
**ISSN Print:** 2394-7500
**ISSN Online:** 2394-5869
**Impact Factor:** 5.2
IJAR 2017; 3(7): 1249-1254
www.allresearchjournal.com
Received: 25-05-2017
Accepted: 26-06-2017

**Kalyan Das**
Information Technology
St. Thomas' College of Engg and Technology, Kolkata, India

**Aromita Sen**
Computer Science & Engineering, St. Thomas' College of Engg and technology Kolkata, India

**Samir Kr. Bandhopadhyay**
Computer Science and Engineering, University of Calcutta, Kolkata, India

**Correspondence**
**Kalyan Das**
Information Technology
St. Thomas' College of Engg and Technology, Kolkata, India

# A secure multi layered image cryptosystem - A blend of chaotic theory and feedback shift register

**Kalyan Das, Aromita Sen and Samir Kr. Bandhopadhyay**

**Abstract**
Cryptography is a study of secure communication over insecure channel. It deals with hiding information in secret codes to make sure that anyone but the intended recipient can't access it. The encryption algorithm is needed to be large to provide high security and to withstand the brute force and statistical attack. The traditional methods like DES, AES are not suitable for image application due to relatively small block size, the nature of digital image, bulky data capacity and high correlation among the pixels. The proposed method uses a combination of transposition and substitution using chaotic theory and feedback register, along with a key factor to encrypt the secret data bits, before transmission, to enhance the security of the image.

**Keywords:** Encryption, decryption, image processing, visual cryptography, chaos theory, shift register

## Introduction
Today we're constantly sharing images on the internet and it is important for us to claim ownership of our content. So we have discovered two concepts visual cryptography and sampling distribution of the means. Visual cryptography is a scheme to hide a secret image using any number of shadow images called shares. When we break an image up into shares they alone don't look like anything, but when layered atop one another the secret image is revealed. This particular algorithm generates shares using these two simple patterns. If we layer the same pattern with itself we can see through half of this two-by-two region however if we layer opposite patterns with one another, light is blocked in this region. Now this is great because the shares can be printed on transparencies. Once the shares are aligned the secret image is revealed [1, 3-5].
Cryptography keeps most of our computers safe today but unfortunately computers are getting more powerful. So there's lots of research going on into new areas to send information using a wonderful lure. So encryption in cryptography is one of those critical pillars of our infrastructure today it's the guardian of your privacy and your security. We need some elegant mathematical trick, which is easy in one direction but tough in reverse, which will power the modern world [6-8].

## Related theory
The basic model of Visual Cryptography was introduced by Naor and Shamir [2] in 1994 accepts binary image I(x, y) as secret image, which is divided into 'n' number of shares. Each pixel of image I(x, y) is represented by 'm' black and white sub pixels in each of the 'n' shared images. Naor and Shamir proposed a k out of n scheme and assumed that the image or message is a collection of binary data 0 and 1displayed as black and white pixels. According to the algorithm, the secret image is divided into n shares and it reveals the secret if at least k of them shares are stacked together. So the image remains hidden for less than k shares. Decryption is achieved by stacking the shares and thus introduces noise. It is impossible to get information about the secret from individual shares. But the main disadvantage is, if someone get all the shares he/she can easily retrieve the secret message by stacking the shares. These are shown in figure 1 and figure 2.

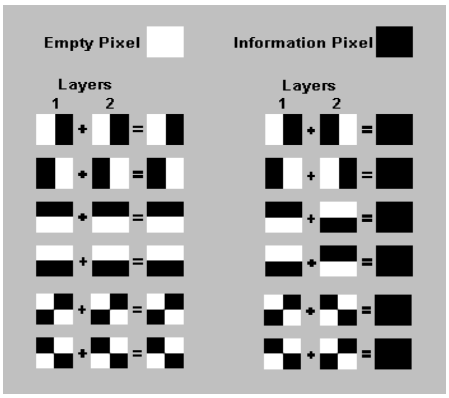
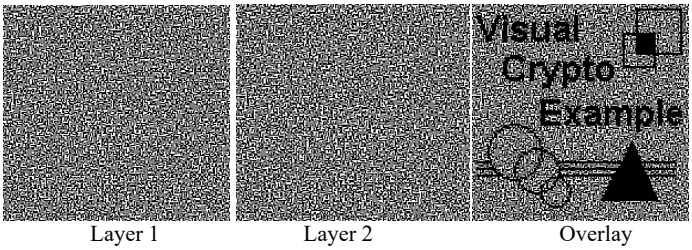



**Fig 1:** Pattern following in (2, 2) VCS during share generation




Layer 1 Layer 2 Overlay

**Fig 2:** Example of traditional (2, 2) -VCS with image size 128x128.

In the existing VCS, there lies some drawbacks due to the contrast loss in the decrypted image, storage space loss due to pixel expansion and also it reveals the existence of the secrecy due to its randomness. So here we have proposed a Encryption such that cipher doesn't reveal any secrecy and the contrast of the received image same as of the original image [9-11].

