Gulf Journal of Mathematics
Vol 4, Issue 4 (2016) 103-107

IMAGE ENCRYPTION BASED ON ARNOLD TRANSFORMATION

M. ESSAID[1*], A. JARJAR[2], I. AKHARRAZ[3] A. SAAIDI[4] AND A. MOUHIB[5]

Abstract. In this paper we present a new color image encryption method based on Arnold transformation and logistic chaotic map. The proposed approach uses the Arnold matrix modified and adapted to simultaneously make a permutation and confusion to image pixels using logistic map, then shifting pixel thus obtained will be put in. The result and analysis take shelter our cryptosystem against static attack and exhaustive.

1. Introduction

The use of multimedia applications has imposed the development of backup techniques and rapid and effective transmission. Currently the need to protect digital information becomes mandatory In this article, we focus on the security of image data, which are considered specific data for their information quality. All recent work concerned with securing data using Shannon basic techniques [1], these general techniques can be classified into two main categories: transformation of values (confusion) and permutation or shifting position (diffusion). The combination therebetween is also possible. In this article we developed a new method for color image encryption of applying a first confusion and diffusion on the pixels of the image to be encrypted using a transformation matrix ARNOLD [2] developed then a translation of the pixels will be involved, and this while ensuring reliable security a reduced calculation time and without information loss. The proposed method uses symmetric key as a logistics map [3, 4, 5].

The Arnold transform, or Arnold's cat map, was set up during the research of ergodic theory by Arnold. Ding and al. [6]. This transformation, using a matrix with 2 dimensions, is widely used in cryptographic systems for square images. The formula is represented in Equation 1.

$$\begin{pmatrix} x_{n+1} \\ y_{n+1} \end{pmatrix} = \begin{pmatrix} 1 & a \\ b & ab+1 \end{pmatrix} \begin{pmatrix} x_n \\ y_n \end{pmatrix} mod(N) \qquad (1)$$

Date: Accepted: Oct 24, 2016.
* Corresponding author.
2010 *Mathematics Subject Classification.* 94A08 , 94A60.
Key words and phrases. Image Encryption, Transformation Arnold, logistic map, translation vector.

Where x_n and y_n represent the positions of pixels in the original image of $N \times N$ square dimensions, and x_{n+1} and y_{n+1} represent the new position after the transformation of Arnold, while a and b are integers such that the determinant of the matrix is 1, $(det \begin{pmatrix} 1 & a \\ b & ab+1 \end{pmatrix} = 1)$

A chaotic signal looks like noise, but which is completely reproducible because it is generated by deterministic mathematical models. This signal is very sensitive to initial conditions, make it difficult reproduction if the generation model remains unknown. Logistics map is part of the non-linear equations that can be applied to generate the symmetric keys. Although it is simple, it can embody the whole nature of non linearity phenomenon. Its function is indicated in Equation 2.

$$\left\{ \begin{array}{l} X_0 \in [0,1] \\ X_{n+1} = \mu X_n(1 - X_n) \qquad (2) \end{array} \right\}$$

Where μ represent the control parameter $\mu \in [0, 4]$; the chaotic behaviour takes place when $\mu > 3.58$. Logistics resulting map will be used to generate keys of confusion, diffusion and pixel shift.

In the same line of research on the image encryption processing of Arnold and the chaotic system, more works was done : the authors of [7] proposed an efficient image encryption algorithm using the generalized Arnold map, the authors of [8] proposed an image Optical color image encryption based on Arnold transform and interference, the authors of [9] developed a color image encryption technique by affine hill cipher over $SL_n(\mathbb{F}_q)$ and $M_n(\mathbb{F}_q)$ domains with Arnold transform.

This article is organized as follows: after an introduction and a brief overview of previous work, a description of the proposed methodology will be presented, then we will present the simulation results obtained after implementation of our method to prove the robustness and reliability of our approach.

