

See discussions, stats, and author profiles for this publication at: <https://www.researchgate.net/publication/385018596>

Memristive Coupled Neural Network Based Audio Signal Encryption

Conference Paper · September 2024

DOI: 10.23919/SPA61993.2024.10715600

CITATIONS

0

READS

56

8 authors, including:



Farah Wahba

The German University in Cairo

3 PUBLICATIONS 0 CITATIONS

[SEE PROFILE](#)



Mohamed Gabr

The German University in Cairo

37 PUBLICATIONS 552 CITATIONS

[SEE PROFILE](#)



Eyad Mamdouh

The German University in Cairo

13 PUBLICATIONS 131 CITATIONS

[SEE PROFILE](#)



Amr Aboshousha



The German University in Cairo

16 PUBLICATIONS 631 CITATIONS

[SEE PROFILE](#)


Memristive Coupled Neural Network Based Audio Signal Encryption

Farah Hamed 
Mohamed Gabr 
Faculty of MET
German University in Cairo
Cairo, Egypt
farah.wahba@student.guc.edu.eg
mohamed.gabr@ieee.org

Eyad Mamdouh 
Amr Aboshousha 
Physics Department
German University in Cairo
Cairo, Egypt
eyad.gaber@ieee.org
amr.aboshousha@guc.edu.eg

Wassim Alexan 
Dina El-Damak 
Faculty of IET
German University in Cairo
Cairo, Egypt
wassim.alexan@ieee.org
dina.eldamak@guc.edu.eg

Abdallah Fathy 
Department of Electronic Engineering Technology
Faculty of Engineering Technology
ElSewedy University of Technology - Polytechnic of Egypt
Cairo, Egypt
abdallah.fathy@sut.edu.eg

Marvy Badr Monir Mansour 
Department of Electrical Engineering
Faculty of Engineering
The British University in Egypt
Cairo, Egypt
marvy.badr@bue.edu.eg

Abstract—This paper proposes a multi-layer audio encryption scheme based on the Memristive Coupled Neural Network (MCNN), S-box, and the Fibonacci Q-matrix. Initially, a pseudo-random key is generated using the MCNN system and XORed with the original audio data. Subsequently, an S-box, created using the OpenSSL Pseudo-random Number Generator (PRNG), is applied to the cipher. Finally, the Fibonacci Q-matrix is used to produce the final encrypted audio. The proposed scheme was evaluated using various metrics, including Peak Signal-to-Noise Ratio (PSNR), Number of Sample Change Rate (NSCR), correlation coefficient, and information entropy. The results demonstrate excellent performance and robust resistance to multiple types of attacks. Additionally, the scheme features a vast key space of 2^{2126} , showcasing significant resistivity to brute-force attacks.

Keywords—Audio signal encryption, chaos theory, neural network.

I. INTRODUCTION

In today's world, where digital communication is pervasive and securing data is crucial, the encryption of audio signals has become an essential field of study [1]. With the rapid advancement of internet technologies, audio data, including voice messages, multimedia content, and sensitive audio recordings, are frequently transmitted over potentially insecure channels [2]. This increases the vulnerability of such data to unauthorized access and malicious attacks. The importance of developing robust encryption algorithms for audio signals cannot be overstated, as they ensure the confidentiality, integrity, and authenticity of information [3]. The timeliness of this topic is underscored by the escalating occurrences of cyber threats and the growing regulatory emphasis on data privacy. Consequently, novel approaches to audio signal encryption are essential to meet the current and future security demands in diverse applications, ranging from personal communications to corporate and governmental operations.

Recent works in this domain include [1], [3]–[7]. In [1], an enhanced improved audio encryption approach is proposed that uses hash of input audio file and two

pseudorandom-based numbers as three secret keys respectively. The authors in [3] provided an audio encryption scheme that utilizes Pseudo-random Number Generator (PRNG) and permutation and substitution processes. In [4], an algorithm that uses a distinct key for each block is presented, where each key is generated using chaotic values of piece-wise linear chaotic map (PWLCM). Another technique for audio encryption that consists of substitution and permutation via adopting chaotic logistic map and 3D-matrix is demonstrated in [5]. In 2023, Demirtaş [6] employs three secret keys that are obtained from raw audio data. Also, scrambling and diffusion of input audio are performed through utilizing chaotic Chebyshev map. Also, Rahul et al. in [7], use hash values of plain audio signals and user's biometric image to generate keys for audio encryption and decryption.

The contributions of this research work are as follows. A secure and efficient audio signal encryption algorithm is proposed. The most important aspect of its security relates to its vast key space of 2^{2126} , thanks to the employment of the MCNN hyperchaotic system of differential equations. This research work is organized as follows. Section II introduces some preliminary mathematical constructs that are employed in the proposed algorithm. Section III describes the proposed audio signal encryption algorithm. Section IV validates the security of the proposed algorithm by showcasing a number of performance evaluation metrics, as well as how they compare to those achieved by counterpart algorithms from the literature. Finally, Section V provides some concluding remarks and possible future research directions.

II. PRELIMINARY MATHEMATICAL CONSTRUCTS

A. Memristive Coupled Neural Network

Lin et al. [8] developed the Memristive Coupled Neural Network Model (MCNNM) by integrating sub-neural

networks constructed using the Hopfield Neural Network (HNN) and a memristive model based on the flux-controlled memristor. The Hopfield neural network, which exhibits brain-like chaotic behavior, is employed to simulate the chaotic dynamics of the brain's nervous system. The mathematical representation of this model is as follows:

$$C_i \dot{v}_i = -\frac{v_i}{R_i} + \sum w_{ij} \tanh(v_j) + I_i \quad (i, j \in N^*), \quad (1)$$

where C_i , R_i and v_i represent the capacitance, resistance, and potential of the cell membrane in neuron i , respectively; w_{ij} are the synaptic weight coefficients that describe the connection strength from neuron j to neuron i ; the hyperbolic tangent function serves as the neuron stimulation function, and I_i denotes an external input current. It is important to note that the chaotic dynamics of the HNN depend on w_{ij} . Consequently, two distinct sub-neural networks with four neurons each can be constructed based on the HNN model in (1) by selecting appropriate synaptic weight coefficients through a trial and error method.

Figure 1 illustrates the connection of the two sub-neural networks using a memristor, where X_i and Y_i represent eight neurons in total. Therefore, assuming $C_i = 1$, $R_i = 1$, and $I_i = 0$ for $i \in \{1, 2, 3, 4\}$, the MCNNM can be expressed as in (2):

$$\begin{cases} \dot{x}_1 = -x_1 + 1.8 \tanh(x_1) + 2 \tanh(x_2) - 0.5 \tanh(x_3) \\ \quad - 12 \tanh(x_4) + p\phi(x_1 - y_1), \\ \dot{x}_2 = -x_2 + \tanh(x_2) + 20 \tanh(x_3) - 0.5 \tanh(x_4), \\ \dot{x}_3 = -x_3 + 0.5 \tanh(x_1) - 4 \tanh(x_2) + 1.8 \tanh(x_3) \\ \quad + 4 \tanh(x_4), \\ \dot{x}_4 = -x_4 + 0.82 \tanh(x_1) - 0.5 \tanh(x_3) + 2 \tanh(x_4), \\ \dot{y}_1 = -y_1 + \tanh(y_1) + 0.5 \tanh(y_2) - 3.5 \tanh(y_3) \\ \quad - \tanh(y_4) - p\phi(x_1 - y_1), \\ \dot{y}_2 = -y_2 + 2.8 \tanh(y_2) + 3 \tanh(y_3) + 0.5 \tanh(y_4), \\ \dot{y}_3 = -y_3 + 3 \tanh(y_1) - 3 \tanh(y_2) + \tanh(y_3) \\ \quad - 0.7 \tanh(y_4), \\ \dot{y}_4 = -y_4 + 0.5 \tanh(y_2) + \tanh(y_3) + \tanh(y_4), \\ \dot{\phi} = \sin(\pi\phi) + (x_1 - y_1). \end{cases} \quad (2)$$

where x_i and y_i represent the membrane potential of neurons X_i and Y_i , respectively; ϕ is the internal state flux variable; $p\phi(x_1 - y_1)$ is the additional nonlinear term that denotes the induction current between adjacent neurons X_1 and Y_1 with different membrane potentials; p is the coupling strength of the memristive magnetic induction effect, and denotes an extra magnetic flux produced by the membrane potential fluctuation.

The robustness of the MCNNM system in (2) is examined using various chaotic analyses, including coupling strength-related dynamic behaviors, initial state-related dynamic behaviors, and initial-boosted coexisting hyperchaotic attractors as discussed in [8].

In this work, and in a similar manner to [9], the system in (2) is numerically solved using Wolfram Mathematica®, then the median value of its solution set is computed.

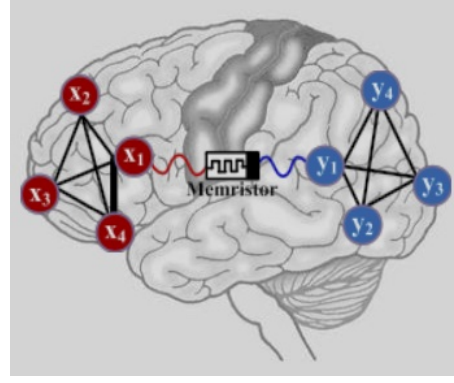


Fig. 1: The joining of 2 sub-neural networks in a memristor [8].

Finally, this median is treated as a threshold, whereby every solution point is compared against, such that if a solution point has a higher value than the threshold, then it is converted into a 1, otherwise, it is converted into a 0. This results in a bit-stream of the same length as that of the solution.

B. OpenSSL S-Box

OpenSSL is a robust and widely used open-source toolkit that provides cryptographic functions and protocols essential for securing communications over computer networks [10]. One of its key features is the implementation of a PRNG, which is crucial for cryptographic applications such as key generation, encryption, and digital signatures [11]. OpenSSL's PRNG is well-suited for these purposes due to its strong entropy sources and rigorous algorithms that ensure high-quality randomness. By continually gathering environmental noise from various system activities to seed the generator, OpenSSL achieves a high level of unpredictability and security [12]. This allows it to be a reliable and trusted selection for developers and security professionals seeking to implement robust cryptographic solutions. In this research work, the algorithm proposed in [13] is adopted in conjunction with an OpenSSL PRNG to construct the S-box shown in Table I.

C. Fibonacci Q-Matrix

The Fibonacci infinite sequence, starts with a 0, then a 1 that is followed by another 1, and then each subsequent element is the sum of the two preceding elements. The sequence $(F_n)_{n=1}^{\infty}$ can be formally described as in [14]:

$$F_n = \begin{cases} 0, & \text{for } n = 0. \\ 1, & \text{for } 1 \leq n \leq 2. \\ F_{n-1} + F_{n-2}, & \text{for } n \geq 3. \end{cases} \quad (3)$$

The Fibonacci Q-matrix is defined in [15] by:

$$Q \equiv \begin{bmatrix} F_2 & F_1 \\ F_1 & F_0 \end{bmatrix} = \begin{bmatrix} 1 & 1 \\ 1 & 0 \end{bmatrix}, \quad (4)$$

whereas the Fibonacci Q-matrix raised to the n^{th} power is defined by:

$$Q^n = \begin{bmatrix} F_{n+1} & F_n \\ F_n & F_{n-1} \end{bmatrix}. \quad (5)$$

TABLE I: Constructed S-box based on OpenSSL.

73	202	161	243	4	252	40	165	168	36	74	253	169	21	238	34
8	29	232	66	111	102	210	71	195	247	32	164	82	58	196	151
62	59	166	112	244	49	193	241	240	200	39	91	228	48	47	137
220	204	50	146	178	245	30	100	117	221	35	107	206	194	149	182
16	52	88	122	205	109	224	67	68	186	158	172	80	86	0	144
118	65	72	199	94	108	251	9	150	99	45	27	159	104	185	249
246	63	17	188	212	95	218	56	152	96	209	44	132	89	76	11
175	113	174	57	128	234	26	79	61	190	2	98	142	207	69	14
123	37	53	18	87	31	124	147	231	84	19	83	145	133	85	106
120	198	46	239	177	155	230	235	43	201	20	78	28	135	163	23
3	125	127	121	139	116	254	171	13	77	7	140	176	170	250	119
208	131	25	225	115	153	75	101	219	237	217	216	10	187	215	189
92	55	38	191	248	143	192	227	197	41	97	70	54	141	12	24
5	33	236	81	22	154	51	130	233	64	60	203	103	15	148	90
181	157	6	138	129	134	126	229	114	242	184	160	42	226	183	222
105	1	110	213	180	223	93	136	179	255	156	167	211	162	214	173

From this matrix, F_n can be extracted directly from the top right element. This method leverages the properties of matrix multiplication to compute Fibonacci numbers in logarithmic time $O(\log n)$, making it much more efficient than the naive recursive approach.

Finally, the inverse of the Fibonacci Q-matrix is defined in [16] by:

$$Q^{-n} = (-1)^n \begin{bmatrix} F_{n-1} & -F_n \\ -F_n & F_{n+1} \end{bmatrix}. \quad (6)$$

The Fibonacci Q-matrix is useful in cryptography applications due to its ability to efficiently compute large Fibonacci numbers, which can be utilized to generate pseudo-random sequences. These sequences are valuable for creating cryptographic keys (either as lengthy bit-streams or matrices) and ones that are difficult to predict or replicate, enhancing security [17].

III. PROPOSED ALGORITHM

This section describes the steps of the proposed audio signal encryption algorithm. Let A_0 denote the plain audio signal, while A_n denotes the encrypted audio signal after layer n of the encryption algorithm for $n > 0$.

- 1) **Obtaining audio sample:** Obtain a 2-channel sample audio and represent its samples as 32-bit real numbers.
- 2) **Serialization:** Processing the audio samples in the real format may lead to loss of data, to avoid that and to ease the upcoming process, we serialize the audio samples.
- 3) **Determining key length:** The first layer of the encryption scheme is XORing the serialized audio data with the key generated from the memristive system, to do that, the key length needs to be equal to the audio length. If the length of the data is 5000 bits or less, we generate a key of the same length as the data right away and jump to step 5; however, if the length of the data is upwards of 5000 bits, we generate a key of 5000 bits and then expand it in step 4.
- 4) **Key expansion:** The prime rotation expansion algorithm introduced in [18] was used in this step to expand the key generated by the memristive system to match the length of the audio to be encrypted.

- 5) **XOR:** Apply the XOR operation between the serialized audio from step 2 with the generated key from step 3 or 4 as such:

$$A_1 = A_0 \oplus \text{key}. \quad (7)$$

- 6) **Substitution box:** For the second layer of encryption, we apply the S-box found in Table I, generated using the method outlined in subsection II-B to obtain A_2 .
- 7) **Prepare for Fibonacci Q-matrix:** To apply the Fibonacci Q-matrix we need the data to be of a length that is divisible by 4 so that it can be partitioned into 2×2 matrices. To achieve that, we check the length of the audio at this step and pad it with 1, 2, or 3 extra zeros at the end as needed, these extra values are later dropped.
- 8) **Partition audio:** Partition the audio sample into 2D arrays that resemble 2×2 matrices.
- 9) **Apply Fibonacci Q-matrix:** As the final layer of encryption, we apply the Fibonacci Q-matrix by obtaining the dot product of the partitioned audio with the Q-matrix modulus 256 as such: let the chosen Q-matrix be $qmatrix$:

$$A_3 = A_2 \cdot qmatrix \pmod{256}. \quad (8)$$

As a result of the preceding steps, we now have the encrypted audio signal. Figure 2 visually illustrates these steps.

The decryption process follows the inverse steps of the encryption procedure, starting with the encrypted audio signal and ending with its lossless decrypted version. Figure 3 visually illustrates these steps.

IV. NUMERICAL RESULTS AND PERFORMANCE EVALUATION

This section highlights the computed performance evaluation metrics and compares them with those achieved by similar algorithms from the literature.

Table II showcases the waveforms and histogram plots of three sample plain audio signals, their encrypted versions, and their decrypted versions. The waveforms of the plain audio signals display clear, recognizable patterns, while

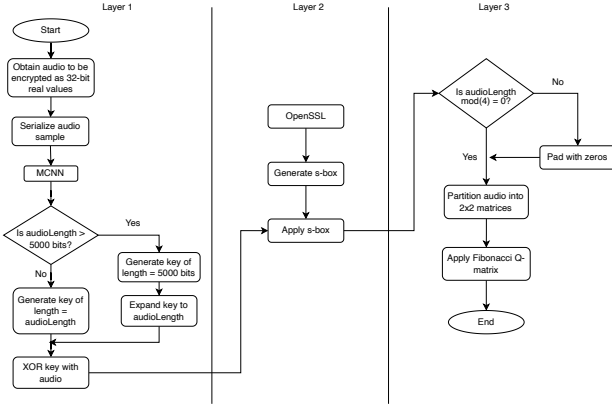


Fig. 2: The encryption process.

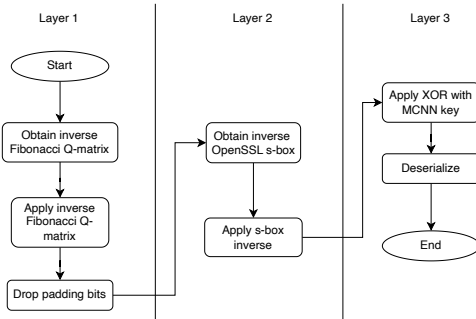


Fig. 3: The decryption process.

the encrypted waveforms appear as random, noise-like patterns, effectively obscuring the original audio content. The decrypted waveforms closely match the plain audio signals, demonstrating the algorithm's capability to accurately reconstruct the original data. The histogram plots further illustrate the distribution of signal values, with the encrypted histograms showing a uniform distribution, indicating successful encryption, and the decrypted histograms resembling those of the plain signals, confirming the integrity of the decryption process.

Table III presents the spectrograms of a plain audio signal, its encrypted version, and its decrypted version. The plain audio spectrogram displays distinct patterns and frequencies corresponding to the original sound content. In contrast, the encrypted audio spectrogram appears as a chaotic and noise-like pattern, devoid of any recognizable structure, demonstrating the effectiveness of the encryption process in obscuring the original signal. Finally, the decrypted audio spectrogram closely matches the original plain audio spectrogram, indicating that the decryption process successfully reconstructs the initial audio content without significant loss of information. This comparison highlights the robustness of the encryption algorithm in securely transforming the audio signal while allowing accurate recovery during decryption.

Table IV presents the entropy values computed for various audio files using the proposed audio encryp-

tion algorithm. The results show that the encrypted entropy values for all audio files—Drums.wav, Bird.wav, FemaleVoice.wav, and NoisyTalk.wav—are consistently low, indicating a high level of data randomness and effective encryption. The decrypted entropy values are significantly higher, suggesting that the original audio information is well-preserved and accurately recoverable post-decryption. These results demonstrate the algorithm's capability to produce highly secure encrypted data while maintaining the integrity of the original audio upon decryption.

Table V compares the performance of the proposed audio encryption algorithm with recent literature based on PSNR, NSCR, and encryption correlation coefficient values. The proposed method achieves a PSNR of 6.004, indicating good fidelity in the decrypted audio. The NSCR value of 99.9112% demonstrates a high degree of sensitivity to pixel changes, reflecting robust security against differential attacks. The encryption correlation coefficient value of 04.091×10^{-7} suggests minimal correlation in the encrypted data, signifying effective obfuscation. Compared to other methods, the proposed algorithm shows competitive performance, particularly in maintaining low correlation and high NSCR, thereby validating its efficacy and robustness in audio encryption.

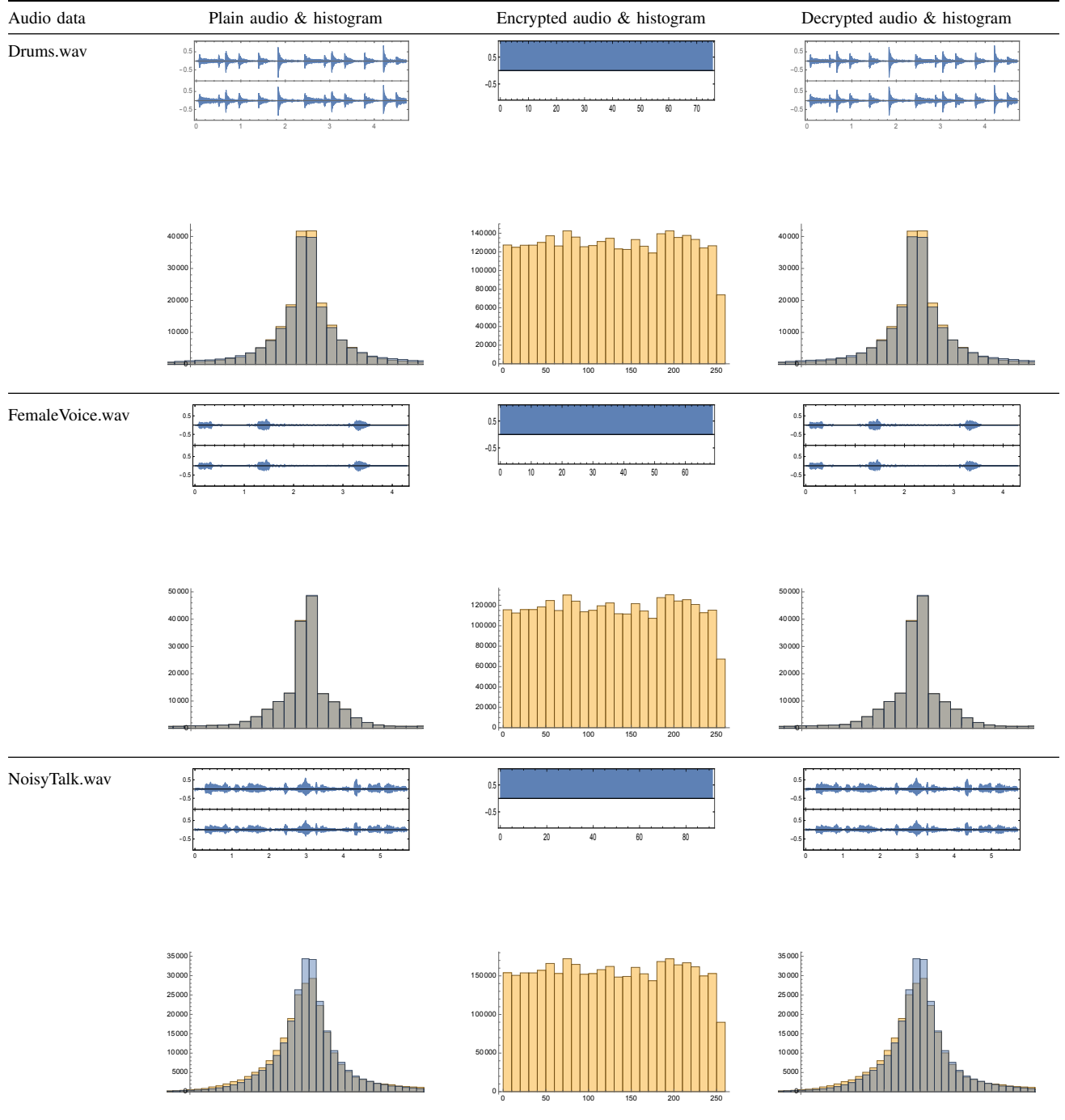
Table VI displays the key space analysis of the proposed audio encryption algorithm compared to existing methods in the literature. The table highlights that the proposed algorithm features a significantly larger key space, ensuring enhanced resistance to brute-force attacks. This comparison underscores the superiority of the proposed method in terms of security, as a vast key space is crucial for preventing unauthorized access and ensuring robust encryption. The analysis confirms the algorithm's potential to offer stronger protection for sensitive audio data compared to traditional encryption techniques.

Table VII compares the performance metrics of the proposed S-box with those from various literature sources. The metrics include Nonlinearity (NL), Strict Avalanche Criterion (SAC), Bit Independence Criterion (BIC), Linear Approximation Probability (LAP), and Differential Approximation Probability (DAP). The proposed S-box demonstrates strong performance, with an NL value of 108 and SAC close to the optimal value at 0.499023. It matches the optimal BIC, LAP, and DAP values, indicating robust cryptographic properties. Compared to [21] and other references, the proposed S-box shows competitive or superior results, particularly in maintaining low LAP and DAP values, essential for resistance against linear and differential cryptanalysis.

V. CONCLUSIONS AND FUTURE WORKS

This paper introduces a multi-layer audio encryption scheme utilizing the Memristive Coupled Neural Network (MCNN), S-box, and Fibonacci Q-matrix. The three-step process—MCNN-generated pseudo-random key XORed with audio data, S-box transformation via OpenSSL PRNG, and Fibonacci Q-matrix application—demonstrates excellent performance in terms of PSNR, NSCR, correlation coefficient, and information entropy, showcasing robustness against various attacks. The vast key space of 2^{2126} further ensures strong resistance to brute-force attacks. Future

TABLE II: Implementation of the proposed audio encryption scheme on different audios.



work will focus on real-time implementation, integration with other cryptographic methods, computational efficiency optimization, and comprehensive security analyses to validate the scheme's applicability in diverse environments.

REFERENCES

- [1] R. I. Abdelfatah, "Audio encryption scheme using self-adaptive bit scrambling and two multi chaotic-based dynamic dna computations," *IEEE Access*, vol. 8, pp. 69 894–69 907, 2020.
- [2] W. Alexan, M. Elbeltagy, and A. Aboshousha, "RGB image encryption through cellular automata, s-box and the lorenz system," *Symmetry*, vol. 14, p. 443, 02 2022.
- [3] K. Kordov, "A novel audio encryption algorithm with permutation-substitution architecture," *Electronics*, vol. 8, no. 5, 2019. [Online]. Available: <https://www.mdpi.com/2079-9292/8/5/530>
- [4] P. K. Naskar, S. Bhattacharyya, and A. Chaudhuri, "An audio encryption based on distinct key blocks along with pwlc and eca," *Nonlinear Dynamics*, vol. 103, pp. 2019–2042, 2021.
- [5] Y. Hameed and N. M. Ali, "An efficient audio encryption based on chaotic logistic map with 3d matrix," *Journal of Theoretical and Applied Information Technology*, vol. 96, pp. 5142–5152, 08 2018.
- [6] M. Demirtaş, "A lossless audio encryption method based on chebyshev map," *Orclever Proceedings of Research and Development*, vol. 2, no. 1, p. 28–38, 2023. [Online]. Available: <https://journals.orclever.com/oprd/article/view/234>
- [7] B. Rahul, K. Kuppusamy, and A. Senthilrajan, "Chaos-based audio encryption algorithm using biometric image and sha-256 hash algorithm," *Multimedia Tools and Applications*, vol. 82, pp. 1–30, 04 2023.
- [8] L. C. Y. S. S. M. I. C. X. Hairong Lin, Chunhua Wang and F. Yu, "Brain-like initial-boosted hyperchaos and application in biomedical image encryption," *IEEE Transactions on Industrial Informatics*, vol. 18, pp. 1–11, 12 2022.
- [9] M. Gabr, R. Elias, K. M. Hosny, G. A. Papakostas, and W. Alexan, "Image encryption via base-n prngs and parallel base-n S-boxes," *IEEE Access*, vol. 11, pp. 85 002–85 030, 2023.
- [10] J. Viegas, M. Messier, and P. Chandra, *Network security with*

TABLE III: Spectrogram for NoisyTalk.wav.

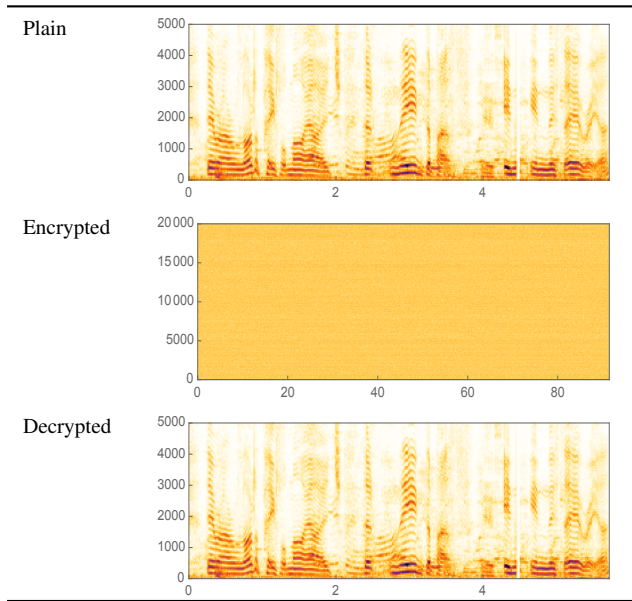


TABLE IV: Entropy Results.

Audio	Enc. Entropy	Dec. Entropy
Drums.wav	0.0348464	2.45144
Bird.wav	0.0376484	3.1343
FemaleVoice.wav	0.03434	2.66103
NoisyTalk.wav	0.0341453	3.96788

TABLE V: PSNR, NSCR & correlation coefficient analysis values comparison with recent literature.

Audio	PSNR	NSCR [%]	Enc. Correlation
Proposed	6.004	99.9112	-4.091×10^{-7}
[1]	4.296	99.994	0.0002616
[19]	10.55	99.99	-0.002754
[20]	-8.607	100	-0.002

TABLE VI: Key space analysis comparison with the literature.

Algorithm	Key-space
Proposed	$10^{640} \approx 2^{2126}$
[1]	2^{928}
[3]	$10^{45} \approx 2^{149}$
[4]	2^{576}
[5]	2^{128}
[6]	$10^{48} \approx 2^{159}$
[7]	$(2^{256})^{256}$

TABLE VII: S-box performance metrics.

S-Box	NL	SAC	BIC	LAP	DAP
Optimal	112	0.5	112	0.0625	0.015625
Proposed	108	0.499023	112	0.0625	0.015625
[21]	108	0.494141	108	0.078125	0.015625
[22]	106	0.5019	112	0.1328	0.0391
[23]	111	0.5036	110	0.0781	0.0234

openSSL: cryptography for secure communications. " O'Reilly Media, Inc.", 2002.

- [11] W. Alexan, N. Alexan, and M. Gabr, "Multiple-layer image encryption utilizing fractional-order chen hyperchaotic map and cryptographically secure prngs," *Fractal and Fractional*, vol. 7, no. 4, p. 287, 2023.
- [12] B. I. Tuleuov and A. B. Ospanova, "Openssl," in *Beginning C++ Compilers: An Introductory Guide to Microsoft C/C++ and MinGW Compilers*. Springer, 2024, pp. 157–163.
- [13] W. Alexan, Y.-L. Chen, L. Y. Por, and M. Gabr, "Hyperchaotic maps and the single neuron model: A novel framework for chaos-based image encryption," *Symmetry*, vol. 15, no. 5, p. 1081, 2023.
- [14] M. Beck and R. Geoghegan, *The Art of Proof*. Springer, 2010.
- [15] E. W. Weisstein, "fibonacci q-matrix," from mathworld—a wolfram web resource." [Online]. Available: <https://mathworld.wolfram.com/FibonacciQ-Matrix.html>
- [16] K. M. Hosny, S. T. Kamal, M. M. Darwish, and G. A. Papakostas, "New image encryption algorithm using hyperchaotic system and fibonacci q-matrix," *Electronics*, vol. 10, no. 9, p. 1066, 2021. [Online]. Available: <https://www.mdpi.com/2079-9292/10/9/1066>
- [17] —, "New image encryption algorithm using hyperchaotic system and fibonacci q-matrix," *Electronics*, vol. 10, no. 9, p. 1066, 2021.
- [18] M. Gabr, Y. Korayem, Y.-L. Chen, L. Y. Por, C. Ku, and W. Alexan, "R 3 —rescale, rotate, and randomize: A novel image cryptosystem utilizing chaotic and hyper-chaotic systems," *IEEE Access*, vol. PP, 10 2023.
- [19] I. Khalid, T. Shah, K. A. Almarhabi, D. Shah, M. Asif, and M. Usman Ashraf, "The spn network for digital audio data based on elliptic curve over a finite field," *IEEE Access*, vol. 10, pp. 127 939–127 955, 2022.
- [20] X. Wang and Y. Su, "An audio encryption algorithm based on dna coding and chaotic system," *IEEE Access*, vol. 8, pp. 9260–9270, 2020.
- [21] W. Alexan, Y. Korayem, M. Gabr, M. El-Aasser, E. A. Maher, D. El-Damak, and A. Aboshousha, "Anteater: When arnold's cat meets langton's ant to encrypt images," *IEEE Access*, vol. 11, pp. 106 249–106 276, 2023.
- [22] M. Gabr, H. Younis, M. Ibrahim, S. Alajmy, I. Khalid, E. Azab, R. Elias, and W. Alexan, "Application of DNA coding, the lorenz differential equations and a variation of the logistic map in a multi-stage cryptosystem," *Symmetry*, vol. 14, no. 12, p. 2559, 2022.
- [23] M. Khan and F. Masood, "A novel chaotic image encryption technique based on multiple discrete dynamical maps," *Multimedia Tools and Applications*, vol. 78, no. 18, pp. 26 203–26 222, 2019.