Audio Encryption and Decryption under Elliptic Curve Cryptography and DNA Algorithm

Md. Imdadul Islam, Samsun Nahar Khandakar, Nadia Afrin Ritu, Md. Masum Bhuiyan and Sarwar Jahan

***Abstract*—Secure audio transmission is crucial in military, telemedicine, and IoT multimedia, where confidentiality and integrity are vital. Traditional methods, such as RSA, are computationally intensive, while DNA cryptography is efficient but less secure. This paper proposes an audio encryption and decryption scheme using Elliptic Curve Cryptography (ECC). In the proposed method, a pair of audio signals is taken as plaintext, and corresponding sample points are combined into ordered pairs. Some points fall outside the elliptic curve and cannot be directly decrypted; these are preserved in a sparse vector. The encrypted vector and sparse vector are transmitted through a noiseless channel, and at the receiving end, they are combined to ensure complete recovery of the original signals. Appropriate ECC parameters are selected to minimize the number of ambiguous points, allowing for 100% accurate recovery. The performance of ECC is compared with RSA and DNA cryptography in terms of processing time and security level. Additionally, encryption rigidity is evaluated using cross-correlation, discrete wavelet transform (DWT) spectral analysis, and fuzzy entropy. Results demonstrate that ECC achieves the strongest security among the three approaches, albeit with higher processing complexity, whereas DNA is most suitable for real-time applications due to its efficiency.**

***Index terms*—Sparse sample, Cross-correlation, Fuzzy entropy, RSA, DWT, and Spectrogram.**

I. Introduction

The growing prevalence of multimedia transmission and Internet of Things (IoT) applications has made the secure exchange of audio data increasingly critical. Audio is an integral part of several sensitive domains such as military communication, telemedicine, surveillance, and smart home devices, where both confidentiality and data integrity must be preserved. In such applications, unauthorized access, tampering, or interception of audio data can lead to severe privacy breaches or operational failures. Therefore, the development of lightweight yet secure encryption techniques suitable for real-time audio transmission has become an important research challenge.

Traditional asymmetric algorithms, particularly the Rivest–Shamir–Adleman (RSA) algorithm, provide strong cryptographic security but suffer from high computational overhead during key generation and decryption, which limits their efficiency in real-time scenarios. On the other hand, DNA-based cryptographic schemes offer greater efficiency and reduced computation time but compromise on encryption strength and resistance to brute-force or statistical attacks. These opposing characteristics reveal a significant research gap between efficiency and security in existing audio encryption methods.

Elliptic Curve Cryptography (ECC) provides a promising balance between computational efficiency and high-level security. ECC achieves an equivalent security level to RSA using much smaller key sizes, resulting in reduced memory usage, faster computation, and lower energy consumption — qualities essential for IoT and embedded multimedia systems. However, ECC has not yet been fully exploited for audio signal encryption, particularly in contexts where signal points do not always map perfectly onto the elliptic curve.

Previous studies have explored various cryptographic methods for multimedia and audio encryption. Works in [6], [7] applied ECC to real-time audio and demonstrated robustness under noisy conditions, though computational efficiency was not analyzed. A comprehensive survey in [9] reviewed ECC, DNA, and hybrid methods, highlighting their potential but lacking experimental validation. DNA-based approaches [10–12] achieved strong diffusion and high Avalanche Effect but were limited to image data. Hybrid DNA–ECC models [13] improved security for IoT devices but incurred high computational cost, while audio-focused methods [14–16] based on image conversion or chaotic maps overlooked efficiency and recovery accuracy. Other studies extended ECC to cloud, IoT, and authentication systems [17–20], confirming its versatility but without comparative performance evaluation. Direct comparisons of RSA and ECC [21–22] confirmed ECC's higher security and resistance to attacks, though runtime and recovery issues remained unexplored. Overall, prior works establish ECC and DNA as promising techniques but leave open challenges in achieving efficient, fully recoverable, and statistically robust audio encryption—the focus of the present research.

Addressing these issues motivates the current research, which proposes a novel audio encryption and decryption scheme based on Elliptic Curve Cryptography (ECC) enhanced with a sparse vector correction mechanism. The proposed method pairs samples from two audio signals and encrypts them using ECC parameters optimized to minimize the number of ambiguous points. Any samples that fall outside the elliptic curve are stored in sparse vectors and reintegrated during decryption to guarantee 100% recovery of the original signal. The performance of the proposed ECC model is compared with RSA and DNA cryptography across statistical, spectral, and fuzzy entropy analyses to evaluate both encryption strength and

Manuscript received June 16, 2025; revised September 5, 2025. Date of publication January 30, 2026. Date of current version January 30, 2026.

Authors are with the Department of Computer Science and Engineering, Jahangirnagar University, Savar, Dhaka-1342 (e-mails: {imdad, samsunnahar, nadiaritu, b.masum}@juniv.edu, sjahan@ewubd.edu).

Digital Object Identifier (DOI): 10.24138/jcomss-2025-0105

computational efficiency. Experimental results demonstrate that ECC offers the strongest security, DNA achieves the fastest runtime, and RSA provides moderate performance, thereby establishing a balanced perspective for selecting cryptographic methods in real-time audio communication and IoT environments.

The main contributions of this research work are as follows:

- A novel ECC-based encryption and decryption algorithm for audio signals that ensures 100% recovery using a sparse vector for ambiguous points.
- A comparative performance analysis of ECC, RSA, and DNA cryptography algorithms in terms of encryption quality, process time, and statistical measures (e.g., variance, entropy, cross-correlation).
- Introduction of fuzzy entropy and spectral component analysis to evaluate the encryption rigidity of each cryptographic method.
- A comprehensive experimental setup with real-time audio signals, including encryption/decryption time analysis across different audio types.
- A demonstration that ECC provides the highest security, while DNA cryptography offers the best efficiency for real-time applications.

The rest of the paper is organized as follows: Section II reviews the related studies and outlines the literature gaps. Section III describes the basic theory behind the ECC, RSA, and DNA cryptographic techniques. Section VI presents the methodology of the proposed encryption and decryption algorithms. Section V illustrates the experimental results and provides a comparative analysis among the algorithms. Finally, Section VI concludes the research and outlines directions for future work.

II. Related Works

Several studies have explored cryptographic techniques for securing audio and multimedia signals using various mathematical and biological approaches. In [6–7], ECC was applied to real-time audio in noisy environments where interference was either channel-induced or user-induced. The study clearly presented system flow diagrams and compared the original and encrypted audio using histograms, correlation, entropy, contrast, energy, and homogeneity measures, as well as spectrograms. The advantage of this work lies in its demonstration of ECC's robustness under noisy conditions. However, the main limitation is that it did not analyze computational complexity, leaving efficiency issues unexplored. The comparison of correlation, entropy, contrast, energy, and homogeneity between original and encrypted signals is shown in several tables for three audio signals. Finally, a comparison of the spectrograms of two audio signals before and after encryption is presented, where their variations are visually apparent at a glance [8].

A comprehensive survey in [9] analyzed various cryptographic methods, including DNA, ECC, homomorphic, hybrid, and lightweight approaches, with a discussion on algorithms, results, applications, and limitations. This work excels in broad coverage and insightful cloud data security recommendations, but lacks experimental validation.

DNA cryptography and its constraints were examined in [10], with similar evaluations in [11], where DNA performance was tested on images using PSNR, NPCR, UACI, correlation coefficients, and entropy. These works contributed valuable statistical benchmarking, but they are limited by focusing solely on image data, rather than audio or real-time signals. In [12], DNA was compared with RSA in terms of bit changes and Avalanche Effect, showing DNA's higher AE. While this highlights DNA's diffusion strength, it lacks broader robustness tests.

A hybrid DNA–ECC model was introduced in [13] for IoT devices. The key advantage is its improved security over standalone methods, verified against brute force attacks. The limitation is its high computational cost and restriction to text-based data rather than multimedia. Audio-specific cryptography was studied in [14–15], where audio signals were converted to two-dimensional matrices for encryption using image-based methods. Performance was evaluated using BER in [14] and SNR in [15]. The novelty lies in treating audio as images for encryption. The drawback is that these works used only limited performance metrics and did not consider computational efficiency. In [16], a chaotic map-based approach was proposed, utilizing pseudo-random numbers and rotation equations, with evaluation based on correlation, NSCR, SNR, PSNR, and encryption time. This method achieved strong randomness and signal similarity across domains**,** but its synchronization overhead and lack of comparison with ECC limit its relevance.

