Enhanced security of audio signal using Logarithm based Encryption/Decryption

R.JeyaSundari[1], V.G.Sri Devi[2]
Department of ECE
[1]PG Scholar,PET Engineering College, Vallioor
[2]Assistant Professor,PET Engineering College, Vallioor

Abstract-*Cryptography plays an important role in the field of system security. There are many encryption/decryption strategies accessible right now to secure the information. This paper use a logarithm based encryption/decryption strategy of audio information with symmetric key cryptography. This is achieved by logarithm encryption of the audio signal using the secret key known only to the sender and desired receiver. Only the trusted receiver with the same secret key can decrypt the audio signal. Thus the logarithmic mathematical function can be used to improve the security of audio communication. The experimental results shows that the suggested algorithm yields an audio signal with high quality and low error rate as exact signal as the original signal.*

I. INTRODUCTION

Cryptography is the study of techniques for secure communication in the presence of third parties called adversaries. In general, cryptography is about constructing and analyzing protocols that prevent third parties or the public from reading private messages. Encryption is the process of encoding messages or information in such a way that only authorized parties can read it.Cryptographic systems can be classified into two categories: Secret-key (Symmetric) cryptosystems and Public-key (Asymmetric) cryptosystems. In this paper, asymmetric key is used.

Encryption does not of itself prevent interception, but denies the message content to the interceptor. In an encryption scheme, the intended communication information or message, referred to as plaintext, is encrypted using an encryption algorithm, generating cipher text that can only be read if decrypted. Decryption is the process of taking encoded or encrypted text or other data and converting it back into text that you or the computer can read and understand. This term could be used to describe a method of un-encrypting the data manually or with un-encrypting the data using the proper codes or keys. There are five cryptography goals Authentication, Secrecy or Confidentiality, Integrity, Non-Repudiation, Service Reliability and AvailabilityAuthentication: This means that before sending and receiving data using the system, the receiver and sender identity should be verified.

Secrecy or Confidentiality: Usually this function (feature) is how most people identify a secure system. It means that only the authenticated people are able to interpret the message (date) content and no one else.

Integrity: Integrity means that the content of the communicated data is assured to be free from any type of modification between the end points (sender and receiver). The basic form of integrity is packet check sum in IPv4 packets.

Non-Repudiation: This function implies that neither the sender nor the receiver can falsely deny that they have sent a certain message.

Service Reliability and Availability: Since secure systems usually get attacked by intruders, which may affect their availability and type of service to their users. Such systems should provide a way to grant their users the quality of service they expect.

Traditional encryption schemes do not work for multimedia data because of their large size and high redundancy. Therefore new encryption schemes have been proposed for multimedia data that are composed of two basic components: permutation of the pixel values and diffusion of the pixel values (XORing with a key) with ciphertext feedback (XORing with a previous iteration of the image) [2,3,4].These two components use pseudo random number sequences generated using a chaotic dynamic system. The two components are also performed alternately for several rounds. Such schemes have been broken using chosen-images attack where several plain-image, cipher-image pairs are known to the cryptanalyst [5,6]. This paper discusses an alternative chaos-based symmetric-key encryption algorithm for securing images and audio signals. We propose an encryption method for multimedia signals that do not allow masks to be of any use in the cryptanalysis. Unlike other popular encryption algorithms, this algorithm manipulates pixels rather than bits. These approach consists of two main components, scrambling data in a pseudorandom manner obtained through chaotic functions and many horizontal/vertical cyclic shift of

scrambled data to render encryption more complex to decipher.

II. PROPOSED METHOD

The acquired audio samples are encrypted using previously generated secret key yielding encrypted (or ciphered) samples. The ciphered samples are sequentially transmitted and when received,each sample is then decrypted at the receiver using the same secret key. It is assumed again, for simplicity, that the transmission channel is free of noise. The proposed method has both the encryption and decryption stages.

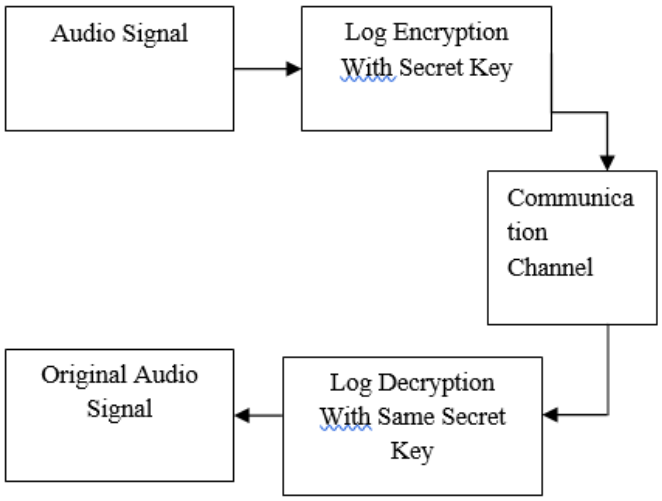

Fig.1 block diagram of audio encryption and decryption

The proposed algorithm is based on symmetric key method and due to the nature of audio signal as real values, the key will be assumed as real number (positive or negative). Assuming the value of the plain audio sample = ***p***, With the condition that-1 ≤ ***p*** ≤ 1, then the value of the ciphered audio sample ***S*** should be within the upper and lower limits as exactly as ***p***: -1 ≤ ***S*** ≤ 1. Assuming the secret key = (***a, b***), where ***a*** and ***b*** are real numbers, then applying the proposed encryption method, the value of the ciphered audio sample ***S*** can be calculated as following:

$$S = \log_b ap = \log_b a + \log_b p.$$

The transmitter sends the ciphered audio sample and assuming that it is purely received (free of noise), we can infer the value of the plain sample as following:
Rearranging Eq.1 yields

$$\log_b p = \log_b ap - \log_b a$$

$$_b[\log_b p] = b^{[\log_b ap - \log_b a]}$$

$$p = b^{[\log_b ap - \log_b a]}$$

$$p = \frac{b^{\log_b (ap)}}{b^{\log_b (a)}}$$

$$p = \frac{b^s}{a}$$

Audio signal is acquired using either a real audio file or real microphone. The encryption block receives the audio signal p and encodes it using (a, b) secret key while the decoder block decrypts it using the same secret key In this method, input variables a and b are set as 0.0003 and 300000 respectively.

Encryption is the process of converting a plaintext message into ciphertext which can be decoded back into the original message. An encryption algorithm along with a key is used in the encryption and decryption of data. There are several types of data encryptions which form the basis of network security. Encryption schemes are based on block or stream ciphers. Decryption is the process of transforming encrypted information so that it is intelligible again. A cryptographic algorithm, also called a cipher, is a mathematical function used for encryption or decryption,here logarithm mathematical function can be used for both encryption and decryption with secret keys a and b.The plain audio sample(p) is encrypted to produce cipher audio sample(s).This cipher audio sample (s) is decrypted to produce original audio plain sample(p).

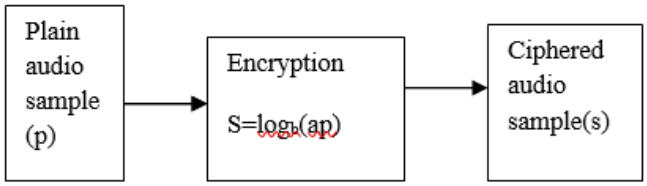

Fig.2 encryption algorithm

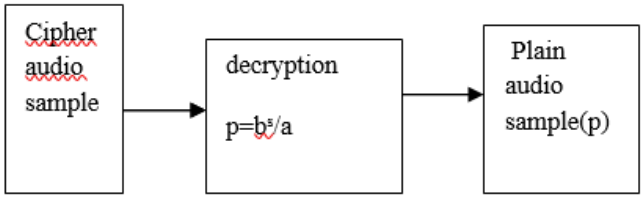

Fig.3 decryption algorithm

The working of encryption is a way to secure and verify data that are traded through public communication channels in the presence of intruder party called antagonists.

Consequently, the transmitted or stored message can be converted to unreadable form except for intended receivers. The decryption techniques allows intended receiver to reveal the contents of previously encrypted message via secrete keys exchanged exclusively between transmitter and receiver. These techniques offer a relatively high level of security and are compatible with today's technical environment. However, like cryptographic techniques, there is again a heavy dependence on synchronization between transmitter and receiver

III. RESULTS AND DISCUSSION

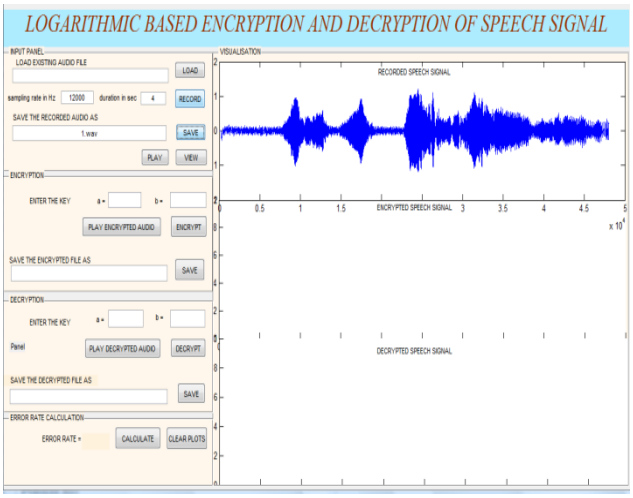

Fig.4 Recorded audio sample

Here, either real-time audio signal recorded using real microphone or a prerecorded audio file can be used as the audio input for the proposed system . Then the recorded speech signal can be plotted and saved in the directory.

