Secret Image Sharing Using Pseudo-Random Sequence

Anil Kumar,[†] *and Navin Rajpal*[††]*,*

Guru Gobind Singh Indraprastha University, Kashmere Gate,Delhi, INDIA

Summary

We propose a new concept which is derived from the cryptography, the substitution of bits in the image and the visual cryptography method. Given some secret data and a set of cover images, in the proposed scheme the secret data is encrypted by the administrator, after that we select the random bit planes of the cover images using the pseudo-random sequence and modify the cover image based on these random bit planes. In our method each participant has a unique modified cover image called stego-image. Therefore these participants are required to reconstruct the encrypted secret data without destroying of its secrecy. After that administrator decrypt the original data. Experiments show the good quality of the stego-image. The proposed scheme also prevents anyone if steal all the shares will not gaining information about the secret data.

Key words:

Steganography, Cryptography, Secret sharing, and Pseudo – Random Sequence

Introduction

In the present era of computers and fast communication, one needs to protect communicated information (message or plain text) from unauthorized user, while sending it through any electronic media. The private-key and the public-key are the two well-known cryptosystems [1, 2, 3, 4, 5, 6, and 7] using these we enable to keep the secret data securely in such a way that that invader cannot able to understand what the secret data means. The data encryption standard (DES) [6, 7] and Rivest, Shamir, Adleman (RSA) and Advanced Encryption Standard (AES) [1, 2, 3, 4, and 5] are three representative methods.

Apart from cryptography, steganography provides another way to keep the data secure. The Steganography [8, 9, 10, 11, 12, 13, 14, 15, and 16] consists of techniques to allow the communication between two persons. It hides not only the contents but also the existence of the communication in the eyes of any observer. These techniques use a second perceptible message, with meaning disjoined by the secret message. This second message works as a "Trojan horse", and is a container of the first one. The new technologies and, in special way, the information networks require more and more sophisticated strategies in order to prevent the message privacy. In this context, digital images and audio is excellent candidate to turn into containers of the messages, since the bits of a secret text message can be superimposed, as slight noise, to the bits employed for coding a digital image.

There are two methods of performing steganography, one in spatial domain, and the other in frequency domain. Each technique has its own advantage and disadvantage. In the spatial domain [11, 12], we can simply insert data into host image by changing the gray levels of some pixels in the host image, but the inserted information may be easily detected using computer analysis. In the frequency domain [13, 14], we can insert data into the coefficients of a transformed image, for example using discrete Fourier transform (DFT), discrete cosine transform (DCT) and discrete Wavelet transform (DWT). But we cannot embed too much data in the frequency domain because the quality of the host image will be distorted significantly.

The mechanism is desirable in which the secret depends not on one person but on a group of people which is known as the secret sharing [17, 18, 19, 10, and 21]. The real life application of this scheme is when it's necessary in a company that the managers to share the digital documents. This concept gives a good solution for data security because all members are required to break the secret and this the main advantage of the secret sharing.

In 1994, Naor and Shamir [17] described a new (k, n) visual cryptographic scheme using black and white images, where the dealer encodes a secret into n participants. The secret is visible only if k or more participants stack in their shares together. The concept of arcs to construct colored visual cryptography scheme has been proposed by Verheul and Van Tilborg [18] where colored secret images could be shared. The number of colors and number of sub pixels determined the resolution of the revealed image and thus if the number of colors was large, then coloring the sub pixels and stacking the shares precisely becomes a difficult task. In [19], a new visual cryptographic scheme to improve the visual effect of the shares was proposed by Hwang. This scheme was useful when the number of

Manuscript received February 25, 2006.
Manuscript revised February 28, 2006.

shares was large and could be implemented only for black and white images. Subsequently Chang, Tsai and Chen [20] modified and extended this scheme to color images using Color Index Tables. In [21], Chang proposed a scheme wherein the size of the shares is fixed and independent of the number of colors appearing in the secret image. Further, the pixel expansion was only 9, which was the least amongst the previously proposed methods. But this algorithm is only applicable for (n, n) schemes. In paper [22] chang gives the concept of the sharing of multiple secrets in the digital image.

