iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 6 **Issue:** IV **Month of publication:** April 2018

DOI: http://doi.org/10.22214/ijraset.2018.4499

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 6.887
Volume 6 Issue IV, April 2018- Available at www.ijraset.com

A Survey of Various Encryption Techniques for Enhancing Audio Security

Deveki Nandan Shukla[1], Jitendra Kurmi[2], Deena Nath[3]
[1, 2, 3]*Department of Computer Science, Babasaheb Bhimrao Ambedkar University.*

***Abstract:** The way the internet is booming, it is creating an immense need for securing our data from any unauthorized access. Cryptography has a very wide use of encryption and authorization techniques, and thus in this paper, we are going to have a brief survey of various conventional cryptographic techniques that we can use for our noble audio file security system. Encryption alone cannot save our data due to increase in the computation power of new systems, so we are in need of a much complex methodology to encrypt an audio file, so that brute force and the statistical attack may not have any scope to break into the system.*

***Keywords:** AES, DES, audio shuffling, genetic algorithm, higher dimensional chaos algorithm, steganography, media format conversion.*

I. INTRODUCTION

We have recently seen a major breakthrough in computer world with the emergence of more powerful processors and coprocessors. With such a computation power, hackers may try to steal data and break into encrypted data using brute force and statistical attacks easily. Cryptography has a very wide range of encryption methodologies that can prevent such attack but will soon fail due to the increased computational power of physical systems. This leads us to start research to develop a new methodology to encrypt our data with a highly complex yet lossless encryption algorithm. Here we will be working on audio data. This will be quiet challenging though as audio data comprise of some positive and negative values of amplitudes. These negative amplitude may never recover when audio undergoes a transformation while encryption.

II. CRYPTOGRAPHIC SYSTEMS

A cryptographic system is described as [1],“ an established set of cryptographic algorithms along with the key managing process which can support the use of the algorithms in some application.” This definition itself provide the knowledge of the whole mechanism needed for a cryptographic system. Various step involved in a conventional cryptographic system are:

1) The sender wants to send a message, which is also known as plaintext.
2) This plaintext is converted into random bits using a key and an algorithm, and this random bit message is known as Ciphertext.
3) The ciphertext is then transmitted over a communication medium, where the receiver will receive it.
4) On receiving, the receiver will use same key and algorithm which was used by the sender to encrypt the plain text, to decrypt the Ciphertext back into plain text.

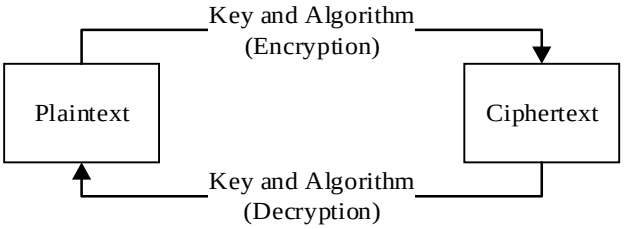


Figure 1: Conventional Cryptographic System

A. Goals of Cryptography

A Cryptographic system must be capable of providing security that can assure the safety of the system. These security goals are listed as five of the following :

1) Authentication: Authentication means that a cryptographic system should verify the identity of sender and receiver before sending and receiving data.
2) Confidentiality: It is also referred as privacy. No other than intended receiver should be able to read the data.

3) Integrity: The Cryptographic system should make sure that the message received was not altered in between in any way.
4) Availability: Cryptographic systems are attacked almost regularly by attackers (intruders and hackers), as such system availability can be affected. Under any circumstance, the system should be able to provide service to its user.
5) Reliability: Such a cryptographic system must be capable of providing service continuously for a long time. There should be no need for making changes in the system again and again.
6) Non-repudiation: Service should be provided in such a way that, neither sender nor receiver can falsely deny about sending some data by them.

B. Types of the cryptographic system:

A cryptographic system is categorized on basis of involvement of key in its encryption algorithm. As such it is categorized into two types which are symmetric encryption and asymmetric encryption.

1) *Asymmetric Encryption Technique (public key cryptography):* In this system, Two different key is used for encryption of plaintext and decryption of ciphertext. These key are mathematically related. The receiver first sends his public key to the sender which is then used by the sender to encrypt plain text. On receiving ciphertext, the receiver then uses his private key for decryption of ciphertext.

