ISSN: 2277-3754
International Journal of Engineering and Innovative Technology (IJEIT)
Volume 1, Issue 1, January 2012

A NEW STEGO-SYSTEM BASED ON LFSR GENERATOR

Sunil Kumar Muttoo, Ismael Abdulsattar
skmuttoo@cs.du.ac.in, asmaell_sj@yahoo.com

Abstract— In this paper we will introduce a new design for a random key generator as a new technique to implement steganography. The proposed algorithm is LFSR-based stream cipher. The simplicity of the design derived from using of four small LFSR, three XOR gates, and a single 3 to 1 multiplexer on the content of an 8-stage LFSR. The sequence (result) from that generator will used as map (secret key) for selection the target place, within the pixel of the cover image itself as well as to encrypts the secret message. The selection of the cover itself not only based on statistical criteria, but also adaptive learning model. Because we have to optimize the selection of the image from huge database and allow hash function (md5) to play role in mapping inside every band.

Index Terms—**Steganography, linear feedback shift registers (LFSR), Hash function (MD5).**

I. INTRODUCTION

Information hiding represents a class of processes used to embed data into various forms of digital data such as image, audio, and video. In digital images the information hiding applications could be divided into two groups depending on the relationship between the embedded message and the cover image [1].The first group is formed by steganography application in which the message has no relationship to the cover image and the cover image plays the role of a decoy to mask the very presence of communication. The content of the cover image has no value to the sender or the decoder.

In this typical example of a steganographic application for covert communication, the receiver has no interest in the original cover image before the message was embedded. Thus, there is no need for lossless data embedding techniques for such applications. The word steganography comes from the Greek name "steganos" (hidden or secret) and "graphy" (writing or drawing) and literally means hidden writing. Steganography uses techniques to communicate information in a way that is hidden [2], [3].

The second group of applications is frequently addressed as digital watermarking. In a typical watermarking application, the message has a close relationship to the cover image. The message supplies additional information about the image, such as image caption, ancillary data about the image origin, author signature, image authentication code, etc. While the message increases the practical value of the image, the act of embedding inevitably introduces some amount of distortion [5].Both steganography and watermarking describe techniques that are used to imperceptibility convey message by embedding it into the cover image. But steganographic methods are interested in extracting the message, so usually it’s not robust against modification of the image. Watermarking, as opposed to steganography, is used for authentication and has the additional requirement of robustness against possible attacks [6], [7].

A. Linear feedback shift register (LFSR)

A shift register whose input bit is a linear function of its previous state. The most commonly used linear function of single bits is XOR. Thus, an LFSR is most often a shift register whose input bit is driven by the exclusive-or (XOR) of some bits of the overall shift register value [4].The initial value of the LFSR is called the seed, and because the operation of the register is deterministic, the stream of values produced by the register is completely determined by its current (or previous) state. Likewise, because the register has a finite number of possible states, it must eventually enter a repeating cycle.[8] However, an LFSR with a well-chosen feedback function can produce a sequence of bits which appears random and which has a very long cycle.

B. Applications of LFSRs [4], [5].

- Generating pseudo-random numbers.
- Generating pseudo-noise sequences.
- Fast digital counters.
- The mathematics of a cyclic redundancy check, used to provide a quick check against transmission errors, are closely related to those of an LFSR.
- Cryptography
- Now we use it in steganography.

II. PROPOSED RANDOM KEY GENERATOR

We have here four LFSR that we will use as random key generator to provide the map that implements the information hiding. The Figure 1 shows the main component of this generator. The random key generator consists of two parts: the driving part and the combining part. The driving part consists of three LFSR's of length 29, 30, 31 stages for each. The tapping stages are (31, 3), (30, 23), (29, 27), each of these feedback functions produce a maximal period. These registers are initialized using a special procedure will be explained later. The combining part consists of a single LFSR of length 8 stages with a feedback function defined by the tapping (8, 5, 3).

