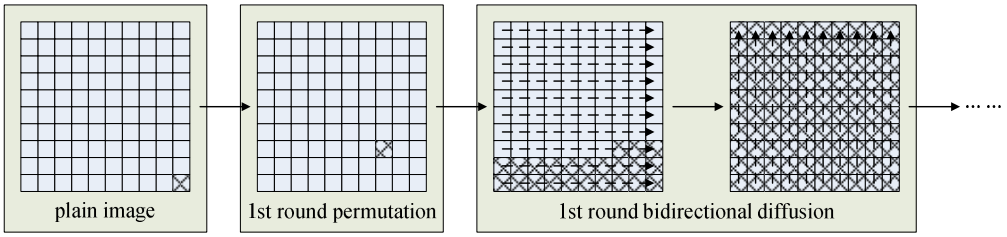


Fig. 4. Bidirectional diffusion scheme.

The new diffusion module consists of two independent diffusion processes with different spreading direction, while the permutation module keeps unchanged. In first stage of bidirectional diffusion, the difference is spread out to all pixels subsequent to (M', N') by modifying the pixel values sequentially left to right, top to bottom, just like conventional diffusion schemes. Then in second stage, a bottom to top, right to left sequential modification is carried out instead of starting next round permutation-diffusion. As a result, the diffused pixels produced by first stage bidirectional diffusion are spread out to the whole cipher image rather than a wider range of the cipher image. Therefore the overall encryption rounds can be reduced while without downgrade the security level.

Moreover, for conventional chaos-based image cipher, the key stream used in diffusion process is solely determined by the key. The same key stream is used to encrypt different plain-images if the key remains unchanged. Therefore, an opponent may obtain the key stream by known plain-text or chosen plain-text attacks, i.e., by encrypting some special plain-text sequences and then comparing them with the corresponding cipher-text sequences. To further enhance the security, a plain-text related chaotic orbit perturbing scheme is proposed, as illustrated by Fig. 5.

#154920 - $15.00 USD Received 20 Sep 2011; revised 13 Jan 2012; accepted 13 Jan 2012; published 19 Jan 2012

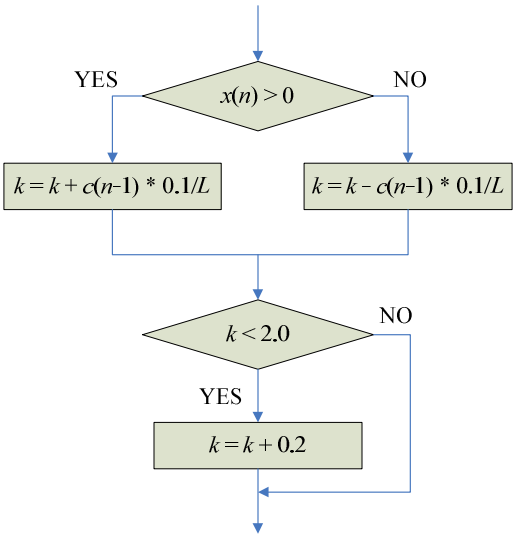


Fig. 5. Chaotic orbit perturbing scheme.

In Fig. 5, L is the gray levels of plain-image, and $x(n)$ is the chaotic sequence generated by Chebyshev map, as described by

$$x(n+1) = T_k(x_n) = \cos(k \cdot \cos^{-1} x_n), \ x_n \in [-1,1], \tag{5}$$

where $k \in [2,\infty)$ is control parameter. The initial value $x(0)$ and parameter k are used as the key. As shown in Fig. 5, k is altered in each round iteration and the modification is related with the previous cipher-pixel $c(n\text{-}1)$. Therefore the quantified key streams are related not only to the key but also to the plain-image.

The detailed diffusion process is described as follows:

Step 1: Iterate Eq. (5) for N_0 times to avoid the harmful effect of transitional procedure, where N_0 is a constant.

Step 2: The Chebyshev map is iterated continuously. Here, notice that the value of -1 is a 'bad' point, trapping the iterations to the fixed point 0. If this case is encountered, a tiny perturbation should apply. For each iteration, we can obtain one key stream element from the current state of the chaotic map according to

$$k(n) = \mathrm{mod}[floor(((x(n)+1)/2) \times 10^{14}), L], \tag{6}$$

where floor(x) returns the value of x to the nearest integers less than or equal to x, mod(x, y) returns the remainder after division.

Step 3: Calculate the cipher-pixel value according to Eq. (4). One may set initial value $c(-1)$ as a constant.

