Chaos based Encryption & Decryption System for Secure Audio/Text Communication

Gunja Shah[1] Yash Hariyani[2] Aniket Patel[3] Keyur Patel[4]
[1,2,3]Student [4]Assistant Professor
[1,2,3,4]Department of Information Technology
[1,2,3,4]Sigma Institute of Engineering, Vadodara, India

Abstract— The Growth rate of the internet exceeds day by day and with this, there is a very obvious need to protecting sensitive data from getting leak or misused anyway. Currently there are many techniques of encryption and decryption out there for audio as well as text data. This paper focuses on Encryption and Decryption Techniques for audio and text knowledge. This presents a literature survey Encryption technique that are used for encoding on Audio and Text Data.

Key words: Steganography, Chaos based Encryption, AES algorithm

I. Introduction

Cryptography can be defined as the art or science of altering information or change it to a chaotic state, so that the real information is hard to extract during transfer over any unsecured channel [1]. The strength of the Encryption technique comes from the fact that no one can read or steal the information without altering its content. This alteration alerts the communicators about the possibility of a hacker and thus promising a highly secure data transfer. During the course of time, various encryption algorithms have been developed to achieve the ultimate aim of safe environment for information transmission. However, the principal objective guiding the design of an encryption algorithm must be security against all possible unauthorized attacks.

Encryption is a technique used to transmit secure information. Over the years several encryption techniques have been implemented. But most of the techniques encrypt only text data, a very few techniques are proposed for multimedia data such as audio data. The techniques which encrypt text data can also apply to audio data but have not achieved satisfactory results. Various encryption techniques are implemented for audio data[1]. Some of which are inefficient to meet real time requirements and some are naive to meet the security requirements. Encryption of an audio data is difficult and complex process than the techniques used for text data. Audio encryption ensures secure audio transmission[1]. With the fast growth of communication technology, protection of audio from the hackers became a critical task for the technologist[1]. So there is always a need of a more secure and faster audio encryption technique.

II. Cryptographic Algorithms

There are several Algorithms, according to the comparison the results are as shown in table.

Factors	DES	3DES	RC2	RC4	RC6	BLOWFISH	AES
Key Size	56 bits	168 bits	8-128 bits	40-128 bits	128,192 or 256 bits	32-448 bits	128,192 or 256 bits
Block Size	64 bits	64 bits	64 bits	Byte Oriented	128 bits	64 bits	128,192 or 256 bits
Cipher Type	Block Cipher	Block Cipher	Block Cipher	Stream Cipher	Symmetric Algorithm	Symmetric Block Algorithm	Symmetric Cipher Algorithm
Keys	Private Key	Private Key	Single Key	Single Key	Single Key	Private Key	Private Key
Attacks	Vulnerab le to Different ial and Linear Attacks	Vulnerable to Differential ,Bruite Force Attacks	Vulnerabl e to Differenti al,Bruite Force Attacks	Vulner able to Bruit Force Attack s	Vulnerable to Differential ,Bruite Force Attacks	Vulnerable to Differential, Bruite Force Attacks	Strong Against Differential, Bruite,Linear Force Attack
Security	Proven Inadequate	Inadequate	Vulnerable	Weak Security	Vulnerable	Less secure	Considered Secure

Fig. 1: Comparison Results

As there are several other but apart from them We chose AES Algorithm.

A. AES Algorithm

AES algorithm, which stands for Advanced Encryption Standard. Like DES, AES is symmetric block cipher, which means same key will be used for both Encryption and Decryption. The algorithm allows for a variety of block and key sizes and not just the 64 and 56 bits of DES block and key size. The block and key can in fact be chosen independently from 128,160,192,224,256 bits and need not be the same[2]. However, the AES standard states that the algorithm can only accept a block size of 128 bits and a choice of three keys - 128,192,256 bits.

A number of AES parameters depend on the key length. For example, if the key size used is 128 then the number of rounds is 10 whereas it is 12 and 14 for 192 and 256 bits respectively. At present the most common key size likely to be used is the 128-bit key.

Characteristics are – 1) Resistance against all known attacks. 2) Speed and code compactness on a wide range of platforms. 3) Design Simplicity.

