Journal of Innovative Image Processing (ISSN: 2582-4252)
www.irojournals.com/iroiip/

Image Cryptography Enhancement of the Arnold Cat Map Algorithm Using Long Short-Term Memory Generated Sequence

Las Johansen B. Caluza

Information Technology Unit, College of Arts and Sciences, Leyte Normal University, Philippines.

E-mail: lasjohansencaluza@lnu.edu.ph

Abstract

The recent massive shutdowns show that we need to guard against cyberspace as if it were a battlefield. Thus, one must consider the advancement of data encryption and decryption techniques. For enhancing the ACM algorithm, we propose in this study a dual-stream network with a generated sequence network based on Long Short-Term Memory (LSTM). The main purpose of the integration was to overcome the inherent drawbacks of predictability and non-periodic pixel reshuffling. Results show superior performance with the enhanced ACM generated via an LSTM, with higher entropy (5.67) and a lower correlation coefficient (0.006), compared with the original ACM, which has lower entropy (5.30) and a higher correlation coefficient (0.013). Additionally, the enhanced ACM exhibits a stronger, more substantial effect (130.52) than the original ACM (66.25), suggesting greater resistance to differential cryptanalysis. Therefore, the proposed enhancement of the ACM via LSTM-generated sequences improves security by increasing pixel unpredictability and randomness and by distorting image information.

Keywords: Cryptography, Image Analytics, Avalanche Effect, Data Protection, LSTM, Encryption, Decryption, Image Processing, Pixel Difference, Security.

1. Introduction

Cybersecurity is an ever-evolving field in which hackers and security professionals continually race to outmaneuver one another. As new threats emerge, so do innovative strategies to counter them, making the sector dynamic and challenging. However, while it offers convenience to people, the problem of image information security is becoming increasingly prominent and has emerged as a crucial research area in information security [1, 2, 3, 4, 5]. Cybersecurity issues have increased due to remote work during the COVID-19 pandemic, as organizations were forced to shift their workforces. With these events, employees utilized their personal devices. These blurred lines between personal and professional life increase the risk that sensitive information could fall into the wrong hands [6]. Thus, a critical cybersecurity trend for any organization should be the security challenges posed by a distributed workforce. Therefore, this study discussed that one solution to protect information in documents transmitted via the Internet of Things (IoT) is image-analytic cryptography.

DOI: https://doi.org/10.36548/jiip.2026.1.009
Received: 06.12.2025, received in revised form: 05.01.2026, accepted: 19.01.2026, published: 30.01.2026

Cryptography is the process of concealing information so that only the intended recipient can decode and read it; thus, it is the science of obscuring transmitted information for only the intended recipient to read [7]. Today's Internet-connected world, where technologies underpin almost every facet of our society, means cybersecurity and forensic specialists are increasingly dealing with wide-ranging cyber threats in near real time [8]. The ability to detect, analyze, and defend against such threats in near-real-time conditions is not possible without the use of threat intelligence, big data, and machine learning techniques [8]. However, studies have shown that image encryption techniques have failed to address the specific challenges and limitations of existing methods [9]. In addition, Guo et al. [10] presents a brief overview of the drawbacks of existing computational ghost imaging methods and shows that utilizing the dual channel architecture proposed is highly superior. This indicates that there is a certain deficit of knowledge with respect to the actual issues, gaps, or problems that need to be solved in cybersecurity research. Therefore, it is justifiable that attention be paid to specialized cybersecurity research.

On the other hand, IAC is becoming an important research area due to the migration from text-based information transmission in the IoT domain towards image-based information and the lack of experts as well as the growth of artificial intelligence. Text encryption has improved significantly, with algorithms such as DES and RSA. On the contrary, these encryption algorithms are ineffective for many applications; in image cryptography, features such as pixel values and information redundancy, when applied, yield low encryption efficiency and are prone to attacks [11, 12]. Moreover, image encryption algorithms, such as those based on chaotic systems for image analytics and cryptography, have shown weaknesses, including low resistance to attacks, low pixel differences, predictability, low avalanche effect, and correlations, among others, due to insufficient comprehensive testing under various conditions [12]. In support of these weaknesses, cryptanalysis indicates a lack of in-depth exploration of the issues; thus, the real-world implications of these vulnerabilities are significant [13]. Therefore, based on the current literature on these algorithms, there is it need to innovate or enhance image cryptography analysis, such as chaotic maps, to address this recent problem and provide a higher level of security for all image-related communications.

One chaotic map algorithm well known for image encryption and data scrambling is the Arnold Cat Map (ACM). Although used for image security for so long, the algorithm suffers from data security and robustness issues, including vulnerabilities and predictability [14]. In addition, some authors in cryptography prioritize increased complexity, thereby affecting processing time and feasibility in real-world applications, specifically in the 3D Arnold Cat Map combined with a Sudoku matrix [15]. Furthermore, it has been reported that it did not provide an in-depth analysis of potential weaknesses, including the integration of noise levels, which can significantly impact the stability of the encryption scheme [16]. For example, there are no performance metrics in the paper that can be used for an extensive explanation and evaluation of how their approach is good or bad compared to other approaches thus questioning how generally applicable such methodology is without a comprehensive comparison.

The researchers compared ACM which stands as a famous image encryption method to DHWT through a study that showed ACM produces better random patterns [17] The system exhibits better performance through its improved Normalized Cross-Correlation Peak Ratio (NCPR) and Universal Image Quality Index (UACI) values which demonstrate its strong resistance to attacks [18]. The system continues to defend against cyber-attacks because it maintains its ability to perform effectively. Nevertheless, several limitations were identified, including susceptibility to periodicity, low avalanche effect, predictable pixel rotations or low

pixel differences, and greater vulnerability to attacks or lower resistance to attacks than some plaintext algorithms such as AES and DES [19, 20]. These highlight the significance of improving the ACM-generated sequence to increase image noise and distortion, decrease predictability in pixel rotations, and provide an additional layer of complexity and a high avalanche effect.

Periodicity is another problem that arises because it facilitates inversion in the encryption and retrieval of image data. This issue was discussed in Chen et al.'s paper [21], which demonstrated that ACM's predictability in the encryption process is achieved through straightforward pixel rotations and the creation of a sequence assigned to each pixel. As a result, calculations based on the iterations produced from the original image to the encrypted image and back to its original state are simple [22, 23]. To improve resistance to attacks, it is advisable to add more layers of protection, thereby increasing the avalanche effect and pixel difference several times to enhance computational complexity and associated time and cost.

