VOL. 13, NO. 3, FEBRUARY 2018 ISSN 1819-6608
ARPN Journal of Engineering and Applied Sciences

www.arpnjournals.com

CIPHER SECRET IMAGE USING HYBRID VISUAL CRYPTOGRAPHY

Reem Ibrahim Hasan[1] and Huda Adil Abdulghafoor[2]
[1]Information Technology Centre, Iraqi Commission for Computers and Informatics, Baghdad, Iraq
[2]Information and Communication Technology Department, Central Bank of Iraq, Baghdad, Iraq
E-Mail: reemhasan@uoitc.edu.iq

ABSTRACT

Attackers always try to break ciphers whether this cipher is image or text in order to reach the required data due to this fact new methods of ciphering are always presenting. This paper discusses a new method employed a chaos system to shuffle image pixels and blocks according to Arnold Cat Map (ACM). The proposed method employed Visual cryptography (VC) as well in order to cover the encrypted image. These concepts are considered as the best techniques used to implement an efficient way to secure images via the internet. This paper includes several statistical attacking and qualification measurements to evaluate the proposed system and its performance. The result of the proposed system obtained with a minimum computational time, storage space and qualified recovered image.

Keywords: blocks shuffling, VC, ACM, cover encrypted image.

1. INTRODUCTION

Image security has become a very important matter. Securing the image is being sent over the internet from one user to another. Hackers are getting used to stealing image data and they are increasing every day. A hacker takes a personal image data in order to use it illegally; a lot of reasons could be due to stealing an image in order to ruin people's reputations on the internet by publishing it in unauthorized and illegal ways. Images must be transferred in a secure way to guarantee the privacy of user's image data. Most of image securing systems are not upgrading to the level of protecting images from most hacking attacks. Cryptography is the science concerns with securing information when it is transmitted and stored on the internet [1]. This research includes several mechanisms to secure the transmitted image; Firstly, Arnold Cat Map is a chaotic map due to scramble image pixels, this algorithm is simple and periodic. Since Arnold is periodic, the image will be restored after several iterations. In order to increase the image security, the second stage includes using Visual Cryptography (VC) sharing [2]. Visual cryptography was originally introduced by Shamir and Naor in the nineties; they suggested a new method in cryptography in order to restore the original text by the human visual system. There is no need for the complex calculation to decrypt the cryptography [3]. Shares are binary images that are usually presented in transparencies. Each participant holds a transparency (share). Unlike other traditional cryptographic methods, VC does not include any complex computation in order to recover the secret image. Decryption is simply done by stacking shares to view the secret image which appears by stacking these shares [3]. This research hybridizes the concept of Arnold Cat Map and creates a new image input to Visual Cryptography (VC) Sharing in order to secure image that is being sent over the internet.

This paper is presented as follows. Section 2 introduces the backgrounds; Section 3 introduces the proposed encryption and decryption methods. Experimental results and quantitative analysis are discussed. Finally, this paper is summarized in Section 5.

2. BACKGROUNDS

Cryptography science concerns about information security by using math techniques that are based on information aspects. These aspects are confidentiality, integrity, authentication and origin authentication. Cryptography work is based on encryption and decryption algorithms. Encryption algorithm is used to change the original appearance of data whether the data is text, image, etc.

The encryption process is done by using several math techniques, the resulted data will not be recognized by any intruder in order to be sent on the internet. Decryption algorithm is used to restore the original appearance of the data. The decryption process is done by reversing the encryption process in order to restore the original data [4].

2.1 Visual cryptography

Visual cryptography can be explained as the science that enables computer users of sharing an image in a private way without any restrictions. At the sending side, the secret image will be divided into multiple shares. Each share is generated by using an artificial intelligence [7] algorithm, cryptographic algorithm [6] and advanced mathematics [8]. Shares are overlapped with cryptographic algorithms in order to increase the security of the shared image. At the receiving side, all shares are combined to form the original secret image [5].

