Audio Encryption Framework Using the Laplace Transformation

Mardan A. Pirdawood[1], Shadman R. Kareem[1,2] and Dashne Ch. Zahir[1]

[1]Department of Mathematics, Faculty of Science and Health, Koya University,
Kurdistan Region – F.R. Iraq
[2]Department of Computer Science, College of Information Technology and Computer Sciences, Catholic University in Erbil,
Kurdistan Region – F.R. Iraq

Abstract—**Digital information, especially multimedia and its applications, has grown exponentially in recent years. It is important to strengthen sophisticated encryption algorithms due to the security needs of these innovative systems. The security of real-time audio applications is ensured in the present study through a framework for encryption. The design framework protects the confidentiality and integrity of voice communications by encrypting audio applications. A modern method of securing communication and protecting data is cryptography. Using cryptography is one of the most important techniques for protecting data and ensuring the security of messaging. The main purpose of this paper is to present a novel encryption scheme that can be used in real-time audio applications. We encrypt the sound using a combination of an infinite series of hyperbolic functions and the Laplace transform, and then decrypt it using the inverse Laplace transform. The modular arithmetic rules are used to generate the key for the coefficients acquired from the transformation. There is no loss of data or noise in the decryption sound. We also put several sound examples to the test.**

Index Terms—**Cryptography, Laplace transformations, Maclaurin series, Sound encryptions.**

I. Introduction

Since the invention of written language, people have yearned to communicate in secret. Imagine sending a message to someone, but being concerned that someone else might view it, read the letter, or hear the electronic message (Mel and Baker, 2001). Conventionally, cryptography is used to provide confidentiality and integrity through encryption methods. Plaintext is the message to be communicated, and it can be text, numerical data, audio, executable programs, or anything else. In a cryptographic system, the original message to be transmitted is called the plaintext. In cryptography, mathematical techniques can be incredibly beneficial. The encryption method varies depending on the key, which alters the algorithm's technical operation. The cryptographic framework transfers plaintext to ciphertext (we keep messages secret by turning them into a code) so only the intended recipient can understand it (Delfs, Knebl and Knebl, 2002).

A considerable scope of investigation pertains to the governance and administration of security imperatives within the modern context framework of multimedia systems see (Ghadi, Laouamer and Moulahi, 2016) (El-Zoghdy, El-sayed and Faragallah, 2020). Audio data applications are extremely important and frequently used in multimedia systems (Kaur and Dutta, 2018; Liu, et al., 2017). The present research focuses on the creation of audio encryption algorithms that show attributes of low-power consumption, high real-time audio presence, and fast multimedia processing (Ghasemzadeh and Esmaeili, 2017; El-Zoghdy, El-sayed and Faragallah, 2020; Al-kateeb and Mohammed, 2020; Dutta, et al., 2020).

The creation of a physical phenomenon called sound is when anything vibrates. A sound wave requires a medium since sound is pressure variations traveling as waves. As previously mentioned, they could form this medium of solids, liquids, or gases. If these variances in specified weight fall within the run of human hearing, which contains a recurrence constraint of 20 Hz to 20 kHz, human eardrums will detect sound (Adriansyah, 2010).

Modern audio or voice applications also demand quick processing durations and low-power consumption. Traditional encryption techniques include symmetric algorithms such as ASE, DES, and public key algorithms such as RSA. While these techniques possess robust cryptographic features, they are unsuitable for low-profile audio applications considering their significant computational complexity. The development of audio encryption algorithms with calculative efficiency, real-time applicability, and effective multimedia processing capabilities is heavily emphasized in current research in digital security.

As Shannon (1998) suggested, diffusion and confusion are two of the key concepts in cryptography, and it is based on this idea that substitution and permutation operations networks (SPNs) become the foundation for many modern cryptography systems.

ARO-The Scientific Journal of Koya University
Vol. XI, No.2 (2023), Article ID: ARO.11165, 7 pages
DOI: 10.14500/aro.11165
Received: 20 February 2023; Accepted: 05 August 2023
Regular research paper: Published: 25 August 2023
Corresponding author's e-mail: mardan.ameen@koyauniversity.org

A single nonlinear component, such as a “substitution box,” creates confusion. In this case, we permute the data value based on a key parameter. As part of the diffusion operation, the data value is replaced by a random number or series of numbers instead of the actual data value. According to this study, both terms have intricate relationships among ciphertexts, plaintexts, and encryption algorithms with symmetric keys; substitution-permutation networks are used as fundamental structural components of algorithms that use symmetric keys by analysts and designers.

