International Journal of Advanced Science and Technology
Vol.95 (2016), pp.37-44
http://dx.doi.org/10.14257/ijast.2016.95.04

An Improved Hybrid Encryption Algorithm for RGB Images

Suolan Liu*[1,2], Chen Yue[1] and Hongyuan Wang[1]

[1]*School of Information Science & Engineering, Changzhou University, Jiangsu, China*
[2]*Department of Electrical Engineering, University of Texas at Dallas, TX, USA*
lan-liu@163.com

Abstract

This paper presents a computationally efficient encryption scheme for RGB images. Firstly, the original plain-image is decomposed to three component images of R, G and B. Secondly, an improved gravitation model is used for value transformation by setting different encryption keys on each component. Thirdly, the improved Arnold transform is applied for position permutation. Finally, we obtain the encrypted image by composing the three component cipher-images. Experimental results show that encrypted image achieved by our algorithm can effectively resist security attacks.

Keywords: *image encryption, gravity, ART, security*

1. Introduction

Nowadays many kinds of information need to be transferred by Internet, such as text, image, audio, video and other multimedia information. How to prevent information copying, stealing and destroying attacks is a challenging task [1-3]. Cryptography is the technique used for secure transmission of data over a communication line. This technique is using encryption to make the information to be transmitted into an unreadable form so that every unauthorized person can not correctly recover the information [4]. The traditional encryption algorithms mainly include symmetric cryptographic algorithm and asymmetric cryptographic algorithm. DES, TDEA, RC5 and IDEA all belong to symmetric cryptographic algorithm, while RSA, ELGAMAL, RABIN, D-H, and ECC are asymmetric cryptographic algorithms. In some cases, image applications require to satisfy their own needs like fast and real-time communication and processing, therefore these traditional encryption algorithms may not be the most desirable algorithms for image encryption because of large data sizes [5-8]. By analyzing recent research results in image encryption, they can be classified into three different categories [1-19], including position permutation, value transformation and visual transformation. The security of image encryption has been extensively researched these years, because encryption is a very important security mechanism. It works by scrambling the information into unreadable information and then unscramble it for reading. Most of these existing schemes use hybrid strategy to scramble image. The reason of the phenomenon is that using a single encryption algorithm usually is unable to overcome its shortcomings, while using another encryption algorithm simultaneously can solve this problem effectively. For example, if we only use Arnold transform (ART) [20] to scramble an image, it may be found that there are same histograms between cipher-image and plain-image, no matter how many times of iterative operation have been done. Therefore, another kind of encryption algorithm should be used at the same time.

In this paper, we present a hybrid encryption scheme simultaneously using both position permutation and value transformation to scramble image. For position permutation, we select ART, and gravity-scrambling model is used for value

ISSN: 2005-4238 IJAST

transformation. The Arnold transformation is used to scramble the digital images and has many applications, especially in digital watermarking [20]. The traditional Arnold transformation is a periodic and invertible mapping. Besides, it is valid for square images only. They are its advantages, but also may be shortcomings from these aspects, such as security and applicability. So, we firstly do some improvement on traditional Arnold transformation to enhance the security and extend its application from square images to rectangle images. In 1687 [21], the Law of universal gravitation was first proposed by Newton in Philosophiae Naturalis Principia Mathematica, which stated that any two particles were attracted to each other in nature. Based on this principle, Sun and Chen [22] used it on scrambling image. To obtain satisfied performance, the parameter of gravity coefficient should be large enough [23]. This need computer have enough storage capacity correspondingly. So, we improved the gravity model to enhance its operability as well as encryption effect.

The remaining of this paper is organized as follows. Section 2 describes the proposed scheme. The overview of the scheme is presented and improved ART and Gravitation model are also given. Section 3 reports experimental results. Section 4 discusses the security of our proposed scheme. Section 5 concludes the paper.

