A Study on Current Scenario of Audio Encryption

Rashmi A. Gandhi
MCA Department
Shri Sunshine College, Rajkot, Gujarat

Atul M. Gosai, Ph.D.
Department of Computer Science
Saurashtra University, Rajkot, Gujarat

ABSTRACT
Cryptography is the backbone for secure communication over networks. The rapid growth of digital data and its security raises the concern for developing more advanced techniques in cryptography. Cryptography is the physical process that scrambles the information by rearrangement and substitution of content, making it unreadable to anyone except the person capable of unscrambling it. Whereas the techniques used for deciphering a message without any knowledge of enciphering is called as Cryptanalysis i.e., "breaking the code". Now cryptography is not limited to only text data. Algorithms are also there for different data like image, audio, video etc. Throughputs, Speed, CPU time, Battery power, memory requirement are few parameters on which cryptographic algorithms are analyzed. In the present paper analysis of some common algorithms like DES, 3DES, AES, Blowfish, Twofish, ThreeFish, RC4 and RC6 are conducted on the above parameters to find out a best solution. This paper provides a comprehensive introduction about some of the existing cryptographic techniques and their performance for all data types particularly audio files.

Keywords
Cryptography, Bio-Cryptography, LFSR (Linear Feedback Shift Register), ASG (Alternating Step Generator), avalanche effect

1. INTRODUCTION
In the present day digital world importance of networks, their effect and their presence can't be ignored. The widespread use of digital data in real life applications and their importance have craved the need of new and effective ways to ensure their security. The quick development in computer technologies and internet had made the security of information as most important factor in information technology and communication.

Information security is the techniques, policies and strategies used to protect and secure computer systems and important information.

Cryptography makes the data incomprehensible to outsiders by various transformations. Here the enemy is allowed to detect, intercept and modify messages without being able to violate certain security premises guaranteed by a cryptosystem.

Just a decade or two before peoples are used to only text data. So emphasis was there only on how to encrypt/decrypt text data. But with the growing use of internet and multimedia data, now there emerges the need for multimedia data security.

Now a day's audio encryption is more required to propagate encrypted voice communication between parties for real time application like voice talk between intelligence bureau officials, CBI officials, defense etc for top secret communication. With the help of audio encryption other hackers or persons with malicious intention will not be able to decrypt such communication for national security [5].

Cryptography at present becomes the backbone of modern security system for secure data communication. With the large scale use of multimedia data like audio files in its different format it now becomes utmost important for its secure transmission without affecting quality.

The message that needs to be protected and communicated is called as plaintext. The method of scrambling the plaintext to make it undetectable is called encryption. The output of encryption process is the ciphertext. The process of getting back plaintext from ciphertext is called decryption. A system that performs encryption and decryption is called cryptosystem. Security of any cryptosystem should depend on the security principle proposed by Kirchhoff. According to the Kirchhoff, the security of the encryption system should depend on the secrecy of the encryption/decryption key rather than encryption algorithm [9].

This paper is intended to provide an overview of the different algorithms used for Audio Encryption. It demonstrates the suitability of various techniques for different applications. Structure of the paper is as follows: Section 2 gives an overview of Cryptography and its Concepts and types. Section 3 specifies a quick overview of the most popular algorithms for Cryptography. Section 4 provides performance evaluation of different encryption techniques in different situations for different data types. Section 5 describes limitations of existing techniques and future improvements are suggested. Conclusion is provided by authors in section 6.

2. OVERVIEW OF CRYPTOGRAPHY
Cryptography is the science of information security. The word is derived from the Greek words *kryptos*, meaning "hidden" and *graphia* meaning "writing or study".

Cryptography is the physical process that scrambles the information by rearrangement and substitution of content, making it unreadable to anyone except the person capable of unscrambling it. In other words a given message is coded into a secure message (ciphertext) by applying some substitution techniques, to make the input message unreadable by anyone during its transmission. Only the intended recipient is able to decode it. With the vast growth of data transmission over internet, its security became a great concern. Since no cryptographic scheme is foolproof, the idea is to make the cost of acquiring information more than the information itself.