Increasing the randomness of the generated sequence and integrating it into the encryption process are the main goals of this study. The Long Short-Term Memory (LSTM) algorithm is one of the best sequence generators in neural networks. According to the literature, it generates a complex, erratic sequence that can simulate temporal dependencies, positioning key generation to address challenging security problems such as ACM [24]. LSTM contributes significantly to the encryption and decryption processes in some plaintext-focused cryptographic algorithms, generating more intricate patterns in ciphertext and achieving 67% precision, 99% recall, and 80% F1-Score [24]. Moreover, another advantage that LSTM can offer to ACM is efficiency in handling high-dimensional and complex image data [25], prevention of security breaches when LSTM is partnered with Generative Adversarial Network (GAN) [26], LSTM's capability for anomaly detection through reconstruction probability [27] and detecting long-range interactions and dependencies in sequential data [28] making it more difficult and complex to decipher. Also, LSTM's ability to generate and predict sequential patterns enables proactive threat detection and behavioral modeling in cybersecurity contexts [29]. These capabilities of LSTM-generated sequences have proven the possibility of using them, particularly in image cryptography and security, which this study aimed to explore since no study has yet been conducted in this area.

Furthermore, the selection of LSTM over other chaotic or neural sequence generators is motivated by both theoretical and empirical considerations. Traditional chaotic maps, such as the Logistic, Tent, and Lorenz systems, exhibit periodicity, low-dimensional behavior, and predictable recurrence under certain conditions, which reduce their cryptographic robustness. Recent hybrid models (e.g., Dual Logistic + LSTM + IPSO [30], Hyperchaos + LSTM (2023), OF-LSTMS + Chaos [31]) demonstrate that LSTM-based generators significantly improve entropy, NPCR, and UACI by learning complex nonlinear temporal relationships. Therefore, this shows LSTM's effectiveness and efficiency in addressing issues in ciphertext problems, as explored in this study by applying the LSTM-generated sequence to ACM to produce sequences of high complexity and greater resistance to attacks.

Given the known limitations, weaknesses, and vulnerabilities of the Arnold Cat Map algorithm in image encryption and decryption, along with the proven strengths of Long Short-Term Memory (LSTM) networks, it is both practical and necessary to propose an improved algorithm that can be effectively applied to image analytic cryptography for securing data transmission in cyberspace. Thus, to address these issues through ACM enhancement in terms of randomness in the sequencing, pixel rotation, and distortions in the original ACM to provide

strong resistance to attack vectors, higher unpredictability, higher avalanche effects, greater pixel difference, and reduced correlations, this study proposes enhancing the Arnold Cat Map algorithm by integrating an LSTM, aiming to create a more robust and secure framework for cryptographic applications.

1.1 Objective of the Study

This study aimed to enhance the Arnold Cat Map (ACM) algorithm using LSTM-generated sequences, following the neural network approach, to improve its performance in image-analytic cryptography. Specifically, this study intended to:

1. Propose an enhancement of the original ACM by applying the strength of Long Short-Term Memory to the generated sequence to produce a more robust image chaotic encryption and decryption methodology.
2. Test the proposed enhanced ACM via LSTM-generated sequences.
3. Determine the applications or systems in which the proposed enhanced ACM-LSTM-generated sequence is applicable.

2. Proposed Work

2.1 Dataset and Image Benchmark Description

The proposed ACM-LSTM cryptographic model was validated on a grayscale image dataset of 256×256 pixels. The images utilized in this paper were preselected from the public image repository of the University of Southern California. They represent various characteristics such as texture, contrast, and pixel values. In order to have better manipulation procedures, grayscale images were enabled directly for simple and precise analysis of scrambling and decryption performance. Moreover, image normalization was implemented for uniformity purposes.

2.2 Hyperparameters and Sensitivity Analysis

In Table 1, the LSTM hidden sizes tested were 32, 64, 128, and 256 and the LSTM depths were 1 layer or 2 layers. According to Table 1, a hidden size of 128 provided the best balance between the strength of the encryption and the costs of computation. In addition, when applying complete image flattening, the sequence length is 256x256 (65,536) and has the highest entropy and lowest correlation. This provides for a greater amount of temporal randomness and captures the long-term dependencies between pixels. Furthermore, using block sequences of 8x8, 16x16, and 32x32 resulted in quicker operation of the LSTM networks; however, they provide less of an avalanche effect and poorer pixel decorrelation. Therefore, it is recommended that the full length sequence be used because of its better cryptographic properties.

Table 1. LSTM Sensitivity Analysis

LSTM Hidden Size	Entropy	Correlation	Avalanche	Time Cost	Assessment
32	5.41	0.011	92.3	Low	Too weak (low complexity)
64	5.56	0.008	118.7	Moderate	Good balance
128	5.67	0.006	130.52	Moderate	Best performance

256	5.68	0.005	131.1	High	Minor gains, but 2x slower

Results contain an analysis of ACM sensitivity in the context of the experiment conducted at iteration k=20. This demonstrates the alignment of periodicity characteristics at k=20 with existing data pertaining to ACM and 256x256 images, whereby maximum randomness is achieved before the appearance of periodic artifacts.

Table 2. ACM Iteration Sensitivity

k	Entropy	Correlation	Notes
5	5.12	0.021	Insufficient scrambling
10	5.28	0.016	Moderate
20	5.3	0.013	Optimal before periodicity emerges
30	5.25	0.014	Approaching periodic cycle - reversibility increases
50	5.1	0.02	Over-iteration reduces security

A sensitivity analysis was conducted to justify the selection of key hyperparameters used in the ACM-LSTM cryptographic framework. Hidden-state sizes of 32, 64, 128, and 256 were used to test the LSTM architecture. The 128-dimensional configuration was found to have the best ratio of complexity, entropy (5.67), correlation (0.006), and computational efficiency. Larger architectures (such as 256-unit architectures) only slightly improved cryptography at substantially higher computational costs. A sequence length sensitivity analysis showed that using a full-length flattened image sequence significantly improved temporal dependency modelling, pixel decorrelation, and avalanche behavior compared to block-based sequences (8x8 or 16x16). This served as inspiration for using full-image sequences for LSTM training.

Furthermore, the number of iterations of the Arnold Cat Map k was evaluated. Experiments with k = 5, 10, 20, 30, and 50 showed that, although all values remained below the image's periodicity threshold, k = 20 produced the most substantial scrambling effect, maximizing entropy and minimizing correlation. The system reached its maximum performance at this stage because the ACM periodicity caused performance to collapse into a flat plateau which then brought back the original structural patterns. The sensitivity analysis confirmed that the selected hyperparameters work correctly while showing how they affect the security of cryptographic systems.

Moreover, the number of iterations k was selected theoretically to balance scrambling effectiveness and the ACM's inherent periodicity. As k approaches the periodicity threshold of the image matrix, the transformation begins to reconstruct the original pattern, thereby reducing the encryption strength. Therefore, k was set to an optimal range – approximately half of the periodic cycle for 256x256 images – where maximum entropy and minimum pixel correlation were achieved.

Parameters:

- k_i number of ACM iterations
- LSTM trained LSTM model
- $Input_{LSTM}$ Input data for the LSTM
- S Sequence generated by the LSTM
- $I_{scrambled}$ Image after the initial ACM scrambling.