The algorithm begins with an Add round key stage followed by 9 rounds of four stages and a tenth round of three stages[2]. This applies for both encryption and decryption with the exception that each stage of a round the decryption algorithm is the inverse of it's counterpart in the encryption algorithm.

The four stages are as follows:

1) Substitute bytes
2) Shift rows
3) Mix Columns
4) Add Round Key

The tenth round simply leaves out the Mix Columns stage. The first nine rounds of the decryption algorithm consist of the following:

1) Inverse Shift rows
2) Inverse Substitute bytes
3) Inverse Add Round Key
4) Inverse Mix Columns

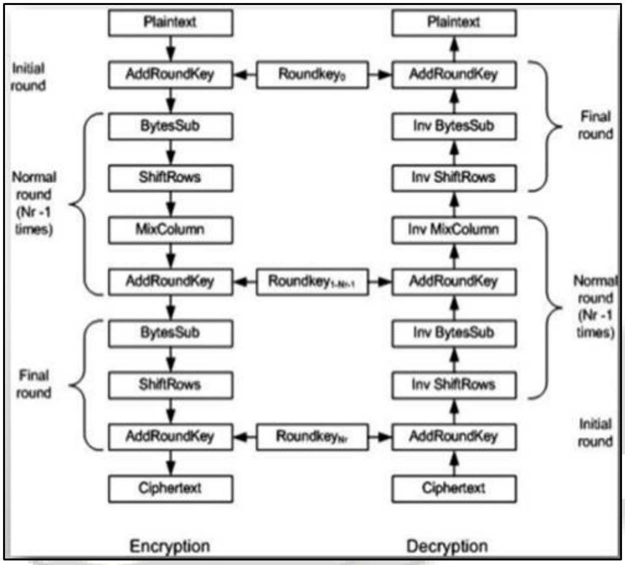

Fig. 1: Overall Structure of AES Algorithm.

III. Proposed System

A. Special Properties of Chaotic Systems

- Plaintext: Denoted by M [a stream of bits, a text file, a bitmap, a stream of digitized voice, digital video image, etc.]
- Encryption: Process of disguising a message M so as to hide its contents Ek(M) = C, E denotes the encryption function and k is key
- Ciphertext: An encrypted message denoted by C.
- Decryption: Process of converting Ciphertext back into Plaintext Dk(C) = M, D denotes the decryption function and k is key
- Cryptanalysis: The art & science of breaking Ciphertext Encryption & Decryption Keys. It is normal for cryptographic algorithms to be publicly known. The secrecy is ensured by use of parameters called keys for encryption and decryption, which are only known to sender and receiver.

Keys could be one or many depending on cryptographic algorithm. The set of permissible values that keys can take is called a key space.

B. Security Features:

A large number of keys and their large key space makes it extremely difficult to guess the right initial conditions and the other parameters. The intruder will have to try all possible combinations of the key set (x0, y, z0, σ, β, R) which are ~ 1096(using double precision reals). The number of time steps, which is used as cipher, does not reflect the dynamics of the system. In fact, they are independent of the choice of parameters. Therefore, brute force attack is extremely difficult. The possibility of statistical attack is reduced as the shape of frequency distribution of the encrypted message is seen to be independent of the nature of the language and type of the message. Two alternative schemes to increase the complexity of cipher further have been tried. They involve use of randomized map sites or imposition of random text on the original message.

C. System Flow:

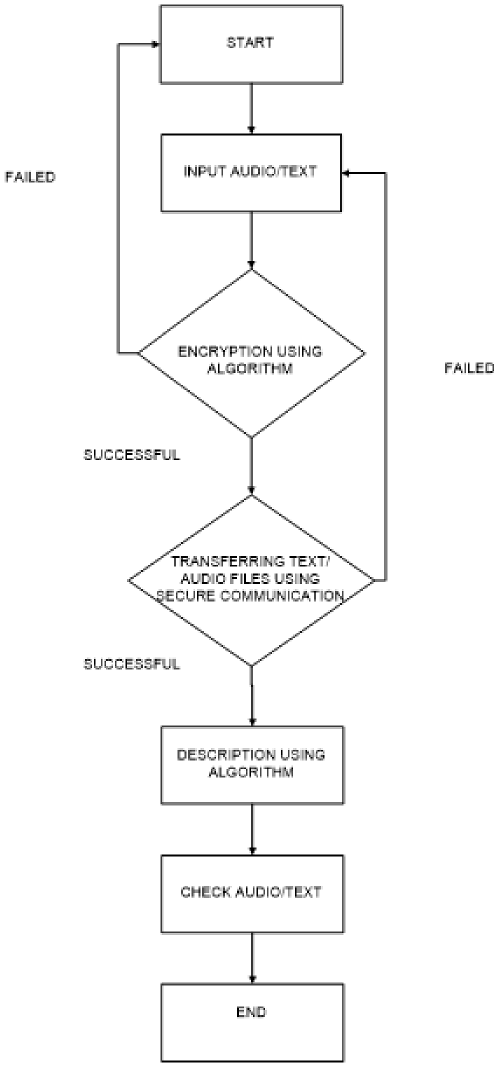
START
INPUT AUDIO/TEXT
FAILED
ENCRYPTION USING ALGORITHM
FAILED
SUCCESSFUL
TRANSFERRING TEXT/ AUDIO FILES USING SECURE COMMUNICATION
SUCCESSFUL
DESCRIPTION USING ALGORITHM
CHECK AUDIO/TEXT
END

Fig. 2: System Flow

As shown in system flow, the proposed system is to very first input text file or audio file. After it using AES Algorithm, procedure of encryption or decryption gets to started. It gets to done after some time, then using secure network, encrypted file gets transferred. In transferred file password and other file which are supposed to be secured is hidden. Receiver gets that file and using algorithm it decrypts file into original one.

IV. CONCLUSION

The study demonstrated the capability of the technique for encrypting a potentially large payload of data with robustness. A tradeoff between noise tolerance and payload, both of which depend on higher bit indices, is needed for a reasonably imperceptible embedding of audio signal. The chaos based encryption thus providing the stronger encryption technique in audio media. In this paper, we have discussed various cryptographic algorithms and chose one which is AES, which is more secure and faster encryption technique which always works better and makes data secure.

ACKNOWLEDGMENT

We would like to extend our gratitude to our respected teacher – Mr. Keyur Patel, for his constant support and for imparting us with the knowledge and helping us throughout the paper.

REFERENCES

[1] Bhaskar Mondal and Tarni Mandal, "A Multilevel Security Scheme using Chaos based Encryption and Steganography for secure audio communication, Jharkhand.

[2] Manpreet Kaur and Sukhpreet Kaur , "Survey of Encryption Techniques for Audio Data", Punjab.

[3] Vishakha Pawar, Pritish Tijare and Swapnil Sawalkar"A review paper on Audio Encryption", Amravati, Maharashtra.

[4] Bhaskar Mondal and et. al. "An Improved Cryptography Scheme for Secure Image Communication", International Journal of Computer Applications (0975 – 8887) Number 18 (ISBN: 973-9380874-18-3) April 2013 Issue. Volume 67(18) pages 23-27.

[5] Bhaskar Mondal, S. K. Singh "A Highly Secure Steganography Scheme For Secure Communication", Proc International Conference of Computation and Communication Advancement (IC3A)-2013, JIS College of Engineering, January, 2013.

[6] Sheetal Sharma,Lucknesh Kumar,Himanshu Sharma "Encryption of an Audio File on Lower Frequency Band for Secure Communication "International Journal of Advanced Research in Computer Science and Software Engineering,Vol.3,Issue7.Julyl2013

[7] History of Secure Voice Coding: Insights Drawn from the Career of One of the Earliest practitioners of the Art of Speech Coding, JOSEPH P.CAMPBELL, JR., and RICHARD A. DEAN.

[8] D. Pan, "A tutorial on MPEG/Audio compression", IEEE Multimedia, 2(2), pp. 60-74, 1995. modifieddiscrete cosine transform of MPEG/Audio Layer III", Proceedings of the 2004 IEEE International Conference on Networking, Sensing & Control,pp.984-989, 2004.