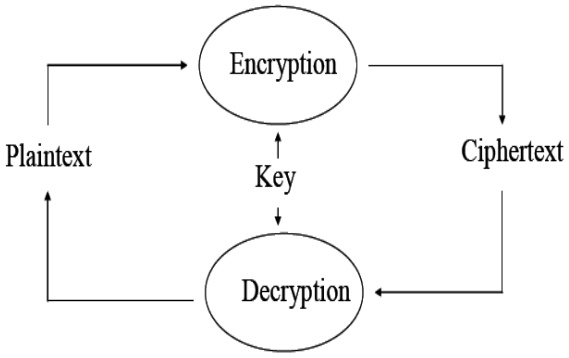

Fig:1 A General Model of Cryptography

2.1 Objectives of Cryptography

Modern cryptography deals with following four objectives:

1) **Confidentiality:** The information cannot be understood by anyone other than its intended uses.

2) **Integrity:** The information cannot be altered in storage or transit between sender and intended receiver without the alteration being detected.

3) **Non-repudiation:** The creator/sender of the information cannot deny at a later stage his or her intentions in the creation or transmission of the information.

4) **Authentication:** The sender and receiver can confirm each other's identity and the origin/destination of the information.

2.2 Different Types of Cryptography

Cryptographic systems can be divided into three independent dimensions:

1. The type of operations used for transforming plaintext to ciphertext:
   - **a)** **Substitution**: Each element in the plaintext is mapped into another element.
   - **b)** **Transposition**: Elements in the plaintext are rearranged.

   In both the schemes, the operation must be reversible that is no information should be lost.
2. The number of key used:
   - **a)** **Symmetric**: Single key, secret key, private or conventional encryption- Sender and receiver use the same key.
   - **b)** **Asymmetric**: Two keys or public key encryption. Sender and receiver use the different key.
3. The way in which plaintext is processed:
   - **a)** **Block Ciphers:** Processes each input block one at a time, producing an output block.
   - **b)** **Stream Ciphers:** Processes input elements continuously, one element at a time.

The widely used symmetric algorithms are DES, 3DES, AES, Blowfish, RC4, RC6, Twofish and Threefish. Rivest-Shamir-Adelman (RSA) and Elliptic Curve Cryptosystem (ECC) are the commonly used asymmetric key algorithms.

3. CRYPTOGRAPHIC ALGORITHMS AT A GLANCE

3.1 DES

DES is a block cipher based on minor variation of Feistel structure [1,2,9]. It was issued in 1977 as FIPS PUB 46 (Federal Information Processing Standards) by NIST (National Institute of Standards & Technology) and then widely used for more than two decades. The plaintext is processed in 64-bit blocks. The key is 56bits in length, which is divided into 16 sub keys for 16 rounds of processing; each one is used for each round. Decryption is same as encryption where ciphertext is used as input to DES and sub-keys Ki are used in reverse order i.e. from K16 in fast round to K1 in last round. With 56 bit key there are 2^{56}= 7.2 x 1016 possible keys are available which makes brute-force attack impractical.

But DES finally and definitively proved insecure in July 1998, when the Electronic Frontier Foundation (EFF98) announced that it had broken a DES encryption using a special-purpose "DES Cracker".

3.2 3DES

Triple DES (3DES) was first standardized for use in financial applications in ANSI standard X9.17 in 1985. It was incorporated as part of the Data Encryption Standard in 1999, with the publication of FIPS PUB 46-3. It is the FIPS approved symmetric block cipher. It is working on 64 bit plaintext with 168 bit key length making brute force attack impossible. It is working as Encrypt-Decrypt-Encrypt sequence and use three keys and three executions of the DES algorithm. 168 bit key length provides it resistant to cryptanalysis. But it is relatively sluggish in software, does not produce efficient software codes and slower due to 3 times more rounds then DES.

3.3 AES

Both DES and 3DES are not good candidates for long term security, NIST in 1997issues a call for proposals for a new Advanced Encryption Standard [1,2,9]. Out of the proposal in first round, 15 algorithms were accepted, out of which in 2nd round 5 algorithms were shortlisted and out of them NIST selected Rijndael as the proposed AES algorithm. AES uses block length of 128 bits and a key length that can be 128, 192 or 256 bits. It is iterative not like Feistel Structure.

