Volume 4, Issue 8, August 2014 ISSN: 2277 128X
International Journal of Advanced Research in Computer Science and Software Engineering
Research Paper
Available online at: www.ijarcsse.com

Image Encryption Based On Arnold Cat Map and S-Box

Priyanka Gupta
Shaheed Sukhdev College of Business studies
University of Delhi, India

Sonia Singh
Shyamlal College(Eve)
University of Delhi, India

Isha Mangal
Vivekananda College
University of Delhi, India

Abstract: In this paper, a new image encryption technique is proposed based on the combination of the pixel shuffling and S-box of AES encryption algorithm. Firstly, the Arnold cat map is used to shuffle the positions of the image pixels in the spatial-domain. Then the shuffled image is encrypted by nonlinear byte-substitution using S-box. In order to evaluate the performance, the proposed algorithm was executed through a series of tests. Experimental results demonstrate that the presented algorithm shows an appropriate resistance against statistical attacks but it is weak against differential analysis.

Keywords: AES, Arnold-cat map, S-box.

I. INTRODUCTION

With the increase popularity of multimedia application over the internet, protection of digital information against unauthorized access has become extremely important. Digital Image is the important information that is exchanged over these channels and is need to be encrypted. Images are large in size and have higher redundancy capacity and have correlation between the pixels. Due to these inherent features of the images, the traditional encryption scheme such as AES [1-4], DES [5-7] for data encryption is not appropriate for the multimedia data.

Although AES and DES are useless in image encryption, the concept of S-box of AES can be used in substitution phase of image encryption. During image encryption, Arnold cat map is also introduced to shuffle the pixel positions of the image in to order to disturb the high correlation among the pixels. As a result, the algorithm is secure against statistical attack.

The paper discusses the new algorithm for image encryption based on Arnold cat map and S-box. The paper is organized as follows. In section II Arnold cat map and its properties and S-box substitution are discussed. Section III covers encryption and decryption algorithm. Section IV describes the experimental analysis of proposed technique. Security analysis is given in section V, and Section VI concludes the introduced algorithm.

II. ARNOLD CAT MAP AND S-BOX

The Arnold cat map is a two-dimensional invertible chaotic map [8-9]; it is used to shuffle the pixel positions of the plain image. Without loss of generality, we assume the dimension of the original image to be N × N. The coordinates of the pixels are $S = \{(x, y) \mid x, y=0, 1, 2... N-1\}$. The 2-D Arnold cat map can be described as follows:

$$\begin{aligned}\begin{bmatrix} x' \\ y' \end{bmatrix} &= A\begin{bmatrix} x \\ y \end{bmatrix}(\bmod N) \\ &= \begin{bmatrix} 1 & p \\ q & pq+1 \end{bmatrix}\begin{bmatrix} x \\ y \end{bmatrix}(\bmod N)\end{aligned}$$

Where p and q are positive integers, determinant (A) = 1. The (x', y') is the new positions of the original pixel position (x, y) when Arnold cat map is performed once. The result after applying the Arnold Cat Map for number of iterations iterating R will be a shuffled image that contains all of the same pixel values of the original image. The number of iteration R to satisfied that depends on the parameters p, q and the size N of the original image. Thus the Arnold cat map's parameters p, q, and the number of iterations R, all can be used as the secret keys.

It is very efficient to shuffle the pixel positions using the Arnold cat map as only linear transformation and mod function need to be performed. After several iterations, the correlation among the adjacent pixels can be disturbed completely. The interesting part of Arnold Cat Map is that if it is applied repeatedly, after a certain number of iterations the original image reappears. Hence it cannot be used alone. So, for enhancing the security of the algorithm it requires further processing.

