TDADL-IE: A Deep Learning-Driven Cryptographic Architecture for Medical Image Security

Junhua Zhou[1], Quanjun Li[1], Weixuan Li[1], Guang Yu[2,3,4], YiHua Shao[4], Yihang Dong[2],
Mengqian Wang[5], Zimeng Li[2*], Changwei Gong[2], and Xuhang Chen[2*]

[1]Guangdong University of Technology
[2]School of Electronic and Communication Engineering, Shenzhen Polytechnic University
[3]School of Computer Science and Engineering, Huizhou University
[4]University of Science and Technology Beijing
[5]Institute of Neuroscience, Chinese Academy of Sciences

Abstract—The rise of digital medical imaging, like MRI and CT, demands strong encryption to protect patient data in telemedicine and cloud storage. Chaotic systems are popular for image encryption due to their sensitivity and unique characteristics, but existing methods often lack sufficient security. This paper presents the Three-dimensional Diffusion Algorithm and Deep Learning Image Encryption system (TDADL-IE), built on three key elements. First, we propose an enhanced chaotic generator using an LSTM network with a 1D-Sine Quadratic Chaotic Map (1D-SQCM) for better pseudorandom sequence generation. Next, a new three-dimensional diffusion algorithm (TDA) is applied to encrypt permuted images. TDADL-IE is versatile for images of any size. Experiments confirm its effectiveness against various security threats. The code is available at https://github.com/QuincyQAQ/TDADL-IE.

Index Terms—Deep learning; Medical image encryption; Chaotic map

I. INTRODUCTION

The rise of medical imaging and telemedicine has increased the need for secure digital image transmission and storage. Medical images like MRI, CT, and ultrasound contain sensitive patient data crucial for diagnosis and treatment. Without strong encryption, these images are vulnerable to unauthorized access and breaches, especially over unsecured networks or in cloud storage. Protecting this data is essential for patient privacy and required by regulations like HIPAA. Traditional text-oriented encryption methods are ineffective for medical images due to their high inter-pixel correlation, large data size, and complex formats. Chaotic systems offer a promising solution for developing robust and efficient image encryption techniques [1].

Chaotic systems, known for their deterministic randomness, ergodicity, and sensitivity to initial conditions, are ideal for cryptographic applications like generating pseudo-random sequences for image encryption [2]. Although one-dimensional

(1D) chaotic maps are simple and easy to implement [3], their predictability and limited chaos can create security risks [2]. Thus, research has turned to more complex chaos-based encryption systems. Recently, deep learning has emerged as a new approach, with efforts like Google Brain's self-encryption model using adjoint networks [4], Long Short-Term Memory (LSTM) networks for assessing chaotic sequence randomness [5], and hybrid neural-chaotic encryption methods [6], [7]. Despite these progressions, deep learning in color image encryption, with its challenges of inter-channel dependencies and high dimensionality, remains underexplored.

Permutation-only encryption schemes, common in image encryption, are vulnerable to various attacks due to discernible statistical properties in ciphertext [8]. Diffusion processes modify pixel values to enhance encryption by obscuring local dependencies. Many existing diffusion schemes lack sensitivity to plaintext and key variations as they operate independently of image content. Recent research has focused on plaintext-aware diffusion [9]–[12]. Murillo et al. used logical maps based on plaintext features [9], and Parvin et al. combined XOR operations with chaotic functions [10]. However, these methods rely on initial plaintext for key generation, limiting their use in real-time scenarios like live video encryption. Their weak nonlinearity and limited key spaces make them susceptible to chosen-plaintext attacks [13], [14]. To address these issues, we propose the Joint Nonlinear Three-dimensional Diffusion Mechanism (TDA), which tightly integrates diffusion with the image content, enhancing sensitivity and avalanche effects.

Our primary contributions are as follows:

1) Existing one-dimensional chaotic maps frequently suffer from constrained chaotic ranges and suboptimal sensitivity to initial conditions, thereby limiting their efficacy in generating secure cryptographic keys. Therefore, a novel 1D-chaotic map 1D-Sine Quadratic Chaotic Map (1D-SQCM) is proposed, which can generate sequences with enhanced randomness and wider chaotic ranges.

2) By synergistically integrating the 1D-Sine Quadratic Chaotic Map (1D-SQCM) with the dynamic modeling

capabilities of Long Short-Term Memory (LSTM) networks, we engineer a novel chaotic sequence generator. This generator exhibits an expanded chaotic regime, superior entropy, and refined temporal correlations, culminating in substantially enhanced randomness and cryptographic robustness.