In recent years, a multitude of encryption techniques have been put forward for encrypting digital audio. Lima and da Silva Neto (2016), they proposed a cryptographic technique based on the cosine number transform (CNT) to encrypt digital audio, which is applied recursively to two blocks of samples of a non-compressed digital audio signal and specified over a finite field. He chooses the blocks by applying a straightforward overlapping rule, which makes sure that the ciphered data are diffused throughout all the blocks that have been processed.

Elliptic curve cryptography (ECC), a method of encrypting data using elliptic curves (EC), was first suggested by Miller (August 1985). The security provided by ECC, which employs the Public Key encryption technique and security it offers, is based on how difficult the discrete logarithm problem (DLP) is to solve. In later applications, elliptic curve (ECC) public key cryptography is gaining traction. The public key approach for audio encryption is provided by Singh, et al. (2014) using a cryptographic scheme based on the ECC mathematical operation. The presented work illustrates how each value of the audio file is converted to an EC point and uses the ECC encryption algorithm. To show how ECC is implemented, the audio file is first converted into an affine point on the EC over the finite field GF (p). The starting point for ECC, *Pm* (*x*, *y*), is an affine point that is on the EC. In this work, he provides how the encryption and decryption processes work.

The combination of different techniques allows us to create more security modules when it comes to security issues, as well as more reliable results when it comes to image processing. As stated by (Al-Khazraji, Abbas, and Jamil, 2022), they have developed an innovative approach that combines neural style transfer (NST) and deep dream techniques to generate a novel image that merges both these advancements. The utilization of pre-trained networks, namely VGG-19 for NST and Inception v3 for deep dream, was integral to their methodology. As a result, by combining these two techniques, you are able to enhance the images that simulate hallucinations that are being experienced by both psychiatric patients and drug addicts.

The works of Hayat, Azam, and Asif (2018) and Hayat and Azam (2019), as cited in the references, involved the development of an EC-based system designed to produce 8 × 8 S-boxes. This system took into account the significant influence of Modell’s Error-Correcting Codes (ECs) within a finite field context. Their research entailed the synthesis of a set of S-boxes utilizing both MEC and S_8 as symmetric groups. In the work by Khalid, et al. (2022), they explored the creation of a novel digital audio encryption method utilizing the Mordell EC (MEC) over a finite prime field within the context of the SPN. Their proposed approach consisted of two distinct components within the framework: the first aimed at managing confusion, while the second dealt with diffusion.

In recent years, unique characteristics of chaotic solutions, such as hypersensitive dependency, ergodicity, and pseudo-randomness, add a significant amount of unpredictability to deterministic nonlinear systems. Chaotic maps were widely used in various audio encryption frameworks. Kordov (2019) designed an audio encryption technique using an SPN structure and chaotic maps. In the study conducted by Shah, Shah, and Jamal (2020), they employed the SPN to propose an alternative method for audio encryption. Within their framework, they developed robust S-boxes for confusion by employing the Mobius transformation and the Hénon chaotic map. These S-boxes were then utilized for pixel-wise permutation to achieve diffusion.

The Laplace transform is a technique with several uses, such as wave equations, signals, systems, electrical circuit analysis, heat conduction, solar systems, hydrodynamics, communication systems, nuclear physics, and solar systems (Ramana, 2017). Lakshmi, Kumar and Sekhar, (2011) proposed a new cryptographic technique based on a new mathematical transformation for cryptography by employing Laplace transforms. In their work, a new approach to cryptography was introduced, involving the combination of a power series derived from the specific function *f(t)* and Laplace transforms. They created the key from the coefficients gained from the transformation by applying the modular arithmetic rules. Later, Hiwarekar (2013, July.) improved that cryptography technique in which the plain text was encrypted using the Laplace transform and cipher text decrypted using the inverse Laplace transform. Using Laplace transforms and infinite series expansion of the hyperbolic function, a new iterative encryption and decryption method has been developed (Hiwarekar, 2013).

We created a novel mathematical transformation for cryptography in this research, based on mixing hyperbolic functions and the Laplace transform for encrypting digital audio data and the corresponding inverse Laplace transform for decryption. The transform, defined over a finite field, is performed recursively to blocks of samples from a non-compressed digital audio input, where the secret key is used to determine how many times the transform is done to each of these blocks. Confusion approached with a power series coefficient. The technique we have employed has been previously utilized across various subjects by several researchers. For instance, Gencoglu (2019) innovatively employed the power series transform in cryptography to encrypt a specific sentence. This was accomplished through the utilization of the extended Laplace transform of an exponential function. The key is constructed by applying the principles of modular arithmetic to the transformation coefficients, while we use this method for encrypting digital audio files through the Maclaurin series of the cosine-hyperbolic transform in conjunction with the Laplacian transformation which is applied to the coefficients of the Maclaurin series.

