Journal of KerbalaUniversity , Vol. 11 No.1 Scientific . 2013

Randomly Steganography using LFSR and NLFSR generation

Assistant Lecturer
Noor Dhia Kadhm Al-Shakarchy
Computer Science Department, Science College, Karbala University, Karbala, IRAQ
Email: noor.dhiya@gmail.com

Abstract:

With the development of information technology, people have paid more and more attention on the information security today. Information hiding research has become the focus of the information security research. Because every web sites and networks communication depend on the multimedia, such as audio, video, image and so on.

Information hiding technology can embed secret information in to a digital media source without impairing the perceptual quality of the source. Steganography could informally be defined as the " cover writing", where it means concealing a message that is the object of the communication. Steganography has its place in security, and is not intended to replace cryptography but to supplemented it.

In this research a new simple approach for active Steganography is presented that can successfully resist recent blind stegoanalysis methods. A proposed method based on embedding data in a randomized manner. The randomization done by used pseudo random generation depending on Linear Feed-back Shift register (LFSR) and Non-Linear Feed-back Shift Register (NLFSR). The proposed method divided the cover image in to blocks then used first generation with (LFSR) to determine the blocks and these arrangement used in embedding process. This represent the first randomization. In each block second randomly generation (NLFSR) apply to determine the pixels and these arrangement using in embedding process. The randomization and don't used all pixels makes the distortion in stego-image very little that's provide strongest against detection and attempts of stegoanalyst.

الملخص:

مع التطور الحاصل في تكنولوجيا المعلومات ازداد الاهتمام بأمن المعلومات. واخذ مجال إخفاء المعلومات تركيزا واسع وذلك لان اغلب مواقع الانترنت وشبكات الاتصالات تعتمد بشكل كبير على الوسائط المتعددة كالصوت والصورة والفيديو وغيرها .تقنية إخفاء المعلومات توفر إمكانية إخفاء المعلومات السرية في وسط رقمي ويسمى الغطاء دون أن يضعف الصفات النوعية للغطاء. و عليه يمكن تعريف علم إخفاء المعلومات بأنه الكتابة السرية. وهذا لا يعني إن علم إخفاء المعلومات يمكن إن يعتبر بديل عن علم التشفير ولكن ممكن اعتباره مكمل له.

في هذا البحث تم تقديم طريقة لإخفاء المعلومات بشكل عشوائي. العشوائية تتم عن طريق استخدام مولد عشوائي يعتمد على مسجل الإزاحة الخطية ذات التغذية الخلفية ومسجل الإزاحة اللاخطية ذات التغذية الخلفية. الطريقة المقترحة تعتمد على تقسيم الصورة إلى كتل و ثم نستخدم المولد العشوائي الأول (مسجل الإزاحة الخطية ذات التغذية الخلفية) هذا المولد سيولد مفتاح الكتل والذي يمثل تسلسل الكتل التي سيتم الإخفاء فيها باستخدام مسجل الإزاحة الخطية ذات التغذية الخلفية . وهذا يمثل العشوائية الأولى للطريقة المقترحة. و لكل كتلة مختارة يطبق المولد العشوائي الثاني (مسجل الإزاحة اللاخطية ذات التغذية الخلفية) الذي يستخدم لتوليد مفتاح الإخفاء الذي يحدد النقاط المختارة للإخفاء وتسلسلها. العشوائية للطريقة المقترحة وعدم استخدام كل الكتل والنقاط للإخفاء تقلل التشويه للصورة الناتجة من عملية الإخفاء والذي بدوره يزيد من قوة النظام بوجه طرق الاكتشاف ومحاولات محللي الإخفاء.

1- Introduction:

Steganography has its place in security, and is not intended to replace cryptography but to supplemented it. If encryption was concerned with protecting the security of information and preventing someone from looking at the contents of a message, then the science of information hiding went one step further, by concealing the transfer of information itself.encryption allows for the transfer of information, but it is not concerned with whether or not others are aware that an encryption communication has taken place. The function of information hiding is to move secret information without arousing even the slightest suspicion that a transmission of information has

occurred. This is done using digital mediums as cover [1]. Hiding a message with Steganography methods reduces the chance of a message being detected. If the message also encrypted then it provides another layer of protection. Therefore some steganographic methods combine traditional cryptography with Steganography; such combination increases the security of the overall communication process, as it is more difficult for an attacker to detect embedded ciphertext (which itself has a rather random appearance) in cover.

