IOSR Journal of Electronics and Communication Engineering (IOSR-JECE)
e-ISSN: 2278-2834,p- ISSN: 2278-8735.
PP 19-23
www.iosrjournals.org

Data Hiding in Audio Signal Using Cryptography and Steganography Techniques

Keerthana.J[1],Kiruthiga .S[1],Kaviya Priya.K[1]S.Navaneethan[2] B.E.,M.E.,
[1]*(Student,Mam College Of Engineering, Tiruchirapalli)*
[2]*(Ap/Ece,Mam College Of Engineering,Tiruchirapalli)*

Abstract :*Information sharing and Transfer has increased exponentially.The information is vulnerable to unauthorised access and so cryptography and steganography techniques used.In cryptography technique informations are scrambled and in steganography technique secret message are embedded into cover medium.Hence in which the data is encrypted as well as the encrypted the encrypted data is hided. This system is to be simulated by Modelsim and synthesized by altera cyclone II fpga.*

Keywords - *cryptography,steganography,cover medium*

I. INTRODUCTION

Secured communication mainly base on cryptography, which encrypts plain text to generate cipher text. However, the transmission of cipher text may easily arouse attackers‟ suspicion, and the cipher text may thus be intercepted, attacked or decrypted violently. In order to make up for the shortcomings of cryptographic techniques, steganography has been developed as a new covert communication means in recent years. It transfers message secretly by embedding it into a cover medium with the use of information hiding techniques.

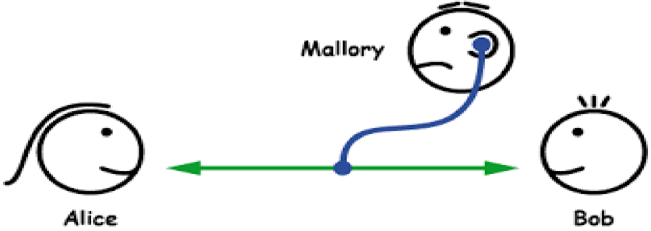


Fig 1: INTERCEPTION

Fig2: STEGANOGRAPHY TECHNIQUE

Cryptography and steganography is a technique aimed at providing the secret communication. By combination of these two techniques the security of secret data increases. In this way encryption here used with pseudorandom key generation technique. Cryptography is the science that studies the mathematical techniques for keeping message secure and free from attacks. Steganography is the art and science of hiding communication. Steganography involves hiding information so it appears that no information is hidden at all.

II. EXISTING SYSTEM

In existing system image is used as a cover medium so that the technique deals with the pixels followings are procedure for image steganography.

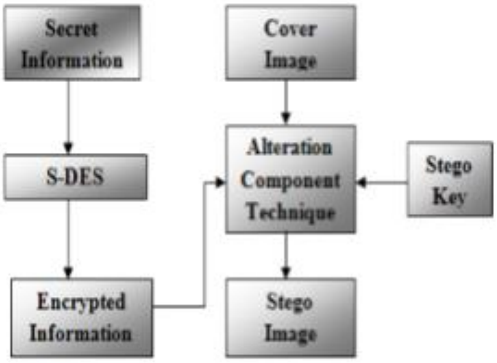


Fig 3: SENDER PROSPECT

The sender's prospect of Proposed Technique in which the secret information is encrypted by using simplified data encrypted standard (SDES) encryption algorithm. Then encrypted message is embedded into cover image by using Alteration component technique. Image containing the secret data is called stego image. Next phase is to select the stego key for encoding. In Embedding process data is hidden by using Alteration component technique in which pixels have been replaced by key and secret message. Firstly key is converted into binary form and its binary form is filled in the first component of first pixels. After then, secret message is converted into binary form and its binary form is filled in first component of next pixels.

Embedding Algorithm

Step (a): Extract all the pixels in the given image and store it in the array called PixelArray.

Step (b): Extract all the characters in the given text file and store it in the array called Character-Array.

Step (c): Extract all the characters from the Stego key and store it in the array called Key- Array.

Step (d): Choose first pixel and pick characters from Key- Array and place it in first component of pixel. If there are more characters in Key- Array, then place rest in the first component of next pixels, otherwise follow step(e).

Step (e): Place some terminating symbol to indicate end of the key. „0" has been used as a terminating symbol in this algorithm.

Step (f): Place characters of Character- Array in each first component (blue channel) of next pixels by replacing it.

Step (g): Repeat step (f) till all the characters has been embedded.