II. Definitions and Basic Concepts

The science of information security is the art and science of secret writing or cryptography. The message's original format is plaintext. They reference the message in disguise in the encrypted text. They encased the last message to be conveyed in a cryptogram. Transforming plaintext into ciphertext is known as encryption. Translating plaintext from cipher text in the other direction is known as decryption. We know the person who decodes the communication as the encipherer (Nichols, 1996).

A. The Laplace Transform

The Laplace transform is a well-known integral transform in mathematics with several applications in science and engineering. It is the most essential integral transformation. Due to a variety of unique characteristics, the Laplace Transform can be thought of as a transformation from the time domain, where inputs and outputs are functions of time, to the frequency domain, where inputs and outputs are functions of complex angular frequency. Modern engineering system analysis and design strategies mainly rely on Laplace transform methods. The concepts of Laplace transforms are employed in a variety of scientific and technological domains, such as electric circuit analysis, communication engineering, control engineering, and nuclear physics (Lakshmi, et al., 2011). It is required to know the following Laplace transform findings:

B. Definition

If *f* (*t*) is a function defined for all t≥0, then its Laplace transform is defined as

$$L\{f(t)\} = F(s) = \int_0^\infty e^{-st} f(t)\,dt \tag{1}$$

for all values of s for which the improper integral converges.

Assuming the integral is present. A real or complex number (Hiwarekar, 2013, July.) is used here as the parameter *s*. The inverse Laplace transform is of the form:

$$L^{-1}\{F(s)\} = f(t) \tag{2}$$

that a limit of integrals across bounded intervals defines an inappropriate integral over an infinite interval that is,

$$\int_0^\infty e^{-st} f(t)\,dt = \lim_{M\to\infty} \int_0^M e^{-st} f(t)\,dt \tag{3}$$

The improper integral is said to converge if the limit in (3) exists; otherwise, it diverges or doesn't exist.

C. Linearity Property

The Laplace transform is a linear transform. It means that, if

$$L\{f_1(t)\} = F_1(s), L\{f_2(t)\} = F_2(s), \ldots, L\{f_n(t)\} = F_n(s),$$

then

$$L\{c_1 f_1(t) + c_2 f_2(t) + \ldots + c_n f_n(t)\} = c_1 F_1(s) + c_2 F_2(s) + \ldots + c_n F_n(s), \tag{4}$$

where c_1, c_2,…,C_n are constants.

III. Proposed Method

The application steps that boost the data security and privacy of this suggested hybrid model by combining cryptography and encryption technology are as follows.

D. Encryption

The Maclaurin series of *t* cosh *t* as follow:

$$t\cosh t = \sum_{i=0}^{\infty} \frac{t^{2i+1}}{2i!} \tag{5}$$

The suggested technique feeds an "audio1.wav" as a carrier input to do simulation studies. MATLAB was used to implement this proposed approach, and we use it with two data sound files (.wav). Figs. 2, 5, and 7 illustrate how the technique behaved during the encryption and decryption phases. Using the Matlab code [*x*, Fs] = outright ("audio1.wav"), we can get the vector that includes the values of the amplitude of our sample voice per second, which is the message that needs encryption. We consider the plot of the audio message to be as shown in Fig. 1. We convert the values of the vector *x* from decimal to integer form. To do this, we can choose the number of digits that should follow the decimal point. Let's say that there are a certain amount of digits following the decimal points (i.e., *m* is number of digits after decimal points.).

Then, the vector y=x*10^m, where *m*=15, as shown in Fig. 3. If we take *m* large, then the error will become small (i.e., the difference between the original audio and the decrypted audio depends on the value of *m*). Depending on the value of m, we ignore the decimal places while converting digital sound values, which are ordinarily decimal numbers, into

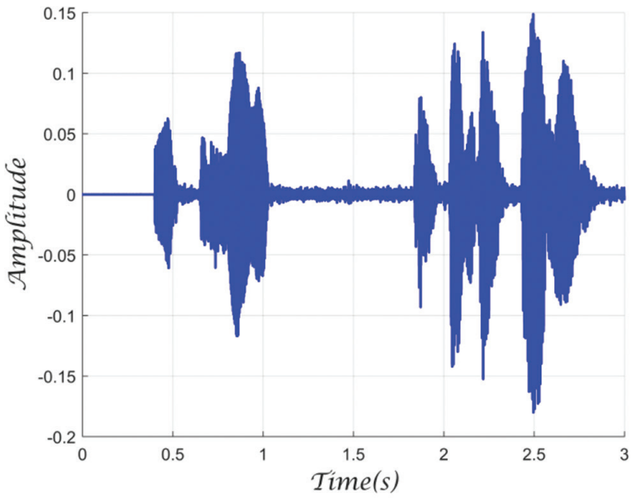


Fig. 1. Time domain plot of the "audio1.wave" signal.