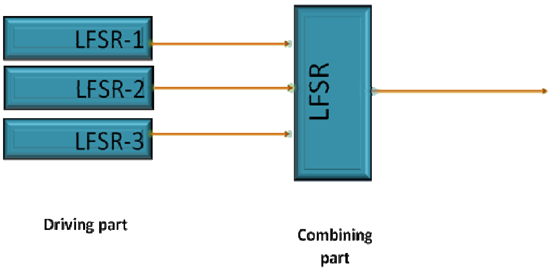

Fig.1. Component of Generator

A. Initialization Procedure

The proposed generator is consists of four LFSR's of lengths 31, 30, 29 (the driving part), LFSR (the combining part), which means that there are 98 stages need to be initialized before the generator start working. The initialization procedure starts by reading fourteen character as seed key (or secret key) of the random generator. Each character is converted to its ASCII value (7 bits), the result is 98 bits fed the LFSR's 32, 30, 29 and 8 respectively.

B. Generator work

After the initialization procedure work the generator will be ready to produce the semi-random output keys. The driving part produce three bits (b0, b1, b2), one from each LFSR (as shown in figure). The output of the driving part is fed to the combining part as an address calculated by the following formula:

$$adr = b0 + b1 * 2 + b2 * 4$$

The value adr is used as an address to address on the combining part as shown in Figure 2:

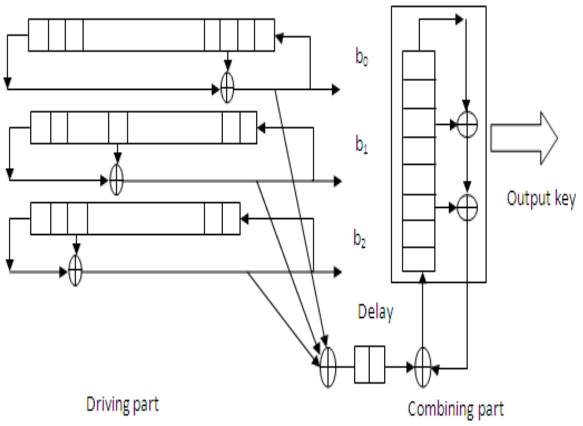

Fig.2. Addr Part of Generator

C. Proposed algorithm

1. Read the image (cover) pixels values.
2. Divide the cover image into set of groups (2x 8) pixel.
3. Separate the R, G and B band of each pixel.
4. Extract hash value (MD5) for the red band for the odd (blocks-1) the final odd block will contain the secret message length.
5. Use MD5 values to determine the selected pixel for each block.
6. Read a seed key (k) of size 14 characters
7. Encrypted seed key (k)using (max interval algorithm) to get secret key ,sk such that sk=E(k), where length (sk)=length(k)
8. Code secret key (sk) into binary of 7 bit representation of each char (14*7=128 bit)
9. Feed all LFSRs with length of 31, 30, 29, and 8 respectively.
10. Turn on the generator and on each turn we obtain three bits (b0, b1, b2) from the driving part that used to addressing Combining part by the Equation.
.
$$adr = b0 + b1 * 2 + b2 * 4$$
11. Grasp the bit which addressed by adr from the combining part and store it in one dimensional array (oput).
12. Generator will stop when we reach length (oput) x3, because every three bit will from oput will use to hide one bit from the secret message.
13. Divide oput into blocks of three bits, and get the mapping using the following equation.

$$adropt = (t0 + t1 * 2 + t2 * 4) \, mod \; 3$$

14. Use the adropt value to find which one of the three LSB will use as place for embedding.

III. TEST SAMPLES

Some of text files and audio files were used as test samples to study the performance of the suggested system. The specifications of the test text files are shown in Table (1). The specifications of the cover images files are shown in Table 2.