3.4 Blowfish

Blowfish [1,2,9] is a keyed block cipher designed in 1993 by Bruce Schneier and widely used in a large number of cryptographic products. It provides good performance in software. Blowfish has 64 bit block size and a variable key length from 32 bit to 448 bits. The algorithm works in two parts: A key expansion part and a data encryption part. The key expansion part is to convert a key of at most 448 bits into several sub key arrays totaling 4168 bytes. The data encryption is by a 16 round Feistel structure and uses a large key dependent S-Boxes.

It is suitable for applications where the key does not change often, like communications link or an automatic file encryption. It is comparatively faster than most encryption algorithms when implemented on 32 bit microprocessors with large data caches.

3.5 RC4

RC4 [11] is a stream cipher designed in 1987 by Ron Rivest for RSA Security. It is officially termed as "Rivest Cipher 4".

It is a variable key-size stream cipher with byte-oriented operations. Stream ciphers are more efficient for real time processing. The algorithm is based on a random permutation. The period of cipher is greater than 10^{100}. Eight to sixteen machine operations are required per output byte. It is simple and quite easy to explain. RC4 was kept as a trade secret by RSA Security. But in September 1994, the RC4 algorithm was posted on the Internet on the Cypherpunks anonymous remailers list. The algorithm can be efficiently implemented in both hardware and software.

3.6 Twofish

Twofish [19] is an algorithm from counterpane Internet Security. It is highly suited for large microprocessors and also for smart card microprocessors. Twofish was designed to meet NIST's design criteria for AES. It is based on Feistel network. Specifically, they are a 128-bit symmetric block cipher with key lengths of 128 bits, 192 bits, and 256 bits. It is working efficiently both on the Intel Pentium Pro and other software and hardware platforms. It supports flexible design like accept additional key lengths, can be implementable on a wide variety of platforms and applications.

3.7 ThreeFish

Threefish block cipher was designed by Niels Ferguson et al. They designed them with speed, security, simplicity, and flexibility in mind. Threefish is a large tweakable block cipher [21]. Tweak serves the purpose of initialization of vectors. It is defined for three block sizes: 256, 512, and 1024 bits. The key size is equal to the block size while the tweak value is 128 bits regardless of the block size. Instead of S-boxes, Threefish uses XOR and modulus addition to achieve non-linearity and hence good security. It is also suitable for hardware and software implementations especially in 64-bit platforms since it operates on words of 64-bit size.

4. BACKGROUND AND RELATED WORKS

To concentrate on the work of Audio Encryption, all types of cryptographic algorithms are analyzed. In the present work media type as well as wired and wireless media is of great concern. While analyzing all the algorithms, factors like throughput, speed, and security are important but the need of computing resources like CPU time, memory and battery power is of utmost concern. These resources are limited in wireless environment. So while considering symmetric or asymmetric encryption algorithm it can be observed that public key encryption is based on mathematical functions, computationally intensive and is not very efficient for small mobile devices [17]. Asymmetric encryption techniques are almost 1000 times slower than Symmetric techniques due to the high amount of computations.

Again with Symmetric ciphers, block ciphers and stream ciphers play important role. A block cipher processes one block of data at a time while a stream cipher processes input elements continuously one element at a time. While encrypting an offline file and sending it over networks block cipher will give good result whereas encrypting real time data on a network in a continuous basis stream cipher will be a better solution. Since the present work is focusing on stored audio files all the algorithms discussed in the previous section are symmetric block ciphers.

Researchers in paper [10,17] had compared the common encryption algorithms like DES, AES, RC2, RC6, 3DES, and Blowfish on parameters like power consumption, Encryption time, CPU process time, CPU clock cycles and had came to the conclusion that Blowfish has better performance than all other algorithms followed by RC6. AES gives better performance than DES, 3DES and RC2. With changing data types like audio and video files the Blowfish continues to be superior. Increasing key size improves security but shows clear increase in battery and time consumption.

Researchers in paper [1] have compared DES and AES on avalanche effect, memory requirement, and time needed for encryption. AES is a better alternative when less memory is required and also with faster encryption. DES is best suited for financial applications. AES is better alternative while encrypting message sent between objects via chat-channels and is useful for objects that are part of a game and anything that is involved in monetary transaction.