Shannon identified three forms of secret communications:(1) concealment systems, including such methods as invisible ink, concealing a message in an innocent text, or in a fake covering cryptogram, or other methods in which the existence of the message is concealed from the enemy. (2) privacy system, and (3) cryptographic systems, [2]. Hiding information into a media requires following elements:

·The cover media(C) that will hold the hidden data
·The secret message (M), may be plain text, cipher text or any type of data
·The stego function (Fe) and its inverse (Fe^{-1})
·An optional stego-key (K) or password may be used to hide and unhide the message.

The embedding efficiency of steganographic schemes is defined as the average number of random message bits embedded using one embedding change. If the secret message is shorter than the embedding capacity, the embedding efficiency can be substantially improved using matrix embedding [2].

Steganography differs from cryptography in the sense that where cryptography focuses on keeping the contents of a message secret, steganography focuses on keeping the existence of a message secret [3]. Steganography and cryptography are both ways to protect information from unwanted parties but neither technology alone is perfect and can be compromised. Once the presence of hidden information is revealed or even suspected, the purpose of steganography is partly defeated [3]. The strength of steganography can thus be amplified by combining it with cryptography.

A successful attack on a steganographic system consists of an adversary observing that there is information hidden inside a file, while a successful attack on a watermarking or fingerprinting system would not be to detect the mark, but to remove it [4]. the security of a steganographic system in terms of the relative entropy (or discrimination) between the distributions of the covertext and the stegotext. A stegosystem is called perfect if this relative entropy is zero [5]. Formally, a stegosystem consists of a triple algorithms for key generation, message encoding, and message decoding, respectively. In the symmetric-key setting considered here, the output of the key generation algorithm is given only to sender (encoder) and to receiver (decoder) .

In this research we present a randomly manner with classical hiding methods (Least Significant Bits LSB and Discrete Cosine Transformation DCT) to avoid the distortion in the stego-image. The proposed system provide a randomization by using Linear Feed-back Sift Register (LFSR) and Non Linear Feed-back Sift Register (NLFSR) generators. The output sequences from these generators represent the randomly keys used to determine the embedding locations.

2-Related Work:

The most of today's steganographic systems use images as cover object because people often transmit digital images over email and other communication media. Several methods exist to utilize the concept of Steganography as well as plenty algorithms have been proposed in this regard. To gather knowledge in this particular research field, we have concentrated on some techniques and methods which are described below.

Least significant bit (LSB) insertion is a common and simple approach to embed information in a cover object. For images as a covering media, the LSB of a pixel is replaced with an M's bit. If we choose a 24-bit image as cover, we can store 3 bits in each pixel by modifying the LSBs of R, G and B array. To the human eye, the resulting stego image will look identical to the cover image [6].

Hiding data in the features of images is also an important technique which uses the LSB modification concept. In this method, to hide data in an image the least significant bits (LSB) of each pixel is modified sequentially in the scan lines across the image in raw image format with the

binary data. The portion, where the secret message is hidden is degraded while the rest remain untouched. An attacker can easily recover the hidden message by repeating the process [6, 7].

An interesting application of steganography and cryptography has been developed by Sutaone, M.S., Khandare, M.V, where a steganography system is designed for encoding and decoding a secret file embedded into an image file using random LSB insertion method. In that method, the secret data are spread out among the cover image in a seemingly random manner. The key used to generate pseudorandom numbers, which will identify where, and in what order the hidden message is laid out. The advantage of this method is that it incorporates some cryptography in that diffusion is applied to the secret message [8].

The next interesting application of steganography is developed by Miroslav Dobsicek, where the content is encrypted with one key and can be decrypted with several other keys. In this process, the relative entropy between encrypt and one specific decrypt key corresponds to the amount of information [9].