ECC was also explored beyond audio, such as for secure authentication in cloud systems [17] and dynamic constellation rotation for wireless encryption [18]. These works underscore ECC's adaptability, but they focus on authentication and physical layer encryption rather than multimedia applications.

Studies in [19–20] have highlighted the prominence of ECC in IoT security, particularly in mitigating man-in-the-middle attacks. While they confirm ECC's growing role in IoT**,** the absence of comparative analysis or statistical evaluation limits the utility of their findings.

A direct RSA–ECC comparison was conducted in [21] using sequences of 8-, 64-, and 256-bit length. The results showed RSA's faster encryption but slower decryption, with ECC overall more secure and efficient. The drawback is that no statistical robustness tests were performed. Similarly, in [22], ECC was applied to audio and evaluated with entropy, correlation, NPCR, UACI, PSNR, MSE, RMS, and crest factor values. This demonstrated ECC's resistance to attacks**,** but it did not examine computational efficiency**.** Finally, [23] applied RSA and DNA to medical images using seven statistical parameters. This extended cryptography into medical IoT data, but it did not integrate ECC, nor did it address audio applications.

The collective insights from these studies reveal that while ECC and DNA cryptography have proven effective for securing multimedia and IoT data, significant gaps remain. Most prior works have not simultaneously addressed computational efficiency, full audio recovery, and robustness against statistical attacks. The present study bridges this gap by proposing an ECC-based audio encryption and decryption method enhanced with a sparse vector correction mechanism, ensuring both strong security and complete recovery of the original audio

signal. A comparison with RSA and DNA cryptography further clarifies the trade-offs between security strength and processing efficiency.

III. Basic Theory

The original messages to be encrypted are known as plaintext, and are transformed by an algorithm with some known parameters called keys. The output of the encryption algorithm, known as the ciphertext, is then transmitted through the communication channel. When the same key parameters are used for both encryption and decryption, it is known as symmetric-key cryptography. Elliptic curve cryptography (ECC) is an asymmetric cryptography method, similar to RSA, where two separate keys — a public key and a private key — are used for encrypting and decrypting data.

A. The elliptic Curve Cryptography

The generalized cubic equation used in Elliptic Curve cryptography (ECC) is expressed as [24-25],

$$y^2 + b_1xy + b_2y = x^3 + a_1x^2 + a_2x + a_3. \quad (1)$$

A simplified form of eq. (1) is used in ECC as,

$$y^2 = x^3 + ax + b\ . \quad (2)$$

The constraint, $4a^3 + 27b^2 \neq 0$, is used as the nonsingular elliptic curve, which has three distinct roots. The ECC algorithm, in the context of audio encryption and decryption, is presented in the next section.

B. DNA Cryptography

In DNA cryptography, four symbols, A, C, G, and T, are used, corresponding to the names of the four bases of biological DNA found in [26-27]. Each symbol is represented by two binary bits, and their complement symbols (bases *A*-*T* and *C*-*G* are connected on the DNA ladder) are shown in Table I.

TABLE I
DNA and Complements

DNA	Complement
C = 00	*G* = 11
T = 01	*A* = 10
A = 10	*T* = 01
G = 11	*C* = 00

Two binary bits (00, 01, 10, and 11) against each of four symbols (*A*, *T*, *C*, and *G*) are assigned in 8 different combinations, and each of the combinations is called a rule. The 8 possible DNA rules are shown in Table II.

TABLE II
DNA and Complements

Rule	Rule -1	Rule -2	Rule -3	Rule -4	Rule -5	Rule -6	Rule -7	Rule -8
00	*A*	*A*	*G*	*G*	*T*	*T*	*C*	*C*
01	*C*	*G*	*A*	*T*	*C*	*G*	*A*	*T*
10	*G*	*C*	*T*	*A*	*G*	*C*	*T*	*A*
11	*T*	*T*	*C*	*C*	*A*	*A*	*G*	*G*

Three DNA operators —addition, subtraction, and XOR — are used on the symbols A, T, G, and C, as shown in Tables III, IV, and V.

TABLE III
DNA Addition

Addition	*C* = 00	*T* = 01	*A* = 10	*G* = 11
C = 00	*C*	*T*	*A*	*G*
T = 01	*T*	*A*	*G*	*C*
A = 10	*A*	*G*	*C*	*T*
G = 11	*G*	*C*	*T*	*A*

TABLE IV
DNA Subtraction

Subtraction	*C* = 00	*T* = 01	*A* = 10	*G* = 11
C = 00	*C*	*G*	*A*	*T*
T = 01	*T*	*C*	*G*	*A*
A = 10	*A*	*T*	*C*	*G*
G = 11	*G*	*A*	*T*	*C*

TABLE V
DNA XOR

XOR	*C* = 00	*T* = 01	*A* = 10	*G* = 11
C = 00	*C*	*T*	*A*	*G*
T = 01	*T*	*C*	*G*	*A*
A = 10	*A*	*G*	*C*	*T*
G = 11	*G*	*A*	*T*	*C*

The steps of the DNA cryptography operation are illustrated with examples in the next section.

C. RSA Algorithm

The simplest form of asymmetric key cryptography was introduced by a research group of M.I.T. in 1978, known as RSA (Rivest, Shamir, Adleman). The steps of the RSA method are presented below, as described in [28-29].

- ✓ Select two prime numbers: p and q
- ✓ Evaluate $n = pq$ and $z = (p-1)(q-1)$
- ✓ Select d such that $gcd\ (d,z) = 1$
- ✓ Choose e such that $de = 1\ mod\ z$

All three of the above algorithms are used in this research work.

D. Fuzzy Entropy

In voice communication, the number of quantization levels is 256. If p_k is the probability of a quantized sample of a voice signal of level k and the corresponding MF of a fuzzy system is $\mu(k)$, then the weighted probabilities [30-31],

$$p_d = \sum_{k=0}^{255} p_k \times \mu_d(k) \quad (3)$$

$$p_m = \sum_{k=0}^{255} p_k \times \mu_m(k) \quad (4)$$

$$p_b = \sum_{k=0}^{255} p_k \times \mu_b(k) \quad (5)$$

Here we consider that the fuzzy variable has three linguistic values: m, d, and b; the corresponding MFs are: $\mu_m, \mu dk$, and $\mu_b(k)$. The MFs are Gaussian, expressed as [31-32],

$$\mu_m(k) = \begin{cases} 0, & k \le a_1 \\ \frac{(k-a_1)^2}{(c_1-a_1)(b_1-a_1)}, & a_1 < k \le b_1 \\ 1 - \frac{(k-c_1)^2}{(c_1-a_1)(c_1-b_1)}, & b_1 < k \le c_1 \\ 1, & c_1 < k \le a_2 \\ 1 - \frac{(k-a_2)^2}{(c_2-a_2)(b_2-a_2)}, & a_2 < k \le b_2 \\ \frac{(k-c_2)^2}{(c_2-a_2)(c_2-b_2)}, & b_2 < k \le c_2 \\ 0, & k > c_2 \end{cases} \quad (6)$$

$$\mu_d(k) = \begin{cases} 1, & k \le a_1 \\ 1 - \frac{(k-a_1)^2}{(c_1-a_1)(b_1-a_1)}, & a_1 < k \le b_1 \\ \frac{(k-c_1)^2}{(c_1-a_1)(c_1-b_1)}, & b_1 < k \le c_1 \\ 0, & k > c_1 \end{cases} \quad (7)$$

$$\mu_b(k) = \begin{cases} 0, & k \le a_2 \\ \frac{(k-a_2)^2}{(c_2-a_2)(b_2-a_2)}, & a_2 < k \le b_2 \\ 1 - \frac{(k-c_2)^2}{(c_2-a_2)(c_2-b_2)}, & b_2 < k \le c_2 \\ 1, & k > c_2 \end{cases} \quad (8)$$

The graphical plot of the above MFs is given in Fig.1, taking a_1= 50, b_1 = 75, c_1 = 100, a_2 = 150, b_2 = 175, and c_2 = 200, where the base variable is the index k of the quantized sample having the values k = 0 to 255.

