International Journal on Applications in Information and Communication Engineering
Volume 1: Issue 4: April 2015, pp 56-59. www.aetsjournal.com ISSN (Online) : 2394-6237

A Secured Video Steganography by Linear Feedback Shift Register Method

Rajpreetha C, Haripriya C, Vanitha Lakshmi M

***Abstract*—** In this paper, the secret message are directly hidden in an specific frame of the original video in a random order with the help of key values. This key values is generated by using linear feedback shift register method. Further to increase the security level by applying Advanced Encryption Standard (AES) algorithm to the stego video to get the result of Encrypted stego video. This proposed method is tested by using two parameters such as Mean Squared Error (MSE) and Peak signal to noise ratio (PSNR) value.

***Keywords*—** LFSR, stego video, key values, random order, AES algorithm

I. INTRODUCTION

Currently, the hacking activities are increasing day by day and attackers can easily hack the secret information and security is not sufficient to stop this problem. Although the stature of the security is on improving at the higher levels, the major significance is security cost. So, a unique technique is needed which is more efficient and provides a better security level with lower cost [1,2]. For this reason, the steganography concept is used. The goal of Steganography method is to hide the secret message within another digital medium such as image, audio, text or video [3]. Steganography is adapted from the Greek word *Steganosgraphia* which means "hidden or covered writing" [4].

Most papers prefers to hiding data in the image, or audio or text. But in this paper preferring to hide the data in a video. Instead of embedding the secret message in separate image, we present a .avi video and embedding the secret message in specific frame of the input video. The video file along with hidden information should not be predicted by hacker [5].

II. BASIC MODEL OF VIDEO STEGANOGRAPHY

The basic model of Video Steganography consists of a cover video (It used to hold secret data inside), the secret text (the secret text that is to be sent), hiding method (It used to hide secret text inside carrier file and produce the result is Stego-file) and an Encryption algorithm (the procedure is to encrypt Stego-file). The result of the process is the Encrypted Stego file which is the encrypted digital video that has the secret message hidden inside. Encrypted Stego-file is sent to the receiver via communication channel.

Rajpreetha C,PG Scholar, Department of ECE,S.A Engineering College, Poonamallee-Avadi Main Road, Veeraraghavapuram, Thiruverkadu Post, Chennai-600 077 ,India (e-mail:rajpreetharul@gmail.com)

Haripriya C, Assistant Professor, Department of ECE, S.A Engineering College, Poonamallee-Avadi Main Road, Veeraraghavapuram, Thiruverkadu post, Chennai-600 077, India (e-mail:haripriya@saec.ac.in)

Vanitha Lakshmi M, Assistant Professor, Department of ECE, S.A Engineering College, Ponamallee-Avadi Main Road, Veeraraghavapuram, Thiruverkadu post, Chennai-600 077, India (e-mail: vanithahitesh08@gamil.com)

A. Secret Text Hiding Process: The flowchart of secret text hiding process is shown in Fig.2 and the explanation of this secret text hiding process as shown below

1. Extract video frames from the original video and generate text files for corresponding all frames which is having only pixel values.
2. Choosing the specific textfile (i.e. 1st textfiles) as input cover image. Next, the secret message is hidded into specific frame of the textfile in a random order based on key values. These key values is generated by using Linear Feedback Shift Register (LFSR) method.
3. This Stego frame and un-embedded Frames i.e. the other frames are combined together to form a Stego video.
4. At last the AES encryption algorithm is applied to that Stego video which produce the output result is Encrypted video with hidden data.

B. Key Generation

Using LFSR method to generate the sequences of key values. The LFSR consists of two parts: a shift register and a feedback function. Initially, when the flip-flops outputs are loaded with a seed value (anyone except all zeros, because it cause the LFSR to provide all zero patterns) and every clock pulses it will generate a pseudo random sequences of ones and zeros. The shift register is initialized with n bits and each time a bit is required, all the bits in the register are shifted 1 bit to the side of right. So the least significant bit is called as the output bit. The most significant bit is calculated by the Exclusive-OR of certain bits in the register [6-8]. It can produce up to 2^n-1 bit-long pseudorandom sequence (referred to as the period) before repeating.