In our paper we introduce the concept of the administrator who is the central authority of the process. The administrator makes our process more secure. The administrator encrypts the secret data using the AES method which is one of the most secure encryption techniques.

Each participant has the digital grayscale image X_i. The participant required this image to share the secret encrypted message with the other participants. We have two participants to share the secret encrypted data. We select the two random bit planes using the pseudo-random sequence from two cover images of the two participants, respectively and modify one of the bit planes for achieving our goal.

This Paper is organized as follows. In Section 2, we give brief of the Advanced Encryption Standard [AES] which is used by the administrator .In Section 3, we introduce the pseudo-random sequence and in Section 4, we introduce secret-sharing using pseudo-random sequence. The Experimental Results& Security Analysis and Conclusion are shown in Section 5 and 6.

2. Advanced Encryption Standard (AES)

This is used to encrypt the secret data by the administrator. We fix the block size and key size to 128 bit. We consider the 10 round versions. We use the following notations.

Let for all round index $i = 0,...,10$ and byte index: $j = 0,...,15$

$X_j^i : jth$ text byte of i-th round (in particular), X_j^0 is the initial input plain text byte and is fixed

$X_j^{11} : jth$ cipher text byte.

$K_j^i : jth$ expanded key byte of i-th round (in particular) K_j^0 is the user defined key :

$K_j^0 :< k_0, k_1, k_2, ..., k_{15} >$

$MK_j^i : jth$ Modified inverse expanded key byte of i-th round

W[i] = i-th key word of 32 bits.

k_n: nth key byte, $n = \{0,1,2,....,175\}$

$N_k =$ (Key size)/32 = 128/32 = 4.

$N_b =$ (Block size)/32 = 128/32 = 4.

N_r No. of cipher rounds = 10.

We use the standard convention of representing elements of F_{2^8} as polynomials of degree 7, over F_2. We also adopt the standard practice of treating the elements of F_{2^8} as integers in the range 0, … ,255. Thus for example, $\alpha \in F_{2^8}$ with $\alpha = x^7 + x^6 + x^2 + x + 1$ would be referred as $\alpha = 199$, without ambiguity.

We define three functions namely Rotbyte(.), Rc(.), and Rcon(.) .

(i) Rotbyte(.) rotates the bytes of key within the word, when word oriented structure is considered for key expansion mechanism. If k_0, k_1, k_2, k_3 are four bytes of i-th key-word $W[i]$ arranged in big endian format, $Rotbyte(W[k_0, k_1, k_2, k_3]) = W[k_1, k_2, k_3, k_0]$ The byte substitution transformation of Rijndael uses an S-box, generated over F_{2^8} with $(x+1) \equiv (03_{base16})$ as primitive element and $g(x) = (x^8 + x^4 + x^3 + x + 1)$ as the defining irreducible polynomial along with an affine transformation of $(x^6 + x^5 + x + 1) \equiv (63_{base16})$. Thus, bs, using S-box, transforms the individual byte a(x) to bs(a(x)).

Mathematically,

$$bs(a(x)) = \begin{array}{c}(x^6 + x^5 + x + 1) \\ + c(x)(x^4 + x^3 + x^2 + x + 1)(\mathrm{mod}(x^8 + 1))\end{array}$$

where $c(x) = a(x)^{-1}(\mathrm{mod}\, g(x))$

(ii) Rc(a(x)) is another round dependent byte oriented constant function defined over F28. POW(a(x)) contains powers of a(x) in the field. Then

$$Rc(a(x)) = POW(a(x))(\mathrm{mod}\, g(x))$$

In particular, for $a(x) \in \{1,2,....10\}$
$Rc(a(x)) = \{1,2,4,8,16,32,64,128,27,54\}$

(iii) Rcon(a(x)) is a round dependent word oriented function such that $Rcon(a(x)) = (Rc(a(x)),0,0,0)$. Here the commas define separation of each byte arranged in big endian format.

2.1. Brief description of Rijndael internals

Rijndael has an elegant algebraic structure over F_{2^8}. The input plain text or the output cipher text of block size of 128-bits is viewed as a 4x4 matrix of 16 bytes arranged in a column major format. Rijndael consists of an initial round of key addition (ak) followed by 10 iterations of round transformations for the key size of 128-bits. Each (except the last) round transformation function is composed of the four sub transformation functions: Byte Substitution or bs, Row Shift or rs, Mix Column or mc and Add Round Key or ak. The last round transformation does not include the mc function.

