Chapter 3

Audio Encryption using DNA state machine

This chapter will discuss the suggested encryption and decryption procedures as shown in Figure 3.3 and 3.4, as well as the performance assessment of the algorithm.

3.1 Encryption Algorithm

The following steps outline a pioneering approach that integrates DNA computing with audio encryption. This innovative process involves the transformation of audio data into DNA sequences, encryption using DNA-based operations, S-Box transformation, and subsequent decryption to reconstruct the original audio file:

1. Audio Data Processing: load an audio file and extract its audio data and dimensions.
2. Serialization of Audio Data: serialize the audio data into a binary format for further processing.
3. Conversion to DNA Bits: the binary audio data is converted into DNA bits as depicted in Figure 2.11. Additionally, a DNA key is generated using the Mersenne Twister algorithm.
4. DNA Encryption using the proposed Moore's Automata as illustrated in Figure 3.2: the data DNA bits are encrypted using the generated DNA key and a specified operations table, as shown in Figure 3.1.
5. S-Box Transformation: an S-Box transformation is applied to the output DNA sequence from the Moore Automata, further enhancing the security of the encrypted audio data.

	A	C	G	T
A	XNOR	XNOR	XOR	XOR
C	XOR	SUB	ADD	SUB
G	SUB	ADD	ADD	ADD
T	ADD	XOR	XOR	SUB

Figure 3.1: The proposed encryption and decryption DNA Operations used in Moore's automata

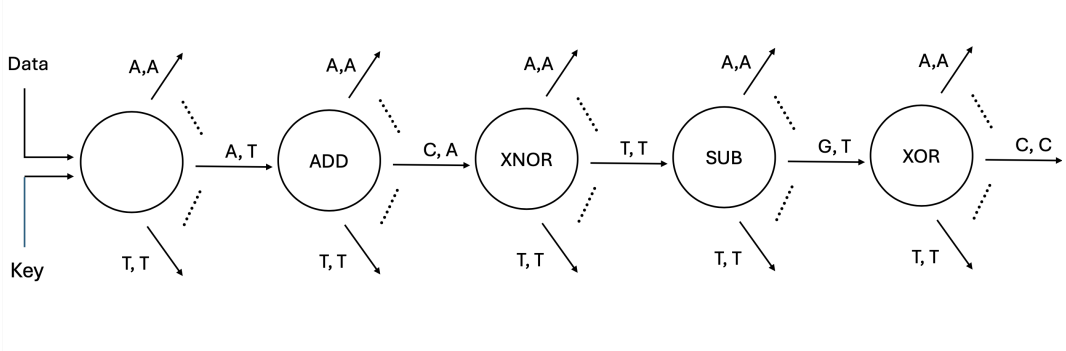

Figure 3.2: The proposed Moore's automata for encryption and decryption

3.2 Decryption Algorithm

In order to retrieve the original audio back again, the following steps are to be followed:

1. Generation of S-Box Inverse: generate the inverse S-Box for decryption.
2. Decryption of Encrypted Bits using the proposed Moore's Automata as illustrated in the same Figure 3.2: the data DNA bits are decrypted using the same generated DNA key and the specified operations table, as shown in Figure 3.1.
3. Conversion of Decrypted Bits to Audio Data: the decrypted DNA bits are converted back to binary format as depicted in Figure 2.11 and deserialized to obtain the decrypted audio data.
4. Reconstruction of Decrypted Audio: reshaping the decrypted audio data to reconstruct the original audio file, thereby completing the decryption process.