2. Proposed Hybrid Scheme

2.1. Improvement on Arnold Transform and Gravity Model

Based on the work in [12, 20, 24], we can improve ART from two aspects. One is decryption, another is to extent its application from square images to rectangle images. According to the above analyzing, to achieve decryption image we must do n_d times operation, $n_d = T - n_e$. That means the more numbers of encryption iterations, the less numbers of decryption iterations is needed, and vice versa. It does not satisfy the real-time demand of image encryption and decryption. Usually, the more numbers of encryption iterations the more numbers of decryption iterations is needed. To solve the problem, we can use inverse transformation based on ART.

$$\begin{aligned} ART(I'(x,y),N) &= \{(v,(x',y')) \mid (x',y')^T \\ &= \begin{pmatrix} 2 & -1 \\ -1 & 1 \end{pmatrix} (x,y)^T (\text{mod } N)\} \end{aligned} \tag{1}$$

By this transformation, there are same numbers of iterations between encryption and decryption, $n_d = n_e$.

Figure 1 shows encrypted and decrypted results of an image. Figure 1(a) is the plain-image. Fig.1(b) and fig.1(c) are cipher-image and decipher-image by using the traditional Arnold method. Sum of encryption and decryption iterations is 384 according to Table 1. Figure 1(d) and Figure 1(e) are cipher-image and decipher-image by using improved Arnold method, in which the iterations of decryption is same as encryption.

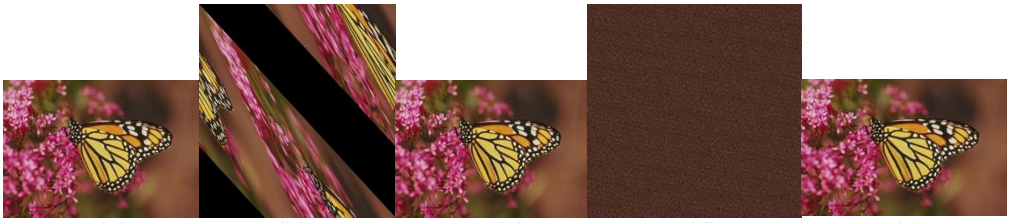
According to the description of ART theory, it can only be used when the image is square. But in many cases, images are non-square. Therefore, it needs be improved to fit any size of width and length of an image. Based on the work of KONG and ZHANG [24], ART could be extended to image sized $M \times N$.

$$\begin{cases} x + y = Mp_1 + x' \\ x + 2y = Np_2 + y' \end{cases} \tag{2}$$

$M, N, p_1, p_2 \in Z, Z$ is an integer.

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

Figure 1. Arnold Transformation by using Different Times of n_e and n_d. (a) Plain-Image Lenna(512*512); (b) cipher-image n_e=100; (c)decipher-image (b), n_d=284; (d) cipher-image n_e=50; (e)decipher-image of (d), n_d=50



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

Figure 2. Improved Arnold Transformation to Non-Square Image. (a) Plain-Image Monarch（768×512）; (b) Cipher-Image n_e=1; (c) Decipher-Image of (b) n_d=1; (d) Cipher-Image n_e=20 (e) Decipher-Image of (d) n_d=20

To an image, if the size of length is greater than width, we need to expand it into a square image according to the length. If the size of length is less than width, we need to expand it into a square image according to the width.

In Figure 2, we expand the plain-image from rectangle into square at the first step, then do position permutation based on ART. Figure 2(b) and Figure 2(c) are encrypted and decrypted results with the same scrambling iteration of 1. Figure 2(d) and Figure 2(e) are encrypted and decrypted results with the same scrambling iterations of 20. One may find that encrypted result in Figure 2(d) is obviously better than that in Figure 2(b).

Gravitation theory was firstly used to encrypt images by Sun and Chen [22]. To obtain good scrambling results, large gravitational coefficient is needed, which leads to a large amount of calculation. To improve it, Wang [23] used it with chaotic system. Experiments show good result when gravitational coefficient is set as 10^3. The effectiveness of his work is proved only on gray value images instead of color images.