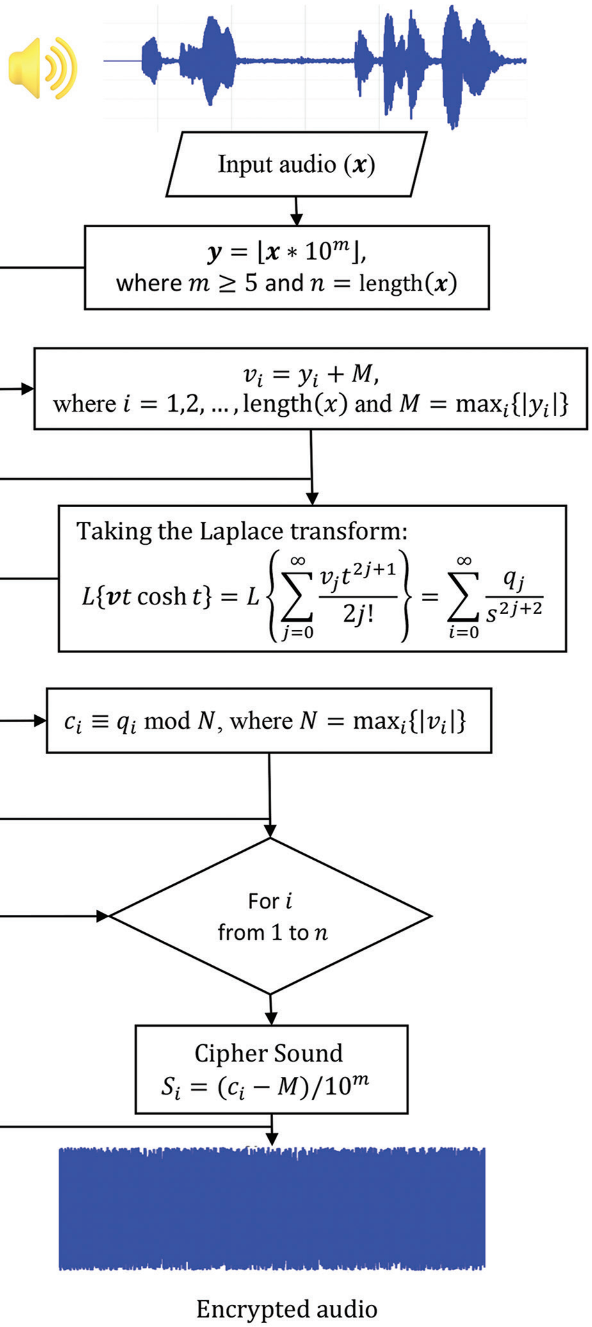

Input audio $(\boldsymbol{x})$
$\boldsymbol{y} = \lfloor \boldsymbol{x} * 10^m \rfloor$,
where $m \geq 5$ and $n = \text{length}(\boldsymbol{x})$
For i from 1 to n
$v_i = y_i + M$,
where $i = 1,2,\ldots,\text{length}(x)$ and $M = \max_i\{|y_i|\}$
Taking the Laplace transform:
$L\{\boldsymbol{v}t\cosh t\} = L\left\{\sum_{j=0}^{\infty}\frac{v_j t^{2j+1}}{2j!}\right\} = \sum_{i=0}^{\infty}\frac{q_j}{s^{2j+2}}$
For i from 1 to n
$c_i \equiv q_i \bmod N$, where $N = \max_i\{|v_i|\}$
For i from 1 to n
Cipher Sound
$S_i = (c_i - M)/10^m$
Encrypted audio

Fig. 2. Flow diagram of the proposed Laplace transformation audio encryption system.

integer numbers using the congruence module N.

For making the values of amplitude become non-negative, we do this calculation $v_i = y_i + M$ where M = max $|y_i|$. We did these calculations because we want the values to become between 0 and $N = \max_i |v_i|$, for i = 0,1,2,…,length (x) not face problems during the encryption and decryption when we take the congruence module N. Then, the plot of the amplitude per second of our audio signal sample is shown in Fig. 3. We can make the entries of on the vector v, as shown in Fig. 3 as a coefficients of the series as in equation (6) as follows:

$$f(t) = vt\cosh t = \sum_{i=0}^{\infty}\frac{v_i t^{2i+1}}{2i!} \qquad (6)$$

By taking the Laplace transform for $f(t)$, we will have

$$L\{f(t)\} = L\{vt\cosh t\} = L\left\{\sum_{i=0}^{\infty}\frac{v_i t^{2i+1}}{2i!}\right\} = \sum_{i=0}^{\infty}\frac{q_i}{s^{2i+2}} \qquad (7)$$

where $q_i = v_i\,(2i-1)$ for $i = 0,1,2,\ldots$

Changing the results values of q_i to mod N, where $N = \max_i |v_i| = 3288\times10^{11}$.The amplitude of our sample audio gets converted to cipher amplitude value, with key k_i for i=0,1,2,3,…. Hence, after calculating the amplitude sound vector s = $(c-M)/10^m$ the message audio 'audio1.wav' of Fig. 1 gets converted to Fig. 5, and it was encrypted.

