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

Gunja Shah[1] Yash Hariyani[2] Aniket Patel[3] Keyur Patel[4]
[4]Assistant Professor
[1,2,3,4]Department of Information Technology
[1,2,3,4]SIE, 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, so that the real information is hard to extract during transfer over any unsecured channel. The strength of the Encryption technique comes from the fact that no one can read or steal the information without altering its content[1]. This system 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[4]. However, the moto the design of an encryption algorithm must provide security against all possible unauthorized attacks.

Encryption is a method used to transmit secure information.in past 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[4]. 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. Some of which are inefficient to meet real time requirements and some are naive to meet the security requirements[2]. Encryption of an audio data is difficult and complex process than the techniques used for text data. Audio encryption ensures secure audio transmission. With the fast growth of communication technology, protection of audio from the hackers became a critical task for the technologist[5]. So there is always a need of a more secure and faster audio encryption technique, we have implemented system using 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[6]. 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. 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[1]. 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

- Resistance against all known attacks.
- Speed and code compactness on a wide range of platforms
- 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[7]. 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[9].

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

II. LITERATURE REVIEW

Cryptography is now routinely used to protect data, which must be communicated and/or saved over long periods, to protect electronic fund transfers and classified communications. Current cryptographic techniques are based on number theoretic or algebraic concepts. Chaos is another paradigm, which seems promising. Chaos is an offshoot from the field of nonlinear dynamics and has been widely studied. A large number of applications in real systems, both man-made and natural, are being investigated using this novel approach of nonlinear dynamics. The chaotic behaviour is a subtle behaviour of a nonlinear system, which apparently looks random. However, this randomness has no stochastic origin. It is purely resulting from the defining deterministic processes. The important characteristics of chaos is its extreme sensitivity to initial conditions of the system. Chaos is one of the possible behaviour associated with evolution of a nonlinear physical system and occurs for specific values of system exhibiting an apparently random behaviour for certain range of values of system parameters are referred to as Chaotic. However, the solutions or trajectories of the system remain bounded

within the phase space. This unstable state has a strong dependence on the values of the parameters and on the way the system begins.

A. A Multilevel Security Scheme Using Chaos Based Encryption And Steganography For Secure Audio Communication

This paper contains various chaos based encryption and steganography schemes to provide security to confidential data. It uses steganography using the bit modification. a chaos based encryption is performed on secret audio data to increase the security.

The weakness of the Human Auditory System (HAS) is used to hide the information in audio steganography. Chaos is a ubiquitous phenomenon existing in deterministic nonlinear systems that exhibit extreme sensitivity to initial conditions and have random like behaviors.

In this paper, we also learnt the Chaos Algorithm through which we can carry out audio encryptions[6]. Certain techniques described in this paper are LSB SUBTITUTION TECHNIQUE, LSB Modification Encoder and LSB Decoder. Out of all the techniques we know for the steganography, lsb modification is one of the easiest techniques which yield the desired output[8]. The requirements of encryption and data robustness in bit modification audio steganography is dealt with the conventional LSB MODIFICATION TECHNIQUE to make it more secure.

B. Survey Of Various Encryption Techniques For Audio Data

Cryptography is defined as the art of modifying information so that the real or original information is hard to extract during the transfer of the message over any unsecured communication channel.

In this paper,several techniques have been described for encryption of audio data :-audio encryption: Encryption is a technique to transmit or to send secure information from sender to the receiver.but most of the techniques are only used for the text data and a very few techniques for audio data.

1) DES

The Data Encryption Standard(DES) was the first encryption standard and was used widely before the introduction of its upgraded version, new Advanced Encryption Standard(AES)[6].DES is a block cipher based symmetric algorithm, which uses the same keys for both encryption and decryption. It makes use of 56 bits key. DES encrypts the data in 64 bits data blocks.

2) Triple DES

It was formed by using the DES cipher three times. When it was found that a 56-bit key of DES is not strong enough, long key size was made for the same algorithm. In 3DES, triple DES is used in order to provide triple security.

3) AES

The Advanced Encryption Standard (AES) algorithm is a symmetric block. AES algorithm can encrypt and decrypt the plaintext and cipher text of 128-bits. It uses variable length key of size 128,192,256 bits. Number of rounds in the encryption or decryption processes depends on the size of the key.

