A Novel Color Image Cryptosystem Using Chaotic Cat and Chebyshev Map

Jianjiang CUI[1], Siyuan LI[2] and Dingyu Xue[3]

[1] School of Information Science and Engineering, Northeastern University, Shenyang 110004, China

[2] School of Information Science and Engineering, Northeastern University, Shenyang 110004, China

[3] School of Information Science and Engineering, Northeastern University, Shenyang 110004, China

Abstract

With the advancement of multimedia and real-time networks, a vast number of digital images are now stored and transmitted over public networks. A lot of researches of chaos-based image encryption technologies have been done. However, the performance of conventional encryption algorithm is not satisfying when used to color image. In this paper, we propose an improved chaos-based color image cryptosystem which significantly increases the efficiency and enhances the security performance. In this algorithm, firstly a color image is divided into three color channels. Then a bit-level permutation is performed in each channel, hence diffusion scheme is introduced into permutation stage. Meanwhile, we provide optional and partial cipher function. Detailed analysis of security performance and results show great advantages in speed, key space, correlation, information entropy ,etc.

Keywords: *chaos-based, bit-level, color image encryption, Chebyshev map*

1. Introduction

The fascinating developments in digital image processing and network communications during the past decade have created a great demand for real-time secure image transmission over the Internet and through wireless networks. Due to some intrinsic features of images, such as bulk data capacity and high correlation among pixels, traditional encryption algorithms such as AES, DES and IDEA are not suitable for practical image encryption, especially under the scenario of on-line communications. The threaten to security of image transmission has become an issue. As is known to all, image is different from text data in many aspects. The conventional block cipher solutions such as DES, AES, IDEA are not suitable for image cipher. In recent years, many researches have shown that there are close relationship between chaos and cryptography. The fundamental features of chaotic dynamical systems such as ergodicity , mixing property, sensitivity to initial parameters can be considered analogous to some ideal cryptographic properties such as confusion, diffusion, balance, avalanche, properties, etc. [1].

In [2], Scharinger proposed a chaotic Kolmogorov-flow-based image encryption algorithm. In his scheme, the plain-image is firstly permuted through a key-controlled chaotic system based on the Kolmogorov flow and then substituted by using shift-registered pseudo-random number generator, which alters the statistical property of the cipher-image. In [3], Fridrich suggested that a chaos-based image encryption scheme should compose of two modules: chaotic confusion and pixel diffusion. The former permutes the pixels of a plain image with an invertible 2D chaotic map while the latter alternates the gray scale of each pixel in a sequential manner. The architecture constitutes the basis of the chaos-based encryption methods proposed subsequently. In [4, 5], the 2D chaotic Cat map and Baker map are generalized to 3D for designing a real-time secure symmetric encryption scheme. The two approaches employ the 3D map to shuffle the positions of image pixels and use another chaotic map to confuse the relationship between the cipher-image and plain-image. In [6], Rhouma et al. proposed an OCML-based color image encryption scheme with a stream cipher structure. In this scheme, a 192-bit-long external key is used to generate the initial conditions and the parameters of the OCML by making some algebraic transformations to the secret keys. In [7], Elashry et al. proposed a new homomorphic image cryptosystem. The idea of this system is based on encrypting the reflectance component after the homomorphic transform and embedding the illumination component as a least significant bit water mark into the encrypted reflectance component. In [8], Wong et al. proposed an efficient diffusion mechanism using simple table lookup and swapping techniques as a light-weight replacement of the 1D chaotic map iteration.

This article proposes a novel chaos-based color image encryption scheme to enhance the security level of color image encryption. Color image is divided into three color channels and a bit-level permutation is employed in each channel, hence diffusion scheme is introduced into permutation stage. This improved scheme protects the

image from being broken in permutation stage. Meanwhile this scheme can reduce the burden of diffusion stage which can significantly increase the overall encryption speed and enhance the security level. Thorough experimental tests are carried out with detailed analysis, indicating that the proposed scheme provides an efficient way for real-time secure image transmission over public networks.