The inverse transform for deciphering is given by

$$p(n) = [k(n) \oplus c(n) \oplus c(n-1) + N - k(n)] \ \mathrm{mod} \ N. \tag{7}$$

Step 4: Perturb the control parameter k according to the perturbing scheme illustrated by Fig. 5.

Step 5: Return to Step 2 until a complete bidirectional diffusion process is done.

The diffusion performance is commonly measured by means of two criteria, namely, the number of pixel change rate (NPCR) and the unified average changing intensity (UACI). The

#154920 - $15.00 USD Received 20 Sep 2011; revised 13 Jan 2012; accepted 13 Jan 2012; published 19 Jan 2012

NPCR is used to measure the percentage of different pixel numbers between two images. Let $P_1(i, j)$ and $P_2(i, j)$ be the (i, j)th pixel of two images P_1 and P_2, respectively, the NPCR can be defined as:

$$NPCR = \frac{\sum_{i=1}^{W}\sum_{j=1}^{H} D(i, j)}{W \times H} \times 100\%, \tag{8}$$

where W and H are the width and height of P_1 or P_2 and $D(i, j)$ is defined as

$$D(i, j) = \begin{cases} 0 & \text{if } P_1(i, j) = P_2(i, j), \\ 1 & \text{if } P_1(i, j) \neq P_2(i, j). \end{cases} \tag{9}$$

The NPCR value for two random images, which is an expected estimate for a good image cryptosystem, is given by

$$NPCR_{\exp ected} = \left(1 - \frac{1}{2^{\log_2 L}}\right) \times 100\%, \tag{10}$$

where L is the gray levels of the image. For instance, the expected NPCR for two random images with 256 gray levels is 99.609%.

The second criterion, UACI is used to measure the average intensity of differences between the two images. It is defined as

$$UACI = \frac{1}{W \times H}\left[\sum_{i=1}^{W}\sum_{j=1}^{H} \frac{\left|P_1(i, j) - P_2(i, j)\right|}{L-1}\right] \times 100\%. \tag{11}$$

The UACI value for two random images is given by

$$UACI_{\exp ected} = \frac{1}{L^2}\left(\frac{\sum_{i=1}^{L-1} i(i+1)}{L-1}\right) \times 100\%. \tag{12}$$

For a 256 gray levels image, the expected UACI value is 33.464%.

To test the NPCR and UACI of the proposed cryptosystem, two plain images with only one bit difference at the lower right corner are employed, as shown in Figs. 6(a) and 6(b). Their corresponding cipher images obtained after only one round of the proposed confusion process are shown in Figs. 6(c) and 6(d), respectively. The two cipher images have 99.61% of pixel different with each other. The difference image between the two cipher images can be found in Fig. 6(e), which is obtained by

$$I_{diff} = \left|P_1(i, j) - P_2(i, j)\right|. \tag{13}$$

The results show that a tiny change in the original image will result in a significant change in the ciphered image, so the proposed scheme has a good ability against known/chosen plaintext attack.

#154920 - $15.00 USD Received 20 Sep 2011; revised 13 Jan 2012; accepted 13 Jan 2012; published 19 Jan 2012

