ISSN:0975-9646

Implementation of Blowfish Algorithm for Efficient Data Hiding in Audio

Ravali.S.V.K , Neelima.P , Sruthi.P , Sai Dileep.P , Manasa.B

Dept. of C.S.E., Lendi Institute of Engineering &Technology,Vizianagaram, Andhra Pradesh, India.

Abstract--**The basic idea behind the paper is to provide a good, efficient for hiding the data from hackers and transmits to the receiver in a safer manner. In this proposed system mainly based on audio Steganography and cryptography to ensure secure data transfer from transmitter to receiver. Blowfish algorithm is used, which is most powerful technique to encrypt and decrypt the data file. Blowfish algorithm is efficient algorithm among other cryptographic techniques such as RSA, DES, TripleDES and other encrypting algorithms. Spread spectrum Steganography technique is used embed the encrypted data file into an audio file. Spread spectrum is efficient technique to hide the data from hackers and transmits to receiver. The Cryptography, Spread Spectrum, Steganography, Stego Object. Main benefits of Spread spectrum system are robust against interference and inherent security. A simple compression algorithm is used to suitable for any size *and CRC algorithm* is *to* check the integrity of the data file.**

Keywords: Blowfish Algorithm, CRC, Cryptography, Spread Spectrum, Steganography, Stego Object

I. INTRODUCTION:

Steganography is a practice of hiding information “distinctly”. This technique relies on a message being encoded and hidden in such a way that the existence of message unknown to the observer. The carrier file is not secret and can be used by any observer for the secret file itself is not transparent and it needs secret key from the sender side to obtain the secret file.

Steganography is different from cryptography which involves making the content of secret message unreadable while not preventing non intended observer from learning about its existence. Whenever a transmitter transmits the secret key to the receiver then unreadable file can be converted into readable form.

The Audio Steganography is software, which tries to alter the originality of the file into some encrypted form and embed the file into an audio file. Then the users can easily and securely carry the compressed data wherever he wants. The major task of the Audio Steganography is to provide the user flexibility of passing the information implementing the encryption standards as per the specification and algorithms proposed and store the information in a form that is unreadable. The Application should have a reversal process as of which should be in a position to de embed the data file from audio file and decrypt the data to its original format upon the proper request by the user.

II. PROPOSED SYSTEM:

This system basically uses the Blowfish encryption algorithm to encrypt the data file. This algorithm is a 64-bit block cipher with a variable length key. This algorithm has been used because it requires less memory. It uses only simple operations, therefore it is easy to implement.

Among the three types of spread spectrum techniques we use DSSS to embed the data in audio file. Sequence Spread Spectrum (SSS) is one such method that spreads the signal by multiplying the source signal by some pseudo random sequence known as a (CHIP). The sampling rate is then used as the chip rate for the audio signal communication. Spread spectrum encoding techniques are the most secure means by which to send hidden messages in audio. Direct sequence spread spectrum (DSSS) system take a user bit stream and perform an (XOR) with a so-called chipping sequence. For each user bit with duration tb, a chip sequence with a smaller duration tc for each chip. Generally the chipping sequence is generated properly it appears as random noise. The bandwidth of the resulting signal is determined by the spreading factor s = tb/tc. That is, the original signal is spreaded by s times.

III. TECHNIQUES USED IN PROPOSED SYSTEM

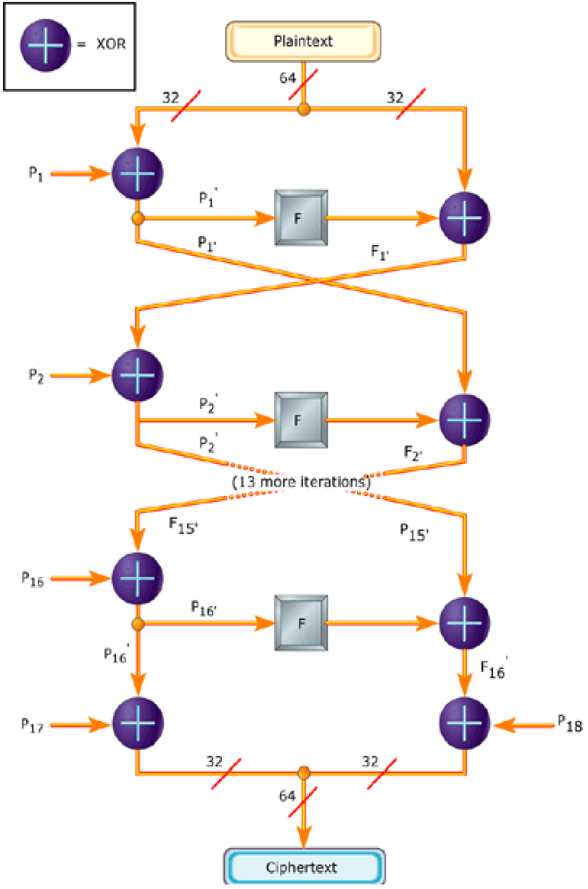

Fig.1 blowfish algorithm

A. *Blowfish algorithm:*

Blowfish is a symmetric encryption algorithm that means it uses the same secret key to both encrypt and decrypt messages. It is one of the block cipher technique which divides a message up into fixed length blocks during encryption and decryption. It is a 64 bit block cipher and it is fast algorithm to encrypt the data. It requires 32 bit microprocessor at a rate of one byte for every 26 clock cycles. It is variable length key block cipher up to 448 bits. Blowfish contains 16 rounds. Each round consists of XOR operation and a function. Each round consists of key expansion and data encryption. Key expansion generally used for generating initial contents of one array and data encryption uses a 16 round feiestel network.