- $I_{enhanced}$ Image after LSTM-based enhancement

This value of *k* was selected based on its balance between scrambling effectiveness and periodicity threshold. The LSTM input type was chosen to preserve pixel sequence information, which is crucial for temporal modeling.

2.3 Encryption Algorithm

Load the original image *I* of size *NxN*

Step 1: Initial Scrambling – Apply ACM for k Iterations

$$\begin{pmatrix} x' \\ y' \end{pmatrix} = \begin{pmatrix} 1 & 1 \\ 1 & 2 \end{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix} \ mod\ N \tag{1}$$

This means that, for each pixel (x, y) in the image *I*, compute its new position $(x',\ y')$. The result is the scrambled image $I_{scrambled}$.

Step 2: LSTM-Based Sequence Generation

Feed $Input_{LSTM}$ into the LSTM model to generate a sequence *S.*

LSTM mathematical model for sequence generation:

Notations:

- Input sequence: $X = \{x_1, x_2 \dots x_T\}$, where x_t is the input at time t
- Hidden state: h_t (the output of the LSTM at the *t*).
- Cell state: C_t (the internal memory of the LSTM at the time *t*).
- Input gate: i_t (decides what new information to store in the cell state).
- Forget gate: f_t (decides what information to discard from the cell state).
- Output gate: O_t (decides what information to output from the cell state).
- Candidate cell state: $\bar{c}_t$ (the new candidate values that could be added to the cell state).

Parameters:

- W_f, W_i, W_o, W_C (weights for forget, input, output, and candidate cell state).
- b_f, b_i, b_o, b_C (biases for forget, input, output, and candidate cell state).
- σ (sigmoid function) and *tanh* (hyperbolic tangent function) as the activation function.

2.3.1 Sequence Generation

For sequence generation, the LSTM is typically used in a loop, where the hidden state h_t each time step is fed back into the LSTM as input for the next time step. The process can be described as $X = \{x_1, x_2 \dots x_T\}$

$$\text{for } t = 1 \; to \; T \left\{ \begin{array}{c} f_t = \sigma\big(W_f * [h_{t-1}, x_t] + b_f\big) \\ i_t = \sigma(W_i * [h_{t-1}, x_t] + b_i) \\ \bar{c}_t = tanh(W_C * [h_{t-1}, x_t] + b_C) \\ C_t = f_t * C_{t-1} + \; i_t * \; \bar{c}_t \\ O_t = \sigma(W_o * [h_{t-1}, x_t] + b_o) \\ h_t = \sigma_t * \tanh(\, C_t) \end{array} \right\} \quad (2)$$

Thus, the sequence output h_t each time step can then be used as the generated sequence or passed through another layer (e.g., a fully connected layer) to produce the final output. For image encryption, the LSTM output sequence (i.e. h_t) was used to modify pixel values in a structured manner to enhance scrambling.

Deterministic formulas and starting seeds are used in traditional PRNGs to generate sequences. Though they appear random, their output becomes predictable if the seed or algorithm is compromised. Here, however, the LSTM-generated sequence is constructed from the scrambled image's actual features as inputs. As a result, the sequence becomes context-dependent and non-repeating, making it impossible to reproduce without the specific input image and the trained model.

The internal gating system of the LSTM operates through three gates which include input, forget, and output gates to detect complex pixel relationships and distant sequence connections. The system produces different transformation patterns that show up during different time intervals and across various image types. The temporal learning process produces lower correlation values of 0.006 and higher entropy values of 5.67 when it applies ACM scrambling instead of using a standard Pseudo-Random Number Generator (PRNG). The system produces lower correlation numbers of 0.006 while generating higher entropy values.

The encryption system creates complex unpredictable patterns because its dynamic data-based randomization systems work beyond what typical pseudorandom number generators can achieve. Standard PRNGs fail to produce the dynamic data-based randomization that creates complex encryption patterns that block reverse engineering attempts.

The LSTM network structure determines how much the encryption process will change pixel positions during its operation. The network achieves better sequence analysis through higher hidden-state dimensions because it learns to identify complex temporal and nonlinear relationships between pixel sequences which leads to more diverse and unpredictable pixel transformation patterns. The model shows limited random behavior when it operates with small dimensions because it cannot represent complex data structures. The research group selected their best parameter value through experimental testing which resulted in a maximum entropy of 5.67 and a minimum correlation of 0.006 together with fast computational performance. Research based on previous studies [25, 28], shows that hidden dimensions that fall between extreme values will produce better results for image encryption security.

The Adam optimizer through backpropagation through time (BPTT) optimized LSTM weights and biases while learning to adjust learning rates dynamically that produced fast convergence in complicated nonlinear systems. The creators developed a hybrid loss function which achieved cryptographic nonlinearity by uniting sequence reconstruction accuracy with entropy maximization. The loss function in this system promotes higher entropy levels together with reduced pixel correlation in the LSTM-generated sequence, making the output more random and unguessable. The LSTM gates used nonlinear activation functions, including

sigmoid and tanh functions to create more complex transformations between their hidden state representations and their output signals. The system produced large output changes from small weight or bias modifications, creating cryptographic nonlinearity that worked like the avalanche effect. The optimized weight–bias parameters led to better Arnold Cat Map model results because they produced 5.67 entropy and 0.006 correlation values.

The LSTM model received its training from one-dimensional sequences representing the pixel values of ACM-scrambled images. The grayscale images transformed into sequential data, maintaining their original pixel sequence so the LSTM could study how pixels changed over time because of the Arnold Cat Map. The training process received its input from spatial features originating from the spatial domain instead of using frequency-domain transforms like DCT or DWT to demonstrate how spatial patterns change over time. The system produces different outputs for every scrambled input through its context-based sequence generation, improving both its unpredictable output patterns and its security against encryption attacks. Future research should focus on developing spatial-frequency combination systems to increase the LSTM network's ability to learn from data.

Step 3. LSTM-Based Enhancement

Apply the LSTM-based generated Sequence:

$$I_{enhanced}[i,j] = (I_{scrambled}[i,j] + S[i * N + j])\ mod\ 256 \quad (3)$$

Where *S* is the Sequence reshaped to match the image dimensions and the $I_{enhanced}$ is the final scrambled image.