For all practical applications, performance and speed are of prime concern. Keeping these factors in mind, in paper [2], researchers have compared DES, AES, 3DES, and Blowfish on different sizes of data blocks and different hardware and software platforms. The outcome is the Blowfish as the best performing algorithm under the security against unauthorized attack. Experiments show that 3DES has almost 1/3 through put of DES or in other words DES is 3 times faster than 3DES.

Since Blowfish is fastest and provides great security with strong key size, it can be used in many applications like Bulk encryption, Random Bit Generation, Network security and packet encryption. Despite all of these advantages it yet suffers from weak key problem which need to be rectified and explored.

Researchers in paper [11] have again confirmed the choice of symmetric algorithms above asymmetric algorithms. They have compared AES and RC4 on parameters like throughput, CPU process time, memory utilization, encryption/decryption time, key size variation and confirmed that RC4 is fast and energy efficient as compared to AES. RC4 can encrypt large amount of data.

4.1 Related work on Audio Encryption

Keeping the volume of audio files in mind researchers in paper [8] have discussed that all encryption techniques can be classified into three broad categories like: Complete encryption, Selective encryption and combined compression-encryption approach.

The complete encryption approach is the traditional way to accomplish content confidentiality which encrypt the whole file with the help of traditional ciphers like DES, AES, 3DES, RC$, or RSA. This leads to high processing and computational complexity. The selective encryption approach encrypts the parts of a multimedia file to reduce the computational requirements of the client side in real time applications. The major issue in this approach is to select the important data that need to be encrypted. The Combined compression encryption approach combines the compression process and the encryption process in a single step.

In their work, researchers of paper [8] had taken full encryption approach for real time multimedia data like image, audio, and video communication applications. A complete Binary tree performs substitution and a two dimensional array performs the linear diffusion. The experimental results prove the algorithm a success with some start-up delay. Researchers are trying to implement their work in embedded/mobile applications.

Researchers in paper [3] have introduced the concept of Bio Cryptography. They have taken AES algorithm as the base for encryption with secret key extracted from iris features. Audio signals taken in real time are converted to binary form using MATLAB. The 128 bit secret key is obtained from iris image. The key with more randomness is selected to increase the security.

Researchers in paper [7] have proposed a novel higher dimensional chaotic system for audio encryption in which variables are treated as encryption key for secure transmission of audio signals. This technique is suitable for large scale data encryption like audio, image and video. The algorithm has the characteristics of sensitive to the initial condition, high key space, pixel distribution uniformity and the algorithm will not break in known/chosen plaintext attack. This algorithm has a good key sensitivity that is the change of a single bit in the secret key should produce a completely different encrypted audio.

Researchers in paper [9] have compared DES, AES and Blowfish on processing time and throughput for audio and video files. They have found AES as a better solution.

In paper [4] researchers have applied RSA encryption technique on the lower frequency bands, since all frequency regions do not participate equally in communication. The purpose is to differentiate important audio information from less significant audio information, based on which selective encryption can be done. They have suggested to improve efficiency of encryption by applying modified RSA or improved DES in future.

In paper [14, 22] researchers have considered total AES, Total DES and selective AES on audio files. The time consumption and SNR values (Signal to Noise Ratio) are calculated for the above described algorithms. Large size of audio files results in more time for encryption/decryption. So audio file is compressed and then selective encryption is applied on it. Finally they had concluded that selective encryption is better than full encryption in terms of performance.

In Paper [13], researchers suggest an efficient encryption technique based on transposition and substitution ciphers. Reversible lossless audio encryption is yet a dream to be fulfilled. So huge prospects is there in implementing cryptography for online applications.

In paper [14], researchers have applied AES technique on the quantized audio data which is performed before the Huffman's entropy coding. Experimental results demonstrate that AES encryption technique provides high security against cryptographic attacks.

Here, the encryption technique is applied to the whole audio data, so it makes difficult for the unauthorized user to access the audio data. Thus, the AES encryption technique enhances the Cryptographic security of the MP3 audio content. A very less discussion is available for .mp4 audio data.

