一种自适应的图像加密算法*

陈 刚[1,2], 赵晓宇[1,2+], 李均利[1]

[1](宁波大学 数字技术与应用软件研究所,浙江 宁波 315211)

[2](浙江大学 图像图形研究所,浙江 杭州 310027)

A Self-Adaptive Algorithm on Image Encryption

CHEN Gang[1,2], ZHAO Xiao-Yu[1,2+], LI Jun-Li[1]

[1](Institute of DSP and Software Techniques, Ningbo University, Ningbo 315211, China)

[2](Institute of Imaging and Computer Graphics, Zhejiang University, Hangzhou 310027, China)

+ Corresponding author: Phn: +86-574-87600948, E-mail: imagelab@cms.zju.edu.cn, http://www.nbu-eied.net/DSP/~Zhaoxiaoyu

Received 2004-06-30; Accepted 2004-08-09

Chen G, Zhao XY, Li JL. A self-adaptive algorithm on image encryption. *Journal of Software*, 2005,16(11): 1975−1982. DOI: 10.1360/jos161975

Abstract: In this paper, a new self-adaptive image encryption algorithm is presented, which takes on a thorough integrity protect function and can be used in data validation. First, ergodic matrices are used to realize the position permutation algorithms. In particular, several novel methods of scrambling are proposed. By analysis of the weakness of pure position algorithms, a novel improved self-adaptive algorithm is proposed, which is strong under known-plaintext attack on image encryption. Finally the speed and safety of the new algorithm are analyzed and some simulation results are given.

Key words: ergodic; image scramble; self-adaptive; validate; encryption

摘 要: 给出一种新的自适应图像置乱加密算法,加密后的图像可以有效防止已知明文的攻击.并且,算法具有良好的完整性保护功能,可用于图像验证.实验结果表明,算法在运算速度、抗攻击能力等方面具有良好的效果.

关键词: 遍历;图像置乱;自适应;验证;加密

中图法分类号: TP309 文献标识码: A

1 Introduction

Due to the development of communications technology, information security becomes increasingly important. The wide use of multimedia technology and the improvement of network transmission gradually lead us to acquire

* Supported by the National Natural Science Foundation of China under Grant No.60302012 (国家自然科学基金); the Special Science and Technology Foundation of Ningbo of China under the Grant No.2005B100016 (宁波市科技攻关项目)

CHEN Gang was born in 1963. He is a professor in Zhejiang University. His researches areas are applied mathematics and image processing. **ZHAO Xiao-Yu** was born in 1978. He is an assistant professor in Ningbo University. His current research areas are applied mathematics, image processing and information security. **Li Jun-Li** was born in 1972. He is an associate professor in Ningbo University. His main research area is image processing.

information directly and clearly through images. Hence, data security has become a critical and imperative issue. In order to protect valuable data from undesirable reader, many encryption algorithms[1−12] have been proposed.

The basic ideas can be classified into three major types: position permutation[2−5], value transformation[6−8], and the combined form Refs.[9,10]. The position permutation scrambles the positions of original data, can be realized with ergodic matrices. In this paper, we introduce the concept of ergodic matrix, and use it to uniformly present scramble algorithms based on pixel shifting. The value transformation algorithms transform the signal value. For example, each pixel is transformed by a neural network in Ref.[6]. Finally, the combined form performs both position permutation and value transformation. For Example, Kuo *et al*.[9] encrypt the signal by scrambling its phase spectrum.

In this paper, we propose a new image encryption/decryption algorithm belonging to the category of the combined form. According to the weakness of pure position permutation algorithm[1], we improve a self-adaptive algorithm, which combine encryption method with the image's position and energy distribution information.

2 Ergodic Matrix

An $m\times n$ digital gray scale image can be noted as follows:

$$Q=\begin{bmatrix} q_{11} & q_{12} & \cdots & q_{1n} \\ q_{21} & q_{22} & \cdots & q_{2n} \\ \cdots & \cdots & \cdots & \cdots \\ q_{m1} & q_{m2} & \cdots & q_{mn} \end{bmatrix}$$

2.1 Conception and definition

2.1.1 Ergodicity

Definition 1. An ergodicity of a two dimensional matrix $Q_{m\times n}=\{q(i,j):1\le i\le m,1\le j\le n\}$ is a bijective function from $Q_{m\times n}$ to the set of $\{1,2,\ldots,mn-1,mn\}$. In other words, an ergodicity of a two dimensional matrix is an order in which each element of the matrix is accessed exactly once.