Nameer N. EL-Emam proposed an algorithmic approach to obtain data security using LSB insertion steganographic method. In this approach, high security layers have been proposed to make it difficult to break through the encryption of the input data and confuse steganalysis too [10].

S. K. Bandyopadhyay, Debnath Bhattacharyya, Swarnendu Mukherjee, Debashis Ganguly, Poulami Das has also proposed a heuristic approach to hide huge amount of data using LSB steganography technique. In their method, they have first encoded the data and afterwards the encoded data is hidden behind a cover image by modifying the least significant bits of each pixel of the cover image. The resultant stego-image was distortion less. Also, they have given much emphasis on space complexity of the data hiding technique [11]. In this research we present a random LSB by randomly chose to block and pixels in that block used to embedding data.

In spatial domain methods a steganographer modifies the secret data and the cover medium in the spatial domain, which involves encoding at the level of the LSBs. Potdar et al. [12] used a spatial domain technique in producing a fingerprinted secret sharing Steganography for robustness against image cropping attacks. Their paper addressed the issue of image cropping effects rather than proposing an embedding technique.

Shirali-Shahreza, M. H. and Shirali-Shahreza, M. [13] exploited Arabic and Persian alphabet punctuations to hide messages. While their method is not related to the LSB approach, it falls into the spatial domain if the text is treated as an image.

JPEG images however, were at the beginning avoided because of their compression algorithm which does not support a direct LSB embedding into the spatial domain. In [14], the authors claimed that changes as small as flipping the LSB of one pixel in a JPEG image can be reliably detected.

3. Steganography:

Although Steganography is an ancient subject, the modern formulation of it is often given in terms of the prisoner's problem proposed by Simmons [15], where two inmates wish to communicate in secret to hatch an escape plan. All of their communication passes through a warden who will throw them in solitary confinement should she suspect any covert communication [16]. The warden, who is free to examine all communication exchanged between the inmates, can either be passive or active. A passive warden simply examines the communication to try and determine if it potentially contains secret information. If she suspects a communication to contain hidden information, a passive warden takes note of the detected covert communication, reports this to some outside party and lets the message through without blocking it. An active warden, on the other hand, will try to alter the communication with the suspected hidden information deliberately, in order to remove the information [17].

3.1 Least Significant Bit

Least significant bit (LSB) insertion is a common, simple approach to embedding information in a cover image [18]. The least significant bit (in other words, the 8th bit) of some or all of the bytes

inside an image is changed to a bit of the secret message. When using a 24-bit image, a bit of each of the red, green and blue colour components can be used, since they are each represented by a byte. In other words, one can store 3 bits in each pixel. An 800 × 600 pixel image, can thus store a total amount of 1,440,000 bits or 180,000 bytes of embedded data [19]. For example a grid for 3 pixels of a 24-bit image can be as follows:
(00101101 00011100 11011100)
(10100110 11000100 00001100)
(11010010 10101101 01100011)
Although the number was embedded into the first 8 bytes of the grid, only the 3 underlined bits needed to be changed according to the embedded message. On average, only half of the bits in an image will need to be modified to hide a secret message using the maximum cover size [19]. Since there are 256 possible intensities of each primary colour, changing the LSB of a pixel results in small changes in the intensity of the colours. These changes cannot be perceived by the human eye - thus the message is successfully hidden. With a well-chosen image, one can even hide the message in the least as well as second to least significant bit and still not see the difference [20].

3.2.Discret Cosine Transformation DCT:

The discrete cosine transform (DCT) transforms a signal or image from the spatial domain to the frequency domain. The dct function computes the two-dimensional discrete cosine transform (DCT) of an image[21]. The DCT has the property that, for a typical image, most of the visually significant information about the image is concentrated in just a few coefficients of the DCT. For this reason, the DCT is often used in image compression applications. The two-dimensional DCT of an M-by-N matrix A is defined as follows[22,23].