3) Addressing the distinct requirements of diffusing non-square and color images, where inter-channel correlations and varying dimensions pose significant challenges, we present the three-dimensional diffusion algorithm (TDA). This mechanism amalgamates forward and backward diffusion processes with inter-channel pixel interactions. Such a design ensures that minute alterations in the plaintext cascade comprehensively throughout the ciphertext, thereby significantly amplifying both key sensitivity and plaintext sensitivity.

II. METHODOLOGY

TDADL-IE is a new encryption algorithm for multi-medical images, using a 1D Sine-Cosine-Exponential Map (1D-SQCM) and neural network enhancement. Its flowchart is shown in Figure 1. The algorithm has two main modules: (1) chaotic sequence generation with 1D-SQCM and BLSTM network, and (2) a Three-dimensional Diffusion Algorithm (TDA). TDADL-IE can encrypt multiple images simultaneously. The secret keys for encryption are Key_{x1}, Key_{y1}, Key_a, and Key_{N_0}. The modules are detailed in the following subsections.
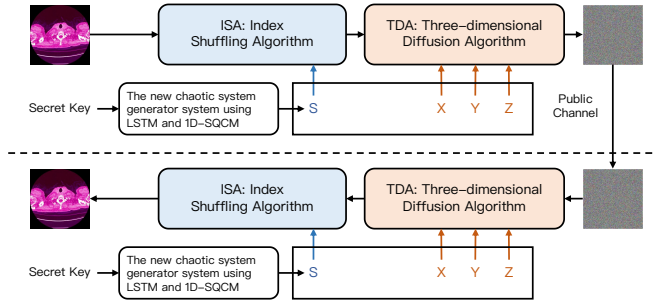

Fig. 1. The process of the encryption algorithm.

A. Chaotic Sequence Generation using 1D-SQCM and BLSTM

Bidirectional Long Short-Term Memory (BLSTM) networks enhance standard LSTMs [15] with a design involving input, forget, and output gates, and a memory cell (LSTM structure shown in Fig. 2). The forget gate f_t regulates retaining information from previous states h_{t-1} and its output is limited to $[0, 1]$. In generating chaotic-like sequences, the forget gate's selective discarding of historical information mirrors the fading memory of chaotic systems, increasing sensitivity to initial conditions and encouraging divergent phase-space trajectories. Simultaneously, the input gate governs new information input,

introducing nonlinear changes that influence system evolution and enhance complex dynamics. The memory cell integrates these inputs, updating its state to capture long-term dependencies and produce intricate, high-dimensional sequences. Altogether, these elements form a robust nonlinear mechanism for modeling and creating complex temporal sequences with chaotic traits.

Leveraging these properties, we introduce a hybrid chaotic sequence generator that synergistically combines the 1D Sine-Cosine-Exponential Map (1D-SQCM) with the temporal modeling capabilities of a BLSTM network. The 1D-SQCM, selected for its inherent characteristics of high entropy and pronounced sensitivity to initial conditions, is defined as:

$$x_{n+1} = \sin(\frac{a^2}{\sin(x_n)}), \tag{1}$$

where x_n denotes the state variable at iteration n, and a is a system control parameter. By subsequently processing the output of the 1D-SQCM through the BLSTM network, we aim to generate sequences that are not only temporally correlated and statistically rich but also exhibit significant phase space divergence. This integrated methodology preserves the fundamental randomness of the chaotic map while empowering the BLSTM to adaptively learn and amplify the complexity and unpredictability of the generated sequences.
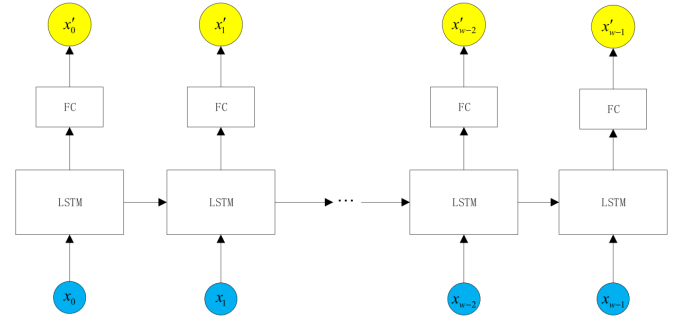

Fig. 2. LSTM training model diagram. a Training diagram of x

Step 1: BLSTM Model Training. The BLSTM model undergoes an initial training phase to learn the complex dynamics of chaotic sequences. This process is initiated as follows:

1) *Training Data Generation*: The system parameter Key_a for the 1D-SQCM (Eq. (1)) and an initial state Key_{x0} (distinct from the encryption keys used for image processing) are specified. The 1D-SQCM is iterated to produce a raw chaotic sequence. To mitigate transient effects and ensure the sequence operates within the chaotic attractor, the initial $N_{\text{discard\_train}} = 6,000$ iterates are discarded. The subsequent $N_{\text{train}} = 24,000$ points are collected to form the training sequence, denoted as X_{train}.