To an image, encryption of pixels value transformation based on gravitational model can be defined as follows.

$$Val'_{(p,q)} = [k\frac{m_{(x,y,z)}m_{(p,q)}}{(x-p)^2+(y-q)^2+z^2}]\bmod 256 \oplus Val_{(p,q)} \quad (3)$$

k is the gravity coefficient. $m_{(x,y,z)}$ is the quality of the particle. To simplify the computation complexity, in our case, we set it as a unit particle $m_{(x,y,z)}=1$. (x,y,z) is its location, where z≠0, so no matter what value of x,y, the distance (denominator) $r^2=(x-i)^2+(y-j)^2+z^2>0$ can be guaranteed. $m_{(p,q)}$ is pixel quality located on (p,q) and $Val_{(p,q)}$ is gray value. $Val'_{(p,q)}$ is pixel's transformed gray value. [] is integer calculations. mod presents modulus computing and $\oplus$ is exclusive or operation.

We set private keys $m_{(p,q)}=55\acute{}\ p^2+q^3+128$, $k=12.1\acute{}\ 10^8$, $x=655$, $y=487$, $z=901$ for R, G and B channel images. In cipher-image, some colorful pixels are shown,

which may be the contours of objects. This means even we set a large gravity coefficient, certain information of plain-image also may be leaked out if only gravitation theory is used to scramble image.

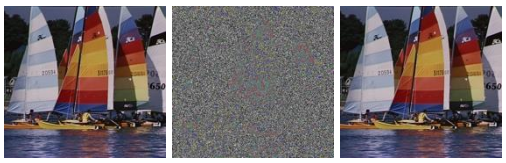


Figure 3. Cipher-image and Decipher-Image based on Gravitation Theory, from Left to Right are Plain-Image, Cipher-Image and Decipher-Image

2.2. Description of the Proposed Scheme

We propose to a hybrid encryption scheme. The input is any natural RGB image sized $M \times N$, output is its cipher-image. The procedure of encryption of an image is delineated in Figure 4.

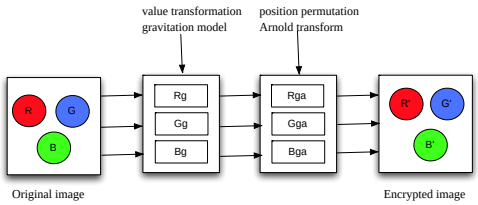


Figure 4. Flowchart of RGB Image Encryption

The steps can be explained as following. In the first stage, we decompose the original RGB image into three component images of R, G and B. Then, to each component image, gravitation model is used to do value transformation. Parameters of encryption keys are $m_{(p,q)} = a \times p^2 + bq^3 + c$, k, x, y and z. By this step, a partially encoded image is produced. Henceforth, Arnold transform is used to do position permutation. We have to compare the width and length of this image in order to discriminant whether extending operation to a square image is need or not. At last, compose these three completely encoded images, and a cipher-image is obtained. Decryption processing is the inverse operation of encryption.

