Journal of ELECTRICAL ENGINEERING, VOL. 65, NO. 2, 2014, 90–96

IMAGE ENCRYPTION BASED ON CHAOTIC MAP AND REVERSIBLE INTEGER WAVELET TRANSFORM

Xiaopeng Wei — Bin Wang — Qiang Zhang — Chao Che *

In recent years, there has been growing interesting in image encryption based on chaotic maps and wavelet transform. In this paper, a novel scheme for image encryption based on chaotic maps and reversible integer wavelet transform is proposed. Firstly, the cipher key which is related to plain-image is used to generate different parameters and initial values of chaotic maps. Then the plain-image is permuted by the order from chaotic maps, and processed by integer wavelet transform. A part of transform coefficient is diffused by the orbits of chaotic maps. Finally, the cipher image is obtained by inverse integer wavelet transform based on the diffused coefficient. Numerical experimental results and comparing with previous works show that the proposed scheme possesses higher security than previous works, which is suitable for protecting the image information.

K e y w o r d s: integer wavelet transform; image encryption; chaotic map; chaos

1 INTRODUCTION

Along with significant improvements in computer and internet technology, it has created an environment in which it is very easy to disclose important information by illegal users, such as personal image. For this reason, the study of image encryption has become an important aspect of protecting security of image information. Since digital image possesses some inherent features such as bulk data capacity and high correlation among adjacent pixels, the algorithms of image encryption are different from the traditional text cryptographic method. At the same time, due to their features of ergodicity, sensitivity to initial conditions and control parameters, *etc*, chaotic maps have good potential for information encryption, especially image encryption. Inspired by the subtle similarity between chaotic map and cryptography, a large number of chaos-based image encryption algorithms had been proposed [1–8].

In [1], the authors generalized two-dimensional chaotic cat map to 3D for designing a real-time secure symmetric encryption scheme, used 3D cat map to permute the position of image pixels in the permutation stage and employed logistic chaotic system to diffuse the permuted image in the diffusion stage. In [2], the authors firstly analyzed the parameter sensitivity of standard map, and compared the secret key space of standard map with that of cat map and baker map. Then an improved standard map was used to realize position permutation, while the diffusion function consisted of logistic map that was used to realize the diffusion of image. In [3], the authors introduced a certain diffusion effect in the permutation stage by simple sequential add-and-shift operations. Although that led to a longer processing time in a single round, the overall encryption time was reduced as fewer rounds were required. In [4], the authors proposed a chaos-based image encryption algorithm with variable control parameters. The control parameters used in the permutation stage and the keystream employed in the diffusion stage were generated from two chaotic maps related to the plain-image. A fast image encryption algorithm combined with permutation and diffusion was proposed in [5], the image was partitioned into blocks of pixels. Then, spatiotemporal chaos was employed to shuffle the blocks, and at the same time, to change the pixel values. Meanwhile, an efficient method for generating pseudorandom numbers from spatiotemporal chaos was suggested, which further increases the encryption speed. A novel image encryption algorithm based on a three dimensional (3D) chaotic map that could defeat the aforementioned attack among other existing attacks was proposed in [6]. The design of the proposed algorithm was simple and efficient, and based on three phases which provided the necessary properties for a secure image encryption algorithm including the confusion and diffusion properties. In [7], this paper proposed a novel chaos-based image encryption algorithm to encrypt color images by using a Coupled Two-dimensional Piecewise Nonlinear Chaotic Map, called CTPNCM, and a masking process. Distinct characteristics of the algorithm were high security, high sensitivity, and high speed that could be applied in encryption of color images. In [9], the authors designed a new shuffling schemes that could efficiently destroy redundancy in the visual data ensuring its secured transmission and distribution over public networks. In [10], the issues pertaining with efficient, fast, cost effective and secured image transmission were addressed in totality. The proposed model employs Compressed Hybrid Cryptosystem constituted compression, encryption and secured session key exchange along with the transmission of image. In the proposed work, the algorithm had been designed to generate diffusion template using 3D Standard map.