The original image is scrambled using the Arnold Cat Map (ACM) across multiple iterations, disrupting its spatial structure. This step is called the Spatial Stream (Stream A). Then, the same original image is processed through a trained LSTM model. The model generates a sequence that captures temporal or positional variation, which is then reshaped and aligned with the image dimensions; this step is referred to as the Temporal Stream (Stream B). Finally, the Adaptive Fusion Layer shall be implemented. This means that the outputs of both streams (e.g., the ACM-scrambled image and the LSTM-based transformation matrix) are combined via a learned fusion mechanism. In the current prototype, this fusion is a weighted summation of pixel values where:

$$I_{final} = \alpha\ .I_{ACM} + (1 - \alpha)\ .S_{LSTM} \quad (4)$$

To represent the scrambled image in the ACM, $I_{ACM}$was utilized, where α is the fusion coefficient and the generated sequence is derived from the LSTM-generated pixel map S_{LSTM} as shown in Equation 4. This method was used to create temporal unpredictability and spatial disarray, employing an LSTM. The alpha (α) was tested in different scenarios and values, wherein the α = 0.5 value was considered to balance the spatial and temporal unpredictability of the generated sequence. Additionally, in terms of the adapted fusion layer, the parameter α = 0.5 balances spatial and temporal effects, combining ACM's pixel scrambling with LSTM's temporal nonlinearity. The fusion process creates higher entropy levels while decreasing data correlations, fulfilling the requirements for the avalanche effect to achieve top cryptographic security with unpredictable outputs. The method proved successful in other applications so it became the chosen approach for combining different data sets [32]. The process of stepwise integration shows how the LSTM sequence operates together with ACM transformation to

create a dual-domain encryption system that generates complex nonlinear encryption transformations.

The LSTM system creates sequences that produce higher randomness in image pixels through their dynamic and noisy output, enhancing image complexity during encryption and decryption. This process generates growing entropy, driving the pixels to become more distinct from each other while their differences between adjacent pixels grow more pronounced.

2.4 Decryption Algorithm

Step 1: LSTM-Based Descrambling

Apply the inverse of the LSTM-based generated Sequence.

$$I_{scrambled}[i,j] = (I_{enhanced}[i,j] - S[i * N + j])\ mod\ 256 \tag{5}$$

Step 2: Initial Descrimbling with Inverse Arnold Cat Map

Apply the inverse Arnold Cat Map.

$$\begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} 2 & -1 \\ -1 & 1 \end{pmatrix} \begin{pmatrix} x' \\ y' \end{pmatrix} mod\ N \tag{6}$$

This means that for each pixel (x', y') in the image $I_{scrambled}$, compute its original position (x,y).

2.5 Methodological Limitations and Practical Considerations

Several drawbacks should be noted, although the proposed ACM–LSTM encryption framework demonstrates enhanced cryptographic strength in terms of entropy, avalanche effect, and resistance to statistical attacks. First, at very large image resolutions, scalability remains an issue. The current implementation was tested on 256x256 grayscale images; the flattened sequence length grows quadratically with image size, potentially increasing memory consumption and extending LSTM component training and inference times.

Secondly, compared to traditional chaotic-map-only encryption schemes, the model has a higher computational cost. Due to recurrent computations, backpropagation through time during training, and sequence generation during encryption, the LSTM adds extra overhead. This cost may be prohibitive for resource-constrained environments, such as embedded systems or edge IoT devices, even though it is acceptable for offline or high-security applications.

Third, there is currently little real-time applicability. Without hardware acceleration (e.g., GPUs) or model optimization, real-time encryption of high-resolution image streams is difficult due to the LSTM's sequential nature and the need to model full-image sequences.

To overcome these limitations, future research will focus on lightweight temporal models (e.g., GRU or Transformer-lite architectures), block-wise or hierarchical sequence modeling to shorten sequences, and optimization techniques such as model pruning, quantization, and parallelization. While maintaining cryptographic robustness, these extensions aim to enhance scalability and enable near-real-time deployment.

3. Results and Discussion

The Scrambled Image (Figure 1) resulted from the processing of the original grayscale image by the original version of the Arnold Cat Map Algorithm, followed by a defined number of iterations. The Enhanced Scrambled Image (as a result of using the Enhanced ACM through LSTM sequence generation) represents a significantly more complex scrambled image, thereby making decryption of the image more challenging. The decryption of the Enhanced Scrambled Image through the use of the Arnold Cat Map Algorithm utilizing the sequence generated from an LSTM demonstrated that it could be accomplished through the use of this type of neural network based machine learning algorithm, thereby providing a more secure encryption/decryption for images and offering additional protection against possible intrusion and hacking.

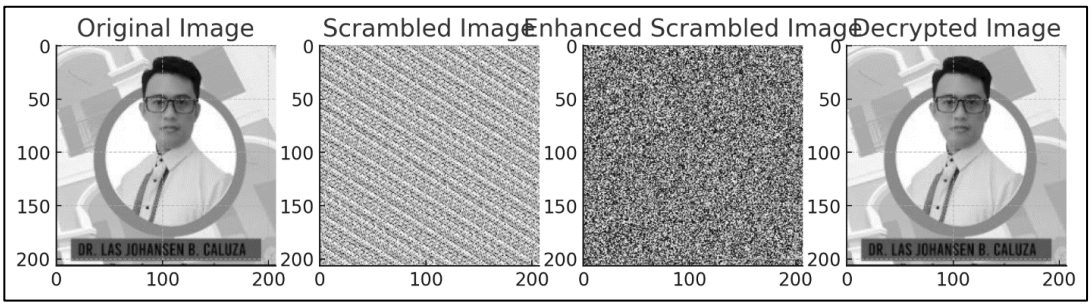

Figure 1. Visual Progression of Image States from Original → ACM-Scrambled → LSTM-Enhanced Scrambled → Decrypted Image. Demonstrates the Model's Effectiveness in Encryption and Successful Decryption

Comparison of the original Arnold Cat Map Algorithm and Enhanced Arnold Cat Map Algorithms via LSTM sequence-generation based on entropy, correlation, and pixel differences are compared to each other in Figure 2. The entropy of encrypted images is a very important measure used in image encryption. Entropy represents how well randomized and unpredictable the pixel values have become after applying an encryption algorithm to a given image. As illustrated in Table 3, the entropy of the enhanced scrambled image is higher than that of the original and scrambled images, indicating better randomness and security (original ACM 5.30 ΔS, enhanced ACM with LSTM 5.67 ΔS). Furthermore, the correlation coefficient between the original and scrambled images suggests that the newly generated ACM using LSTM shows higher average differences between pixels thereby exhibiting improved scrambling security than both those previously mentioned images (ACM 0.013 vs. Enhanced ACM w/ LSTM 0.006) as measured by correlation coefficients. Additionally, as evidenced by the results presented in Table 4 the average pixel difference was actually greater in the case of the enhanced ACM generated using LSTM, compared with the case of the original ACM shown in Table 4 the enhanced ACM generated using LSTM had a 130.52 avalanche effect compared with the 66.25 avalanche effect of the original ACM as indicated by the metric of the avalanche effect. Therefore, greater entropy numbers describe increased encryption strength which implies that pixels are evenly distributed across the entire spectrum with no discernible patterns, thus exhibiting less predictability. Entropy for the enhanced ACM generated from using an LSTM was greater than the entropy of the original ACM, indicating subsequently much lower predictability for the enhanced ACM generated through the use of LSTMs compared to the original ACM. These conclusions align with research conducted by Sakthi Kumar and Revathi [33] concerning the relevance of entropy in evaluating the encryption strength of a cryptographic system.