Here we have performed the encryption in two different steps, firstly the transposition using chaotic map and then LFSR to perform substitution technique.

In transposition the positions held by units of plaintext are shifted according to a regular system, so that the cipher text constitutes a permutation of the plaintext. In case of substitution, the units of plaintext are replaced with cipher text, according to a fixed system

**Chaotic Theory**

In the field of data encryption, chaotic maps are widely used for their very complicated dynamics within a simple model and desired characteristics related to requirements of cryptography. It is used to generate random numbers for some given inputs.

Arnold Cat Map (ACM) or Arnold transforms is a type of discrete system which shears and folds the images mathematically into itself in phase space, which is a typical character of chaotic map. This confusion and diffusion property of the ACM makes it more suitable for image security.

The General notation for 2D cat map used for image encryption can be given by equation (1), which has two control parameters, P and Q. A digital image can be seen as 2D matrix in which (x, y) represents the pixel position in the image. After performing the 2D Arnold scrambling it becomes x' and y', the new pixel position as in equation (2). This makes the traverse of the pixel movement completely within the size of the image (M). Here x' & y' are the locations of the pixel after mapping, x & y are the locations of the pixel before mapping.

$$A = \begin{pmatrix} 1 & P \\ Q & PQ+1 \end{pmatrix}$$

$$\begin{pmatrix} x' \\ y' \end{pmatrix} = A \begin{bmatrix} x \\ y \end{bmatrix} mod\ M$$

**Equation 1. 2D Arnold Cat Map**

The basic concept behind this is to convert the arrangement of the pixels of an image by iterating chaotic map using initial conditions. After a small number of iterations, a certain number of cycles and changing pixel positions using Arnold cat map, image becomes unpredictable. Image size, initial conditions, number of iterations, number of cycles and Arnold cat map parameters are considered to be the secret keys for encryption. Due to change of any one of this, the system produces undesired results at the receiver side. The number of the rounds in the Arnold cat map is not directly proportional to the size of the image but related.

The Arnold Cat Map is Invertible because the matrix has determinant 1 and therefore its inverse has integer entries After some operational research on Mathematical Functions, we have found that any 3*3 matrix with determinant 1, along with a modulus operator can work as a periodic function with different periodicities depending on the modulus operand and the input matrix.

According to Arnold's transformation function, when it is applied on an image, it apparently randomizes the original organization of its pixels. And if iterated enough times, eventually the original image reappears. The number of considered iterations is known as the Arnold's period. The periodicity of the functions depends on the various parameters of the image for example size of the image.

Identity Matrix=I, Periodic Matrix= M, Periodicity=p

M*M*M*M** …….p times….. *M = I

That means, suppose an input image with size m*n, can be operated using the periodic function, resulting a periodicity

value P. Therefore, key space = O (N)= O(m*n) where m and n denotes the rows and columns of the image respectively.

Now in the sender side we apply the periodic function in an iterative manner for suppose T times, where T<P, resulting a totally different Random Image.

Now in the receiver side, we need to again apply the periodic function P-T times in order to get back the original meaningful image. If we try to apply the function for different times, the output will be random, can't get the original one.

If during transmission the eavesdropper tries to intercept, there will be a change in the transmitted data, so the original image can't be retrieved back. Thus we can try to detect the presence of eve.

**Linear Feedback Shift Register**

A Linear Feedback Shift Register (LFSR) is a sequential shift register with combinational logic that makes it to pseudo-randomly cycle through a sequence of binary values. In this paper we have considered the polynomial $x_8+x_6+x_5+x_4+1$ to generate a random bit. Feedback around a shift register comes from a selection of points (D) in the register chain and constitutes XORing these taps to provide tap(s) back into the register as shown in the figure4. The 8 bit LFSR case D0,D4,D5,D6 are XORed and feeding back to MSB bit(D8) and this bit is used as a sequence bit in future. The 8-bit sequence will repeat every after 255 cycle (1 cycle= one shift) and all generated sequence are purely based on the initial 8-bit data present in the register. This is shown in figure 4.