2.2 Arnold cat map

It is a chaotic map on a tour, in which individuals movement is free on a path of a specific length with their coordinates x and y. ACM named according to V.I.Arnold who clarified the manner in which the map is constructed. He used a cat face picture. There are two transformation procedures to construct the map. The first transfer is geometrically, it depends on pixels coordinates of the image on the map. The second transfer is the transfer of elements inside a unit square [13].

More precisely, in each iteration pixels of the image shuffled to a new coordination according to (1) until

they return to their original axes after a certain number of iterations.

$$\Gamma\begin{bmatrix} x \\ y \end{bmatrix} \rightarrow \begin{bmatrix} x+y \\ x+2y \end{bmatrix} \bmod n \quad (1)$$

Where n represents the number of pixels in each row. Modulo n operation determines the length of the path. For example a pixel in an image of size 124*124 needs 15 iterations in order to complete the tour and to return to its original position. (1) Applied to each pixel in an image. It determines the new movement of the pixel in the path.

3. SUGGESTED METHOD

The suggested method has proposed a model to encrypt a colored image through two stages: the first stage is based on Arnold cat map algorithm, in which pixels of the secret image are shuffled in a randomize manner that changes the original arrangement of these pixels. The second stage is based on a VC method in which a random technique is used to generate a share. The created share will be used to encrypt the image. It does not contain any comprehensible information about that image.

3.1 Pixel permutation using ACM transformation

The colored image is split into three layers (Red, Green, Blue). Each layer is represented by a matrix of size n*n as the original image size. ACM algorithm is applied on the three matrices with a determined number of iterations.

3.2 Visual cryptography

In the second stage, the visual cryptography is applied.

3.2.1 Share generation

A share of three layers is generated. Each layer of the generated share will be XOR with its correspondence layer that is resulted from the first stage. The share is generated as follows: two temporary shares are generated; both have the size of the original image. First, one is random, and the second is based on matrices that are generated in the first stage Section (3.1) but with the complementary colors as follows:

```
For ii=0 to N
For jj=0 to N
CompR [ii,jj]= 255- Red[N-ii,jj]
CompG [ii,jj]= 255- Green[N-ii,jj]
CompB [ii,jj]= 255- Blue[N-ii,jj]
Next
Next
```

These two shares will be used to create a third share. The third share will be the cover of the intended image to be encrypted. The odd rows will be copied from the first share. The even rows will be copied from the second share. The resulted share does not have any information about the original image because the pixels have been rearranged and the contents of the cells have been changed too.

3.2.2 Image encryption

In this stage the resulted share 3 of Section (3.2.1) will be divided into 3 layers (R, G, B). Each layer is XOR with its correspondence layer resulted from the first stage.

3.2.3 Share encryption

The third share will be encrypted before sending it as follows: it will be converted to binary then each zero is followed by one will be transformed to its complementary. That means, they will be transformed to one followed by zero. Contrarily, in even rows, one is followed by zero will be transformed to its complementary. That means, they will be transformed to zero followed by one.

3.2.4 Image and share block shuffling using ACM

The encrypted image and the encrypted share will be divided into m blocks and these blocks will be divided into another m blocks. These m*m blocks will be shuffled using ACM. Each block will be treated as a pixel. Each block will be shuffled according to (1).

3.3 The proposed algorithm

Input: Colored image of size N*N

Output: encrypted share with the encrypted image

Steps:

a) Split the selected image to three layers red, green and blue.

b) Shuffle the pixels of step 1 using Arnold Cat Map method on these layers (R,G,B) for ten iterations.

c) Generate the share as follows:

- Generate share 1 randomly (RandR,RandG,RandB) of size N*N.
- Generate share 2 by taking color complementary of step 2(CompR, CompG, CompB).
- Generate Share 3 by copying odd rows from share 1 and even rows from share2.

(Share 3R, Share 3G, share 3Blue).

d) XOR (R,G,B) of step 2 with (Share 3R, Share 3G, share 3B) after converting them to binary.

e) Encrypt (Share 3R, Share 3G, share 3B) as follows:

- Transform each 01 to 10 in the odd row.

- Transform each 10 to 01 in the even row.

f) Share3 will be divided into m*m blocks, these blocks will be shuffled a certain number of iterations according to ACM.

g) Results of step 4 will be divided into m*m blocks, these blocks are shuffled by a certain number of iterations according to ACM.