The remainder of this paper is organized as follows. Section 2 introduces the architecture and implementation of the proposed algorithm. Section 3 introduces the permutation stage of the proposed algorithm. Section 4 introduces the substitution stage of the proposed algorithm. Section 5 illustrates a number of analysis of the algorithm performance. Finally, section 5 concludes the whole thought of this paper and puts forward some prospects.

2. Architecture of proposed scheme

There are two stages in conventional permutation-substitution type chaos-based image cryptosystem. They are permutation stage and substitution stage. In permutation stage, the position of each pixel is shuffled in a different and usually quite complex order while its value keeps unchanged. Three types of two-dimensional investable chaotic maps named Arnold Cat map, Baker map and Standard map are usually employed to realize pixel permutation. In substitution stage, the pixel values are altered sequentially and the modification made to a particular pixel value depends on the accumulated effect of all the previous pixel values, so the diffusion effect is introduced in this stage. Chaotic map is used to generate pseudorandom image for substitution.

According to traditional method, we found that the permutation and substitution stage are independent from each other. In permutation stage, only the position of each pixel is changed, the pixel value remains unchanged. From all concerns above, the security level of this stage is low, and the security of cryptosystem is mainly depends on the substitution stage. Based on the situation above, it is highly possible that the permutated image can be captured and broken by statistical attack. So we introduce a substitution scheme into permutation stage. Firstly, we divide color image into three color channels; then different parameters of Arnold-Cat Map are introduced to shuffle the images; finally the shuffled images are mixed into one image. The architecture of this strategy is shown in Fig. 1 as follows.

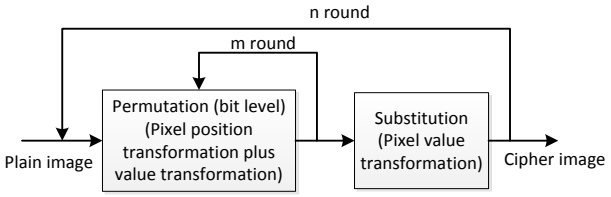


Fig. 1 Architecture of the proposed permutation-substitution type chaos-based image cryptosystem

In this permutation stage, both the shuffling on pixel position and the modification of pixel value are carried out simultaneously while the substitution process remains unchanged. As a result, the pixel value mixing effect is contributed by two levels of substitution operations: the improved permutation process and the original substitution function. Different parameters are employed to encrypt three color channel images. The security of the permutation module is significantly improved since the substitution effect is introduced, and the same level of security can be achieved in fewer overall rounds. The efficiency of the cryptosystem is thus improved. The experiment result is shown in Fig. 2 as follows.

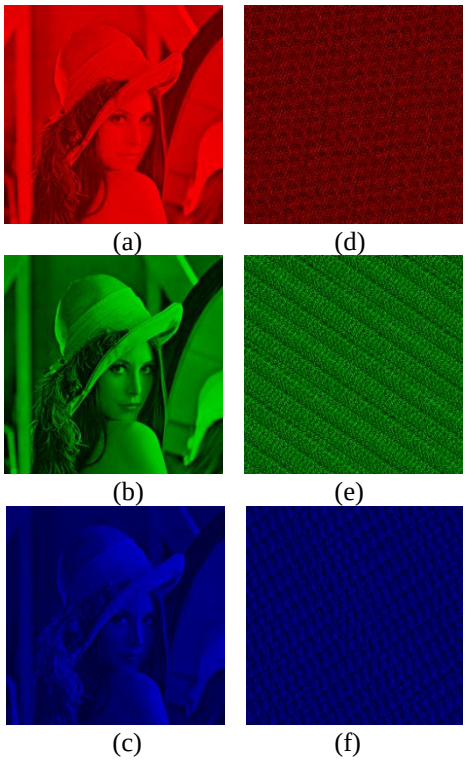


Fig. 2 The divided R,G,B channels and shuffled images: (a) R channel image, (b) G channel image, (c) B channel image, (d) shuffled R channel image, (e) shuffled G channel image, (f) shuffled B channel image

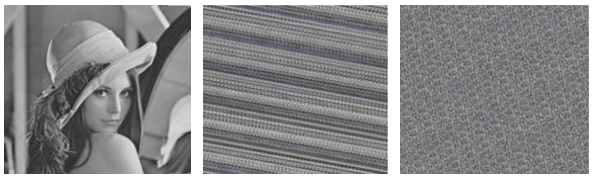
3. Permutation stage of proposed image cryptosystem

The map is area-preserving since the determinant of its linear transformation matrix is equal to 1.In this stage, a unit square is first stretched by the linear transform and then folded by the module operation, mod.

Since encryption is a kind of transformation operated on a finite set, in order to incorporate a chaotic map into image encryption, one has to discretize it, while reserving some of its useful features such as the mixing property and the sensitivity to initial conditions and parameters. The map is discretized according to the following formula.

$$\begin{bmatrix} x_{n+1} \\ y_{n+1} \end{bmatrix} = \begin{bmatrix} 1 & p \\ q & pq+1 \end{bmatrix} \begin{bmatrix} x \\ y \end{bmatrix} \bmod N \quad (1)$$

where N is the width or height of the image. We conduct experiment on Lenna image. The experiment result is shown in Fig. 2 as follows.



(a) (b) (c)

Fig. 3 1 round and 3 round iteration permutated images for plain image: (a) plain image, (b) shuffled image (p=10, q=5, 1 round iteration), (c) shuffled image (p=10, q=5, 3 round iteration)

Inverse transformation for deciphering is given as follows.

$$\begin{bmatrix} x_{n+1} \\ y_{n+1} \end{bmatrix} = \begin{bmatrix} pq+1 & -p \\ -q & 1 \end{bmatrix} \begin{bmatrix} x_n \\ y_n \end{bmatrix} \bmod N \quad (2)$$

4. Substitution stage of proposed image cryptosystem

Chebyshev Map is employed in this stage to change the pixel values. The substitution stage is based on permutation stage, we can change two dimensional image into one dimensional pixel sequence, then alter the pixel sequence according to certain rule. Generally, the latter pixel is determined by a few former pixel values. In this way, every changed pixel will affect a few latter pixel values, then by next permutation stage, the changed value is diffused into the whole image. In substitution stage, we can further change the pixel values. In the proposed substitution stage, Chebyshev Map is employed in order to achieve enough key space. The expression of Chebyshev Map is given as follows.

$$x_{n+1} = T_k(x_n) = \cos(k \cdot \cos^{-1} x_n), x_n \in [-1, 1]. \quad (3)$$

Where k is the encryption parameter, x_n is chaos sequence. The system enter chaotic stage when $k \in [2, \infty)$.

The detailed procedure of this algorithm is described as below:

Step 1. Iterate N_0 times according to Eq. (3), this procedure is supposed to avoid disadvantages brought by transition of chaotic state.

Step 2. Iterate the Chebyshev system, and get key stream elements according to Eq. (4) each time after iteration.

$$k_n = mod[floor\left(\left(\frac{x_n+1}{2}\right) \times 10^{14}\right), L] \quad (4)$$

Here, k_n represents key stream elements, function floor is used to return numerical approximation of x, function mod is used to return surplus value of each part, L is possible grey scale value.

$$c_n = k_n \oplus \{[p_n + k_n] \, mod \, N\} \oplus c_{n-1} \quad (5)$$

Where k_n is key stream, p_n is plaintext and $c_n$is the cipher.

Step 3. Encrypt the present pixel value using Eq. (5).

$$p_n = [k_n \oplus c_n \oplus c_{n-1} + N - k_n] \, mod \, N \quad (6)$$

Here p_n is the pixel value of present pixel, c_{n-1} is the former encrypted value, and as to the first pixel, c_{-1} is set as a constant. The decryption Eq. (6) is given as above.

Step 4. Return to step two and perform diffusion operation, until every pixel of the image from top to bottom, from left to right is diffused. The picture shown below is the encrypted image for the plain image. And $k = 4.0$, $x_n = 0.30000000$, L and c_{-1} is set as 256 and 128.

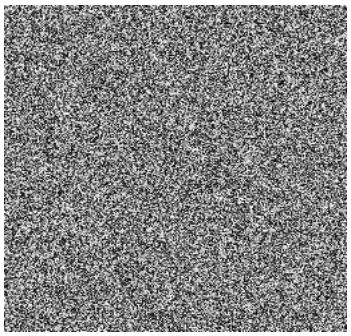


Fig. 4 Encrypted image for the plain image

5. Speed and security analysis for proposed chaos-based cryptosystem

5.1 The comparison test of speed

Digital image has the characteristic of high redundancy and high-capacity, conventional encryption methods such as DES, IDEA, AES are slow and have large time delay, they can't meet the requirement of increasing demand of real-time networks. Compared with other methods, chaos-

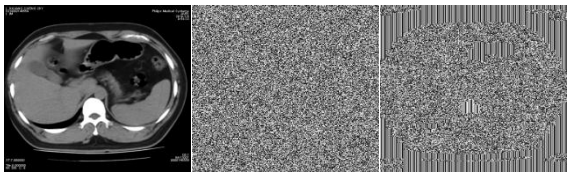
based image encryption has great advantage in speed, it can reduce about 50% encryption time. The test CPU of the analysis is AMD Phenom(tm) II N930 Quad-Core Processor (basic frequency 2.0GHz) with 2G memory. The detailed results of our test is shown in Table 1.

Table 1 Comparison of the speed of Chaotic encryption and DES method

Resolution Ratio	*Image Format*	*Image Size*	*Chaotic encryption speed*	*DES Speed*
256×256	24 bit true color	192K	62 ms	124 ms
512×512	24 bit true color	768K	249 ms	514 ms
1024×1024	24 bit true color	3.0M	1.03 s	1.97 s
2048×2048	24 bit true color	12.0M	4.12 s	8.07 s
4096×4096	24 bit true color	48.0M	13.10 s	33.20 s

5.2 Image encryption effect analysis

Digital image has high redundancy, that is the relative pixels are equal and similar. Conventional encryption methods, such as DES, IDEA, AES most of them are block cipher schemes. Block cipher schemes will produce similar results when they are applied to images with high redundancy. As is shown in Fig. 5, some lump is still visible in ciphered image which is encrypted by DES. While chaos-based encryption is typical stream cipher, the ciphered image is random distributed.



(a) (b) (c)

Fig. 5 Comparison of Chaos and DES encrypted image: (a) plain image, (b) chaos encryption, (c) DES encryption.

5.3 Key Space analysis and comparison

As mentioned above, the key of the proposed cryptosystem is composed of two parts: ① the initial parameter and condition (k, x0) of chaotic Chebyshev map, where $x_0 \in [-1, 1]$ and k can have any real value greater than 2.0; ② the control parameters (p, q) and iteration times m of Cat map, where $p, q, m \in N^+$. According to the IEEE floating-point standard [9], 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 2×1015. 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 2π×1015 different values possible.

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

$$H(p, q, x_0, k) = \text{key} - P \times \text{key} - S \approx 12.57 \times 10^{30} \times (N^2)^m \quad (7)$$

If $m = 3$, $N \geq 256$, the complete key space is

$$H(p, q, x_0, k) > 3.54 \times 10^{45} \approx 2^{153} \quad (8)$$

Comparison of the key space of chaos-based encryption and conventional method is shown in Table 2.

Table 2 Comparison of the key space of chaos-based encryption and conventional methods (DES, AES, IDEA)

Method	*Chaos-based Method*	*DES Method*	*AES Method*	*IDEA Method*
Key Space	153	56	128	128

From the data in Table 2, we know that Chaos-based encryption method has great advantage in key space, it can better resist brute force.

5.4 Histogram analysis and comparison

Histogram analysis provides the information of pixel value distribution, the histogram of ciphered image should be smooth, well-distributed and different from the histogram of plain image greatly, if they have many similarities, the attacker may get some information by statistical analysis. The histogram of plain image and ciphered image are shown in Fig. 6. Through some analysis, we know that compared with plain image, the pixel value of ciphered image is more distributed and smoother. Besides, it varies a lot from plain image histogram, the ciphered image shows great randomness.

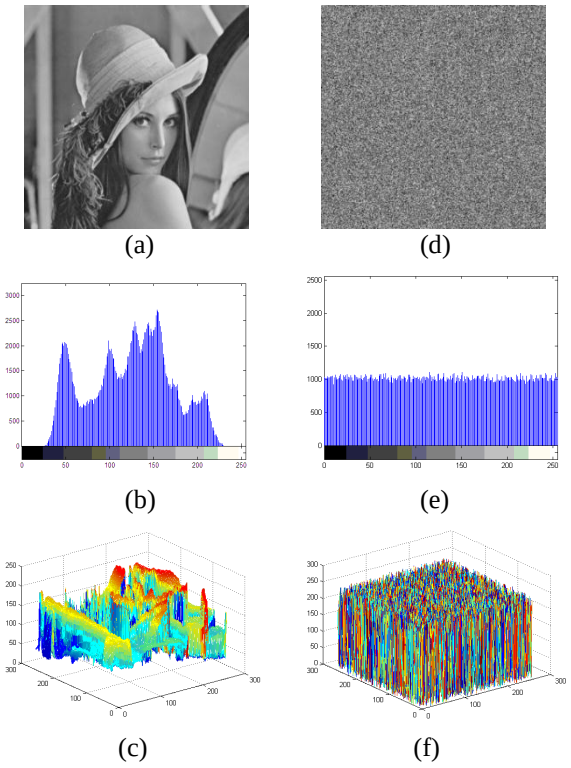


Fig. 6 Histogram analysis and comparison for plain image and ciphered image: (a) plain image, (b) histogram of plain image, (c) three dimension joint histogram of plain image, (d) ciphered image, (e) histogram of ciphered image, (f) three dimension joint histogram of ciphered image

5.5 Analysis for correlation of adjacent pixels

Generally speaking, adjacent pixels in plain image have high correlation, however, adjacent pixels in ciphered image should have low correlation [10, 11]. In order to test the correlation of adjacent pixels in the ciphered image which is encrypted according to proposed scheme, a test is designed. The detailed step of the test is described as follows.

Step 1. Pick 2000 pixels randomly;

Step 2. Perform correlation test in horizontal, vertical and diagonal direction by following formulas

$$r_{x,y} = \frac{E\{[x-E(x)][y-E(y)]\}}{\sqrt{D(x)}\sqrt{D(y)}} \quad (9)$$

$$E(x) = \frac{1}{N}\sum_{i=1}^{N} x_i \quad (10)$$

$$D(x) = \frac{1}{N}\sum_{i=1}^{N}[x_i - E(x)]^2 \quad (11)$$

In these formulas, x and y are values of two different pixels, E(x) is mathematical expectation of x, D(x) is variance of x, N is total number of sample pixels, the correlation coefficient calculation results are shown in Table 3.

Table 3 Comparison of pixels correlation coefficients of plain image and ciphered image

Coefficients	*Plain Image*	*Ciphered Image*
Horizontal	0.971616	0.00200584
Vertical	0.984931	-0.00255918
Diagonal	0.968348	0.00329009

From Table 3, the correlation coefficients of plain image are in the neighborhood of 1, while the correlation coefficients of ciphered image are in the neighborhood of 0. In order to show the correlation intuitively, the distribution of the horizontal correlation of adjacent pixels is shown in Fig. 7 .

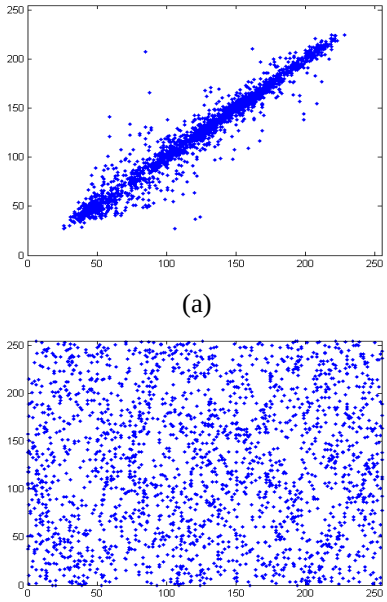


Fig. 7 Distribution of correlation coefficients: (a) distribution of the horizontal correlation coefficients of adjacent pixels of plain image, (b) distribution of the horizontal correlation coefficients of adjacent pixels of ciphered image

Similar results can be obtained on vertical and diagonal direction as well. The analysis above shows that the correlation of adjacent pixels is eliminated and the ciphered image has great randomness.

5.6 Information entropy analysis

In information theory, entropy is one of the most significant feature of disorder, or more precisely unpredictability. To calculate the entropy H(m) of a source m, the formula is given as follows.

$$H(m) = \sum_{i=0}^{2^N-1} p(m_i)\log\frac{1}{p(m_i)} \quad (12)$$

where N is the number of bits to represent a symbol $m_i \in m$ and $p(m_i)$ represents the probability of symbol m_i, so that the entropy is expressed in bits. For a truly random source emitting 2N symbols, the entropy is $H(m) = N$. Therefore, for a ciphered image with 256 gray levels, the entropy should ideally be $H(m) = 8$.

5.7 Key Sensitivity analysis

Ⅰ. Key sensitivity in encryption stage

Key sensitivity is a very important index of a cryptosystem. That means tiny key difference will cause completely different encryption results. On the other hand, it will not be broken even with very similar key. Compared with conventional methods, the advantage of chaos-based system is the extreme sensitivity of initial value.

In order to test the sensitivity of key, we modify the key from (4.3234565432，0.135264897) to (4.3234565432，0.135264898), that is only 0.000000001 different from the true parameter. The results of the test is shown in Fig. 8. By comparison, we found that 99.63% of the pixels are different, that is the key sensitivity performance of proposed scheme.

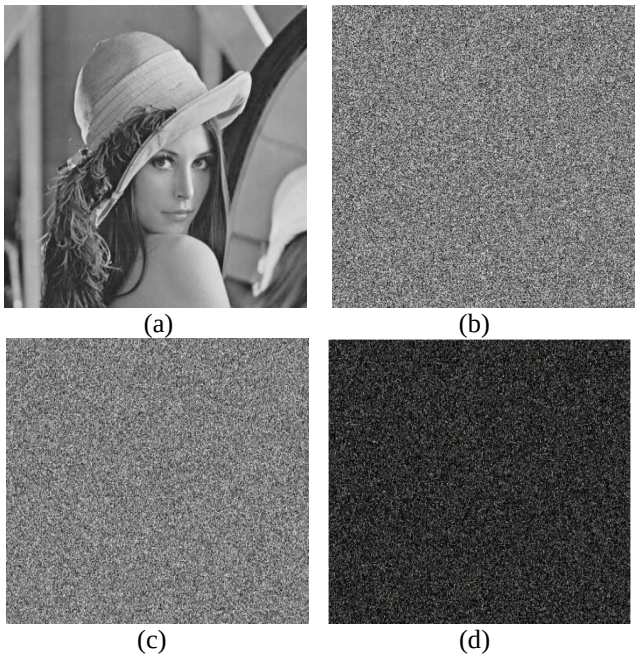


Fig. 8 Key sensitivity test in encryption stage: (a) plain image, (b) ciphered image with original key, (c) ciphered image with modified key, (d) difference of the two ciphered images

Ⅱ. Key sensitivity in decryption stage

In this test, initial key is employed to encrypt and decrypt one Lenna image, then we use modified key to decrypt it, the results is shown in Fig. 9. The initial key is (4.3234565432，0.135264897), and the modified key is (4.3234565433，0.135264898).

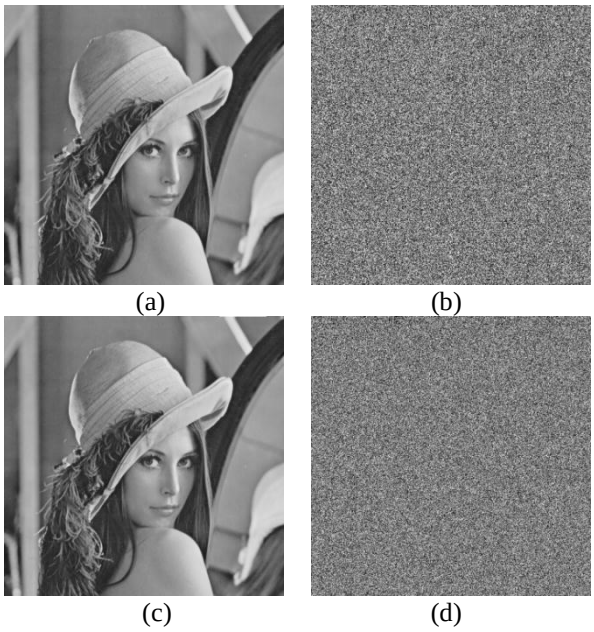


Fig. 9 Key sensitivity test in decryption stage: (a) plain image, (b) ciphered image with initial key, (c) deciphered image with initial key, (d) deciphered image with modified key

By comparison, we can see that 0.0000000001 difference of key will cause completely unrecognizable result; it demonstrates the method is of great key sensitivity.

6. Conclusions

This paper proposed a chaotic color image encryption method. A color image is divided into three color channel. Then we use a bit-level permutation in each channel and introduce diffusion scheme into permutation stage. In permutation stage, both the position and pixel value are changed using Arnold-Cat map simultaneously. This improved scheme protects the shuffled image from being broken in permutation stage and reduces the iterative round of substitution. Meanwhile this scheme improves the security of permutation module and hence significantly increases the overall encryption speed and enhances the security level. The results of security and speed analysis are very encouraging which indicate that this cryptosystem serves as a good candidate for real-time secure image transmission over the Internet and through wireless networks.

Acknowledgments

Portions of the research in this paper are supported by the National Nature Science Foundation of China (No. 61174145).

References

[1] Chong Fu, Bin-bin Lin, Yu-sheng Miao, Xiao Liu and Jun-jie Chen, "A Novel Chaos-based Bit-level Permutation Scheme for Digital Image Encryption", Optics Communications, 284, 23, 2011, 5415-5423.
[2] Josef Scharinger, "Fast encryption of image data using chaotic Kolmogorov flows", Journal of Electronic Imaging 7, 2, 1998, 318-325.
[3] Jiri Fridrich, "Symmetric ciphers based on two-dimensional chaotic maps", International Journal of Bifurcation and Chaos, 8, 6, 1998, 1259-1284.
[4] Chen GR, Mao YB, Chui CK, "A symmetric image encryption scheme based on 3D chaotic cat maps", Chaos, Solitons &Fractals, 21, 3, 2004, 749-761.
[5] Mao YB, Chen GR and Lian SG, "A novel fast image encryption scheme based on 3D chaotic Baker maps", International Journal of Bifurcation and Chaos, 14, 10, 2004, 3613-3624.
[6] R. Rhouma, S. Meherzi and S. Belghith, "OCML-based colour image encryption, Chaos", Solitons & Fractals, 40, 1, 2009, 309-318.
[7] I.F. Elashry, O.S.F. Allah, A.M. Abbas, et al., "Homomorphic image encryption", Journal of Electronic Imaging, 18, 3, 2009, 033002.
[8] 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, 2009, 2652-2663.
[9] IEEE Computer Society. IEEE standard for binary floating-point arithmetic, ANSI/IEEE std. 754-1985, August 1985.
[10]Jolfaei, A. and A. Mirghadri, "Survey: image encryption using Salsa20", International Journal of Computer Science Issues, 7, 5, 2010, 213-220.
[11]A. B. Abugharsa and Hamida Almangush, "A Novel Image Encryption using an Integration Technique of Blocks Rotation based on the Magic cube and the AES Algorithm", International Journal of Computer Science Issues, 4, 1, 2012, 41-47.

Jianjiang CUI received his PhD degree from Northestern University, China. He is currently the Assistant Professor of Northestern University, China. He also serves as the committee member of the Chinese Association of Automation. His major research interests are Industrial process control, computer simulation and digital image processing.

Siyuan LI received the BS degree in automation in 2012 from the Northeastern University, China. He is currently working toward the MS degree at Northestern University, China. His current areas of interest include information security, pattern recognition and image processing.

Dingyu XUE received his PhD degree in 1992 from Sussex University, UK. He is currently the Professor of Northestern University, China. His major research interests are Fractional control system, computer-aided design of control system, system simulation and virtual reality, intelligent image processing technology and network control.