$$B_{pq} = \alpha_p \alpha_q \sum_{m=0}^{M-1} \sum_{n=0}^{N-1} A_{mn} \cos\frac{\pi(2m+1)p}{2M} \cos\frac{\pi(2n+1)q}{2N}, \quad \begin{matrix} 0 \le p \le M-1 \\ 0 \le q \le N-1 \end{matrix} \qquad \text{..... (1)}$$

$$\alpha_p = \begin{cases} 1/\sqrt{M}, & p=0 \\ \sqrt{2/M}, & 1 \le p \le M-1 \end{cases} \quad \alpha_q = \begin{cases} 1/\sqrt{N}, & q=0 \\ \sqrt{2/N}, & 1 \le q \le N-1 \end{cases} \qquad \text{..... (2)}$$

The values Bpq are called the *DCT coefficients* of A. (Note that matrix i ; start at 1 rather than 0; therefore, the MATLAB matrix elements A(1,1) and B(1,1) correspond to the mathematical quantities A00 and B00, respectively.)
The DCT is an invertible transform, and its inverse is given by:

$$A_{mn} = \sum_{p=0}^{M-1} \sum_{q=0}^{N-1} \alpha_p \alpha_q B_{pq} \cos\frac{\pi(2m+1)p}{2M} \cos\frac{\pi(2n+1)q}{2N}, \quad \begin{matrix} 0 \le m \le M-1 \\ 0 \le n \le N-1 \end{matrix} \qquad \text{..... (3)}$$

$$\alpha_p = \begin{cases} 1/\sqrt{M}, & p=0 \\ \sqrt{2/M}, & 1 \le p \le M-1 \end{cases} \quad \alpha_q = \begin{cases} 1/\sqrt{N}, & q=0 \\ \sqrt{2/N}, & 1 \le q \le N-1 \end{cases} \qquad \text{..... (4)}$$

4. Defining Security of Steganography system:

The security of a stegosystem is defined in terms of an experiment that measures the capability of the adversary to detect the presence of an embedded message. In a secure stegosystem, anyone except the reciver cannot distinguish whether Alice is sending legitimate covertext or stegotext. The attack considered here is a *chosen-message attack,* where the adversary may influence the embedded message but has otherwise no access to the encoding and decoding functions. It parallels the notion of a chosen-plaintext attack against a cryptosystem [24].

5. Embedding key generation :

The basic element in proposed Steganography system is the embedding key generators, which will generate the sequence these determine the location of embedding in cover image. The method

that is most often used in hardware pseudo generations by means of the following recurrence relation:

$X_i = \sum_{k=1}^{m} a_k x_{i-k}$ I = 0,1,2,3, ….., m …… (5)

Where i is a timing index , Xi €{ 0, 1} are output sequence digits. ak € {0, 1} are constant coefficients. And the summation is modulo-2 addition. With an appropriate choice of the {ak} coefficients, the generated sequence will have the maximal length of period (for a given m) and is called an M-sequence.

A major advantage of the maximal length M-sequence generation methods, is the simplicity of its implementation as Linear feedback Shift Register (LFSR). It is simply implemented using m-bits shift registers, which consist of a register R= (rm , rm-1, ….. , r1), and a tap T = (tm , tm-1, ….. , t1), where each ri and ti is one binary digit as illustrate in figure …… . at each step, bit ri is appended to the key stream, bits rm, …, r1 are shifted to right, and a new bit is derived from T and inserted into the left end of the register R.

The cyclic properties of sequence generator are defined by a characteristic polynomial [25]:

$\varphi = \sum_{k=1}^{m} a_k x_{i-k}$ …….. (6)

$a_0 = a_m = 1$ and akj € {0, 1} with j = 1, 2, ……, m-1.

In another meaning, for any m-stage register with feedback constant c0, c1, …, cn-1; the characteristic polynomial $f(x) = c_0x^0 + c_1x^1 + \ldots + c_{m-1}x^{m-1} + x$.

The periodic of the sequence generated by the circuit depends on whether polynomial $\varphi(x)$ is primitive and irreducible. Maximal length sequence with period $(2^m -1)$ are generated only in case when the characteristic generating polynomial $\varphi(x)$ is primitive and irreducible; that's shown in figure -1.