Researchers in paper [6] have concentrated on secure distribution of compressed audio without affecting its quality. Selective encryption is done using stream ciphers generated based on modular division circuit and LFSR. Encryption is done by XORing the audio data with key. Key is obtained using LFSR (Linear Feedback Shift Register). The proposed technique has less hardware complexity and capable of resisting different types of attacks like ciphertext only attack and known plaintext attack. The technique is suitable for encrypting MP3 audio format as well as other forms of audio for commercial as well as confidential applications.

In paper [12] researchers have advocated Selective encryption approach as compared to Full encryption approach. They have compared some of the existing selective encryption techniques against full encryption and came to the conclusion that full encryption techniques are slow whereas selective encryption techniques save computational power, overhead, speed and time.

Researchers in paper [16] have suggested that block cipher algorithms like DES, AES and public key systems are not suitable for real time audio data due to complexity and lesser speed. In their work researchers have taken selective audio encryption method with lower implementation costs and compatible with standards.

Here Audio data is encoded based on LFSR based key stream generators. The long key stream generated from modified ASG is divided into smaller key stream so that it can be used as the different key streams for different frames of audio data. The proposed algorithm is secure against known plaintext attack and is compatible to any audio coding standards.

Researchers in paper [15] are considering selective encryption technique with a different approach. In this paper the power spectrum of an audio wav file is partially encrypted using RSA encryption technique. A time domain audio signal is converted to transform domain signal (frequency domain) by using Fast Fourier Transform. A transform domain can separate a signal into different frequency regions with respective magnitude and phase values. Then encryption technique is applied to the low frequencies which have higher magnitude values.

Though the technique can be considered as a good solution in terms of cryptanalysis attacks but it needs substantial efforts in identifying important and unimportant portions in audio sample dynamically.

In paper [19] researchers have analyzed AES and Twofish algorithms on security and performance on different size of RAMs for different data types. It was found that AES has a safety factor less than 2 which makes it prone to cryptanalysis attack. To make AES at par with Twofish in terms of security 24 rounds are needed which results in reduced performance.

It was observed that for text and image encryption, AES is faster than Twofish but with increasing RAM Twofish becomes faster than AES. For Sound Encryption Twofish performs better and with increasing RAM size its speed increases.

Blowfish's creator in 2007 recommended Twofish as compared to Blowfish. In the recent work researchers in paper [18] have demonstrated modified Blowfish which is a symmetric block cipher which takes variable length key from 32 bits to 448 bits. In the modified algorithm, for the same input plaintext each time different ciphertext is generated and it's less time consuming and gives more throughputs. Researchers are willing to continue with modified Blowfish for image, audio and video applications.

Researchers in paper [20] have used Blowfish algorithm for encrypting an image with the file formats like TIF, .bmp, PNG, and jpg. They have found that Blowfish can't be broken until an attacker tries 28r+1 combinations where r is

the number of rounds. By increasing the number of rounds, security of the algorithm can be increased.

5. LIMITATIONS

After studying a number of research papers it was found that all audio encryption techniques can be divided into either full encryption or partial encryption. While analyzing full and partial encryption it was found that a good amount of overhead increases with partial encryption like: identifying important/ unimportant audio data, to encrypt the important audio data, to merge the encrypted audio data with unimportant audio data, then finally sending it over communication network. At the receiving end same efforts have to be given for separating encrypted and unencrypted data, finally the important audio information needs to be taken out of encrypted data. It increases complexity in algorithm. Another factor should be concentrating on fixed audio file or real time audio.

6. CONCLUSION

The work presented here demonstrates that enough scope is left for research in this field. So we need to design a new algorithm that will provide full encryption, less complexity, high energy efficiency in terms of CPU time and high transmission speed. It is also considering reversible effective original audio generation based on speed and time with higher security key and less noise in original encrypted audio. So our work is trying to focus on Design and implementation of a new algorithm for audio encryption based on above parameters.

7. REFERENCES

[1] Akash Kumar Mondal, Chandra Prakash, and Mrs Archana Tiwari "Performance Evaluation of Cryptographic Algorithms: DES and AES",IEEE Students' Conference on Electrical, Electronics and Computer Science, 2011.

[2] O P Verma, Ritu Agarwal, Dhiraj Dafouti, Shobha Tyagi, "Performance Analysis Of Data Encryption Algorithms", IEEE, 2011.

