An Enhanced Audio Encryption Method using Unicode and Dynamic Message Mapping in Elliptic Curve Cryptography

SREEKALA M[1]
VARGHESE PAUL[2]
RATHEESH T K[3]
SONIA SUNNY [4]

[1] Department of Computer Applications,
Cochin University of Science
Technology, Kochi
[1] Department of Computer Science
Vimala College (Autonomous), Thrissur
[2,3] Division of Information Technology,
School of Engineering, Cochin University of Science
Technology
[4] Department of Computer Science,
Prajyoti Niketan College, Pudukkad
[1]sreekalam@vimalacollege.edu.in
[2]vp.itcusat@gmail.com
[3]ratheeshtk@gecidukki.ac.in
[4]soniasunny@prajyotiniketan.edu.in

Abstract. This paper presents a novel paradigm for audio cryptosystems that uses elliptic curve encryption to secure audio data. It has the goal of increasing the level of security in digital audio transmission. The suggested method works by mapping an audio message into an Elliptic Curve, then encrypting and decrypting it. This work's uniqueness stems from the use of ECC for encryption, which is the first of its type in audio streaming. The choice of an acceptable mapping method was difficult; hence the dynamic mapping method was used. ECC was chosen for encryption because it is a discrete logarithm problem that is not susceptible to attack by quantum computers. Different audio samples representing bird sound, lion sound, and music sound were used to assess the performance of the recommended cryptosystem. The proposed model's usefulness for quick audio encryption and computational simplicity has been demonstrated. Various statistical analyses have been performed on the suggested model, and the results show that audio signals are better protected from various security risks.

Keywords: Audio Encryption; Elliptic Curve Cryptography; Dynamic Message Mapping

(Received November 12th, 2022 / Accepted June 1th, 2023)

1 INTRODUCTION

Hundreds and thousands of smart gadgets, ranging from smartphones and tablets to industrial equipment and smart-home appliances, now require various forms of connectivity. The IoT era's inexorable quest for greater connectivity has raised expectations that even the most basic smart gadgets will be able to interpret real-time audio. Data-over-sound is one connectivity solution that's quickly gaining traction among engineers and developers aiming to build seamless interactions between

an ever-increasing number of linked devices. Nowadays, digital audio transmission [2, 1] is ubiquitous, and there is growing concern regarding the privacy of inter-party communication. Real-time audio [17, 7, 15] and video conferencing, aircraft traffic monitoring and control, broadcast monitoring [6, 16], and voice triggered instructions for machine management and operations have all made extensive use of multimedia data. Many programmes on the market now promise to offer secure audio communication without disclosing the underlying technology, making end users distrustful of the level of security. End users must be able to determine the level of confidentiality of their communication in order to feel secure. In order to secure the transmission of voice messages, we describe a novel method of encryption/decryption utilising elliptic curves [14]. This paper analyses various audio encryption methods and proposes a new method for encrypting audio data using dynamic mapping and Elliptic Curve Cryptography. For attaining the goal of audio encryption, elliptic curve cryptography is more than adequate. The efficiency of elliptic curve cryptography is stated as follows when compared to the RSA method. The elliptic curve discrete logarithm problem (ECDLP) is used to ensure the security of elliptical curves, allowing ECC to achieve the same level of security as RSA while using fewer keys and more efficient computing. This fact is sufficient to construct an elliptic curve-based

2 RELATED WORKS

2.1 ELLIPTIC CRYPTOGRAPHY

Elliptic Curve Cryptography is a public-key cryptography technique that is based on elliptic curves over finite fields. In 1985, Neal Koblitz and Victor Miller proposed the concept on their own. The Elliptic Curve Discrete Logarithm issue is a well-known NP-Hard problem, and the ECC is based on it [10]. The equation of elliptic curve is given as,

$$y^2 = x^3 + ax + b \tag{1}$$

Elliptic Curve Cryptography comprises three major operations: Key Generation process, Encryption process and Decryption process. The operations are explained in Figure 1.

2.2 MESSAGE MAPPING IN ELLIPTIC CURVE CRYPTOGRAPHY

The process of generating points on Elliptic Curve from plain text is known as message mapping [18]. There are two types of message mapping static mapping and dynamic mapping.

1.png

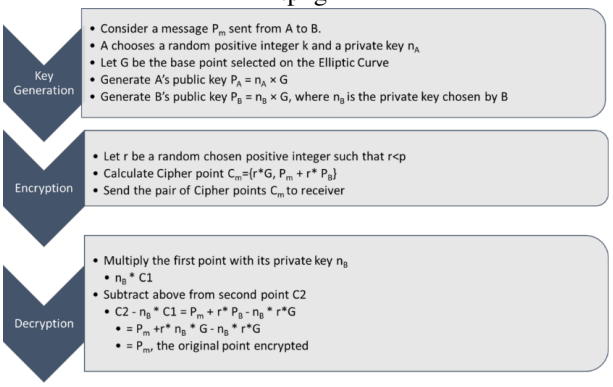


Figure 1: An Overview of Elliptic Curve Cryptography

a) Static (one-to-one) Mapping Method Given value of x, there will be two values for y which is used to map any character. Once mapping is done, the points are encoded by Elliptic Curve Encryption and sends through the communication channel. On the receiver side, original message is retrieved by Elliptic Curve decryption technique. The advantage is that the method is very simple but, it has a major disadvantage. Same characters will be mapped to same points causing the problem of overlapping.

b) Dynamic (One-to-N) Mapping Methods In dynamic mapping method, characters are dynamically mapped on to the points of the Elliptic curve. This method increases the strength of ECC. It is very hard to identify which character is mapped to which point. In this paper we are focusing on dynamic message mapping.

2.3 AUDIO ENCRYPTION METHODS

There are various methods used for encrypting audio signals using different encryption approaches. Each method has application in diverse areas and has its own advantages and disadvantages. Some of the related works in audio encryption are described here.

Ganesh Babu and Ilango, 2013 [8]: Audio encryption keys are made of of variables. A higher dimension cat map is used to create a lookup table. The architecture of Cipher Block Chaining is used. When greater dimension, greater confusion is there and provides more security. But, more memory is required and complexity is also high

Arnold, 2000 [4]: A statistical procedure in the Fourier domain is used in this strategy. A 1-bit watermark is embedded in every 1.2-second time slice and reads the

watermark without requiring the original audio stream or any additional data. This method provides security and is resistant to standard signal processing. There is no protection against eavesdropping and tattooing is more difficult.

Asok et al., 2013 [5]: The iris feature yields the secret key, which is utilised to encrypt and decrypt audio communications using AES. This method provides authentication and the problem is in authentication if pattern is distorted.

Wang et al., 2010 [23]: This approach employs a selective encryption scheme based on the modified discrete cosine transform (MDCT) with resource allocation. The MDCT audio index is utilised to identify the audio importance, and the audio data is subjected to energy-efficient selective encryption. This method saves energy, provides better encryption and good audio transmission quality. This can only be used in Wireless Multimedia Sensor Networks.

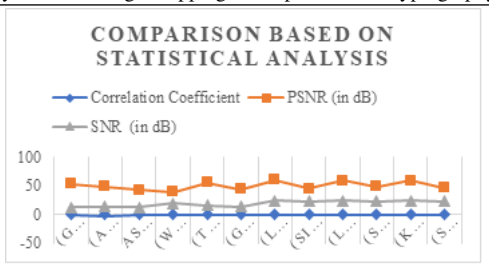
Tamimi & Abdalla, 2014 [22]: This approach employs a stream cypher shuffle as an encryption mechanism. The audio file and key are used as input, and then byte shuffling is performed. The encryption of an audio file is dependent on both the data and the key. In this method, a brute force assault is impossible and high level of resistance against statistical attacks. But, not ideal for low-quality audio files since statistical attacks will occur.

Gupta & Sharma, 2013 [9]: Voice data is protected in this process by a multilayer security system that employs a variety of advanced and difficult encryption methods. This method provides high levels of security and maintains the clarity and quality of your voice. It is impossible to collect data to decrypt if any of the encryption techniques is broken.

Luma & Ameti, 2014 [12]: This approach enables the encryption of audio messages (.wav), their transmission over the network, and their decryption using elliptic curve cryptography. This method is adapted to offer parties with secure audio communication. But it is not the best option for securing real-time mobile communication.

Singh et al., 2014 [21]: In this method, first convert the audio stream into an affine point on the Elliptic Curve (EC) over the finite field GF (p). This method provides higher speeds, lower power consumption, bandwidth savings and storage efficiency. When a static method is used, the same place is mapped every time the same signal is utilised.

Luma et al., 2014 [13]: The voice message bytes are saved in an array. The array is then split into two arrays, with the first array including the first 44 bytes representing the header bytes and the second array containing the remaining bytes representing the voice data. The array's bytes will be mapped to the elliptic curve's corresponding points, which will be placed in the other two arrays. A smaller length key result in stronger encryption. There is overhead of using arrays and memory requirement is high.



2.png

Figure 2: Comparison of various papers based on Statistical Analysis

Shelke & Nemade, 2018 [20]: Single-dimensional audio signals were turned into two-dimensional signals. Experimental simulations were run to assess the encryption algorithm's performance using various settings and under general signal processing threats.

Kordov, 2019 [11]: The strategy for a new pseudo-random generator is described, and it is employed as the foundation for chaotic bit-level permutations and replacements applied to the structure of audio files in order to achieve successful encryption. This method is susceptible to detailed cryptography analysis. The header bits of audio files are not updated because they contain information on the file size, number of samples, and bits per sample.

Shah et al., 2021 [19]: A revolutionary block cypher building process has been used, which covers prominent arithmetic operations such as binary Galois field inversion and multiplication. The proposed technique constructs numerous substitution boxes (S-boxes). The use of several S-boxes creates effective confusion in the data and increases the security of the ciphered audio.

2.4 PERFORMANCE ANALYSIS OF AUDIO ENCRYPTION METHODS

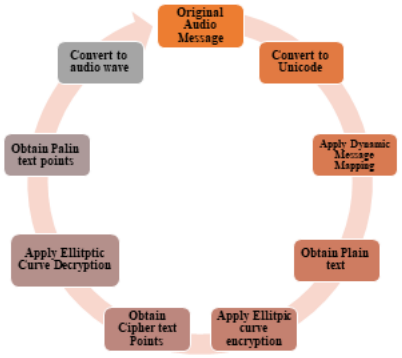
The statistical analysis of each method is done. Also, PSNR and SNR values are calculated. The following table describes the comparison of various methods based on the statistical analysis.

3 PROPOSED METHOD

To encode the audio message to elliptic curve, first the wave form is converted into digital data using Unicode

Table 1: Statistical Analysis of Various Methods

Reference	Correlation Coeffi-cient	PSNR (in dB)	SNR (in dB)
(Ganesh Babu and Ilango, 2013)	Close to zero	53.4	12
(Arnold, 2000)	-0.1317	48.64	13.44
(Asok et al., 2013)	-0.00357	43.38	12.57
(Wang et al., 2010)	4.616E-05	39.7	18.97
(Tamimi & Abdalla, 2014)	-0.002949	55.5	15.65
(Gupta & Sharma, 2013)	0.000064	43.8	13.33
(Luma & Ameti, 2014)	-0.028267	59.8	24.55
(Singh et al., 2014)	0.0032	45.4	23.44
(Luma et al., 2014)	0.0.0007	58.87	24.34
(Shelke & Nemade, 2018)	0.0383	48.99	23.12
(Kordov, 2019)	0.05493	59.23	24.67
(Shah et al., 2021)	-0.028245	46.77	23.32



3.png

Figure 3: Proposed method

and matrix mapping method. To encode message characters to an elliptic curve, the suggested approach uses Unicode with Matrix mapping. The goal of this method is to add another layer of security to the elliptic curve. ASCII has the limitation of 256 characters which is resolved by Unicode. The characters in the message are first converted in to Unicode characters and Matrix mapping is then used to encode the data to the curve. Then apply Elliptic Curve encryption and decryption to obtain the plain text and cipher text points respectively. The received cipher text signal is again converted back to audio wave signal.

3.1 Proposed Algorithm

This method first converts audio signal to plain text and maps onto elliptic curve dynamically. The following algorithm explains the proposed method in detail.

Input: An audio file

Output: Decrypted audio file

Step 1: Let 'M' be an audio input file

Step 2: Generate plain text 'P' from audio file by converting audio file to digital data using Unicode.

Step 3: Let 'p' be each value of plaintext 'P', and represent it as coordinates (X_p, Y_p) on the elliptic curve using matrix mapping method [3].

Step 4: Let 'K' be the random positive integer, then $X_m = p * K + j$, where $j = 0, 1, 2, \ldots$ and $Y_m = \sqrt{(x^3 + ax + b)}$

Step 5: Let 'G' be a point on the curve and $E_p(a, b)$ be an elliptic group

Step 6: Sender 'A' chooses a secret integer 's', compute $Q = s.G$

Step 7: Receiver 'B' consists of public key $E_p(a, b)$, and the points G and Q, s is kept private

Step 8: Let P_m be the plaintext message from A to B

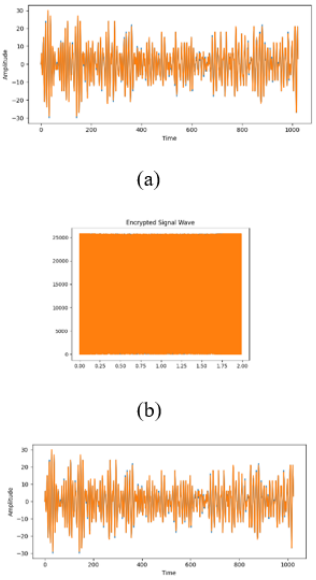
Step 9: A selects a random positive integer k and produce the ciphertext $C_m = kG, P_m + kQ$

Step 10: Perform decryption using the method $\{P_m + kQ - s.(kG) = P_m + k(s.G) - s.(kG)\} = P_m$

Step 11: Generate the deciphered audio file

3.2 Implementation of the Proposed Method and Results

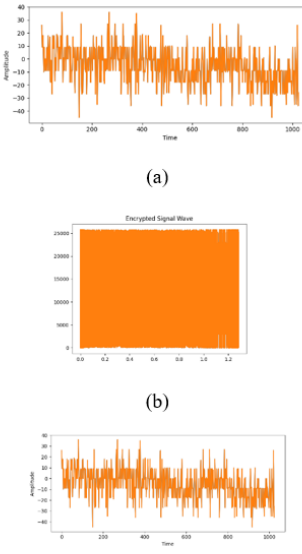
The proposed method is implemented in Python. Three audio wave files are chosen (Bird sound, Lion Sound, Music sound). Each wave form is plotted on Elliptic curve using Unicode and Matrix Mapping technique. Results of the implementation are summarized. The chosen curve is highly suited to encrypting all three types of audios including bird sound, lion sound, and music sound.



(a) (b) (c)

4 hz.png

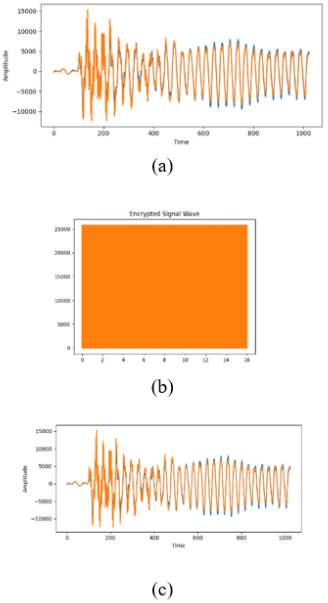
Figure 4: (a) Bird sound, (b) encrypted bird sound, (c) decrypted bird sound



(a) (b) (c)

5 Hz.png

Figure 5: (a) Lion sound, (b) encrypted lion sound, (c) decrypted lion sound



(a) (b) (c)

6 Hz.png

Figure 6: (a) Music sound, (b) encrypted music sound, (c) decrypted music sound

4 PERFORMANCE ANALYSIS OF PROPOSED METHOD

Different types of analysis like correlation analysis SNR and PSNR analysis are performed on the proposed method. The correlation coefficients are used to examine the statistical features of the original signal and encrypted signal. In science and engineering, the signal-to-noise ratio (SNR or S/N) compares the level of a desired signal to the amount of background noise. The signal-to-noise ratio (SNR) is frequently given in decibels and is defined as the ratio of signal power to noise power. The ratio of the mean square difference between two sounds to the greatest mean square differences between two audio files is known as PSNR. Correlation, SNR and PSNR analysis shows that the proposed method is better than all existing methods discussed in this paper. From the tables it is clear that,

Table 2: Correlation Analysis

Audio file	Correlation coefficient of original audio	Correlation coefficient of ciphered audio
Bird audio	0.997	0.0133
Lion audio	0.9876	-0.0040
Music audio	0.95497	-0.001

Table 3: SNR and PSNR Analysis

Audio file	SNR	PSNR
Bird audio	26.3	61.3
Lion audio	25.5	65.7
Music audio	29.3	60.8

PSNR levels are typically between 60 and 80 dB. For networks that use voice applications, an SNR of 25 dB or higher is suggested. While using the proposed method it is also ensured that SNR level is always near 25 dB.

5 CONCLUSION & FUTURE WORKS

The audio signal's secrecy, integrity, accessibility, and confidentiality are all ensured by audio security. This work, according to the application of ECC, is one of a kind because it is suitable for digital encryption. The proposed model uses less calculation time to enable faster encryption. Despite its mathematical complexity, this paradigm is simple to execute and provides a greater degree of flexibility. Various statistical analyses have been carried out, with the results confirming the better level of security and ensuring that it is not prone to statistical attacks, making it more prudent for audio processing. Only wav files are used as sample data. Audio with duration less than 5 seconds are considered. It can be extended to audios with long duration by applying effective compression techniques. The work can be extended by using different types of audio files.

ACKNOWLEDGEMENT

This research did not receive any specific grant from funding agencies in the public, commercial, or not-for-profit sectors.

References

[1] Affonso, E. T., Nunes, R. D., Rosa, R. L., Pivaro, G. F., and Rodriguez, D. Z. Speech quality assessment in wireless voip communication using deep belief network. *IEEE Access*, 6:77022–77032, 2018.

[2] Affonso, E. T., Rosa, R. L., and Rodriguez, D. Z. Speech quality assessment over lossy transmission channels using deep belief networks. *IEEE Signal Processing Letters*, 25(1):70–74, 2017.

[3] Amounas, F. and El Kinani, E. Fast mapping method based on matrix approach for elliptic curve cryptography. *International Journal of Information & Network Security (IJINS)*, 1(2):54–59, 2012.

[4] Arnold, M. Audio watermarking: Features, applications and algorithms. In *2000 IEEE International conference on multimedia and expo. ICME2000. Proceedings. Latest advances in the fast changing world of multimedia (cat. no. 00TH8532)*, volume 2, pages 1013–1016. IEEE, 2000.

[5] Asok, S. B., Karthigaikumar, P., Sandhya, R., Jarold, K. N., and Mangai, N. S. A secure cryptographic scheme for audio signals. In *2013 International Conference on Communication and Signal Processing*, pages 748–752. IEEE, 2013.

[6] Dantas Nunes, R., Lopes Rosa, R., and Zegarra Rodríguez, D. Performance improvement of a non-intrusive voice quality metric in lossy networks. *IET Communications*, 13(20):3401–3408, 2019.

[7] de Almeida, F. L., Rosa, R. L., and Rodriguez, D. Z. Voice quality assessment in communication services using deep learning. In *2018 15th International Symposium on Wireless Communication Systems (ISWCS)*, pages 1–6. IEEE, 2018.

[8] Ganesh Babu, S. and IIango, P. Higher dimensional chaos for audio encryption. In *Proceedings of the 2013 IEEE Symposium on Computational Intelligence in Cyber Security, CICS 2013-2013 IEEE Symposium Series on Computational Intelligence, SSCI 2013*, pages 52–58, 2013.

[9] Gupta, H. and Sharma, V. K. Role of multiple encryption in secure voice communication. *IJCSEE*, 1, 2013.

[10] Kapoor, V., Abraham, V. S., and Singh, R. Elliptic curve cryptography. *Ubiquity*, pages 1–8, 2008.

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

[12] Luma, A. and Ameti, L. Ecc secured voice transmitter. In *Proceedings of the World Congress on Engineering*, volume 1, 2014.

[13] Luma, A., Selimi, B., and Ameti, L. Original research paper. *International Journal of Applied Mathematics, Electronics and Computers*, 2(4):54–58.

[14] Luma, A., Selimi, B., and Ameti, L. Using elliptic curve encryption and decryption for securing audio messages. In *Transactions on Engineering Technologies: World Congress on Engineering 2014*, pages 599–613. Springer, 2015.

[15] Rodriguez, D. Z. and Bressan, G. Video quality assessments on digital tv and video streaming services using objective metrics. *IEEE Latin America Transactions*, 10(1):1184–1189, 2012.

[16] Rodriguez, D. Z. and Junior, L. C. B. Determining a non-intrusive voice quality model using machine learning and signal analysis in time. *INFOCOMP Journal of Computer Science*, 18(2), 2019.

[17] Rodríguez, D. Z., Rosa, R. L., Almeida, F. L., Mittag, G., and Möller, S. Speech quality assessment in wireless communications with mimo systems using a parametric model. *IEEE Access*, 7:35719–35730, 2019.

[18] Sengupta, A. and Ray, U. K. Message mapping and reverse mapping in elliptic curve cryptosystem. *Security and Communication Networks*, 9(18):5363–5375, 2016.

[19] Shah, D., Shah, T., Hazzazi, M. M., Haider, M. I., Aljaedi, A., and Hussain, I. An efficient audio encryption scheme based on finite fields. *IEEE Access*, 9:144385–144394, 2021.

[20] Shelke, R. and Nemade, M. Audio encryption algorithm using modified elliptical curve cryptography and arnold transform for audio watermarking. In *2018 3rd International Conference for Convergence in Technology (I2CT)*, pages 1–4. IEEE, 2018.

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

[22] Tamimi, A. A. and Abdalla, A. M. An audio shuffle-encryption algorithm. In *The world congress on engineering and computer science*, 2014.

[23] Wang, H., Hempel, M., Peng, D., Wang, W., Sharif, H., and Chen, H.-H. Index-based selective audio encryption for wireless multimedia sensor networks. *IEEE Transactions on Multimedia*, 12(3):215–223, 2010.