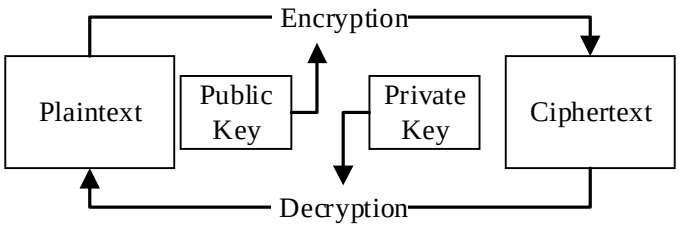


Figure 2: Asymmetric encryption technique

2) *Symmetric Encryption Technique:* In Symmetric Encryption, a single key is used, and that same key is used for both encryption as well as decryption of plaintext and ciphertext respectively. Sender and receiver decide and agree to a common key for both before encryption.

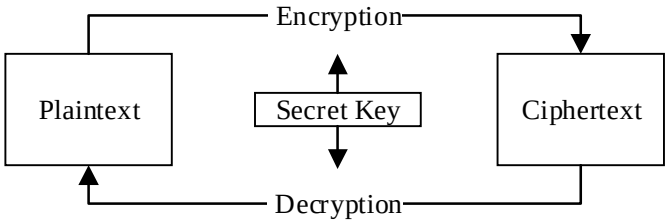


Figure 3: Symmetric Encryption Technique

C. Encryption Algorithms

DES also to be known as Data Encryption Standard, was the first ever encryption standard that was designed by IBM. It was based on Lucifer cipher. It uses 56 bit key for encrypting a 64-bit data in order to output 64-bit encrypted data. This algorithm later was found prone to many attacks and this made it an insecure block cipher. Later this algorithm was further enhanced using three 56 bit keys and running this algorithm thrice, and thus eventually we got TDES or 3DES. Due to increased computation, the performance of 3des was slow, but with an increased level of security. Later with an increase in computation power of systems, this algorithm was also found to be prone to many attacks.

AES or advanced encryption standard is also known to be Rijndael is a symmetric key algorithm. It is one of the fastest encryption algorithm, which is secure enough to provide security. Currently, AES has key size options of 128, 192, 256 bits. 512, 1024 and 2048 bit variant are also available but have very low performance due to very large computation requirements. It uses a fixed block size of 128 bits. Brute force and side channel attack are the only known attacks ever recorded to be successful, but the practicality of such attacks are often criticized.

RSA algorithm is an example of public key cryptography where two keys are used and were introduced by Rivest, Shamir, and Adelman in 1978. It is very slow, but secure algorithm ever known as the private key is only known to the receiver. Key size used

in RSA is greater than 1024 bits, whereas block size used is minimum 512 bit. Despite being a public key algorithm and using large key size, RSA is vulnerable to chosen-plaintext and chosen-ciphertext attacks.