Note that the amplitude of the audio in terms of i, i = 0,

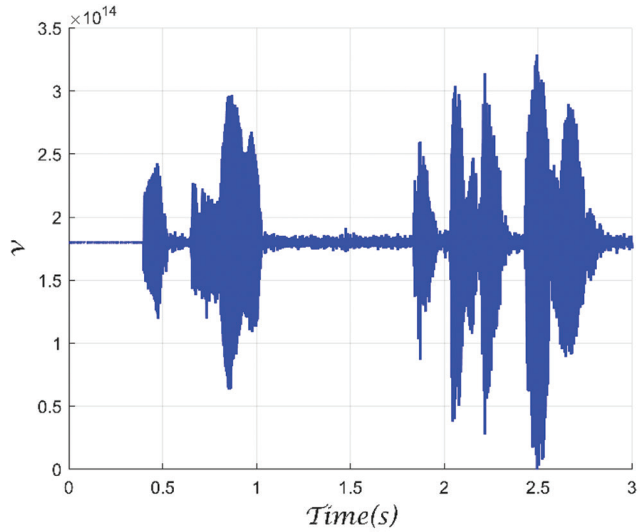


Fig. 3. The positive integer values of the amplitude per second need to be encrypted.

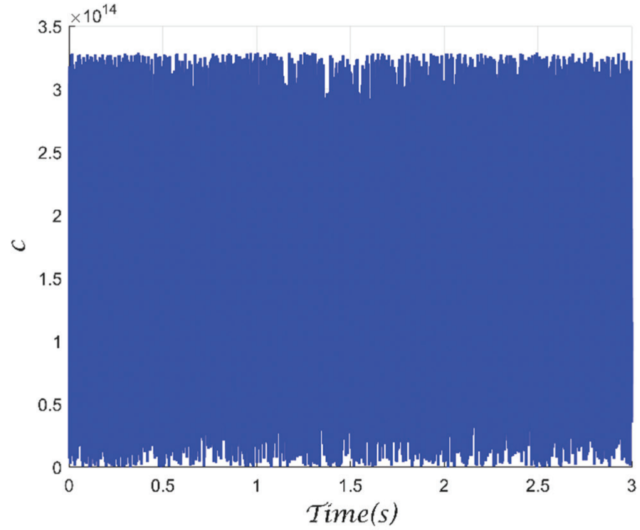


Fig. 4. The encrypted positive integer values of the vector *c*.

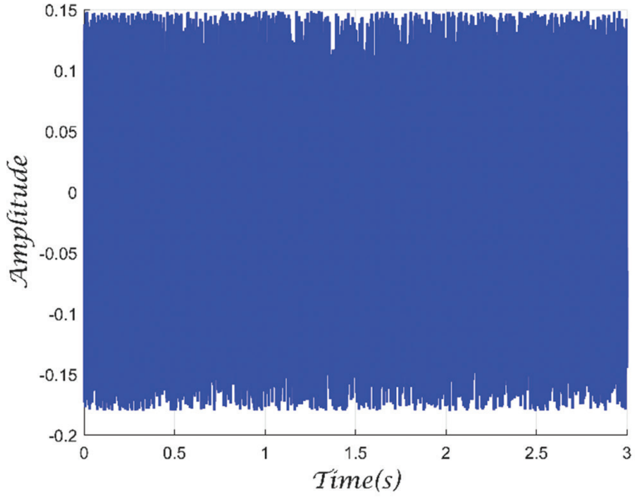


Fig. 5. The encrypted audio.

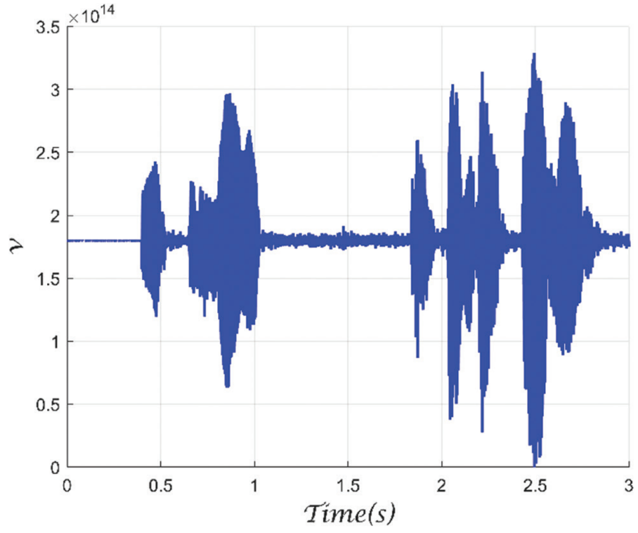


Fig. 6. The decrypted positive integer values of the vector *v*.