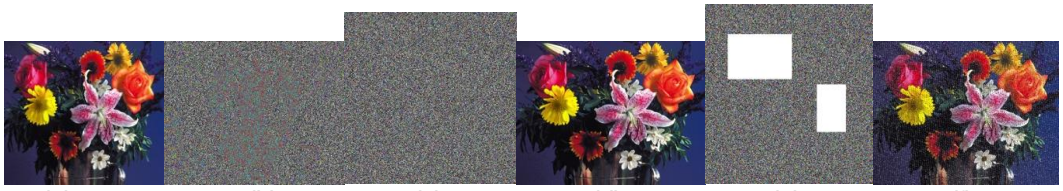
3. Experimental Results

The procedure is applied on JPEG RGB images. In Figure 5, the plain-image size is 656×476. Figure 5 (b) shows partially encrypted image based on gravitation model. Private keys in this step are setting as following: for red, $m_{R(p,q)} = 73 \times p^2 + q^3 + 278$, $k_R = 11.8 \times 10^{15}$, $x_R = 130$, $y_R = 99$ and $z_R = 372$. For green, $m_{G(p,q)} = 263 \times p^2 + q^3 + 117$, $k_G = 24.7 \times 10^{11}$, $x_G = 285$, $y_G = 243$ and $z_G = 57$. For blue, $m_{B(p,q)} = 112 \times p^2 + q^3 + 213$, $k_B = 19 \times 10^{12}$, $x_B = 302$, $y_B = 111$ and $z_B = 314$. Figure 5(c) is completely encrypted image, for red $n_{\mathrm{Re}} = 94$, for blue $n_{Ge} = 54$, for green $n_{Be} = 105$. Figure 5 (d) represents correctly decrypted RGB image with exact keys and numbers of decryption iterations are same to encryption iterations.

In Figure 6, the plain-image size is 824×656. Fig.6 (b) shows partially encrypted image based on gravitation model. Private keys in this step are: for red, $m_{R(p,q)} = 147 \times p^2 + q^3 + 95$, $k_R = 13 \times 10^8$, $x_R = 173$, $y_R = 114$ and $z_R = 370$. For green, $m_{G(p,q)} = 65 \times p^2 + q^3 + 128$, $k_G = 21 \times 10^{12}$, $x_G = 250$, $y_G = 216$ and $z_G = 97$. For blue,

$m_{B(p,q)}=129\times p^2+q^3+79$, $k_B=17\times 10^{14}$, $x_B=364$, $y_B=283$ and $z_B=141$. Figure 6 (c) is completely encrypted image, for red $n_{\mathrm{Re}}=136$, for blue $n_{Ge}=93$, for green $n_{Be}=55$. Figure 6 (d) represents correctly decrypted RGB image with exact keys and numbers of decryption iterations are same to encryption iterations.

As can be seen from Figure 5 (b) and Figure 6(b), certain numbers of contour pixels are shown in partially encrypted image based on gravitation model. However, excellent performance show in completely encrypted images, such as Figure 5(c) and Figure 6(c). The keys used in experiments are selected randomly under proper difference.



(a) (b) (c) (d) (e) (f)

Figure 5. Test Results 1

(a) (b) (c) (d) (e) (f)

Figure 6. Test Results 2

4. Security Analysis

Security is the one of most important issues in cryptology. A good image encryption scheme should have these performances, such as enough large key space, key sensibility, anti-cropping, as well as resisting various attacks.

4.1. Analysis against Cropping Attacks

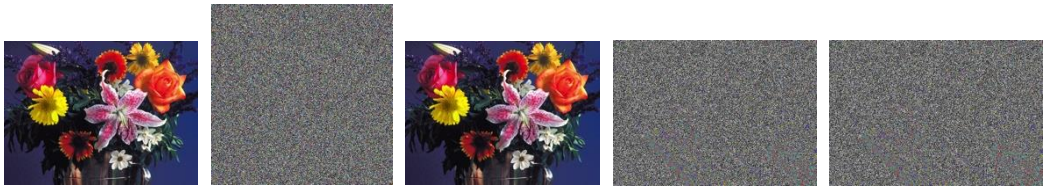
Figure 5 (e) shows two blocks cropped in the cipher-image of Figure5 (c). The first block size is 205×156, locates from (79, 62) to (284, 218). The second block size is 138×119, locates from (517, 335) to (655,454). Figure 5 (f) shows decrypted image got from the corresponding Figure 5 (e), with all correct keys. Figure 6 (e) shows two blocks cropped in the cipher-image of Figure 6 (c). Figure 6 (f) shows decrypted image got from the corresponding Figure 6 (e), with all correct keys. From these results we can see that quantities of decrypted images Figure 5 (f) and Figure 6 (f) are lower than Figure 5 (d) and Figure 6 (d), respectively. The reason of the phenomenon is ascribed to cropped blocks. Blocks destroy the integrity of image information. But the main information of the plain-images can be recognized visually. So, we may draw a conclusion that the proposed image encryption scheme has effective ability against cropping attacks.

