

## Copyright protection using non linear forward feedback shift register and error-correction technique

**Dr. Navin Rajpal, Anil Kumar\*, Sureka Dudhani\*\* and Pravesh Raja Jindal\*\*\***

Reader , SIT, Guru Gobind Singh Indraprastha University, Delhi, INDIA

(Phone: 23862856 (O); 27056154 (R), 9811489759(mob))

[Navin\\_rajpai@yahoo.com](mailto:Navin_rajpai@yahoo.com)

\*Lecturer, IT Deptt, Bharati Vidyapeeth College of Engg, A-4, Pacschim Vihar, Delhi-110063, INDIA. (Tel 01276210841)

[Dahiyaanil@yahoo.com](mailto:Dahiyaanil@yahoo.com)

\*\*Reader, Electrical Deptt, Bharati Vidyapeeth College of Engg, A-4, Pacschim Vihar, Delhi-110063, INDIA.

[Sureka65@rediffmail.com](mailto:Sureka65@rediffmail.com)

\*\*\*IT Deptt, Bharati Vidyapeeth College of Engg, A-4, Pacschim Vihar, Delhi-110063, INDIA. (Phone: 27673891(R), 9891550700(mob))

[Pravesh\\_raja@yahoo.com](mailto:Pravesh_raja@yahoo.com)

### ABSTRACT

In this paper we are suggesting a method of Copyright Protection with incorporated techniques of Error Correction Coding, Steganography, NLFFSR (Non Linear Forward Feedback Shift Register). The Aim of this suggested technique is to make Steganography a perfect tool for secure Copyright Protection. The technique of Error Coding is made impeccable by using the Block Error Detection and Correcting Codes and Duplication of Bits. The error coding applied on the pseudo random binary sequences generated by NLFFSR (which has best randomness and statistical properties) is incorporated in the Steganography. The data stream is hidden in the digital image by using the LSB (Least Significant Bit) technique. This technique ensures minimum bit changes in the image and hence it is far more difficult to trace out that the image has a secret Copyright hidden in it, even if one makes out that a secret information is hidden the data cannot be retrieved because it is processed significantly before embedding. Thus the whole aim of this paper is to demonstrate use of Error Correction Coding and NLSFFR in the field of Steganography to make it a perfect tool with foolproof method, so

that it can be used more usefully in Copyright in Maps.

**Key word:** NLFFSR, LSB technique, Error Correction Coding, Steganography, Copyright, Cryptography.

### 1. INTRODUCTION

The Steganography consists of techniques to allow the communication between two persons, hiding not only the contents but also the very existence of the communication in the eyes of any observer. These techniques use a second perceptible message, with meaning disjointed by the secret message. This second message works as a "Trojan horse", and is a container of the first one [1-2]. 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 are excellent candidates to turn into containers of textual messages, since the bits of a secret text message can be superimposed, as slight noise, to the bits employed for coding a digital image. In fact, the first ones are usually much less than the second

ones. Historically, the first instance of the use of Steganography is found when the Greeks received warning of Xerxes hostile intentions from a message underneath the wax of a writing tablet [3].

**2. NON LINEAR FORWARD FEEDBACK SHIFT REGISTER?**

A Non-Linear feedback shift Register (NLFFSR) is a mechanism for generating binary sequences [7]. Figure 1 shows a general model of an n-bit NLFFSR. It is a Non linear forward feedback shift register with a feedback function f.

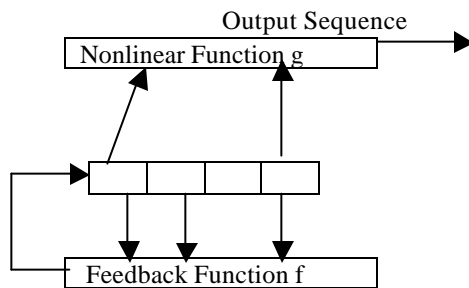


Figure 1

**3. PSEUDO RANDOM BINARY SEQUENCE GENERATION USING NLFFSRS**

NLFFSR are extremely good pseudorandom binary sequence generators [8, 9,10, 11]. 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  $a_{n-1}.a_{n-3} (+) a_{n-2}.a_{n-4}$  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. The usefulness of the sequences such as derived above 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. Now suppose we want to hide the letter 'A' in the Image first we will crypt it with the secret key stream generated by our register. Suppose the binary value of 'A' is 10000011 in any code and our generated key stream is 01111100000, we XOR this two bit streams to get the cryptic bit stream 00000000(Cryptic value of 'A'). Now our next aim would be to error protect this bit stream and hide this in digital image.