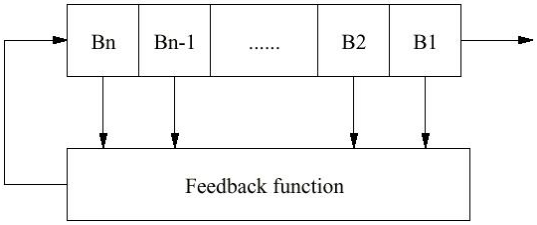



**Fig 4:** Linear Feedback Shift Register Block Diagram

**Proposed method**

**Level 1**

In the 1st level for encryption, we have used Arnold cat map where the pixels of the image are rearranged generating a random image. Here the number of iterations applied to the image (N) need to be kept secret for the time of decryption. The cat map used here has a determinant 1 which confirms it to be a reversible procedure.

**Level 2**

For more enhancements during the encryption procedure, here we are applying LFSR to map an input intensity to a corresponding output intensity which is a reversible procedure and thus providing 100% successful decryption. The method is shown in figure 5.


**Fig 5a:** Flow Chart of Encryption process


**Fig 5b:** Flow Chart of Decryption process

**Fig 5:** Flow chart representation of the Encryption & Decryption Scheme

**Implementation details**

In the proposed system, the number of pixel in the decoded image is same as in the original secret. After testing on many different images the results are as our expectation and the retrieved images are clear without any visual abnormality. This technique can work for both color images as well as gray scale images. All that is required is to transmit key on a secret channel while the cipher images can be transmitted on an insecure channel.

**Result and analysis of the proposed encryption algorithm**

This section first shows the simulated result of the proposed technique. Then the analysis of the proposed technique is done based on histogram analysis and PSNR calculation.

Here is the set of input and its corresponding output along with the statistical view and approx time complexity after applying the proposed encryption algorithm. Here N denotes the loop values and [row col] denotes the input image size. The analysis of results are given in Table 1, Table 2, Figure 6 and figure 7.

**Table 1:** Approx Time complexity of the Proposed Encryption Scheme

| Original Image | Arnold Cat Map | LFSR | Reverse LFSR | Reverse Arnold Cat Map |
|---|---|---|---|---|
| Time Complexity | O(N*row*col*2) | O(row*col*2) | O(row*col*2) | O(N*row*col*2) |

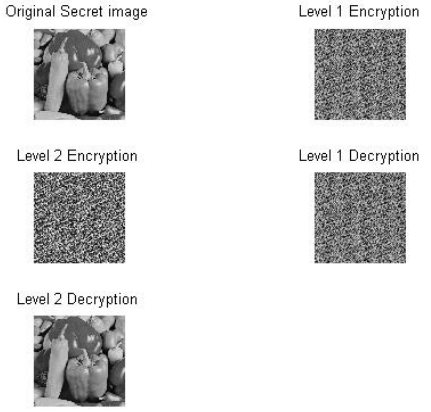



**Fig 6a:** Encryption on Gray Image1

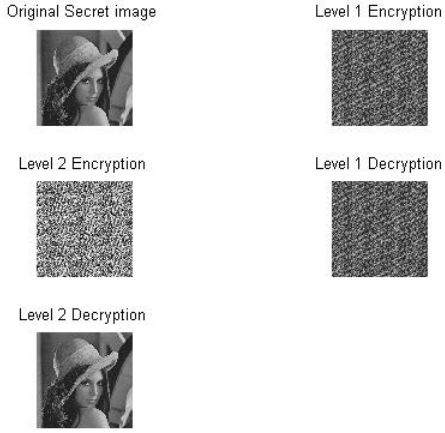



**Fig6b.** Encryption on Gray Image2
**Fig6.** Resultant Output of the Proposed Encryption Scheme over Grayscale Image

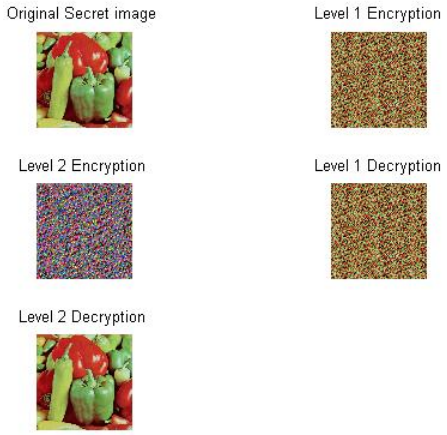



**Fig 7a:** Encryption on Color Image1

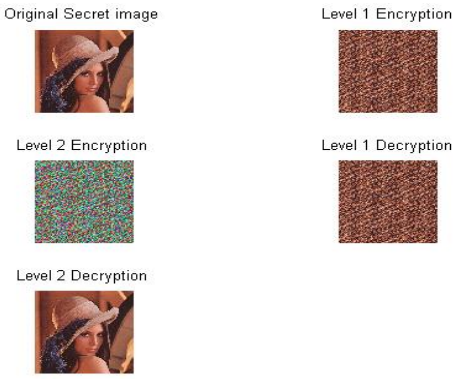



**Fig 7b:** Encryption on Color Image2
**Fig 7:** Resultant Output of the Proposed Encryption Scheme over Color Image

**Table 2:** Test data set for proposed encryption scheme

| Original Image | | | Level 1 Encryption | | | Level 2 Encryption | | | Level 1 Decryption | | | Level 2 Decryption | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 1 | 29 | 8 | 1 | 160 | 189 | 2 | 65 | 123 | 1 | 160 | 189 | 1 | 29 | 8 |
| 23 | 110 | 103 | 165 | 146 | 152 | 74 | 36 | 48 | 165 | 146 | 152 | 23 | 110 | 103 |
| 2 | 108 | 117 | 31 | 100 | 67 | 63 | 201 | 165 | 31 | 100 | 67 | 2 | 108 | 117 |

## Quality Measurement

For performance calculation we have used the PSNR index, to measure the quality between two images. In PSNR quality measurement one of the images are compared provided the other image is regarded as of perfect quality. The formulae used are given below:

$$\mathrm{MSE} = \frac{1}{\mathrm{N} * \mathrm{M}} \sum_{\mathrm{i}=0}^{\mathrm{N}-1} \sum_{\mathrm{j}=0}^{\mathrm{M}-1} [\mathrm{X}(\mathrm{i},\mathrm{j}) - \mathrm{Y}(\mathrm{i},\mathrm{j})]^2$$

$$\mathrm{PSNR} = \log_{10}\left(\frac{\mathrm{Imax}^2}{\mathrm{MSE}}\right)$$

**Equation 2:** Formula of MSE and PSNR

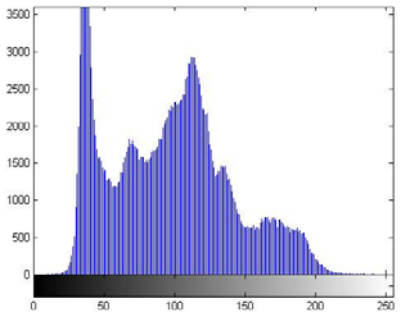
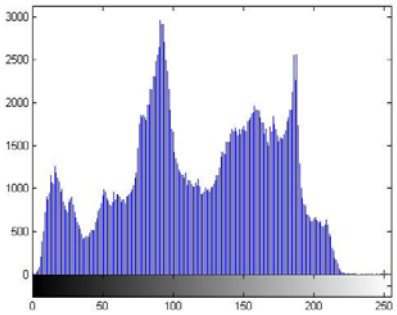
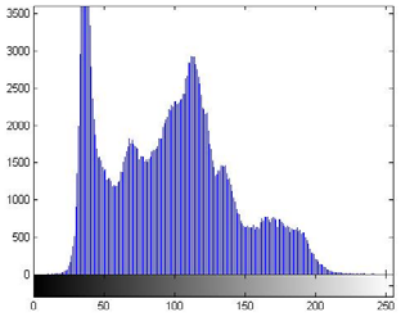
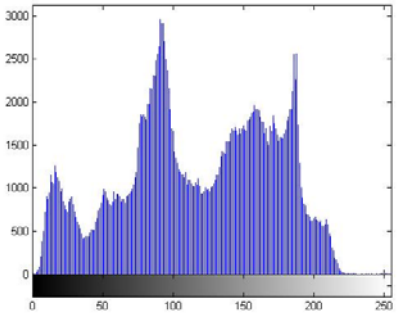
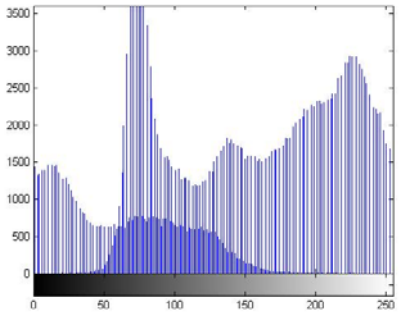
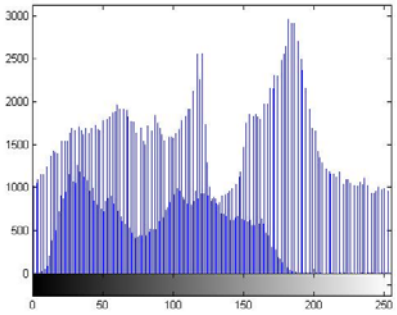
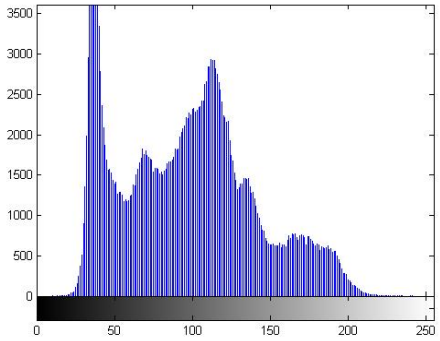
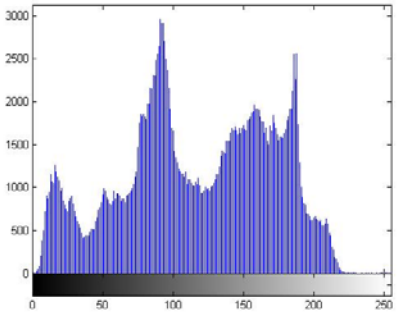
[X is the original image and Y is the output image; I is the dynamic range of pixel values normally 255; (M, N) are the dimensions of the image]

The quality measures are calculated between the original image and the encrypted/decrypted image. Table3 shows the quality measures of the images after encryption / decryption process. Table 4 shows Histogram of the Encrypted Images and comparison with the Original Image.

**Table 3:** Experimental results for proposed encryption scheme

| Original Image | PSNR index for Color Secret | | PSNR index for Grayscale Secret | |
|---|---|---|---|---|
| | Color Image 1 (lena.bmp) | Color Image2 (peppers.jpg) | Gray Image 1 (lena.pgm) | Gray Image 2 (peppers.pgm) |
| Level 1 Encryption | 12.0207 | 10.2196 | 12.2789 | 10.5794 |
| Level 2 Encryption | 9.6405 | 9.0097 | 8.8473 | 9.5234 |
| Decrypted Image | INF | INF | INF | INF |

**Table 4:** Histogram of the Encrypted Images and comparison with the Original Image

| | Image Set 1 | Image Set 2 |
|---|---|---|
| Original Image Histogram |  |  |
| Encryption Level 1 |  |  |
| Encryption Level 2 |  |  |
| Decrypted Image Histogram |  |  |

## Conclusion & future work

In the proposed algorithm the original secret image can be retrieved in totality and thereby it's a lossless encryption procedure. There is no pixel expansion and hence storage requirement is same as original image. The same technique can also be used on binary or grayscale images, without any change in the algorithm. Here the proposed method is a symmetric encryption procedure and the key space is dependent on various image parameters, so variable in nature. Our future work will be to improve the security of retrieval of the encoded message.

## References


1. A Secure Keyless Colored Image Encryption', Amit B. Chougule, Nilam Nisar Shaikh, International Journal of Advanced Technology in Engineering and Science, 2014.
2. Naor, Shamir A. Visual cryptography, Advances in Cryptology EUROCRYPT 94, M Lecture Notes in Computer Science, 1995.
3. RKO Technique for Color Visual Cryptography, Ms. Moushmee Kuri, Dr. Tanuja Sarode, IOSR Journal of Computer Engineering, 2014.

4. Survey of Visual Cryptography Schemes, P.S. Revenkar, Anisa Anjum, W.Z. Gandhare. International Journal of Security and Its Applications. 2010.
5. A Three Way Visual Cryptography & its Application in biometric Security: A Review, Mr. Praveen Chouksey, Mr. Reetesh. Rai. International Journal for Research in Applied Science and Engineering Technology. 2015.
6. Survey of Visual Cryptography Schemes, P.S. Revenkar, Anisa Anjum, W.Z.Gandhare. International Journal of Security and Its Applications. 2010.
7. A New Visual Cryptography Scheme for Color Images, B. SaiChandana, S. Anuradha. International Journal of Engineering Science and Technology. 2010.
8. Visual Cryptography Scheme for Color Image Using Random Numberwith Enveloping by Digital Watermarking, Shyamalendu Kandar, Arnab Maiti, Bibhas Chandra Dhara. International Journal of Computer Science. 2011.
9. Secret Sharing Using Visual Cryptography, Renu Poriye, Dr S. S Tyagi. International Journal of Research Studies in Computer Science and Engineering. 2014.
10. Moni Naor and Adi Shamir, Visual Cryptography, advances in cryptology– Eurocrypt, 1995.
11. New Visual Cryptography Algorithm for Colored Image, Sozan Abdulla. Journal of computing. 2010.