4.2. Key Sensibility

In this proposed scheme, encryption and decryption are highly sensitive on the key space. High keys sensitivity is needed for secure image cryptosystems. Figure 7(a) is a plain-image. Figure 7(b) is cipher-image by our approach. Figure 7(c) represents decrypted image with correct keys. In Figure 7(d), we show decrypted image with parameters changes in inverse gravitation transform. For red, $m_{R(p,q)}=68\times p^2+q^3+270$,

$k_R = 11.8' 10^{13}$, $x_R = 122$, $y_R = 105$ and $z_R = 283$. For green, $m_{G(p,q)} = 266' p^2 + q^3 + 105$, $k_G = 19' 10^{12}$, $x_G = 294$, $y_G = 203$ and $z_G = 88$. For blue, $m_{B(p,q)} = 107' p^2 + q^3 + 334$, $k_B = 14.7' 10^{14}$, $x_B = 282$, $y_B = 151$ and $z_B = 306$. Numbers of decryption iterations are same to encryption iterations in all component images in the process of inverse Arnold transform. In Figure 7(e), we show decrypted image with parameters changes in inverse Arnold transform. For red $n_{Rd} = 72$, for blue $n_{Gd} = 103$, for green $n_{Be} = 94$. Set same keys to encryption operation in all component images in the process of inverse gravitation transform.

Figure 8(a) is plain-image of pens. Figure 8(b) is cipher-image by our approach. For all component images, keys are set as $m_{(p,q)} = 185' p^2 + q^3 + 266$, $k = 29.88' 10^{19}$, $x = 285$, $y = 474$ and $z = 312$. $n_e = 35$. Figure 8(c) represents correctly decrypted image with correct keys. In Figure 8(d), we show decrypted image with parameters changes in inverse gravitation transform $m_{(p,q)} = 185' p^2 + q^3 + 265$, but no changes to other parameters. In Figure 8(e), we show decrypted image with parameters changes in inverse Arnold transform $n_e = 34$, but no changes to other parameters. Subsequently, comparison results show incorrectly decrypted image with mere change in keys, even though they are nearly close to the original keys.



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

Figure 7. Test Results of Key Sensibility on 'flowers'

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

Figure 8. Test Results of Key Sensibility on 'pens'

5. Conclusions

In this paper we proposed an efficient RGB image encryption scheme by using improved gravitation model and Arnold transform. Three component images are encrypted respectively by setting different encryption keys and iterations for pixel value and pixel position transformation. Comparison tests have been carried out with detailed and numerical analysis, which demonstrates our scheme's high key sensibility and security.

References

[1] R. Zunino, "Fractal circuit layout for spatial decorrelation of images", Electronics Letters, vol. 34, **(1998)**, pp. 1929-1930.
[2] A. R. Butz, "Alternative algorithm for hilbert's space-filling curve", Computers, vol. 20, no. 4, **(1971)**, pp. 424-426.
[3] G. Zhang and Q. Liu, "A novel image encryption method based on tatal shuffling scheme", Optics Communications, vol. 284, **(2011)**, pp. 2775-2780.