2.1.1 Byte Substitution transformation: bs

This is the only non-linear transformation in the entire Rijndael structure. It operates independently on each byte using a substitution table (S-box). The S-box, which is invertible in nature, is composed of two transformations:

Taking multiplicative inverse of the desired byte in the finite field GF (28) with $(x+1) \equiv (03_{base16})$ as primitive element and $g(x) = (x^8 + x^4 + x^3 + x + 1)$ as the defining irreducible polynomial. The element 00_{base16} is mapped to itself.

Applying an affine transformation of $(x^6 + x^5 + x + 1)$ equivalently 63_{base16}.

Thus, the byte substitution operation transforms a byte a(x) to bs(a(x)) as per the following relation. Let

1. $c(x) = a(x)^{-1} (\bmod g(x))$

2.
$$bs(a(x)) = \begin{array}{c} (x^6 + x^5 + x + 1) \\ + c(x)(x^4 + x^3 + x^2 + x + 1)(\bmod(x^8 + 1)) \end{array}$$

The inverse S-box is constructed by taking an inverse affine transform followed by a multiplicative inverse in the finite field F_{2^8}.

1.
$$\begin{array}{c} c(x) = (x^2 + 1) + \\ bs(a(x))(x^6 + x^3 + x)(\bmod(x^8 + 1)) \end{array}$$

2. $a(x) = c(x)^{-1} (\bmod g(x))$

2.1.2 Row Shift transformation: rs

The 16 input bytes are arranged in a column major format of a 4x4 matrix. To achieve the desired confusion, a linear transformation rs is applied. Here, the bytes in each row of the matrix are given a cyclic left shift. For i = 1, 2, 3, 4 the bytes in the i-th row are circularly left shifted by (i-1) bytes.

The inverse of a row shift transformation is obtained by cyclically shifting the bytes in the reverse direction i.e. circularly right shifting 0, 1, 2, and 3 bytes in the first, second, third and fourth row of the 4x4 input matrix respectively.

2.1.3 Mix Column: mc

The linear transformation mix column provides the diffusion by mixing the bits of each column. The function β(z), given below, operates on the input column by treating it as a degree three polynomial in $F_{2^8}[z]$. This polynomial is multiplied by a rotated version of a standard polynomial $m(z) \in F_{2^8}[z]$ given by

$$[m(z)] \;= 03z^3 + 01z^2 + 01z^1 + 02$$

and reduced modulo the polynomial $(z^4 + 1) \in F_{2^8}[z]$. Here the coefficients denote elements of F_{2^8}. It is known that the coefficients of m(z) are so chosen that the result β(z).m(z) is invertible modulo (z^4 + 1) although this polynomial is reducible over F_2.

For example, a column of mc, [a0, a1, a2, a3]T is considered as

$$\beta(z) = a_3 z^3 + a_2 z^2 + a_1 z \;\; + a_0 \in F_{2^8}[z]$$

Then,

$$\begin{aligned} m(z)\cdot\beta(z) = & (03\cdot a_3)z^6 + (03\cdot a_2 + 01\cdot a_3)z^5 \\ & + (03\cdot a_1 + 01\cdot a_3 + 01\cdot a_2)z^4 \\ & + (03\cdot a_0 + 02\cdot a_3 + 01\cdot a_2 + 01\cdot a_1)z^3 \\ & + (01\cdot a_0 + 02\cdot a_2 + 01\cdot a_1)z^2 \\ & + (01\cdot a_0 + 02\cdot a_1)z \ + (02\cdot a_0)z^0 \\ & (\mathrm{mod}(z^4+1)) \end{aligned}$$

$$m(z).\beta(z) = \begin{bmatrix} 02 & 03 & 01 & 01 \\ 01 & 02 & 03 & 01 \\ 01 & 01 & 02 & 03 \\ 03 & 01 & 01 & 02 \end{bmatrix} \begin{bmatrix} a_0 \\ a_1 \\ a_2 \\ a_3 \end{bmatrix}$$