3.4 Image decryption

Decryption procedure is similar in every detail to encryption scheme. The difference is only in a number of iterations which is predefined between sender and receiver. According to ACM, each shuffled pixel needs a certain number of iterations to return to its original place. It depends on the number of pixels the rows.

4. EXPERIMENTAL RESULTS AND DISCUSSION

The proposed method ran by using Visual Studio 2013, visual basic language under the configuration of Windows 7 OS of Core i7 and 8 GB RAM. The total execution time of encryption level is 3 seconds (2 seconds are needed for 10 iterations of pixels shuffling by using ACM. ACM is applied for the three layers). Total execution time of decryption level is 2 seconds. The results of each stage of encryption are shown in Figure2, samples of the applied method in encryption and decryption levels are shown in Figure-4.

4.1 Encryption stage

The encryption method has been applied on many colored images of size 124*124. In the first stage of encryption, the pixels of the secret image are shuffled ten times according to ACM then XOR operation is applied to the shuffled pixels with the generated share. The share will be encrypted. The encrypted share is divided into four blocks. Each block is divided into another four blocks. The resulted 16 blocks are shuffled by using ACM. The number of iterations will be predefined between the sender and the receiver.

1	2	3	4
5	6	7	8
9	10	11	12
13	14	15	16

(a)

1	15	9	7
8	2	16	10
11	5	3	13
14	12	6	4

(b)

Figure-1. Encrypting Share3 (a) dividing the encrypted share to 16 blocks,(b) shuffled blocks after1 iteration according to ACM.

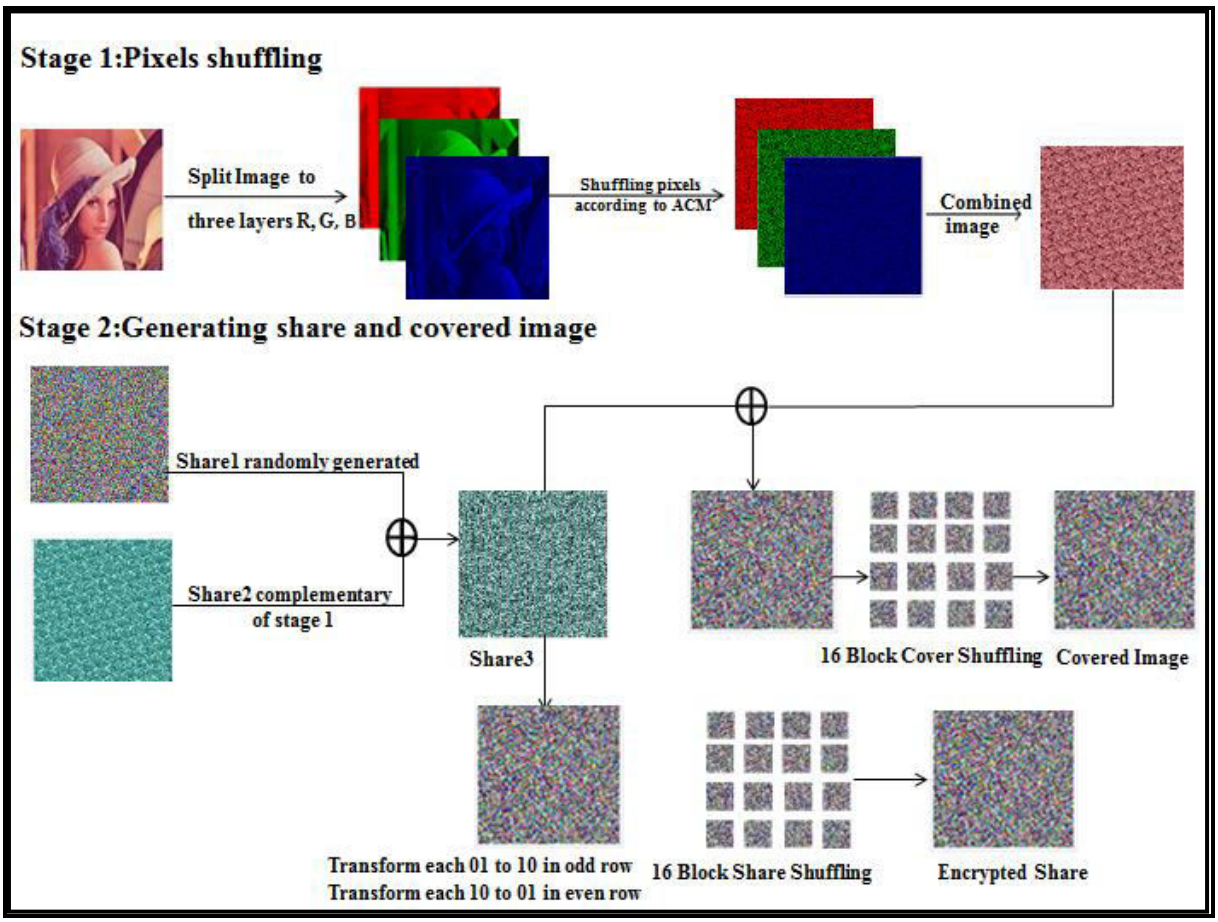


Figure-2. It shows the result of each stage of the encryption method.

4.2 Decryption stage

As mention in section 3.4 the decryption process is a reversed order of the encryption process. For blocks suffling 2 cycles of ACM are needed.For pixels shuffling 5 cycles of ACM are needed.

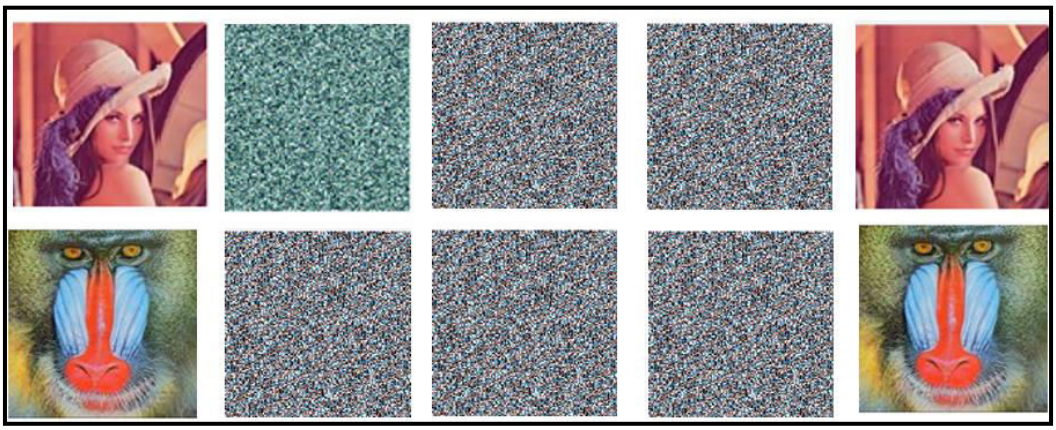
1	6	11	16
10	15	4	5
3	8	9	14
12	13	2	7

(a)

1	2	3	4
5	6	7	8
9	10	11	12
13	14	15	16

(b)

Figure-3. Share 3 decrypting. Blocks shuffling in decryption level according to ACM a shown in Figure-3 (a), (b) the required form of the rearranged blocks.



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

Figure-4. The original, encrypted and decrypted images: (a) original colored image, (b) generated share3, (c) encrypted image, (d) encrypted share3, (e) recovered image.

4.3 Quality measures

Results have been evaluated using Mean Squared Error (MSE) and Peak Signal to Noise Ratio (PSNR) measures. MSE can be considered as the square difference between the reference image and reconstructed image as shown in (2). The closer the MSE is to zero, the higher quality has the restored image. There is the mathematical relation between PSNR and MSE due to the fact that the higher value of PSNR indicates that the image has a high quality as shown in (3).

$$\text{MSE} = \frac{\sum_{i=1}^{M}\sum_{j=1}^{N}[f(i,j)-f`(i,j)]^2}{MN} \quad (2)$$

$f(i, j)$ is the $(i,j)^{th}$ | pixel value of the original image and $f'(i, j)$ is the pixel value of the recovered image.

$$PSNR = \frac{10\log(2^n-1)^2}{MSE} \quad (3)$$

For the proposed encryption model, the MSE was high. The PSNR is measured in dB values for different samples. Table-1 shows the differences between encrypted images and the original ones. While in decryption model, the MSE reached zero. That means the proposed algorithm is qualified. Table-1 shows as well the differences between generated share 3 for each image and the encrypted share.

Table-1. PSNR (in dB) value for encrypted images samples.

Colored image of size (124x124)	PSNR for encrypted image of size (124x124)	PSNR for generated shares3 of size (124x124)
Lena	7.63	7.21
Baboon	7.69	7.23

5. SECURITY ANALYSIS

5.1 Correlation of adjacent pixels

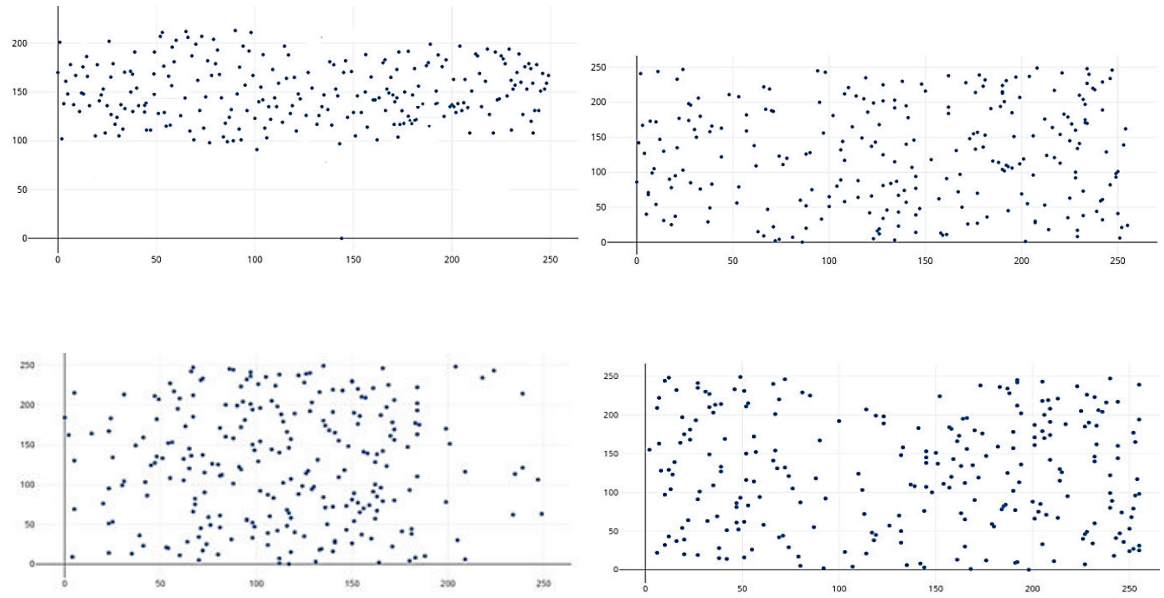
It is used to measure the statistical correlation between adjacent pixels in image direction. Simply done by randomly selecting a thousand pairs of adjacent pixels in a (vertical or horizontal or diagonal direction) of image pixels from the original image and the encrypted image, the correlation coefficient is computed by (4).

$$r_{xy} = \frac{|Cov(x,y)|}{\sqrt{D(x)}\ \sqrt{D(y)}}$$

$$E = \frac{1}{N}\sum_{i=1}^{N} x_i,$$

$$D(x) = \frac{1}{N}\sum_{i=1}^{N}(x_i - E(x))^2$$

$$Cov(x,y) = \frac{1}{N}\sum_{i=1}^{N}(x_i - E(x))(y_i - E(x))$$



(a) (b)

(c)(d)

Figure-5. Correlation horizontally of adjacent pixels (a) original image, (b) encrypted image, (c) decrypted Share3, (d) encrypted Share3.

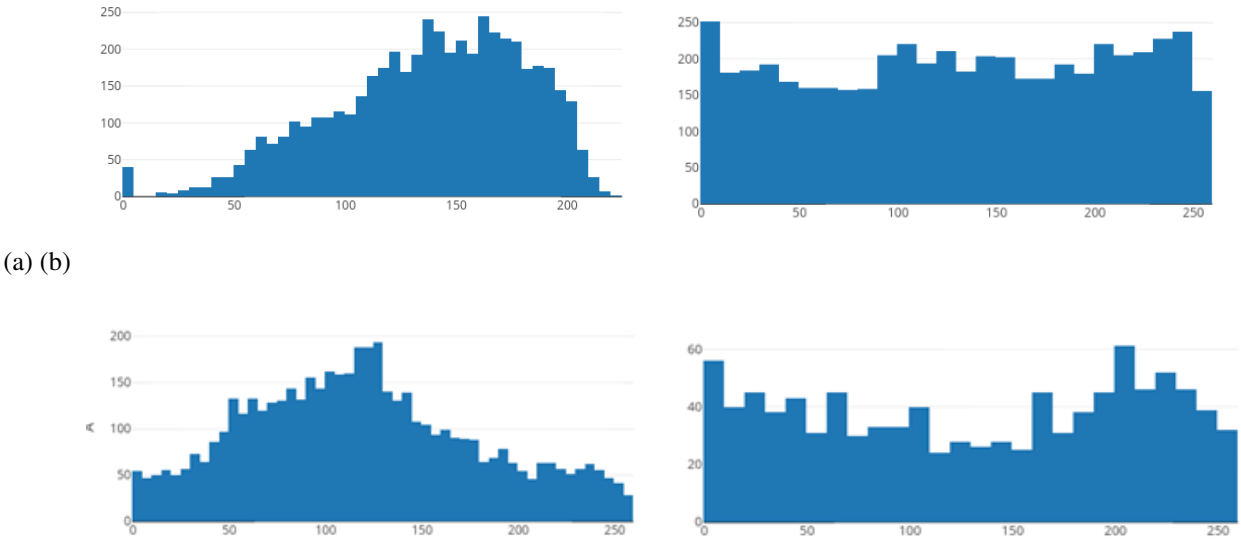
The distribution of the correlated adjacent pixel increased using the proposed method as shown in Table-2, due to the fact that this system is passed statistical analysis from an intruder or attacker. Figure-6 represents Baboon image, in (a) original image most adjacent pixels are grouped horizontally, in (b) the proposed system increased the distribution of the adjacent pixels. While in (c), the Share3 adjacent pixel is already distributed and in (d) the proposed system increased the distribution more.

Table-2. Horizontal Correlation of two Adjacent Pixels: applied on 250 pair samples.

Colored image of size (124x124)	Correlation for generated shares3 of size (124x124)	Correlation for generated shares3 of size (124x124) for each image
Lena	0.0003	0.0008
Baboon	0.0004	0.0007

5.2 Histogram

The data allocation of the encrypted image is a significant factor [11], [12]. The histogram is a graph that represents the distribution of pixel values in an image. The statistical attack can be performed by analysing the image distribution of the pixel value in order to prevent the attack, histogram of the image must be flattened by simply flattening the histogram of the image. The flat image histogram is required in encryption to strength the proposed system.



(a) (b)

(c) (d)

Figure-6. Histogram of pixels (a) original image, (b) encrypted image,(c) generated share 3 (d) encrypted share 3.

Figure-5 shows histogram of the original image Baboon (a) and its cipher (b). It's clear that the histogram of original image is completely different from the histogram of the encrypted image. The histogram in Figure-5(b) is flatter than the original one. As well as Figure-6(c) is the histogram of the generated Share 3 that is less flat than the encrypted one.

5.3 Information entropy

Information entropy is another qualitatively measure which is used to measuring the pixel value distribution of the image. Let x be the information source and the equation for computing the information entropy as follows:

$$H = -\sum p(x)\log p(x)$$

P(x) represents the probability of pixel value, assuming that instance of the pixel value as the information source and exists with the same probability. In (4) the ideal information entropy can reach 8 that means the proposed system is random in order to prevent revealing the cover image. The information entropy of the encryption must be close to 8 to prove it is a good encryption system. The information entropy is applied on many samples of images; and all the results of the proposed system are equal to 7.99.

5.4 Data loss, attacks and the effect of cropping

In order to verify whether the proposed method is efficient or not through applying a kind of image attacks like cropping attack [9], [10] that has been applied on image Baboon of size 124x124. The percentage of cropped data is 24% of the original image as shown in Figure-7(a), (b). The recovered image maintains most of the data in spite of the existence of some spots in the decrypted image. Due to this fact, the proposed method provides better performance in resistance of data loss and cropping effect. The cropping attack also has been applied on Share 3 to see its effect on the recovered image as shown in Figure-7 (c),(d).

(a) (b)

Figure-7. Data loss and cropping effect on encrypted image: (a) encrypted image, (b) decrypted image of (a).

(c) (d)

Figure-7. Data loss and cropping effect on encrypted Share 3: (c) encrypted share 3, (d) decrypted image.

6. CONCLUSIONS

This paper proposed image encryption scheme based on chaos diffusion and a share masking structure. The Arnold Cat Map is employed to shuffle pixels positions. The Visual Cryptography structure is employed to cover the secret image of the shuffled positions. This cover then is encrypted by using again Arnold Cat Map. Experiments and quantitative analysis show that the proposed method has good results in security, storage space, and computational time.

REFERENCES

[1] Priya Deshmukh. 2016. An image encryption and decryption using AES algorithm. International Journal of Scientific & Engineering Research. 7(2).

[2] Min Li, Ting Liang, Yu-jie He. 2013. Arnold Transform Based Image Scrambling Method. 3rdInternational Conference on Multimedia Technology (ICMT 2013).

[3] Jagdeep Verma, Dr. Vineeta Khemchandani. 2012. A Visual Cryptographic Technique to Secure Image Shares. International Journal of Engineering Research and Applications (IJERA). 2(1): 1121-1125.

[4] R. F. Churchhouse. 2004. Codes and ciphers. Cambridge university press.

[5] Paolo D'Arco, Roberto De Prisco. 2016. Visual Cryptography Models, Issues, Applications and New Directions. Springer International Publishing AG, 9th International Conference, SECITC.

[6] Shankar K, Eswaran P. 2015. Sharing a Secret Image with Encapsulated Shares in Visual Cryptography. Elsevier, 4th International Conference on Eco-friendly Computing and Communication Systems, ICECCS. 70: 462-468.

[7] Chong Fu, Ou Bian, Hui-yan Jiang, Li-hui Ge, Hong-feng Ma. 2016. A Chaos-based Image Cipher Using a Hash Function. IEEE/ACIS 15th International Conference on Computer and Information Science (ICIS).

[8] Mohit Rajput. 2016. Secure (n, n + 1)-Multi Secret Image Sharing Scheme Using Additive Modulo. Elsevier Procedia Computer Science. 89: 677-683.

[9] Liu Rui. 2015. New Algorithm for Color Image Encryption Using Improved 1D Logistic Chaotic Map. The Open Cybernetics & Systemics Journal. 9: 210-216.

[10] Nallagarla. Ramamurthy and Dr. S. Varadarajan. 2012. Effect of Various Attacks on Watermarked Images. (IJCSIT) International Journal of Computer Science and Information Technologies. 3(2): 3582-3587.

[11] Xing-Yuan Wanga, Ying-Qian Zhanga, Xue-Mei Baoa. 2015. A novel chaotic image encryption scheme using DNA sequence operations. www.elsevier.com/locate/optlaseng, Elsevier, Optics and Lasers in Engineering. 73: 53-61.

[12] Reza Moradi Rad, Abdolrahman Attar, and Reza Ebrahimi Atani. 2013. A New Fast and Simple Image Encryption Algorithm Using Scan Patterns and XOR. International Journal of Signal Processing, Image Processing and Pattern Recognition. 6(5):275-290.

[13] Sergy P. Kunetsov. 2012. Hyperbolic Chaos, doi:10.1007/978-3-642-23666-2, Springer.