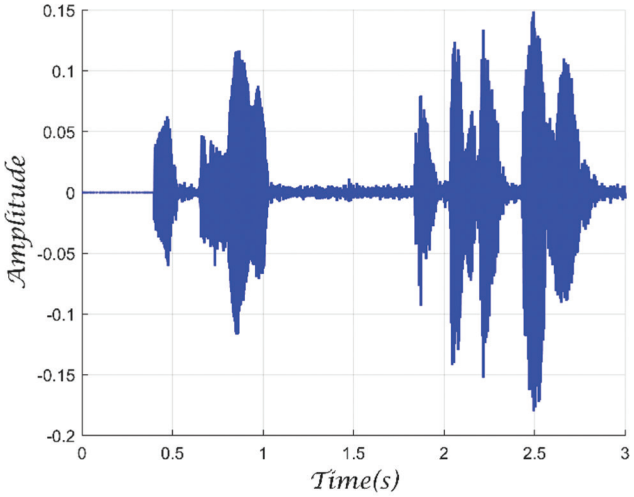


Fig. 7. The decrypted audio.

1, 2,…,length (*x*) under Laplace transform of *vt* cosh *t* can be converted to cipher vector *c* where the components of this vector are given by

$$c_i = q_i - Nk_i, \text{for } i = 0,1,2,\ldots,\text{lenght}\left(\boldsymbol{x}\right) \tag{8}$$

and

$$q_i = \left(2i+1\right)v_i, \text{for } i = 0,1,2,\ldots,\text{lenght}(\boldsymbol{x}) \tag{9}$$