2) *BLSTM Configuration and Training*: The architecture of the BLSTM network is defined, including the number of hidden layers and units. Key hyperparameters, such as

the learning rate and the length of input subsequences for training, are optimized. The BLSTM model is then trained using X_{train} to learn its underlying temporal patterns and statistical properties.

Upon completion of this training phase, the BLSTM model is equipped to generate enhanced chaotic sequences for the encryption process.

Step 2: Hybrid Chaotic Sequence Generation for Encryption. For the encryption process, the secret keys Key_{x1}, Key_{y1}, Key_a, and Key_{N_0} are employed. The generation proceeds as follows:

1) *1D-SQCM Sequence Generation*: A primary chaotic sequence, denoted X_{SQCM}, of length $2mn$ is generated using the 1D-SQCM (Eq. (1)). The map is initialized using Key_{x1} as the initial state x_0, and Key_a serves as the control parameter. The keys Key_{y1} and Key_{N_0} may influence aspects such as the number of initial iterations to discard prior to collecting sequence values for encryption.

2) *BLSTM Sequence Enhancement*: The trained BLSTM model is then utilized to produce a secondary chaotic sequence, X_{BLSTM}, also of length $2mn$. This sequence can be generated by feeding an initial seed (derived from the keys or from a segment of X_{SQCM}) to the BLSTM and allowing it to predict subsequent values.

3) *Sequence Concatenation*: The two sequences, X_{SQCM} and X_{BLSTM}, are horizontally concatenated to form a hybrid chaotic sequence S_{hybrid} of total length $4mn$. This hybrid sequence benefits from both the fundamental chaotic properties of the 1D-SQCM and the learned complexity introduced by the BLSTM.

The length mn typically corresponds to the number of pixels in a single channel of an image of size $m \times n$. The total length $4mn$ prepares for processing data equivalent to an $m \times n$ image with four components per pixel (*e.g.*, RGBA) or four distinct $m \times n$ sequences for cryptographic operations.

Step 3: Chaotic Sequence Processing and Derivation. The hybrid chaotic sequence S_{hybrid} of length $4mn$, generated as described in Step 2, is subsequently processed to derive tailored sequences for the various stages of the encryption algorithm. This processing is performed as follows:

1) *Sequence Partitioning*: The sequence S_{hybrid} is partitioned into four sub-sequences, s, x, y, and z, each of length $L = mn$. (Here, $L = mn$ represents the number of elements in each sub-sequence, corresponding to the pixel count of a single-channel $m \times n$ image).

2) *Derivation of Diffusion Sequences*: From the sub-sequences x, y, and z, three new sequences, X, Y, and Z, also of length $L = mn$, are computed using the transformations defined in Eq. (2).

$$\begin{cases} X(i) = \text{mod}(\lfloor x(i) \cdot y(L-i+1) \cdot 10^9 \rfloor, 256) + 1, \\ Y(i) = \text{mod}(\lfloor x(L-i+1) \cdot y(i) \cdot 10^9 \rfloor, 256) + 1, \\ Z(i) = \text{mod}(\lfloor z(i) \cdot 10^9 \rfloor, 256) + 1, \end{cases}$$
$$(2)$$

for $i = 1, 2, \ldots, L$.

3) *Matrix Reshaping*: The resulting one-dimensional sequences X, Y, and Z are reshaped into $m \times n$ matrices, denoted X_{2D}, Y_{2D}, and Z_{2D}, respectively. These matrices are subsequently employed in the TDA module. The sequence s is reserved for the Index Shuffling Algorithm.

This multi-stage derivation ensures that distinct, complex pseudo-random sequences are available for different cryptographic operations, enhancing the overall security.