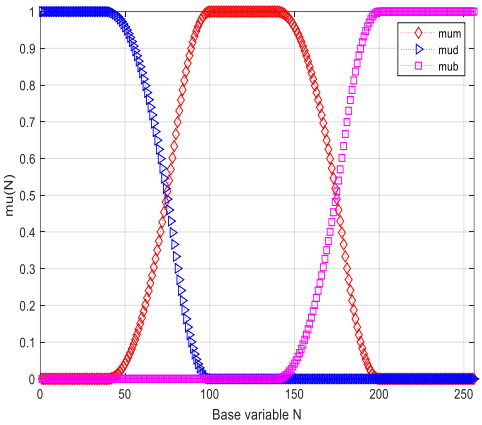


Fig. 1. MFs of fuzzy values

The Fuzzy entropy of each MF,

$$H_d = -\sum_{k=0}^{255} \frac{p_k \times \mu_d(k)}{p_d} ln\left(\frac{p_k \times \mu_d(k)}{p_d}\right) \quad (9)$$

$$H_m = -\sum_{k=0}^{255} \frac{p_k \times \mu_m(k)}{p_m} ln\left(\frac{p_k \times \mu_m(k)}{p_m}\right) \quad (10)$$

$$H_b = -\sum_{k=0}^{255} \frac{p_k \times \mu_b(k)}{p_b} \times ln\left(\frac{p_k * \mu_b(k)}{p_b}\right) \quad (11)$$

The whole fuzzy entropy [32-33] is

$$H = H_d + H_m + H_b. \quad (12)$$

In this paper, we vary the parameters $a1$, $b1$, $c1$, $a2$, $b2$, and $c2$ to attain the maximum value of fuzzy entropy for both the original and encrypted signals, in order to assess the rigidity of encryption algorithms.

IV. Methodology

This section deals with three cryptographies: (1) ECC, (2) RSA, and (3) DNA cryptography. The algorithm for audio signal encryption and decryption using a sparse vector under ECC is presented below.

E. Pair of Audio Signal Encryption and Decryption using ECC

E.1 Encryption Algorithm

1. Select the encryption parameters based on a simplified elliptic curve $y^2 = x^3 + ax + b$ as: a, b, p, $e_1 = (x_1, y_1)$, $e_2 = (x_2, y_2)$; where a and b are the coefficients of the elliptic curve, p is the prime number used in GF, e_1 is a point on the elliptic curve and e_2 is another point determined from e_1 using the private key.
2. Vary the parameters of step 1 until getting the minimum number of ambiguous points for the sparse vector.
3. Select two audio signals: $v_1(t)$ and $v_2(t)$, each of the same length, i.e., N samples.
4. Create an ordered pair, Pi = ($v1(i)$, $v2$ (i)), using the ith sample of audio signals.
5. Encrypt and decrypt the ordered pair, P_i = ($v_1(i)$ and $v_2(i)$), for i = 1, 2, 3, …, N
6. The encrypted ordered pair is E_i= ($e_1(i)$, $e_2(i)$) and that of decrypted ordered pair is, D_i = ($d_1(i)$, $d_2(i)$)
7. The sample outside of the elliptic curve is checked and replaced by 0 to form the transmitted signal, and those ambiguous samples are preserved separately on a sparse vector.

```
%The transmitted vector-1
for i = 1 to N do
    if d1(i) ≠ v1(i) then
        Tx1(i) = 0;
        sparse_vector1(i) = v1(i)
    else
        Tx1(i) = e1(i);
        sparse_vector1(i) = 0;
    end if
end for
```

8. Repeat step 6 for vector 2
9. Select random key r, evaluate cipher text $C_1 = r \times e_1$ and $C_2 = P + r \times e_2$.

E.2 Decryption Algorithm with sparse vectors

10. Evaluate the point $d \times C_1$, then invert it to get the point Q
11. Add Q with C_2 to get P_i = ($v_1(i)$ and $v_2(i)$) for i = 1, 2, 3, …, N

12. To count the ambiguous points:

```
if v1(i) = 0 then
    v1(i) ← sparse_vector1(i)
end if
if v2(i) = 0 then
```

$v_2(i) \leftarrow$ sparse_vector$_2(i)$
end if
13. Repeat steps 10 to 12 for i = 1 to N

F. RSA Algorithm

1. Select the length of the audio signal *N*.
2. Load the audio signal **S**, and resize it to length *N* as ***S****(1…N)*.
3. Normalize the numerical values of samples of audio signal.
4. Select encryption parameters: $e = 3$, $n = 33$, $d = 7$.

for *i = 1 to N*:
Determine encrypted signal: $E(i)=\text{mod}(S(i)^e, n)$
end for

for *i = 1 to N:*
Decrypt the signal: $D(i)=\text{mod}((E(i))^d, n)$
end for

5. Show original, encrypted, and decrypted signals
6. Determine the statistical parameters of the above three signals

G. Steps of Operation under DNA Cryptography

Step 1: Take the input plain text data, *P = 150*
Step 2: Convert it into binary, 150 ↔ 10 01 01 10
Step 3: Apply rule-1 on the bit sequence,
P = 10 01 01 10 ↔ G C C G
Step 4: Take the key 75 ↔ 01 00 10 11 ↔ *C A G T*
Step 5: Apply DNA addition for encryption as:
plain text + key = encrypted sequence
G C C G + C A G T = G A G C
Step 6: Apply DNA subtraction to get the plain text again:
encrypted sequence - key = plain text
G A G C - C A G T = G C C G ↔ 10 01 01 10
↔150 = P

Under the XOR operation, steps 5 and 6 are replaced by the following operation:
plain text XOR key = encrypted sequence
encrypted sequence XOR *key = plain text*

For example,
Plain text ⊕ *key = G C C G* ⊕ *C A G T*
= G A G A
= Encrypted sequence
Encrypted sequence ⊕ *key = G A G A* ⊕ *C A G T*
= G C C G
= P

H. Lowest Spectral Components of Original and Encrypted Signals

1. Size of the audio samples, N = 1024
2. Size of lowest spectral components, M = 8
3. Read the audio file as *Ir*
4. Extract N samples to create an array *I*.
for *i = 1 to N*
I(*i*) = *Ir*(*i*)
end for
5. Convert samples to double-precision floating-point representation
Io=double(I);
6. Encrypt the audio block, *Ie = encrypt_audio*(*Io*)
7. Initialize the variables,
yn = Io, ye = Ie, L=length(yn)
8. Perform iterative operation.
while L >= M **do**
yn = dwt(Io)
ye = dwt(Ie);
L= length(y);
end while
9. Compare yn and ye.

I. Fuzzy entropy of audio signal

1. Read the audio file as Ir
2. **for** i = 1 to *N* **do**:
3. Iq ← Quantize(Ir(*i*))
4. Io(*i*) ← Iqd
5. **end for**
6. Io ← double(I);
7. Generate histogram of the audio sample, R← imhist(I)
8. Normalize the histogram, P=R/max(R) where $0 \le P(i) \le 1$
9. **for** i = 0 to 255
$\mu_1(i), \mu_2(i), \mu_3(i)$ ← Create fuzzy MFs based on Eq. (6) - (8)
10. **end for**
11. Determine the weighted probability of Eq. (3) to (5)
12. P1, P2, P3 ← 0;
13. **for** i = 0 to 255 **do**
P1 ← P1 + P(*i*) × $\mu_1(i)$
P2 ← P2 + P(*i*) × $\mu_2(i)$
P3 ← P3 + P(*i*) × $\mu_3(i)$
14. **end for**
15. Determine fuzzy entropy
16. H1, H2, H3 ← 0
17. **for** i =1 to 256 **do**
18. **if** $\mu_1(i) \neq 0$ and P(*i*) ≠ 0 **then**
19. $H1 \leftarrow H1 - \frac{P(i)\times\mu_1(i)}{P1} log_2 \frac{P(i)\times\mu_1(i)}{P1}$
20. **end if**
21. **if** $\mu_2(i) \neq 0$ and P(*i*) ≠ 0 **then**
22. $H2 \leftarrow H2 - \frac{P(i)\times\mu_2(i)}{P2} log_2 \frac{P(i)\times\mu_2(i)}{P2}$
23. **end if**
24. **if** $\mu_3(i) \neq 0$ and P(*i*) ≠ 0 **then**
25. $H3 \leftarrow H3 - \frac{P(i)\times\mu_3(i)}{P3} log_2 \frac{P(i)\times\mu_3(i)}{P3}$
26. **end if**
27. **end for**
28. H=H1+H2+H3;

Function Quantize(*s*)

1. $I(i) = \frac{Io(i)}{\max(Io)} \times 255$
2. I(*i*) = uint8(I(*i*))
3. **return** I(*i*)

J. Complexity Analysis

In this paper, the application of ECC on a pair of voice sequences includes 'verification of the ordered pair falling on the curve', and 'inclusion of two sparse vectors' makes the proposed algorithm more complex compared to conventional ECC of $O(k^2)$, taking k as the bit-length of the key. During transmission, each sample of $v_1(t)$and $v_2(t)$ is encrypted and decrypted; the complexity will be$O(4Nk^2)$, the comparison of each plain-text and decrypted value will change it to$O(4Nk^2 + 2N)$, and finally, the inclusion of two sparse vectors will make it$O(4Nk^2 + 2N + 2N)$. For the case of space complexity, the inclusion of sparse vectors is the only considerable component. The other two algorithms, RSA and DNA, use the conventional form; hence, their complexity is avoided here, but both of them possess lower complexity compared to the proposed ECC technique.