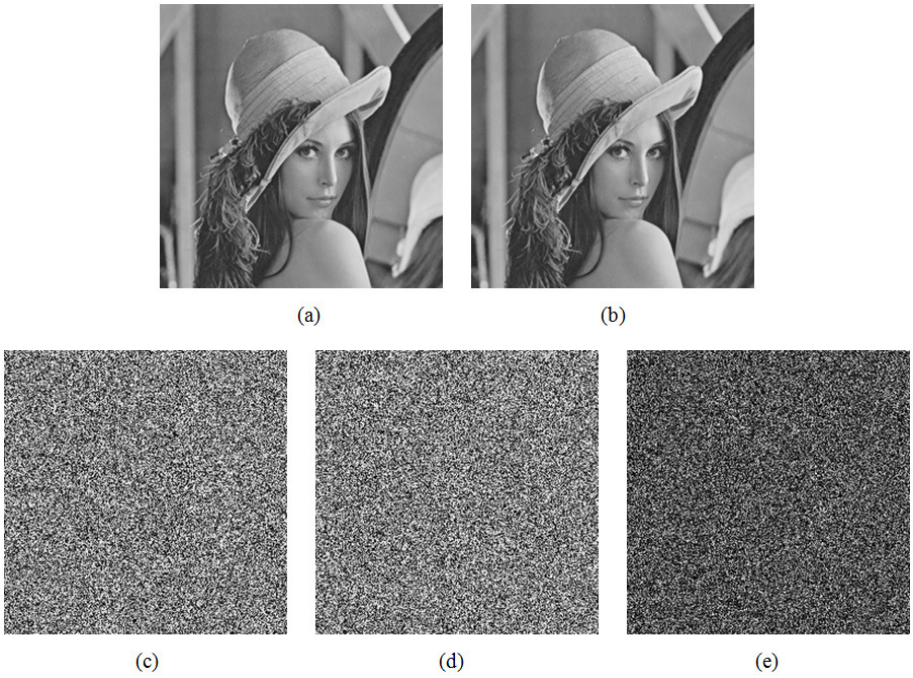


Fig. 6. NPCR and UACI test. (a) and (b) are two plain images with only one bit difference at the lower right corner. (c) Cipher image of (a). (d) Cipher image of (b). (e) Differential image between (c) and (d).

To evaluate the performance promotion of the new diffusion scheme, the NPCR and UACI are plotted against the cipher cycles and compared with that of the conventional scheme, as shown in Figs. 7(a) and 7(b), respectively. As can be seen from Fig. 7, three overall encryption rounds are needed to achieve a satisfactory security level by using conventional diffusion scheme. While using the proposed scheme, a fairly good result can be obtained with only one cipher cycle, thus the efficiency of the image cryptosystem is significantly improved.

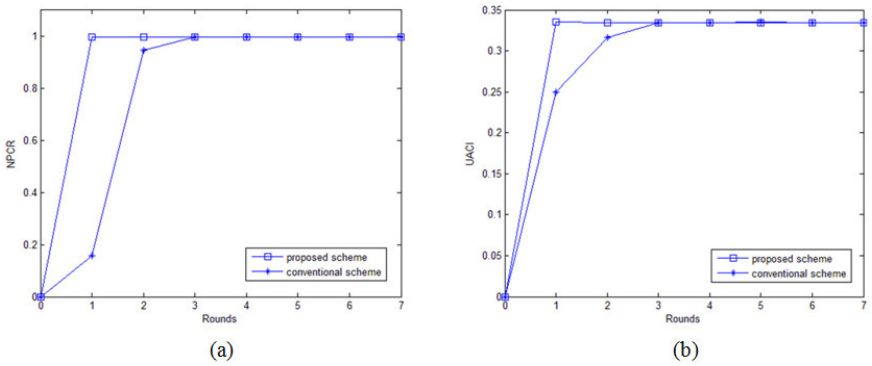


Fig. 7. NPCR and UACI performance of the proposed scheme and conventional scheme. (a) NPCR performance. (b) UACI performance.

In the following security analysis, one cipher cycle is adopted so that a fast encryption scheme is obtained in our design.

#154920 - $15.00 USD Received 20 Sep 2011; revised 13 Jan 2012; accepted 13 Jan 2012; published 19 Jan 2012

4. Security analysis

The crucial measure for the quality of a cryptosystem is its capability to withstand the attempts of an unauthorized participant, or an opponent, to gain knowledge about the unencrypted information. A good cryptosystem should resist all kinds of known attacks, such as known/chosen plain-text attack, cipher-text only attack, statistical attack, differential attack, and various brute-force attack. Some security analysis has been performed on the proposed scheme, including the most important ones like key space analysis, statistical analysis and key sensitivity analysis, which has demonstrated the satisfactory security of the proposed scheme, as discussed in the following.

4.1 Key space analysis

The key space is the total number of different keys that can be used in the encryption/decryption procedure. For an effective cryptosystem, the key space should be large enough to make brute-force attack infeasible. As mentioned above, the key of the proposed cryptosystem is composed of two parts: permutation key K and diffusion key (x_0, k), where $K \in N^+$, $x_0 \in [-1, 1]$ and k can have any real value greater than 2.0. Since most of the modern C/C + + compilers support a maximum of 64-bit integer types, the possible choices of K is around 9.2×10^{18}. According to the IEEE floating-point standard [26], the computational precision of the 64-bit double-precision number is about 10^{-15}. Therefore, the total number of possible values of x_0 that can be used as a part of the key is approximately 2×10^{15}. As in the proposed image encryption scheme, k can have any real value greater than 2.0 hence it has infinite number of possible values that can be used as a part of the key. However, the range of k should be restricted to a particular interval of 2π to prevent Chebyshev map from producing periodic orbits, then for k there will be approximately $2\pi \times 10^{15}$ different values possible.

The two parts of the key are independent of each other. Therefore, the complete key space of the proposed image encryption scheme is

$$H(K, x_0, k) \approx 1.156\times10^{50} = 2^{167}, \tag{14}$$

which is large enough to resist brute-force attack.

