Information Encryption Scheme Based on Visual Cryptography and Nonlinear Pseudorandom Sequence

Thin Thin Yu, Khin Than Mya
University of Computer Studies, Yangon, Myanmar
thinthinyu.ucsm@gmail.com, khinthanmya@gmail.com

Abstract

Security requires the integration of people, process, and technology. Strong information encryption and decryption scheme are crucially important for information technology. Nowadays, secret sharing is one popular method for distributing a secret amongst a group of participants, each of which is allocated a share of the secret. This paper presents a scheme which is derived from the substitution of bits in the image by using nonlinear pseudorandom sequence and visual cryptography method and triple data encryption method. 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. Therefore the administrator is the central authority of the process. 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.

1. Introduction

All in the present era of computers and fast communication, one needs to protect communicated information from unauthorized user, while sending it through any electronic media. The private key and the public key are the two well known cryptosystems 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) and Rivest, Shamir, Adleman (RSA) and Advanced Encryption Standard (AES) are three representative methods. Secret sharing scheme have many interesting application in the real world. Shamir and Blakley independently devised secret sharing schemes for the application of key distribution. Informally, a secret sharing scheme allows a dealer to protect a secret among participants with each participant holding one share. A secret sharing scheme is called perfect if any subset in the access structure can recover the secret while any unauthorized subset cannot gain any information about the secret.

In this 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 Triple DES 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 triple DES which is used by the administrator. In Section 3, we introduce the nonlinear pseudo-random sequence and in Section 4, we present a proposed method using pseudo-random sequence. Security Analysis and Conclusion are shown in Section 5 and 6.

2. Triple Data Encryption Standard

This is used to encrypt the secret data by the administrator. Let $E_K(I)$ and $D_K(I)$ represent the DES encryption and decryption of I using DES key K respectively. Each TDEA encryption/decryption operation is a compound operation of DES encryption and decryption operations. The following operations are used:

- TDEA encryption operation: the transformation of a 64-bit block I into a 64-bit block O that is defined as follows:

$$O = E_{K3}(D_{K2}(E_{K1}(I)))$$

- TDEA decryption operation: the transformation of a 64-bit block I into a 64-bit block O that is defined as follows:

$$O = D_{K1}(E_{K2}(D_{K3}(I)))$$

The standard specifies the following keying options for bundle *(K1, K2, K3).*

- Keying Option 1: *K1, K2* and *K3* are independent keys;
- Keying Option 2: *K1* and *K2* are independent keys and *K3 = K1*;
- Keying Option 3: *K1 = K2 = K3*.

A TDES mode of operation is backward compatible with its single DES counterpart, with compatible keying options for TDES operation,

- An encrypted plaintext computed using a single DES mode of operation can be decrypted correctly by a corresponding TDES mode of operation; and
- An encrypted plaintext computed using a TDES mode of operation can be decrypted correctly by a corresponding single DES mode of operation. When using Keying Option 3 *(K1 = K2 = K3)*, TECB, TCBC, TCFB and TOFB modes are backward compatible with single DES modes of operation ECB, CBC, CFB, OFB respectively.

3. Nonlinear Pseudo Random Sequence

NFSR is extremely good pseudorandom binary sequence generator. When this register is loaded with any given initial value, it generates pseudorandom sequence, which has very good randomness and statistical properties. A model of NFSR is considered to demonstrate the functioning of LFSR with the feedback function $f(x) = x^2 - 28x - 26 \in Z_{29}(x)$ and the non-linear function z defined by $R_H(A,B) = H((e_A + B) \bmod 2^n)$ forming nonlinear generator. The design of this generator is as shown in figure 1.

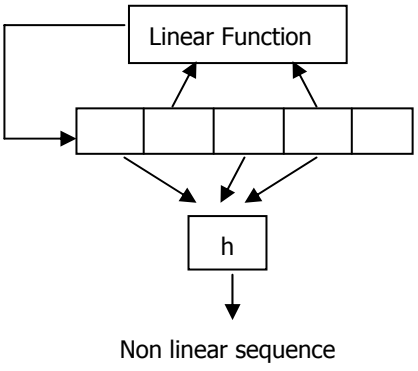

Figure 1. General design for producing nonlinear sequence

Its initial values are obtained from curve equation $\mathbf{E}: \mathbf{y}^2 = \mathbf{x}^3 + \mathbf{x} + 4$ over **GF**(23). The first point sequence from linear feedback function is **P** = (P, 2P, 24P, 28P, 16P, 16P, 23P, 16P, 2P, 8P, 15P, 19P, 23P, 7P, 11P, 26P, 28P, 10P, 22P, 6P, 15P, 25P, 17P, 24P, 12P, …).

The second sequence generated from nonlinear function by using Random box is z = { 6, 6, 9, 4, 12, 12, 10, 12, 6, 12, 1, 5, 10, 4, 8, 3, 4, 14, 2, 15, 1, 10, 5, 9, 12, …}. The final output sequence is derived from $h(z) = (\sum_{i=1}^{m} z_i \bmod 4) + 1$ and its value is {3, 3, 2, 1, 1, 1, 3, 1, 3, 1, 2, 2, 3, 1, 1, 4, 1, 3, 3, 4, 2, 3, 2 …}.