The next section presents the results obtained from each of the algorithms and compares them.

V. Results and Discussions

First of all, two audio signals, each of 1200 samples, are taken for the experiment as shown in Fig. 2. Next, the comparison of the original and encrypted signals is shown in Fig. 3 in the time domain, where they are completely different, which indicates the secrecy level of ECC. The original and decrypted signals are compared at the receiving end, as shown in Fig. 4, where some discrepancies are observed at a few sampling points.

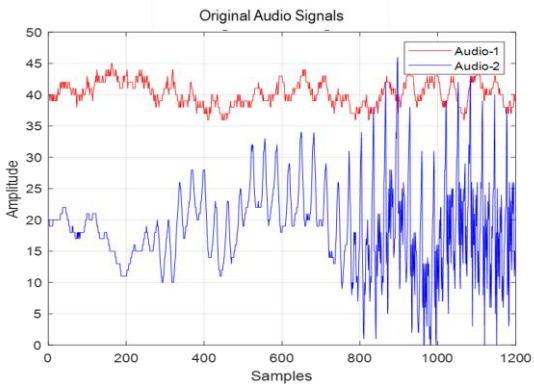


Fig. 2. Two audio signals as the input.

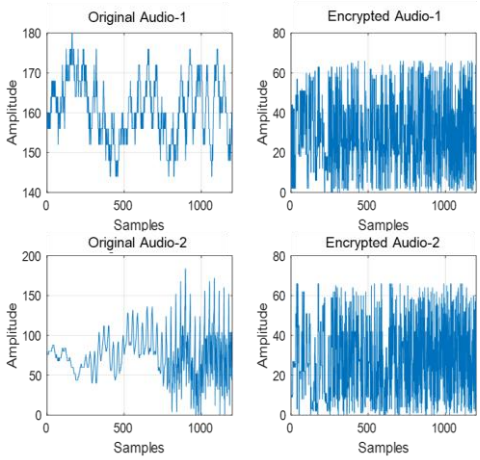


Fig. 3. Comparison of original and encrypted signals.

This happened because some points on the audio signal fell outside of the elliptic curve. These ambiguous points are shown in the discrete plot of Fig. 5 and represent the sparse vector elements.

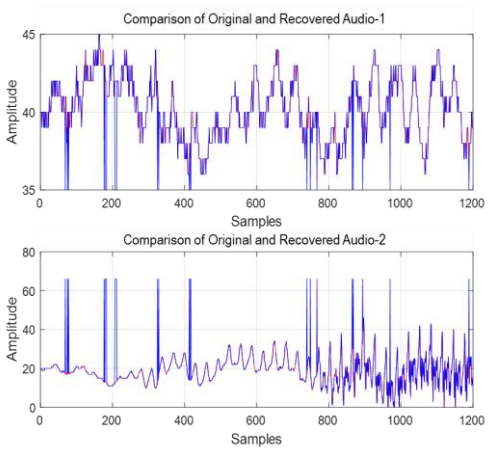


Fig. 4. Original and recovered audio.

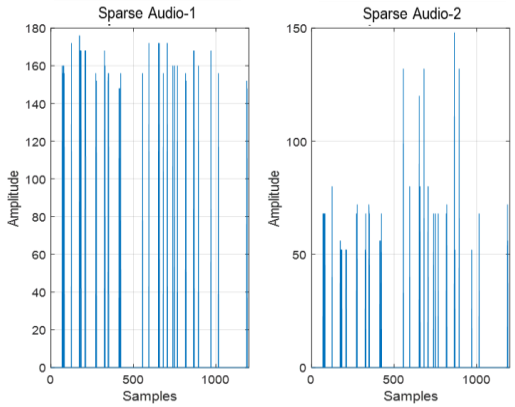


Fig. 5. Sparse samples of audio before the addition of sparse samples.

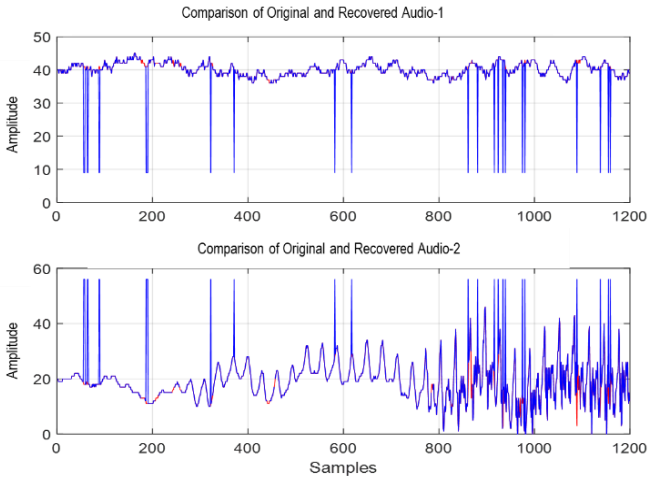
Now, the combination of the decrypted vector and the sparse vector is used based on the proposed algorithm of the paper, and 100% matching between the original and the decrypted is found.

Three statistical parameters (Variance, Entropy, and cross-correlation coefficient) of original, recovered, and encrypted audio signals are compared in Table VI. The tabular data reveal that the recovered signal resembles the original signal, but no similarity is found with the encrypted signal; hence, the rigidity of the encryption algorithm (ECC) is again confirmed by the numerical data.

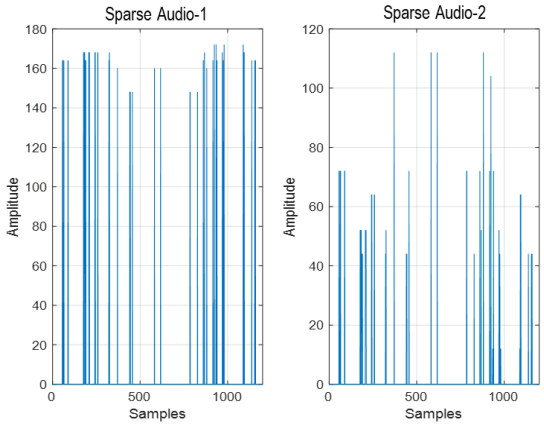
The sparse vector may vary with audio data and also with the chosen parameters of the ECC algorithm. For example, 4.5% of mismatched points are found for the parameters of the encryption algorithm (a = 2, b = 1, and p = 71) against audio-1. The audio-2 gives 4.82% miss-matched points shown in Fig. 6(a)-(b). Similar results are shown for the parameters of the encryption algorithm: a = 1, b = 1, and p = 61 in Fig. 7(a)-(b), which improves the performance of the algorithm in this context.

TABLE VI
COMPARISON OF SIGNAL PARAMETERS (ECC)

Parameters	Audio-1	Parameters	Audio-1	ρ_{xy} (original-1 and encrypted-1)
Variance of Original Audio	3.6025	Entropy of Original	2.9335	
Variance of Recovered Audio	3.6025	Entropy of Recovered	2.9335	0.072
Variance of Encrypted Audio	15.7239	Entropy of Encrypted	0.0933	
Parameters	Audio-2	Parameters	Audio-2	ρ_{xy} (original-2 and encrypted-2)
Variance of Original Audio	44.6589	Entropy of original	4.6966	
Variance of Recovered Audio	44.6589	Entropy of Recovered	4.6966	0.0062
Variance of the encrypted Audio	2.4628	Entropy of Encrypted	0.0933	

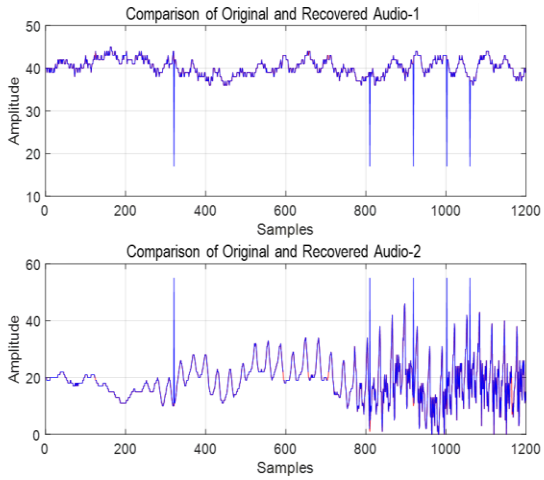


(a) Original and recovered audio before the addition of sparse samples

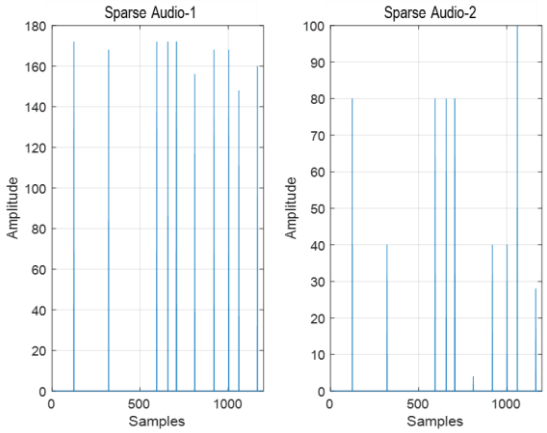


(b) Sparse samples

Fig. 6. Results of audio encryption for $a = 2$, $b = 1$ and $p = 71$.



