The SPN Network for Digital Audio Data Based on Elliptic Curve Over a Finite Field

IJAZ KHALID, TARIQ SHAH, KHALID ALI ALMARHABI, DAWOOD SHAH, MUHAMMAD ASIF, AND M. USMAN ASHRAF

1Department of Mathematics, Quaid-I-Azam University Islamabad, Islamabad 45320, Pakistan
2Department of Computer Science, College of Computing in Al-Qunfudah, Umm Al-Qura University, Makkah 24381, Saudi Arabia
3Department of Mathematics, University of Management and Technology, Sialkot Campus, Sialkot 51310, Pakistan
4Department of Computer Science, Government College Women University, Sialkot 51310, Pakistan

Corresponding author: Muhammad Asif (muhammad.asif@math.qau.edu.pk)

This work was supported by the Deanship of Scientific Research at Umm Al-Qura University under Grant 22UQU4310108DSR04.

ABSTRACT The mathematical operation of the Elliptic Curve over the prime finite field is wildly used for secure data communication as it provides high security while utilizing the same size as the secret key. This manuscript presents a novel approach to the SPN (Substitution Permutation Network), for a new digital audio encryption scheme based on Mordell elliptic curve (MEC) over a finite prime field. The proposed scheme consists of a confusion and diffusion module. For the confusion module, the scheme initially generates $5 \times 5$ bijective S-boxes, which have never been applied in the present literature with good cryptographic properties. The generated S-box is then used parallel in the substitution module, which provides optimum confusion in the cipher data. For the diffusion property, the scheme generates pseudo-random number sequences used for block permutation and achieves the property of diffusion. The scheme has been thoroughly securitized against various attacks. The result shows the efficiency of the proposed algorithm over the existing schemes. In addition, the framework that is used to generate MEC points is based on the searching technique. Consequently, it significantly reduces the computational cost and enhances the scheme’s performance compared to the schemes presented in the literature.

INDEX TERMS Elliptic curve cryptography, Mordell elliptic curve, digital audio encryption, s-box.

I. INTRODUCTION

Nowadays, voice-based transmission has become conspicuous in respective areas like military intelligence, phone banking, secret voice conferencing, education, etc. With the increasing demand for secure audio communication, the audio encryption protocol is highly important for the storage and communication of sensitive data over the exposed scheme. The conventional cryptographic algorithm is highly poorly situated for audio encryption, such as traditional algorithms like AES [2], DES [4], TDEA [1], and RSA [3] is not suitable for audio communication. With the assured development of security level, the chaotic theory competes for a significant role in such an encryption algorithm. The two underlying cryptographic terms, diffusion and confusion, are introduced by Claude Shannon [5]. These two terms are substitution and permutation operations. In diffusion operation, the data values are substituted by some random number or sequences of numbers. In confusion, the data value is permuted corresponding to some key parameter to dismantle the neighboring samples. But both terms are shown complex relation between ciphertext, plaintext, and the encryption of symmetric key algorithms; different analysts and designers use the substitution-permutation network (SPN) as a fundamental structural element [6]. Chaos theory also plays an essential role in such encryption algorithms because its inherited properties such as sensitivity to the initial condition, dynamical system, integrable system, topological transitivity, predictability, and deterministic randomness properties fulfill the essential, necessary items for theoretical cryptography. Predominantly chaotic algorithms such as multiple iterations, bit-level scrimmaging techniques,
bit-level confusion approaches, and hybrid key techniques [7], [8], [9], [10], [11], [12] were designed based on the above-recommended properties. Public key cryptography was developed in 1976 by W.Diffie and M.Hellman. We are familiar that every cryptographic algorithm is based on complex mathematical algorithms that appear unattainable to solve. Public key cryptography has widespread use in the communication system, digital signatures, data hiding, data encryption, etc. Elliptic curve cryptography (ECC) [13], [14] proceed toward public-key cryptography based on a different algebraic structure over real, rational, and finite filed. ECC permits smaller keys to provide the same security as compared to a non-elliptic cryptographic algorithm based on the Galois field [15]. In 1970, Fredrich proposed a technique for image encryption based on a chaotic map and developed the concept of chaos-based cryptography. Following that, the researchers discovered that chaotic systems’ distinguishing characteristics, such as their dependence on initial conditions and high sensitivity to the parameter and initial condition, randomness, and ergodicity, make the theory of chaos suitable for the application of multimedia data security Manish et al devised RGB image encryption based on DNA encoding and Diffie Hellman encryption using elliptic curves. The RGB image was encoded into DNA nucleotides, and elliptic curve-based asymmetric cryptosystems were used to encrypt it [39]. Moreover, Zhang [40] proposed an RGB image encryption technique based on DNA encoding and ECC. In this technique, instead of the RGB image’s pixel values, ECC was employed to encrypt the key. In addition, Singh and Singh [16] developed an image encryption scheme using the concept of ECC. In the reported scheme, they grouped the pixel values of the image into big integers to less the number of encryption operations and carried out the encryption procedure with the aid of ECC. In [16], [17], [18], and [19], different researchers recommended various encryption algorithms based on the ECC systems for text and digital images and ensured that the existing scheme achieves high-level security in the field of cryptography.

A. RELATED WORK

In literature, numerous encryption techniques are shown for digital audio, but no single algorithm fascinates all the digital audio formats. In 2008 Wei-Qi Yan et al. presented a scheme of digital audio scrambling in the compressed domain [20]. The presented work uses the scramble digital audio data before key transmission. Nonetheless, the suggesting work has not proven the security against brute force attacks [21]. Juliano B. Lima et al. suggested a digital audio encryption technique based on the cosine number transform (CNT) [22]. The anticipated approach of encryption was applicable to encrypt different blocks of audio format. The rule used to select the audio data blocks is overlapping that produced confusion and diffusion in the encrypted data. Niels J. Thorwirth et al suggest a technique of encryption based on perceptual digital audio coding and lossy compression [23]. To upgrade the encrypted audio stream using the security functions, the presented work the author’s main target on the security analyses of cipher MP3 encoded data. In 2001 Emad Mosa et al. proposed an audio speech signal based on chaotic encryption [24]. The presented scheme used the Bakar map for permutation of speech segments and using masks and both time and transform domains to achieve the substitution. The audio encryption scheme is based on the Fast Walsh Hadamard Transform mix with chaotic keystreams proposed by F.J. Farsana et al [25]. In the suggested work, the encryption algorithm is based on permutation using a discrete Hanon map and generated keystreams using the Lorenz-Hyperchaotic system; in the proposed work, the target of high-level security is achieved. Next, Prabir Kumar Naskar et al. introduced an audio encryption scheme based on DNA Encoding and Channel Shuffling [26]. The suggested work shows that the correlation between original and cipher files is very low without multiple rounds. Afterward, in 2016 Hongjun Liu introduced a scheme of audio encryption by the operation of diffusion and confusion based on multi-scroll chaotic encryption and one-time keys [27]. The proposed work shows that a chaotic system with varying multi-scroll generates key streams to produce diffusion and confusion in audio data. Moreover, Subhajit Adhikari et al. [35] presented a novel audio encryption technique based on the chaotic Henon and Tent map to generate the key and xored the key with the original audio data. Instead of an invitation link, the encrypted audio file may be utilized in the e-learning process to produce an audio password that can be used as login credentials. Besides, Haris Aziz et al [36] developed a noise-tolerance audio encryption scheme by the application of chaotic and symmetric group $S_8$. The proposed design exploits MEC and S8 symmetric groups to facilitate military and real-time audio communication. The suggested approach also includes tree chaotic maps to improve robustness. In 2021, Motilal Singh Khoirom et al [37] also presented an audio encryption algorithm using Ameliorated ElGamal public key encryption(AEPK) Over finite fields. In the suggested work, first, utilize the koblitz embedding technique to convert the message to EC coordinate and then use EPK to ensure that the proposed algorithm is suitable for audio encryption. In the same year, Prabir Kumar Naskar et al [38] also recommended a new approach to audio encryption algorithm using piecewise linear chaotic map (PWLCM) along with elementary cellular automata (ECA). They performed the encryption process with three different phases cycling shifting, shuffling, and ciphering with the aid of PWLCM and, ECA. The theory of ECC is widely used in multimedia data encryption and achieves high-level security in the field of cryptography. Rahul Singh et al. present an audio encryption algorithm based on the mathematical operation of ECC [28]. The proposed work shows that each value of the audio file is transformed to the elliptic curve point and applies the encryption algorithm of ECC to achieve high-security use of small keys as compared to other non-elliptic cryptographic algorithms. Next, Richard
Apau proposed a new approach of audio encryption using ECC [29]. The authors use the Huffman and low-bit encoding algorithms to achieve the reduced file size and the compressed, encrypted audio file embedded in the convenient frame of converted cipher file based on histogram analysis. In the suggested work, the goal of tremendous security has been accomplished. In the same year, Ramesh Shelke et al. introduced a technique of audio encryption using Arnold transform and ECC. Moreover, the recent existing literature based on chaotic and hyperchaotic utilized for the applications of audio encryption and image encryption is present in [16], [31], [32], [33], [34], [35], [36], [37], [38], [39], [40], and [41]. In the above-related literature, the existing schemes based on chaotic maps, due to the less no of parameters of the one-dimensional chaotic map, are proven to not secure against cryptanalysis. Moreover, techniques based on high-dimensional chaotic sequences are extremely complicated, necessitating additional storage space, and most chaotic-based encryption algorithms are subject to a variety of hardware constraints. The absence of mathematical non-integer operations, which require a lot of space, is the cause of this constraint. Therefore, researchers used different mathematical structures for the development of a secure digital audio encryption scheme having infinitesimal computational complexity. For this reason, we study some of the quality research works related to elliptic curve cryptography.