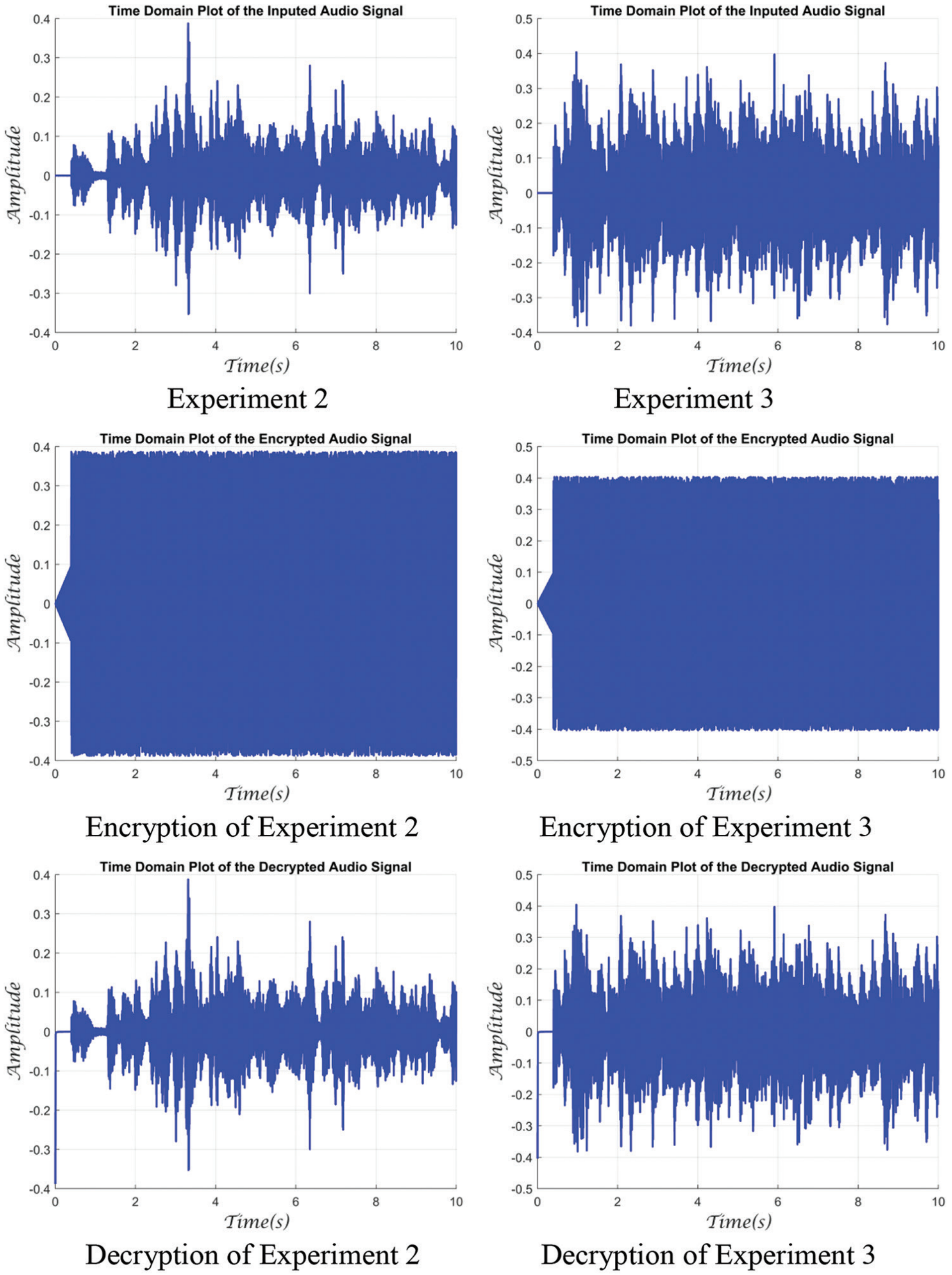
with key

$$k_i = \frac{q_i - c_i}{N}, \text{for } i = 0,1,2,\ldots,\text{lenght } (\boldsymbol{x}) \tag{10}$$

E. Decryption

We assume that the received cipher amplitude of the audio is shown in Fig. 4 as a vector *c*. The given key k_i for i = 0,1,2,…, as defined in equation (10). Let

$$q_i = Nk_i + c_i, \text{for } i = 0,1,2,\ldots,\text{lenght}\left(\boldsymbol{x}\right) \tag{11}$$



Experiment 2

Experiment 3

Encryption of Experiment 2

Encryption of Experiment 3

Decryption of Experiment 2

Decryption of Experiment 3

Fig. 8. The results of simulations for the proposed scheme were applied to other audio samples.

We will take the inverse Laplace transform for $\sum_{i=0}^{\infty}\frac{q_i}{s^{2i+2}}$, we obtain:

$$\boldsymbol{v}t\cosh t = \sum_{i=0}^{\infty}\frac{v_i t^{2i+1}}{2i!} \qquad (12)$$

The decrypted positive integer values of the vector *v* are shown in the Fig. 6.

Hence, after calculating the amplitude of the sound vector $\boldsymbol{s} = \frac{\boldsymbol{v} - M}{10^m}$, we have the decrypted audio, as shown in Fig. 7.

We can do other experiments on the other audios for more understanding and see how this technique works on them (Fig. 8).

TABLE I
Comparison of the Error Rates of Three Audio Encoding Techniques

Method	Cipher Key (*N, m*)	Error rate
LOG Method	(*a, b*) = (0.0003, 300000)	0.00017
RSA Method	(*e, n*) = (5,35)	0.973701
Our proposed Method	(*N, m*) = (3288×$10^{11,15}$)	1.1348×10–^{14}

The first goal, lossless, was accomplished by this approach since there was no data loss throughout the encryption and decryption operations when we took very large value of *m*, as seen from the aforementioned experiment results. The original audio stream and the decoded version are identical.

IV. Error Rate

By comparing the audio signals that have been decrypted to the original input signals, we may have obtained the error rate. For instance, in Figs. 1 and 7, the MATLAB Simulink system for measuring error rates is approaches to 10^{-15}. The error rates of the RSA method and the LOG method proposed by Khalil (2016) are 0.00017 and 0.973701, respectively. These values indicate that our technique performs significantly better, as demonstrated in Table I. The proposed method outperforms the RSA and LOG methods in terms of error rate, as shown in table. Since the encryption algorithms use encoding techniques, it is obvious that some signals may have been lost during the recovery steps in (Khalil, 2016).

V. Conclusion

The security of real-time audio applications makes sure in the current study through a framework for encryption. The design framework protects the confidentiality of military voice communications by encrypting audio applications. The private key in the proposed work is the sum of multiples of the mod, and it suggests a novel cryptographic technique for the encryption of digital audio through the combination of infinity series of particular hyperbolic functions and employing Laplace transforms for encryption and corresponding inverse Laplace transforms for decryption. Due to this, it is highly challenging for an eyedropper to find the secret key using either a brute-force attack or any other assault. The performance and documented outcomes of the procedure clearly indicate that our method was successful in achieving its primary aim of sound data encryption.

Acknowledgment

The authors thank Koya University for their financial assistance.