The inverse of Mix column transformation is similar to the forward operation with the only difference that the inverse of the fixed polynomial i.e. [m(z)]-1 is used and it is given by $[m(z)]^{-1} = 11z^3 + 13z^2 + 09z + 14$

Hence, $$[m(z)]^{-1}.\beta(z) = \begin{bmatrix} 14 & 11 & 13 & 09 \\ 09 & 14 & 11 & 13 \\ 13 & 09 & 14 & 11 \\ 11 & 13 & 09 & 14 \end{bmatrix} \begin{bmatrix} a_0 \\ a_1 \\ a_2 \\ a_3 \end{bmatrix}$$

2.1.4 Add Round Key: ak

In this function, the round key is added to the current byte as bit-wise exclusive OR. The XOR operation is the inverse of itself.

3. Pseudo Random Sequence

A Non-Linear forward feedback shift Register (NLFFSR) is a mechanism for generating Pseudo random binary sequences [23, 24, 25, 26, and 27]. Figure 1 shows a general model of an 4-bit NLFFSR. It is a Non-linear forward feedback shift register with a feedback function f

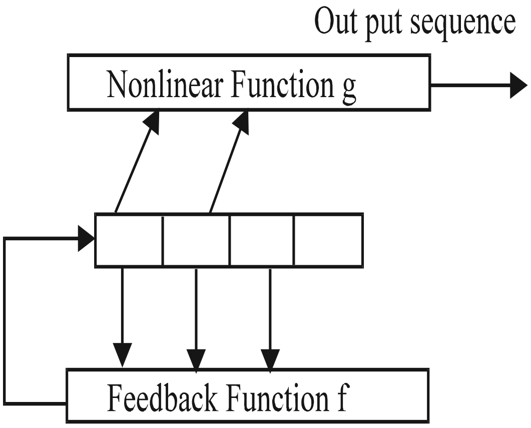


Figure-1: A General model of 4-bit NLFFSR

NLFFSR are extremely good pseudorandom binary sequence generators. When this register is loaded with any given initial value (except 0 which will generate a pseudorandom binary sequence of all 0s) it generates pseudorandom binary sequence, which has very good randomness and statistical properties. The only signal necessary for the generation of the binary sequence is a clock pulse. With each clock pulse a bit of the binary sequence is produced.

A model of 4-bit NLFFSR is considered to demonstrate the functioning of NLFFSR with the feedback function $f = 1 + x + x^4$ and the non-linear function g defined by $a_{n-1}.a_{n-3} \oplus a_{n-2}.a_{n-4}$ forming non-linear feed forward shift register generator. Its initial bit values are used (1111).

The output sequence $Z_n : 011111000000001$ Generated by NLFFSR in is periodic of period 15, which is the same as the period of the sequence generated by NLFFSR of 4 bits.

Period of the sequence generated by NLFFSR is the maximum if we use the primitive polynomial. To design any stream cipher system, one needs to consider the NLFFSR with primitive feedback polynomials as the basic building blocks. Period of the enciphering sequence can be increased if it is generated by following methods:

(1) Addition of maximal length sequences.
(2) Multiplication of maximal length sequences.
(3) Using multi logic generalized Non-linear feedback shift register.

The usefulness of these sequences depends in large part on there having nearly randomness properties. Therefore such sequences are termed as pseudorandom binary sequences. The balance, run and correlation properties of these sequences make them more useful in the selection of secret keys. The NLFFSR generated sequences are of great importance in many fields of engineering and sciences.

4. Secret Image Sharing using Pseudo-Random Sequence

Suppose the dealer wants two participants P_1 and P_2 to share the secret original data T and first we encrypt the secret data as E which is encrypted by the administrator. Then we will share this encrypted data E. We are taking the digital grayscale image in which each pixel of 8-bits or 1-byte, representing the gray levels from black to white. The encrypted text to be hidden is E and two image X$_1$ and X$_2$ in which we will share the encrypted data. We will take two pseudo-random sequences which is generated by the NLFFSR. Let the sequences generated are S_1 and S_2. Let the sequence generated as follows

$$S_1 = \{2, \quad 4, \quad 1, \quad 2, \quad 3, \quad 2, \quad 1\}$$
$$S_2 = \{3, \quad 1, \quad 2, \quad 4, \quad 3, \quad 2, \quad 1\}$$

We will take the collection of the bits from the image X$_1$ by the sequence S_1 i.e. the 2nd LSB of the first pixel, the 4th LSB from the second pixel, 1st LSB from the third pixel , the 2nd LSB from fourth pixel and ……… and the collection of the bits from the image X$_1$ is consider as C_1 array.

