Optik 125 (2014) 717–720

Contents lists available at ScienceDirect

Optik

journal homepage: www.elsevier.de/ijleo

Chaotic encryption and decryption of JPEG image

Dinghui Zhang*, Fengdeng Zhang

School of Optical-Electrical Information and Computer Engineering, Shanghai Key Lab of Modern Optical System, University of Shanghai for Science and Technology, Shanghai 200093, China

ARTICLE INFO

Article history:
Received 10 March 2013
Accepted 6 July 2013

Keywords:
JPEG image
Encryption and decryption
Chaotic sequence
Scramble

ABSTRACT

According to encrypting principles of digital images, integrating the characteristic of JPEG image, and using discrete chaotic sequence, this paper has studied encryption and decryption of JPEG image, and has compared and analyzed the corresponding relations between the encryption and decryption effects and their security of two different encrypting schemes of the JPEG image chaotic encryption studied by this paper. In a basic unit of an 8×8 data block, image encryption and decryption not only are fast, but also match with JPEG format. The JPEG image encryption can meet the security requirement of the storage and transmission of JPEG images in some common application occasions, and provides an effective and feasible way of encrypting JPEG images.

1. Introduction

The fundamental measure to ensure the security of electronic information is to encrypt it. Image encryption is an important research realm of information encryption. JPEG image is a common compression format of image files applied in the storage and the transmission of images, which greatly saves the storage space and the transmission band of images. Therefore, researches on the encryption and decryption of JPEG images have an important value of theoretic researches and practical applications. On the basis of studying and analyzing the structural feature of JPEG image, according to the basic encryption principles and methods of digital images, utilizing the stochastic characteristic of chaotic sequences, this paper has studied an effective and feasible method for encryption and decryption of JPEG image, and has analyzed the performances of the chaotic encryption algorithm.

2. Chaotic sequence

Owing to many natural features of chaos systems, such as non-periodicity, divergence, irrelevance, non-prediction, sensitivity of initial conditions, easy generation and duplication, and so on, they are natural cryptography systems, and are widely applied in modern privacy communications and information encryption [1–5]. Utilizing the random of chaotic sequences, and combining the structural feature of JPEG images, in a basic unit of an 8×8 data block, we scramble the corresponding coordinates of the all pixels of an original JPEG image to encrypt it, and inversely scramble the corresponding coordinates of the all pixels of an encrypted JPEG image to decrypt it. Logistic chaotic sequence is selected for image encryption and decryption, which is a one-dimensional chaotic sequence and is defined as follows:

$$x_{n+1} = \mu x_n(1 - x_n), \quad x_n \in (0, 1) \tag{1}$$

when $3.569945 < \mu < 4$, logistic sequences are chaotic [6,7].

3. JPEG image encryption

JPEG image is a compression image, which uses the YC_bC_r color system. In the light of the basic characteristic of JPEG image, according to the encryption principles and methods of digital images, drawing lessons from traditional cryptography theories and methods, making the best of many natural advantages of discrete chaotic sequences in privacy communications and information encryption, and synthetically considering some crucial factors of JPEG image encryption algorithm, such as security, implementing complexity, encrypting and decrypting effects, encrypting and decrypting rates, and so on [8,9], on the basis of iterative theoretical analyses and experiment contrast validation, this paper studies and proposes an effective and feasible chaotic encryption method of JPEG image. The main steps of the JPEG image encryption are as follows:

Step 1. Open a JPEG image file and decompress it, read every pixel value of the image, organize and denote all pixel values of the image by means of two-dimensional data matrix. If the image is gray, then it is denoted by a two-dimensional data matrix. If the image is color, then it is denoted by three two-dimensional data matrixes. Therefore, a color JPEG image is

* Corresponding author.
E-mail address: zdhui@126.com (D. Zhang).

0030-4026/$ – see front matter © 2013 Elsevier GmbH. All rights reserved.
http://dx.doi.org/10.1016/j.ijleo.2013.07.069

Fig. 1. The original image.