S-box is the most important component in the block cipher. S-box is constructed by the composition of two transformations [10]:

1 First, taking the multiplicative inverse in GF (2^8). '00' is mapped onto itself.

2. Then applying an affine transformation defined by:

$$\begin{bmatrix} b_1 \\ b_2 \\ b_3 \\ b_4 \\ b_5 \\ b_6 \\ b_7 \\ b_8 \end{bmatrix} = \begin{bmatrix} 1 & 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 1 & 1 & 0 & 0 & 0 & 1 & 1 & 1 \\ 1 & 1 & 1 & 0 & 0 & 0 & 1 & 1 \\ 1 & 1 & 1 & 1 & 0 & 0 & 0 & 1 \\ 1 & 1 & 1 & 1 & 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 1 & 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 & 1 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 \end{bmatrix} \begin{bmatrix} a_1 \\ a_2 \\ a_3 \\ a_4 \\ a_5 \\ a_6 \\ a_7 \\ a_8 \end{bmatrix} + \begin{bmatrix} 1 \\ 1 \\ 0 \\ 0 \\ 0 \\ 1 \\ 1 \\ 0 \end{bmatrix}$$

III. PROPOSED ALGORITHM

The image encryption algorithm starts with the shuffling of the pixel position using Arnold cat map and then it performs the substitution of the pixel values of the result using s-box table. These two steps are performed for k iterations. Figure 1 illustrates the block diagram of the proposed algorithm. The proposed algorithm is implemented in MATLAB.

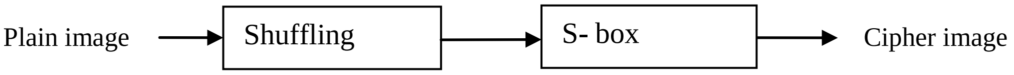


Fig.1 Block diagram of proposed scheme

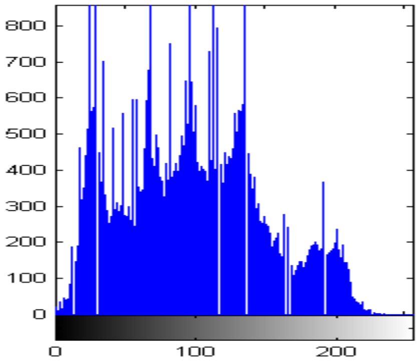
Let the dimension of the original grayscale image *I* is *N* x *N*. The encryption algorithm is as follows:

```
Generate S-box
I' = I
For   i=1 to k
        Shuffle the positions of the pixels of the image I' using Arnold cat map which result in shuffled image E'.
        Substitute the pixel values of the shuffled image E' using the s-box table.
        I' = E'
End For
```

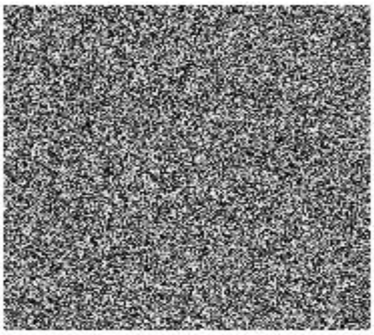
The encrypted image is stored in *E*'. The decryption algorithm is similar to the encryption algorithm, but with replacing the Arnold cat map with its inverse and using the inverse S-box substitution at the beginning of the iteration. The decryption algorithm restores the original image without loss of quality. The decryption algorithm is described as follows:

```
Generate inverse S-box
  D = E'
For   i=1 to k
        Substitute the pixel values of the image D using the inverse s-box table.
        Shuffle the positions of the pixels of the image D using inverse transformation of Arnold cat map which result in image D'.
        D = D'
End For
```

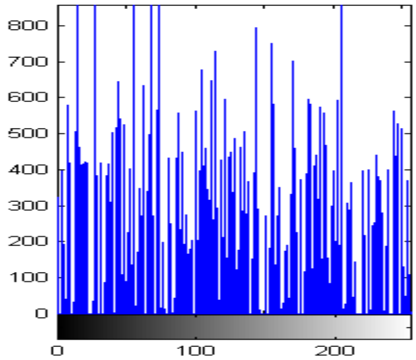
(a) Original image



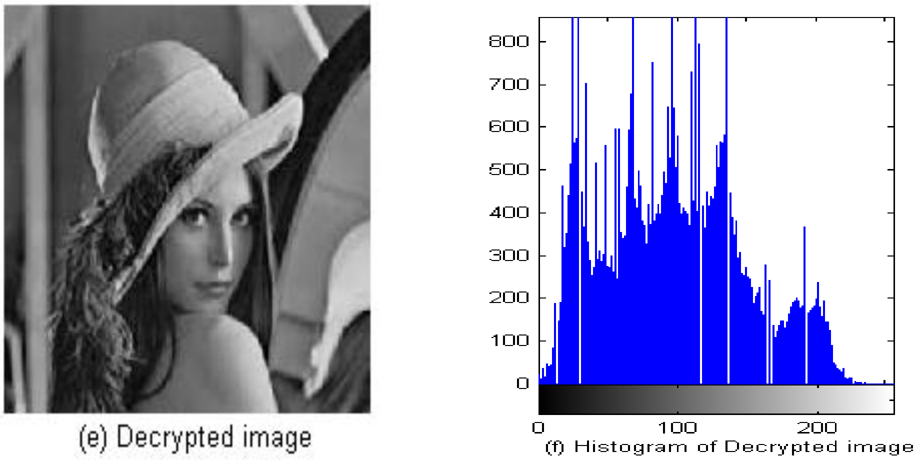
(b) Histogram of original image



(c) Encrypted image



(d) Histogram of the Encrypted image



(e) Decrypted image

(f) Histogram of Decrypted image

Fig. 2 Image encryption and decryption experimental result.

IV. EXPERIMENTAL ANALYSIS

Experimental analysis of the proposed image encryption algorithm in this paper has been done. The plain-image with the size 256 × 256 is shown in Fig. 2(a) and the histogram of the plain-image is shown in Fig. 2(b). The secret keys are chosen as p = 1, q = 1 and number of iterations k = 5. The encrypted image is shown in Fig. 2(c) and the histogram is shown in Fig. 2(d). From the figure, one can analyze that the histogram of the encrypted image is approximately uniformly distributed and is different from that of the original image. The decrypted image is shown in Fig. 2(e) and the histogram is shown in Fig. 2(f).

V. SECURITY ANALYSIS

A. Measurement of encryption quality

The quality of image encryption [11] may be determined as follows:

Let P and E denote the original image and the encrypted image respectively each of size M*N pixels with L grey levels. $P(x, y)$, $E(x, y)$ ε $\{0,..., L-1\}$ are the grey levels of the images P and E at position (x, y) $(0 \le x \le M-1,\ 0 \le y \le N-1)$. Let $H_L(P)$ denote the number of occurrences of each grey level L in the original image P and $H_L(E)$ denotes the number of occurrences of each grey level L in the encrypted image E. The encryption quality represents the average number of changes to each grey level L and is expressed mathematically as:

$$Encryption\,Quality = \frac{\sum_{L=0}^{255} \left| H_L(E) - H_L(P) \right|}{256}$$

The encryption quality of proposed scheme for input image of size 256×256 is computed as 233.9688.

B. Analysis of correlation of two adjacent pixels

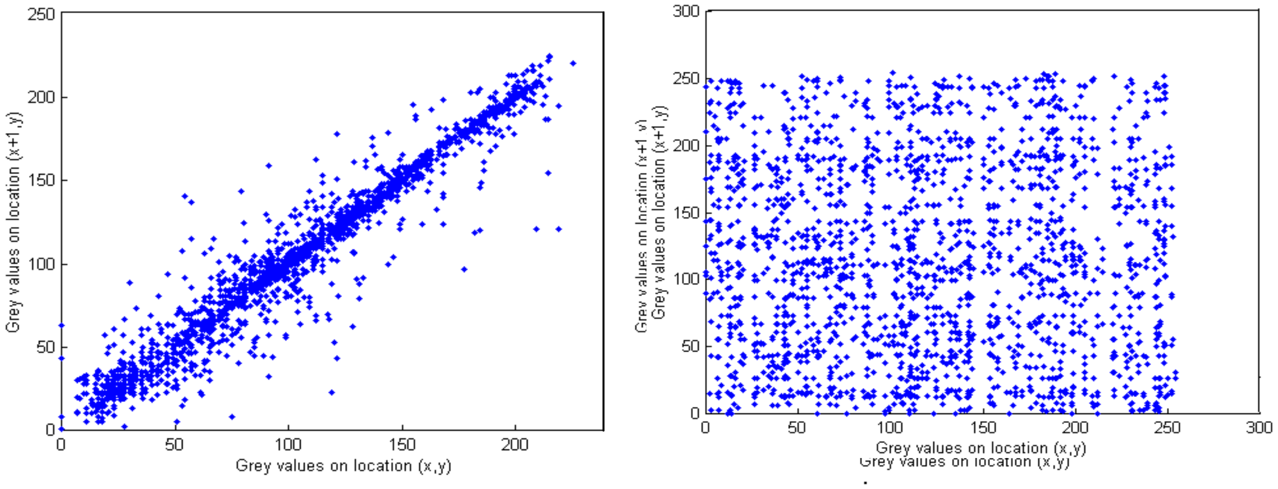
To examine the correlation property between two vertically adjacent pixels, two horizontally adjacent pixels, two diagonally adjacent pixels in the encrypted image, the following method **is** used.

First, we randomly select 2000 pairs of two adjacent pixels from the image. Second, we calculate the correlation coefficient of each adjacent pair by using the following formulas [11]:

$$\overline{A} = \frac{1}{N}\sum_{i=1}^{N} x_i \qquad \overline{B} = \frac{1}{N}\sum_{i=1}^{N} y_i$$

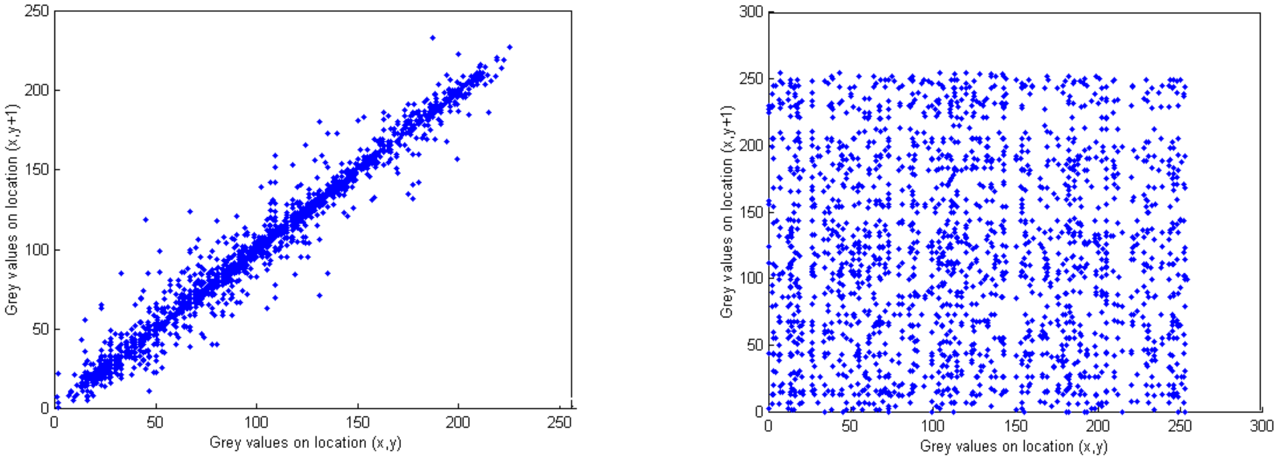
$$r = \frac{\sum_{i=1}^{N}\left(x_i - \overline{A}\right)\left(y_i - \overline{B}\right)}{\sqrt{\left(\sum_{i=1}^{N}\left(x_i - \overline{A}\right)^2\right)\left(\sum_{i=1}^{N}\left(y_i - \overline{B}\right)^2\right)}}$$

where N is the number of number of adjacent pixels selected from the image to calculate the correlation in an image, x_i and y_i are the values of adjacent pixels vertically, horizontally and diagonally in the image.



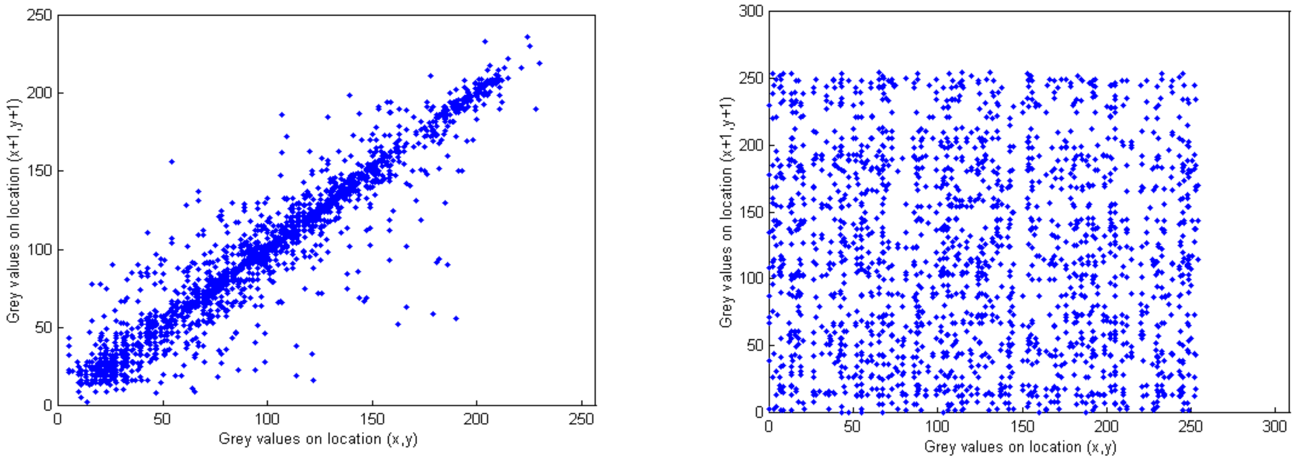
(a) Correlation in the original image (b) Correlation in the encrypted image

Fig. 3 Correlations of two horizontally adjacent pixels in the original image and in the encrypted image.



(a) Correlation in the original image (b) Correlation in the encrypted imagee

Fig. 4 Correlations of two vertically adjacent pixels in the original image and in the encrypted image.



(a) Correlation in the original image (b) Correlation in the encrypted image

Fig. 5 Correlations of two diagonally adjacent pixels in the original image and in the encrypted image.

Figure 3 shows the correlation distribution of two horizontally adjacent pixels in the original image and that in the encrypted image. Figure 4 shows the correlation distribution of two vertically adjacent pixels in the original image and that in the encrypted image. Figure 5 shows the correlation distribution of two diagonally adjacent pixels in the original image and that in the encrypted image. It is observed that neighboring pixels in the plain-image are highly correlated either in horizontally, vertically or diagonally, while there is a little correlation between neighboring pixels in the encrypted image. The correlation coefficient values are shown in table 1.

Table I. Correlation coefficients of two adjacent pixels in two images

Correlation coefficients analysis			
Image	Orientation		
	Horizontal	Vertical	Diagonal
Original image	0.9671	0.9852	0.9464
Encrypted image	-0.0160	-0.0165	-0.0362