Example. Some common ergodic patterns are shown in Fig.1.

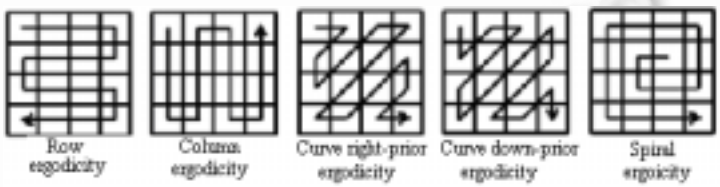


Fig.1 Some ergodicity patterns

2.1.2 Ergodic matrix

Definition 2. An $m\times n$ matrix R is defined as an ergodic matrix, if every element of which is in the set of $\{1,2,\ldots,mn\}$ and $r(i,j)=r(i',j')$, if and only if $i=i'$, $j=j'$. We note that $r_{(i-1)n+j}=r(i,j)$.

Example. A matrix as follows is defined as a main ergodic matrix.

$$\begin{pmatrix} 1 & 2 & 3 & \cdots & n \\ n+1 & n+2 & n+3 & \cdots & 2n \\ \cdots & \cdots & \cdots & \cdots & \cdots \\ (m-1)n+1 & (m-1)n+2 & (m-1)n+3 & \cdots & mn \end{pmatrix}_{m\times n}$$

In a similar way, we also present the definition of row, column, curve, spiral ergodic matrix, shown in Fig.2.

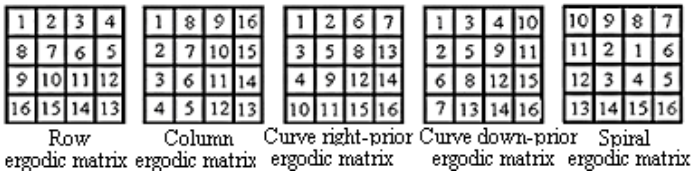


Fig.2 Some ergodic matrices

2.2 Ergodic matrix and permutation

A quick scrambling of image pixel permutation can be realized by ergodic matrix.

2.2.1 Realizing permutation by ergodic matrix

Example. For instance, we can make an Ergodicity of digital image matrix through the ergodic pattern represented by $R_{m\times n}$ and arrange the results line by line, shown in Fig.3. Hence, an image data permutation is realized.

$$Q_{4\times4}=\begin{bmatrix} q_{11} & q_{12} & q_{13} & q_{14} \\ q_{21} & q_{22} & q_{23} & q_{24} \\ q_{31} & q_{32} & q_{33} & q_{34} \\ q_{41} & q_{42} & q_{43} & q_{44} \end{bmatrix}_{4\times4} \xrightarrow{R=\begin{bmatrix} 7 & 2 & 10 & 3 \\ 15 & 1 & 9 & 11 \\ 4 & 6 & 8 & 13 \\ 14 & 12 & 16 & 5 \end{bmatrix}} \begin{bmatrix} q_{22} & q_{12} & q_{14} & q_{31} \\ q_{44} & q_{32} & q_{11} & q_{33} \\ q_{23} & q_{13} & q_{24} & q_{42} \\ q_{34} & q_{41} & q_{21} & q_{43} \end{bmatrix}_{4\times4}$$

Fig.3 Realizeing permutation by erogic matrix

2.2.2 Some ergodic matrix

Some ergodic matrices are listed as follows, shown in Fig.4.