B. Index Shuffling Algorithm (ISA)

The Index Shuffling Algorithm (ISA) implements a pixel-level permutation to obfuscate spatial correlations within the input image. This process is applied to each $m \times n$ image or image channel independently, using the chaotic sequence s (of length mn) derived as described in Section II-A (Step 3). The ISA proceeds as follows:

1) *Vectorization*: The $m \times n$ pixel data of an image (or an individual channel thereof) is flattened into a one-dimensional vector P of length mn.

2) *Permutation Index Generation*: The chaotic sequence s is utilized to derive a set of permutation indices. A common method involves obtaining the indices that would sort the elements of s. Let these indices be $Idx = [\text{idx}_1, \text{idx}2, \ldots, \text{idx}mn]$.

3) *Pixel Scrambling*: The pixels in vector P are reordered according to these indices. Specifically, the j-th pixel in the permuted vector P' is $P(\text{idx}_j)$. This operation effectively scrambles the original pixel arrangement.

4) *Reshaping*: The permuted vector P' is reshaped back into its original $m \times n$ two-dimensional structure, yielding the shuffled image (or channel).

This permutation step significantly enhances the algorithm's resistance to statistical attacks by decorrelating adjacent pixels.

C. Three-dimensional Diffusion Algorithm (TDA)

The Three-dimensional Diffusion Algorithm (TDA) is designed to spread pixel information across spatial dimensions and color channels in images $m \times n$. It uses forward and backward diffusion passes to ensure changes to a single plaintext pixel impact many ciphertext pixels, ensuring diffusion. The forward pass processes pixels in raster order *e.g.* from top-left $(1,1)$ to bottom-right (m,n), while the backward pass goes in the reverse direction *e.g.* from (m,n) to $(1,1)$.

TDA's cross-channel pixel interactions boost encryption strength, especially for color images, by ensuring diffusion occurs across color planes. Conceptually shown in Fig. 3, a pixel in one channel is influenced by neighboring pixels in other channels. For instance, during diffusion, a Green (G) channel pixel at (i,j) is updated using nearby Red (R) channel pixels (*e.g.* from $(i-1,j)$ and $(i,j-1)$), its previous G neighbor, and a key-derived element. A Blue (B) channel pixel may also rely on G channel values. This inter-channel dependency is vital to counteract independent channel analysis. TDA's operations and updates are detailed in Algorithm 1, using key-dependent matrices X_{2D}, Y_{2D}, and Z_{2D}.

Algorithm 1 Three-dimensional Diffusion Algorithm

Input: The scrambled image A with size $M \times N$ and the chaotic matrices X_{2D}, Y_{2D}, and Z_{2D}

1: $C(1,1,1) \leftarrow mod(A(1,1,1) + X_2D(1,1), 256)$
2: $C(1,1,2) \leftarrow mod(A(1,1,2) + Y_2D(1,1), 256)$
3: $C(1,1,3) \leftarrow mod(A(1,1,3) + Z_2D(1,1), 256)$
4: **for** $j = 2$ to N **do**
5:    $C(1,j,1) \leftarrow mod(A(1,j,1) + X_2D(1,j) + C(1,j-1,1) + C(1,j-1,3), 256)$
6:    $C(1,j,2) \leftarrow mod(A(1,j,2) + Y_2D(1,j) + C(1,j-1,2) + C(1,j-1,1), 256)$
7:    $C(1,j,3) \leftarrow mod(A(1,j,3) + Z_2D(1,j) + C(1,j-1,3) + C(1,j-1,2), 256)$
8: **end for**
9: **for** $i = 2$ to M **do**
10:    $C(i,1,1) \leftarrow mod(A(i,1,1) + X_2D(i,1) + C(i-1,1,1) + C(i-1,1,3), 256)$
11:    $C(i,1,2) \leftarrow mod(A(i,1,2) + Y_2D(i,1) + C(i-1,1,2) + C(i-1,1,1), 256)$
12:    $C(i,1,3) \leftarrow mod(A(i,1,3) + Z_2D(i,1) + C(i-1,1,3) + C(i-1,1,2), 256)$
13: **end for**
14: **repeat**
15:    **for** $i = 2$ to M **do**
16:      **for** $j = 2$ to N **do**
17:       $C(i,j,1) \leftarrow mod(A(i,j,1) + X_2D(i,j) + C(i,j-1,3) + C(i-1,j,3), 256)$
18:       $C(i,j,2) \leftarrow mod(A(i,j,2) + Y_2D(i,j) + C(i,j-1,1) + C(i-1,j,1), 256)$
19:       $C(i,j,3) \leftarrow mod(A(i,j,3) + Z_2D(i,j) + C(i,j-1,2) + C(i-1,j,2), 256)$
20:      **end for**
21:    **end for**
22: **until** The image encryption process is complete.
23: **Output:** The encrypted image C