* Key Laboratory of Advanced Design and Intelligent Computing (Dalian University), Ministry of Education, Dalian, 116622, China, zhangq@dlu.edu.cn

DOI: 10.2478/jee-2014-0013, Print ISSN 1335-3632, On-line ISSN 1339-309X,

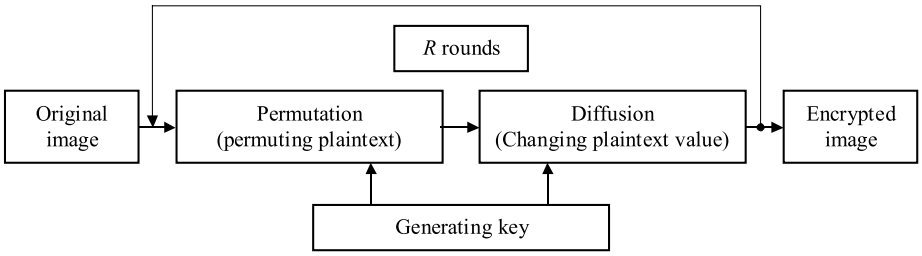


Fig. 1. Flowchart of permutation-diffusion type of chaos-based image cryptosystems

As an important method, wavelet transforms are widely used in image processing, such as image compression and image watermarking. A number of works on image compression and image watermarking are based on reversible integer wavelet transform [11–14]. In [11], the authors presented the factors affecting the compression performance of reversible integer-to-integer wavelet transforms, and supported by both experimental data and theoretical arguments. In [12], the author used the reversible integer wavelet transform to implement the technique of difference expansion, which was widely employed in image watermarking. The Ref. [13] proposed a high capacity reversible image watermarking scheme based on integer-to-integer wavelet transforms. It divided an input image into non-overlapping blocks and embedded a watermark into the high-frequency wavelet coefficients of each block. An intelligent reversible watermarking approach GA-RevWM for medical images was proposed in [14]. GA-RevWM was based on the concept of block-based embedding using genetic algorithm (GA) and integer wavelet transform (IWT).

However, in recent years, many proposed chaotic cryptosystems are broken by some kinds of cryptanalysis [1, 15–17]. The main broken reasons can be briefly stated as follows: (1) in the different rounds, the same control parameters for permutation are used; (2) the key stream obtained from the chaotic map only depends on the key, namely the parameters or initial value of chaotic map. Using the first loophole, the attacker can easily divide the permutation-diffusion process into two unrelated stages by choosing the plain-image with identical pixels [4]. Due to the second loophole, the attacker can obtain the key stream, which is extracted from the chaotic map in the diffusion, by the cryptoanalytic solution, such as known-plaintext and chosen-plaintext attacks [18–20].

In this paper, a novel scheme for image encryption based on chaotic map and reversible integer wavelet transform is proposed. The initial key is randomly generated, and relates to plain-image to generate cipher key, which is used as the different parameters and initial values of chaotic maps. It can overcome the flaws above. The plain-image is firstly permuted by the order from chaotic maps. Then the permuted image is processed by integer wavelet transform. In order to diffuse the image, a part of coefficient is diffused by the obits of chaotic maps. Finally, the inverse integer wavelet transform is used to obtain the cipher image based on the diffused coefficient. Numerical experimental results and comparing with previous works show that the proposed scheme possesses higher security than previous works, which is suitable for protecting the image information.

The paper is organized as follows. In the next section, the related works are described in detail. In Section 3, the process of encryption and decryption is described in detail. Performance analyses and simulation results are reported in Section 4. Finally, conclusions are drawn in Section 5.

2 RELATED WORKS

In [1], the authors proposed a general cryptographic chaos-based architecture for image encryption, namely permutation-diffusion architecture, which s shown as Fig. 1. This architecture includes two iterative stages, namely permutation stage and diffusion stage. The former permutes the plain-image but not change the value of pixel. The latter changes the value of pixel but not change the position of pixel. In order to improve encryption effect of algorithms, the whole permutation-diffusion round will be repeated R times.

2.1 Chaotic maps used in image encryption

There are three types of two-dimensional chaotic maps which are widely used in the permutation stage, namely Standard chaotic map, Cat chaotic map and generalized Baker chaotic map [1, 2, 10]. Although these three chaotic maps can effectively confuse the position of image pixel in the permutation stage, some parameters used in the in the permutation stage may cause a secure loophole [4, 19, 20]. There are many works on these chaotic maps, such as parameter space, key space, and iteration time. More details of this step can be obtained from [2, 21–23].

In the diffusion stage, logistic map and tent map are frequently employed to generate the key stream or subkey for the stream cipher or block ciphers, respectively, and change the value of pixels which have been permuted [2, 3, 17]. It can be denoted as follows

$$x_{i+1} = \mu x_i(1 - x_i)\,. \tag{1}$$

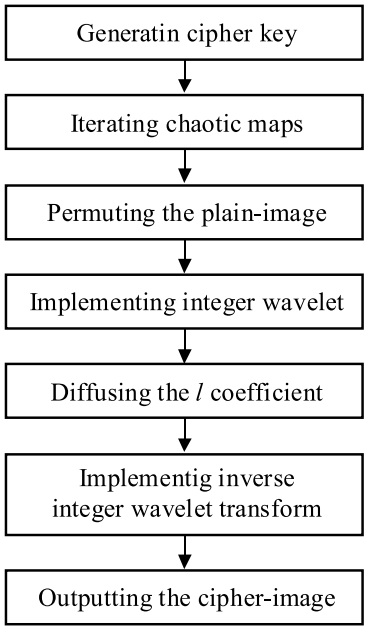


Fig. 2. The flowchart of encryption

Here, μ is control parameter for chaotic map, x_i and x_{i+1} are the ith and the $(i+1)$th state of chaotic map, respectively. Some other chaotic map can be employed in the diffusion stage, such as Chen's chaotic system, Lorentz chaotic system and so on [16, 23, 24]. However, these chaotic systems are more complex the logistic map and tent map, which makes the rise of runtime of chaos-based image encryption. Designing fast image encryption architecture, the complex chaotic map is not advised to use. A number of works related on the logistic map and tent map have been published, including parameter sensitivity, initial value sensitivity, statistical properties and degradation phenomenon [25, 26]. So we use two logistic maps with different parameters and initial value to implement the permutation-diffusion architecture in this paper.

2.2 Reversible integer wavelet transform

Recently, reversible integer wavelet transforms are widely used in image compression and image watermarking. A reversible integer wavelet transform is used in this paper. It can be denoted as follows

$$l = \left\lfloor \frac{x+y}{2} \right\rfloor , \; h = x - y \, . \tag{2}$$

Inverse transform of (2) is

$$x = l + \left\lfloor \frac{h+1}{2} \right\rfloor , \;\; y = l - \left\lfloor \frac{h}{2} \right\rfloor \tag{3}$$

The reversible integer transforms (2) and (3) are also called integer Haar wavelet transform, or the S transform. The reversible integer transforms set up a one-to-one correspondence between (x, y) and (l, h) [12]. For example, we have a pair pixels $x = 156, y = 141$. Then, by (2), $l = \lfloor \frac{156+141}{2} \rfloor = 148$, $h = 156 - 141 = 15$. Recovering the original pixels $x = l + \lfloor \frac{h+1}{2} \rfloor = 148 + 8 = 156$, $y = l - \lfloor \frac{h}{2} \rfloor = 148 - 7 = 141$ by (3).

2.3 Preventing the overflow and underflow problems

For the gray image, to prevent the overflow and underflow problems, it must restrict x, y in the range of $[0.255]$. From (3), it is equivalent to have $0 \le l + \lfloor \frac{h+1}{2} \rfloor \le 255$, and $0 \le l - \lfloor \frac{h}{2} \rfloor \le 255$. Then, $-\lfloor \frac{h+1}{2} \rfloor \le l \le 255 - \lfloor \frac{h+1}{2} \rfloor$, and $\lfloor \frac{h}{2} \rfloor \le l \le 255 + \lfloor \frac{h}{2} \rfloor$. For the different values of h, there is

$$\begin{aligned} \left\lfloor \frac{h}{2} \right\rfloor \le l \le 255 - \left\lfloor \frac{h+1}{2} \right\rfloor , \; h \ge 0 \, , \\ -\left\lfloor \frac{h+1}{2} \right\rfloor \le l \le 255 + \left\lfloor \frac{h}{2} \right\rfloor , \; h < 0 \, . \end{aligned} \tag{4}$$

One can derive that the above inequalities are equivalent to:

$$\begin{aligned} 0 \le l - \left\lfloor \frac{h}{2} \right\rfloor \le 255 - \left\lfloor \frac{h+1}{2} \right\rfloor - \left\lfloor \frac{h}{2} \right\rfloor , \; h \geqslant 0 \, , \\ 0 \le l + \left\lfloor \frac{h+1}{2} \right\rfloor \le 255 + \left\lfloor \frac{h}{2} \right\rfloor + \left\lfloor \frac{h+1}{2} \right\rfloor , \; h < 0 \, . \end{aligned} \tag{5}$$

3 THE PROCESS OF ENCRYPTION AND DECRYPTION

3.1 Encryption algorithm

According to the characteristic of logistic map, logistic map is chosen as the chaotic map in the proposed architecture. The different parameters and initial values for Eq (1) are denoted as μ_1, μ_2, $x_1(0)$ and $x_2(0)$, respectively, where $\mu_1, \mu_2 \in [3.9, 4]$ and $x_1(0), x_2(0) \in (0, 1)$. Ikey is denoted as the initial key. The detailed of encryption is described as follows:

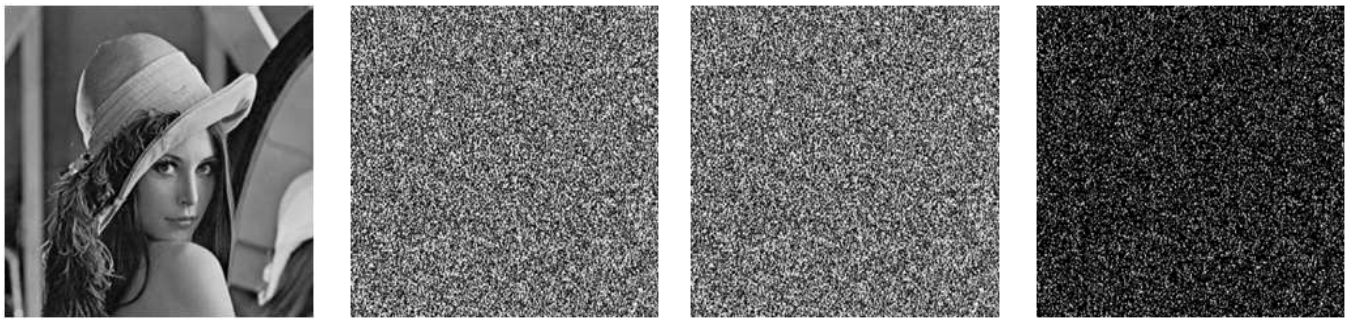
Step 1. Randomly generating the initial key and obtaining cipher key by relating to the plain-image;

Step 2. Evenly dividing cipher key into four parts as the parameters and initial values of logistic maps, iterating logistic maps for Q times to get rid of the transient effect, where $Q = 100$;

Step 3. Sorting the chaotic orbit obtained from previous step from small to large, and permuting the plain-image by this order only once

$$Mim(i) = permute\big(P(i), Order(i)\big) \, , \; i = 1, 2, \ldots M * N \, ; \tag{6}$$

Step 4. Processing the permuted image by integer wavelet transform, namely by (2), and obtaining the transform coefficient l, h;



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

Fig. 3. (a) – Plain-image of Lena, (b) – Encrypted image by key 1234567890123456, (c) – Encrypted image by key 1234567890123457, (d) Difference image

Step 5. Obtaining new coefficient l' based on (7);

$$\begin{aligned} l' &= l - \left\lfloor \frac{h}{2} \right\rfloor,\ h \geq 0\,, \\ l' &= l + \left\lfloor \frac{h+1}{2} \right\rfloor,\ h < 0\,; \end{aligned} \tag{7}$$

Step 6. Diffusing the coefficient l once by the logistic chaotic orbits

$$Cl(i) = l'(i) \oplus Orbit(i)\,,\ i = 1, 2, \ldots, M * N/2\,; \tag{8}$$

Step 7. Recovering image by inverse integer wavelet transform with the diffused coefficient l, and obtaining the cipher-image;

Step 8. Output the cipher-image.

Where $P(i)$ is the original image pixel value, $Mim(i)$ is the pixel value permuted by the order, $Order(i)$ is the ordered position of $P(i)$, $Orbit(i)$ are the logistic chaotic orbit from step 2, and $Cl(i)$ is the diffused coefficient l'. M and N are the width and height of the plain-image. $\oplus$ denotes the xor operator.

Note that implementing the Step 5 is convenient to deal with the overflow and underflow problems while calculating (8). If $Cl(i)$ out off the constraint from (5), $Cl(i)$ is processed by

$$\begin{aligned} &\mathrm{mod}\Big(Cl(i), 255 - \left\lfloor \tfrac{h+1}{2} \right\rfloor - \left\lfloor \tfrac{h}{2} \right\rfloor\Big),\ h \geq 0\,, \\ &\mathrm{mod}\Big(Cl(i), 255 + \left\lfloor \tfrac{h}{2} \right\rfloor + \left\lfloor \tfrac{h+1}{2} \right\rfloor\Big),\ h < 0\,. \end{aligned} \tag{9}$$

And the scheme saves the location of i for decrypting the cipher image in one piece. The detailed of encryption is illustrated in Fig. 2.

3.2 Decryption algorithm

The decryption process is similar to that of encryption procedure in the reversed order. It can be briefly stated as follows *Step* 1. Iterating the logistic maps for Q times to get rid of the transient effect;

Step 2. Concurrently generating the chaotic orbits and order as encryption process;

Step 3. Obtaining $Orbit(i)$ and $Order(i)$;

Step 4. Implementing integer wavelet transform and obtaining the coefficient Cl, h;

Step 5. Recovering the $l(i)$ by (10)

$$l(i) = \mathrm{Cl}(i) \oplus Orbit(i)\,,\ i = 1, 2, \ldots, M * N/2\,; \tag{10}$$

Step 6. Implementing inverse wavelet transform by the coefficient l and h, and obtaining the $Mim(i)$;

Step 7. Recovering the $P(i)$ by (11)

$$P\big(\mathrm{Order}(i)\big) = Mim(i)\,,\ i = 1, 2, \ldots, M * N\,; \tag{11}$$

Step 8. Outputting the plain-image.

4 PERFORMANCE ANALYSES AND SIMULATION

4.1 The space of key

In a good image cryptosystem, the space of key should be enough large to make brute-force attack infeasible. In this proposed architecture, the Ikey consists of 16 elements, namely Ikey $= \{x_i\}$, $i = 1, 2, \ldots, 16$, $x_i \in [0, 255]$. So the key space of the proposed architecture is equal to $2^{128} \approx 3.4 \times 10^{38}$, which is sufficiently large to meet the need for practical application.

4.2 Key sensitivity

In this part, the key sensitivity will be performed as follows:

Step 1. Calculate the Imkey of the standard test 256×256 image Lena;

Step 2. Encrypt the test image by Ikey 1234567890123456;

Step 3. Slightly change the generated Ikey 1234567890123457, and encrypt the same plain-image;

Step 4. Compare the cipher-image which is encrypted by different key.

The results are: the image encrypted by the key 1234567890123456 has 99.59 % of different from the image encrypted by the key 1234567890123457 in terms of

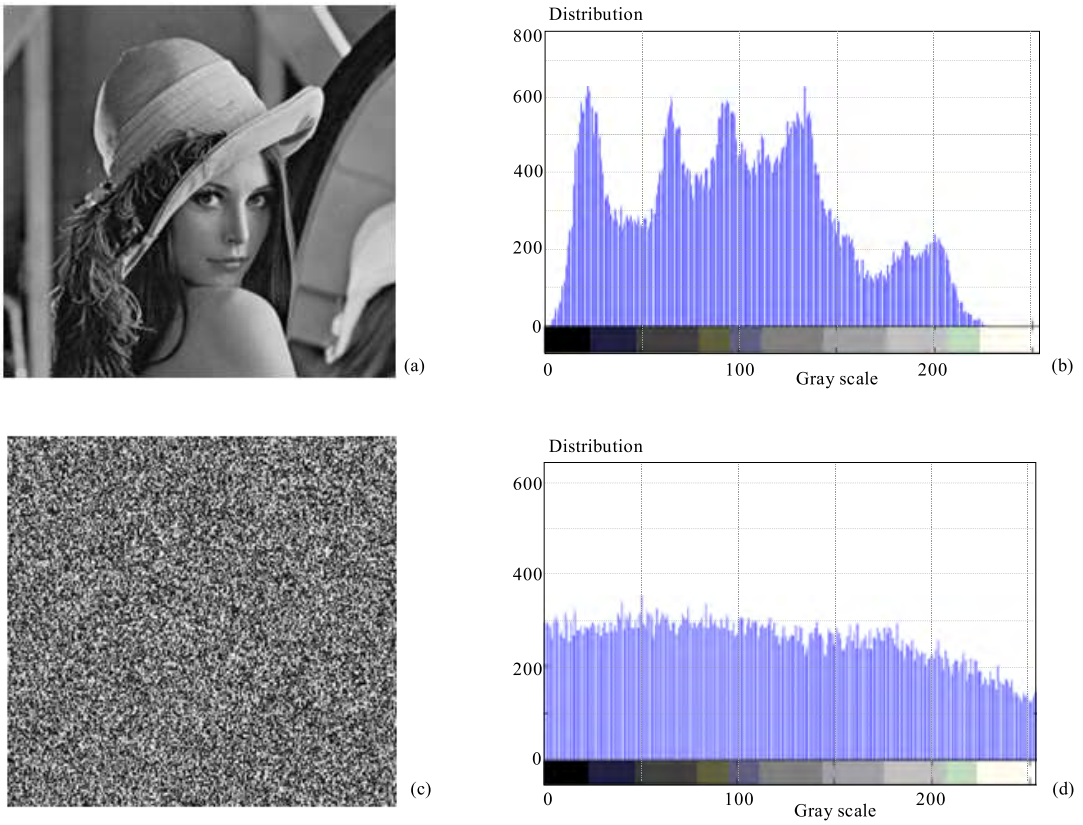


Fig. 4. (a) – plain-image of Lena, (b) – histogram of the plain-image, (c) – cipher-image, (d) – histogram of the cipher-image

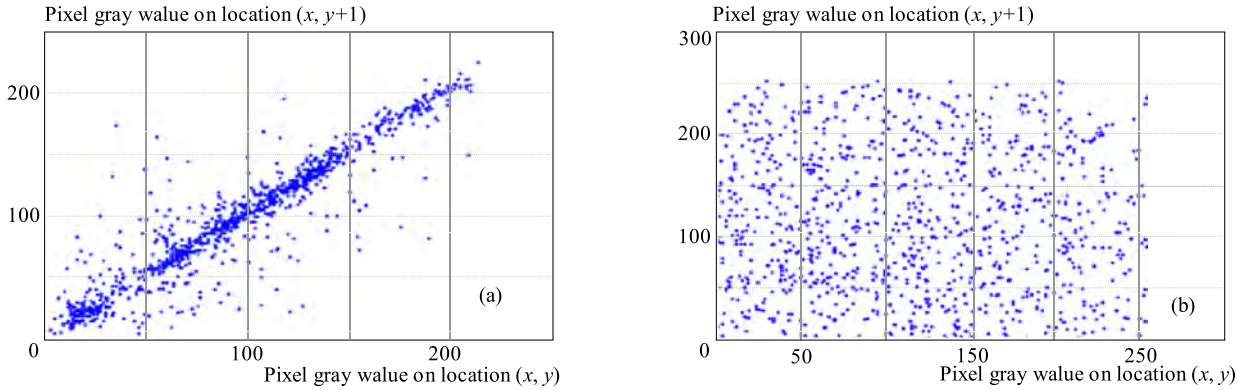


Fig. 5. (a) – the correlation of vertical adjacent two pixels for original image, (b) – the correlation of vertical adjacent two pixels for cipher-image

pixel values, although there is only one bit difference in the two keys. Figure 3 shows the test result. Moreover, when a key is used to encrypt an image while another trivially changed key is used to decrypt the ciphered image, the decryption also completely fails.

4.3 Statistical analysis

As Shannon said: 'It is possible to solve many kinds of ciphers by statistical analysis' [27]. Therefore, he suggested two methods of diffusion and confusion should be used in any cryptosystems. In this proposed architecture, the standard Lena test image of size 256×256 is selected to test the property of resisting statistical analysis.

The histograms of encrypted image are shown in Fig. 4. From the figure, one can see that the histogram of the ciphered image is fairly uniform and is significantly different from that of the original image. To test the correlation between two vertically adjacent pixels, two horizontally adjacent pixels, and two diagonally adjacent pixels, respectively, in a ciphered image, the following procedure is carried out. First, randomly select 1000 pairs of two adjacent pixels from an image. Then, calculate the correlation coefficient of each pair by using the following two

Table 1. Comparing results

	NPCR	UACI
Proposed scheme	99.59%	28.21%
Wang's work	44.27%	14.874%
Gupta's work	99.62%	17.30%

formulas [1]

$$\operatorname{cov}(x,y) = E\big\{\big(x - E(x)\big)\big(y - E(y)\big)\big\}\,, \tag{12}$$

$$R_{xy} = \frac{\operatorname{cov}(x,y)}{\sqrt{D(x)}\sqrt{D(y)}} \tag{13}$$

Where x and y are grey-scale values of two adjacent pixels in the image. In numerical computation, the following discrete formulas are employed

$$E(x) = \frac{1}{N}\sum_{i=1}^{N} x_i\,, \tag{14}$$

$$D(x) = \frac{1}{N}\sum_{i=1}^{N}\big(x_i - E(x)\big)^2, \tag{15}$$

$$\operatorname{cov}(x,y) = \frac{1}{N}\sum_{i=1}^{N}\big\{\big(x_i - E(x)\big)\big(y_i - E(y)\big)\big\}. \tag{16}$$

Figure 5 shows the correlation distribution of two vertically adjacent pixels in the plain-image and that in the cipher-image: the correlation coefficients are 0.9299 and -0.0039, respectively, which are far apart.

4.4 Differential attack

To test the property of resisting differential attack of the proposed architecture, two common quantitative criteria are employed: number of pixels change rate (NPCR) and unified average changing intensity (UACI). The NPCR and UACI are defined as follows [10, 28]

$$NPCR = \frac{\sum_{i,j} D(i,j)}{W \times H} \times 100\%\,, \tag{17}$$

$$UACI = \frac{1}{W \times H}\Big[\sum_{i,j} \frac{|C_1}{(}i,j) - C_2(i,j)\big|255\Big] \times 100\% \tag{18}$$

where C_1 and C_2 are the two cipher-image whose corresponding Ikeys have only difference, the grey-scale values of the pixels at poison (I,j) of C_1 and C_2 are denoted as $C_1(i,j)$ and $C_2(i,j)$, respectively; W and H are the width and height of the cipher-image; $D(i,j)$ is determined by $C_1(i,j)$ and $C_2(i,j)$, namely, if $C_1(i,j) = C_2(i,j)$ then $D(i,j) = 0$ otherwise, $D(i,j) = 1$.