1st Pixel	11001000
2nd Pixel	11101000
3rd Pixel	11101011
4th Pixel	11001000

These are the pixel of the image X$_1$ selection based on the pseudo-random sequence S_1 and the content of the array $C_1 = \{0, \quad 1, \quad 1, \quad 0, \quad . \quad .\}$ and we will combine 8-bit as one byte.

4.1 The secret sharing procedure proposed scheme

We are having the encrypted text E given by the administrator and the array C_1 which we have derived from the cover image X$_1$ and the permutation functions perm$_e$, perm$_1$ and perm$_2$ and the other cover image X$_2$.

Step 1: a) Let the length of the encrypted text E is ‘l’.
for i=0 to l

$$E^1[i] = E[perm_e[i]]$$

Where E^1 is the permutated encrypted data

Step 2: If l < min(sizeof(X$_1$), sizeof(X$_2$)) then: proceed
Else: The cover images are not suitable and different images to be selected.

Step 3: for $i = 0$ to l

$$C_2[perm_2(i)] = C_1[perm_1(i)] \oplus E^1[i]$$

Step 4: The C_2 array value have to be hide in the image X$_2$ using the sequence S_2 . E.g. let the array $C_2 = [0, \quad 1, \quad 0, \quad 0, ...]$ in the bits-form and the sequence $S_2 = \{3, \quad 1, \quad 2, \quad 4, \quad 3, \quad 2, \quad 1\}$.

Let the cover image X$_2$ having the pixel value in bit-form before hiding the data

1st Pixel	00100111
2nd Pixel	00100111
3rd Pixel	11001000
4th Pixel	00100111

After hiding secret share in the image X$_2$ using the sequence S_2 and array C_2 in bit-form

1st Pixel	00100011
2nd Pixel	00100111
3rd Pixel	11001000
4th Pixel	00100111

In this way we are hiding the data in the 2nd image using pseudo-random sequence.

Step 5: Secret sharing is complete. Exit .

4.2 The secret recovery procedure of the proposed scheme

Now the two participants P_1 and P_2 want to recover the data and the cover image are X$_1$ and X$_2$ respectively, and the pseudo-random sequence are the S_1 and S_2 respectively and the array generated by these sequence are C_1 and C_2 respectively.

Step 1: For i=0 to l ,

$$E^1[i] = C_1[perm_1(i)] \oplus C_2[perm_2(i)]$$

Step 2: For i=0 to l ,

$$E[i] = E^1[inv(perm_e(i)]$$

Step 3: Administrator decrypt the data.

Step 4: Exit

5. Experimental Results and Security Analysis

We will discuss the experiments along with the security analysis.

5.1 Experiments Results

In the experiments, we have taken the two participants P_1 and P_2 sharing the encrypted secret data and we are having two image X_1 and X_2 as shown in the figure 2.

The secret data can be extracted from the cover-images are in the lossless form. Overall advantage of the technique is that it is effective because the quality of the stego-image visually acceptable because we are hiding the data in pseudo-random method with-in first four planes only; the stego-images will be very close to the original image if we hide the data within first four planes. Finally, we are not hiding data in one plane only and it leaves no area of doubt for simple operation.

5.2 Security Analysis

We will analyze the effectiveness of the scheme, which is proposed by us. We produce the stego-images which are owned by the participants. It is very tough for the attackers to get the stego-images from the participations. It is very difficult to know in which image is contain the hidden information.