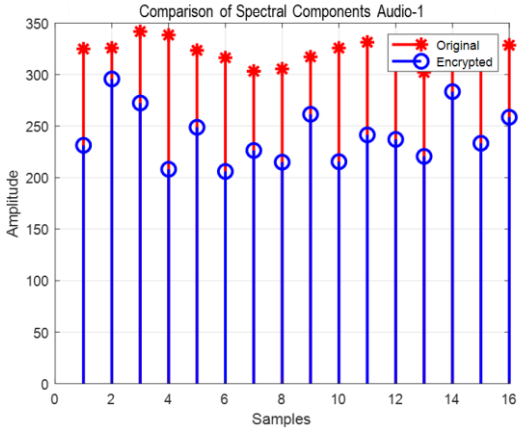
(a) Original and recovered audio before the addition of sparse



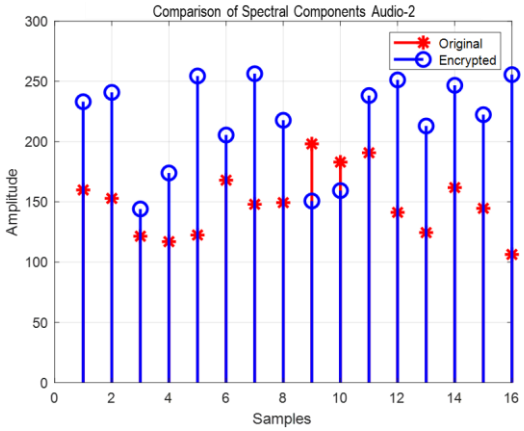
(b) Sparse samples

Fig. 7. Results of audio encryption for $a = 1$, $b = 1$ and $p = 61$.

To verify the wide difference between the original and encrypted signals, the lowest 16 spectral components of the original and encrypted signals are determined using DWT. A comparison of their spectral components for different values of encryption parameters is shown in Figs. 8 to 10 for both audio signals. Again, their wide variation indicates the rigidity of the ECC.

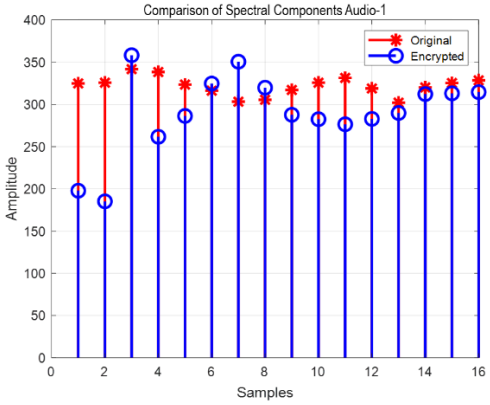


(a) Audio 1

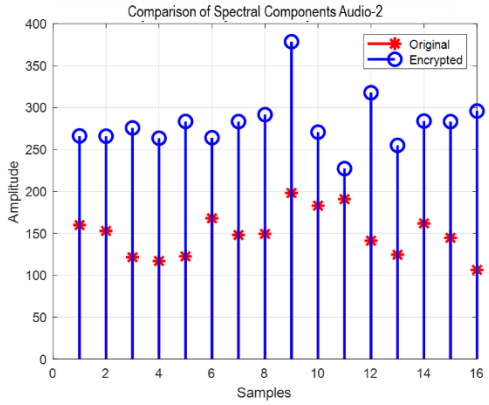


(b) Audio 2

Fig. 8. Comparison of spectral components of the audio signal for $a = 2$, $b = 3$, and $p = 76$.



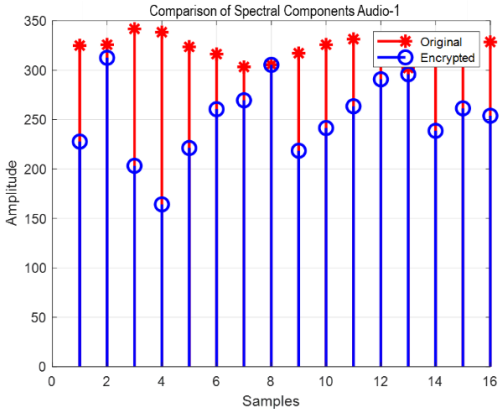
(a) Audio 1



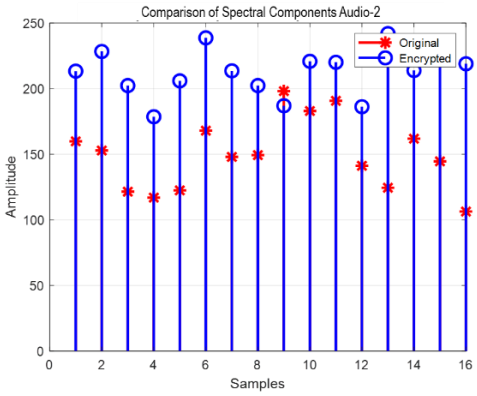
(b) Audio 2

Fig. 9. Comparison of spectral components of audio signal for $a = 2$, $b = 1$, and $p = 71$.

We applied the RSA algorithm to the audio signal, using the following parameters: $e = 3$, $n = 33$, and $d = 7$. A comparison of statistical parameters is shown in Table VII, where the randomness of encrypted data is less prominent compared to ECC.



(a) Audio 1



(b) Audio 2

Fig. 10. Comparison of spectral components of audio signal for $a = 1$, $b = 1$, and $p = 61$.

TABLE VII
COMPARISON OF SIGNAL PARAMETERS (RSA)

Parameters	Audio-1	Parameters	Audio-1	ρ_{xy} (original-1 and encrypted-1)
Variance of Original Audio	26.1542	Entropy of Original	4.2154	
Variance of Recovered Audio	26.1542	Entropy of Recovered	4.2154	0.3228
Variance of Encrypted Audio	70.8612	Entropy of Encrypted	1.2049	
Parameters	Audio-2	Parameters	Audio-2	ρ_{xy} (original-2 and encrypted-2)
Variance of Original Audio	58.4602	Entropy of original	3.3777	
Variance of Recovered Audio	58.4602	Entropy of Recovered	3.3715	0.2588
Variance of Encrypted Audio	105.9864	Entropy of Encrypted	0.3722	

Next, DNA cryptography is applied to the audio samples under MATLAB. The decimal values and corresponding DNA sequences for both plain text and encrypted data, against 20 samples, are shown below.

Input message,
P= [19 19 19 20 20 21 21 21 22 22 22 22 22 23 23 23 24 25 26 27]

Plain text in DNA symbol,
P = 'ACAT' 'ACAT' 'ACAT' 'ACCA' 'ACCA' 'ACCC' 'ACCC' 'ACCC' 'ACCG' 'ACCG' 'ACCG'
'ACCG' 'ACCG' 'ACCT' 'ACCT' 'ACCT' 'ACGA' 'ACGC' 'ACGG' 'ACGT'

The encrypted DNA sequence under the XOR operation,
E = 'AATC' 'AATC' 'AATC' 'AAGG' 'AAGG' 'AAGT' 'AAGT' 'AAGT' 'AAGA' 'AAGA'
'AAGA' 'AAGA' 'AAGA' 'AAGC' 'AAGC' 'AAGC' 'AACG' 'AACT' 'AACA' 'AACC'

The decimal value of the encrypted DNA sequence,
E = 13 13 13 10 10 11 11 11 8 8 8 8 8 9 9 9 6 7 4 5

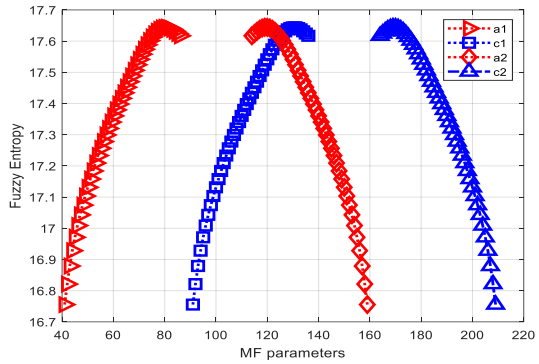
A comparison of statistical parameters is shown in Table VIII, where the randomness of encrypted data is less prominent compared to ECC but more prominent compared to RSA.

TABLE VIII
COMPARISON OF SIGNAL PARAMETERS (DNA)

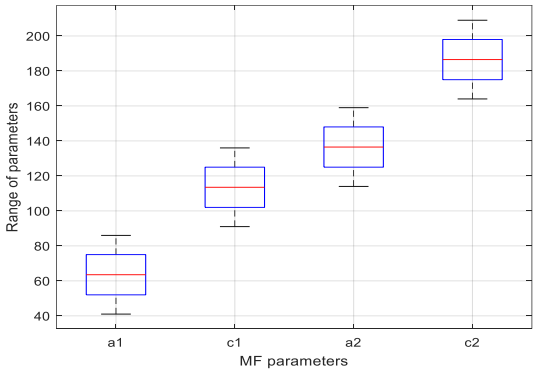
Parameters	Audio-1	Parameters	Audio-1	ρ_{xy} (original-1 and encrypted-1)
Variance of Original Audio	44.6589	Entropy of Original	0.0517	
Variance of Recovered Audio	44.6589	Entropy of Recovered	0.0517	0.0243
Variance of Encrypted Audio	44.6589	Entropy of Encrypted	0.0317	
Parameters	Audio-2	Parameters	Audio-2	ρ_{xy} (original-2 and encrypted-2)
Encrypted	3.6025	Entropy of original	2.9335	
Variance of Recovered Audio	3.6025	Entropy of Recovered	2.9335	0.186
Variance of Encrypted Audio	3.6025	Entropy of Encrypted	1.9335	

Four parameters of MFs, *a1, c1, a2, and c2, are varied*, and the numerical value of fuzzy entropy is evaluated for both original and encrypted audio signals. Here, the other two parameters, b1 and b2, are excluded since they depend on the other four parameters, like $b_1 = (a_1 + c_1)/2$ and $b_2 = (a_2 + c_2)/2$. The variation of fuzzy entropy against a_1, c_1, a_2, and c_2 is shown in Fig. 11 (a), and the box plot of four parameters is shown in Fig. 11(b). The fuzzy entropy attains its maximum value at $a_1 = 78.4$, $c_1 = 130.2$, $a_2 = 120$, and $c_2 = 172.3$. Now the vector, $\mathbf{s} = [a_1\ c_1\ a_2\ c_2]$ corresponding to the maximum value of fuzzy entropy will be used as the feature of the audio signal.

The profile of fuzzy entropy of ECC, RSA, and DNA-encrypted audio is shown in Fig. 12(a)-(c), where the maxima are quite different, even shifted from the original signal. The feature vector corresponding to the maximum value of fuzzy entropy is found to be S_ECC = [52.3, 108.4, 145.75, 192.4], S_RSA = [76.3, 122.2, 128.6, 176.3], and S_DNA = [69.8, 118.2, 130.5, 182.6].

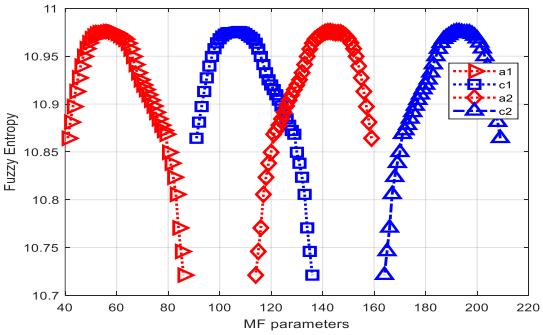


(a) Fuzzy entropy

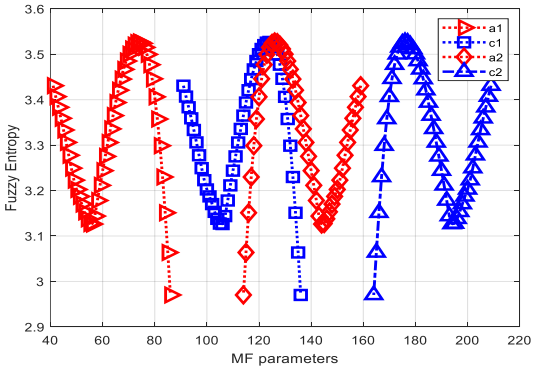


(b) Box plot of four parameters

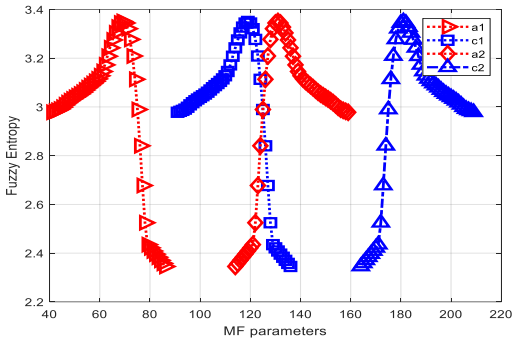
Fig. 11. Fuzzy entropy and box plot of parameters of the original audio signal



(a) ECC



(b) RSA



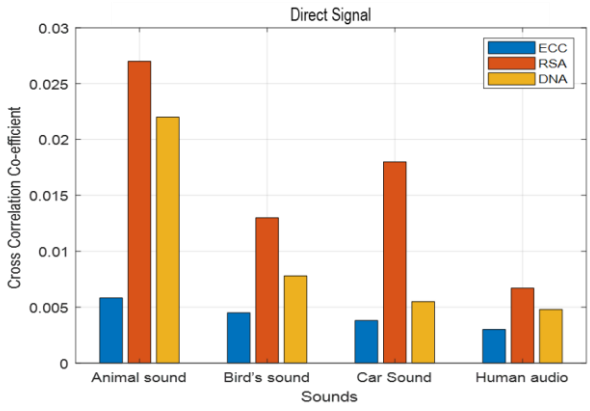
(b) DNA

Fig. 12. The profile of fuzzy entropy of encrypted audio

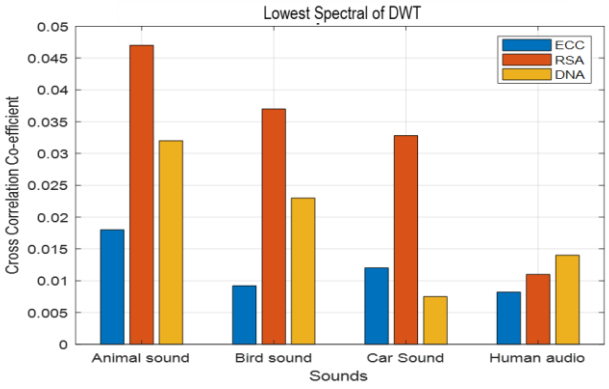
Finally, four types of audio signals in *.wav format are taken, and 15,00,000 samples are considered for encryption and decryption. The encryption time, decryption time, and 'cross-correlation coefficients between original and encrypted signal' are measured for all three algorithms. The experiment was conducted on a machine with the following specifications: Intel(R) Core (TM) i7-1065G7 CPU, 1.50 GHz, 16.0 GB RAM, and MATLAB 2023R was used. The entire results are shown in Table IX. For ECC, the encryption time is highest, but the decryption time is moderate. The decryption time of RSA is found to be the highest, but its encryption time is moderate. For DNA, both encryption and decryption times are the minimum.