In the Table 1, we compare our results of NPCR with the Wang [5] and Gupta [10] works. The whole permutation-diffusion round is repeated only once. Our results are the average of ten trials. Comparing with previous works, it suggests that our scheme has higher security.

4.5 Resistance to known-plaintext and chosen-plaintext attacks

In the proposed scheme, this scheme uses different parameters and values of chaotic maps which are used in the permutation and diffusion stage to overcome the first flow. At the same time, it makes the cipher key related to the permuted image to overcome the second flow. So the different control conditions, key streams and non-identical cipher-images will be generated by distinct plain-images. The attacker cannot obtain useful information by encrypting some special images since the resultant information is only related to those chosen-images. Therefore, the proposed algorithm can well resist the known-plaintext and the chosen-plaintext attacks.

5 CONCLUSIONS

A novel scheme for image encryption based on chaotic maps and reversible integer wavelet transform has been proposed in this paper. The different parameters and initial values of chaotic maps are obtained by cipher key which is related to the plain-image. Then the order is from chaotic maps that are used to permute plain-image. Subsequently, the permuted image is processed by integer wavelet transform. The coefficient is diffused by the orbits of chaotic maps. Finally, the cipher image is obtained by inverse integer wavelet transform based on the diffused coefficient. Numerical experimental results and comparing with previous works show that the proposed scheme possesses higher security than previous works, which is suitable for protecting the image information.

Acknowledgment

We would like to thank the anonymous reviewers for helpful comments. This work is supported by the National High Technology Research and Development Program ('863'Program) of China (No. 2009AA01Z416) the National Natural Science Foundation of China (31170797, 30870573), Program for Changjiang Scholars and Innovative Research Team in University(IRT1109), the Program for Liaoning Innovative Research Team in University(LT2011018), the Program for Liaoning Excellent Talents in University (LR201003), the Program for Liaoning Science and Technology Research in University (LS2010179) and the open fund of Key Laboratory of Advanced Design and Intelligent Computing (Dalian University), Ministry of Education, Dalian University (ADIC2010012).

References

[1] CHEN, G.—MAO, Y.—CHUI, C. K.: A Symmetric Image Encryption Scheme based on 3D Chaotic Cat Maps, Chaos, Solitons & Fractals **21** (2004), 749–761.

[2] LIAN, S.—SUN, J.—WANG, Z.: A Block Cipher based on a Suitable Use of the Chaotic Standard Map, Chaos, Solitons & Fractals **26** (2005), 117–129.

[3] WONG, K. W.—KWOK, B. S. H.—LAW, W. S.: A Fast Image Encryption Scheme based on Chaotic Standard Map, Physics Letters A **372** (2008), 2645–2652.

[4] WANG, Y.—WONG, K. W.—LIAO, X.—XIANG, T.—CHEN, G. A Chaos-Based Image Encryption Algorithm with Variable Control Parameters: Chaos, Solitons & Fractals **41** (2009), 1773–1783.

[5] WANG, Y.—WONG, K. W.—LIAO, X.—CHEN, G.: A New Chaos-Based Fast Image Encryption Algorithm, Applied Soft Computing **11** (2011), 514–522.

[6] KANSO, A.—GHEBLEH, M.: A Novel Image Encryption Algorithm based on a 3D Chaotic Map, Communications in Nonlinear Science and Numerical Simulation **17** (2012), 2943–2959.

[7] SEYEDZADEH, S. M.—MIRZAKUCHAKI, S.: Signal Processing **92** (2012), 1202-1215.

[8] TANEJA, N.—RAMAN, B.—GUPTA, I.: Selective Image Encryption in Fractional Wavelet Domain, AEU-International Journal of Electronics and Communications (2010).

[9] GUPTA, R.—AGGARWAL, A.—PAL, S. K.: Design and Analysis of New Shuffle Encryption Schemes for Multimedia, Defence Science Journal **62** (2012), 159–166.

[10] GUPTA, K.—SILAKARI, S.: Novel Approach for Fast Compressed Hybrid Color Image Cryptosystem, Advances in Engineering Software **49** (2012), 29-42.