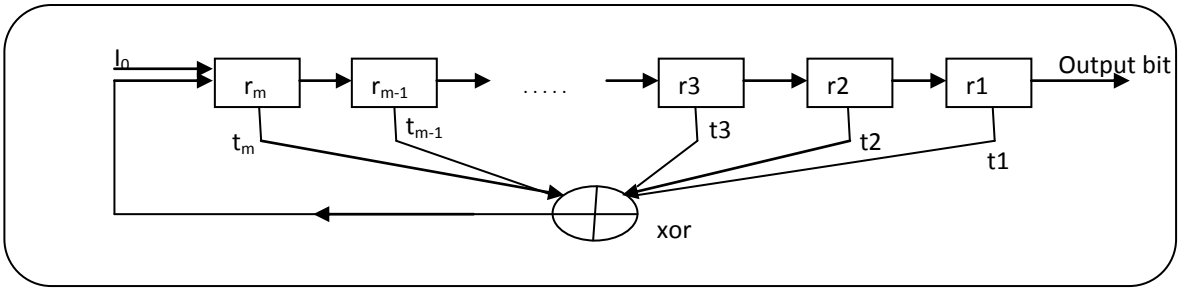

Figure -1 M-sequence Generation (LFSR)

5.1 Linear Shift Registers:[25, 26, 27]

A feed back shift register is an implementation of the key stream generator. It is made up of two parts: a shift registers and a feedback function. The shift register is a sequence of bits. Each time a bit is needed, all the bits in the register are shifted 1 bit to the right. The new left-most bit is computed as a function of the other bits in the register. The output of the shift register is one bit. The simplest kind of feedback shift register is a linear feedback shift register (LFSR) the feedback function is simply the XOR function.

Three parameters; initial state, primitive polynomial, and the length of the register affect the output stream of the linear shift register. Foe each linear shift register there exist a linear equivalence, which defined as; the length of the smallest linear shift register which can be used to generate the sequence.

5.1.1. Register Stages:

Shift registers consist of finite length of binary memory, called stages, for m-binary memory, called m-stages shift register, and in any given time the contents of the register, called **state**. The register could be in one of 2m states. Zero state is ignored because; it causes endless sequence of zeros, thus, we left with 2m-1 states. Next states depends on the feedback function (the mixer).

To achieve maxim length of 2m-1 stages of LFSR; the tap sequence must cause the register to cycle through 2m-1 non zero bit sequence before repeating; this will happen if the polynomial formed from the elements in the tap sequence is primitive.

5.1.2 Primitive polynomial:

When talking about the polynomials, the term prime is replaced by irreducible. Primitive polynomial of degree n is defined as an irreducible polynomial that divides $x^{2n-1} + 1$, but not $x^d + 1$ for any d that divides 2^n-1. A polynomial is irreducible if it cannot be expressed as the product of two other polynomials (except 1 and itself). In another meaning maximal length sequence with period 2^n-1 are generated only in the case when the characteristic (generating) polynomial $\varphi(x)$ is primitive, irreducible, and the initial state of the register must be other than zero.

5.1.3 Linear Equivalence:

Linear equivalent is defined as the length of the smallest linear register which can be used to generate the sequence. The primitive polynomial for the linear equivalence is called minimal polynomial. Linear equivalence determines the complexity of the generated sequence. For a sequence with n linear equivalence; it needs only 2n of the generated sequence to deduce the whole sequence. Hence for good cipher secrecy, it is needed to have a generator with large linear equivalence.

5.2 Non Linear Shift Register: [27,28]

Linear feedback shift registers are unsafe because they have relatively small linear complexity, and hence a relatively small fragment of the key (LFSR sequence) can be used to obtained the entire sequence by solving a set of linear equation. To increase the linear complexity of LFSR, one or more output sequence of LFSR's are combined with some nonlinear function to produce relatively high linear complexity.

5.2.1 Non Linear Feedback Shift Register system:

In which the key generator is a shift register with non linear feedback function, as illustrated in figure-2. In this type, one LFSR is used with n- stages and non- linear feedback function.