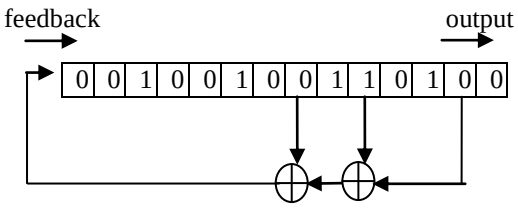


Fig.1 14-bit LFSR

In this paper, the key values is generated by using 14-bit LFSR is shown in Fig.1. The sequences are 00100100110100 (0934), 10010010011010 (149a), 01001001001101 (124d), etc. The initial value (0934) of this sequences is represented as seed value. Sequentially the first '3' bit from all sequences indicated as decimal value separately. The decimal value for the seed value is "4".

Decimal values for other sequences are 2,5,6,etc. The hiding process are done in two ways such as

1) With the help of Pseudorandom sequence to determine/ represent the location number of pixel used to hide data.

2) Hiding data in chosen pixel by using decimal values.

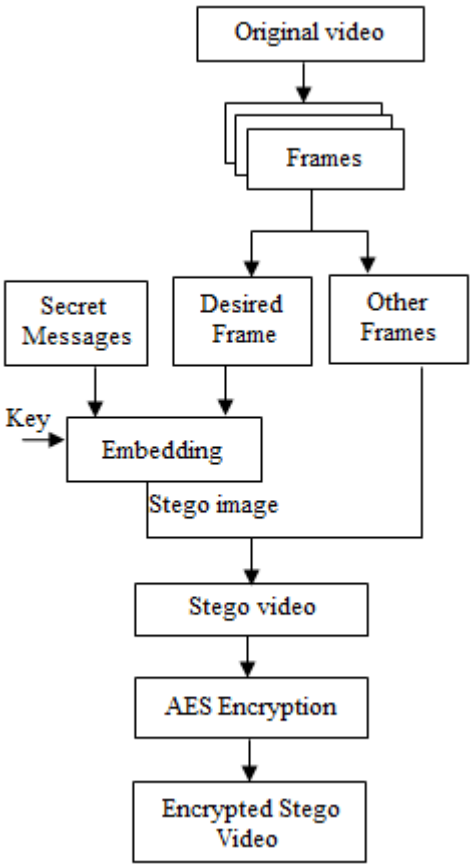


Fig. 2 Flowchart of secret text hiding process

C. Advanced Encryption Standard (AES) Algorithm

AES algorithm is used to encrypting the carrier file for making it not readable and secure. The AES-128 is a block oriented symmetric key encryption algorithm, which will works on a 128 bit input plaintext at a time and uses a 128 bit length key. The 128 bit input plaintext is divided into 16 bytes and then arranged into a 4*4 matrix (column wise). This is the State matrix [9,10]. The conversion of 128-bit input key into key matrix as like conversion of input data to state matrix. Both these matrices should produce the necessary inputs to the AES algorithm for 1st round. The AES algorithm consists of an initial round (0), nine general rounds (1to 9) and a final round (10). In round zero the two matrices (state matrix and key matrix) are simply X-ored under AddRoundKey transformation. The output of Round 0 is given as the input to the Round1. Any general round is composed of four distinct uniform and invertible transformation: Sub Bytes, Shift Rows, Mix Column and AddRoundKey. The final round follows the same procedure of general round except that Mix Column is neglected. The Sub Keys needed for all the rounds from Round1 to Round 10 are derived from the original 128-bit key provided. After finishing all the ten rounds the output is 128 bits, which is the encrypted output.