D. Decryption Algorithm

The decryption procedure for TDADL-IE is designed as the exact inverse of the encryption process. Given that the core operations—chaotic sequence generation, index shuffling (permutation), and three-dimensional diffusion (typically involving operations such as XOR and modular arithmetic)—are deterministic and reversible when the correct secret keys (Key_{x1}, Key_{y1}, Key_a, Key_{N_0}) are known, the original plaintext image can be perfectly reconstructed. The decryption involves:

1) *Chaotic Sequence Regeneration*: The same set of chaotic sequences (s, X_{2D}, Y_{2D}, Z_{2D}) are regenerated using the secret keys identically to the encryption phase.
2) *Inverse Three-dimensional Diffusion*: The TDA operations are applied in reverse. This typically involves processing in the reverse order of diffusion passes (*e.g.*, inverse backward pass followed by inverse forward pass) and applying the mathematical inverse of each encryption operation (*e.g.*, XOR is its own inverse; modular
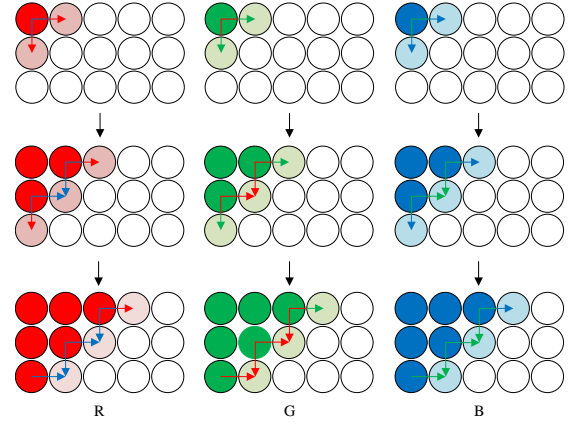

Fig. 3. The Illustration of Three-dimensional Diffusion Algorithm (TDA)

subtraction for modular addition). The cross-channel dependencies are also reversed according to the defined inverse rules.
3) *Inverse Index Shuffling*: The inverse permutation, derived from the same chaotic sequence s by determining the reverse mapping of indices, is applied to the diffused image to restore the original pixel order.

The successful recovery of the plaintext image hinges on the precise application of these inverse steps and the availability of the identical secret keys used during encryption.

III. EXPERIMENTAL RESULTS

This section evaluates the proposed cryptosystem, focusing on the efficiency and security of the TDADL-IE algorithm and the performance characteristics of the 1D-SQCM chaotic map.

A. Experimental Setup

The validation consists of analyzing the 1D Sin-Cos Pi Hyperchaotic Map (1D-SQCM) and evaluating the TDADL-IE encryption algorithm. The chaotic behavior of 1D-SQCM is compared to three one-dimensional chaotic maps Table I and two-dimensional systems. For TDADL-IE, three standard grayscale test images, "IMG1", "IMG2", and "IMG3" of sizes $M \times N$, *e.g.*, and 512×512 pixels [16], are used. It's compared with state-of-the-art encryption techniques [17]–[21] using standard metrics. Experiments ran on an AMD Ryzen 7 7800X3D CPU at 4.20 GHz, 32 GB RAM, with Windows 11 and MATLAB R2024a.

B. Performance Analysis of the 1D-SQCM Chaotic Map

This subsection presents a comparative analysis of the chaotic dynamics exhibited by the proposed 1D-SQCM and other existing chaotic maps, with detailed comparisons provided in Table I. The objective is to demonstrate the enhanced chaotic properties of 1D-SQCM.

1) Lyapunov Exponent Analysis: The Lyapunov exponent (LE) quantifies the sensitivity of a dynamical system to infinitesimal perturbations in its initial conditions, with positive LEs indicating chaotic behavior. Figure 4 illustrates the

TABLE I
TESTED MAPS.