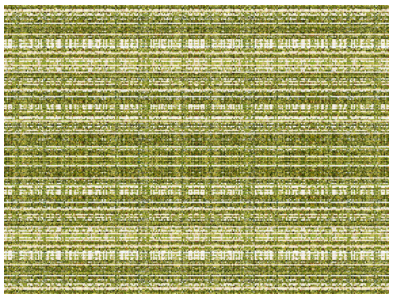

Fig. 2. The encrypted image encrypted by the first encryption scheme.

denoted by three components, every component is corresponding to a two-dimensional data matrix.

Step 2. Every 8×8 data block of every two-dimensional data matrix is scrambled in row and column positions by chaotic sequences. Scrambling the row and column positions of every 8×8 data block of the two-dimensional data matrix is to move the 8×8 data block to the row and column positions of some 8×8 data block of the two-dimensional data matrix, and that every numerical value of the moved 8×8 data block keeps unchanged. The 8×8 data block of the row and column positions occupied by some 8×8 data block is moved to the row and column positions of another 8×8 data block, all 8×8 data blocks of the two-dimensional data matrix are moved to their corresponding row and column positions of the two-dimensional data matrix, the original row and column positions occupied by an 8×8 data block and its new occupying positions through scrambling are one to one. The row and column positions of all the data of the two-dimensional data matrix are scrambled in a basic unit of an 8×8 data block, the row and column positions of every number in an 8×8 data block keep unchanged.

Step 3. A or three two-dimensional scrambled data matrixes are denoted by JPEG format, an encrypted JPEG image is gotten.

A 1704×2272 original color decompressed JPEG image is shown in Fig. 1. Because the JPEG image is color, so it is denoted by three two-dimensional data matrixes after it is decompressed. According to the chaotic encryption method of JPEG image proposed above, this paper utilizes two schemes to respectively encrypt the image shown in Fig. 1. The first scheme and the second scheme are just the same in step 1 and step 3, they are little different in step 2.

3.1. The first encryption scheme

Two one-dimensional chaotic sequences generated by arbitrarily selecting two sets of initialization are used to scramble row and column positions of all the data of a two-dimensional data matrix. The two one-dimensional chaotic sequences combine together, and scramble the row and column positions of all the 8×8 data blocks of three two-dimensional data matrixes of the color image. Because every two-dimensional data matrix of three two-dimensional data matrixes is scrambled by two chaotic sequences in the same way, the color of every pixel of the encrypted image is the same as the one of the every corresponding pixel of the original image.

Arbitrarily select two sets of initialization (μ_1, x_0^1) and (μ_2, x_0^2), suppose that μ_1 and μ_2 are respectively 3.768953657942978 and 3.657584686754865, x_0^1 and x_0^2 are respectively 0.596247685326853 and 0.386856274314657, respectively generate two one-dimensional chaotic sequences by (1), which respectively scramble the row and column positions of all the 8×8 data block of three two-dimensional data matrixes of the original image shown in Fig. 1, the scrambling operations of three two-dimensional data matrixes are just the same. The encrypted image is shown in Fig. 2.

3.2. The second encryption scheme

Arbitrarily select six sets of initialization and respectively generate six one-dimensional chaotic sequences by (1), every two sequences combine together, in this way, three groups of assembled sequences respectively scramble the row and column positions of all the 8×8 data blocks of three two-dimensional data matrixes of the original image. The row and column positions of all the 8×8 data blocks of very two-dimensional data matrix corresponding to every component of the color image is scrambled by a group of assembled sequences respectively, therefore, the color of every pixel of the encrypted image is reset, the encrypted image looks disorganized, the encrypting effect is better.