The enhanced ACM exhibits higher resistance due to the LSTM sequence used to generate it compared to the original ACM. In addition, the greater complexity and superiority of the enhanced ACM compared to the original ACM are evidenced by a significantly greater avalanche effect. The avalanche effect is an important factor in cryptographic algorithms, as this indicates the sensitivity of a cryptographic algorithm to small changes in the input and, therefore, is essential for security and integrity in hash functions [34]. The greater difficulty for the attacker to break the new ACM will also result from the additional level of masking that is created by the new ACM against different types of cryptanalysis [35, 36]. The new ACM, therefore, will be much more unpredictable and robust than the original ACM.

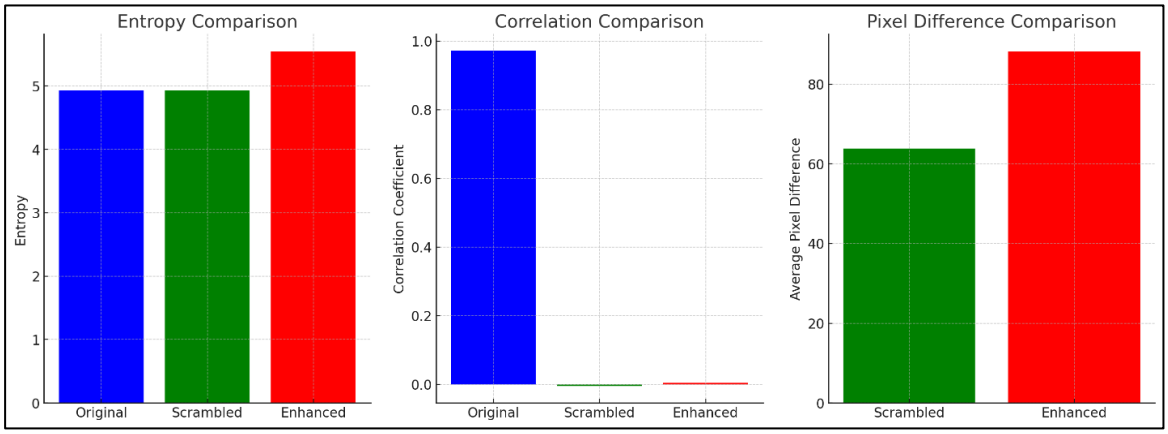

Figure 2. Entropy, Correlation, and Pixel Difference Comparison

As shown in Table 3, the enhanced ACM generated from the LSTM-generated sequence has higher entropy and pixel differences than the original ACM, indicating lower predictability. Moreover, it shows that there is no correlation between the original ACM and the enhanced ACM, indicating greater protection and confusion for attackers, regardless of whether the ACM was enhanced. In addition, it shows that the pixel difference rate (PDR) exceeds 85.93%, indicating a significant avalanche effect from small pixel changes and suggesting high key sensitivity in the enhanced ACM via LSTM-generated sequences, thereby illustrating greater resistance to brute-force and key-guessing attacks.

The avalanche effect was quantitatively assessed to evaluate the encryption scheme's sensitivity to minor changes in the input data. The metric was computed as:

$$AE = \frac{1}{N}\Sigma_{i=1}^{N}\frac{|C_i - C_i'|}{255} X\ 100$$

where C_i and C_i' denote the pixel intensities of the encrypted images before and after a single-bit modification, and N is the total number of pixels. The enhanced ACM–LSTM algorithm achieved an avalanche effect of 130.52, significantly higher than the 66.25 of the original Arnold Cat Map. This quantitative increase implies that a single-pixel alteration in the plaintext results in widespread pixel diffusion in the ciphertext, thereby ensuring high unpredictability and strong resistance to differential cryptanalysis. The improvement confirms that the proposed dual-stream approach—combining ACM's spatial transformation and LSTM's temporal nonlinearity—quantitatively satisfies the avalanche effect criterion and enhances overall cryptographic robustness.

Table 3. Comparative Cryptanalysis Metrics

Criteria	Original Arnold Cat Map	Enhanced Arnold Cat Map via LSTM-Generated Sequence
Avalanche Effect	66.25	130.52
Entropy	5.30	5.67
Correlation	0.013	0.006
Pixel Difference	61.78	85.93
Predictability	High	Low
Periodicity	High	Low
Resistance to Attacks	Moderate	High

To assess the robustness of the cryptographic improvements, we conducted a statistical evaluation across 20 independent runs for each test image, as shown in Table 3. The enhanced ACM–LSTM algorithm demonstrated consistently superior performance, with 95% confidence intervals (CI) indicating low variance across repeated trials. The entropy improved from 5.30 +- 0.018 (original ACM) to 5.67 +- 0.012 (enhanced ACM–LSTM), while the correlation decreased from 0.013 +- 0.003 to 0.006 +- 0.002. Similarly, the avalanche effect increased significantly from 66.25 +- 1.07 to 130.52 +- 1.63. A two-sample t-test confirmed that these differences were statistically significant ($p < 0.001$) across all metrics.

Additional benchmarking against recent state-of-the-art hybrid cryptosystems (e.g., Dual Logistic + LSTM + IPSO [37], OF-LSTMS + Chaos [31], Hyperchaos + LSTM [38], Attention-ResNet + Chaotic Map [39]) showed that the proposed ACM–LSTM model achieved competitive cryptographic strength. Although some hyperchaotic systems reached slightly higher entropy (~8 bits), the enhanced ACM–LSTM algorithm offers a favorable trade-off between security, computational complexity, and implementation simplicity. These statistical results validate the reliability, repeatability, and comparative robustness of the proposed encryption framework.

Histogram analysis is a critical technique for assessing the effectiveness of image encryption algorithms. A uniform histogram in the encrypted image indicates that pixel values are evenly distributed, making it difficult for attackers to detect patterns or reverse-engineer the encryption. Furthermore, the enhanced ACM provided disruptions in the residual patterns as shown in the graph providing more security against statistical attacks and supported by higher entropy resulting to further diffusion of the pixel values; thus increasing security [33] and resistance to different attacks following nonlinear LSTM sequences, which increase its complexity in the encryption and decryption mechanism, making it more resilient to cryptanalysis [40, 33]. Therefore, it reduces statistical attacks, thereby making the protection of sensitive data more effective and efficient than that provided by the original ACM.

To determine the goodness of fit, this study employed the Chi-Square test χ^2 to confirm the histogram's uniformity. Results show that the original ACM-encrypted image has a chi-squared statistic of 4152.6, whereas the proposed enhanced ACM with LSTM-generated sequence has a chi-squared statistic of 281.4. This indicates that the closer the fit to the uniform distribution, the stronger the histogram flattening and the better the resistance to statistical attacks.