4.2 Statistical analysis

It is well known that many ciphers have been successfully analyzed with the help of statistical analysis and several statistical attacks have been devised on them. Therefore, an effective cipher should be robust against any statistical attack. To prove the robustness of the proposed scheme, we have performed statistical analysis by calculating the histogram, the information entropy, the correlation of two adjacent pixels in the ciphered image, and key stream statistical characteristics.

4.2.1 Histogram

An image histogram illustrates that how pixels in an image are distributed by plotting the number of pixels at each grayscale level. The distribution of cipher-text is of much importance. More specifically, it should hide the redundancy of plain-text and should not leak any information about the plain-text or the relationship between plain-text and cipher-text.

The histograms of plain-image (Fig. 8(a)) and its ciphered image (Fig. 8(c)) produced by the proposed scheme are shown in Figs. 8(b) and 8(d), respectively. It's clear from Fig. 8(d) that the histograms of the cipher-image are fairly uniform and significantly different from that of the plain image and hence does not provide any clue to employ statistical attack.

#154920 - $15.00 USD Received 20 Sep 2011; revised 13 Jan 2012; accepted 13 Jan 2012; published 19 Jan 2012

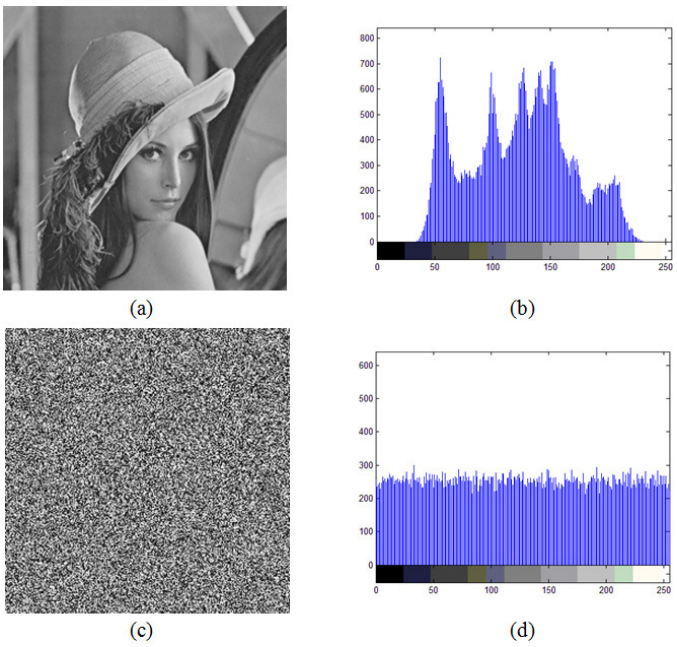


Fig. 8. Histograms of plain-image and cipher-image. (a) Plain-image. (b) Histogram of plain-image. (c) Cipher-image. (d) Histogram of cipher-image.

4.2.2 Correlation of adjacent pixels

For an ordinary image having definite visual content, each pixel is highly correlated with its adjacent pixels either in horizontal, vertical or diagonal direction. However, an efficient image cryptosystem should procedure the cipher image with sufficiently low correlation in the adjacent pixels.

To quantify and compare the correlations of adjacent pixels in the plain and cipher image, the following procedure is carried out. First, randomly select 2000 pairs of adjacent pixels in each direction from the plain image and its ciphered image. Then, calculate the correlation coefficient $r_{x,y}$ of each pair by using the following three formulas:

$$r_{xy} = \frac{\frac{1}{N}\sum_{i=1}^{N}(x_i - \overline{x})(y_i - \overline{y})}{\sqrt{\left(\frac{1}{N}\sum_{i=1}^{N}(x_i - \overline{x})^2\right)\left(\frac{1}{N}\sum_{i=1}^{N}(y_i - \overline{y})^2\right)}}, \tag{15}$$

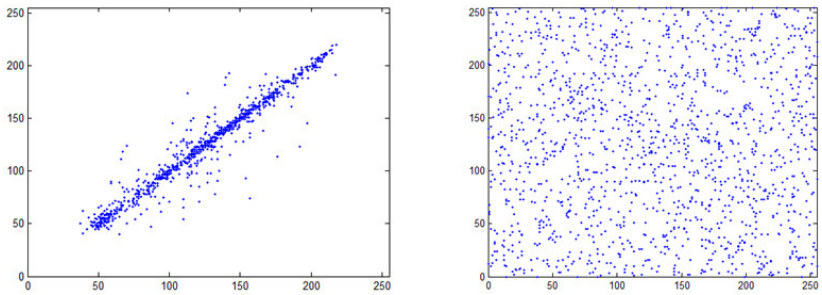
$$\overline{x} = \frac{1}{N}\sum_{i=1}^{N} x_i, \tag{16}$$

$$\overline{y} = \frac{1}{N}\sum_{i=1}^{N} y_i, \tag{17}$$

where x_i and y_i are grayscale values of ith pair of adjacent pixels, and N denotes the total number of samples.

