Data Hiding in Audio Signal Using Cryptography and Steganography Techniques

Keerthana.J\textsuperscript{1}, Kiruthiga .S\textsuperscript{1}, Kaviya Priya.K\textsuperscript{1} S.Navaneethan\textsuperscript{2} B.E., M.E.,
\textsuperscript{1}(Student, Mam College Of Engineering, Tiruchirapalli) \textsuperscript{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

How to Hide a secret message in Audio

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.
Data Hiding In Audio Signal Using Cryptography And Steganography Techniques

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.

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 used 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](image)

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

![Fig 6: Sender Prospect](image)

![Fig 7: Receiver Prospect](image)
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

**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 hidden into the Least Significant Bit in audio signal conveniently.

**Fig 9: MODELSIM SIMULATION RESULT**

In the Modelsim software, the Verilog program is coded for encryption and decryption. In which encrypted data can be hidden 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