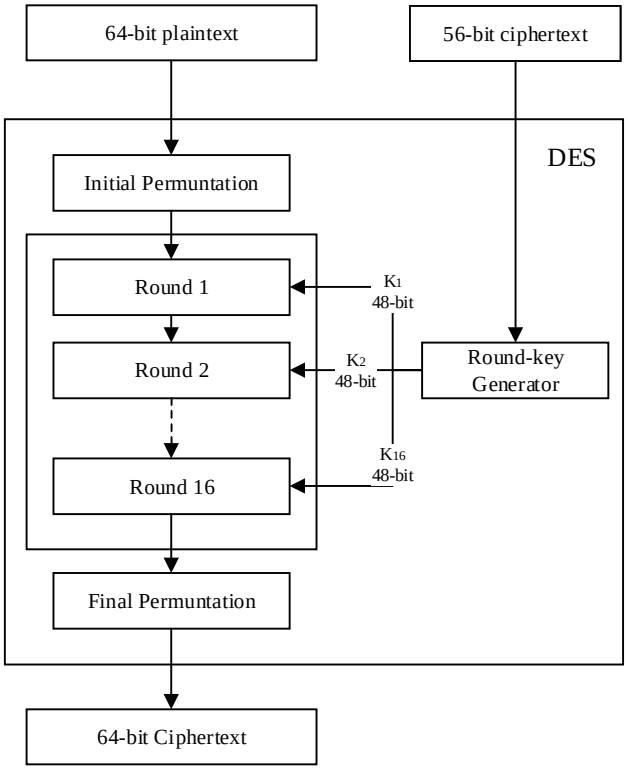


Figure 4: DES encryption technique

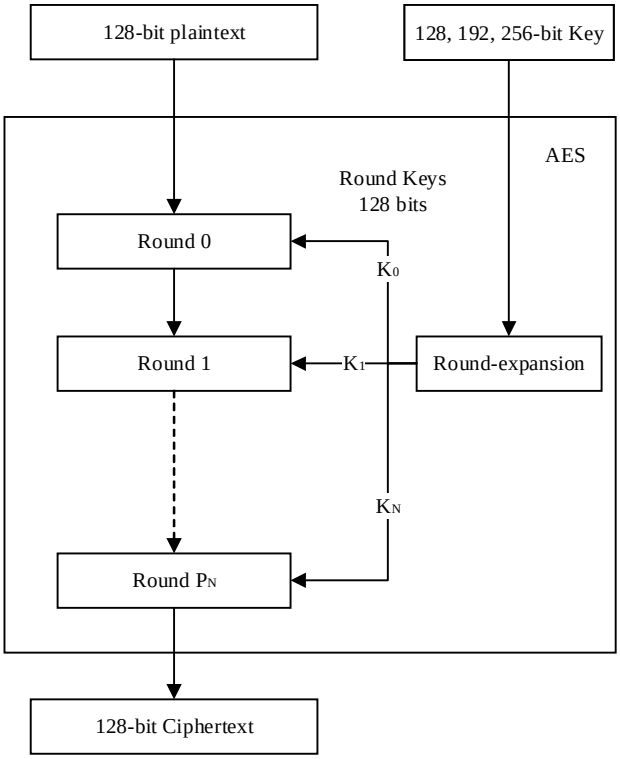


Figure 5: AES encryption technique

III. TECHNIQUES TO IMPROVE COMPLEXITY AND RELIABILITY OF AN ALGORITHM

Higher Dimensional Chaos theory [2] is used in cryptography, hashing, steganography, and in the generation of pseudo-random numbers. Cryptographic keys highly rely on diffusion and confusion properties of chaos. Diffusion means that each binary bit of key should be dependent on several another part of the keys. Confusion means that if a single bit is changed, then it should change about half of the bits of data. This creates a relationship between the key and its ciphertext and drastically changes the ciphertext as compared to plain text. Sometimes Chaos need a dimensional table to encrypt data, but as the dimensional table size increase, its performance may degrade with it.

Genetic Algorithm [3] is a very new topic introduced to cryptographic systems. Generally, genetic algorithm based attacks are getting popular due to its better optimization and learning techniques. In cryptography, we can use population generation, crossover and mutation properties of the genetic algorithm. Repeated cycle and mutation of data encrypts data at a very extreme level with high degree of randomness. Original data cannot be extracted using brute force and statistical attacks. Randomness along with the permutation makes algorithm robust and reliable.

IV. PREVIOUS WORK RELATED TO AUDIO SECURITY.

S. Sharma et.al. in [4] worked on implementing RSA algorithm for audio encryption. They later found that RSA algorithm was efficient only on lower frequencies of audio.This result was expected as audio contains the negative value of amplitude which could have been left unrecoverable after applying transformations.

Rahul R. Upadhyay in [5], introduced a way to convert an audio file into image format successfully using MATLAB. This research helped him to introduce a new factor of ambiguity/confusion to his work. He completed this technique on WAV file format which is most widely used audio format. This image format can also be converted back into audio. Also this research open doors for image steganography for audio encryption.

Bismita Gadanayak et.al. in [6] worked to analyze the performance of total AES and total DES vs. selective AES when applied to an audio. They found that selective AES have better time complexity that compared to total AES or DES. Selective encryption in audio

takes much lesser time to degrade audio quality. It should be noted that total AES and DES will be more secure that selective AES, but time complexity of total AES/DES will make them impractical to use.

Narendra K Pareek et.al. in [3] successfully applied genetic algorithm technique to encrypt a greyscale image and then decrypt it back into original image without any loss of data. This encryption provided a very high amount of randomness and mutation changed data entirely from original data.