Name	Mathematical expressions	Parameter settings
1D-SQCM	$x_{n+1} = \sin\left(\frac{a}{\sin(x_n)}\right)$	$a \in (0, \infty)$
sine	$x_{n+1} = b \times \sin(\pi x_n)$	$b \in (0, \infty)$
1-DFCS	$x_{n+1} = \frac{\cos((\eta x_n + 1)^2 + 1)}{\sin((\eta x_n + 1)^2 + 1) + 2}$	$\eta \in (0, \infty)$
1D-Chebyshev	$x_{n+1} = \cos(k \times \arccos(x_n))$	$k \in (0, \infty)$

Lyapunov exponents for the 1D-SQCM and other benchmarked 1D chaotic maps across a control parameter range of $(0, 10000)$. The results demonstrate that the 1D-SQCM maintains positive Lyapunov exponents throughout this range. Furthermore, these values are consistently larger than those of the compared chaotic maps, signifying robust chaotic characteristics and heightened sensitivity to initial conditions, which are desirable for cryptographic applications.
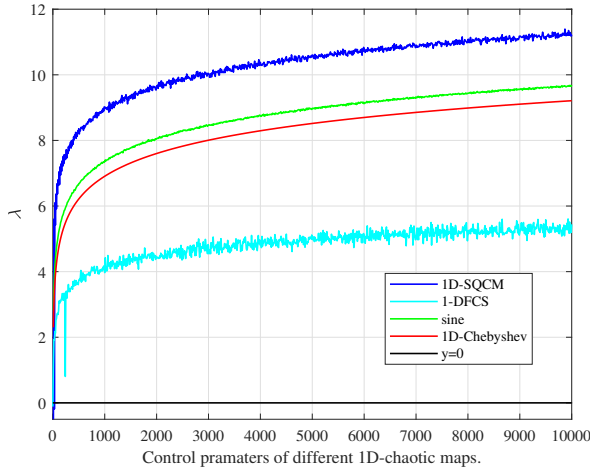

Fig. 4. The Lyapunov exponent of 1D-SQCM, 1-DFCS, Sine and 1D-Chebyshev map.

2) NIST SP 800-22 Statistical Test Suite: The randomness of the sequences generated by the 1D-SQCM was rigorously evaluated using the NIST SP 800-22 statistical test suite. This suite comprises a set of tests designed to detect deviations from true randomness in binary sequences. Table II presents the P-values obtained from these tests applied to sequences derived from the 1D-SQCM output. For all generated sequences, the P-values consistently exceed the standard significance threshold of 0.01.

3) Deep Learning-based Predictability Assessment: The 1D-SQCM's output was analyzed using a Bidirectional Long Short-Term Memory (BLSTM) network, with training details in Fig. 6. The low root-mean-square error (RMSE) and loss function values suggest the BLSTM's ability to learn the short-term patterns of the chaotic sequence. A comparison between the actual sequence $\{X_{true}\}$ and the BLSTM prediction $\{X_{pred}\}$ is presented in Fig. 6. The divergence between

TABLE II
NIST TEST RESULTS OF 1D-SQCM.

Test index	P−value	Result
Frequency (Monobit) Test	0.0909	PASS
Frequency Test within a Block	0.0711	PASS
Runs Test	0.2368	PASS
Longest Run of Ones in a Block Test	0.4190	PASS
Binary Matrix Rank Test	0.7981	PASS
Discrete Fourier Transform (Spectral) Test	0.3504	PASS
Non-overlapping Template Matching Test	0.2368	PASS
Overlapping Template Matching Test	0.2757	PASS
Maurers Universal Statistical Test	0.9780	PASS
Linear Complexity Test	0.8676	PASS
Serial Test	0.8343	PASS
Approximate Entropy Test	0.5341	PASS
Cumulative Sums (Cusums) Test	0.2896	PASS
Random Excursions Test	0.8623	PASS
Random Excursions Variant Test	0.8676	PASS

Fig. 5. BLSTM training loss

$\{X_{true}\}$ and $\{X_{pred}\}$ over extended predictions highlights the long-term unpredictability of the 1D-SQCM, a trait of robust chaotic systems.

C. Security and Performance Analysis of TDADL-IE Cryptosystem

1) Key Space Analysis: A fundamental requirement for robust cryptographic security against exhaustive search attacks is a key space substantially larger than 2^{100}. The TDADL-IE cryptosystem utilizes four secret keys with the following initial theoretical ranges: $Key_{x1} \in (0, 1)$, $Key_{y1} \in (0, 1)$, $Key_a \in (0, \infty)$, and $Key_{N0} \in (2000, \infty)$. In a practical digital implementation, these continuous ranges are discretized based on the precision of the numerical representation. Consequently, the effective discrete key space is vast, estimated to be approximately 2^{208}. This significantly surpasses the aforementioned security threshold, rendering brute-force attacks computationally infeasible and thereby providing a high level of protection.