$$\begin{bmatrix} 1 & 14 & 11 & 8 \\ 12 & 5 & 2 & 15 \\ 3 & 16 & 9 & 6 \\ 10 & 7 & 4 & 13 \end{bmatrix}_{4\times4} \qquad \begin{bmatrix} 6 & 7 & 10 & 11 \\ 5 & 8 & 9 & 12 \\ 4 & 3 & 14 & 13 \\ 1 & 2 & 15 & 16 \end{bmatrix}_{4\times4} \qquad \begin{bmatrix} 16 & 3 & 13 & 14 \\ 11 & 12 & 6 & 9 \\ 7 & 8 & 10 & 4 \\ 5 & 15 & 1 & 2 \end{bmatrix}_{4\times4}$$

Arnold permutation Hilbert permutation Magic square permutation

Fig.4 Ergodic matrices of basic permutation

Arnold permutation, Hilbert permutation and Magic square permutation mentioned above are limited to $n\times n$ matrices. Furthermore, some kinds of permutations are limited to particular degree, such as Hilbert permutation, which can only be realized for matrix with degree of 2^k (k=2,3,4,…). Meanwhile, due to the special matrix used for permutation, encryption security is reduced.

In the next section we propose some kinds of permutation algorithms induced from erogic matrix, having a better chaos property.

3 Standardization and Derivative Algorithms

3.1 Standardization of normal digital matrix

According to an ergodic pattern such as a main ergodicity, we list the elements in a matrix $Q_{m\times n}$, which hasn't been listed and appears the first time. At the same time, the appearance order of each element is recorded in the corresponding position in a new ergodic matrix $R_{m\times n}$. We denote $R_{m\times n}$ as an Ergodition of matrix $Q_{m\times n}$ by main ergodicity.

For an arbitrary matrix $Q_{m\times n}$, if its elements set is a sub-set of a totally ordered set, then $Q_{m\times n}$ can give birth to an new ergodic matrix sorted by the main ergodicity, shown in Fig.5.

Example.

$$\begin{pmatrix} 7.1 & 9.4 & 3.5 & 4.2 \\ 6.3 & 4.2 & 5.3 & 1.2 \\ 9.2 & 4.2 & 1.7 & 1.7 \\ 3.5 & 8.5 & 3.5 & 7.4 \end{pmatrix} \xrightarrow{based\_on\_main\_ergoditicity} \begin{pmatrix} 12 & 16 & 4 & 7 \\ 11 & 8 & 10 & 1 \\ 15 & 9 & 2 & 3 \\ 5 & 14 & 6 & 13 \end{pmatrix}$$

$Q_{4\times4}$ $R_{4\times4}$

Fig.5 Ergodic matrices of basic permutation

Note that, in this paper, all discussions are on the basis of main ergodicity without special explanation.

3.2 Permutation method deduced

3.2.1 Random-matrix permutation

In previous section, for each matrix, we can transform it into an ergodic one. Then, by using randomizer and setting user's password as seed, we can get $m\times n$ numbers to generate an digital matrix $P_{m\times n}$, which will produce an ergodic matrix $R_{m\times n}$. Shown in Fig.6.

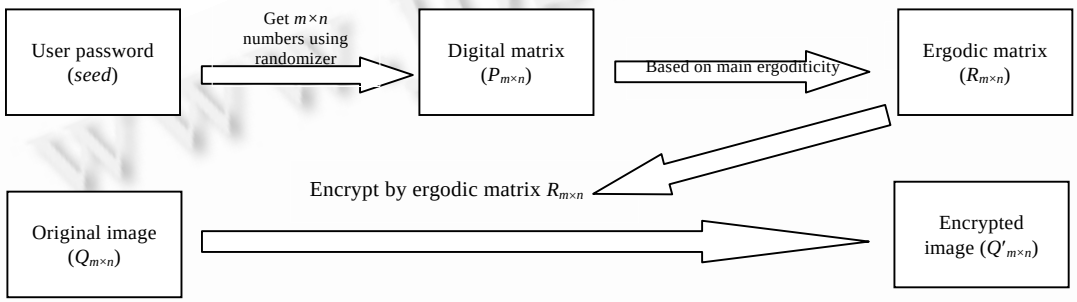


Fig.6 Sketch map of random-matrix permutation

3.2.2 Image-Aided permutation

First, we can choose an assistant image Q' with the same dimensions as the one waiting for encryption and then produce an ergodic matrix $R_{m\times n}$ using the pixel data of Q'.