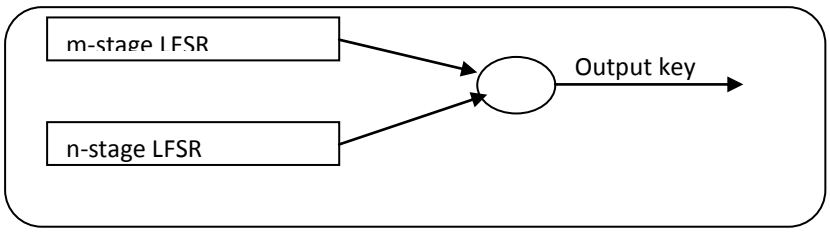

Figure -2 Non Linear Feedback Shift Register (NLFSR)

In this research we used these generators to produced the embedding key ; this key determine the order of pixel number in cover that used to embedding the desired message. This key gives a randomness of embedding message inside an cover image. these randomness make stego system most harder against stegoanalyst.

6. The proposed system :

In order to enable secure communication in the presence of blind steganalysis, the steganographer must embed information in to host signals in such a way that no image features are significantly perturbed during the embedding process. However, we must not forget that the steganalyst must depend on stego image to derive the approximate cover image statistics via some sort of self-calibration process. The steganographer can, instead of trying to preserve the feature vectors, embed data in such a way that it distorts the steganalyst's estimate of the vector image statistics. This can practically be achieved using the following approaches.

1. Hiding with high embedding strength: by embedding data with high strength, the cover image is distorted so much that the cover image statistics can no longer be derived reliably from the available stego image .
2. Randomized hiding: by randomizing the embedding approach, the algorithm to estimate the cover statistics can be effectively disabled. Key generation with LFSR and NLFSR used to achieve this pseudo random embedding .

6.1 Proposed Algorithm:

In this research we present a JPEG image and embedded data in matrix blocks each block chose randomly using LFSR generator (which generate pseudo random sequence) and the pixel in each block which used to embed chose randomly also using NLFSR generator then hiding data using LSB first; and other proposed system by generate pseudo random sequence to determine the number of block used to embedding then apply DCT on this block and hiding the data. the main steps involved in this randomized block hiding method illustrates bellow:

Step1: Divide the image into blocks of size B*B such as 8*8.

Step2:Applying LFSR with primitive polynomial to generate pseudo random sequence using to select the order of blocks used to embedding data in cover images pseudo randomly. The order of blocks represent blocks key and shared between the encoder and the decoder process (side). In this research we apply LFSR with primitive polynomial $T(x) = x^5+x^3+x^2+x+1$; and initial value such as I0 = 01011 to produced the pseudo random sequence, such as:

1101	0001	0010	1011	0000	1110	0110	1111	……
13	1	2	11	0	14	6	15	

Then captured each d bits (according to number of images blocks) we used d=4 bits and convert each 4bits block to decimal number represent the blocks order used to embedding.

Step3: For each selected block generate the embedding key pseudo randomly also by using NLFSR generator to plan the embedding process in block pixels. This key represent embedding key and shared also between the encoder and the decoder process. The NLFSR generator generate pseudo random sequence represent the location number of pixel used to hide data.

Practically that done in this research by using NLFSR with 2LFSR . first LFSR used primitive polynomial $T(x) = x^4+ x + 1$ and initial value I_0= 1001. Second LFSR used primitive polynomial $T(x) = x^3+ x + 1$ and initial value I_0= 100. The outputs of these two LFSRs xoring to produced the output sequence , such as :

101010	111001	111111	001010	000001	……
42	57	63	10	1	

Then captured each d bits (according to size of image blocks) we used d=6 bits because the size of each block in this research 8*8 that's mean each block contained 64 pixels(0 – 63) and convert each 6bits block to decimal number represent the pixels order used to embedding.

Step4: In this research this step (embedding step) done in two ways: by using randomly Least Significant Bits (LSB) and by using Discrete Cosine Transformation (DCT) as illustrate in 3.1 and 3.2 above .

a. Embedding using LSB by using the embedding key to determine the pixel in selected block used to replaced least significant bits (lest 2 bits) with (2 bits) of desired embedding data after converting it (the massage) to binary using asscii code. The figure-2 below shows the images before and after data hidden using LSB.