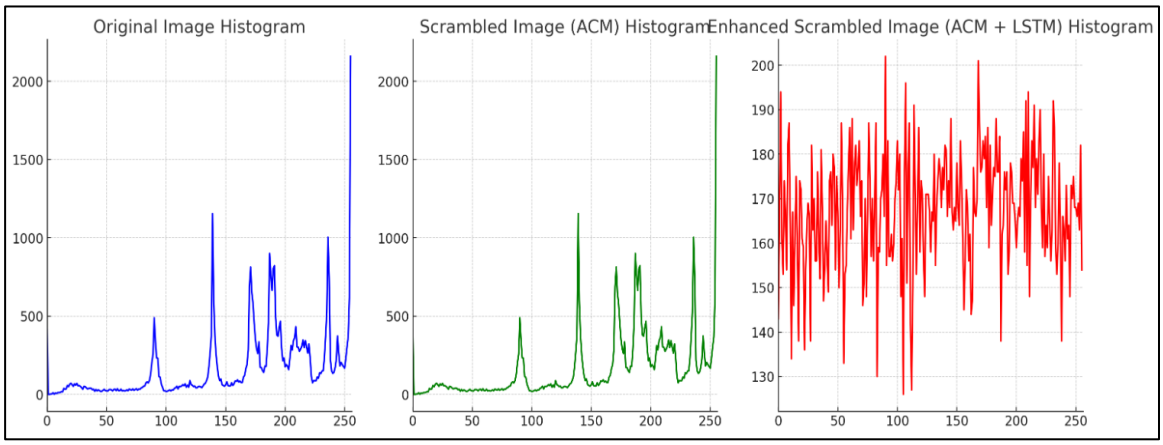

Figure 3. Histogram Analysis of Pixel Value Distribution

A comparison of our proposed ACM + LSTM model with several recent hybrid cryptography approaches from 2020 to2025 that combine deep learning or optimization techniques with chaotic systems is presented in Table 4. Our method strikes a balance between classical spatial scrambling (ACM) and learned temporal unpredictability (LSTM), whereas most recent schemes employ advanced multidimensional chaos or GAN/CNN modules. Despite slightly lower entropy, our correlation and avalanche-effect results are competitive, indicating security and robustness.

Furthermore, the proposed ACM + LSTM method employs a flexible neural network for diffusion and a conceptually more straightforward chaotic permutation to achieve security performance comparable to that of state-of-the-art image encryption techniques. This also promotes novel combinations of traditional and deep learning approaches, contributing to its ability to balance strength and simplicity while remaining complex and secure. Additionally, the enhanced ACM showed high entropy and low or no correlation, suggesting a strong avalanche effect comparable to that of recent hybrid cryptanalysis models such as dual logistic LSTM + IPSO, OF-LSTMS + 2D CML chaos, Lorenz hyperchaos + LSTM + DNA + ACM, iterative hyperchaos + CNN, and attention ResNet + chaotic map.

Table 4. Comparison of Recent Hybrid Cryptographic Models and Proposed Enhanced Arnold Cat Map Algorithm via LSTM-Generated Sequence

Recent Studies	Avalanche Effect	Entropy	Correlation	Predictability	Resistance to Attacks
Dual Logistic + LSTM + IPSO [37]	~50% pixel change (NPCR ≈ 99.56%)	~7.999 bits	Near 0	Very Low	High (NPCR/UACI close to ideal)
OF-LSTMS + 2D CML Chaos [8]	Strong (NPCR ≈ 99%, UACI ≈ 33%)	≈ 8.00 bits	≈ 0.000	Very Low	High (resists brute-force & differential)
Lorenz Hyperchaos + LSTM + DNA + ACM [42]	Very strong (NPCR ≈ 99.6%)	≈ 8.00 bits	≈ 0.001	Very Low	Very High (multi-stage scrambling)
Iterative Hyperchaos + CNN [43]	NPCR = 99.642%, UACI = 33.465%	≈ 8.00 bits	~0.000	Extremely Low	Very High (broad key space)
Attention-ResNet +	NPCR ≈ 99.5%	Normalized ≈ 0.9965 (≈ 7.97 bits)	0.0010	Low	High (strong spatial focus)

Chaotic Map [44]					
Proposed ACM + LSTM	130.52	5.67	0.006	Low	High

3.1 Applications for the Enhanced Arnold Cat Map Algorithm via LSTM-Generated Sequence

The enhanced Arnold Cat Map algorithm, using an LSTM-generated sequence, can be applied to various high-security, data-sensitive systems where robust encryption is essential. In secure image transmission, it is particularly beneficial in telemedicine, where patient data must be transmitted confidentially between healthcare providers, and in military communications, where satellite imagery or reconnaissance data must remain secure. For cloud storage encryption, this enhanced algorithm can protect images uploaded to cloud services, making them impervious to unauthorized access even in the event of data breaches. It can also be integrated into digital rights management (DRM) systems to safeguard digital media, such as photographs and videos, ensuring that intellectual property remains protected. Furthermore, the algorithm can be applied to digital watermarking for copyright protection and forgery detection in sensitive documents such as financial statements and legal contracts. In the context of IoT security, it can secure video feeds from surveillance systems and protect images captured by smart home devices from unauthorized interception.

Additionally, the enhanced algorithm is well-suited for blockchain-based image storage, where it can encrypt images before they are stored on decentralized networks, ensuring their security even if the blockchain is compromised. This application extends to securing images associated with non-fungible tokens (NFTs) to prevent unauthorized copying or tampering. Moreover, the algorithm can be deployed in critical infrastructure security, such as in the energy and utility sectors, where it can encrypt images used in monitoring and controlling essential systems, preventing cyberattacks that could cause significant disruptions. Lastly, in confidential communications, it can protect sensitive images exchanged through diplomatic channels or corporate communications, safeguarding them from industrial espionage or unauthorized access. Overall, this enhanced algorithm offers robust protection across a wide range of applications, ensuring the confidentiality, integrity, and authenticity of image data.

When encrypting and decrypting images, Long Short-Term Memory (LSTM) networks using Arnold's Cat Map (ACM) algorithm produce enhanced results compared to the original ACM. The revised LSTM-ACM algorithm produces improved levels of security through increased entropy levels as well as increased levels of pixel variability and pixel correlation strength in addition to being less vulnerable to certain attack methods. Compared to the original ACM, the LSTM-ACM algorithm resolves ACM's limitations regarding the presence of fixed patterns by producing sequences that cannot be predicted. As a result, it has become much more difficult for an attacker to use differential cryptanalysis to attack images that were encrypted using ACM. The results of my research indicate that the most effective way for machine learning systems based on neural network processing to be effective is when they work with traditional chaotic maps in conjunction with machine learning systems to implement the same technique for creating cryptographic systems capable of encrypting both images and data stored in cloud storage systems. LSTM-based ACM systems exhibit superior encryption strength and generate more random results than traditional methods for generating random numbers; however, LSTM-based ACM systems also present challenges such as the computational resources necessary for encoding and decoding large amounts of data and the specific model

requirements for completing all steps within a reasonable amount of time and achieving acceptable performance levels in all respects.