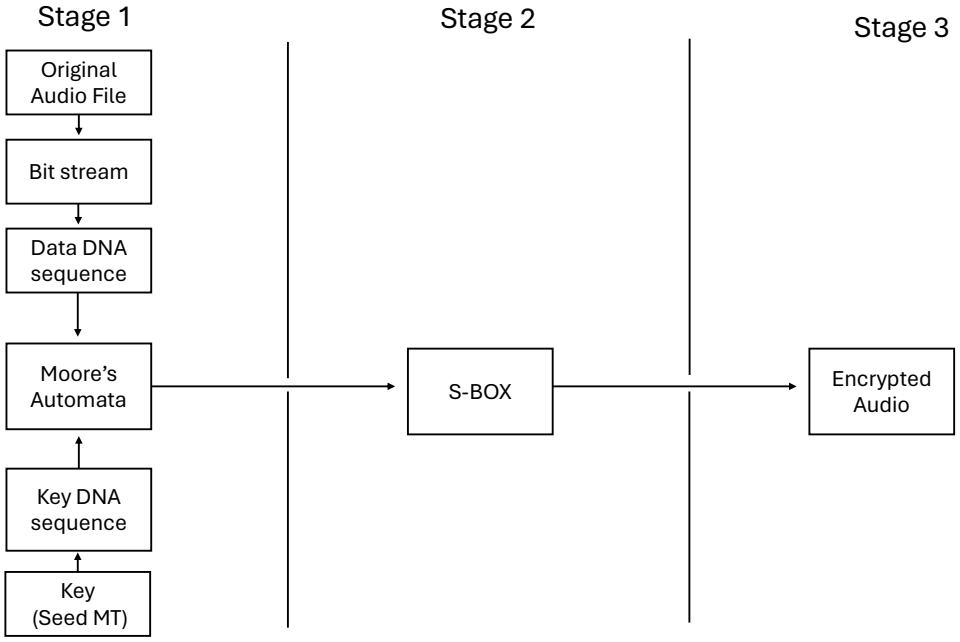

Figure 3.3: Encryption Process

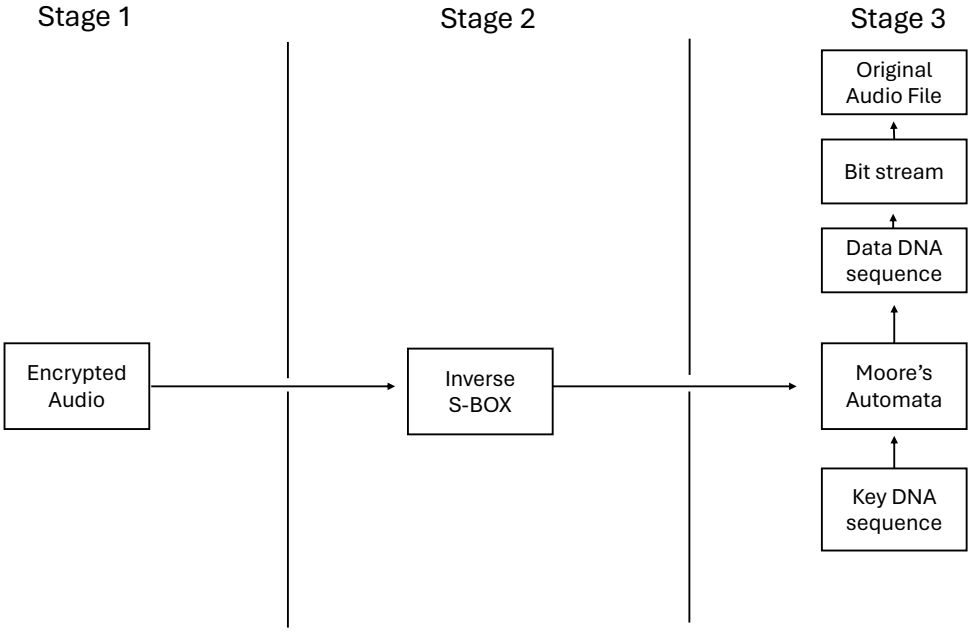

Figure 3.4: Decryption Process

Chapter 4

Performance Evaluation

This chapter discusses the performance evaluation of the proposed algorithm, meticulously examining their operational intricacies across three distinct audio files: Bee, Dogbark, and War plan. The subsequent unveiling of performance evaluation metrics offers nuanced insights into the algorithms' efficacy in handling varied audio content. Notably, the high Mean Square Error (MSE) values in Table (4.1) for the three audio files (16224.2, 16237.7, 16156.9) not only underscore the algorithm's ability to eliminate audio similarity but also affirm its robustness in preserving the distinct characteristics of each audio sample. Conversely, the low Peak Signal-to-Noise Ratio (PSNR) values depicted in Table (4.2) for the respective audio files (6.02921, 6.02555, 6.04721) serve as compelling evidence of the algorithm's resilience and its capacity to maintain fidelity across diverse sound profiles. Furthermore, the encrypted entropy values of (0.0684082, 0.0556345, 0.0546831) and decrypted entropy values of (3.27179, 2.22026, 2.45144) presented in Table (4.3) and Table (4.4) respectively, serve as significant indicators of the level of randomness and unpredictability in the encrypted data, crucial attributes in ensuring the security of sensitive audio information. The algorithm's adeptness in thwarting differential attacks is conspicuously demonstrated by the Number of Pixel Change Rate (NPCR) values (99.9688, 99.7808, 99.9259) in Table (4.6) and the Unified Average Changing Intensity (UACI) values (49.632, 49.6314, 49.6249) in Table (4.5) across the three audio files. These comprehensive metrics collectively underscore the algorithm's prowess in securing audio data and highlight its efficiency in processing encrypted audio files, thereby showcasing its adaptability and reliability across diverse audio content. The thorough evaluation across multiple audio samples reaffirms the algorithm's capacity to consistently deliver robust and secure encryption for various real-world audio scenarios, thus positioning it as a dependable solution for audio data security and privacy preservation.

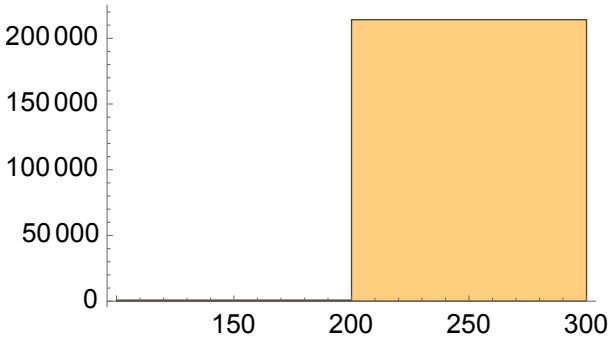

Figure 4.1: Encrypted Histogram of bee audio

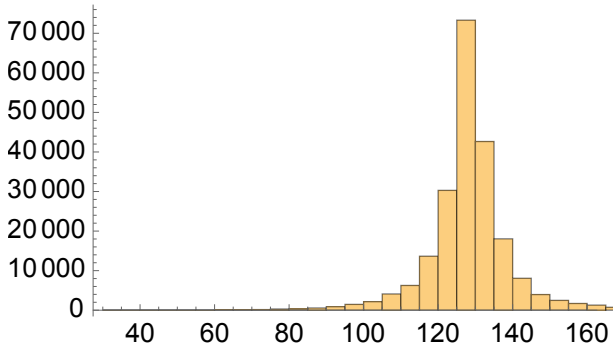

Figure 4.2: Decrypted Histogram of bee audio

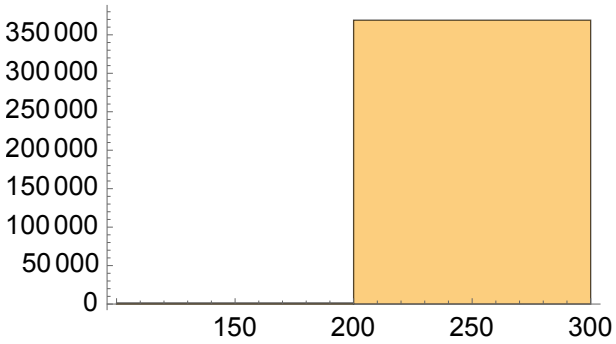

Figure 4.3: Encrypted Histogram of dog bark audio

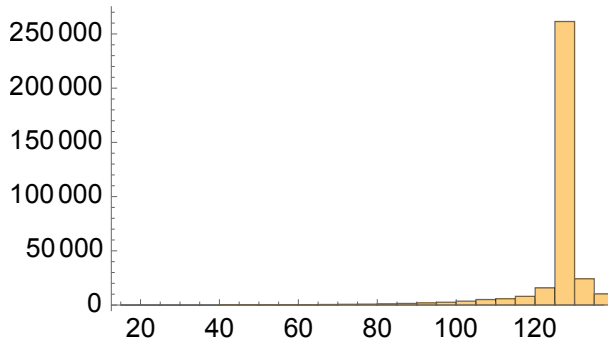

Figure 4.4: Decrypted Histogram of dog bark audio

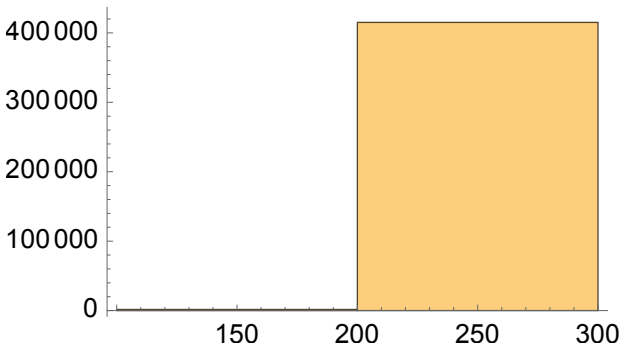

Figure 4.5: Encrypted Histogram of war plan audio

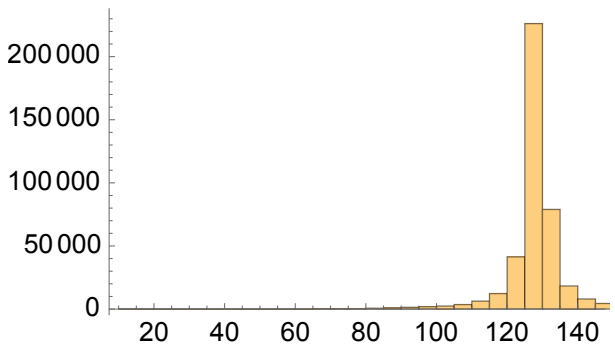

Figure 4.6: Decrypted Histogram of war plan audio

Audio	Proposed
Bee	16224.2
Dog bark	16237.7
War plan	16156.9

Table 4.1: MSE comparisons of different audios

Audio	Proposed
Bee	6.02921
Dog bark	6.02555
War plan	6.04721

Table 4.2: PSNR comparisons of different audios

Audio	Proposed
Bee	0.0684082
Dog bark	0.0556345
War plan	0.0546831

Table 4.3: Encrypted Entropy

Audio	Proposed
Bee	3.27179
Dog bark	2.22026
War plan	2.45144

Table 4.4: Decrypted Entropy

Audio	Proposed
Bee	49.632
Dog bark	49.6314
War plan	49.6249

Table 4.5: UACI comparisons of different audios

Audio	Proposed
Bee	99.9688
Dog bark	99.7808
War plan	99.9259

Table 4.6: NPCR comparisons of different audios