[3] Sruthi B. Asok, P.Karthigaikumar, Sandhya R, Naveen Jarold K, N.M Siva Mangai, "A Secure cryptographic scheme for Audio Signals", International Conference on communication and Signal Processing, April 3-5, 2013, India.

[4] Sheetal Sharma, Lucknesh Kumar Himanshu Sharma, "Encryption of an Audio File on Lower Frequency Band for Secure Communication", International Journal of Computer Science and Software engineering, volume 3, Issue 7, July -2013.

[5] Rashmi A. Gandhi, Dr. Atul M. Gosai, "Steganography – A Sin qua non for Diguised Communication", International Journal of Innovative Research in Advanced Engineering", Vol 1, Issue 8, 2014.

[6] Shine P James, Sudish N George, Deepthi P P , "Secure Selective Encryption of Compressed Audio", International Conference on Microelectronics, communication and Renewable Energy, IEEE-2013.

[7] Ganesh Babu S, IIango. P, " Higher Dimensional Chaos for Audio Encryption " IEEE, 2013.

[8] N. Radha Aathithan, Venkatesulu. M, "A Complete Binary Tree Structure Block Cipher for real-time multimedia", Science and Information Conference 2013, October 7-9, London, UK.

[9] S. Pavithra, E.Ramadevi, "Throughput Analysis of Symmetric Algorithms", International Journal of Advanced Networking and Applications, Volume-4, Issue-2, Pages:1574-1577, 2012.

[10] Diaa Salama1, Hatem Abdual Kader, and Mohiy Hadhoud, "Evaluating The Performance of Symmetric Encryption Algorithms", International Journal of Network Security, Vol.10, No.3, Page.213-219, May 2010.

[11] Nidhi Singhal, J.P.S Raina, " Comparative Analysis of AES and RC4 Algorithms for Better Utilization", International Journal of Computer Trends and Technology, July-August, 2011.

[12] Saurabh Sharma, Pushpendra Kumar Pateriya, "A Study on Different Approaches of Selective Encryption Technique", International Journal of Computer Science and Communication Networks, Vol.2(6),658-662.

[13] Majdi Al-qdah, Lin Yi Hui, "Simple Encryption/Decryption Application", International Journal of Computer Science and Security, Vol.1, Issue.1.

[14] Bismita Gadanayak , Chittaranjan Pradhan , "Encryption on MP3 Compression". MES Journal of Technology and Management.

[15] *Sheetal Sharma, Himanshu Sharma and Lucknesh Kumar, "* Power Spectrum Encryption and Decryption of an Audio File", International Journal of Research in Computer Science, Volume 1, August-2013.

[16] Shine P James, Sudhish N. George, Deepthi P P, "An Audio Encryption Technique based on LFSR based Alternating Step Generator", IEEE Connect 2014.

[17] Diaa Salama1, Hatem Abdual Kader, and Mohiy Mohammad Hadhoud, "Evaluating the Effects of Symmetric Cryptography Algorithms on Power Consumption for Different Data Types", International Journal of Network Security, Vol.11, No.2, PP.78-87, Sep 2010.

[18] Rajendra Kumar, Balwinder Saini, Satish Kumar, "A Novel Approach to Blowfish Encryption Algorithm", International Journal of Advanced Foundation and Research in Science and Engineering, Vol.1, Issue.2, July 2014.

[19] Dr.S.A.M Rizvi, Dr.Syed Zeeshan Hussain, Neeta Wadhwa, "Performance Analysis of AES and Twofish Encryption Schemes", International Conference on Communication Systems and Network Technologies, 2011.

[20] Pia Singh, Prof.Kamaljeet Singh, "Image Encryption and Decryption Using Blowfish Algorithm in Matlab", International Journal of Scientific and Engineering research, Vol.4, Issue.7, July-2013.

[21] Khaldoon M. Mhaidat, Mohammad A. Altahat, Osama D. Al-Khaleel, "High Throughput Hardware Implementation of Threefish Block Cipher on FPGA".

[22] Raghunandhan K R1, Radhakrishna Dodmane2, Sudeepa K B3,Ganesh Aithal, "Efficient Audio Encryption Algorithm For Online Applications Using Transposition And Multiplicative Non-Binary System", International Journal of Engineering research And Technology, Volume 2, Issue 6, June-2013.