**4. HOW TO ERROR PROTECT THE DATA**

To handle the errors during the transmission of data we error code the data so that even if the data is distorted when it reached at destination it can be recovered fully. This error can be introduced by the noise in the transmission media or even the active intruder who may suspect there is some data hidden and want that the intended recipient doesn't get the desired message may introduce it intentionally. In the copyright protection of the Images this phase becomes more important as the Image can be modified or distorted to make sure that the owner does not recognize or claim the ownership of his Image. In this process we first duplicate each bit 8 times and then apply error detecting and correcting code to this duplicated bit sequence. This may well mean that the copyright will take much more space than it should ought to take but the importance of the data we are hiding in the Image makes it a requirement for the success of this Technique. To simply illustrate the error coding process we take single occurrence of each bit.

D <sub>7</sub>	D <sub>6</sub>	D <sub>5</sub>	R <sub>4</sub>	D <sub>3</sub>	R <sub>2</sub>	R <sub>1</sub>
----------------	----------------	----------------	----------------	----------------	----------------	----------------

**R: Redundancy Bits**

**D: Data Bits**

To error code the data we use the concept of the redundancy bits, to enhance the performance of the error coding we use three redundancy bits to error code 4 data bits. The redundancy bits are interspersed with the original data bits; these bits are placed in positions 1,2,4 and 8(powers of 2). Each redundancy bit is the VRC bit for one combination of data bits.

R<sub>1</sub>: Bits 1,3,5,7

R<sub>2</sub>: Bits 2,3,6,7

R<sub>4</sub>: Bits 4,5,6,7

#### **4.1 Calculating R values**

In first step, we place each bit of the original data in its appropriate place in the 7bit unit. Then we calculate the even parity for the various bit combinations. The parity value for each combination is the value of the corresponding R bit. The value of the cryptic 'A' is 00000000. Now we will apply the error code in it first taking the first 4 bits and then applying the steps we just mentioned we get a seven bit error coded data as 0000000. Now again to the next 4 bit we do the same and get another seven bit coded data as 0000000. So the cryptic 'A' has become 0000000 0000000 after error coding.

#### **4.2 Error Detection & Correction**

Now imagine that by the time the above transmission is received a error in the bit has occurred. The receiver recalculates four new VRC using the same sets of bits used by the sender plus the relevant parity(R) bit for each set. Then it assembles the new parity values into a binary number in order of r position ( $R_4R_2R_1$ ). Now the decimal value we get is the precise location of the bit in error. Once the bit is identified, the receiver can reverse its value and correct the error. Now after the bit sequence has been recovered we compress the bit sequence which we have duplicated 8 times, during error coding. We may find that many bits in the block of 8 bits have changed, so we compress this block to a value which is in majority in the block. This makes our error coding technique very robust and useful.

### **5. HOW THE STEGANOGRAPHY WORKS**

The design principle of steganographic systems is based on the premise that most communication channels – such as telephone lines and radio broadcasts – transmit signals accompanied by some kind of noise [4, 5]. This noise can be replaced by a transformed secret signal indistinguishable from the noise without the secret key. In this way, the secret signal can be transmitted undetected. In the same way hiding data in an image requires two files. The first file, called the “cover-image”, will be the innocent looking image that holds the hidden information. The second file will contain the information to be hidden. When combined, the two files will generate a “stego-image”. There exists a number of ways to create a stego-image from the given cover-image and the data to be hidden. These include least significant bit (LSB) insertion,

masking and filtering, redundant pattern encoding, and other spread spectrum methods [4, 5, 6].

### **6. INCORPORATING THE CRYPTED AND ERROR CODED BINARY SEQUENCE IN THE IMAGE**

The amount of data that can be hidden in the Image directly depends on the size of the image. To a computer, an image is an array of numbers that represent light intensities at various points (pixels). Digital Images are generally stored as pixels color information with a particular header telling how the image should be read and interpreted. We leave the header as it is and modify the pixel's color information bits. The amount of the color information stored for each pixel depends upon the color depth of the image. The bit stream is hidden in the Image using the LSB insertion technique.