Simple patching and shearing can solve the problem of dimensional unfitness when the dimensions of Q and Q' does not mate with each other.

Image-aided permutation is an easy and fast algorithm. Because there is a great deal of data in an image, just simple scrambling can make it difficult to distinguish the encrypted image from the original one.

We give an illustration in Fig.7.

4 Self-Adaptive Image Encryption

The position permutation algorithms[2−5], which scramble the positions of original data, can be uniformly realized with ergodic matrices. However, the weakness of pure position permutation algorithm is pointed out, and the decryption probability of pure-position permutation algorithms is verified theoretically using probability theory[1].

So we must improve permutation algorithm to defend the known-plaintext attack. Inspired by the image-aided permutation algorithm, maybe, we could encrypt images by the data.

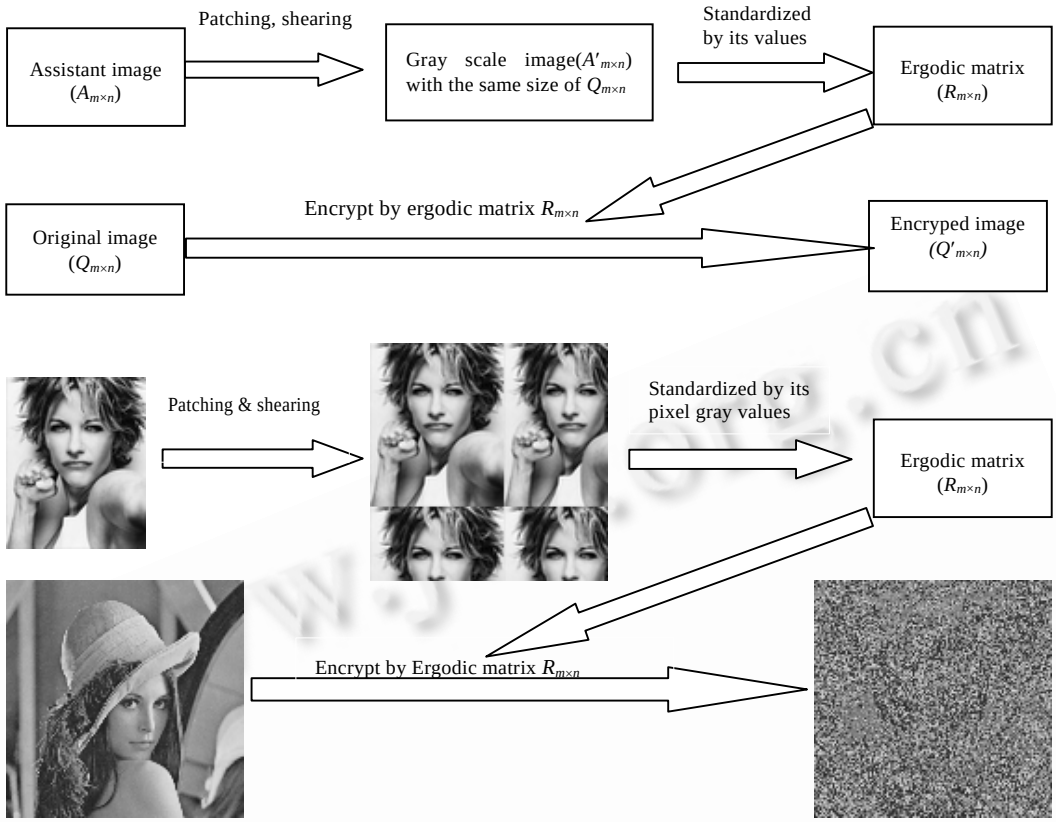


Fig.7 Sketch map of image-aided permutation

4.1 Encryption rule

We define encryption rules as follows, shown in Fig.8.