B. OUR CONTRIBUTION

In this manuscript, we have introduced a new approach to digital audio encryption based on the Mordell elliptic curve over a finite field, with the combination of highly nonlinear components (i.e., S-box). The framework of MEC points generation utilized the searching techniques which significantly reduce the time complexity up to the exceptional margin. The high-quality pseudo-random number sequences are subsequently utilized for the aid of the diffusion process. The phase of confusion is utilized with the help of multiple strong 5 × 5 dynamic S-box, which have never been applied before the existing literature. The motivation behind the dynamic S-box instead of the static S-box is that the attacker does not know which S-box is being used, and hence there are many advantages, such as defence against an unknown attack, and the complexity of the s-box constructed can increase the strength of the cipher. The experimental findings show that the suggested technique is effective and resistant to different types of attacks. The rest of this manuscript is organized as follows: Section 2 introduces some basic preliminaries and related results. The proposed encryption methodology is introduced in section 3. The construction 5 × 5 S-box and its security analysis are addressed in section 4. The suggested scheme simulation and performance results are demonstrated in section 5. The final section, Section 6, concludes the discussion.

II. PRELIMINARIES

Generally, some basic preliminaries and related results for this section are Washington and Galbraith [31], [32]. An elliptic curve over a finite field \( F_p \) is defined as:

\[
E^{a,b}_{p} = \{ \infty \} \cup \{(x, y) : y^2 = x^3 + ax + b \mod p \}
\]

where both \( a \) and \( b \) are the parameters of EC, with the discriminant \( 4a^3 + 27b^2 \neq 0 \). Otherwise, the EC is singular. All the points \( E^{a,b}_{p} \), that have a specific sort of addition law form an abelian group with the neutral element \( \infty \), which is called the point of infinity. Additionally, the graphical representations of an elliptic curve with different parameters are illustrated in Figure 1.

A. ELLIPTIC CURVE ARITHMETIC OPERATION

An elliptic curve over a finite field is governed by the following mathematical equation. Let \( P_1 = (x_1, y_1) \) and \( Q_1=(x_2,y_2) \) are the two points of the elliptic curve such that \( P_1 \neq Q_1 \), then the addition of \( P_1 \) and \( Q_1 \) compute using the following mathematical formula.

\[
R = P_1 + Q_1 = (x_3, y_3)
\]

whereas

\[
(x_3 = \xi^2 - x_1 - y_1 \mod p), y_3 = \xi (x_1 - x_3) - y_1 \mod p.
\]

\[
\xi = \frac{y_2 - y_1}{x_2 - x_1} \mod p.
\]

If \( P_1 \) and \( Q_1 \) are the same points (i.e \( P_1 = Q_1 \)) then the point doubling calculation is defined as:

\[
2Q = (x'_3, y'_3).
\]

whereas

\[
x'_3 = \xi^2 - 2x_1 \mod p,
\]

\[
y'_3 = \xi (x_1 - x'_3) - y_1 \mod p
\]

and

\[
\xi = \frac{y_2 - y_1}{x_2 - x_1} \mod p
\]

In addition to scalar point multiplication, multiple point addition is also carried out.

\[
MQ_1 = Q_1 + Q_1 + Q_1, \ldots, M \text{ times}
\]

The cardinality of points on the EC is calculated by following Hass’s inequality theorem.

Theorem 2.1 Let \( E^{a,b}_{p} \) over finite field \( F_p \). Then the cardinality (order) of \( E^{a,b}_{p} \) should be satisfy

\[
p + 1 - 2\sqrt{p} \leq #E^{a,b}_{p} \leq p + 1 + 2\sqrt{p}
\]

The special case of EC when the parameter \( a=0 \) and \( b \neq 0 \) is called the Mordell elliptic curve \( M_{EC}^{0,b} \).
Theorem 2.2 Let $P$ be prime (i.e., $p > 3$) such that $p \equiv 2 \pmod{3}$. Then for each $b \in F_p$, the $M_{EC}^{0,b}$, has exactly $p + 1$ unique points. As the $y$-coordinate of each integer in $[0, p–1]$ appears exactly once.

III. PROPOSED WORK

In this section, we discuss the proposed algorithm for audio data. The proposed algorithm is to work out to secure the digital audio in (.wav formatted) before sending it to the insecure channel. The step-by-step procedure of the proposed work is given as follows.

Step 1:
First, read the audio file in sixteen-bit integer data whose range lay in the interval of $[2^{-15}, 2^{15}]$. Reshape the original audio data in the new matrix $\hat{\Lambda}$ of dimension $N \times N'$, where $N, N'$, represent the number of rows and columns, respectively.

Step 2:
Next, matrix $\hat{\Lambda}$ contains both non-negative and negative data in the class of signed bit integers. To identify the position of both data, the scheme creates a binary matrix $\beta$, consisting of 1 and 0. The mathematical formulation of the binary matrix is given as follows.

$$
\beta(i,j) = \begin{cases} 
0, & \text{if } \hat{\Lambda}_{ij} < 0 \\
1, & \text{if } \hat{\Lambda}_{ij} \geq 0
\end{cases}
$$

(10)

where $\hat{\Lambda}_{ij}$, the data is a set element of matrix $\hat{\Lambda}$ at the $(i,j)_{th}$ position and $\beta(i,j)$ is to show the element of binary matrix $\beta$ at $(i,j)_{th}$ position. Therefore, we get a binary matrix $\beta$ of dimension $N \times N'$.

Step 3:
Next, convert the audio data set $[2^{-15}, 2^{15} – 1]$ to $[2^{-15}, 1, 2^{15} – 1]$ to get new data set matrix $\hat{\Lambda}'$ of dimension $N \times N'$. Consequently, get the new matrix $\hat{\Lambda}'$, which contains the data values of 15-bit-digit integers. The mathematical formula for the new data set is given below.

$$
\hat{\Lambda}'(i,j) = \begin{cases} 
\hat{\Lambda}_{ij}, & \text{if } \hat{\Lambda}_{ij} \geq 2^{-15} \\
\hat{\Lambda}_{ij} - 1, & \text{if } \hat{\Lambda}_{ij} = 2^{-15}
\end{cases}
$$

(11)

Step 4:
In the next step, apply the absolute function to the data set of $\hat{\Lambda}'(i,j)$ to obtain the new data set $\hat{\Lambda}''(i,j)$, whose entries lay in the interval of $[0,2^{15}]$. Hence the $\hat{\Lambda}''(i,j)$ transform to a 15-bit positive integer.

Step 5:
Afterward, generate pseudo-random sequences using the following $M_{EC}^{0,b}$, equation and pick the $y$-coordinates of $E_{Y_1}, E_{Y_2}, E_{Y_3}$.

$$
E_{Y_1} = (M_{EC}^{0,b_{p1}}) \mod N
$$

(12)

$$
E_{Y_2} = (M_{EC}^{0,b_{p2}}) \mod N'
$$

(13)

$$
E_{Y_3} = (M_{EC}^{0,b_{p3}}) \mod N''
$$

(14)

where $M_{EC}^{0,b_{p1}}, M_{EC}^{0,b_{p2}}, M_{EC}^{0,b_{p3}}$, are the MEC sequences with the specified modulus $N, N'$ and $N''$.