Fig1 shows how the blowfish algorithm works. Plain text and key are the inputs of this algorithm. 64 bit Plain text is taken and divides into two 32bits data and at each round the given key is expanded & stored in 18 p-array and gives 32bit key as input and XOR ed with previous round data. The function F shown in above diagram as its own functionality is to divide a 32-bit input into four bytes and uses those as indices into an S-array. The lookup results are then added and XOR ed together to produce the output. At 16th round there is no function .The output of this algorithm should be 64bit cipher text.

ALGORITHM STEPS:

```
Divide X into two 32-bit halves XL and XR
For i=1 to 16:
XL = XL Å Pi
XR = F (XL) Å XR
Swap XL and XR
End for
Swap XL and XR (Undo the last swap.)
XR = XR Å P17
                    XL = XL Å P1
      Recombine XL and
      Output X (64-bit data block: cipher text)
```

For decryption, the same process is applied, except that the sub-keys Pi must be supplied in reverse order. The nature of the Feiestel network ensures that every half is swapped for the next round (except, here, for the last two sub-keys P17 and P18)

B. *Spread Spectrum*

Direct sequence: A carrier is modulated by a digital code sequence in which bit rate is much higher than the information signal bandwidth. DSSS is combination of data signal and higher data rate bit sequence of transmitter-processing gain /chipping code. Each bit is represented by multiple bits using a spreading code and spreads across a wider frequency band which is similar to FHSS.

Direct-sequence spread-spectrum transmissions multiply the data being transmitted by a "noise" signal. This noise signal is a pseudorandom sequence of 1 and −1values, at a frequency much higher than that of the original signal, thereby spreading the energy of the original signal into a much wider band.

The resulting signal resembles white noise, like an audio recording of "static". However, this noise-like signal can be used to exactly reconstruct the original data at the receiving end, by multiplying it by the same pseudorandom sequence (because 1 × 1 = 1, and −1 × −1 = 1). This process, known as "de-spreading", mathematically constitutes a correlation of the transmitted PN sequence with the PN sequence that the receiver believes the transmitter is using.

C. *Transmitter Design*

Initially the sender selects the data file which is to be sent secretly to the receiver. To ensure any size of data file 1st the data file is to compress to decrease the size. The compressed data is given to encryption algorithm along with key to encrypt it forms a cipher data. This cipher data is to embed in audio cover media using spread spectrum then returns a stego object it.

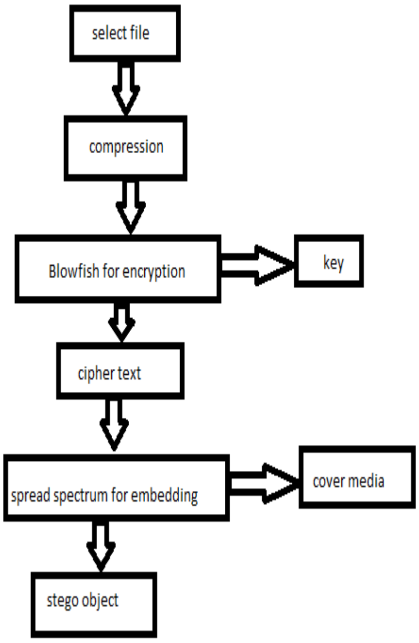

Fig.2 transmitter design

D. *Receiver Design*

The receiver receives a stego object from the sender and performs extraction using spread spectrum and retrieves the cipher data .the cipher data given to blowfish algorithm along with key and performs decryption and then apply decompress the data file to get original data .

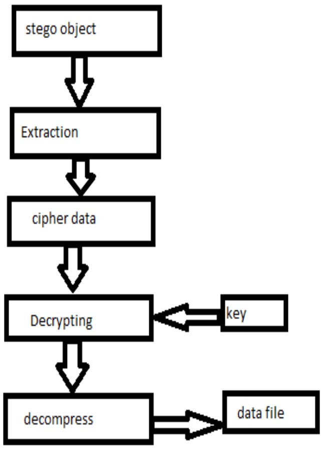

Fig.3 receiver design

IV. CONCLUSION

This system is the combination of Cryptography and Steganography provides greater protection of data from intruders. This proposed system is to provide a good, efficient method for hiding the data from hackers and it will not change the size of the file even after embed using spread spectrum . Encryption and Decryption techniques have been used to make the security system robust using blowfish algorithm. It is suitable for any size of data file and any type of audio file.By using EBCDIC to compress the given data file and CRC is used to check integrity of data.

FUTURE SCOPE

There are several improvements that can be taken as future work for this project:

1. This system can be extended as mobile apps.
2. This system uses a simple compression technique can extends by other complex compression techniques.
3. This can be implemented for video files.
4. Strong Authentication can be provided to restrict the access.

REFERENCES

[1] CRYPTOGRAPHY JOHN E. HERSHEY DEMYSTIFIED.

[2] Steganography Based on Payload Transformation by K B Shiva Kumar.

[3] http://www.hotpixel.net/software.html.

[4] http://www.w3schools.com/.

[5] Audio Steganography :A Survey on Recent Approaches

[6] Robust audio Steganography using direct sequence spread spectrum technology by Wei Qin cheng.

[7] [Nadeem2005]Aamer Nadeem et al, "A Performance Compression of Data Encryption Algorithms ",IEEE 2005