Step (h): Again place some terminating symbol to indicate end of data.

Step (i): Obtained image will hide all the characters that we input.

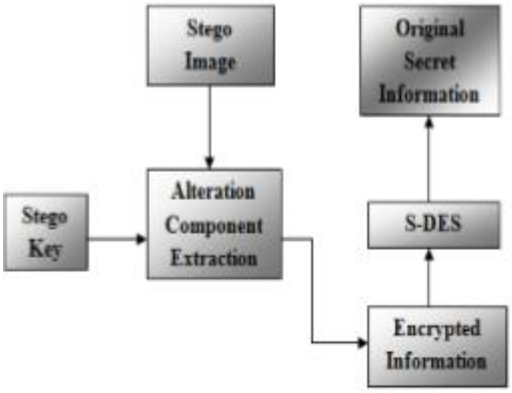


Fig 4: RECEIVER PROSPECT

The receiver's prospect of Proposed Technique in which the sender sends a stego-image to the receiver or legitimate user. The legitimate user having the stego key to extract secret data from stego image. The legitimate user must have the same key with which the image is embedded. On Stego image Extracting process is applied by using Alteration component technique. After data extraction I get the secret message which is in encrypted form. Simplified data encryption standard (S-DES) decryption algorithm is used to decrypt message. Finally we get the Secret Data which is embedded

III PROPOSED SYSTEM

In a proposed system the audio signal is used as a cover medium. In which the LFSR technique is use to generate the pseudo random key. And the data is converted into hexadecimal value for convenience of encryption and where for this conversion hex-editor tool is used to get the value. After encryption the converted value is replace in the least significant bit in audio signal. LSB technique is used with LFSR technique(Linear Feedback Shift Register). A LFSR is shift register whose input bit is linear function of its previous state. The most commonly used linear function of single bits is XOR. In which the initial value is called seed and because the operation of the register is deterministic, the stream of values produced by the register is completely determined by its current state.

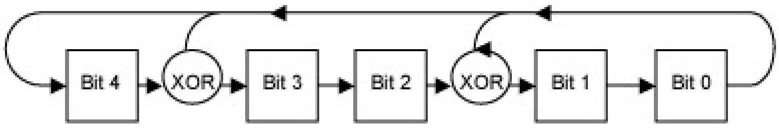


Fig 5:LFSR TECHNIQUE

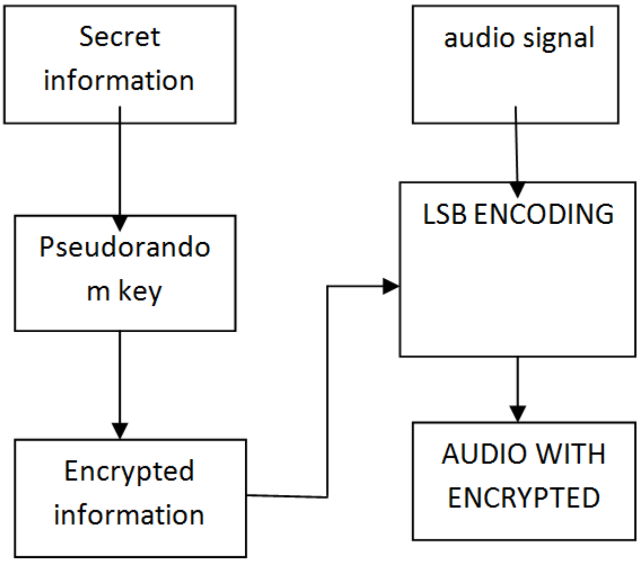


Fig 6: SENDER PROSPECT

In the sender prospect encryption is done by LFSR technique using Verilog program in modelsim software.