Step 6:
In the next step, the proposed algorithm utilizes the generated sequences in previous step 5 and permutes with the matrix $\hat{\Lambda}''$. Consequently, the aim of this diffusion phase is to break the strong-willed correlation among neighbour integers. The mathematical formulation of step 6 is given below in eq. (15)

$$
\hat{\Lambda}''^{-P}(i,j) = \hat{\Lambda}''(E_{Y_1}, E_{Y_2})
$$

(15)

Step 7:
The phase of confusion is a cryptographic approach devised to enhance the vagueness of cipher data. In this step, the proposed algorithm performed the substitution process to establish that the cipher data gives no hint regarding the original data, producing confusion in the cipher data. Since in the proposed work, the permuted data is a 15-bit positive integer so it will be computing hard to substitute the whole block of 15-bit positive data for the sake of this purpose, the algorithm divided the block into three sub-blocks of a 5-bit positive integer using the following mathematical maps defined by:

$$
\zeta : \mathbb{Z}_2^{15} \rightarrow \mathbb{Z}_2^{5}
$$

$$
\zeta(a_1, . . . , a_{14}, a_{15}) \rightarrow \zeta (a_1, a_2, a_3, a_4, a_5, \ldots , 0, 0)
$$

(16)

$$
\zeta : \mathbb{Z}_2^{15} \rightarrow \mathbb{Z}_2^{5}
$$

$$
\zeta(a_1, . . . , a_{15}) \rightarrow \zeta(0, 0, a_6, a_7, a_8, a_9, a_{10}, \ldots , 0, 0)
$$

(17)
Therefore, get 3 -subblocks Å′′′5-bit, respectively.

Step 8:
Generate an S-box of 5 × 5 using an elliptic curve over a finite field. Since the 5 × 5 S-box has never been utilized and evaluated before, therefore in this manuscript, we briefly mentioned the construction procedure and security analysis of 5 × 5 S-boxes in section 4.

Step 9:
Then substitute the 3-subblocks Å′′′P51, Å′′′P52, Å′′′P53, with the 5 × 5 S-boxes, the substitution procedure of the subblocks is the same. Initially converts the subblocks data into binary form. Next, split the chunks of five bits of each block element into 2 and 3 bits-string and then convert a 2-bit string in the decimal range of 0 to 3 (or binary 11 to 00) and 3-bit strings in the decimal range of 0 to 7 (or binary 000 to 111), then substitute each element of the S-boxes with the element of S-box S′′′p. For a better explanation, read example 4.1. The mathematical representation of the substitution process is defined below.

\[
\begin{align*}
\hat{A}^{npS_{51}} & = S_{a,b}(\hat{A}^{npS_{51}}) \\
\hat{A}^{npS_{52}} & = S_{a,b}(\hat{A}^{npS_{52}}) \\
\hat{A}^{npS_{53}} & = S_{a,b}(\hat{A}^{npS_{53}})
\end{align*}
\]

Step 10:
After the phase of substitution, one can get three new subblocks Å′′′P51, Å′′′P52, and Å′′′P53. Finally, using the xor operation and xor, the sequences of \(E^3 \mod 32\) with the three new subblocks obtained in step 8 to get three new encrypted data. The mathematical form of this step is given in this equation, \(C_1 = (E^3 \mod 32 \oplus \hat{A}^{npS_{51}})\).

\[
\begin{align*}
C_2 & = (E^3 \mod 32 \oplus \hat{A}^{npS_{52}}) \\
C_3 & = (E^3 \mod 32 \oplus \hat{A}^{npS_{53}})
\end{align*}
\]

Step 11:
To reverse the data form \(C_1, C_2\) and \(C_3\) of 5-bit each block to a single 15-bit block by using the following mathematical formula

\[
\begin{align*}
\zeta^{-1}: \mathbb{Z}_2^5 \times \mathbb{Z}_2^5 \times \mathbb{Z}_2^5 & \rightarrow \mathbb{Z}_2^{15} \\
\zeta^{-1}((a_1, \ldots, a_5)(a_6, \ldots, a_{10})(a_{11}, \ldots, a_{15})) & \rightarrow (a_1, a_2, a_3, \ldots, a_{14}, a_{15}).
\end{align*}
\]

Finally, we get a matrix \(\hat{A}^{ns}_{15}\) of dimension \(N \times N'.\)

Step 12:
At the final step of the proposed algorithm map, the data set \([012, \ldots, 2^{15} - 1]\) of the matrix \(\hat{A}^{ns}_{15}\) to the data set \([-2^{15} - 1, \ldots, 2^{15} - 1]\), using a binary matrix defined in eq (25). The mathematical representation of the last step is given as follows.

\[
\hat{A}^E(i,j) = \begin{cases} 
-\hat{A}^{ns}_{15}(i,j) & \text{if } \beta(i,j) = 0 \\
\hat{A}^{ns}_{15}(i,j) & \text{if } \beta(i,j) = 1
\end{cases}
\]

Eventually, one can get a matrix \(\hat{A}^E\), then convert to an audio file which is the required cipher audio file. The flow chart of the proposed scheme is illustrated in Figure 2. To evaluate the proposed scheme’s security, we have encrypted multiple audio files of varied sizes and different characters. The analysis of the results is presented in the next section. Moreover, the source codes of encoding and decoding of the proposed audio encryption algorithm are given in Tables 4 and 5, respectively.
TABLE 1. Propose $5 \times 5 E^{1.1}_{211}$ s-box.

|   |  2 |  3 |  4 |  5 |  6 |  7 |  8 |  9 |
|---|----|----|----|----|----|----|----|----|
| 2 | 13 | 22 | 29 |  5 | 15 | 30 | 16 |    |
| 4 | 14 | 24 |  0 |  6 | 21 | 31 | 19 |    |
| 8 | 17 | 25 |  1 | 10 | 23 |  7 | 26 |    |
|12 | 18 | 28 |  3 | 11 | 27 |  9 | 20 |    |

TABLE 2. Proposed $5 \times 5 E^{1.3}_{197}$ s-box.

|   |  3 |  4 |  5 |  6 |  7 |
|---|----|----|----|----|----|
| 3 |  9 | 20 | 28 |  4 | 18 |
| 5 | 10 | 21 | 29 | 12 | 26 |
| 6 | 11 | 24 |  0 | 15 | 30 |
| 7 | 16 | 25 |  2 | 17 | 13 |

TABLE 3. Proposed $5 \times 5 E^{0.1}_{293}$ s-box.

|   |  3 |  4 |  5 |  6 |  7 |
|---|----|----|----|----|----|
| 2 | 24 | 12 | 22 | 11 | 20 |
| 2 | 13 | 25 | 15 | 26 | 17 |
|14 | 18 | 31 | 16 | 30 | 27 |
|23 | 19 |  6 | 21 |  7 | 10 |

IV. CONSTRUCTION OF $5 \times 5$ S-BOX AND THEIR
SECURITY ANALYSIS
Since the $5 \times 5$ S-box has never been applied before, in this section, we briefly discuss the construction procedure and their performance analysis of the $5 \times 5$ S-box. The $5 \times 5$ S-boxes used to substitute three sub-blocks composed of five-bit integers are based on elliptic curves over prime fields $F_p$. There are four main steps in the algorithm, which are described in the following steps.

Step 1: Select two distinct domain parameters, $a$ and $b$, from the prime field $F_p$, where $p$ is a large prime number, i.e., $a, b \in F_p, a \neq b$.

Step 2: Next, our approach to generating EC points using the searching method, which reduces the complexity up to a significant extent. The following Weierstrass cubic elliptic curve utilizes to generate the points.

$$E^{a,b}_p = y^2 = x^3 + ax + b \mod p \quad (26)$$

Step 3: Afterward, pick the $y$-coordinate $E^{a,b,v}_{p}(u,v)$ of all orders paired $E^{a,b}_p (u,v)$ then apply the modulo 32 operation on $E^{a,b,v}_{p}(u,v)$ to get the $E^{a,b,v}_{32}(u,v)$. The aim of modulo 32 is to substitute the three sub-block each of five-bit integer data. The mathematical formulation of this step is given below.

$$\partial: E^{a,b}_p \rightarrow E^{a,b}_{p'}$$

$$\partial: E^{a,b}_{p'} \rightarrow E^{a,b}_{p''}$$

$$\partial (u,v) = v \mod (p') \quad (27)$$

Step 4: In the final step, we choose the first 32 unique elements of $E^{a,b,v}_{32}(u,v)$ to generate an s-box $S^p_{a,b}$, and transmute into a $4 \times 8$ lookup table.