Figure -2 images before and after data hidden using LSB

b. Second way of hiding data in chosen pixel by applying LSB technique during discrete cosine transformation (DCT) on cover image; The following steps are followed in this case: -

1.Working from top-left to bottom-right of the cover image, DCT is applied to each chosen pixel of each chosen block.

2.After applying DCT, one DCT Coefficient is generated for each chosen pixel in chosen block.

3.Each DCT coefficient is then quantized against a reference quantization table.

4. The LSB of binary equivalent the quantized DCT coefficient can be replaced by a bit from secret message.

5. Encoding is then applied to each modified quantized DCT coefficient to produce compressed Stego Image.

The figure-3 below shows the images before and after data hidden using second way.

Figure -3 images before and after data hidden using LSB during DCT

6.2 Extracting Algorithm (Decoding):

In receiver side the stego Image used to extracting the hidden message in image cover, the following steps represent this algorithm:

Step1: Divide the stego- image into blocks of size B*B such as 8*8.

Step2:Applying LFSR with same primitive polynomial to generate same pseudo random sequence using to select the same order of blocks used to embedding data in cover images pseudo randomly. The order of blocks represent blocks key and shared between the encoder and the decoder process (side). Such as encoding (embedding) process.

Step3: For each selected block generate the same embedding key pseudo randomly also by using same NLFSR generator to plan the embedding process in block pixels. This key represent embedding key and shared also between the encoder and the decoder process. The NLFSR

generator generate pseudo random sequence represent the location number of pixel used to hide data. Such as encoding (embedding) process.

Step4: the embedding step done in two ways such as illustrate in encoding (embedding) process. And the extracting the desired message from stego- image must done in two ways also :

a. With LSB embedding; using the embedding key to determine the pixel in selected block using in embedded then extract the least 2 bits from it to obtained the desired message in binary then convert the message to character using asscii code.
b. Second way of Hiding data in chosen pixel by applying LSB technique during discrete cosine transformation (DCT) on cover image; The following steps are followed in this case: -

1.Working from top-left to bottom-right of the selected stego-block- image.
2. Decoding is applied to each selected pixel in with stego-image block using inverse DCT to produced modified quantized DCT coefficient.
3. Extract LSB of modified quantized DCT coefficient to produced secret (desired image) message in binary then convert the message to character using asscii code.

7. Conclusion:

The main points we can detected from proposed system:

1- The proposed system depend on hiding data in randomly manner; such as; don't use all pixel in embedding process and used different pixels in each embedding process according to embedding key generation used .
2- The proposed hiding manner considered secure manner to hide information in image because the distortion in stego-image very little by hiding data in chosen blocks and pixels (not all pixels). All that's makes the proposed system is strongest against the detections.
3- If the attacker explore the existence of the message he/ she can't recover the message because this message distributed in blocks and pixels randomly, and he / she needed to know the embedding key to obtained the message. That's mean the cryptanalyst working together with stegoanalyst to attempt breaking the proposed system.
4- It can be able to manage the number of pixels used in embedding process according to the size of data wanted to hide The number of blocks and pixels determined by the polynomial used in LFSR and NLFSR key generators.

Reference:

[1]the technical mujahid, Issu2, Safar," Secret Information: Hid Secret Inside Pictures", march 2007.

[2] Soumyendu Das, Subhendu Das, Bijoy Bandyopadhyay and Sugata Sanyal, "Steganography and Steganalysis: Different Approaches", University of Calcutta, Kolkata, India, Tata Institute of Fundamental Research Mumbai, India, 2005.

[3] T Morkel, JHP Eloff and MS Olivier, "An Overview of Image Steganography," in Proceedings of the Fifth Annual Information Security South Africa Conference (ISSA2005), Sandton, South Africa, June/July 2005.

[4] Anderson, R.J. & Petitcolas, F.A.P., "On the limits of steganography", IEEE Journal of selected Areas in Communications, May 1998

[5] Christian Cachin, "An Information-Theoretic Model for Steganography", March 4, 2004

[6] S.K.Bandyopadhyay, Debnath Bhattacharyya, Poulumi Das, S. Mukherjee, D. Ganguly, "A Tutorial Review on Steganography", IC3 Noida, pp. 106-114, August 2008.