[4] Z. Eslami and A. Bakhshandeh, "An improvement over an image encryption method based on total shuffling", Optics Communications, vol. 286, **(2013)**, pp. 51-55.
[5] Z.-L. Zhu, W. Zhang, K.-W. Wong and H. Yu, "A chaos-based symmetric image encryption scheme using a bit-level permutation", Information Sciences, vol. 181, no. 6, **(2011)**, pp. 1171-1186.
[6] V. I. Arnold and A. Avez, "Ergodic Problems in Classical Mechanics", New York: Benjamin, **(1968)**.
[7] L. Abraham and N. Daniel, "Secure Image Encryption Algorithms: A Review", International journal of scientific & technology research, vol. 2, **(2013)**, pp. 186-189.
[8] Y. Wu, J. P. Noonan and S. Agaian, "NPCR and UACI Randomness Tests for Image Encryption", Journal of Selected Areas in Telecommunications (JSAT), April Edition, **(2011)**, pp. 31-38.
[9] K. Loukhaoukha, J.-Y. Chouinard and A. Berdai, "A Secure Image Encryption Algorithm Based on Rubik's Cube Principle", Hindawi Publishing Corporation Journal of Electrical and Computer Engineering, **(2012)**, pp. 1-13.
[10] G. Bhatnagar and Q. M. Jonathan Wu, "Selective image encryption based on pixels of interest and singular value decomposition", Digital Signal Processing, vol. 22, **(2012)**, pp. 648-663.
[11] A. K. Mahmood and S. Tawalbed, "A value transformation and random permutation-based coloured image encryption technique", Information and computer security, vol. 5, no. 4, **(2013)**, pp. 290-300.
[12] L. Chen, D. Zhao and F. Ge, "Image encryption based on singular value decomposition and Arnold transform in fractional domain", Optics Communications, vol. 291, **(2013)**, pp. 98-103.
[13] L. Abraham and N. Daniel, "An improved color image encryption algorithm with pixel permutation and bit substitution", International Journal of Research in Engineering and Technology, vol. 02, no. 11, **(2013)**, pp. 333-338.
[14] M. Naor and A. Shamir, "Visual cryptography. In advance in cryptology", EUROCRYPT'94, Lecture notes in computer science, Springer-verlag, vol. 950, **(1995)**, pp. 1-12.
[15] P. Eisen and D. Stinson, "Threshold visual cryptography schemes with specified whiteness levels of reconstructed pixels", Designs, Codes and Cryptography, vol. 25, no. 1, **(2002)** January, pp. 15-61.
[16] P. D'Arco, R. D. Prisco and A. D. Santic, "Measure-independent characterization of contrast optimal visual cryptography schemes", The Journal of Systems and Software, vol. 95, **(2014)**, pp. 89-99.
[17] M. Nakajima and Y. Yamaguchi, "Extended visual cryptography for natural images", University of Tokyo, **(2002)**.
[18] S. Chenthara, M. P. Deepika and Dr. V. Paul, "A Novel Approach on Color Extended Visual Cryptography for General Access Structures using Error Diffusion", International Journal of Advanced Research in Computer and Communication Engineering, vol. 3, no. 2, **(2014)**, pp. 5675-5679.
[19] P.-L. Chiu and K.-H. Lee, "User-friendly threshold visual cryptography with complementary cover images", Signal Processing, vol. 108, **(2015)**, pp. 476-488.
[20] K. Hamdnaalla, A. Wahaballa and O. Wahballa, "Digital Image Confidentiality Depends upon Arnold Transformation and RC4 Algorithms", International Journal of Video & Image Processing and Network Security IJVIPNS-IJENS, vol. 13, no. 04, **(2013)**, pp. 6-17.
[21] N. Isaac, Philosophiae Naturalis Principia Mathematica, 1687.
[22] Y. Sun and J. Chen, "A novel image scrambling method based on the model of the law of gravity", Journal of Fu zhou Univ. (Nat. Sci.), vol. 34, no. 1, **(2006)**, pp. 47-50.
[23] X. Yuan Wang, N. Wei and D. dou Zhang, "A novel image encryption algorithm based on chaotic system and improved Gravity Model", Optics Communications, vol. 338, **(2015)**, pp. 209-217.
[24] T. Kong and D. Zhang, "A new anti-arnold transformation algorithm", Journal of software, vol. 15, no. 10, **(2004)**, pp. 1558-1564.