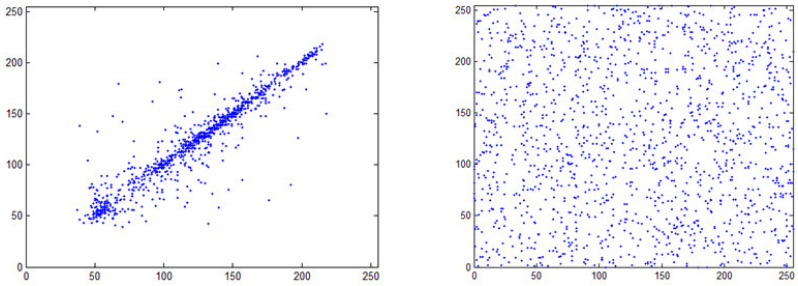
The results of the correlation coefficients for horizontal, vertical and diagonal adjacent pixels for the plain image and its cipher image are given in Table 1. The visual testing of the correlation distribution of two horizontally adjacent pixels, two vertically adjacent pixels and two diagonally adjacent pixels of the plain image and the cipher image produced by the proposed scheme is shown in Figs. 9-11, respectively.

#154920 - $15.00 USD Received 20 Sep 2011; revised 13 Jan 2012; accepted 13 Jan 2012; published 19 Jan 2012



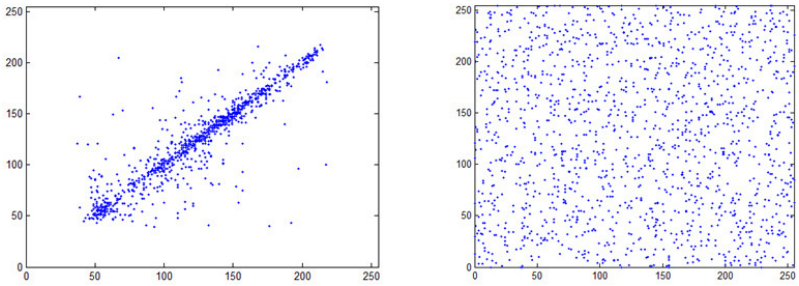
(a) (b)

Fig. 9. Correlation of horizontal adjacent two pixels. (a) Plain image. (b) Ciphered image.



(a) (b)

Fig. 10. Correlation of vertical adjacent two pixels. (a) Plain image. (b) Ciphered image.



(a) (b)

Fig. 11. Correlation of diagonal adjacent two pixels. (a) Plain image. (b) Ciphered image.

It's clear from Fig. 9-11 and Table 1 that the strong correlation between adjacent pixels in plain image is greatly reduced in the cipher image produced by the proposed scheme.

Table 1. Correlation Coefficients of Two Adjacent Pixels in Two Images

	Plain image	Ciphered image
Horizontal	0.9404	0.0088
Vertical	0.9299	–0.0087
Diagonal	0.9257	–0.0060

4.2.3 Information entropy

In information theory, entropy is the most significant feature of disorder, or more precisely unpredictability. To calculate the entropy $H(s)$ of a source s, we have:

#154920 - $15.00 USD Received 20 Sep 2011; revised 13 Jan 2012; accepted 13 Jan 2012; published 19 Jan 2012

$$H(S) = -\sum_{i=0}^{2^N-1} P(s_i) \log_2 P(s_i), \tag{18}$$

where N is the number of bits to represent a symbol $m_i \in m$ and $P(s_i)$ represents the probability of symbol m_i so that the entropy is expressed in bits.

For a truly random source emitting 2^N symbols, the entropy is $H(m) = N$. therefore, for a ciphered image with 256 gray levels, the entropy should ideally be $H(m) = 8$. If the output of a cipher emits symbols with entropy less than 8, there exists certain degree of predictability, which threatens its security.

Let us consider the cipher text of the test image encrypted using the proposed scheme, the number of occurrence of each cipher text pixel m_i is recorded and the probability of occurrence is computed. The entropy for plain image and its cipher image are $H(m) = 5.3883$ and $H(m) = 7.9902$, respectively. The entropy of the output ciphered image is very close to the theoretical value of 8. This means that information leakage in the encryption process is negligible and the cryptosystem is secure against entropy attack.