References

Adriansyah, Y., 2010. *Simple Audio Cryptography*. Institute Teknologi Bandung Indonesia, Indonesia.

Al-Kateeb, Z.N., and Mohammed, S.J., 2020. A novel approach for audio file encryption using hand geometry. *Multimedia Tools and Applications*, 79(27-28), pp.19615-19628.

Al-Khazraji, L.R., Abbas, A.R., and Jamil, A.S., 2022. Employing neural style transfer for generating deep dream images. *Aro-The Scientific Journal of Koya University*, 10(2), pp.134-141.

Delfs, H., Knebl, H., and Knebl, H., 2002. *Introduction to Cryptography*. Vol. 2. Springer, Heidelberg.

Dutta, H., Das, R.K., Nandi, S., and Prasanna, S.M., 2020. An overview of digital audio steganography. *IETE Technical Review*, 37(6), pp.632-650.

El-Zoghdy, S.F., El-sayed, H.S., and Faragallah, O.S., 2020. Transmission of chaotic-based encrypted audio through OFDM. *Wireless Personal Communications*, 113, pp.241-261.

Gencoglu, M., 2019. Embedded image coding using laplace transform for Turkish letters. *Multimedia Tools and Applications*, 78(13), pp.17521-17534.

Ghadi, M., Laouamer, L., and Moulahi, T., 2016. Securing data exchange in wireless multimedia sensor networks: Perspectives and challenges. *Multimedia Tools and Applications*, 75, p.3425-3451.

Ghasemzadeh, A., and Esmaeili, E., 2017. A novel method in audio message encryption based on a mixture of chaos function. *International Journal of Speech Technology*, 20, pp.829-837.

Hayat, U., and Azam, N.A., 2019. A novel image encryption scheme based on an elliptic curve. *Signal Processing*, 155, pp.391-402.

Hayat, U., Azam, N.A., and Asif, M., 2018. A method of generating 8×8 substitution boxes based on elliptic curves. *Wireless Personal Communications,* 101, p.439-451.

Hiwarekar, A., 2013. A new method of cryptography using Laplace transform of hyperbolic functions. *International Journal of Mathematical Archive*, 4(2), pp.208-213.

Kaur, A., and Dutta, M.K., 2018. An optimized high payload audio watermarking algorithm based on LU-factorization. *Multimedia Systems*, 24, pp.341-353.

Khalid, I., Shah, T., Almarhabi, K.A., Shah, D., Asif, M., and Ashraf, M.U., 2022. The SPN network for digital audio data based on elliptic curve over a finite field. *IEEE Access*, 10, pp.127939-127955.

Khalil, M., 2016. Real-time encryption/decryption of audio signal. *International Journal of Computer Network and Information Security*, 8(2), pp.25-31.

Kordov, K., 2019. A novel audio encryption algorithm with permutation-substitution architecture. *Electronics,* 8(5), p.530.

Lakshmi, G.N., Kumar, B.R., and Sekhar, A.C., 2011. A cryptographic scheme of laplace transforms. *International Journal of Mathematical Archive*, 2(12), pp.2515-2519.

Lakshmi, G.N., Kumar, B.R., Suneetha, C., and Chandra, A., 2011. A cryptographic scheme of finite fields using logical operators. *International Journal of Computer Applications,* 975, p.8887.

Lima, J.B., and da Silva Neto, E.F., 2016. Audio encryption based on the cosine number transform. *Multimedia Tools and Applications,* 75, pp.8403-8418.

Liu, Z., Huang, J., Sun, X., and Qi, C., 2017. A security watermark scheme used for digital speech forensics. *Multimedia Tools and Applications*, 76, pp.9297-9317.

Mel, H., and Baker, D., 2001. *Cryptography Decrypted.* Addison-Wesley, Reading, MA.

Miller, V., 1985, Use of Elliptic Curves in Cryptography. In: *Conference on the Theory and Application of Cryptographic Techniques.* Springer, Berlin, Heidelberg, pp.417-426.

Nichols, R., 1996. *Classical Cryptography Course*. Vol. 2. Aegean Park Press, California.

Ramana, B., 2017. *Higher Engineering Mathematics*. Tata McGraw-Hill Education, United States.

Shah, D., Shah, T., and Jamal, S.S., 2020. Digital audio signals encryption by Mobius transformation and Henon map. *Multimedia Systems*, 26, pp.235-245.

Shannon, C., 1998. Communication theory of secrecy systems. 1945. *MD Computing: Computers in Medical Practice*, 15(1), pp.57-64.

Singh, R., Chauhan, R., Gunjan, V.K., and Singh, P., 2014. Implementation of elliptic curve cryptography for audio-based application. *International Journal of Engineering Research and Technology* (*IJERT*), 3(1), pp.2210-2214.