[11] ADAMS, M. D.—KOSSENTNI, F.: Reversible Integer-to-Integer Wavelet Transforms for Image Compression: Performance Evaluation and Analysis, Image Processing, IEEE Transactions on **9** (2000), 1010–1024.

[12] TIAN, J.: Reversible Data Embedding using a Difference Expansion, Circuits and Systems for Video Technology, IEEE Transactions on **13** (2003), 890-896.

[13] LEE, S.—YOO, C. D.—KALKER, T.: Reversible Image Watermarking based on Integer-to-Integer Wavelet Transform, Information Forensics and Security, IEEE Transactions on **2** (2007), 321-330.

[14] ARSALAN, M.—MALIK, S. A.—KHAN, A.: Intelligent Reversible Watermarking in Integer Wavelet Domain for Medical Images, Journal of Systems and Software **85** (2012), 883–894.

[15] GUAN, Z. H.—HUANG, F.—GUAN, W.: Chaos-Based Image Encryption Algorithm, Physics Letters A **346** (2005), 153–157.

[16] GAO, T.—CHEN, Z.: A New Image Encryption Algorithm based on Hyper-Chaos, Physics Letters A **372** (2008), 394–400.

[17] YE, G.: Image Scrambling Encryption Algorithm of Pixel Bit based on Chaos Map, Pattern Recognition Letters **31** (2010), 347–354.

[18] GE, X.—LIU, F. L.—LU, B.—WANG, W.: Cryptanalysis of a Spatiotemporal Chaotic Image/Video Cryptosystem and its Improved Version, Physics Letters A **375** (2011), 908–913.

[19] HERMASSI, H.—RHOUMA, R.—BELGHITH, S.: Security Analysis of Image Cryptosystems only or Partially based on a Chaotic Permutation, Journal of Systems and Software **85** (2012), 2133–2144.

[20] ZHAO, L.—ADHIKARI, A.—XIAO, D.—SAKURAI, K.: On the Security Analysis of an Image Scrambling Encryption of Pixel Bit and its Improved Scheme based on Self-Correlation Encryption, Communications in Nonlinear Science and Numerical Simulation **17** (2012), 3303–3327.

[21] LIAN, S.—SUN, J.—WANG, Z.: Security Analysis of a Chaos-Based Image Encryption Algorithm, Physica A: Statistical Mechanics and its Applications **351** (2005), 645–661.

[22] ALVAREZ, G.—LI, S. Some Basic Cryptographic Requirements for Chaos-Based Cryptosystems: International Journal of Bifurcation and Chaos in Applied Sciences and Engineering **16** (2006), 2129.

[23] XIAO, D.—LIAO, X.—WEI, P.: Analysis and Improvement of a Chaos-Based Image Encryption Algorithm, Chaos, Solitons & Fractals **40** (2009), 2191–2199.

[24] GAO, T.—CHEN, Z.: Image Encryption based on a New Total Shuffling Algorithm, Chaos, Solitons & Fractals **38** (2008), 213–220.

[25] LI, S.—LI, Q.—LI, W.—MOU, X.—CAI, Y.: Statistical Properties of Digital Piecewise Linear Chaotic Maps and their Roles in Cryptography and Pseudo-Random Coding, Cryptography and Coding (2001), 205–221.

[26] LI, S.—CHEN, G.—MOU, X.: On the Dynamical Degradation of Digital Piecewise Linear Chaotic Maps, International JournAL of Bifurcation and Chaos in Applied Sciences and Engineering **15** (2005), 3119.

[27] SHANNON, C. E.: Communication Theory of Secrecy Systems, MD Computing **15** (1998), 57–64.

[28] KWOK, H.—TANG, W. K. S.: A Fast Image Encryption System based on Chaotic Maps with Finite Precision Representation, Chaos, Solitons & Fractals **32** (2007), 1518–1529.

Received 4 January 2013

Xiaopeng Wei is a professor at Dalian University of Technology and Dalian University, Dalian, China. His research areas include computer animation, intelligent CAD. So far, he has (co-) authored about 160 papers published.

Bin Wang is a doctoral student of School of Mechanical and Engineering at Dalian University of Technology Dalian, China. His research areas include DNA Computing, DNA Sequence designing, DNA Cryptography and Biological Network. So far, he has (co-) authored about 16 papers published.

Qiang Zhang is a professor at Dalian University, Dalian, China. His research interests are computer animation, intelligent computing. Now he has served as editorial boards of seven international journals and has edited special issues in journals such as Neurocomputing and International Journal of Computer Applications in Technology.

Chao Che is a lectuer at Dalian University, Dalian, China. He has received his PhD degree in 2010 from Dalian University of Technology.