2) Differential Attack Analysis: Plaintext and Key Sensitivity: An encryption algorithm's resilience to differential attacks is measured by its sensitivity to small changes in plaintext or key, assessed via NPCR and UACI metrics. Ideal NPCR and UACI values are about 99.6% and 33.4% for 8-bit grayscale images with random-like cipher images. The TDADL-IE algorithm's NPCR and UACI scores when altering a single bit are high and near these ideal levels, indicating strong
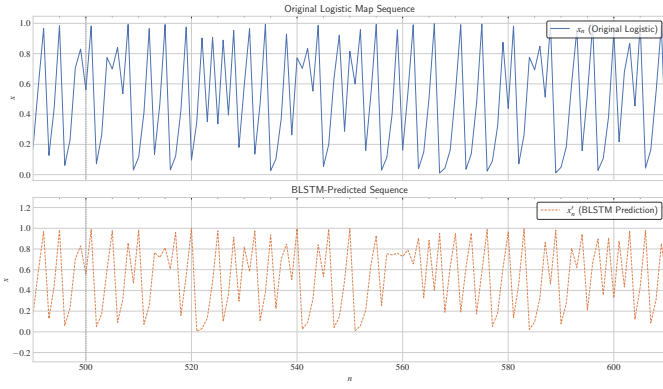
Fig. 6. The difference of chaotic signals.

diffusion properties and robustness to differential cryptanalysis Section III-C2.

TABLE III
COMPARING COEFFICIENTS OF CORRELATION SCHEMES OF ONE IMAGE.

Algorithm	Correlation coefficients			Information entropy ↑	Time (s) ↓	NPCR	UACI	Key space ↑
	H ↓	V ↓	D ↓					
Proposed	**0.0011**	**-0.0009**	**0.0016**	7.9993	**0.3814**	**99.6094(*)**	**33.4641(*)**	2^{208}
Kamal *et al.* [21]	0.0145	0.0115	0.0087	7.9992	3.0901	99.6010	33.4389	2^{115}
Ye *et al.* [22]	0.0085	-0.0056	0.0040	7.9992	3.3714	99.6132	33.4268	2^{156}
Xu *et al.* [23]	0.0067	-0.0086	0.0140	7.9935	0.5509	99.6102	33.4812	2^{30}

(*This value is closest to the ideal value)

3) Correlation Coefficient Analysis: Plaintext images show high correlation among adjacent pixels. An effective encryption algorithm should reduce these correlations in ciphertext, preventing statistical attacks. Section III-C2 shows that while original images have strong correlations, the TDADL-IE encrypted images have coefficients near zero in all directions. This reduction indicates that TDADL-IE effectively decorrelates pixel values, enhancing security against statistical cryptanalysis.

4) Encryption Efficiency: Computational efficiency is crucial for an image encryption algorithm's practicality. The TDADL-IE scheme's encryption speed was evaluated in the specified environment and compared with other algorithms in [17]–[21]. According to Section III-C2, it processes images competitively, proving its efficiency and suitability for applications requiring timely processing.

IV. CONCLUSION

This paper presents a novel color image encryption method addressing low key and plaintext sensitivity. The method uses a new one-dimensional chaotic system (1D-SQCM) and Two-Directional Diffusion Algorithm (TDA) for high security and efficiency. 1D-SQCM generates pseudo-random sequences, and the Index Shuffling Algorithm (ISA) rearranges pixel data in the permutation phase. The TDA ensures modifications in plaintext are diffused thoroughly, enhancing security and efficiency. Experiments show strong resilience against attacks, establishing the method as an effective and secure digital image encryption approach.

REFERENCES

[1] J. Chen, L. Chen, L. Y. Zhang, and Z.-l. Zhu, "Medical image cipher using hierarchical diffusion and non-sequential encryption," *Nonlinear Dynamics*, vol. 96, pp. 301–322, 2019.

[2] W. Xiaofu, S. Songgeng *et al.*, "A general efficient method for chaotic signal estimation," *IEEE Transactions on signal processing*, vol. 47, no. 5, pp. 1424–1428, 1999.

[3] L. Huang, S. Cai, X. Xiong, and M. Xiao, "On symmetric color image encryption system with permutation-diffusion simultaneous operation," *Optics and Lasers in Engineering*, vol. 115, pp. 7–20, 2019.