[7] Kh. Manglem Singh, S. Birendra Singh and L. Shyam Sundar Singh, "Hiding Encrypted Message in the Features of Images", IJCSNS, VOL. 7, No.4, April 2007.

[8] Sutaone, M.S., Khandare, M.V, "Image based steganography using LSB insertion technique", IEEE WMMN, pp. 146-151, January 2008.

[9] M. Dobsicek, "Extended steganographic system", 8th International Student Conference on Electrical Engineering, FEE CTU 2004, Poster 04.

[10] Nameer N. EL-Emam, "Hiding a large amount of data with high security using steganography algorithm", Journal of Computer Science, Page(s): 223 – 232, April 2007.

[11] S.K.Bandyopadhyay, Debnath Bhattacharyya, Poulumi Das, S. Mukherjee, D. Ganguly, "A Secure Scheme for Image Transformation", IEEE SNPD, pp. 490-493, August 2008.

[12] V.M. Potdar, S. Han and E. Chang, Fingerprinted secret sharing steganography for robustness against image cropping attacks, in: Proceedings of IEEE 3rd International Conference on Industrial Informatics (INDIN), Perth, Australia, 10-12 August 2005, pp. 717-724.

[13] M.H. Shirali-Shahreza and M. Shirali-Shahreza, A new approach to Persian/Arabic text steganography, in: Proceedings of 5th IEEE/ACIS International Conference on Computer and Information Science (ICISCOMSAR 2006), 10-12 July 2006, pp. 310-315.

[14] J. Fridrich, M. Goljan and D. Hogeg, steganalysis of JPEG images: Breaking the F5 algorithm, in: Proceedings of Information Hiding: 5th International Workshop, IH 2002 Noordwijkerhout, The Netherlands, LNCS, Springer, October 7-9, 2002, 2578/2003, pp. 310-323.

[15] Simmons, G., "The prisoners problem and the subliminal channel", CRYPTO, 1983

[16] Chandramouli, R., Kharrazi, M. & Memon, N., "Image steganography and steganalysis: Concepts and Practice", Proceedings of the 2nd International Workshop on Digital Watermarking, October 2003

[17]Anderson, R.J. & Petitcolas, F.A.P., "On the limits of steganography", IEEE Journal of selected Areas in Communications, May 1998

[18]Johnson,N.F.&Jajodia,S.,"Exploring Steganography: Seeing the Unseen", Computer Journal, February 1998

[19] Krenn, R., "Steganography and Steganalysis", http://www.krenn.nl/univ/cry/steg/article.pdf

[20]T. Morkel [1], J.H.P. Eloff [2], M.S. Olivier [3], "AN OVERVIEW OF IMAGE STEGANOGRAPHY" , Information and Computer Security Architecture (ICSA) Research Group, Department of Computer Science, University of Pretoria, 0002, Pretoria, South Africa

[21]Andreas Westfeld[1] and Gritta Wolf[2] , "Steganography in a Video Conferencing System" , 1 Institute for Theoretical Computer Science, 2 Institute for Operating Systems, Databases and Computer Networks, Dresden University of Technology, Germany.

[22]Syed Ali Khayam, "The Discrete Cosine Transform (DCT): Theory and Application", Department of Electrical & Computer Engineering, Michigan State University, March 2003

[23]Mr C Rafferty, :Steganography & Steganalysis of Images" , Msc Comms Sys Theory 2005

[24]Christian Cachin , "An Information-Theoretic Model for Steganography" , India, March 4, 2004.

[25]Yarmolik, V. N.& S. N Demidenko, " Generation and Application of Pseudo Random Sequences for Random Testing " , John Wiley & Suns, 1988.

[26]Serberry, Jennifer and Joserf Pieprzyk, " Cryptography, An Introduction to Computer Security", Prentice Hall, 1989.

[27]Schneier, Bruce, " Applied Cryptography, Protocols, Algorithms, and Source Codes in C" , Second Edition, John Wiley & Sons, 1996.

[28]William Stalling, " Cryptography and Network Security Principle and Practices, Fourth Edition", Prentice Hall, November 16, 2005.