TABLE IX
COMPARISON OF THREE ENCRYPTION METHODS

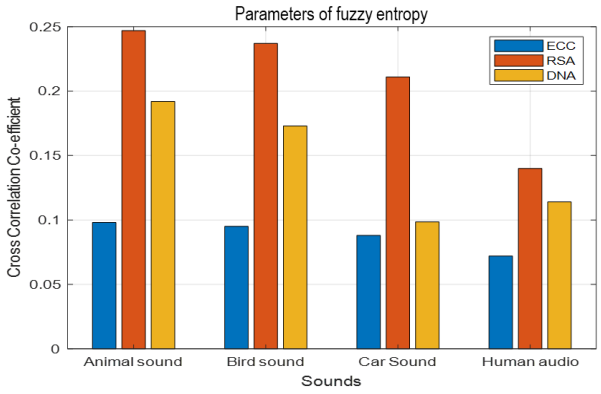
Category of Audio	Algorithm	Encryption Time (s)	Decryption Time (s)
Human audio	ECC	3.84	1.96
	RSA	3.33	2.24
	DNA	3.00	1.67
Car's Sound	ECC	5.78	3.12
	RSA	5.56	3.92
	DNA	5.53	2.18
Bird's sound	ECC	4.16	3.18
	RSA	4.12	3.86
	DNA	3.94	1.98
Animal's sound	ECC	4.36	1.88
	RSA	3.98	2.12
	DNA	3.67	1.57



(a) Original and encrypted signal



(b) Lowest spectral components of DWT



(c) Fuzzy parameters

Fig. 13. Cross-correlation, the ECC is the best of all, although DNA shows a close result, parameters

In the context of security (Cross-correlation coefficient), the ECC is the best of all, although DNA shows a close result, visualized in Fig. 13(a)-(c). Here, the correlation coefficient is taken for four types of audio under three techniques: (i) between original and encrypted audio directly, (ii) between the 16 lowest spectral components of original and encrypted audio, (iii) between fuzzy parameters of original and encrypted audio. For image or audio encryption, ECC provides the best result, but for real-time operation, DNA compromises process time and security level.

Although the proposed ECC-based audio encryption model guarantees complete recovery of the original audio through sparse vectors and offers stronger security than RSA and DNA, it has several limitations. The study assumes a noiseless transmission environment, whereas real-world networks involve noise, jitter, and packet loss that can impair recovery. ECC also introduces higher computational complexity, resulting in longer processing times compared to DNA, which may hinder its real-time use. Furthermore, the experiments were limited to a small set of clean audio signals, which does not accurately reflect the diversity of real-world multimedia data. The model's resilience against advanced attack scenarios, such as side-channel, adaptive chosen-plaintext, or quantum-based attacks, was also not examined. Finally, to enhance security, the proposed model's complexity increases by a factor of 4N compared to conventional ECC, as detailed in Section IV.

VI. Conclusion and Future Work

This study proposes an ECC-based audio encryption scheme with sparse vector correction, compared against RSA and DNA using statistical, spectral, and fuzzy entropy analyses. Results show that ECC provides the strongest security, DNA offers the best real-time efficiency, and RSA offers moderate performance. The work extends ECC to audio communication, introduces fuzzy entropy as a new rigidity metric, and offers guidelines for balancing security and computational cost in IoT and multimedia applications.

From a practical perspective, the proposed method guarantees 100% audio recovery through sparse vector correction, ensuring data integrity, and offers stronger resistance to statistical attacks than RSA and DNA, making ECC preferable where security outweighs latency.

Despite its advantages, the study is limited by testing in a noiseless environment, a higher ECC processing time that may hinder real-time use, a restricted dataset, and the lack of evaluation against advanced cryptanalytic attacks.

Future work should extend the model to noisy transmission environments and evaluate its performance under realistic channel conditions. Lightweight ECC optimizations should be explored to reduce computational overhead and enhance suitability for real-time and IoT applications. The concept can also be applied to image transmission by converting an image of size N×M into a vector of NM×1, although this increases complexity at both the sender's and receiver's end.

References

[1] A. Asaker, Z. F. Elsharkawy, S. Nassar, N. Ayad, O. Zahran, and F. E. Abd El-Samie, "A Novel Iris Cryptosystem Using Elliptic Curve Cryptography," in 9th International Japan-Africa Conference on Electronics, Communications, and Computations (JAC-ECC), pp. 155-158, December 2021, doi:10.1109/JAC-ECC54461.2021.9691307.

[2] M. Koppl, M. Paulovic, M. Orgon, S. Pocarovsky, A. Bohacik, K. Kuchar, and E. Holasova, "Application of Cryptography Based on Elliptic Curves," in 2nd International Conference on Electronics, Communications and Information Technology (CECIT), pp. 268-2722, December 2021, doi:10.1109/CECIT53797.2021.00054.

[3] J. Venkata Giri, and A. Murty, "Elliptical Curve Cryptography Design Principles," in International Conference on Recent Trends on Electronics, Information, Communication & Technology (RTEICT), pp. 889-893, August 2021, doi:10.1109/RTEICT52294.2021.9573662.

[4] K. M. Hosny, M. A. Zaki, N. A. Lashin, M. M. Fouda, and H. M. Hamza, "Multimedia Security Using Encryption: A Survey," in IEEE Access, vol. 11, pp. 63027-63056, June 2023, doi: 10.1109/ACCESS.2023.3287858.

[5] H. N. Almajed, and A. S. Almogre, "SE-Enc: A Secure and Efficient Encoding Scheme Using Elliptic Curve Cryptography," in IEEE Access, vol. 7, pp. 175865-175878, December 2019, doi:10.1109/ACCESS. 2019.2957943.

[6] H. Aziz, S. M. Mustuzhar Gilani, I. Hussain, A. K. Janjua, and S. Khurram, "A Noise-Tolerant Audio Encryption Framework Designed by the Application of S8 Symmetric Group and Chaotic Systems," Mathematical Problems in Engineering, pp.1-15, 2021, https://doi.org/10.1155/2021/5554707.

[7] D. Shah, T. Shah, M. M. Hazzazi, M. I. Haider, A. Aljaedi, and I. Hussain, "An Efficient Audio Encryption Scheme Based on Finite Fields," in IEEE Access, vol. 9, pp. 144385-144394, October 2021, doi:10.3390/math11183824.

[8] Q. Zhang, Y. Li, Y. Hu, and X. Zhao, "An Encrypted Speech Retrieval Method Based on Deep Perceptual Hashing and CNN-BiLSTM," in IEEE Access, vol. 8, pp. 148556-148569, August 2020, doi: 10.1109/ACCESS.2020.3015876.

[9] K. Sasikumar, and Sivakumar Nagarajan, "Comprehensive Review and Analysis of Cryptography Techniques in Cloud Computing," in IEEE Access, pp. 52325-52351, April 2024, doi: 10.1109/ACCESS. 2024.3385449.

[10] G. Singh, and R. Kumar Yadav, "DNA-Based Cryptography Techniques with Applications and Limitations," in International Journal of Engineering and Advanced Technology (IJEAT), vol. 8, pp. 3997-4004, August 2019, doi: 10.35940/ijeat.F9285.088619.

[11] M. A. Alhija, N. Turab, A. Abuthawabeh, H. Abuowida, and J. Al Nabulsi, "DNA Cryptographic Approaches: State of Art, Opportunities, and Cutting Edge Perspectives," in Journal of Theoretical and Applied Information Technology, vol. 100, no. 18, pp. 5346-5358, September 2022, doi: 100(18):5346-5358.

[12] H. Al-Mahdi, M. Alruily, O. R. Shahin, and K. Alkhaldi, "Design and Analysis of DNA Encryption and Decryption Technique based on Asymmetric Cryptography System," in (IJACSA) International Journal of Advanced Computer Science and Applications, vol. 10, no. 2, pp. 499-506, 2019, doi: 10.14569/IJACSA.2019.0100264.

[13] H. Durga Tiwari, and J. Hyung Kim, "Novel Method for DNA-Based Elliptic Curve Cryptography for IoT Devices," in ETRI Journal, vol. 40, no. 3, pp.396-409, June 2018, doi: 10.4218/etrij. 2017-0220.

[14] W. Dutta, S. Mitra, and S. Kalaivani, "Audio encryption and decryption algorithm in image format for secured communication," in 2017 International Conference on Inventive Computing and Informatics (ICICI), pp. 517-521, November 2017, doi: 10.1109/ICICI.2017.8365185.

[15] N. Barua, and Md. A. Kabir, "Encryption and Decryption of Audio by Changing Properties and Noise Reduction," International Journal of Innovative Science and Research Technology, vol. 7, pp. 805-809, September 2022, doi: 10.5281/zenodo. 7143298.

[16] K. Kordov, "A Novel Audio Encryption Algorithm with Permutation-Substitution Architecture," in Electronics 2019, vol. *8*, no. 5, pp.1-15, May 2019, doi:10.3390/electronics8050530.

[17] A. A. Parveen, and P. S. S. Akilashri, "Secured Authentication Using ECC Based Fractal Fuzzy in Cloud," in International Journal of Intelligent Systems and Applications in Engineering, vol.12, no.17, pp. 184–194, Feb 2024.