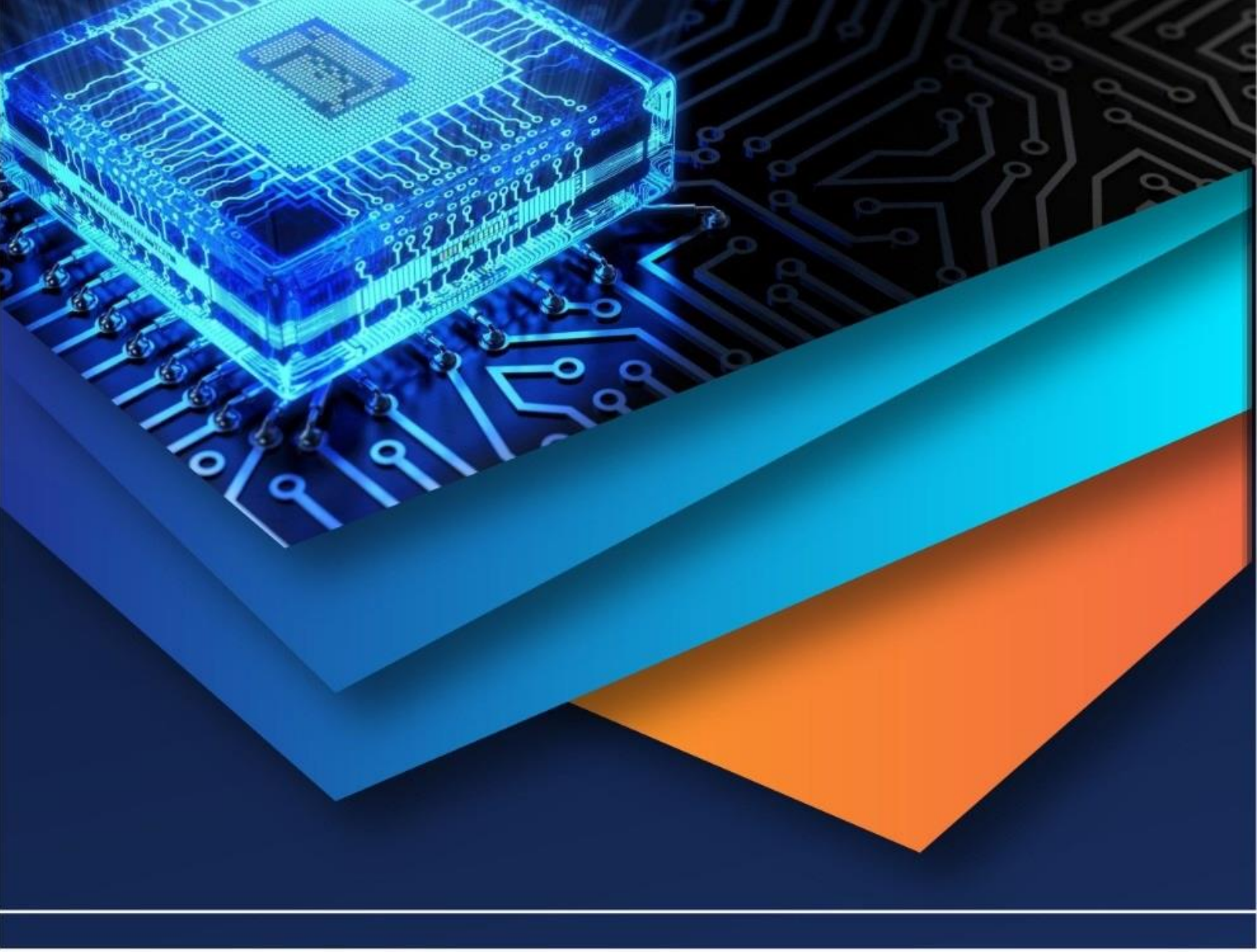
Abdelfatah A. Tamimi et.al. in [7] implemented audio encryption using the audio shuffling technique. The frequency value of audio is shuffled in a fixed permutation that the audio becomes inaudible as its meaning is changed and it's very hard to understand. Although this method is effective but original, values of amplitude are still intact in this system making it prone to statistical and brute force attacks.

V. CONCLUSION

After reviewing and studying works done by different authors and learning about encryption algorithms and the techniques to increase their complexity, we can say that there is more scope of research in this field. Using Genetic Algorithm with audio media conversion can help us to build a more complex and reliable new encryption algorithm for audio security. By merging more than two techniques one can build a new system to secure audio data with more reliability and performance.

REFERENCES

[1] [RFC2828],"Internet Security Glossary", http://www.faqs.org/rfcs/rfc2828.html.
[2] S. Ganesh Babu and P. Ilango, "Higher dimensional chaos for Audio encryption," IEEE Symposium on Computational Intelligence in Cyber Security, Singapore, 2013, pp. 52-58.
[3] Narendra K. Pareek and Vinod Patidar, “Medical image protection using genetic algorithm operations,” Soft Computing, Volume 20, Issue 2, pp. 763-772, February 2016
[4] S. Sharma, L. Kumar, and H. Sharma. “Encryption of an audio file on lower frequency band for secure communication,” International Journal for Advanced Research in Computer. Science & Software Eng., 3, no. 7, 79-84, 2013.
[5] Rahul R Upadhyay, “Study of Encryption and Decryption of Wave File in Image Formats,” International Journal of Advanced Networking and Applications, Vol.5, Issue7,2013
[6] Bismita Gadanayak, Chittaranjan Pradhan, and Utpal Chandra Dey “ Comparative Study of Different Encryption Techniques on MP3 Compression,” International Journal of Computer Applications, Volume 26– No.3, July 2011.
[7] Abdelfatah A. Tamimi and Ayman M. Abdalla, “An audio shuffle-encryption algorithm,” World Congress on Engineering and Computer Science Volume 1, October 2014



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY