Audio Steganography with Enhanced Security using Cryptography

Pratik Kamat[1] Punit Korgaonkar[2] Rachana Mulik[3] Chinmay Pednekar[4] Tejas Pathak[5]
[1,2,3,4,5]Agnel Institute of Technology & Design, India

Abstract— In the current internet community, due to attack made on data communication secured data transfer is limited. Hence data hiding method such as steganography is chosen which ensures secured data transfer. However, existing steganographic systems have become more predictable, have a limit on length of secret message for a given cover file which opens door for advanced techniques such as audio steganography. Limitation of current steganographic system is that, if the method used is deduced by attacker then extraction of secret message may be known. Therefore, the proposed system uses steganography along with cryptographic approach to make data more secure such that even if the steganographic method is deduced by attacker, it would still be in encrypted form.

Key words: Blowfish, Phase Coding, Cryptography, Audio Steganography

I. Introduction

When two parties are communicating via a communication channel the major concern is confidentiality, integrity and authenticity. Hence data must be secured in some manner. Common approach is to use cryptography or steganography.

Cryptography converts data for transmission over public network, into a form that is unreadable, which protects it from theft or legible alteration. The original text called "plaintext" is turned into a coded equivalent called "ciphertext" via an encryption algorithm. The ciphertext is then decrypted at the receiving end and turned back into plaintext. Steganography is the technique of hiding data in a cover file, making the existence of the information secret. Cover file can be an audio file, an image file or a video file. Steganography is the technique of hiding data in a cover file, making the existence of the information secret. Cover file can be an audio file, an image file or a video file.

II. Proposed architecture

A. Flow of the System

1) Encrypt the text file by applying Blowfish encryption algorithm [1].
2) Embed the encrypted file in cover audio file using Phase coding [4], which gives stego file.
3) Transmit this stego file to the intended receiver.
4) The receiver then extracts the encrypted file using the extraction step of Phase coding.
5) The receiver then applies Blowfish decryption algorithm to get the original data.

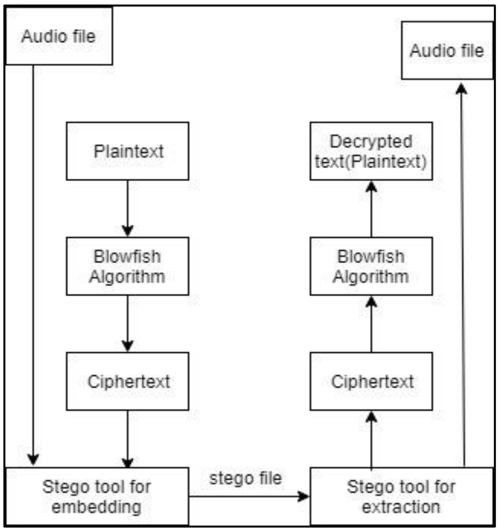

Fig 1: Block Diagram of Proposed System

B. Blowfish Algorithm

Blowfish uses large number of Substitution boxes (S-boxes). It is a basic component of the algorithm which performs substitution, S-boxes are basically used so that there is no relationship between the plaintext and the encrypted text. In general, some number of input bits are transformed into some number of output bits by the S-box. Similarly, Permutation boxes used to permute or transpose bits across S-boxes inputs. The combination of S-boxes are P-boxes makes it more difficult to understand the relation between plaintext and cipher text.

The algorithm is divided into two parts

1) Key expansion
2) Data encryption

1) Key Expansion

It converts a key of at most 448 bits into several subkey arrays totaling 4168 bytes. These keys should be generated before data encryption or decryption.

– Subkey Generation

Input: 32 bit P-array P[1,2,....,18] each consisting of 32 bit subkeys

Four 32-bit S-boxes S1[0,1,2...255], S2[0,1,2...255], S3[0,1,2...255], S4[0,1,2...255]

1) Initialize the P-arrays and then the S-boxes with the fixed string of hexadecimal digits of pi.
   P[1] = 0x243f6a88, P[2] = 0x85a308d3, P[3] = 0x13198a2e, P[4] = 0x03707344, etc.
2) XOR P[1] with the first 32 bits of the key, XOR P[2] with the second 32 bits of the key and so on XOR the entire P-array with the key bits.
3) Encrypt the all zero string with blowfish algorithm using the subkeys from step (1) and step (2).
4) Replace P[1] and P[2] with the output of step (3).
5) Encrypt output of step (3) using blowfish algorithm with the modified subkeys.
6) Replace P[3] and P[4] with the output of step (5).

7) Continue the process, until all the entries of the P-array and S-boxes are replaced in order, with the output of the continuously changing blowfish algorithm.

2) Data Encryption

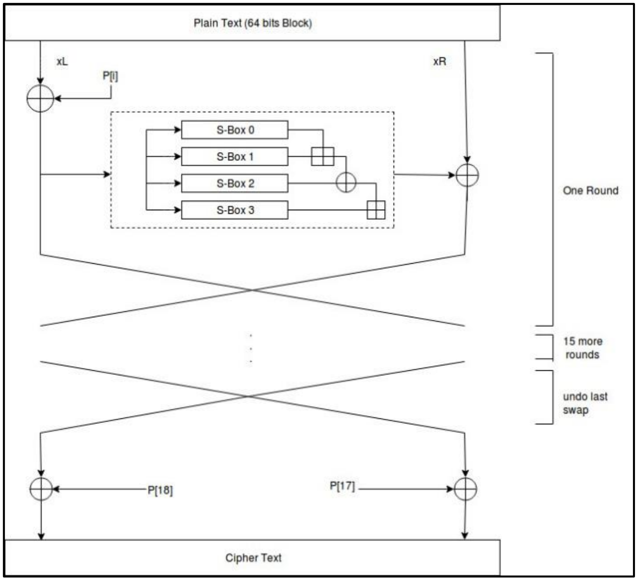

Fig. 2.1: Block diagram of Blowfish Encryption

Input: x, 64-bit data element

1) Divide x into 2 halves 32bit each xL, xR.
2) for i=1 to 16:
   xL = xL XOR P[i]
   xR = F(xL) XOR xR
   swap xL and xR
3) swap xL and xR
4) xR = xR XOR P[17]
5) xL = xL XOR P[18]
6) Recombine xL and xR

3) Decryption

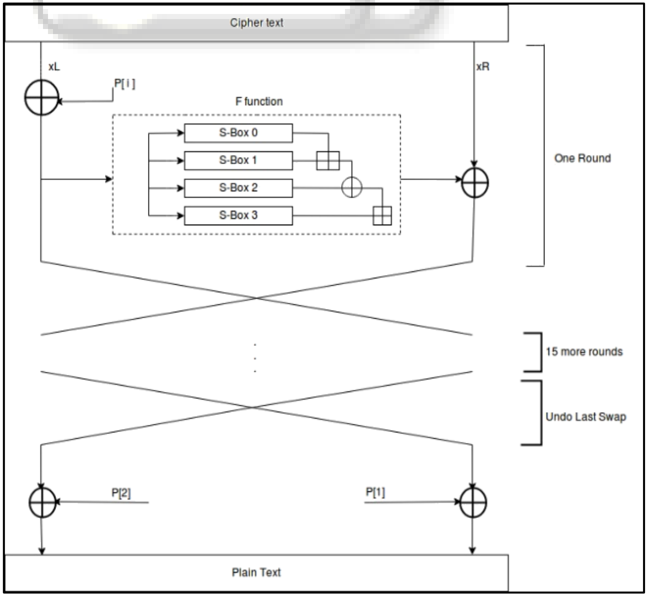

Fig. 2.2: Block diagram of Blowfish Decryption

For decryption of the data, same procedure is used except that the subkeys P-array must be supplied in reverse order. Starting from P[18] to P[1].

C. Phase Coding Algorithm

In phase coding, the initial audio segment is replaced by a reference phase which represents the secret message. The remaining segments phase is adjusted to maintain relative phase between the segments. This method relies on the fact that the phase components of sound are not perceptible to the human ear as noise is.

1) Embedding

1) Divide original sound signal into segments.
2) Calculate phase and magnitude of each segment applying Discrete Fourier Transform(DFT) to each segment.

$$X[k] = \sum_{0}^{N-1} x[n]e^{\frac{-i2\pi kn}{N}} \qquad (1.1)$$

3) To calculate the relative phase, find the phase difference between adjacent segments.
4) Change the phase value of first segment as follows:
   if message bit = 0
   {New Phase = π/2}
   else if message bit = 1
   {New Phase = - π/2}
5) Update the phase values of remaining segment using the new phases of first segment and the relative difference.
6) Reconstruct the sound signal applying Inverse Discrete Fourier Transform(IDFT)

$$x[n] = \frac{1}{N}\sum_{0}^{N-1} X[k]e^{\frac{i2\pi kn}{N}} \qquad (1.2)$$

The generated sound signal is called stego file.

2) Extraction

1) Divide the sound signal into segments.
2) Calculate the phase of first segment.
3) If phase value is pi/2 data is 0

If phase value is -pi/2 data is 1

III. CONCLUSION

In this hybrid approach we use Blowfish algorithm for cryptographic technique which has high throughput among all the symmetric key algorithm and Phase Coding for steganographic technique in which changes made to audio file are inaudible to Human Auditory System (HAS). Combining these two techniques the message is not only obscured but also its existence is hidden.

REFERENCES

[1] Bruce Schneier, “Description of a New Variable-Length Key, 64-Bit Block Cipher (Blowfish)”, Counterpane Systems, 730 Fair Oaks Ave, Oak Park, IL 60302, schneir@chinet.com.

[2] Arfan Shaikh, Kirankumar Solanki, Vishal Uttekar, Neeraj Vishwakarma “Audio Steganography and Security using Cryptography”, International Journal of Emerging Technology and Advanced Engineering, Website: www.ijetae.com (ISSN 2250-2459, ISO 9001:2008 Certified Journal, Volume 4, Issue 2, February 2014)

[3] P. Princy, “A comparison of Symmetric key Algorithm DES, AES, Blowfish, RC4, RC6: Survey”, International Journal of Computer Science & Engineering Technology (IJCSET), ISSN: 2229-3345, Vol. 6, No. 05, May 2015

[4] Joel T. George, A. Arokiaraj Jovith, “A Fragmented Approach: Audio Steganography using Phase Coding

and LSB", International Journal of Applied Engineering Research ISSN 0973-4562 Volume 11, Number 7 (2016) pp 5228-5230 © Research India Publications. www.ripublication.com

[5] Jayaram P., Ranganatha H R, Anupama H S, "Information Hiding Using Audio Steganography – A Survey", The International Journal of Multimedia and its Applications (IJMA), Vol. 3, No. 3 August 2011.

[6] Saikumar Manku, K. Vasanth. "Blowfish Encryption Algorithm For Information Security", ARPN Journal of Engineering and Applied Sciences, ISSN 1819 – 6608 Vol. 10, No. 10, June 2015, www.arpnjournals.com

[7] Prof. Samir Kumar, BandyopadhyaBarnali, Gupta Banik "LSB Modification and Phase Encoding Technique of Audio Steganography Revisited" ISSN: 2278 – 1021 International Journal of Advance Research in Computer and Communication Engineering. Vol. 1, Issue 4, June 2012

[8] Ranjeet Masram, Vivek Shahare, Jibi Abraham, Rajni Moona "Analysis and Comparison of Symmetric Key Cryptographic Algorithms Based on Various File Features" Department of Computer Engineering and Information Technology, College of Engineering Pune, India. International Journal of Network Security & Its Applications (IJNSA), Vol.6, No.4, July 2014