4.2.4 Key stream statistical characteristics

Most chaotic cryptosystem including the proposed scheme in essence belong to stream ciphers: the nonlinear equations governing the evolution of the system are used to generate a key stream by using the system parameters, initial conditions, etc., as the key. It is crucial to the security of the key stream cipher that the key stream should be as long as the message, unpredictable, and never reused, thus preventing two different messages encrypted with the same portion of the key stream being intercepted or generated by an attacker [27].

Autocorrelation and cross-correlation are two major measures of key stream randomness. For a truly random series such as white noise, the autocorrelation and cross-correlation are δ function and zero, respectively.

The autocorrelation coefficient at lag k of a series $x_0, x_1, x_2, ..., x_{N-1}$ is normally given as

$$\text{autocorr}(k) = \frac{\sum_{i=0}^{N-1} (x_i - \overline{x})(x_{i+k} - \overline{x})}{\sum_{i=0}^{N-1} (x_i - \overline{x})^2}, \tag{19}$$

where $\overline{x}$ is the mean of the series.

The cross correlation of two series $x(i)$ and $y(i)$ where $i = 0,1,2,...,N-1$ at delay k is defined as

$$\text{crosscorr}(k) = \frac{\sum_{i=0}^{N-1} (x_i - \overline{x})(y_{i-k} - \overline{y})}{\sqrt{\sum_{i=0}^{N-1} (x_i - \overline{x})^2} \sqrt{\sum_{i=0}^{N-1} (y_i - \overline{y})^2}}, \tag{20}$$

where $\overline{x}$ and $\overline{y}$ is the mean of the series.

The autocorrelation function of chaotic key stream generated with initial parameter $k = 4.0$ and $x_0 = 3.0$ is shown in Fig. 12(a) and its cross-correlation with another key stream generated with $k = 4.0$ and $x_0 = 0.30000001$ is shown in Fig. 12(b). From Fig. 12 we can see that the randomness of the key stream generated by the proposed scheme is very close to that of a truly random source, thus the security of the key stream cipher are well guaranteed.

#154920 - $15.00 USD Received 20 Sep 2011; revised 13 Jan 2012; accepted 13 Jan 2012; published 19 Jan 2012

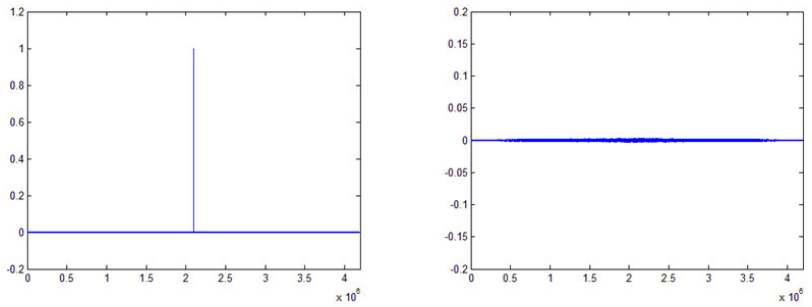


Fig. 12. Correlation functions of key stream. (a) Autocorrelation function. (b) Cross-correlation function.

4.3 Key sensitivity analysis

This test is intended to emphasize the diffusion property of the proposed cryptosystem under consideration with respect to small changes in keys. This is important because otherwise an intruder might reconstruct parts of the plain-image from the observed cipher-image by a partly correct guess of the key used for encryption. The key sensitivity of a cryptosystem can be observed in two ways: (i) completely different cipher images should be produced when slightly different keys are used to encrypt the same plain image; (ii) the cipher image cannot be correctly decrypted even though there is only a slight difference between the encryption and decryption keys.

To evaluate the key sensitivity of the first case, the plain Lenna image is encrypted using four slightly different test keys, respectively, as listed in Table 2. The corresponding cipher images are shown in Figs. 13(a), 13(b), 13(d) and 13(f), respectively. The differences between any two cipher images are computed and given in Table 2. The differential images between (a) and (b), (a) and (d), and (a) and (f) are shown in (c), (e) and (g) of Fig. 13, respectively.

Table 2. Differences between Cipher Images Produced by Slightly Different Keys

Figure	Test Keys			Differences			
	K	k	x_0	(a)	(b)	(d)	(f)
(a)	512	5.78259581295362	0.48729650284971	——	99.59%	99.64%	99.60%
(b)	513	5.78259581295362	0.48729650284971	99.59%	——	99.61%	99.62%
(d)	512	5.78259581295363	0.48729650284971	99.64%	99.61%	——	99.61%
(f)	512	5.78259581295362	0.48729650284972	99.60%	99.62%	99.61%	——

As can be seen from Table 2 and Fig. 13, the four cipher images show no similarities at all and there is no significant correlation that could be observed from the differential images.