The implementation of the proposed algorithm is demonstrated on several ECs with different parameters for the generation of S-boxes. For example, the s-boxes $S^{32}_{1,1}$, $S^{32}_{1,3}$ and $S^{32}_{0,1}$ are generated by $E^{1,1}_{211}, E^{1,3}_{197}$ and $E^{0,1}_{293}$ respectively shown in Tables 1, 2, and 3. Furthermore, the security analysis of the proposed dynamic s-box generation technique given in Table 6 ensures that the suggested nonlinear layer is resistant against linear and differential attack

Example 4.1

Let the input data $I = (21)_2 = (10101)$ of the S-box, i.e. $S^{32}_{1,3}$, then the outer bits $(11)$ of 1 identify row 3, while the inner bits $(010)$ represent column 2. The numbering of rows and columns start from 0 to 3 and 0 to 7 respectively. If substitute the input data I with the S-box, i.e. $S^{32}_{1,3}$ show in Table 2, then the output data of S-box is $S^{32}_{1,3} (21) = 25$.

V. SECURITY ANALYSIS OF AUDIO ENCRYPTION
An efficient multimedia data encryption scheme should be strong enough to withstand all types of attacks, namely statistical, eavesdropping, brute-force, and other cryptanalytic approaches. Throughout part of this section will examine how the proposed encryption scheme is vulnerable to several types of attacks. A portable PC is used to conduct the simulations using MATLAB 2021(a). To analyze the suggested scheme, we picked the collection of audio samples with various characteristics such as voice, music, etc., and then encrypted them using different elliptic curve key parameters. The waveforms of the plan-audio and encrypted audio files are shown in Figure 3. The amplitude depicted in the waveform of the encrypted audio is uniform and has no resemblance to the amplitude of the plan audio data, proving that the audio
TABLE 4. Pseudocode of encoding of digital audio data.

| Step | Description |
|------|-------------|
| 1.   | \( O \) = Original audio data |
| 2.   | Output = Encrypted audio data (wave) |
| 3.   | \( F \leftarrow \text{Frequency} \) |
| 4.   | \([O, F] \leftarrow \text{read} (O, \text{native})\) |
| 5.   | \([m, n] = \text{sizeof}(O)\) |
| 6.   | Length \((m, n)\) |
| 7.   | Sequence generation |
| 8.   | for \( i = 1 \) to \( L \) do |
| 9.   | \( E_1^Y = M_{EC}(p_{1}, b) \) |
| 10.  | \( E_2^Y = M_{EC}(p_{2}, b) \) |
| 11.  | \( E_3^Y = M_{EC}(p_{3}, b) \) |
| 12.  | End |
| 13.  | Binary matrix generation |
| 14.  | for \( i = 1 \) to \( m \) do |
| 15.  | for \( j = 1 \) to \( n \) do |
| 16.  | \( \beta(i, j) = 1 \) |
| 17.  | if \( \tilde{A}_{i,j} \geq 0 \) |
| 18.  | else |
| 19.  | \( \beta(i, j) = 0 \) |
| 20.  | end |
| 21.  | \( \tilde{A} = \text{Abs} (\tilde{A}) \) |
| 22.  | Data conversion |
| 23.  | for \( i = 1 \) to \( m \) do |
| 24.  | for \( j = 1 \) to \( n \) do |
| 25.  | if \( \tilde{A}_{i,j} > 2^{-15} \) |
| 26.  | \( \tilde{A}(i, j) = \tilde{A}_{i,j} \) |
| 27.  | else |
| 28.  | \( \tilde{A}(i, j) = 2^{-15} \) |
| 29.  | Diffusion phase |
| 30.  | for \( i = 1 \) to \( m \) do |
| 31.  | for \( j = 1 \) to \( n \) do |
| 32.  | \( \tilde{A}^{**}(i, j) = \tilde{A}^{**}(E_1^Y, E_2^Y) \) |
| 33.  | end |

The histogram analysis is a useful tool for assessing the effectiveness of the cryptosystem and examining how the cryptosystem is vulnerable to statistical attacks. A well-organized cryptosystem may provide uniformity in the distribution of data of encrypted audio files, which is unlike the histogram of the plain audio data. As a result, a well-managed cryptosystem should transform the original audio data to equally likely values, ensuring that the encrypted data contains no information that would allow an attacker to decode the data without knowing the cryptographic private key. The analysis of the histogram is illustrated in Figure 5. Figures 4(a-d) and 4(e-h) show the histogram of plain and encrypted audio data, respectively. As can be observed the histogram of plan audio data is randomized and approaches a fixed location, while on the other hand, the histogram of encrypted audio data nearly resembles each other. As a result, the recommended encryption scheme is extremely secure against statistical attacks, and eavesdroppers were incapable of decrypting the encrypted data.

### A. HISTOGRAM ANALYSIS

The histogram analysis is a useful tool for assessing the effectiveness of the cryptosystem and examining how the cryptosystem is vulnerable to statistical attacks. A well-organized cryptosystem may provide uniformity in the distribution of data of encrypted audio files, which is unlike the histogram of the plain audio data. As a result, a well-managed cryptosystem should transform the original audio data to equally likely values, ensuring that the encrypted data contains no information that would allow an attacker to decode the data without knowing the cryptographic private key. The analysis of the histogram is illustrated in Figure 5. Figures 4(a-d) and 4(e-h) show the histogram of plain and encrypted audio data, respectively. As can be observed the histogram of plain audio data is randomized and approaches a fixed location, while on the other hand, the histogram of encrypted audio data nearly resembles each other. As a result, the recommended encryption scheme is extremely secure against statistical attacks, and eavesdroppers were incapable of decrypting the encrypted data.

### B. SPECTROGRAM ANALYSIS

The spectrogram analysis is an accurate and visual representation of audio data, it’s the tool for analyzing the sound data. A spectrogram is a standard two-dimensional plot in which one axis represents the time domain while the other axis visualizes the frequency with the colour of each point indicating its amplitude. As a result, a spectrogram shows amplitude variations for each signal frequency component. To evaluate the recommended encryption scheme, we used spectrogram analysis, and the results are shown in Figure 5. Figure 5(a-d) depicts the spectrogram graph of the plain audio file, while Figure 5(e-h) depicts the spectrogram graph of the encrypted audio file, respectively. From Figure 5, one can determine that the spectrogram analysis of the encrypted audio is flat, has a significant amplitude, and is different from...
TABLE 5. Pseudocode of decoding of digital audio data.