III. PROPOSED METHODOLOGY

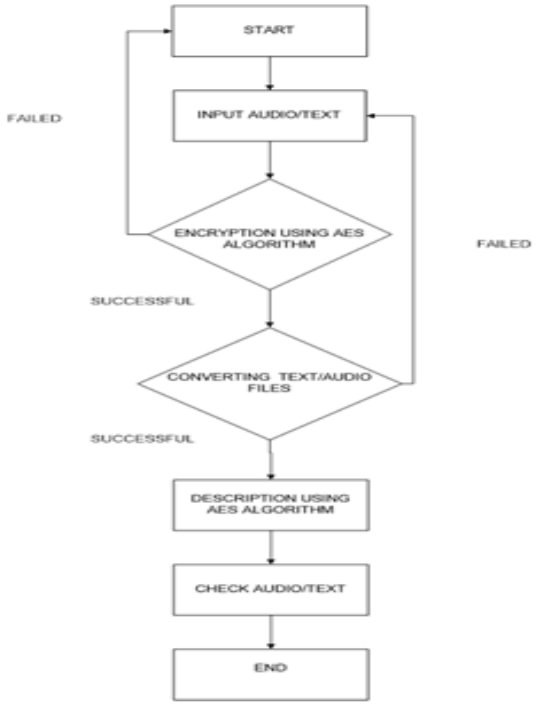

Fig. 1: System Flow

The Advanced Encryption Standard (AES) is a symmetric-key block cipher published by the National Institute of Standards and Technology (NIST).

AES is a non-Feistel cipher that encrypts and decrypts a data block of 128 bits. Round keys are always 128 bits. AES defines 10, 12, or 14 rounds. The key size, which can be 128, 192, or 256 bits, depends on the number of rounds.

AES uses four types of transformations for encryption purpose :

Substitute bytes, shift rows, mix columns, add round keys.

A. Substitute Bytes

A simple substitution of each byte is done.

Uses table of 16x16 containing permutation value of all 256 8-bits value.

To substitute a byte, we interpret the byte as two hexadecimal digits.

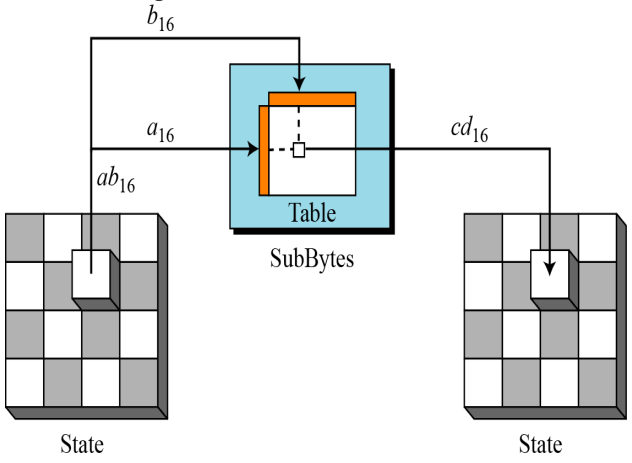

Fig. 2:

For example, byte {EA} is replaced by byte in row E and column A which has value {87}

B. Shift Rows

A circular byte shift in each row
1st row remains unchanged.
2nd row does 1 byte circular shift to left.
3rd row does 2 byte circular shift to left.
4th row does 3 byte circular shift to left.
Decryption is done shifting the byte to right.

Since the state is processed by columns, this step permutes bytes between the columns.

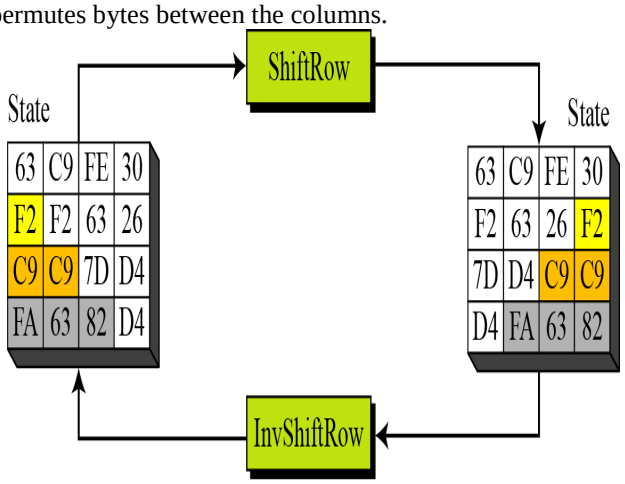

Fig. 3:

C. Mix Columns

Each column is processed separately.

Each byte is replaced by a value dependent on all 4-bytes in the columns.

Effectively a matrix multiplication in GF(28) using prime poly m(x)=x8+x4+x3+x+1.

D. Add Round Key

XOR state with 128-bits of the round key.

Again process by the column through a series of byte operation.

Add Round Key adds a round key word with each state column matrix; the operation in Add Round Key is matrix addition.

E. Key Expansion

It takes 128-bits(16 bytes)key and expands into array of 44,52,60 32-bit words.

Start by copying key into first four words.

Then loop creating words that depends in the value in previous and four places back.

If the number of rounds is Nr , the key-expansion routine creates Nr + 1 128-bit round keys from one single 128-bit cipher key.

IV. Result

Step 1:-Select the file you want to encrypt.
Step 2:-Create new file for the encrypted data.
Step 3:-Type the message you want to hide.
Step 4:-Give password for the security purpose.
Step 5:-Select “Embed button” for embedding the file.
Step 6:-For retrieving the file, select the embedded file.
Step 7:-Create new file for storing the retrieved data.
Step 8:-Type the password for retrieving the file.
Step 9:-At last, select “retrieved button” for retrieving the embedded file.