1. *Sub Bytes*: Operates in each byte of the state independently. Each byte in the s-box is replaced by the corresponding byte in the S-box.
2. *Shift Row:* Cyclically shifts the rows state over different offsets.
3. *Mix Column:* In this operation, the column state are initialized as polynomials over GF(2^8) and are multiplied with a fixed polynomial. The mix column component is neglected in the last round of the algorithm.
4. *AddRoundKey:* Involves bitwise XOR operation.

III. EXPERIMENTAL RESULTS AND EVALUATION OF PROPOSED METHOD

The input video is considered as "traffic" in .avi format (160x120 dimensions) at the frame rate of 6frames/second of 101KB size is used for simulation for both LSB technique and Proposed method. And also extracting and saving of video frames from input video for both techniques is generated through MATLAB. Totally input video having 10 frames.

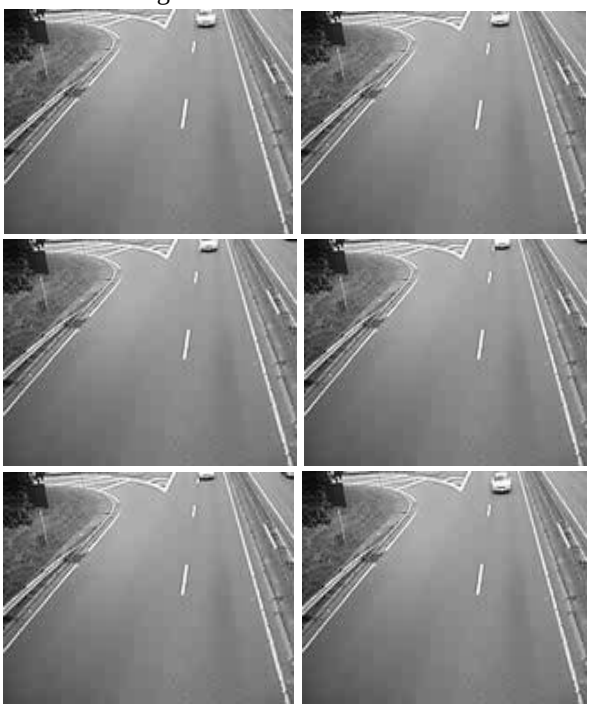


Fig. 3 Input video frames

Due to space limitations, we don't list the results of all frames. The first 6 frames are shown in below Fig.3. LSB method have been implemented in MATLAB but proposed method have been implemented in both MATLAB and Modelsim software because of using Linear feedback shift register method.

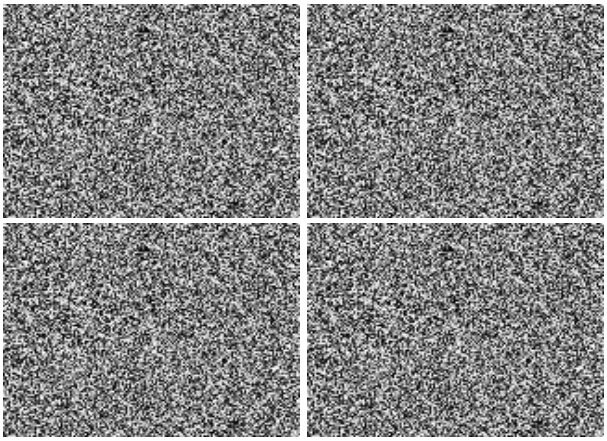
Using least significant bit (LSB) method to hide a secret message i.e. SA ENGINEERING into 1st frame of the video. The frame along with hidden information is referred as stego frame. The cover frame and stego frame is shown in Fig 4

Fig. 4 1st Frame (before hidding) and stego frame (after hiding)

Using LFSR method to generate the memory addresses and random order. The corresponding binary values for the secret message of "SA ENGINEERING" is {00100000010100110100000100100000010001010100111 00100011101001001010011100100010101000101010100100100100101001110010001110010000} is used to hide in 1st frame of the text files. The memory address are 00100100110100 (0934), 10010010011010 (149a), 01001001001101 (124d), etc. This memory addresses having individually the pixel values are 01110110, 10010101, 01100011. The random order is 4,2,5, etc. Data hiding in 1st frame is shown in Table I.