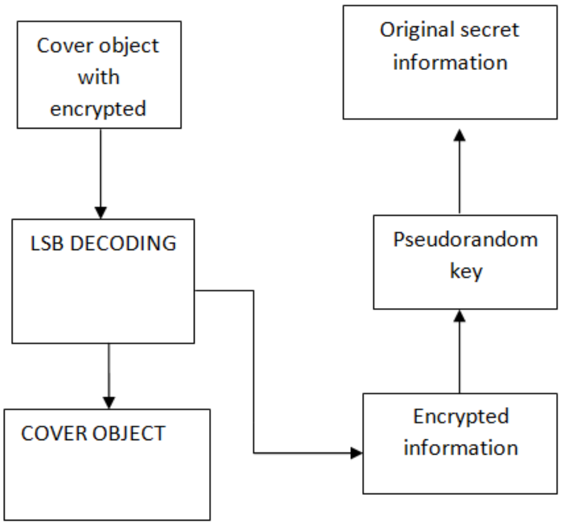
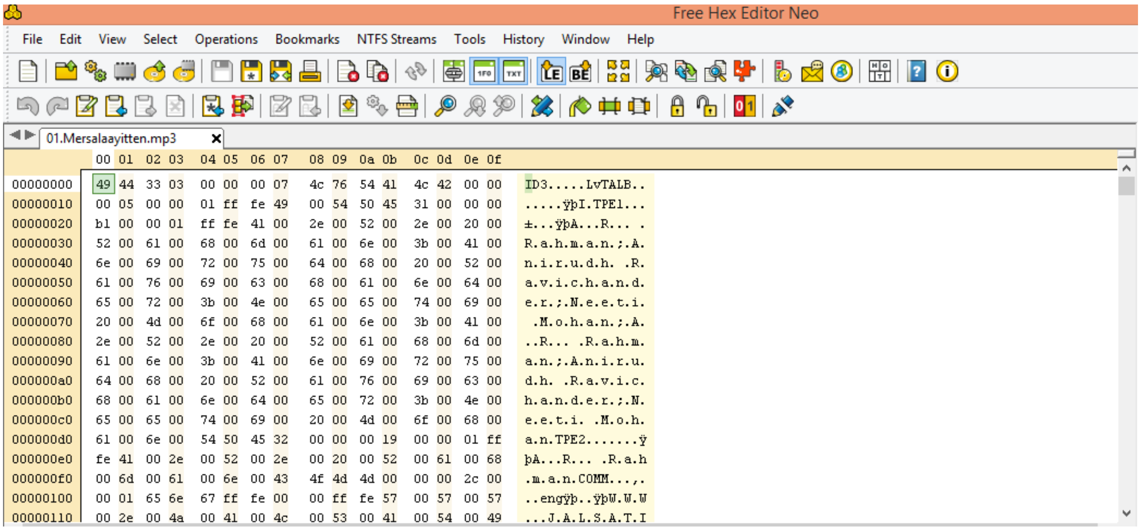


Fig 7: RECEIVER PROSPECT

In the receiver prospect decryption is done by reverse process of encryption in which the received audio signal is converted into hexadecimal value and then converted into original secret information.