Arbitrarily select six sets of initialization (μ^1, x_0^1), (μ^2, x_0^2), (μ^3, x_0^3), (μ^4, x_0^4), (μ^5, x_0^5) and (μ^6, x_0^6), suppose that μ^1, μ^2, μ^3, μ^4, μ^5 and μ^6 are respectively 3.689746458848672, 3.824354686652895, 3.729813857245649, 3.764554986954858, 3.974953250943736 and 3.944654682814256; and that x_0^1, x_0^2, x_0^3, x_0^4, x_0^5 and x_0^6 are respectively 0.296426597523568, 0.636859576213549, 0.885331568527346, 0.626954954514253, 0.485324598342875 and 0.275850624858627; Respectively generate six corresponding chaotic sequences by (1). Suppose that the first sequence and the second sequence combine, the third sequence and the fourth sequence combine, the fifth sequence and the sixth sequence combine, respectively scramble the row and column positions of all the 8×8 data blocks of three two-dimensional data matrixes of the original image shown in Fig. 1. The encrypted image is shown in Fig. 5.

4. The decryption of the encrypted JPEG image

The decryption of the encrypted image is the inverse procedure of the encryption of the original image. The decryption process of a color encrypted JPEG image is as follows:

Step 1. Decompress the color encrypted JPEG image into three two-dimensional data matrixes.

Step 2. Implement inverse scrambling of the row and column positions of the three scrambled two-dimensional data matrixes in a basic unit of an 8×8 data block, namely every 8×8 data block is moved to the row and column positions before it is encrypted.

Step 3. Denote the three inversely scrambled two-dimensional data matrixes with JPEG file format, namely get the decrypted JPEG image.

The following first decryption scheme and the second decryption scheme are respectively corresponding to the inverse procedures of the above first encryption scheme and the second

Fig. 3. The right decrypted image decrypted by the first decryption scheme.

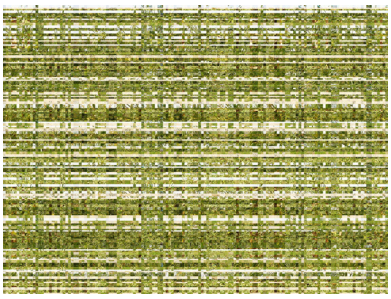

Fig. 4. The falsely decrypted image decrypted by the first decryption scheme.

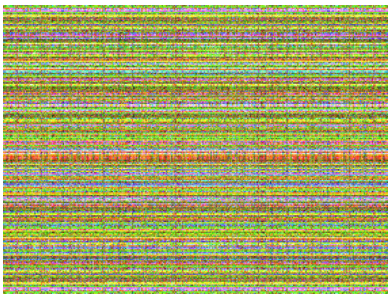

Fig. 5. The encrypted image encrypted by the second encryption scheme.

Fig. 6. The right decrypted image decrypted by the second decryption scheme.

encryption scheme. When the two decrypting scheme decrypt the encrypted image, they all implement the above three decryption procedures, only they are little different in the decryption step 2.

4.1. The first decryption scheme

The first decryption scheme is the inverse procedure of the first encryption scheme, arbitrarily choose two sets of initialization and respectively generate two corresponding chaotic sequences, two sequences combine together, and inversely scramble the row and column positions of all the 8×8 data blocks of the three two-dimensional data matrixes of the encrypted image shown in Fig. 2 respectively.

Select just the same two sets of initialization as the image encryption, and generate two one-dimensional chaotic sequences, and decrypt the encrypted image shown in Fig. 2, the right decrypted image is shown in Fig. 3. For simplicity, select two sets of initialization slightly different from the ones of the image encryption, and validate the sensitivity of the chaotic sequence to its initialization, letting that the values of μ^1 and μ^2 are just the same as the image encryption, but that the values of x_0^1 and x_0^2 are 0.000000000000001 larger than those of the image encryption, namely 10^{-15}, and generate two corresponding chaotic sequences, the scrambling operation of the image decryption is just the same as the one of the right image decryption, and decrypt the encrypted image shown in Fig. 2. Though the initialization of the two chaotic sequences for the image decryption is slightly different from the one for the image encryption, the encrypted image shown in Fig. 2 cannot be right decrypted; the falsely decrypted image is shown in Fig. 4.

4.2. The second decryption scheme

The second decryption scheme is the inverse procedure of the second encryption scheme, arbitrarily choose six sets of initialization and respectively generate six corresponding chaotic sequences, two sequences combine together, and inversely scramble the row and column positions of all the 8×8 data blocks of the three two-dimensional data matrixes of the encrypted image shown in Fig. 5 respectively.

Six sets of initialization selected by image decryption are just the same as those selected by image encryption, and generate six one-dimensional chaotic sequences, besides, scrambling operation for image decryption is just the same as the one for image encryption, when the image shown in Fig. 5 is decrypted, the corresponding right decrypted image is shown in Fig. 6. Six sets of initialization selected by image decryption are not slightly the same as those selected by image encryption, for simplicity, letting that μ^1, μ^2, μ^3, μ^4, μ^5 and μ^6 for image decryption are just the same as those for image encryption, and that x_0^1, x_0^2, x_0^3, x_0^4, x_0^5 and x_0^6 for image decryption are all 0.000000000000001 larger than those for image encryption, namely 10^{-15}, and generate six corresponding chaotic sequences, besides, the scrambling operations for decryption are just the same as those for the right image decryption, when the encrypted image shown in Fig. 5 is decrypted, owing to the sensitivity to chaotic sequences to their initialization, the encrypted image cannot be right decrypted, the corresponding falsely decrypted image is shown in Fig. 7.

5. The performance comparison and analyses of the encryption schemes

The following section respectively compares and analyzes the performances of the first encryption scheme and the

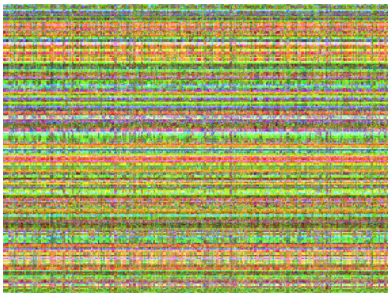

Fig. 7. The falsely decrypted image decrypted by the second decryption scheme.

second encryption scheme from three aspects of encrypting effect, decrypting effect and security.

5.1. Comparison and analysis of the encrypting effect

The first encryption scheme uniformly scrambles the three components of the color image, therefore, comparing with the original image, the color of every pixel of the encrypted image keeps unchanged, the encrypting effect of the first encryption scheme is not very ideal, Fig. 2 illustrates this. The second encryption scheme does not uniformly scramble the three components of the color image, therefore, comparing with the original image, the color of every pixel of the encrypted image keeps changed, the encrypting effect of the second encryption scheme is ideal, and is better than the one of the first encryption scheme, Fig. 5 illustrates this.

5.2. Comparison and analysis of the decrypting effect

When the first decryption scheme decrypts the encrypted image encrypted by the first encryption scheme, the grid effect in the decrypted image is not seen basically, Fig. 3 illustrates this. This is because that the relevance among 8×8 data blocks is not badly destroyed, comparing with the original image, the first encrypting scheme uniformly scrambles the three components of the color image, and makes the color of every pixel of the encrypted image keep unchanged. When the second decryption scheme decrypts the encrypted image encrypted by the second encryption scheme, the grid effect in the decrypted image is obvious, Fig. 6 illustrates this. The second encryption scheme does not uniformly scramble the three components of the color image, comparing with the original image, and makes the color of every pixel of the encrypted image keep changed, and destroys the relevance among 8×8 data blocks.

5.3. The encryption security comparison and analysis

Comparing with the original image, the color of every pixel of the encrypted image encrypted by the first encryption scheme keeps unchanged. If the encrypted image is magnified, because the encrypted image is composed of lots and lots of 8×8 data block, some bits and pieces of the image scenery are faintly visible, therefore, the security of the encrypted image is lower. When the second encryption scheme encrypts the original image, comparing with the original image, the color of every pixel of the encrypted image changes, therefore, even though the encrypted image is magnified, any the visual feature of the image scenery is not visible, not only the encrypting effect is better, but also the security of the encrypted image is higher. Suppose that the encryption algorithm is known, if an enumerative decryption is applied, there are about $284! \times 213!$ possibilities that the encrypted image encrypted by the first encryption scheme is decrypted, and that there are $(284! \times 213!)^3$ possibilities that the encrypted image encrypted by the second encryption scheme is decrypted. If the chaotic sequence decryption is applied, and suppose that the initializations of the chaotic sequence, namely x_0 and μ all accurately obtain the 15th decimal place, there are about $10^{14} \times 10^{15} = 10^{29}$ possibilities that the encrypted image encrypted by the first encryption scheme is decrypted, and that there are $(10^{14} \times 10^{15})^3 = 10^{87}$ that the encrypted image encrypted by the second encryption scheme is decrypted. Therefore, even though the encryption algorithm studied by this paper is known, whether which of the above two decryption schemes is applied, in limited time, it is very difficult that a big encrypted color JPEG image encrypted by the first encryption scheme or the second encryption scheme is right decrypted.

6. Conclusions

The JPEG image encryption studied by this paper considers the feature of the JPEG image compression, and scrambles the image in a basic unit of an 8×8 data block, not only greatly decreases the operations of the image encryption and decryption, but also makes the size of the encrypted image file or the decrypted image file keep basically accordant with the one of the original image file. The encryption algorithm is comparatively fit for encrypting bigger JPEG image files, and is not comparatively fit for encrypting smaller JPEG image files. This is because that it cannot ensure enough security of smaller encrypted JPEG images. The two encryption and decryption procedures and performances corresponding to the two encryption schemes and the two decryption schemes of the encryption algorithm are slightly different. When the security of the encrypted image is desired to be lower, the encryption and decryption operations of the image are desired to be faster, the quality of the decrypted image is desired to be higher, the first encryption scheme should be chosen. When the security of the encrypted image is desired to be higher, the encryption and decryption operations of the image are desired to be slower, the quality of the decrypted image is desired to be lower, the second encryption scheme should be chosen. Therefore, according to actual cases, the corresponding encryption and decryption of images should be studied and chosen to meet practical requirements.

References

[1] N.K. Pareek, V. Patidara, K.K. Sud, Discrete chaotic cryptography using external key, Phys. Lett. A 309 (2003) 75–82.
[2] C. Li, Z. Han, The new evolution of image encryption techniques, Inform. Control 32 (4) (2003) 339–343, 351.
[3] S. Mazloom, A.M. Eftekhari-Moghadam, Color image encryption based on coupled nonlinear chaotic map, Chaos Soliton. Fract. 42 (2009) 1745–1754.
[4] C. Wang, F. Wang, Z. Hu, Digital image encryption via a truncated baker transformation, Comput. Eng. 30 (18) (2004) 103–104, 129.
[5] L. Tian, Security communication of true-color digital image based on chaotic maps, Comput. Appl. Softw. 24 (5) (2007) 170–171, 191.
[6] L. Zhao, X. Zhang, J. Fan, A digital image encryption algorithm based on chaotic sequences, Microelect. Comput. 24 (2) (2007) 73–74, 78.
[7] J. Liu, Z. Wang, Q. Wang, Solution of secure information encryption based on chaotic mirror-like image encryption algorithm, Inform. Secur. Commun. Privacy 3 (2007) 89–91.
[8] Y. Fan, X. Sun, New algorithm to measure scrambling degree of scrambling images, Comput. Eng. Appl. 43 (29) (2007), 93–94, 97.
[9] Q. Li, K. Zhao, Z. Deng, et al., Research on deciphering method of a kind of chaotic encryption picture, J. Natl. Univ. Def. Technol. 29 (3) (2007) 45–49.