Suppose the attackers some how able to get the two stego-images X_1 and X_2 from participants P_1 and P_2 respectively. Even if the attackers know everything about the proposed schemes. The attackers problem is to find first about the two pseudo-random sequences S_1 and S_2 some how if he is able to know about the two pseudo-random sequences. After the attackers cannot able obtain the permutation functions $perm_1(i)$ and the $perm_2(i)$ for every i without this knowledge of this function he cannot able to obtain the E^1 . Some how he recover the E^1 but without the knowledge of the $perm_e(i)$ for every i. He is not able to recover the E . Even if some how he recover the E . But the data is encrypted by the Advanced Encryption Standard (AES) with 128-bits.

Consider the brute force attack only the AES code breaking require the 2^{128} guess to break the AES code. And to guess the E^1 or $C_2[perm_2(i)]$ or $C_1[perm_1(i)]$ require the 2^l possible case and same for the E . This satisfies the requirement of the practical security [28] as suggested by Shannon. Therefore we can say this proposed scheme is secure under this case.

6. Conclusion

The main purpose of our proposed scheme is to make a full-proof method. We provide the concept of the administrator in the secret sharing as well the encryption of the original data. And we are also using the concept of the pseudo-random sequence to make our proposed scheme our secure from any attack. Our method is much better than the Visual Cryptography because the cover images do not have to be expanded and this prevents the disorderliness and the spots of the shadows on the images. And it is very tough to break this proposed scheme even by any computer of this age.

References

[1] B.Gladman, “Implementation experience with the AES candidate algorithms,” Proc. of 2nd AES candidate conference, March 22-23, 1999, Rome, pp.7-14. (http://fp.gladman.plus.com/cryptography_technology/rijndael)

[2] Courtois, N.T. and J. Pieprzyk, “Cryptanalysis of Block Ciphers with Overdefined Systems of Equations,” Asiacrypt 2002, LNCS 2501,Springer-Verlag, pp 267-287. (http://eprint.iacr.org/2002/044/)

[3] J.Daemen and V.Rijmen, “The block cipher Rijndael,” available from NIST's AES homepage, (http://www.nist.gov/aes)

[4] J.Daemen and V.Rijmen. AES proposal: Rijndael. In AES Round 1 Technical Evaluation, NIST 1998. (http://www.nist.gov/aes)

[5] J.Daemen and V.Rijmen. "The Design of Rijndael," AES - Advanced Encryption Standard}, ISBN 3-540-42580-2 Springer-Verlag Berlin Heidelberg, New York.

[6] "Data Encryption Standard (DES)," National Bureau Standards FIPS Publication 46(1977).

[7] R. L. Rivest, A. Shamir, and L. Adleman, "A method for obtaining digital signatures and public key cryptosystems," Commun. Assoc. Comput. Mach. 21,120-126(1978).

[8] W. Bender, D. Gruhl, N. Morimoto, A.Lu, "Techniques for data hiding. IBM systems Journal, Vol. 35, no. 3-4, 1996. p313-336

[9] N.F. Johnson and S. Jajodia, "Exploring Steganography: Seeing the Unseen," IEEE computer, Vol. 31, No. 2, February 1998,pp. 26-34.

[10] R. J. Anderson and F.A.P. petitcolas, "On the Limits of steganography," IEEE Journal on Selected Areas in Communications, vol. 16,No.4, May 1998

[11] N. Nikolaidis,I. Pitas:,"Robust image watermarking in the spatial domain," Signal Process,66 (3) (1998),385-403.

[12] O. Bruyndonckx, J. J. Quisquater, B. Macq, "Spatial method for copyright labeling of digital images," Proceeding of IEEE Workshop on Nonlinear Signal and Image Processing, Neos Marmaras, Greece, 20-22 June 1995, pp. 456-4 59.

[13] Jiwu Huang, Yun Q. Shi, Yi Shi ," Embedding image watermarks in DC components," IEEE Trans. CSVT 10 (6) (2000) 974-979.

[14] Shinfeng D. Lin, Chin-Feng Chen," A robust DCT-based watermarking for copyright protection," IEEE Trans. Consumer Electron. 46 (3) (2000) 415-421.

[15] N. F. Johnson and S. Jajodia, "Steganalysis: The Investigation of Hidden Information," Proceedings of IEEE Information Technology Conference, 1998

[16] Y. K. Lee and L. H. Chen, "High Capacity Image Steganographic Model," IEE Proceedings – Vision, Image, and signal processing, vol.147, No. 3, June 2000, pp. 288-294.

[17] M. Naour and A. Shamir.," Visual cryptography," Advances in Cryptology- EUROCRYPT '94, Lecture Notes in Computer Science,(950):1-12,1995.

[18] E. Verheul and H. V. Tilborg, ,"Constructions and properties of k out of n visual secret sharing schemes,". Designs, codes and cryptography, 11(2):179-196,1997.

[19] R. Hwang and C. Chang," Some secret sharing schemes and their applications," PhD dissertation of the Department of Computer Science and Information Engineering, National Chung Cheng University, Chiayi, Taiwan,1998.

[20] C. Chang, C. Tsai, and T. Chen.," A new scheme for sharing secret color images in computer network," Proceedings of International conference on Parallele and Distributed Systems, Pp21-27, July2000.

[21] Chen-chen Chang ," Sharing a Secret Gray Image in Multiple Images," National Chung Cheng University, Taiwan ,2002

[22] Chwei-Shyong Tsai, Chin-Chen Chang and Tung-Shou Chen ," Sharing multiple secrets in digital images" The Journal of Systems and Software , pp 163-170, 64(2002)

[23] N. Rajpal, A. Kumar, S. Dudhani and P. R. Jindal, "Copyright Protection Using Non Linear Forward feedback Shift Register and Error correction technique," 7th Annual International conference Map India 2004, pp. , New Delhi, India, January 2004.

[24] N. Rajpal, Anil kumar ,"Stegnaography using No-Linear Forward Feedback Shift Register Technique ", IWAIT'2004 in National University of Singapore , Singapore 12-13th Jan 2004, pp117-122.

[25] N. Rajpal, A. Kumar and P. R. Jindal, "Demonstrating the Use of Error Coding Technique in the field of Steganography, along with Linear Feedback shift Register Technique," 2nd Workshop on Computer Vision, Graphics and Image Processing, pp. 22-27, Gwalior, India, February 2004.

[26] N. Rajpal, A. Kumar, P. R. Jindal and A. Saroagi, "An Investigation into the use of Linear Feedback Shift Register for Data Encrypting and Data Hiding in the field of Steganography," Conference on e-security, Cyber Crime & Law, pp., Chandigarh, India, February 2004.

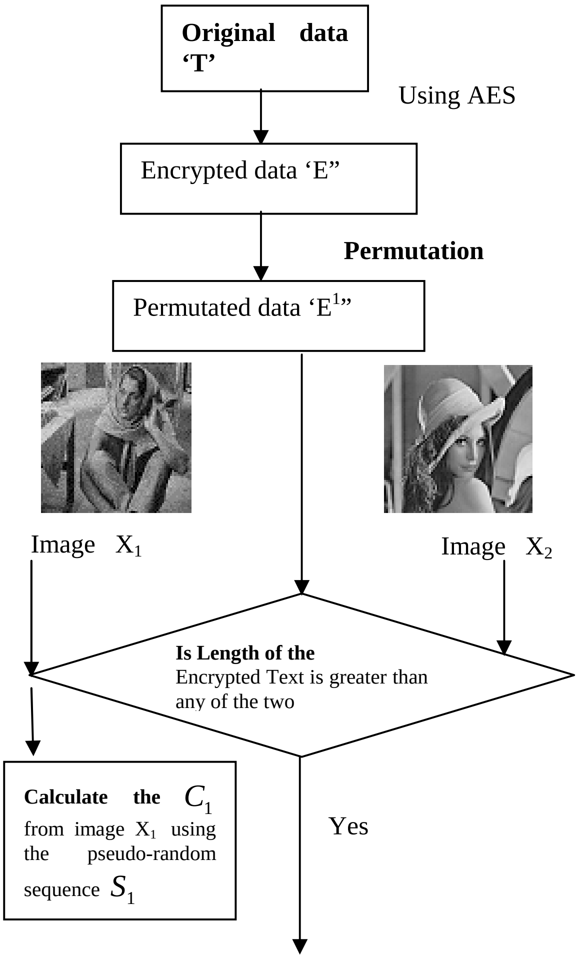
[27] A. Ahmad, M. J. Al-Musharafi, S. Al-Busaidi, A. Al-Naamany, and J. A. Jervase, "An NLFSR Based Sequence Generation for Stream Ciphers", Proceedings of International Conference on Sequences and their Applications (SETA '01). May 2001, pp. 11-12.