[4] M. Abadi and D. G. Andersen, "Learning to protect communications with adversarial neural cryptography," *arXiv preprint arXiv:1610.06918*, 2016.

[5] Y. He, Y.-Q. Zhang, X. He, and X.-Y. Wang, "A new image encryption algorithm based on the of-lstms and chaotic sequences," *Scientific reports*, vol. 11, no. 1, p. 6398, 2021.

[6] C. Wei, G. Yuan, and J. Shi-Wei, "General image encryption algorithm based on deep learning compressed sensing and compound chaotic system," *Acta Physica Sinica*, vol. 69, no. 24, 2020.

[7] Z.-P. Zhao, S. Zhou, and X. Wang, "A new chaotic signal based on deep learning and its application in image encryption," *Acta Phys. Sin*, vol. 70, p. 23, 2021.

[8] A. Jolfaei, X.-W. Wu, and V. Muthukkumarasamy, "On the security of permutation-only image encryption schemes," *IEEE transactions on information forensics and security*, vol. 11, no. 2, pp. 235–246, 2015.

[9] M. A. Murillo-Escobar, C. Cruz-Hernández, F. Abundiz-Pérez, R. M. López-Gutiérrez, and O. A. Del Campo, "A rgb image encryption algorithm based on total plain image characteristics and chaos," *Signal Processing*, vol. 109, pp. 119–131, 2015.

[10] Z. Parvin, H. Seyedarabi, and M. Shamsi, "A new secure and sensitive image encryption scheme based on new substitution with chaotic function," *Multimedia Tools and Applications*, vol. 75, pp. 10 631–10 648, 2016.

[11] X. Wu, B. Zhu, Y. Hu, and Y. Ran, "A novel color image encryption scheme using rectangular transform-enhanced chaotic tent maps," *IEEE Access*, vol. 5, pp. 6429–6436, 2017.

[12] L. Li, Y. Yao, and X. Chang, "Plaintext-dependent selective image encryption scheme based on chaotic maps and dna coding," in *2017 International Conference on Dependable Systems and Their Applications (DSA)*. IEEE, 2017, pp. 57–65.

[13] H. Fan, M. Li, D. Liu, and K. An, "Cryptanalysis of a plaintext-related chaotic rgb image encryption scheme using total plain image characteristics," *Multimedia Tools and Applications*, vol. 77, pp. 20 103–20 127, 2018.

[14] B. Norouzi and S. Mirzakuchaki, "Breaking an image encryption algorithm based on the new substitution stage with chaotic functions," *Optik*, vol. 127, no. 14, pp. 5695–5701, 2016.

[15] S. Hochreiter and J. Schmidhuber, "Long short-term memory," *Neural computation*, vol. 9, no. 8, pp. 1735–1780, 1997.

[16] M. Nickparvar, "Brain tumor mri dataset," 2021. [Online]. Available: https://www.kaggle.com/dsv/2645886

[17] Y. Luo, X. Ouyang, J. Liu, and L. Cao, "An image encryption method based on elliptic curve elgamal encryption and chaotic systems," *IEEE Access*, vol. 7, pp. 38 507–38 522, 2019.

[18] X. Zhang and X. Wang, "Multiple-image encryption algorithm based on dna encoding and chaotic system," *Multimedia Tools and Applications*, vol. 78, pp. 7841–7869, 2019.

[19] N. Iqbal, M. A. Khan, and S.-W. Lee, "Multi-image cipher based on the random walk of knight in a virtual 3d chessboard," *Multimedia Tools and Applications*, pp. 1–33, 2023.

[20] Q. Lu, C. Zhu, and X. Deng, "An efficient image encryption scheme based on the lss chaotic map and single s-box," *IEEE Access*, vol. 8, pp. 25 664–25 678, 2020.

[21] S. T. Kamal, K. M. Hosny, T. M. Elgindy, M. M. Darwish, and M. M. Fouda, "A new image encryption algorithm for grey and color medical images," *IEEE Access*, vol. 9, pp. 37 855–37 865, 2021.

[22] G. Ye, H. Wu, M. Liu, and Y. Shi, "Image encryption scheme based on blind signature and an improved lorenz system," *Expert Systems with Applications*, vol. 205, p. 117709, 2022.

[23] Q. Xu, K. Sun, C. Cao, and C. Zhu, "A fast image encryption algorithm based on compressive sensing and hyperchaotic map," *Optics and Lasers in Engineering*, vol. 121, pp. 203–214, 2019.