To evaluate the key sensitivity of the second case, the plain Lenna image is firstly encrypted using the test key (K = 768, k = 4.71052756328493, x_0 = 0.73195538124604) and the resultant cipher image is shown in Fig. 14(a). Then the ciphered image is tried to be decrypted using four decryption keys: (i) (K = 768, k = 4.71052756328493, x_0 = 0.73195538124604), (ii) (K = 767, k = 4.71052756328493, x_0 = 0.73195538124604), (iii) (K = 768, k = 4.71052756328492, x_0 = 0.73195538124604) and (iv) (K = 768, k = 4.71052756328493, x_0 = 0.73195538124603). The resultant decrypted images are shown in Figs. 14(b), 14(c), 14(d) and 14(e), respectively. The differences between wrong deciphered images (c), (d) and (e) to plain image are 99.62%, 99.63% and 99.62%, respectively.

#154920 - $15.00 USD Received 20 Sep 2011; revised 13 Jan 2012; accepted 13 Jan 2012; published 19 Jan 2012

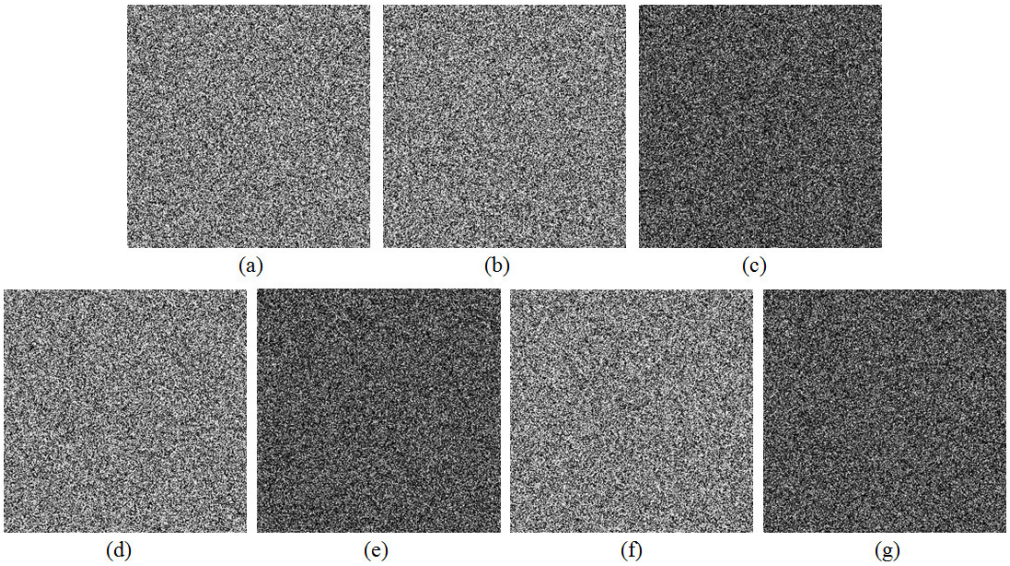


Fig. 13. Key sensitivity test: result 1. (a) Ciphered image using key (K = 512, k = 5.78259581295362, x_0 = 0.48729650284971). (b) Ciphered image using key (K = 513, k = 5.78259581295362, x_0 = 0.48729650284971). (c) Differential image between (a) and (b). (d) Ciphered image using key (K = 512, k = 5.78259581295363, x_0 = 0.48729650284971). (e) Differential image between (a) and (d). (f) Ciphered image using key (K = 512, k = 5.78259581295362, x_0 = 0.48729650284972). (g) Differential image between (a) and (f).