[28] Shannon, C. E.," Communication theory of secret systems," Bell System Technical Journal 28v(4), 656-715 (1949).

Navin Rajpal received the B.Sc.(Engg), M.Tech (IIT ,Delhi), Ph.D.(IIT, Delhi) He is currently working as Professor at USIT GGSIP University since Sept 2004. He worked as Reader at USIT GGSIP University. He worked as Assistant Professor at CRSCE Murthal from 1996-2000. He worked as Scientific Officer at CARE, IIT Delhi from 1987-1995. Published more than 50 research papers in Journals and Conference Proceddings. Worked on 7 Sponsored and 2 Consultancy projects and released 3 softwares for copyright at IIT Delhi. Supervised several M.Tech., MCA and B.Tech. Projects and supervising 5 Ph.D Students. His research interest include Computer Vision, Image Processing, Pattern Recognition, Artificial Neural Networks, Computer Graphics, Algorithms Design and Digital Hardware Design.

Anil Kumar born in Delhi(INDIA) in 1972. He received the B.E.(Electronics) degree from the I.E.T.E ,Delhi , in 1995. He received the M.E. (Computer) degree from Delhi College of Engineering , Delhi in 2000. He is currently working on his Ph.D.. degree in the Department of Information Technology, Guru Gobind Singh Indraprastha University, Dehi(INDIA). He is currently working as Asstt. Professor in MSIT, Delhi(INDIA) in the department of Computer Science Engineering, before that he has worked as lecturer in IT Department , in BVCOE, Delhi since 2002 to 2005, Before that worked in DRDO (Ministry of Defense) as RA since 2000 to 2002. He worked as Lecturer in Electronics Department in GNDP since 1997 to 1999. He worked as Lecturer in Electronics Department in CRRIT(Delhi) since 1995 to 1997. He has published more than 20 research paper in journal and conference. His research interests include Image processing algorithm, Cryptography, Artificial Intelligence, Signal and System, Neural System and Genetic Algorithm .

Flow Chart of the algorithm


Original data 'T'
Using AES
Encrypted data 'E"
Permutation
Permutated data 'E1"
Image X1
Image X2
Is Length of the Encrypted Text is greater than any of the two
Calculate the C1 from image X1 using the pseudo-random sequence S1
Yes

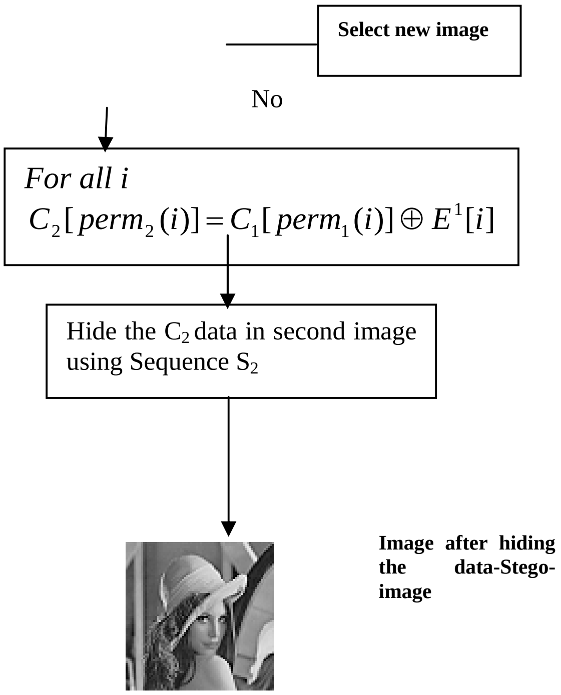

Select new image
No
For all i
$C_2[perm_2(i)] = C_1[perm_1(i)] \oplus E^1[i]$
Hide the C_2 data in second image using Sequence S_2
Image after hiding the data-Stego-image

Fig 2. Flow chart of the algorithm