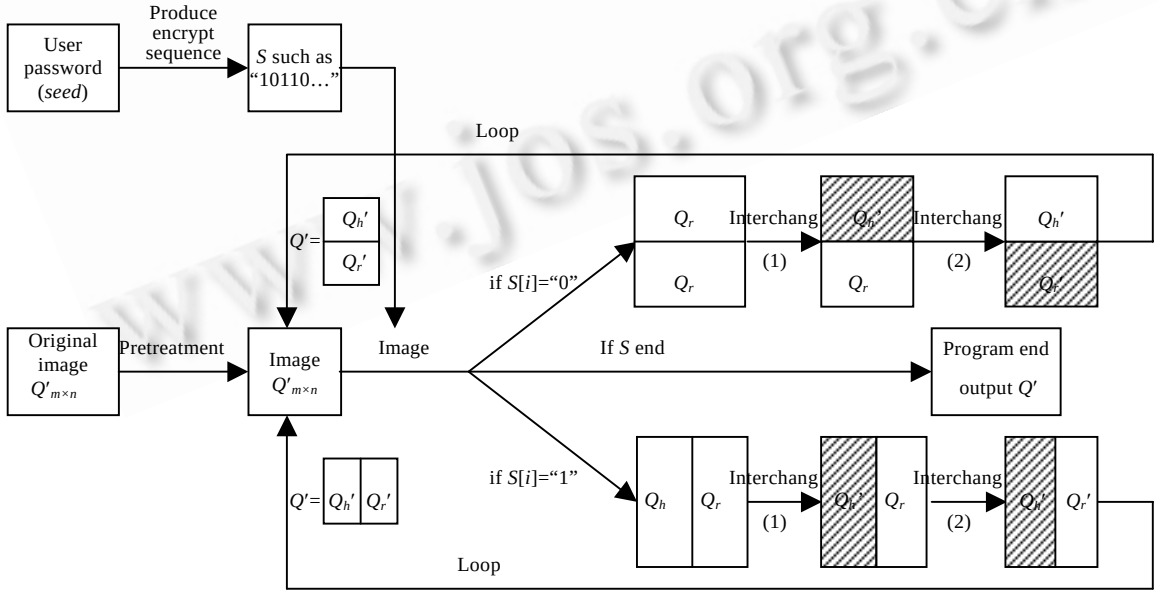


Fig.8 Flow chart of self-adaptive encryption algorithm

Step 1. Produce encryption sequence

At first, we get user's password and change it into a binary stream S, such as "1010110…". In the encryption system, "0" and "1" have been explained as ergodic patterns, which are noted as R_0 and R_1 respectively.

Step 2. Pretreatment

Before encryption, we scramble the image Q first. For example, we can use Hilbert erogdicity.

Step 3. Image division

We divide the image Q into two equal parts(head part Q_h and rear part Q_r), by the ergodic pattern of R_0 or R_1, according to the following:

$$\begin{cases} \text{divided by } R_0 \text{ pattern} & \text{if } S[i]=\text{"0"} \\ \text{divided by } R_1 \text{ pattern} & \text{if } S[i]=\text{"1"} \\ \text{program end} & \text{if the binary stream } S \text{ end} \end{cases}$$

Step 4. Interchange encryption

First, we standardize Q_r to R_{Q_r}, then use R_{Q_r} to scramble Q_h to Q_h'. Second, we standardize Q_h' to $R_{Q'_h}$, then use $R_{Q'_h}$ to scramble Q_r to Q_r'. Finally, we combine Q_h' and Q_r' together.

① if S_i=0 ② if S_i=1

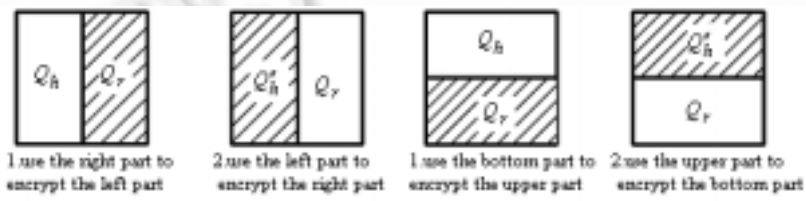


Fig.9 Sketch map of self-adaptive encryption sheering

Step 5. Loop

After this, we continue as following:

$$\begin{cases} \text{go to Step 3} & \text{if binary stream not end;} \\ \text{program end, return} & \text{if binary stream end} \end{cases}$$

4.2 Speed and safety

(1) The speed of the algorithm is very fast.