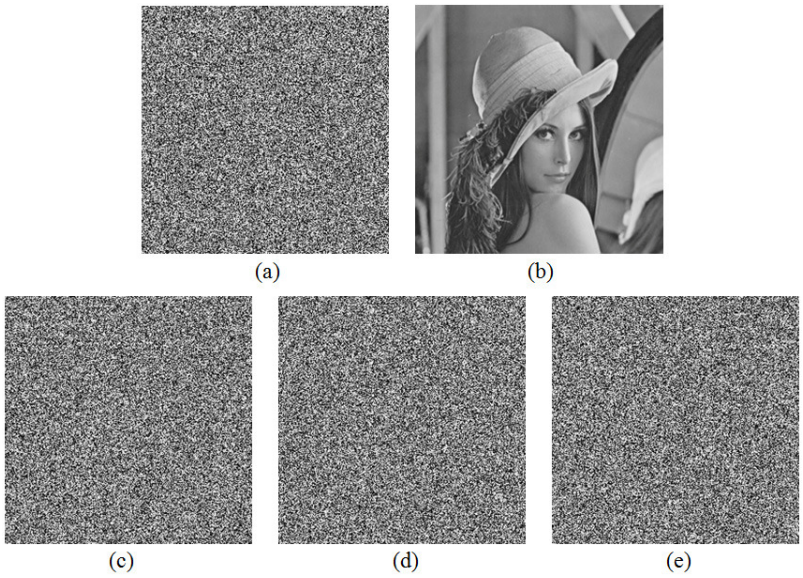


Fig. 14. Key sensitivity test: result 2. (a) Ciphered image using key (K = 768, k = 4.71052756328493, x_0 = 0.73195538124604). (b) Deciphered image using key (K = 768, k = 4.71052756328493, x_0 = 0.73195538124604). (c) Deciphered image using key (K = 767, k = 4.71052756328493, x_0 = 0.73195538124604). (d) Deciphered image using key (K = 768, k = 4.71052756328492, x_0 = 0.73195538124604). (e) Deciphered image using key (K = 768, k = 4.71052756328493, x_0 = 0.73195538124603).

Above two tests indicate that the proposed scheme is highly sensitive to the key. Even an almost perfect guess of the key does not reveal any information about the plain-image. Instead

#154920 - $15.00 USD Received 20 Sep 2011; revised 13 Jan 2012; accepted 13 Jan 2012; published 19 Jan 2012

any attempt to decrypt with a wrong key is in fact another encryption operation. Therefore differential attack would become very inefficient and practically useless.

5. Efficiency analysis

Apart from the security consideration, efficiency is also an important aspect for a good image cryptosystem, particular for real-time Internet applications. Table 3 lists the time required for encrypting a 256 × 256 grayscale Lenna image with different overall rounds by using the proposed and conventional schemes. The computer used in this test is 2.4GHz Intel Core2 Duo with 2G memory. In addition to the encryption time, two performance indices NPCR and UACI are also listed in Table 3.

Table 3. Encryption Time and NPCR & UACI Performance of the Proposed and Conventional Schemes

Rounds	Encryption Time (*ms*)		NPCR		UACI	
	Proposed	Convention	Proposed	Convention	Proposed	Convention
1	***78***	46	***99.61%***	15.74%	***33.48%***	25.03%
2	152	90	99.63%	94.63%	33.45%	31.62%
3	236	***141***	99.62%	***99.58%***	33.46%	***33.47%***
4	303	179	99.63%	99.58%	33.47%	33.46%

From Table 3 we can see that to achieve a satisfactory security level such as NPCR > 99.6 and UACI > 33.4%, the proposed scheme only requires one overall round. While for conventional schemes, three overall rounds are needed. The encryption time of the proposed scheme is approximate a half of the conventional schemes even though a single round encryption needs more time due to the computational complexity of bidirectional diffusion. The significant acceleration in encryption speed is due to the reduction of the number of overall rounds. Fewer time-consuming diffusion operations are need and thus the encryption time is shortened. With such a speed, this image cryptosystem is appropriate to be used for real-time secure image transmission over broadband network, where the encryption time should be short relative to the transmission time.

6. Conclusions

In this paper, an improved diffusion strategy is proposed to promote the efficiency of the most widely used permutation-diffusion type image cipher. By using the novel bidirectional diffusion strategy, the spreading process is significantly accelerated. As a result, the same level of security can be achieved with fewer overall encryption rounds and hence the encryption speed is much faster than that of conventional schemes. Moreover, to further enhance the security of the cryptosystem, a plain-text related chaotic orbit turbulence mechanism is introduced in diffusion procedure by perturbing the control parameter of the employed chaotic system according to the cipher-pixel. Extensive security analysis has been carried out on the proposed image encryption technique using differential analysis, key space analysis, key sensitivity analysis and various statistical analyses. Based on the results of our analysis, we conclude that the proposed image encryption technique is perfectly suitable for the real time secure image and video communication applications.

Acknowledgments

This work was supported by the National Natural Science Foundation of China (No. 60872040, 61071124), the Fundamental Research Funds for the Central Universities (No. N100404016).

#154920 - $15.00 USD Received 20 Sep 2011; revised 13 Jan 2012; accepted 13 Jan 2012; published 19 Jan 2012