Int. J. Electron. Commun. (AEÜ) 70 (2016) 1–7

Contents lists available at ScienceDirect

International Journal of Electronics and Communications (AEÜ)

journal homepage: www.elsevier.com/locate/aeue

Encryption method based on a new secret key algorithm for color images

Shihua Zhou[a,*], Ziqi Wei[b], Bin Wang[a], Xuedong Zheng[a], Changjun Zhou[a], Qiang Zhang[a]

[a] *Key Laboratory of Advanced Design and Intelligent Computing, Dalian University, Ministry of Education, Dalian 116622, China*
[b] *Computing Science Department, University of Alberta, Edmonton, Alberta T6E 1P6, Canada*

ARTICLE INFO

Article history:
Received 31 March 2014
Accepted 26 August 2015

2010 MSC:
00-01
99-00

Keywords:
Color image
Discrete cosine transform
Encryption
Secret key
YUV space

ABSTRACT

In order to improve the security of color image encryption, the secret key of the encryption algorithm must have a strong correlation with the original image, but it should not reveal its information. It is difficult to meet this requirement using the current secret key generation algorithm. Thus, we propose a new secret key generation algorithm based on operations on the DC and AC values in YUV space. These two values are extracted from the process discrete cosine transformation of the data after image color space transformation. By combining the new secret key and the given secret key together as the initial values of chaotic maps, we can encrypt a color image in YUV and RGB space through multi-chaotic maps. Our experimental results indicate that this secret key algorithm is highly effective and the encryption method has a relatively high security.

1. Introduction

Unknown persons or hackers can easily intercept important image information during transmission via the Internet. Therefore, the security of images is becoming increasingly important and researchers are investigating this field extensively. Image encryption [1,2] is generally used to protect important information from all types of threats. First, the sender selects a secret key and uses a specific function to encrypt the original image based on an encryption algorithm and only the authorized receiver can decrypt this information with the secret key.

In general, encryption techniques [3–7] include mathematical transform, compression methodology, modern cryptography, matrices mixing, chaos, and DNA techniques. In particular, the chaos-based image encryption algorithms [8,9] are the most important methods because the chaotic sequences have characteristics such as ergodicity, nonperiodicity, and randomicity. The principle of image encryption based on chaos requires operations on both the original information and chaotic sequence, where the original information becomes similar to random noise. The chaotic sequence depends on the chaos map and an initial value, where the initial value is used as the secret key. For an encryption algorithm, the secret key is the most important information and it is transmitted over a secure channel. Therefore, we can improve the security of the encryption algorithm by designing the chaotic initial image related to the original image.

In this study, we propose a new secret key generation algorithm based on operations on the DC and AC values in YUV space. These two values are extracted via discrete cosine transformation (DCT) of the data after image color space transformation. By combining the new secret key and the given secret key together as the initial value for chaotic maps, we can encrypt the color image in YUV and RGB spaces through multi-chaotic maps.

2. Secret key algorithm

2.1. Secret key information

During image encryption, several numbers are used as the secret keys, where the sensitive relationships between the secret keys and the image itself are very important. Cryptography research has confirmed that all encryption methods can be cracked, except for one-time pad. This is also the case for image encryption system based on chaos. The characteristics of chaotic systems make them sensitive to the chaotic initial value, and thus a chaotic system changes greatly when the initial value undergoes a very small change. This can improve the security of an encryption algorithm. If a highly sensitive value can be found relative to the original image

[*] Corresponding author. Tel.: +86 041187402106; fax: +86 04117402106.
E-mail address: shihuajo@gmail.com (S. Zhou).

http://dx.doi.org/10.1016/j.aeue.2015.08.010
1434-8411/© 2015 Elsevier GmbH. All rights reserved.

as the secret key (i.e., the chaotic initial value used in the chaotic encryption system), this can have a useful auxiliary effect in image encryption, thereby resisting differential attack as well. The image key has the following main requirements.

(1) The value cannot provide much information about the original image or secure hidden information problems may occur after leakage. If the value contains too much information about the original image, the attacker can use this information to analyze the information in the original image. In particular, when the value contains important information about the original image, the attacker can break the encrypted image completely by analyzing this value.

(2) If the value is excessively large, it is not conducive to transmission via a secure channel. The encrypted image is transmitted via a non-secure channel, whereas the value is transmitted through a secure channel. Ensuring the safety of the channel may require more space, time, or money. Therefore, if the value is excessively large, it is difficult to guarantee secure transmission.

(3) The value needs to have a strong correlation with the original image. Even if one pixel value in the original image is modified, the value may change greatly. Differential attack is one of the most important methods used for encrypted image attack. The basic idea of a differential attack is that the largest possible key is obtained based on the difference between a pair of plaintexts and the corresponding ciphertexts. During differential attack on image encryption, the original image is changed slightly by the attacker, and the original image and the changed image are encrypted according to the image encryption method. The correlation between the original image and the encrypted image can be found by comparing the two encrypted images. Therefore, the value must be strongly correlated with the original image in order to ensure that if the original image changes to only a subtle extent, the value can change sufficiently. This is the only way that the encrypted image can resist a differential attack.

2.2. YUV space and DCT transform

A color space [10] is used to describe a type of sampling model where a set of values is used to express colors. The most widely used color space models in image processing include the RGB, CMYK, and YUV models. Different color spaces can be transformed into others using various methods. The YUV model employs general terms and it contains space types such as Y′UV, YUV, YCbCr, and YPbPr. The common terms of "Y," "U," and "V" represent brightness, chromaticity, and concentration, respectively. The following functions describe how to convert a pixel with r, g, and b values into a pixel in the YUV space, where the r, g, and b values are in the R, G, and B spectral components, respectively:

$$\begin{aligned} y &= Y(r, g, b), \\ u &= U(r, g, b), \\ v &= V(r, g, b). \end{aligned} \tag{1}$$

The transformation is given by the following equation.

$$\begin{bmatrix} y \\ u \\ v \end{bmatrix} = \begin{bmatrix} 0.299 & 0.587 & 0.114 \\ -0.173 & -0.339 & 0.511 \\ 0.511 & -0.428 & -0.083 \end{bmatrix} \begin{bmatrix} r \\ g \\ b \end{bmatrix} \tag{2}$$

The DCT [11] is one of the most popular transforms used in multimedia compression, which is an orthogonal transform and its inverse can be calculated easily without complex computation. For a two-dimensional image, an $N \times N$ block of pixels can be operated upon by the DCT.

2.3. New secret key algorithm

Most key generation methods for image encryption require that all of the pixels in the original image are treated as a set. After digitizing the original image, all of the pixel information is extracted. In the usual methods, the data from the original image are obtained by simple sum or difference operations. Mathematically, these methods only comprise a small number of operations, so the layer of the original image information is shallow. In addition, these methods are applied directly to the pixels in the original image and only addition or subtraction operations are performed, so the encryption effect of these four simple operations is not very good. In this study, we propose a new type of algorithm for the initial value of chaos, which is inspired by JPEG compression. We assume that the original image has a size of 128 × 128 is BMP format and the steps required to generate the initial value are as follows.

Step 1: Extract the pixels from the original image and save them in the RGB format.
Step 2: The data are converted from the RGB space into the YUV space via a transformation formula between the two color spaces.
Step 3: The value ranges of three-dimensional data are different, where the data in Y space range to minus 128 and they are controlled in the range of [−128, 127].
Step 4: The weight of YUV in three dimensions is divided into square matrices that all measure 8 × 8, which are then operated upon by the DCT transform and 256 × 3 square matrices are generated.
Step 5: One sequence is obtained by extracting the first values from the existing 256 × 3 square matrices and this sequence is then treated as the DC values.
Step 6: A sequence is obtained by arranging the sums of the other values for the existing 256 × 3 square matrices and this sequence is treated as the AC values.
Step 7: To add the DC values and AC values, the sums are taken of the absolute values and the modulus, and the resulting value is generated by operating on the two numbers defined above.

The size of the key space is changed by choosing a different modulus. The resulting value is merged with a given value and the initial value of chaotic encryption is generated, which is regarded as the new secret key. The process employed to generate a key is introduced using a specific example. Fig. 2(a) shows a BMP image that measures 128 × 128. The weight in three dimensions for YUV is divided into 256 × 3 square matrices, which all measure 8 × 8. The first values are extracted from these square matrices and the DC values are obtained: DC = {371.4902, 295.8078, 327.2783, 345.2063, 404.4576, 435.5268, 484.5976, 476.6267, 501.9408, 510.3143, . . ., 461.8460, 488.7821, 507.0992, 496.0219, 479.5565, 495.7012, 430.1677, 448.4427, 455.9841, 465.0886}. Next, the sums of the other values in the existing 256 × 3 square matrices are arranged in a sequence and the AC values are obtained: AC = {376.0118, 355.9169, 316.0552, 295.8998, 305.3467, 309.0863, 299.0510, − 83.0663, − 20.4295, − 11.2338, . . ., −0.5192, 0.0220, − 0.4140, 0.4136, 0.2551, − 0.0000, − 0.3609, 0.3541, 0.1682, − 0.5791}. To add the DC values and AC values, the sums are taken of the absolute values, where $Sum_{DC} = 2.957117772921423e^5$, $Sum_{AC} = 1.818397883992129e^6$. These two numbers are operated upon by modulus and addition and the resulting value is generated: $x' = 0.21141096612842713$.

2.4. Theoretical illustration

Two main transform methods, i.e., the color space transform and DCT, are applied to calculate the chaotic initial value. A demonstration of differential attack resistance is provided based