For TEXT

A. Text Encryption

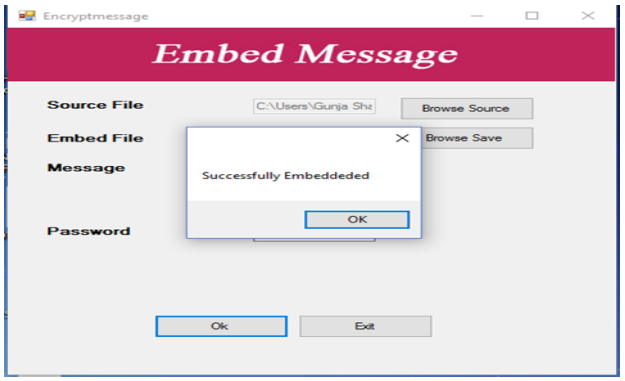

Fig. 4:

B. Text Retrieving

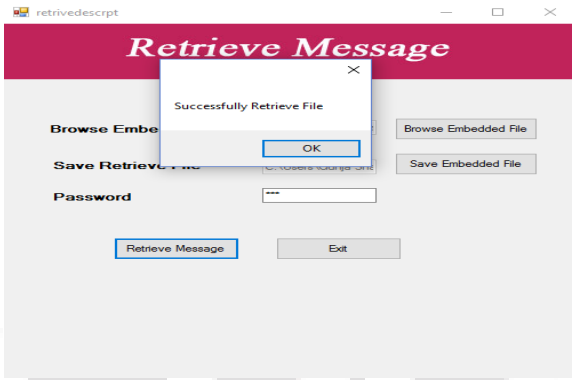

Fig. 5:

C. Audio Encryption

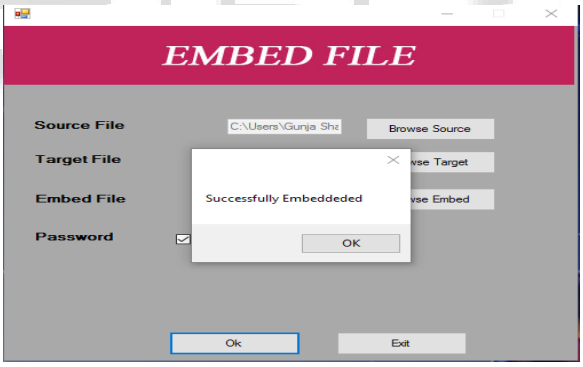

Fig. 6:

D. Audio Retrieving

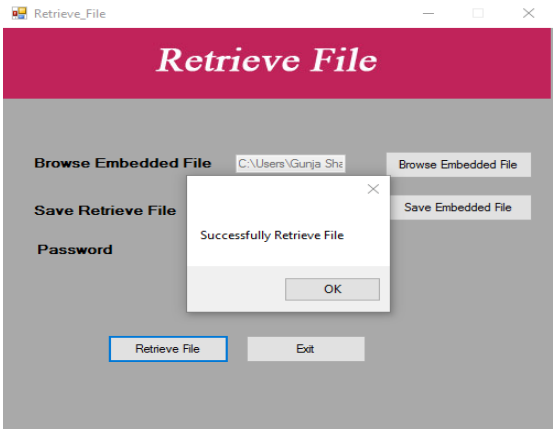

Fig. 7:

Results are so positive and as per the requirements. In text files, one text is hiding inside the other text file and it is password protected so everything is safe. Apart from that process of encryption or decryption, it takes few seconds so based on that it is very reliable.

Main advantage of this system is whether the audio file contains large file or small size, system encrypts in few seconds or minutes, so it is faster than ever and ofcourse it is password protected so it is very secure and reliable.

V. FUTURE WORK

In this paper, everything about steganography and encryption, decryption using AES algorithm is already mention or we can say described. As mentioned earlier we have defined our own steganography flow so we can work more upon that, and obviously on AES algorithm there are plenty of research that can be researched. So the future work is to research and implement more upon these two topics.

REFERENCES

[1] Bhaskar Mondal and Tarni Mandal, "A Multilevel Security Scheme using Chaos based Encryption and Steganography for secure audio communication, Jharkhand.
[2] Gunja Shah, Yash Hariyani, Aniket Patel,Keyur Patel" Chaos Based Encryption & Decryption System for Secure Audio/Text Communication"
[3] Manpreet Kaur and Sukhpreet Kaur , "Survey of Encryption Techniques for Audio Data", Punjab.
[4] Vishakha Pawar, Pritish Tijare and Swapnil Sawalkar"A review paper on Audio Encryption", Amravati, Maharashtra.
[5] 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.
[6] 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.
[7] 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
[8] 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.
[9] 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.