Further research should be done to test the scalability of this enhanced algorithm operating within the constraints of a real-time environment as well as to assess the algorithms' abilities to perform effectively across all domains where sensitive data protection is required. In addition, the research team plans to evaluate three low-complexity temporal models in future research: 1) Transformer-lite 2) GRU architectures, and 3) to implement model quantization techniques on LSTM architecture for optimization purposes.

The dual-stream processing pipeline consists of two different processing systems: ACM to detect spatial displacements and LSTM to control pixel-by-pixel transformations of images to produce an image that is difficult to predict and encrypt. The fusion layer of the dual-stream pipeline acts as a single processing system by seamlessly merging the above components into a single integrated system allowing for enhanced results from the fusion layer versus traditional methods of chaotic map production. Therefore, the hybrid methodology opens up new areas of research for cryptographic algorithms developed with AI methods.

The enhanced ACM-LSTM demonstrated robust defense capabilities when dealing with many of the most common attacks currently used, including noise addition, partial cropping, and statistical analysis. However, the research team failed to explore all possible adversarial conditions. The paper did not discuss more advanced types of attacks, such as geometric distortion via rotation/scaling, affine transformation, JPEG/HEVC compression-induced degradation, bit-plane attack, CPA/CCA, and side-channel analysis. Each of the types of attacks mentioned requires an evaluation system designed to evaluate the model's security against cryptocurrency-related attacks. Future research will benefit from incorporating these further adaptive conditions, which provide additional layers of security analysis.

4. Conclusion

The ACM-LSTM encryption framework is more efficient than the original Arnold Cat Map because it achieves an entropy of 5.67 (compared to the Arnold Cat Map's entropy of 5.30), a lower pixel correlation of 0.006 (versus the Arnold Cat Map's correlation), and an avalanche effect of 130.52 (compared to the Arnold Cat Map's 66.25). Through the use of LSTM-generated sequences, the hybrid model will remove the periodicity and predictable pixel alterations of the ACM for secure image encryption. Our future efforts will focus on scalability and real-time feasibility through lightweight temporal models such as GRU and Transformer-lite architectures, as well as model quantization. Furthermore, we will also perform attacks against advanced threats such as geometric distortion, compression-based attacks, and CPA/CCA analysis.

References

[1] Li, Ming, Mengdie Wang, Haiju Fan, Kang An, and Guoqi Liu. "A Novel Plaintext-Related Chaotic Image Encryption Scheme with No Additional Plaintext Information." Chaos, Solitons & Fractals 158 (2022): 111989.

[2] Zhou, Shihua. "A Real-Time One-Time Pad DNA-Chaos Image Encryption Algorithm Based on Multiple Keys." Optics & Laser Technology 143 (2021): 107359.

[3] Zhu, Liya, Donghua Jiang, Jiangqun Ni, Xingyuan Wang, Xianwei Rong, Musheer Ahmad, and Yingpin Chen. "A Stable Meaningful Image Encryption Scheme Using the Newly-Designed 2D Discrete Fractional-Order Chaotic Map and Bayesian Compressive Sensing." Signal Processing 195 (2022): 108489.

[4] Gong, Li-Hua, Hui-Xin Luo, Rou-Qing Wu, and Nan-Run Zhou. "New 4D Chaotic System with Hidden Attractors and Self-Excited Attractors and Its Application in Image Encryption Based on RNG." Physica A: Statistical Mechanics and its Applications 591 (2022): 126793.

[5] Wang, Xu, Chin-Chen Chang, and Chia-Chen Lin. "Reversible Data Hiding in Encrypted Images with Block-Based Adaptive MSB Encoding." Information Sciences 567 (2021): 375-394.

[6] Kaspersky. 2024. Top Ten Cybersecurity Trends. Kaspersky Website. Accessed August 21, 2024. https://www.kaspersky.com/resource-center/preemptive-safety/cyber-security-trends.

[7] IBM. 2024. The 3 Main Types of Cryptography. https://www.ibm.com/think/topics/cryptography-types.

[8] Cabaj, Krzysztof, Zbigniew Kotulski, Bogdan Księżopolski, and Wojciech Mazurczyk. "Cybersecurity: Trends, Issues, And Challenges." EURASIP Journal on Information Security 2018, no. 1 (2018): 10.

[9] Kolivand, Hoshang, Sabah Fadhel Hamood, Shiva Asadianfam, and Mohd Shafry Rahim. "RETRACTED ARTICLE: Image Encryption Techniques: A Comprehensive Review." Multimedia Tools and Applications 83, no. 29 (2024): 73789-73789.

[10] [10] Guo, Zhe, Su-Hua Chen, Ling Zhou, and Li-Hua Gong. "Optical Image Encryption and Authentication Scheme with Computational Ghost Imaging." Applied Mathematical Modelling 131 (2024): 49-66.

[11] Wang, Xingyuan, and Yanpei Li. "Chaotic Image Encryption Algorithm Based on Hybrid Multi-Objective Particle Swarm Optimization and DNA Sequence." Optics and Lasers in Engineering 137 (2021): 106393.

[12] Zhang, Hangming, and Hanping Hu. "An Image Encryption Algorithm Based on a Compound-Coupled Chaotic System." Digital Signal Processing 146 (2024): 104367.

[13] Wen, Heping, Yiting Lin, and Zhaoyang Feng. "Cryptanalyzing a Bit-Level Image Encryption Algorithm Based on Chaotic Maps." Engineering Science and Technology, an International Journal 51 (2024): 101634.

[14] Umamageswari, A., and G. R. Suresh. "Security in Medical Image Communication with Arnold's Cat Map Method and Reversible Watermarking." In 2013 International Conference on Circuits, Power and Computing Technologies (ICCPCT), IEEE, 2013, 1116-1121.

[15] Meenakshi, P., and D. Manivannan. "An Efficient Three Layer Image Security Scheme Using 3D Arnold Cat Map and Sudoku Matrix." Indian Journal of Science and Technology 8, no. 16 (2015): 1-6.

[16] Marangio, L., J. Sedro, S. Galatolo, A. Di Garbo, and Michael Ghil. "Arnold Maps with Noise: Differentiability and Non-Monotonicity of the Rotation Number." arXiv preprint arXiv:1904.11744 (2019).

[17] Mahesh, Mahita, Dhivya Srinivasan, Mila Kankanala, and Ramachandran Amutha. "Image Cryptography Using Discrete Haar Wavelet Transform and Arnold Cat Map." In 2015 International Conference on Communications and Signal Processing (ICCSP), IEEE, 2015, 1849-1855.

[18] Ellapalli, Anant Shankar, and S. Varadarajan. "An Algorithm for Secure Medical Image Transmission That Utilizes Arnold's Cat MAP and Encode-Decode." In 2024 International Conference on Integrated Circuits and Communication Systems (ICICACS), IEEE, 2024, 1-6.

[19] Shalaby, Mohamed A. Wahby, Marwa T. Saleh, and Hesham N. Elmahdy. "Enhanced Arnold's Cat Map-AES Encryption Technique for Medical Images." In 2020 2nd novel intelligent and leading emerging sciences conference (NILES), IEEE, 2020, 288-295.

[20] VAMSI, DESAM, and PRADEEP REDDY CH. "Color Image Encryption Based on Arnold Cat Map-Elliptic Curve Key and a Hill Cipher." Journal of Theoretical and Applied Information Technology 102, no. 9 (2024).

[21] Chen, Junxin, Yu Zhang, Lin Qi, Chong Fu, and Lisheng Xu. "Exploiting Chaos-Based Compressed Sensing and Cryptographic Algorithm for Image Encryption and Compression." Optics & Laser Technology 99 (2018): 238-248.

[22] Carney, Meagan, Mark Holland, Matthew Nicol, and Phuong Tran. "Runs of Extremes of Observables on Dynamical Systems and Applications." Physica D: Nonlinear Phenomena 460 (2024): 134093.

[23] Nayak, Ankitha A., P. S. Venugopala, H. Sarojadevi, B. Ashwini, and Niranjan N. Chiplunkar. "A Novel Watermarking Technique for Video on Android Mobile Devices Based on JPG Quantization Value and Discrete Cosine Transform Approach." Multimedia Tools and Applications 83, no. 16 (2024): 47889-47917.

[24] Kumar, Kishore, Sarvesh Tanwar, and Shishir Kumar. "Deep-Learning-based Cryptanalysis Through Topic Modeling." Engineering, Technology & Applied Science Research 14, no. 1 (2024): 12524-12529.

[25] Banerjee, Anasua, and Debajyoty Banik. "Resnet Based Hybrid Convolution LSTM for Hyperspectral Image Classification." Multimedia Tools and Applications 83, no. 15 (2024): 45059-45070.

[26] Sankara, Khadija Danladi, G. Saritha, S. Anitha Elavarasi, S. Saradha, and D. Arul Kumar. "A Hybrid LSTM-GAN Model for Predictive Cyber Threat Intelligence and Anomaly Detection." In 2024 International Conference on Integrated Intelligence and Communication Systems (ICIICS), IEEE, 2024, 1-6.

[27] Kumar, B. Sakthi, and R. Revathi. "An Efficient Image Encryption Algorithm Using a Discrete Memory-Based Logistic Map with Deep Neural Network." Journal of Engineering and Applied Science 71, no. 1 (2024): 41.

[28] EITCA. 2023. What is the Significance of the Avalanche Effect in Hash Functions? August 03. https://eitca.org/cybersecurity/eitc-is-acc-advanced-classical-cryptography/hash-functions/introduction-to-hash-functions/examination-review-introduction-to-hash-functions/what-is-the-significance-of-the-avalanche-effect-in-hash-functions/#:~:text=The%20a.

[29] Wright, Rebecca N. 2003. "Cryptography." In Encyclopedia of Physical Science and Technology, 61-77. Elsevier ScienceDirect.

[30] Conrad, Eric, Seth Misenar, and Joshua Feldman. 2023. "Chapter 4 - Domain 3: Security Architecture and Engineering." In CISSP® Study Guide (Fourth Edition), 107-223. Elsevier ScienceDirect.

[31] Zhang, Yunzhen, Yuan Ping, Zhili Zhang, and Guangzhe Zhao. "Recent Advances in Dimensionality Reduction Modeling and Multistability Reconstitution of Memristive Circuit." Complexity 2021, no. 1 (2021): 2747174.

[32] Chawla, Ashima, Paul Jacob, Brian Lee, and Sheila Fallon. "Bidirectional LSTM Autoencoder For Sequence Based Anomaly Detection in Cyber Security." International Journal of Simulation–Systems, Science & Technology 20, no. 5 (2019): 1-6.

[33] Yamada, Kazunori D., and Kengo Kinoshita. "De Novo Profile Generation Based on Sequence Context Specificity with the Long Short-Term Memory Network." BMC bioinformatics 19, no. 1 (2018): 272.

[34] Wu, Lin, Michele Haynes, Andrew Smith, Tong Chen, and Xue Li. "Generating Life Course Trajectory Sequences with Recurrent Neural Networks and Application to Early Detection of Social Disadvantage." In International Conference on Advanced Data Mining and Applications, pp. 225-242. Cham: Springer International Publishing, 2017.

[35] Guang, Xingxing, Yanbin Gao, Pan Liu, and Guangchun Li. "IMU Data and GPS Position Information Direct Fusion Based on LSTM." Sensors 21, no. 7 (2021): 2500.

[36] Feng, Luoyin, Jize Du, and Chong Fu. "Digital Image Encryption Algorithm Based on Double Chaotic Map and LSTM." Computers, Materials & Continua 77, no. 2 (2023).

[37] He, Yi, Ying-Qian Zhang, Xin He, and Xing-Yuan Wang. "A New Image Encryption Algorithm Based on the OF-LSTMS and Chaotic Sequences." Scientific reports 11, no. 1 (2021): 6398.

[38] Li, Shuangyuan, Mengfan Li, Qichang Li, and Yanchang Lv. "Hyperchaotic Image Encryption System Based on Deep Learning LSTM." International Journal of Advanced Computer Science & Applications 14, no. 11 (2023)

[39] Liu, Gang, Guosheng Xu, Chenyu Wang, and Guoai Xu. 2025. "Hyper-Chaos and CNN-Based Image Encryption Scheme for Wireless Communication Transmission." Computers, Materials & Continua 84 (3).

[40] Li, Xiaowu, and Huiling Peng. "Chaotic Medical Image Encryption Method Using Attention Mechanism Fusion ResNet Model." Frontiers in Neuroscience 17 (2023): 1226154.

[41] Li, Shuangyuan, Mengfan Li, Qichang Li, and Yanchang Lv. "Hyperchaotic Image Encryption System Based on Deep Learning LSTM." International Journal of Advanced Computer Science & Applications 14, no. 11 (2023).

[42] Feng, Luoyin, Jize Du, and Chong Fu. "Digital Image Encryption Algorithm Based on Double Chaotic Map and LSTM." Computers, Materials & Continua 77, no. 2 (2023).

[43] He, Yi, Ying-Qian Zhang, Xin He, and Xing-Yuan Wang. "A New Image Encryption Algorithm Based on the OF-LSTMS and Chaotic Sequences." Scientific reports 11, no. 1 (2021): 6398.

[44] Koubaâ, Karama, and Nabil Derbel. "DNA Image Encryption Scheme Based on a Chaotic LSTM Pseudo-Random Number Generator." International Journal of Bifurcation and Chaos 33, no. 06 (2023): 2350067.