TABLE I
DATA HIDING IN 1ST FRAME

Memory Address	Pixel values	Random order	Secret Data	Before hiding	After hiding
0934	01110110	4	0	011**1**0110	011**0**0110
149a	10010101	2	0	10010**1**01	10010**0**01
124d	01100011	5	0	01**1**00011	01**0**00011
2926	01101001	6	0	0**1**101001	0**0**101001
3493	01101100	3	0	0110**1**100	0110**0**100
1a49	01011111	1	1	0101111**1**	0101111**1**



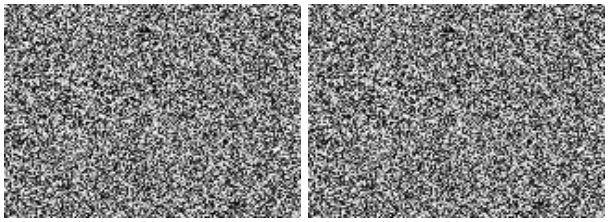


Fig. 5 Encrypted stego frames

After hiding all secret data in desired text file and then encrypting this text file through Model Sim6.4a. Other frames have a similar effect of encryption is done to increase the security level. This encryption step is not doing in LSB method. Then, all this text file is converted to images through MATLAB is depicted in Fig. 5. After that combining all frames to make a Encrypted stego video.

Then we test the stego images by Peak Signal to noise ratio (PSNR) parameter is shown in Table II. The image quality measure of PSNR is defines as the ratio of maximum power of a signal to the power of corrupting noise that affects the fidelity of its representation. It is expressed in decibel scale. If the PSNR value is greater than forty five for a stego image then we can treat as a good quality image.

TABLE II
COMPARISON RESULTS BETWEEN LSB AND PROPOSED METHOD

Stego image	LSB Method		Proposed Method	
	MSE	PSNR (dB)	MSE	PSNR (dB)
1st frame with hidden data	0.0259	63.99	0.0229	64.53

IV. CONCLUSION

A simple method of hiding data in video was created and implemented successfully, which it makes difficult to identify the presence of hiding data. Performance analysis of the developed technique have been evaluated by comparing it with simple LSB technique, which have resulted a very good MSE and PSNR values for the stego images. The overall experimental results have shown that the proposed method can preserve the video file size and makes our technique more secure and efficient.

REFERENCES

[1] Ankit Chaudhary, J.Vasavada, J.L.Raheja, S.Kumar, M.Sharma, "*A Hash based Approach for Secure Keyless Steganography in Lossless RGB Images*", 22nd International Conference on Computer Graphics and Vision, 2012.

[2] Kousik Dasgupta, J.K. Mandl. Paramartha Dutta, "*Hash Based Least Significant Bit Technique for Video Steganography (HLSB)*", International Journal of Security, Privacy and Trust Management (IJSPTM), Vol.1, Issue No.2, April, 2012.

[3] Punita meelu, "*AES Asymmetric key cryptographic system*", International Journal of Information Technology and Knowledge Management, Vol.4, 113-117, 2011.

[4] Saurabh singh, "*Hiding Image to Video*", International Journal of engineering science and Technology, Vol.2(12), 6999-7003, 2010.

[5] M.Pavani, S.Naganjaneyulu, and C.Nagaraju, "*A Survey on LSB Based Steganography Methods*", International Journal of Engineering and Computer Science, Vol.2, Issue No.8, 2464-2467, April, 2013.

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

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

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

[9] B. Subramanan, "*Image Encryption based on AES Key Expansion*", in IEEE applied second international conference on emerging application of information technology, 978-0-7695-4329-1/11, 2011.

[10] Hemant Gupta, Dr.Setu Chaturvedi, "*Video Steganography through LSB Based Hybrid Approach*", International Journal of Engineering Research and Development, Vol.6, Issue 12, 32-42, May,2013.