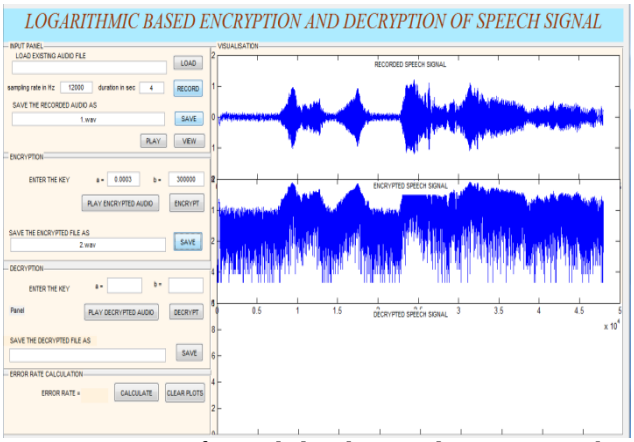

Fig.5 Encryption of recorded audio sample using secret key

Here the encryption of recorded audio signal using secret key(a,b) At the transmitter side, the key value of a and b is chosen as 0.0003 and 300000 respectively .Then the encrypted speech signals can be plotted and saved in the directory.if the value of a and b changes,the corresponding encrypted audio signal also changes and can be plotted at the same time.

Fig.6 Decryption of ciphered audio sample using secret key

The decryption of recorded audio signal using secret key(a,b)is performed At the receiver side , if the same key value is chosen (a and b is 0.0003 and 300000 respectively).Then the decrypted speech signal is same as the original recorded signal.The decrypted signal can be plotted saved in the specified directory. The ciphered and deciphered audio samples are traced and compared with the original acquired signal calculate the error rate.

Fig.7 Failed Decryption of ciphered audio sample without the right secret key

Here the value of secret key (a,b) is not same as the secret key chosen by the sender(a and b is 0.3and 3 respectively). Thus the decrypted speech signal does not match with the original signal thus unauthorized access of the audio signal can be avoided. From above fig 4.4 have mismatch decrypted signals with error rate 0.579.Thus the mismatched decrypted signal error rate was very high as compared to the matched decrypted signals error rate.

IV. CONCLUSION

The proposed logarithm based encryption and decryption algorithm with symmetric cryptography technique enhance the security of audio signal and having error rate is low.The Matlab software tool is used for implementing and

simulating via acquiring real-time audio signal and applying the encryption and decryption algorithms. The ciphered and deciphered audio samples are traced and compared with the original acquired signal and calculate the error rate. The suggested cipher method can be developed and can be applied to video signal.

ACKNOWLEDGEMENT

I would like to thank my guide V.G. Sri Devi, Assistant Professor, Department of ECE, PET Engineering College

REFERENCES

[1] Anupam Mondal and Shiladitya Pujari, "A Novel Approach of Image Based Steganography Using Pseudorandom Sequence Generator Function and DCT Coefficients", IJCNIS Vol. 7, No. 3, pp.42-49. February 2015.

[2] ElGamal.T, "A prublic key cryptosystem and a signature scheme based on discrete logarithms", in Advances in Cryptology (CRYPTO '84), Springer, vol. 196, pp. 10–18 1985.

[3] Gnanajeyaraman.R, K.Prasadh , Dr.Ramar, Audio encryption using higher dimensional chaotic map, International Journal of Recent Trends in Engineering, Vol. 1, No. 2, May 2009.

[4] Jingli Zheng, Zhengbing Hu, Chuiwei Lu, "A Lightweight Symmetric Encryption Algorithm Based on Feistel Cryptosystem Structure", IJCNIS, Vol. 7, No. 1, pp. 16-23. December 2014.

[5] Koumal Kaushik and Suman, "An Innovative Approach for Video Steganography", IJCNIS, Vol. 7, No. 11,pp. 72-79,October 2015.

[6] Mamta. Juneja, and Parvinder S. Sandhu, "A Review of Cryptography Techniques and Implementation of AES for Images", International Journal of Computer Science and Electronics Engineering (IJCSEE) Volume 1, Issue 4 ISSN 2320-401X; EISSN 2320-4028-2013.

[7] Meligy.M, Mohammed M. Nasef, Fatma T. Eid, "An Efficient Method to Audio Steganography based on Modification of Least Significant Bit Technique using Random Keys", IJCNIS Vol. 7, No. 7, pp. 24- 29 June 2015.

[8] Ritesh D.Yelane, Nitiket. N. Mhala and B. J. Chilke, "Security Approach by Using Visual Cryptographic Technique", ijarcsse, Vol. 5, No. 1, January 2015.

[9] Sheetal Sharma and Lucknesh Kumar, 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, Issue 7, July 2013.

[10] Thiruppathy Kesavan, V, "Secret Key Cryptography based Security Approach for Wireless Sensor Networks", (RACSS), International Conference, IEEE 2012.

[11] Ueli Maurer and Björn Tackmann, "On the Soundness of Authenticate-then-Encrypt: Formalizing the Malleability of Symmetric Encryption", Proceedings of the 17th ACM Conference on Computer and Communication Security, ACM, pp. 505–515, Oct 2010.

[12] Ueli Maurer and Stefano Tessaro, Basing {PRF}s on Constant-Query Weak {PRF}s: Minimizing Assumptions for Efficient Symmetric Cryptography Advances in Cryptology Lecture Notes in Computer Science, Springer-Verlag, vol. 5350, pp. 161– 178, Dec 2008.