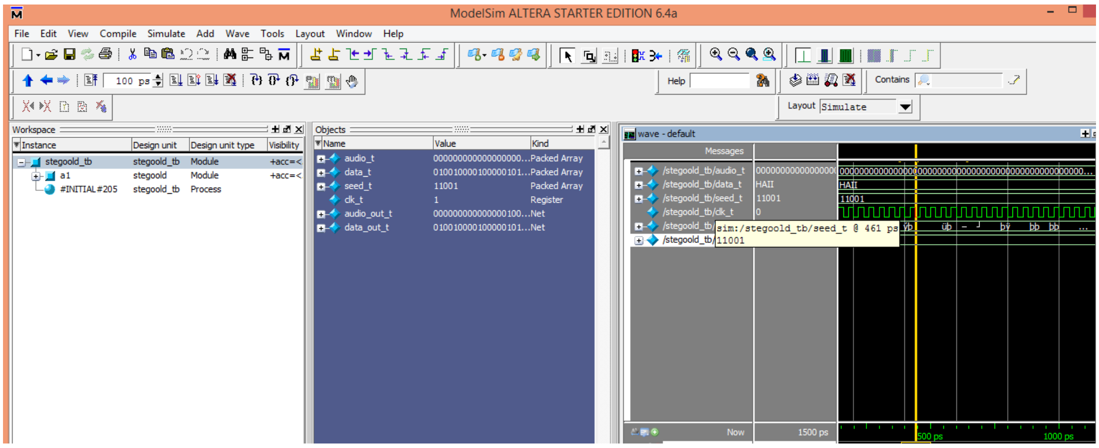
III. SIMULATION RESULTS



```
          00 01  02 03  04 05  06 07  08 09  0a 0b  0c 0d  0e 0f
00000000  49 44  33 03  00 00  00 07  4c 76  54 41  4c 42  00 00   ID3.....LvTALB..
00000010  00 05  00 00  01 ff  fe 49  00 54  50 45  31 00  00 00   .....ÿþI.TPE1...
00000020  b1 00  00 01  ff fe  41 00  2e 00  52 00  2e 00  20 00   ±...ÿþA...R... .
00000030  52 00  61 00  68 00  6d 00  61 00  6e 00  3b 00  41 00   R.a.h.m.a.n.;.A.
00000040  6e 00  69 00  72 00  75 00  64 00  68 00  20 00  52 00   n.i.r.u.d.h. .R.
00000050  61 00  76 00  69 00  63 00  68 00  61 00  6e 00  64 00   a.v.i.c.h.a.n.d.
00000060  65 00  72 00  3b 00  4e 00  65 00  65 00  74 00  69 00   e.r.;.N.e.e.t.i.
00000070  20 00  4d 00  6f 00  68 00  61 00  6e 00  3b 00  41 00    .M.o.h.a.n.;.A.
00000080  2e 00  52 00  2e 00  20 00  52 00  61 00  68 00  6d 00   ..R... .R.a.h.m.
00000090  61 00  6e 00  3b 00  41 00  6e 00  69 00  72 00  75 00   a.n.;.A.n.i.r.u.
000000a0  64 00  68 00  20 00  52 00  61 00  76 00  69 00  63 00   d.h. .R.a.v.i.c.
000000b0  68 00  61 00  6e 00  64 00  65 00  72 00  3b 00  4e 00   h.a.n.d.e.r.;.N.
000000c0  65 00  65 00  74 00  69 00  20 00  4d 00  6f 00  68 00   e.e.t.i. .M.o.h.
000000d0  61 00  6e 00  54 50  45 32  00 00  00 19  00 00  01 ff   a.n.TPE2.......ÿ
000000e0  fe 41  00 2e  00 52  00 2e  00 20  00 52  00 61  00 68   þA...R... .R.a.h
000000f0  00 6d  00 61  00 6e  00 43  4f 4d  4d 00  00 00  2c 00   .m.a.n.COMM...,.
00000100  00 01  65 6e  67 ff  fe 00  00 ff  fe 57  00 57  00 57   ..engÿþ..ÿþW.W.W
00000110  00 2e  00 4a  00 41  00 4c  00 53  00 41  00 54  00 49   ...J.A.L.S.A.T.I
```

Fig 8: HEX EDITOR TOOL RESULT

In the Hex editor tool, it is used to convert the audio signal data into hexadecimal value so that the encrypted data hided into the Least Significant Bit in audio signal conveniently.



Instance	Design unit	Design unit type	Visibility
stegoold_tb	stegoold_tb	Module	+acc=<
a1	stegoold	Module	+acc=<
#INITIAL#205	stegoold_tb	Process	

Name	Value	Kind
audio_t	000000000000000000...	Packed Array
data_t	0100100001000001 01...	Packed Array
seed_t	11001	Packed Array
clk_t	1	Register
audio_out_t	000000000000000100...	Net
data_out_t	0100100001000001 01...	Net

/stegoold_tb/audio_t	0000000000000000	0000000000000000000000000000000000000000000000...
/stegoold_tb/data_t	HAII	HAII
/stegoold_tb/seed_t	11001	11001
/stegoold_tb/clk_t	0	
/stegoold_tb/		ÿb üb – ┘ bÿ bb bb ...
/stegoold_tb/		

sim:/stegoold_tb/seed_t @ 461 ps
11001

Fig 9:MODELSIM SIMULATION RESULT

In the Modelsim software, the Verilog program is coded for encryption and decryption. In which encrypted data can be hided into the cover medium as audio signal by Verilog program. So the security of the communication is increased.

IV. CONCLUSION

The process is done as per the diagram block.The simulation is done with the help of Modelsim software and hex-editor tool. The simulation result shows how the data gets encrypted in sender prospect.

REFERENCES

[1] Kessler, G. “An Overview of Steganography for the Computer Forensics Examiner “, Computer & Digital Forensics Program, Champlain College, Burlington, Vermont, February 2004

[2] S. Hetzl, StegHide, http://steghide.sourceforge.net, 2003.

[3] Bennett, K. “Linguistic Steganography: Survey, Analysis, and Robustness Concerns for Hiding Information in Text“ Technical Report, Center for Education and Research in Information Assurance and Security (CERIAS), 2004.

[4] Fridrich ,J, M. Goljan, and R. Du, “Detecting LSB steganography in color and grayscale images,” IEEE Multimedia Special Issue on Security, pp. 22–28, October- November 2001.