| 1. | Input=Encrypted audio data |
| 2. | Output=original Audio Data |
| 3. | F=Frequency; |
| 4. | [E, F] ←read (E.', native'); |
| 5. | [m, n] =size(E); |
| 6. | L=length(m, n); |
| 7. | $\hat{A}_{15}$= $E$; |
| 8. | % Binary matrix generation |
| 9. | for $i$ = 1: m do |
| 10. | for $j$ = 1: n do |
| 11. | $\beta(i, j)$ = 1 |
| 12. | if $\hat{A}_{15}^{ij}$ ≥ 0 |
| 13. | else |
| 14. | $\beta(i, j)$ = 0 |
| 15. | end |
| 16. | $\hat{A}''$ = Abs ($\hat{A}$) |
| 17. | % Data conversion |
| 18. | for $i$ = 1: m do |
| 19. | for $i$ = 1: n do |
| 20. | if $\hat{A}_{ij}''$ > $2^{-15}$ |
| 21. | $\hat{A}(i, j)$ = $\hat{A}_{ij}''$ |
| 22. | else |
| 23. | $\hat{A}(i, j)$ = $\hat{A}_{ij}''$ - 1 |
| 24. | % Five-bit shifting |
| 25. | $\hat{A}_{15}^{''}$ $\leftarrow$ bitshift(bitshift($\hat{A}''$, -5), 5); |
| 26. | $\hat{A}_{15}^{'''}$ $\leftarrow$ bitshift(bitshift($\hat{A}''$, -5), 5); |
| 27. | $\hat{A}''$ $\leftarrow$ bitshift($\hat{A}''$, -5), 5); |
| 28. | % Generation of inverse S-box |
| 29. | $S_{13}^{2}$ $\leftarrow$ inv($E_{1}^{1.2}$, 121); |
| 30. | $S_{13}^{2}$ $\leftarrow$ inv($E_{1}^{1.3}$, 197); |
| 31. | $S_{13}^{2}$ $\leftarrow$ inv($E_{01}^{1.293}$) |
| 32. | % Re-substitutions phase |
| 33. | $\hat{A}_{15}^{'''}$ $\leftarrow$ $S_{13}^{2}$$\hat{A}_{15}^{'''}$ |
| 34. | $\hat{A}_{15}^{'''}$ $\leftarrow$ $S_{13}^{2}$$\hat{A}_{15}^{'''}$ |
| 35. | $\hat{A}_{15}^{'''}$ $\leftarrow$ $S_{13}^{2}$$\hat{A}_{15}^{'''}$ |
| 36. | % Inverse Sequence generation |
| 37. | for $i$ = 1: L do |
| 38. | $E_{1}^{i}$ $\leftarrow$ inv($M_{EC}^{0.0}$, $p_{1}$) |
| 39. | $E_{2}^{i}$ $\leftarrow$ inv($M_{EC}^{0.0}$, $p_{2}$) |
| 40. | $E_{3}^{i}$ $\leftarrow$ inv($M_{EC}^{0.0}$, $p_{3}$) |
| 41. | end |
| 42. | % Bit-xor operation |
| 43. | $C_{1}$ $\leftarrow$ ($E_{3}^{i}$ mod 32) $\oplus$$\hat{A}_{15}^{'''}$ |
| 44. | $C_{2}$ $\leftarrow$ ($E_{3}^{i}$ mod 32) $\oplus$$\hat{A}_{15}^{'''}$ |
| 45. | $C_{3}$ $\leftarrow$ ($E_{3}^{i}$ mod 32) $\oplus$$\hat{A}_{15}^{'''}$ |
| 46. | $\hat{A}_{15}^{'''}$ $(i,j)$ $\leftarrow$ $C_{1}$ $\oplus$ $C_{1}$ $\oplus$ $C_{1}$ |
| 47. | % Diffusion phase |
| 48. | for $i$ = 1: m do |
| 49. | for $i$ = j: n do |
| 50. | $\hat{A}''(i,j)$ $\leftarrow$$\hat{A}_{15}^{'''}$ ($E_{1}^{i}$, $E_{2}^{i}$) |
| 51. | end ; end |
| 52. | % Reverse conversion |
| 53. | for $i$ = 1: m do |
| 54. | for $i$ = j: n do |
| 55. | $\hat{A}_{ij}$ $\leftarrow$$\hat{A}''(i,j)$ |
| 56. | if $\beta(i,j)$ ≥ 0 |
| 57. | else |
| 58. | $\hat{A}_{ij}$ $\leftarrow$$-\hat{A}''(i,j)$ |
| 59. | end ; end |
| 60. | audiowrite(‘original data.wav’, $\hat{A}_{ij}$, F) |

TABLE 6. Security analysis of proposed 5 × 5 S-boxes.

| S-box | NL | SAC | BIC | SAC-BIC | LP | DP | LS | LBN | DBN |
|-------|----|-----|-----|---------|----|----|----|-----|-----|
| Proposed $S_{13}^{2}$ (5 × 5) | 10 | 0.527 | 0.600 | 0.5250 | 0.25 | 0.25 | 0 | 2 | 2 |
| Proposed $S_{13}^{2}$ (5 × 5) | 8 | 0.5124 | 0.6181 | 0.5250 | 0.3125 | 0.25 | 0 | 2 | 2 |
| Proposed $S_{13}^{2}$ (5 × 5) | 8 | 0.5122 | 0.5222 | 0.4625 | 0.25 | 0.1875 | 0 | 2 | 2 |
| Ref [33], S-box (8 × 8) | 108 | 0.4988 | 52.851 | 0.4988 | — | — | 0 | 2 | 2 |
| Ref [34], S-box (8 × 8) | 107 | 0.4990 | — | 0.50635 | 0.03906 | 0.1250 | 0 | 2 | 2 |
| Ref [35], S-box (7 × 7) | 52 | 0.4978 | 102.8 | 0.504 | 0.09375 | 0.0156 | 0 | 2 | 2 |
| Ref [41], S-box (4 × 4) | 4 | 0.4922 | — | 0.2500 | 0.2500 | 0.0625 | 0 | 2 | 2 |

The correlation coefficient is a prominent technique used to detect the robustness and linear relationship among the adjacent sample of audio data, as well as examine the suggested encryption scheme as vulnerable to statistical attacks. Since the sample of audio data is highly correlated with one another. Therefore, a highly secured cryptosystem should break the correlation between samples of audio data.

Correlation coefficients can be represented mathematically as follow:

$$\xi_{uv} = \frac{\text{Cov}(x', y')}{\sqrt{D(x')D(y')}}$$  \hspace{1cm} (28)

$$\text{Cov}(x', y') = \frac{1}{x'} \sum_{j=1}^{x'} (x'_j - e(x'))(y'_j - e(y'))$$  \hspace{1cm} (29)

$$D(x') = \sum_{j=1}^{x'} ((x'_j - e(x'))^2$$  \hspace{1cm} (30)

$$D(y') = \frac{1}{x'} \sum_{j=1}^{x'} y'_j$$  \hspace{1cm} (31)

the spectrogram of the plan audio data, ensuring that the audio file has been effectively encrypted.

C. CORRELATION ANALYSIS

The correlation coefficient is a prominent technique used to detect the robustness and linear relationship among the adjacent sample of audio data, as well as examine the suggested encryption scheme as vulnerable to statistical attacks. Since the sample of audio data is highly correlated with one another. Therefore, a highly secured cryptosystem should break the correlation between samples of audio data.
where $x'_j$, represent the chosen sample and $y'_j$, respective neighbouring samples at $j_{th}$ position. Analysis of correlation coefficients is used to evaluate the proposed scheme. Therefore, we picked different adjacent samples to examine the correlation coefficient in multiple dimensions, such as diagonal, vertical, and horizontal dimensions. After all, the samples of audio data are organized in a single array of strings, so we investigate the analysis of the correlation of the
suggested scheme in the horizontal dimension. The result is summarized in Table 7. According to the table, the coefficient of correlation for the plan audio data is 1, which indicates the segments in audio data are highly associated with one another. Nevertheless, the results of encrypted audio data are nearly equal to zero, which shows that the recommended

| S.no | Audio samples         | Size/KB | Plain audio | Cipher audio |
|------|-----------------------|---------|-------------|--------------|
| 1    | Alarm sound.wav       | 186/kb  | 0.89735     | −0.00221     |
| 2    | Dog barking sound.wav | 279/kb  | 0.95292     | 0.00623      |
| 3    | Explosion sound.wav   | 533/kb  | 0.52226     | 0.00161      |
| 4    | Male sound.wav        | 345/kb  | 0.86710     | 0.00844      |
| 5    | Femalesound.wav       | 23.3/kb | 0.85605     | 0.00318      |
| 6    | Baby sound.wav        | 279/kb  | 0.96987     | −0.04283     |
| 7    | Cartoon sound.wav     | 488/kb  | 0.97841     | 0.00154      |
| 8    | Gutter sound.wav      | 270/kb  | 0.96887     | 0.00083      |
| 9    | Lion sound.wav        | 221/kb  | 0.99856     | −0.00158     |
| 10   | Ref [35]              | 395/kb  | −           | 0.02021      |
| 11   | Ref [36]              | −       | −           | 0.00311      |
| 12   | Ref [37]              | 228/kb  | 0.815998    | −0.00938     |
| 13   | Ref [38]              | −       | −           | 0.00029      |
encryption algorithm disrupts the highly connected audio segments. Furthermore, the analysis of plan and encrypted audio data is illustrated in Figure 6. From Figure 6, we can see that the proposed encryption scheme is highly resistant to statistical attacks.

D. INFORMATION OF ENTROPY
Information entropy analysis is used to quantify the level of uncertainty in the encrypted data. In the encrypted audio file, the value of entropy has a direct relationship to the level of uncertainty; the higher its value, the larger the degree of
uncertainty. The information of entropy is computed using the following mathematical formula,

$$H = - \sum_{i=0}^{t} P(i) \log_2 P(i)$$  \hspace{1cm} (32)$$

where $t$ represents the gray audio data file and $p(i)$ shows the probability of occurrence of the gray value $i$. Consequently, a cryptosystem is considered secure if the information entropy value of the encrypted file is close to the ideal value. Table 8
TABLE 8. Entropy analysis.

| S.no | Audio samples             | Size/KB | Plain audio | Cipher audio |
|------|---------------------------|---------|-------------|--------------|
| 1    | Alarm sound.wav           | 186/kb  | 2.3184      | 4.1622       |
| 2    | Dog barking sound.wav     | 279/kb  | 1.6067      | 4.1045       |
| 3    | Explosion sound.wav       | 533/kb  | 2.6766      | 5.6153       |
| 4    | Male sound.wav            | 345/kb  | 1.5477      | 4.5071       |
| 5    | Femalesound.wav           | 23.3/kb | 1.9385      | 4.7672       |
| 6    | Baby sound.wav            | 279/kb  | 2.3182      | 4.1622       |
| 7    | Cartoon sound.wav         | 488/kb  | 2.6223      | 4.7075       |
| 8    | Gutier sound.wav          | 270/kb  | 2.1482      | 5.3487       |
| 9    | Lion sound.wav            | 221/kb  | 2.3132      | 4.7688       |
| 10   | Ref [35]                  | 395/kb  | 2.2661      | 5.0058       |
| 11   | Ref [36]                  | –       | –           | 7.9471       |
| 12   | Ref [37]                  | 228/kb  | –           | –            |

TABLE 9. Differential analysis.

| S.no | Audio samples          | Size/KB | Npocr     | UACI   |
|------|------------------------|---------|-----------|--------|
| 1    | Alarm sound.wav        | 186/kb  | 99.999721 | 33.341312 |
| 2    | Dog barking sound.wav  | 279/kb  | 99.999823 | 33.442345 |
| 3    | Explosion sound.wav    | 533/kb  | 99.999752 | 33.141256 |
| 4    | Male sound.wav         | 345/kb  | 99.999602 | 33.341534 |
| 5    | Femalesound.wav        | 23.3/kb | 99.999501 | 33.445467 |
| 6    | Ref [35]               | 395/kb  | 99.999506 | –      |
| 7    | Ref [36]               | –       | 99.531614 | 25.798423 |
| 8    | Ref [37]               | 228/kb  | 99.734812 | 33.687823 |
| 9    | Ref [38]               | –       | 99.99950 | 33.559915 |
| 10   | Ref [25]               | –       | 99.9997 | 33.3421 |
| 11   | Ref [26]               | –       | 99.9977 | –       |
| 12   | Ref [29]               | –       | 57.23 | –       |

TABLE 10. Peak signal to noise ratio analysis.

| S.no | Audio samples          | Size/KB | PSNR       | MSE    |
|------|------------------------|---------|------------|--------|
| 1    | Alarm sound.wav        | 186/kb  | 10.35740   | 3.26444 × 10^4 |
| 2    | Dog barking sound.wav  | 279/kb  | 10.62277   | 3.26475 × 10^4 |
| 3    | Explosion sound.wav    | 533/kb  | 10.22475   | 3.26379 × 10^4 |
| 4    | Male sound.wav         | 345/kb  | 10.76211   | 3.26511 × 10^4 |
| 5    | Femalesound.wav        | 23.3/kb | 10.75679   | 3.26707 × 10^4 |
| 6    | Baby sound.wav         | 279/kb  | 10.57626   | 3.26446 × 10^4 |
| 7    | Ref [35]               | 395/kb  | 4.2145     | –       |
| 8    | Ref [36]               | –       | 10.7163    | 37.4487 |
| 9    | Ref [37]               | 228/kb  | –          | –       |
| 10   | Ref [38]               | –       | +4.49      | –       |

summarizes the results of an information entropy analysis for the suggested cryptosystem. The suggested scheme information value is significantly closer to the ideal value for every encrypted audio, resulting in optimal uncertainty significantly closer to the ideal value for every encrypted audio, resulting in optimal uncertainty in the audio file, and therefore the presented scheme can withstand an entropy attack, as shown in Table 8.

E. DIFFERENTIAL ATTACKS

The differential attacks utilize two analyses to secure the cryptosystem’s sensitivity: the number of sample change rates (NSCR) and the Unified Average Changing Intensity (UACI). A well-organized cryptographic algorithm should be sensitive enough that a minor change in plain data results in a significant difference in the encrypted data. The mathematical description of NSCR and UACI
TABLE 11. Execution time of proposed algorithm.

| S.no | Audio samples             | Size/KB | Encryption time/sec |
|------|---------------------------|---------|---------------------|
| 1    | Alarm sound.wav           | 186/kb  | 0.00221/sec         |
| 2    | Dog barking sound.wav     | 279/kb  | 0.00334/sec         |
| 3    | Explosion sound.wav       | 533/kb  | 1.07653/sec         |
| 4    | Male sound.wav            | 345/kb  | 0.00734/sec         |
| 5    | Lion sound.wav            | 221/kb  | 0.00311/sec         |
| 6    | Ref[37]                   | 228/kb  | 0.281/sec           |
| 7    | Ref[38]                   | 488/kb  | 1.010126/sec        |

is given as follows.

\[ N_{pcr} = \frac{\sum_{v,v_1} C(v, v_1)}{K} \]  \hspace{1cm} (33)

\[ C(v, v_1) = \begin{cases} 0, & \text{if } S_1(v, v_1) \neq S_2(v, v_1) \\ 1, & \text{if } S_1(v, v_1) = S_2(v, v_1) \end{cases} \]  \hspace{1cm} (34)

\[ U_{aci} = \frac{1}{K} \sum_{v,v_1} \left| S_1(v, v_1) - S_2(v, v_1) \right| \times 100 \]  \hspace{1cm} (35)

where \( K \) in eq(35) represents the audio data set cardinality. The simulation result of the proposed encryption algorithm is shown in Table 9. From the table, we can observe that the simulation score of both analysis NSCR and UACI lie in the optimum range. This reveals the suggested encryption algorithm’s significant reliance on the plan audio data and suggests that it may be more robust against differential attacks.

F. PEAK SIGNAL-TO-NOISE RATIO

Corrupted noise influences the effectiveness of signal representation. After the decryption of any cryptosystem, the Peak signal-to-noise ratio (PSNR) is a robust analysis to investigate the quality of data. The peak signal-to-noise ratio (PSNR) is a decibel(dB) unit metric that quantifies the ratio between the highest power of a signal to the power of a noisy signal value. Furthermore, the greater value of PSNR underscores the effectiveness of the encryption scheme. The PSNR is calculated using the following mathematical expression

\[ P_{SNR} = 20 \times \log_{10} \left( \frac{255}{\sqrt{MSE}} \right) \]  \hspace{1cm} (36)

where Mean square error (mse) is calculated via the following mathematical form

\[ MSE = \frac{1}{M \times N} \sum_{m} \sum_{n} [D(m, n) - E(m, n)]^2 \]  \hspace{1cm} (37)

where \( D(m, n) \), indicate the plan audio data while \( E(m, n) \), is corresponding encrypted audio data. Table 10 indicates the performance analysis of PSNR and MSE of the suggested encryption algorithm. From Table 10 we can observe that the higher value of PSNR and lower value of MSE generally underscore the small amount of data retained in decrypted data. And hence the proposed algorithm is securitized against Robustness analysis.

G. NATIONAL INSTITUTE OF STANDARD AND TECHNOLOGY (NIST) STATISTICAL ANALYSIS

In this subsection of security analysis, we utilize NIST statistical analysis to evaluate the Modell elliptic curve-based pseud random number sequences (MEC-PRNS) and investigate whether the suggested scheme is suitable for the cryptographic application. Since NIST tests work on binary data, so convert the generated sequence to binary to ensure the randomness of the proposed algorithm. There are sixteen (16) tests in the NIST testing suite that are usually performed to examine the randomness of data, as shown in Table 12. From the table, we can notice that MEC-PRNS succeeded in the complete randomness tests of NIST, proving that the MEC-PRNS are highly random and sufficient for audio encryption.

H. ASYMPTOTIC COMPLEXITY AND RUNNING SPEED ANALYSIS

This section theoretically analyzes the proposed encryption over asymptotic complexity. The asymptotic complexity summarizes the growth of the execution time with increasing the size of input data. It divulges the mathematical dept of the algorithm, which is independent of hardware implementation. The algorithm begins by generating random using the arithmetic operation of the Elliptic curve. For this step, we used the search method for generating the EC point, which requires \( O(n^2) \), operation that is the most computationally costly in the scheme. Next, the algorithm uses the random numbers and permutes the plain data, which requires \( O(N \times M) \) operation, where \( N \times M \) is the plain data block size. In the substitution step, the algorithm divides the permuted block data into three subblocks in constant time \( O(1) \). Then substitute each subblock with a different S-box since the substitution step performs in constant time \( O(1) \), therefore, for \( N \times M \) block size, the step also requires \( O(N \times M) \) operations. So, for \( n \geq N \times M \) the whole algorithm performs \( O(n^2) \) operations that are polynomial time. The running time of the proposed encryption scheme is measured in kb/second. We encrypt the different sizes of audio.wav, and the average time of encryption and decryption are 0.00334kb/sec and 0.000539kb/respectively as shown in Table 11. Table 11 indicate that the proposed encryption scheme is less time requirements than ref [35], [36], [37]. As a result, the encryption scheme is efficient and can be used for real-world applications.
### TABLE 12. NIST randomness analysis for cryptographic applications.

| S.no | Test Name                                      | P-Value    | Result   |
|------|-----------------------------------------------|------------|----------|
| 1    | Frequency-Test (single-bit)                   | 0.93432071088934 | Success  |
| 2    | Frequency-Test(block)                         | 0.31475830512155 | Success  |
| 3    | Run Test                                      | 0.41535210874214 | Success  |
| 4    | Longest Run of 1’s in a Block                 | 0.42347212437727 | Success  |
| 5    | Rank test of Binary matrix                    | 0.65746634332441 | Success  |
| 6    | Discrete Fourier Transform (DFT) Spectral test| 0.13758358862813 | Success  |
| 7    | Matching Test of Non-Overlapping Template     | 0.21767757131905 | Success  |
| 8    | Matching Overlapping Template                 | 0.16716577128047 | Success  |
| 9    | Maurer's Universal Statistical test (MUST)    | -1.0        | Not      |
|      |                                               |            | Success  |
| 10   | Linear Complexity (LC) Test                   | 0.54215767242552 | Success  |
| 11   | Approximate Entropy Test (AET)                | 0.04554663062186 | Success  |
| 12   | Forward Cumulative Sums (FCS) test            | 0.98745143218243 | Success  |
| 13   | Reverse Cumulative Sums (RCS) test            | 0.98678134070164 | Success  |
| 14   | Serial test (ST)                              | 0.12491742322324 | Success  |
| 15   | Random Excursions Test                         | P – value  | Result   |
| 16   | Random excursions variant test                | P – value  | Result   |
|      | State                                         | Chai-squared value |         |
| -4   | -4                                            | 4.123469951021149 | 0.5836458638476241 | Success |
| -3   | -3                                            | 1.744271338713358 | 0.8736591835003546 | Success |
| -2   | -2                                            | 4.844693165257315 | 0.4141356734512387 | Success |
| -1   | -1                                            | 5.240705127776518 | 0.4012356714687765 | Success |
| 1    | 1                                             | 3.563295336645158 | 0.64757776412386  | Success |
| 2    | 2                                             | 4.076914662345544 | 0.5476836646123396 | Success |
| 3    | 3                                             | 5.623125337746047 | 0.3761126757224412 | Success |
| 4    | 4                                             | 3.5459267601847782 | 0.6234512475488964 | Success |
|      | State                                         | Chai-squared value |         |
| 1.0  | 1.0                                           | 334        | 0.1237659854642848 | Success |
| 2.0  | 2.0                                           | 353        | 0.2834649944849434 | Success |
| 3.0  | 3.0                                           | 335        | 0.2347374842019319 | Success |
| 4.0  | 4.0                                           | 325        | 0.4546373846476437 | Success |
| 5.0  | 5.0                                           | 305        | 0.3453848434811987 | Success |
| 6.0  | 6.0                                           | 298        | 0.3645367465353636 | Success |
| -1.0 | -1.0                                          | 251        | 0.4763544688346878 | Success |
| -2.0 | -2.0                                          | 248        | 0.1234687473534484 | Success |
| -3.0 | -3.0                                          | 253        | 0.7464364454193768 | Success |
| -4.0 | -4.0                                          | 276        | 0.1236294849734841 | Success |
| -5.0 | -5.0                                          | 247        | 0.537848646234648  | Success |
| -6.0 | -6.0                                          | 253        | 0.6473543878434384 | Success |
VI. CONCLUSION
This manuscript proposed a new approach to digital audio encryption for real-world communication. In the first section of the manuscript, we demonstrated the MEC over a finite field and examined it through phase diagrams and bifurcation plots. To achieve the diffusion phase, utilized nonlinear sequences generated through MEC. As a result, the correlation between the original and encrypted data of audio samples is negligible. The selection of $5 \times 5$ S-boxes was employed for the confusion module. Initially, the fifteen-bit data dived into three subblocks each of five-bit and substituted the block’s five-bit integer data with the three different $5 \times 5$ S-boxes, which eventually produced optimum confusion in encrypted blocks. Furthermore, the process of points generation utilized the searching method which significantly reduces the time complexity up to the exceptional margin, but still the proposed audio encryption scheme based on generating MEC points is time-consuming, and the algorithm computational complexity is reasonably high. Therefore, the effort may be given to make this computation efficient for a strong random number generation scheme with less computational complexity in the future. Moreover, the proposed algorithm is validated for offline audio files, although live encrypted audio streaming is in demand these days. Thus, in the future, an attempt may be made to speed up this algorithm to expand the use of this application for live audio streaming. The simulation result presents that the suggested encryption efficiently encrypts and turns the audio data into an indistinguishable uniform sound. Moreover, the proposed scheme is analyzed against several attacks, and the results show that the suggested encryption scheme is more resistant to statistical and differential attacks.

REFERENCES
[1] E. Barker and N. Mouha, “Recommendation for the triple data encryption algorithm (TDEA) block cipher,” Nat. Inst. Standards Technol., Gaithersburg, MD, USA, Tech. Rep., 800–67, 2017.
[2] J. Daemen and V. Rijmen, “Reijnald: The advanced encryption standard,” J. Softw. Tools Prof. Programmer, vol. 26, no. 3, pp. 137–159, 2001.
[3] R. L. Rivest, A. Shamir, and L. Adleman, “A method for obtaining digital signatures and public-key cryptosystems,” Commun. ACM, vol. 21, no. 2, pp. 120–126, Feb. 1978.
[4] Data Encryption Standard (DES), Standard FIPS PUB 3-46, 1999.
[5] J. Pierce, “The early days of information theory,” IEEE Trans. Inf. Theory, vol. IT-19, no. 1, pp. 3–8, Jan. 1973.
[6] C. Li, Y. Zhang, and E. Y. Xie, “When an attacker meets a cipher-image in 2018: A year in review,” J. Inf. Secur. Appl., vol. 48, Oct. 2019, Art. no. 102361.
[7] J.-X. Chen, Z.-L. Zhu, C. Fu, H. Yu, and L.-B. Zhang, “A fast chaos-based image encryption scheme with a dynamic state variables selection mechanism,” Commun. Nonlinear Sci., vol. 20, no. 5, pp. 846–860, Mar. 2015.
[8] G. Ye and J. Zhou, “A block chaotic image encryption scheme based on self-adaptive modelling,” Appl. Soft Comput., vol. 22, pp. 351–357, Sep. 2014.
[9] X. Chai, “An image encryption algorithm based on bit level Brownian motion and new chaotic systems,” Multimedia Tools Appl., vol. 76, no. 1, pp. 1159–1175, Jan. 2017.
[10] C. Fu, B.-B. Lin, Y.-S. Miao, X. Liu, and J.-J. Chen, “A novel chaos-based bit-level permutation scheme for digital image encryption,” Opt. Commun., vol. 284, no. 23, pp. 5415–5423, 2011.
[11] W. Zhang, K.-W. Wong, H. Yu, and Z.-L. Zhu, “A symmetric color image encryption algorithm using the intrinsic features of bit distributions,” Commun. Nonlinear Sci. Numer. Simul., vol. 18, no. 3, pp. 584–600, Mar. 2013.
[12] F. J. Farsana and K. Gopakumar, “A novel approach for speech encryption: Zaslavsky map as pseudo random number generator,” Proc. Comput. Sci., vol. 93, pp. 816–823, Jan. 2016.
[13] S. Nagaraj, G. S. V. Raju, and K. K. Rao, “Image encryption using elliptic curve cryptography and matrix,” Proc. Comput. Sci., vol. 48, pp. 276–281, Jan. 2015.
[14] A. Soleymani, M. J. Nordin, and Z. M. Ali, “A novel public key image encryption based on elliptic curves over prime group field,” J. Image Graph., vol. 1, no. 1, pp. 49–59, 2013.
[15] D. Mahato, D. A. Khan, and D. K. Yadav, “Security analysis of elliptic curve cryptography and RSA,” in Proc. World Congr. Eng., vol. 1, Jun. 2016, pp. 419–422.
[16] L. D. Singh and K. M. Singh, “Image encryption using elliptic curve cryptography,” Proc. Comput. Sci., vol. 54, pp. 472–481, Aug. 2015.
[17] A. Soleymani, M. J. Nordin, A. N. Hoshyar, Z. M. Ali, and E. Sundararajan, “An image encryption scheme based on elliptic curve and a novel mapping mechanism,” Int. J. Dig. Tech. Eng., vol. 7, no. 13, p. 85, 2015.
[18] L. D. Singh and K. M. Singh, “Implementation of text encryption using elliptic curve cryptography,” Proc. Comput. Sci., vol. 54, pp. 73–82, Aug. 2015.
[19] L. Li, A. A. El-Atif, and X. Niu, “Elliptic curve ElGamal based homomorphic image encryption scheme for sharing secret images,” Signal Process., vol. 92, no. 4, pp. 1069–1078, Apr. 2012.
[20] W. Q. Yan, W. G. Fu, and M. S. Kankanhalli, “Progressive audio scrambling in compressed domain,” IEEE Trans. Multimed., vol. 10, no. 6, pp. 960–968, Oct. 2008.
[21] J. Zhou and O. C. Au, “Security and efficiency analysis of progressive audio scrambling in compressed domain,” in Proc. IEEE Int. Conf. Acoust., Speech Signal Process., Mar. 2010, pp. 1802–1805.
[22] J. B. Lima and E. F. D. S. Neto, “Audio encryption based on the cosine number transform,” Multimedia Tools Appl., vol. 75, no. 14, pp. 8403–8418, Jul. 2016.
[23] N. J. Thorwirth, P. Horvatic, R. Weis, and J. Zhao, “Security methods for MP3 music delivery,” in Proc. 34th Asilomar Conf. Signals, Syst. Comput., 2000, pp. 1831–1835.
[24] E. Mosa, N. W. Messiha, O. Zahrani, and F. E. Abd El-Samie, “Chaotic encryption of speech signals,” Int. J. Speech Technol., Nov. 2014, pp. 285–296, Dec. 2011.
[25] F. J. Farsana, V. R. Devi, and K. Gopakumar, “An audio encryption scheme based on fast Walsh Hadamard transform and mixed chaotic keystreams,” Appl. Comput. Inform., Aug. 2018, doi: 10.1016/j.aci.2019.10.001.
[26] P. K. Naskar, S. Paul, D. Nandy, and A. Chaudhuri, “DNA encoding and channel shuffling for secured encryption of audio data,” Multimedia Tools Appl., vol. 78, no. 17, pp. 25019–25042, Sep. 2019.
[27] H. Liu, A. Kadir, and Y. Li, “Audio encryption scheme by confusion and diffusion based on multiscroll chaotic system and one-time keys,” Optik, vol. 127, no. 19, pp. 7431–7438, 2016.
[28] R. Singh, R. Chauhan, V. K. Gunjan, and P. Singh, “Implementation of elliptic curve cryptography for audio-based application,” Int. J. Eng. Res. Technol., vol. 3, no. 1, pp. 2210–2214, 2014.
[29] R. Apau and S. Adu, “Data hiding in audio signals using elliptic curve cryptography, Huffman code algorithm and low-bit encoding,” Int. J. Comput. Appl., vol. 180, no. 39, pp. 24–34, May 2018.
[30] R. Shelke and M. Nemade, “Audio encryption algorithm using modified elliptical curve cryptography and Arnold transform for audio watermarking,” in Proc. 3rd Int. Conf. Converg. Technol. (ICT), Apr. 2018, pp. 1–4.
[31] L. C. Washington, Elliptic Curves: Number Theory and Cryptography. Boca Raton, FL, USA: CRC Press, 2008.
[32] S. D. Galbraith, Mathematics of Public Key Cryptography. Cambridge, U.K.: Cambridge Univ. Press, 2012.
[33] M. A. B. Farah, R. Guesmi, A. Kachouri, and M. Samet, “A new design of cryptosystem based on S-box and chaotic permutation,” Multimedia Tools Appl., vol. 79, nos. 27–28, pp. 19129–19150, Jul. 2020.
[34] M. I. Haider, A. Ali, D. Shah, and T. Shah, “Block cipher’s non-linear component design by elliptic curves: An image encryption application,” Multimedia Tools Appl., vol. 80, no. 3, pp. 4693–4718, Jan. 2021.
[35] S. Adhikari and S. Karforma, “A novel audio encryption method using Henon–Tent chaotic pseudo random number sequence,” Int. J. Inf. Technol., vol. 13, no. 4, pp. 1463–1471, 2021.
[36] H. Aziz, S. M. M. Gilani, I. Hussain, A. K. Janjua, and S. Khurram, “A noise-tolerant audio encryption framework designed by the application of $S_4$ symmetric group and chaotic systems,” Math. Problems Eng., vol. 2021, pp. 1–15, Apr. 2021.

[37] M. S. Khoirom, D. S. Laiphrakpam, and T. Tuithung, “Audio encryption using ameliorated ElGamal public key encryption over finite field,” Wireless Pers. Commun., vol. 117, no. 2, pp. 809–823, Mar. 2021.

[38] P. K. Naskar, S. Bhattacharyya, and A. Chaudhuri, “An audio encryption based on distinct key blocks along with PWLCM and ECA,” Nonlinear Dyn., vol. 103, no. 2, pp. 2019–2042, Jan. 2021.

[39] M. Kumar, A. Iqbal, and P. Kumar, “A new RGB image encryption algorithm based on DNA encoding and elliptic curve Diffie–Hellman cryptography,” Signal Process., vol. 125, pp. 187–202, Aug. 2016.

[40] Z. Zhao and X. Zhang, “ECC-based image encryption using code computing,” in Proc. Int. Conf. Commun., Electron. Automat. Eng. Berlin, Germany: Springer, 2013, pp. 859–865.

[41] I. Khalid, S. S. Jamal, T. Shah, D. Shah, and M. M. Hazzazi, “A novel scheme of image encryption based on elliptic curves isomorphism and substitution boxes,” IEEE Access, vol. 9, pp. 77798–77810, 2021.

**IAZ KHALID** is currently a Ph.D. Research Scholar at the Department of Mathematics, Quaid-i-Azam University, Islamabad, Pakistan. He has been working on Elliptic Curve Cryptography, since 2018.

**TARIQ SHAH** received the Ph.D. degree in mathematics from the University of Bucharest, Romania, in 2000. He is currently a Professor with the Department of Mathematics, Quaid-i-Azam University Islamabad, Pakistan. His research interests include commutative algebra, non-associative algebra, and error-correcting codes and cryptography.

**KHALID ALI ALMARHABI** received the B.Sc. degree in computer science from King Abdulaziz University, Jeddah, Saudi Arabia, in 2009, the M.Sc. degree in information technology from the Queensland University of Technology, Brisbane, Australia, in 2014, and the joint Ph.D. degree in computer science from King Abdulaziz University and the Queensland University of Technology. He is currently an Associate Professor at the Computer Science Department, College of Computing in Al-Qunfudah, Umm Al-Qura University, Saudi Arabia. His research interests include information security, BYODs research, access control policies, information system management, and cloud computing.

**DAWOOD SHAH** received the M.Phil. degree and the Ph.D. degree in mathematics from Quaid-i-Azam University, Islamabad, Pakistan. His research interests include coding theory, finite fields, and cryptography.

**MUHAMMAD ASIF** received the Ph.D. degree in mathematics from Quaid-i-Azam University, Islamabad, Pakistan, in 2020. He is currently an Assistant Professor with the Department of Mathematics, University of Management and Technology, Sialkot, Pakistan. His research interests include large scale of coding theory, cryptography, information theory, and algebra.

**M. USMAN ASHRAF** received the Ph.D. degree in computer science from King Abdul-Aziz University, Saudi Arabia, in 2018. He is currently an Assistant Professor with GC Women University, Sialkot, Pakistan. His research on exascale computing systems, high performance computing (HPC) systems, parallel computing, and HPC for deep learning and location-based services system has appeared in IEEE ACCESS, IET Software, International Journal of Advanced Research in Computer Science, International Journal of Advanced Computer Science and Applications, IJ Information Technology and Computer Science, International Journal of Computer Science and Security, and several International IEEE/ACM/Springer conferences. He has served as a HPC Scientist at the HPC Centre King Abdul-Aziz University.