Table 1 the tested text samples

Name	Size (KB)	Forma t	Data Type
Text1	55.1	TXT	Text
Text2	48.4	TXT	Text
Text3	7.35	TXT	Text

Table 2 the tested cover image samples

Name	Size (pixel)	Format	Data Type
Test1	512X512	BMP	Image
Test2	512X512	BMP	Image
Test3	300X300	BMP	Image

IV. Measurement Quality After Hiding

To measure the quality of the stego-image we apply objective and subjective measurement on the selected images as shown in the following Table 3.

Table 3 the tested cover image samples

Selected cover	Selecte d text file	PSNR	Subiective Measurement
Test1	55.1	61.7315	Perceptual (no difference visible)
Test2	48.4	64. 450463	Perceptual (no difference visible)
Test3	7.35	69.2180 6	Perceptual (no difference visible)

V. Conclusion

The main conclusions from designing and implementation of the proposed system are:

1- The automatic proposed hiding system deals with people who have not skill in computer sciences.

2- By using hiding method and extracted the message at the receiver site, we guarantee the secure communication between sender and the recipient.

3- By using encryption and decryption method we can provide more security to the proposed system.

4- The size of the secret message is very important role invisibility of stego image.

5- The complexities of the LFSR, MD5 increase the security level.

6- The objective quality measurement is preferred on the subjective measurement due to the randomness of LFSR sequence.

VI. Future Work

There are some suggestions for future work which can be taken to improve the proposed system. These suggestions are:

1. Encryption of the secret message by using other encryption methods can also be used for future increase the security of hiding algorithm.
2. Apply fuzzy logic and build optimization function to select the proper image from huge database.
3. Improvement of the proposed system to deal with the other types of image such as JPEG, GIF, etc.
4. Developing the proposed system by using new technique to hiding secret message data to replace the LSB technique such as DCT technique.

References

[1] Katzenbeisser S. and Petitcolas F., "Information Hiding Techniques for Steganography and Digital Watermarking", Artech House, USA, 2000.

[2] Jonathan. C, Patrick .D, Samuel .L and Robert .P, “Steganography and Digital Watermarking ", University of Birmingham, School of Computer science, URL: http://www.gnu.org/copyleft/fdl.html, 2004.

[3] Stefano Cacciaguerra and Stefano Ferretti, "Data Hiding: Steganography and Cryptography Marking", Department of computer science, university of Bologna, 2000.

[4] Eric Cole, "Hiding in Plain Sight: Steganography and the Art of Covert Communication", Wiley Publishing, Canada 2003.

[5] Alexia .B, Panagiotis. T and Athanasios .s, "Hiding Message in Heavy-Tails: DCT-Domain Watermarking Detection Using Alpha- Stable Models”, IEEE Transactions on Multimedia, June 2003.

[6] Mohanty Saraju P.,"Digital Watermarking A Tutorial Review", University of South Florida Tampa, FL 33620, 1999

[7] Nameer N. EL-Emam "Hiding a Large Amount of Data with High Security Using Steganography Algorithm" Applied Computer Science Department, Faculty of Information Technology Philadelphia University, Jordan, 2007.

[8] Shin, N, "One-time Hash steganography", Information Hiding, Third International Workshop, Lecture Notes in computer. Science vol. 2000.

AUTHOR BIOGRAPHY

Dr. Sunil Kumar Muttoo is Associate Professor in Department of Computer Science in University Delhi. He completed Mtech from Computer Science and Data Processing from Department of Mathematics, Delhi University in 1990.Currently he is Reader in computer Science department. His Research area of Interest is Information Security. He has published more than 50 Research Papers in

National or International Journals or Confernces.He is Life Member of CSI and India member of association for computing Machinery, USA.

ISMAEL ABDULSATTAR JABBAR is Member of staff (Assistant programmer) in the Computer Science Department at Al-Mustansiriyah University and Chairman of the Training and Development Committee in The Iraqi Association for Information Technology and He is Member of Iraqi Programmer Union and Member of Iraqi association of information technology. he has published more than 07 Research Papers in National Or International Journals or Conferences.