### **7. SUMMARY AND CONCLUSION**

In this paper, we have presented a review of the field of Steganography and concentrated on improving the security of the data hidden by first encrypting data by strong encryption mechanism using NLFFSR and then further error coding it for much improved security. After it we hide this data in the image using the LSB insertion technique. This technique of hiding secret information is highly safe and reliable to hide the Copyright in the Images. By choosing the best techniques of different fields we achieve the best security in the method of Steganography to hide Copyright. Illustration of this Technique using a Image of a sample map.

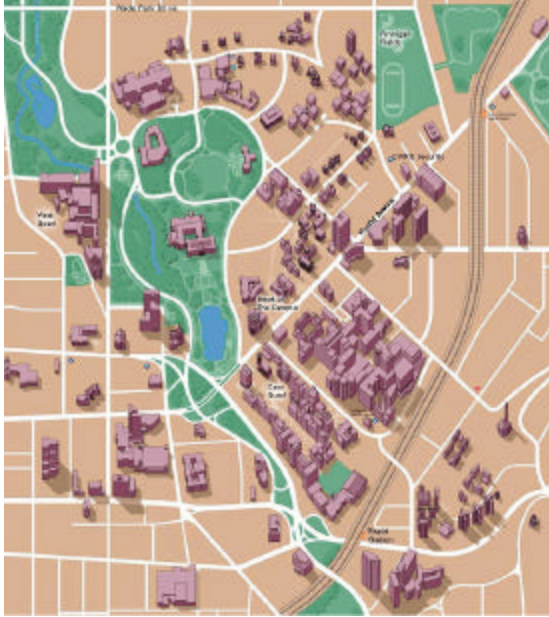


Figure 2 : A sample cover Image.



Figure 4: The stego-image after distorting the image

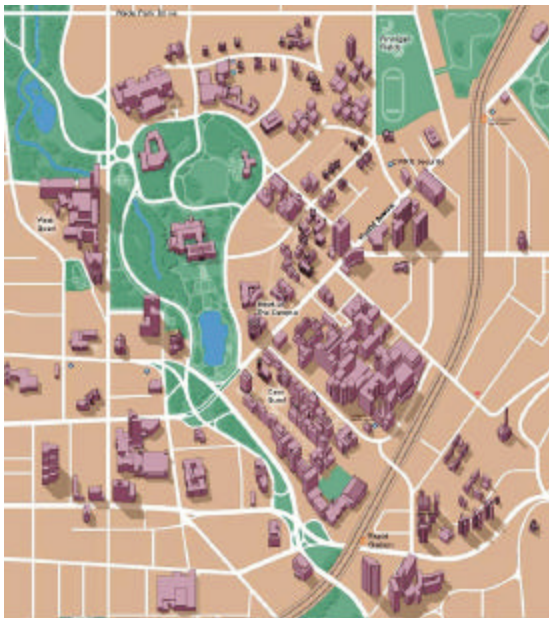


Figure 3: The stego-image after hiding The Text

## 8. REFERENCES

- [1] W. Bender, D. Gruhl, N. Morimoto, A.Lu, "Techniques for data hiding. IBM systems Journal, Vol. 35 , no. 3-4, 1996. p313-336.
- [2] N.F. Johnson and S. Jajodia, "Exploring Steganography: Seeing the Unseen," IEEE computer, Vol. 31, No. 2, February 1998, pp. 26-34.
- [3] 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
- [4] N. F. Johnson and S. Jajodia, "Steganalysis: The Investigation of Hidden Information," Proceedings of IEEE Information Technology Conference, 1998
- [5] 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.
- [6] H.K. Pan, Y.Y. Chen, and Y.C. Tseng, "A secure data hiding scheme for two color images," Proceedings of the 5<sup>th</sup> IEEE Symposium on Computers and Communications, 2000, pp. 750-755.
- [7] 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.
- [8] A. Ahmad and A. M. Elabdalia, "An efficient method to determine linear feedback connections in the shift registers that generate maximal length

pseudorandom up and down binary sequences”,  
Journal of Computer & Electrical Engineering, Vol.  
23, No.1, 1997, pp. 33-39.

[9] A. Ahmad, M. J. Al-Musharafi, S. Al-Busaidi,  
“A new algorithm procedure to test m-sequences  
generating feedback connections of Stream cipher’s  
LFSRs,” Proceedings of the IEEE TENCON’2001,  
August 2001, pp.366-369.

[10] B. Schneier, Applied Cryptography, Second  
Edition, 1995, John Wiley and sons.