(2) The algorithm is strong under known-plaintext attack.

4.3 Data validity

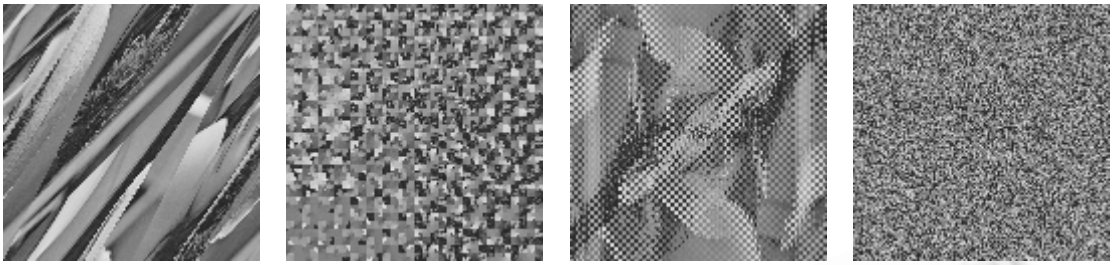
In image-aided encryption algorithm, if the assistant image has one pixel different with the original one, the recover result is different obviously. This is named ergodic matrix encryption's chaos property. If the encrypted image data have few loss during transformation, it can't be recovered. For its location information have been changed, if transform it some times, the difference is expanded distinctly and it can't be recovered. We can use this to validate the data.

Moreover, we can prove that encryption affection has relation with encrypt order, namely, if one bit is not accorded, the encrypted image can't be recovered.

5 Simulation Results and Conclusions

We select gray image of size 128×128, called "Lenna", as image waiting for encryption, and use pure position algorithm and self-adaptive encrypt algorithm respectively

5.1 Pretreatment using pure-permutation algorithms (shown in Fig.10)



Arnold Hilbert Magic-Square Random-Matrix

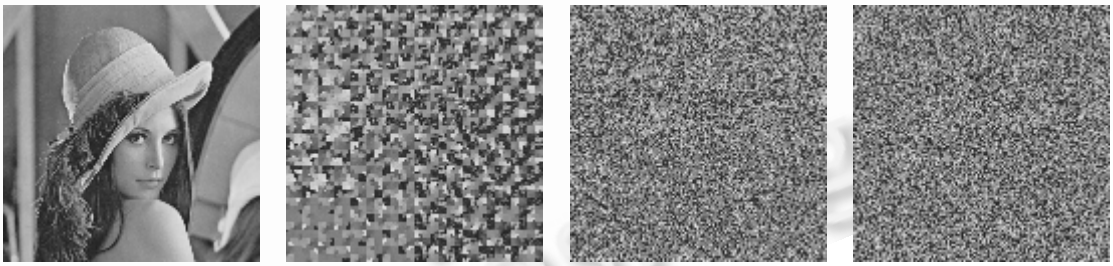
Fig.10 Some pure permutation algorithms iterative once

5.2 Image division (shown in Fig.11)

Original image Divided pattern After Interchange (1) After Interchange (2)

Fig.11 Image division

5.3 Self-Adaptive algorithm (shown in Fig.12)



Original image After pretreatment *S*="1" *S*="10110"

(by Hilbert ergodicity)