2. Our method

The proposed method is to create the Arnold improved three-dimensional matrix shown in equation (3), which will be used to permut the positions of pixels and a scramble the levels values of the original image, after diffusion and permutation, a translation by an vector is involved, the formula is shown in equation (4) :

$$\begin{pmatrix} x_{n+1} \\ y_{n+1} \\ z_{n+1} \end{pmatrix} = \begin{pmatrix} 1 & q & 0 \\ p & pq+1 & 0 \\ 0 & 0 & a \end{pmatrix} \begin{pmatrix} x_n \\ y_n \\ z_n \end{pmatrix} mod(256) \qquad (3)$$

Where (x_{n+1}, y_{n+1}) represents the new pixel positions after permutation, z_{n+1} is scrambled pixel value, while (x_n, y_n) are the pixel positions of the original image and z_n the pixel color value within the coordinates (x_n, y_n). Then a shift of the pixels thus obtained by applying a translation, the formula is shown in equation (4).

$$\begin{pmatrix} x_{n+1} \\ y_{n+1} \\ z_{n+1} \end{pmatrix} = \begin{pmatrix} 1 & q & 0 \\ p & pq+1 & 0 \\ 0 & 0 & a \end{pmatrix} \begin{pmatrix} x_n \\ y_n \\ z_n \end{pmatrix} + \begin{pmatrix} T_n \\ T_n \\ T_n \end{pmatrix} mod(256) \qquad (4)$$

Where T_x is an integer in the $\mathbb{Z}/n\mathbb{Z}$ for a next shift the x-axis, T_y is an integer in the $\mathbb{Z}/m\mathbb{Z}$ for a next shift the y-axis, and T is an integer in $\mathbb{Z}/256\mathbb{Z}$ for a color shift levels. The diagram below shows the encryption principle by the proposed method.

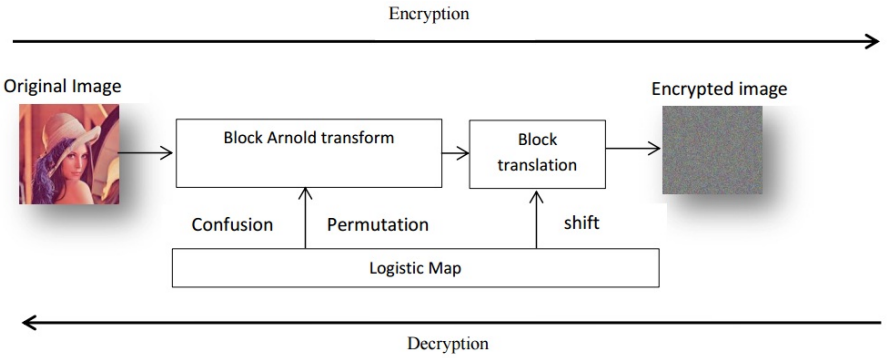

FIGURE 1.

The image encryption principle indicated in the scheme in Figure 1, consists in simultaneously applying a xorification and a permutation of the original image by the logistic map created, then a shift of pixels obtained by a translation vector. Decryption is to follow the steps indicated in Fig 1 in the opposite direction.

3. Simulation results and safety analysis

All simulations are performed under the windows 8 environment, Core i5, 2GHZ frequency processor and 4GB RAM capacity with the Java development language, while the images used come from the web site [10].

2.1. Sensitivity of key brutal attacks

The key used is formed of two real numbers double precision namely and 64 bits each, so our key space is 128 bits, which requires a comprehensive attack 1036 which is more than enough to shelter the key used against a brutal attack.

1.2. Statistical analysis

An image histogram is a graphical representation of the number of pixels having the same gray level. Therefore cryptography color distribution of an encrypted image is very important, hence the histogram of the encrypted image may in some cases raise information on the original image, the histogram analysis is a control of visual form encryption quality, a theoretical study, it makes use of entropy analysis [1] entropy is used to express the randomness of the information for an

image entropy can measure distribution of gray level values in the image. More the distribution of gray values of the pixels, the more the information entropy is higher, we also measured the time of encryption and decryption. The figure 1 shows the histograms of clear images and those of the encrypted images, the entropy of the original image and that of the encrypted image and the time of encryption and decryption.