where m =maximum period of sequence

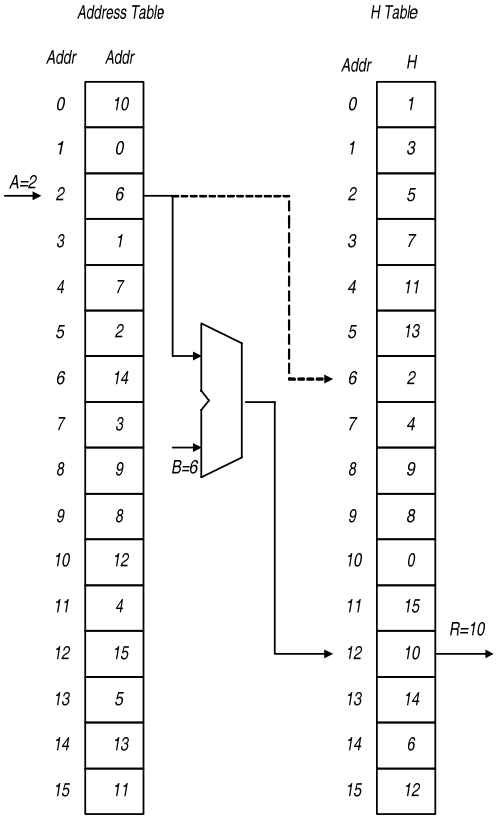

Figure 2. Logic Work of R Box

Period of the enciphering sequence can be increased if it is generated by following methods:

- Addition of maximal length sequences.
- Multiplication of maximal length sequences.
- 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 the balance, run and correlation properties of these sequences make them more useful in the selection of secret keys. The NFSR generated sequences are of great importance in many fields of engineering and sciences.

4. Proposed Method

Our proposed method consists of three parts: encryption, permutation and data hiding. Suppose the administrator 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 images X_1 and X_2 in which we will share the encrypted data. We will take two pseudo-random sequences which are generated by the NFSR. Let the sequences generated are S_1 and S_2. Let the sequence generated as follows:

$S1 = \{2, 4, 1, 2, 3, 2, 1\}$

$S2 = \{3, 1, 2, 4, 3, 2, 1\}$

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 etc and the collection of the bits from the image X_1 is consider as C_1 array.

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

These are the pixel of the image X_1 selection based on the pseudo-random sequence S_1 and the content of the array

$C_1 = \{1, 0, 0, 1, . .\}$ 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: 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, 1, 0, 0, ...] in the bits form and the sequence

S_2 = . {3, 1, 2, 4, 3, 2, 1}

Let the cover image X_2 having the pixel value in bit-form before hiding the data

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

After hiding secret share in the image X_2 using the sequence S_2 and array C_2 in bit-form

1st Pixel	11001000
2nd Pixel	11101001
3rd Pixel	11101001
4th Pixel	11000000

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

Step 5: Secret sharing is complete. Exit.

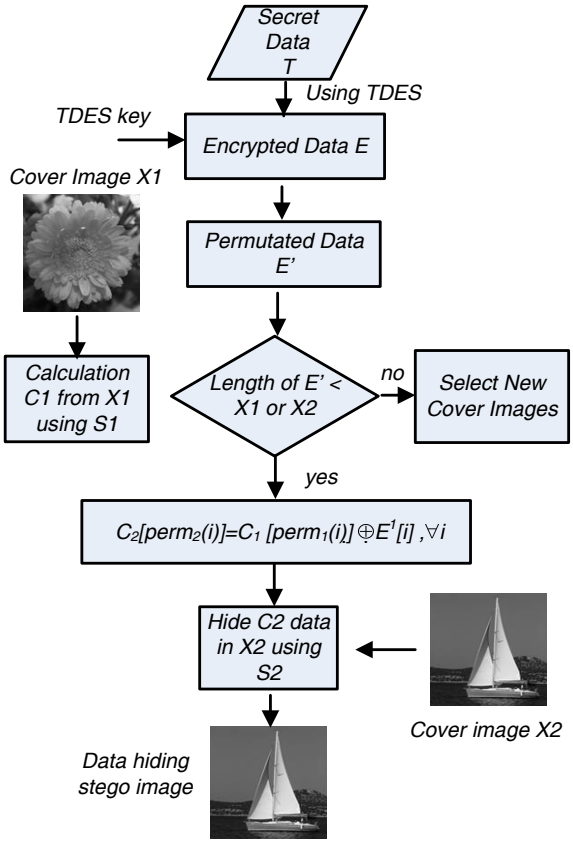

Figure 3. Flow chart of the algorithm

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,
$E^1[i] = C_1\,\text{perm}_1(i)] \oplus C_2[\,\text{perm}_2(i)]$

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. 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 contained 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 attacker's 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 pseudorandom 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 because administrator uses TDES. And to guess the E^1 or C_2 $[perm_2\,(i)]$ or C_1 $[perm_1(i)]$ require the 2^l possible cases and same for the E. This satisfies the requirement of the practical security [8] 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. This method is appropriate for data security 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.

7. Reference

[1] 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.

[2] C.W. Chan and Y.D. Wu, "A Visual Information Encryption Scheme Based on Visual Cryptography and D-H Key Agreement Scheme" *IJCSNS International Journal of Computer Science and Network Security*, VOL.8 No.4, April 2008.

[3] N. Rajpal, A.Kumar, "Secret Image Sharing Using Pseudo-Random Sequence" *IJCSNS International Journal of Computer Science and Network Security*, VOL.6 No.2B, February 2006.

[4] 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.

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

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

[7] R.G. Kammer, W.M. Daley, *Data Encryption Standard (DES)*, Federal Information Processing Standards Publication, October 1999.

[8] Shannon, "Communication theory of secret stems", *Bell System Technical Journal* 28v(4), 656-715, 1949.

[9] T.T.Yu, "Nonlinear Pseudorandom Sequence", International Conference on Recent and Emerging Advanced Technologies in Engineering", Kuala Lumpur Malaysia, November 2009.