[18] T. K. Oikonomou, and G. K. Karagiannidis, "Elliptic Curve Modulation (ECM) for Extremely Robust Physical Layer Encryption." in Scientific Reports, vol. 15, pp.1-17, April 2025.

[19] A. E. Adeniyi, R. G. Jimoh, and J. B. Awotunde , "A systematic review on elliptic curve cryptography algorithm for internet of things: Categorization, application areas, and security," in Computers and Electrical Engineering, vol. 118, August 2024, doi: 10.1016/j.compeleceng.2024.109330.

[20] X. Wang, and Y. Su, "An Audio Encryption Algorithm Based on DNA Coding and Chaotic System," in IEEE Access, vol. 8, pp. 9260-9270, 2020, doi: 10.1109/ACCESS.2019.2963329.

[21] J. Bao, "Research on the Security of Elliptic Curve Cryptography," in Proceedings of the 2022 7th International Conference on Social Sciences and Economic Development, Advances in Economics, Business and Management Research, vol. 215, pp.984-988,2022, doi: 10.2991/aebmr.k.220405.164.

[22] H. Ur Rehman, M. Mazyad Hazzazi, T. Shah, Z. Bassfar, and D. Shah, "An Efficient Audio Encryption Scheme Based on Elliptic Curve over Finite Fields," in Mathematics, vol. 11, pp.1-18, September 2023, doi:10.3390/math11183824.

[23] M. M. Elamir, M. S. Mabrouk, and S. Y. Marzouk, "Secure framework for IoT technology based on RSA and DNA cryptography," in Egyptian Journal of Medical Human Genetics, vol. 23, pp.1-17, December 2022, doi:10.1186/s43042-022-00326-5.

[24] S. Hamsanandhini, P. Balusubramanie, and A. B. Abinaya, "Securing Data in the Image Using SHA & ECC," in 2023 2nd International Conference on Edge Computing and Applications (ICECAA), pp. 268-274, July 2023, India, doi:10.1109/ICECAA58104.2023.10212191.

[25] P. More, S. Sakhare, and P. Sawane, "Implementation and Analysis of ECC (Elliptic Curve Cryptography) Security Routing Protocol in NS2," in 2023 3rd Asian Conference on Innovation in Technology (ASIANCON), pp. 1-5, August 2023, doi: 10.1109/ASIANCON58793.2023.10270716.

[26] V. Yadav, and M. Kumar, "A Hybrid Cryptography Approach Using Symmetric, Asymmetric and DNA Based Encryption," in 2023 3rd International Conference on Intelligent Communication and Computational Techniques (ICCT), pp. 1-5, January 2023, doi:10.1109/ICCT56969.2023.10076124.

[27] T. Mahjabin, A. Olteanu, Y. Xiao, W. Han, T. Li, and W. Sun, "A Survey on DNA-Based Cryptography and Steganography," in IEEE Access, vol.11, pp. 116423-116451, October 2023, doi: 10.1109/ACCESS. 2023.3324875.

[28] E. Jintcharadze, and M. Abashidze, "Performance and Comparative Analysis of Elliptic Curve Cryptography and RSA," in 2023 IEEE East-West Design & Test Symposium (EWDTS), pp.1-4, September 2023, doi: 10.1109/EWDTS59469.2023.10297088.
[29] P. Gurunathan, and R. S. Devi, "RSA Cryptography and GZIP Steganography Techniques for Information Hiding and Security using Java," in 2023 7th International Conference on Trends in Electronics and Informatics (ICOEI), pp. 654-659, April 2023, doi:10.1109/ICOEI56765.2023.10125906.
[30] M. Versaci, F. C. and Morabito, "Image Edge Detection: A New Approach Based on Fuzzy Entropy and Fuzzy Divergence," in International Journal of Fuzzy Systems, vol. 23, pp. 918–936, February 2021, doi: 10.1007/s40815-020-01030-5.
[31] M. S. R. Naidu, P. R. Kumar, and K. Chiranjeevi, "Shannon and Fuzzy entropy based evolutionary image thresholding for image segmentation," in Alexandria Engineering Journal, vol. 57, pp. 1643-1655, September 2018, doi: 10.1016/j.aej.2017.05.024.
[32] Y. Xiao, W. Yu, and J. Tian, "Image segmentation based on fuzzy entropy and Bee Colony Algorithm," in 2010 Sixth International Conference on Natural Computation, vol. 1, pp. 340-343, August 2010.
[33] F. Li, C. Wang, X. Zhang, F. Hu, W. Jia, and Y. Fan, "Features of Hierarchical Fuzzy Entropy of Stroke Based on EEG Signal and Its Application in Stroke Classification," in 2019 IEEE Fifth International Conference on Big Data Computing Service and Applications (BigDataService), pp. 284-289, April 2019, doi: 10.1109/BigDataService.2019.00050.

Md. Imdadul Islam has completed his B.Sc. and M.Sc Engineering in Electrical and Electronic Engineering from Bangladesh University of Engineering and Technology, Dhaka, Bangladesh in 1993 and 1998 respectively and has completed his Ph.D degree from the Department of Computer Science and Engineering, Jahangirnagar University, Dhaka, Bangladesh in the field of network traffic in 2010. He is now working as a Professor at the Department of Computer Science and Engineering, Jahangirnagar University, Savar, Dhaka, Bangladesh. Previously, he worked as an Assistant Engineer in Sheba Telecom (Pvt.) LTD (A joint venture company between Bangladesh and Malaysia, for Mobile cellular and WLL), from Sept.1994 to July 1996. Dr Islam has a very good field experience in installation and design of mobile cellular network, Radio Base Stations and Switching Centers for both mobile and WLL. His research field is network traffic, wireless communications, wavelet transform, adaptive filter theory, ANFIS, neural network, deep learning and machine learning. He has more than two hundred research papers in national and international journals and conference proceedings.

Samsun Nahar Khandakar received her B.Sc. (Honors) and M.Sc. in Computer Science and Engineering from Jahangirnagar University, Dhaka, Bangladesh in 2017 and 2018 respectively. Previously, she worked as a lecturer in the Department of Computer Science and Engineering, University of Information Technology and Science, Dhaka, Bangladesh. Currently, she is working as a Lecturer in the Department of Computer Science and Engineering, Jahanginagar University, Savar, Dhaka-1342, Bangladesh. Her research interest is focused on Artificial Intelligence, Machine Learning, Deep Learning and IoT and Network Security.

Nadia Afrin Ritu received her B.Sc. (Honors) and M.Sc. in Computer Science and Engineering from Jahangirnagar University, Dhaka, Bangladesh in 2016 and 2017 respectively. Previously, she worked as a lecturer in the Department of Computer Science and Engineering, Daffodil International University, Dhaka, Bangladesh. Previously, she also worked as a lecturer in the Department of Computer Science and Engineering, Bangladesh University of Business and Technology (BUBT), Dhaka, Bangladesh. Currently, she is working as a lecturer in the Department of Computer Science and Engineering, Jahanginagar University, Savar, Dhaka-1342, Bangladesh. Her research interest is focused on Artificial Intelligence, Machine Learning and Expert System, and Data Mining.

Mr. Masum Bhuiyan is a Lecturer in the Department of Computer Science and Engineering at Jahangirnagar University, teaching and researching AI/ML-based real-world applications. With a distinguished background as a former Software Engineer at Samsung R&D Institute, where he contributed to the development of the Samsung Galaxy Watch and worked on a patent-pending technology graded A1(Highest Grade). Recognized for his outstanding contributions, he earned the Icon Award 2022. Academically, he has excelled with both M.Sc and B.Sc degrees in Computer Science and Engineering from Jahangirnagar University, graduating at the top of his class. As an innovator and leader, he founded Open AIR, a research community dedicated to fostering innovation. His top achievements include being the 2nd Runner-up in the National AI for Bangla 2.0 competition and securing a Special Innovation Fund grant from the ICT Ministry.

Sarwar Jahan is serving as an Associate Professor in the Department of Computer Science and Engineering at East West University, Dhaka, Bangladesh. He received his B.Sc. degree in Electrical and Electronics Engineering from Ahsanullah University of Science and Technology, Dhaka, Bangladesh, and M.S. degrees in Telecommunication Engineering from the University of Technology, Sydney, Australia in 2001, and 2005 respectively. He has completed his Ph.D. degree from the Department of Computer Science and Engineering, Jahangirnagar University, Dhaka, Bangladesh in the field of wireless communications in 2022. He is currently doing his research in Communication Engineering, Network Traffic, and different disease detection using artificial intelligence and machine learning algorithm.