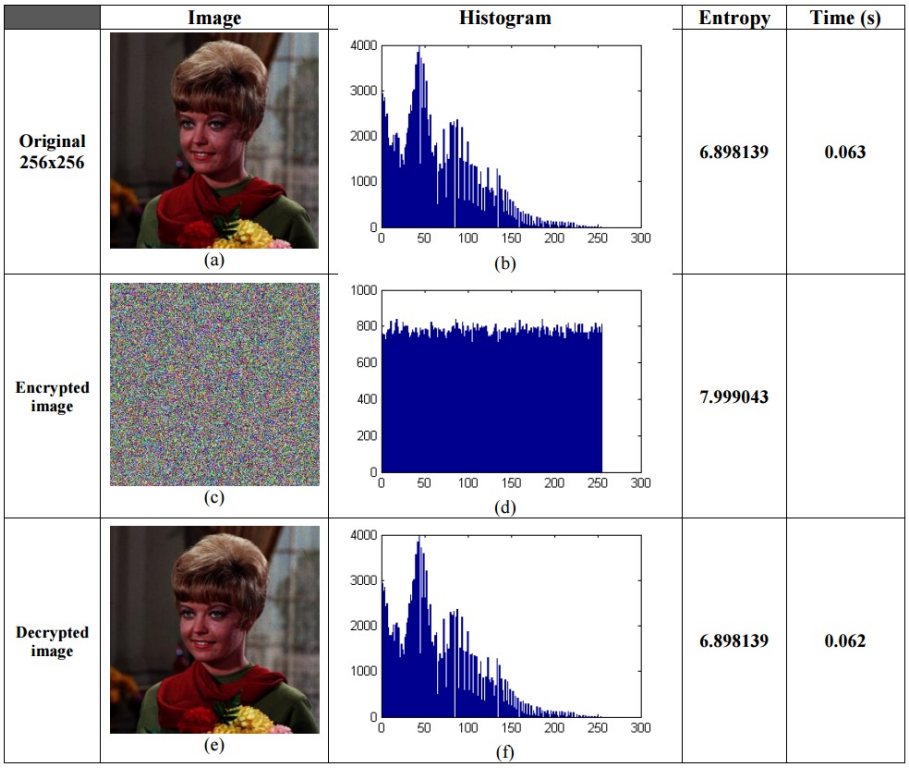

FIGURE 2. a) The plain image "girl", b) original histogram, c) Encryption of "girl" using our method, d) Encrypted histogram, e) Image decrypted "girl", f) decrypted histogram

4. Conclusion

In this article we have proposed a new simple and effective approach based on the transformation of Arnold improved and developed to apply a permutation and confusion on the pixels of the image and to make our robust cryptographic system we applied a shift on the pixels with a dynamic translation vector, the simulation results presented by a flat histogram of the encrypted image, entropy almost equal to 8 show a remarkable strength of our approach against any cryptanalysis.

References

1. Claude S., Communication theory of secrecy systems, Bell System Technical Journal 28(4), (1949), pp. 656715.

2. W.Ding and al., Digital image scrambling technology based on Arnold transformation, J. Comput. Aided Des. Comput. Graph., 2001, 13, (4) (China), pp. 338341.
3. Mao-Yu Huang and al., Image Encryption Method Based on Chaotic Map, International Computer Symposium (ICS), 2010, pp. 154-158.
4. A.N. Pisarchik and al., Image encryption with chaotically coupled chaotic maps, Physica D 237 (2008), pp. 2638-2648.
5. N.K. Pareek and al., Cryptography using multiple one-dimensional chaotic maps, Commun. Nonlinear Sci. Numer. Simul. 10 (7) (2005), pp. 715-723.
6. Y.Wang and al., A new chaos-based fast image encryption algorithm, Appl. Soft Comput. 11, (2011), pp. 514522
7. Ye.Guodong and al., An efficient chaotic image encryption algorithm based on a generalized Arnold map, Nonlinear Dyn 69, (2012), pp. 20792087.
8. W. Chen and al., Optical color image encryption based on Arnold transform and interference method, Optics Communications 282, (2009), pp. 36803685.
9. D. C. Mishra and al., Security of RGB image data by affine hill cipher over $SL_n(\mathbb{F}_q)$ and $M_n(\mathbb{F}_q)$ domains with Arnold transform, 09/086(1068), 2010.
10. http://sipi.usc.edu/database 21/09/2013.

[1 2 3 4 5]Department of Mathematics, Physics and Computing, LSI, FPT, University S.M. Ben Abdellah, Taza, Box 1223, , Morocco.
E-mail address: [1]essaid_mouhsin@yahoo.fr,[2]abdoujjar@gmail.com,
E-mail address: [3]ismail.akharraz@usmba.ac.ma, [4]abderrahim.saaidi@usmba.ac.ma
E-mail address: [5]mouhibali@yahoo.fr