C. Differential analysis

To test the influence of one-pixel change on the whole image encrypted by the proposed algorithm, two common measures were used: NPCR and UACI [12]. NPCR means the number of pixels change rate of encrypted image while one pixel of original image is changed. UACI which is the unified average changing intensity, measures the average intensity of the differences between the original image (plain-image) and encrypted image (ciphered image). Consider two encrypted images (cipher-images), *E*1 and *E*2, whose corresponding original images (plain-images) have only one pixel difference. The NPCR of these two images is defined in

$$NPCR = \frac{\sum_{i,j} D(i,j)}{M \times N} \times 100\%$$

Where *D(i j)* is defined as

$$D(i,j) = \begin{cases} 0, & if \quad C_1(i,j) = C_2(i,j) \\ 1, & if \quad C_1(i,j) \neq C_2(i,j) \end{cases}$$

Another measure, UACI, is defined by the following formula:

$$UACI = \frac{1}{M \times N} \sum_{i,j} \left[\frac{|C_1(i,j) - C_2(i,j)\ |}{255} \right] \times 100\%$$

Tests have been performed on the proposed scheme, about the one-pixel change influence on a 256 gray-scale input image size 256×256. The NPCR and UACI test results are shown in table 2. Results obtained from NPCR show that the encryption scheme is not sensitive to small changes in the input image. The UACI estimation result shows that the rate influence due to one pixel change is very low. It is observed from the results that a swiftly change in the original image will result in a negligible change in the encrypted image (ciphered image), so the proposed algorithm is weak against differential analysis.

Table II. NPCR and UACI of proposed algorithm.

Measure	Value
NPCR	0.0015%
UACI	$8.3774\text{x}10^{-4}$ %

VI. CONCLUSION

In this paper, an image encryption algorithm based on combination of Arnold map and s-box non-linear byte substitution which is used by other cipher algorithms such as AES, DES has been discussed. Experimental results show that the presented algorithm is not vulnerable to statistical attack but it is weak against differential analysis.

REFERENCES

[1] AES, N. I. S. T. "Advanced encryption standard." Federal Information Processing Standard, FIPS-197 12 (2001).

[2] Daemen, Joan, and Vincent Rijmen. The design of Rijndael: AES-the advanced encryption standard. Springer, 2002.

[3] Miller, Frederic P., Agnes F. Vandome, and John McBrewster. "Advanced Encryption Standard." (2009).

[4] Rijmen, Vincent, and Joan Daemen. "Advanced Encryption Standard."Proceedings of Federal Information Processing Standards Publications, National Institute of Standards and Technology (2001): 19-22.

[5] Biham, Eli, and Adi Shamir. Differential cryptanalysis of the data encryption standard. Vol. 28. New York: Springer-Verlag, 1993.

[6] Diffie, Whitfield, and Martin E. Hellman. "Special feature exhaustive cryptanalysis of the NBS data encryption standard." Computer 10.6 (1977): 74-84.

[7] Coppersmith, Don. "The Data Encryption Standard (DES) and its strength against attacks." IBM journal of research and development 38.3 (1994): 243-250.

[8] Zhenwei Shang, Honge Ren, Jian Zhang. 2008.A Block Location Scrambling Algorithm of Digital Image Based on Arnold Transformation. The 9 th International Conference for Young Computer Scientists, 978-0-7695-3398-8/08/$25.00 © IEEE.

[9] Zhu Liehuang, Li Wenzhuo, Liao Lejian, LiHong. 2006. A Novel Algorithm for Scrambling Digital Image Based on Cat Chaotic Mapping. Proceedings of the 2006 International Conference on Intelligent Information Hiding and Multimedia Signal Processing (IIH-MSP'06), 0-7695-2745-0/06© IEEE.

[10] http://csrc.nist.gov/archive/aes/rijndael/Rijndael-ammended.pdf

[11] Hossam El-Din H. Ahmed, Hamdy M. Kalash, And Osama S. Farag Allah, "Encryption Quality Analysis Of RC5 Block Cipher Algorithm For Digital Images", Journal Of Optical Engineering, Vol. 45, 2006.

[12] G. Alvarez And S. Li, "Some Basic Cryptographic Requirements For Chaos-Based Cryptosystems," International Journal Of Bifurcation And Chaos, Vol. 16, No. 8, Pp. 2129–2151, 2006.