Fig.12 Self-Adaptive permutation algorithm

5.4 Testing data validity (shown in Fig.13)

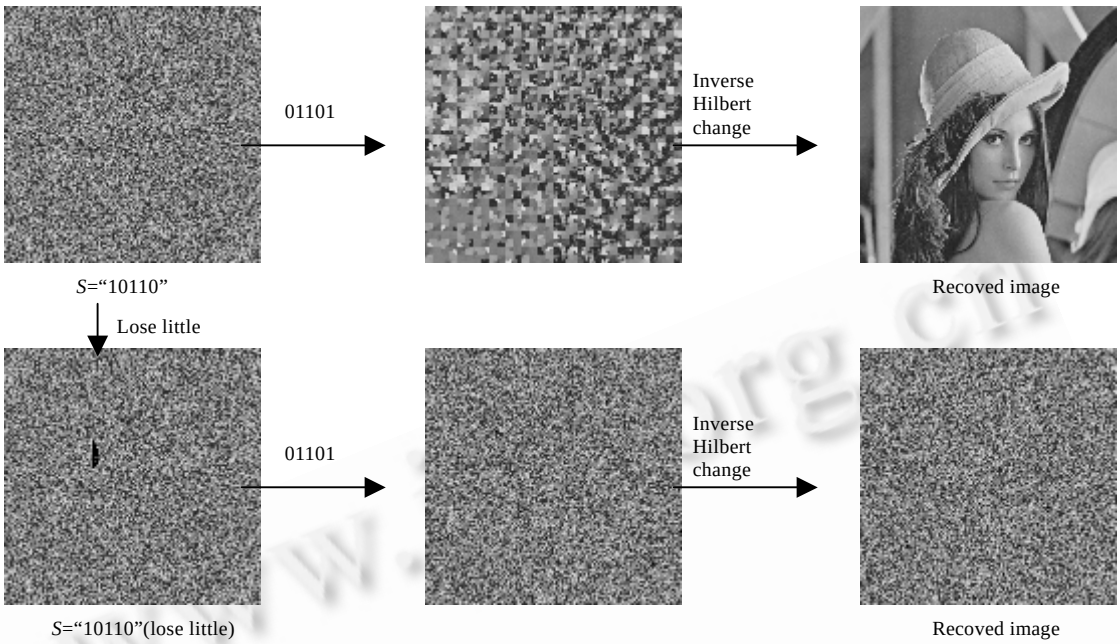


Fig.13 Testing data validity

Acknowledgement We thank Prof. Dong Guangchang and all attendants at the workshop on image processing and related mathematical problems 2004 in Hangzhou for discussing some issues about this paper.

References:

[1] Qiao LT, Nahrstedt L. Camparison of MPEG encryption algorithms. Computer & Graphics, 1998,22(4):437−448.

[2] Zhao XY, Chen G. Ergodic matrix in image encryption. SPIE, 2002,4875:4875−4878.

[3] Zhao XY, Chen G. Holographic Information Storage and Image Restoration. In: Proc. of the 8th Join Int'l Computer Conf. JICC2002. Ningbo, 2002. 199−203.

[4] Chen G. Region-of-Interest based flower images retrieval. In: Proc. of the IEEE ICASSP'03. 2003. 589−592.

[5] Matlas Y, Shamir A. A video scrambling technique based on space filling curves. In: Proc. of the CPYPTO'87. 1987,76(5):550−559.

[6] Bourbakis N, Alexopoulos C. Picture data encryption using SCAN patter. Pattern Recognition, 1992,25(6):567−581.

[7] Yen JC, Guo JI. A chaotic neural network for signal encryption/decryption and its VLSTI architecture. In: Proc. of the 10th VLSI Design/CAD Symp. Nantou, 1999. 319−322.

[8] Refregier P, Javidi B. Optical-Image encryption based on input plane and forier plane random encoding. Optics Letters, 1995,20(7): 767−769.

[9] Yang HG, Kim ES. Practical image encryption scheme by real-valued data. Optical Engineering, 1996,35(9):2473−2478.

[10] Kuo CJ, Chen MS. A new signal encryption technique and its attack study. In: Proc. of IEEE Int'l Conf. on Security Technology. Taipei, 1991. 149−153.

[11] Sridharan S, Dawson E, Goldburg B. Fast fourier transform based speech encryption system. Communications, Speech, and Vision, 1991,138(3):215−223.

[12] Ding W, Qi DX. Digital Image Transformation and information hiding and disguising technology. Chinese Journal of Computers, 1998,21(9):838−843 (in Chinese with English abstract).

附中文参考文献:

[12] 丁玮,齐东旭.数字图像变换及信息隐藏与伪装技术.计算机学报,1998,21(9):838−843.