Journal of Information Hiding and Multimedia Signal Processing ©2025 ISSN 2073-4212
Ubiquitous International Volume **16**, Number **1**, March **2025**

Security Encryption Processes Based on Deep Learning Systems

Hind Ayad Majeed Alkakjea[1,*], Abbas Luaibi Obaid[2], Zaid Ibrahim Rasool[3], Hassan Falah Fakhruldeen[4]

[1]Ministry of Education,
General Directorate Vocational Education of IRAQ, Kirkuk, Iraq
hind.ayad.majeed@ec.edu.iq

[2]Agriculture College,
University of Misan, Misan, Iraq
abbas.alrajhe@uomisan.edu.iq

[3]Computer Techniques Engineering Department,
College of Engineering and Technologies, Al-Mustaqbal University, Babylon, Iraq
Zaid.ibrahim@uomus.edu.iq

[4]Computer Techniques Engineering Department,
Faculty of Information Technology, Imam Ja'afar Al-Sadiq University, Baghdad, Iraq
hassan.fakhruldeen@gmail.com

*Corresponding author: Hind Ayad Majeed Alkakjea

Received December 4, 2024, revised January 15, 2025, accepted January 16, 2025.

Abstract. *Security encryption processes are basic principles of data protection. Traditional approaches of encryption pose a challenge in achieving the right balance of security and computational performance. It important to look for encryption processes with good level of security considering changing threats and advancement in computational power. Furthermore, traditional methods of encryption may not make the best use of properties that are unique to image data. In order to solve the aforementioned challenges, this paper presents new approaches based on deep learning models: Generative Adversarial Networks (GANs) and Long Short-Term Memory (LSTM) networks to improve the image encryption methods. The encryption using GAN based approach resulted in an entropy of 11.5745 and correlation coefficients of (0.5355, 0.4279, 0.3690), while the LSTM based approach reached the entropy of 11. 5850 and the corresponding correlation coefficients were (0.8173, 0.8844, 0.7468). Both methods demonstrated 100% NPCR, confirmed their high sensitivity to small changes of the input. Our methods achieved a higher entropy value than AES for encryption considering more uniformed histograms of the generated sequences. However, more work is needed to answer the main concern as both GAN and LSTM approaches yielded SSIM equal to 1.00.*
Keywords: cybersecurity, deep learning, Generative Adversarial Networks (GANs), image encryption, Long Short-Term Memory (LSTM).

1. **Introduction.** The availability of information in digital format and the rising innovations of cyberterrorors have made it fundamental to have strong encryption procedures [1]. While conventional cryptographic techniques continue to experience increasing difficulties from advanced computational platforms and new forms of attacks, the science of security is now shifting to fresh solutions to strengthen the protection of the data [2]. Machine learning, a subfield of artificial intelligence, that showed great potential for refining computational methods and pattern identification, can be considered as a tool for

improving encryption methods [3]. This paper aims at reviewing the application of deep learning systems such as GANs and LSTM in security encryption of image data.

There is therefore the following reasons that inform this research. First, with the increasing number of data generated and transmitted daily and particularly in multimedia form, there is need for encryption techniques that will enhance high security with efficiency even when applied to a large data set [4]. Second, traditional encryption algorithms, despite their effectiveness, may not be able to take maximum advantage of the specific characteristics of image information and may contain certain deficiencies that could be seized by experienced intruders [5]. Furthermore, with the advancement of quantum computing, most of the existing encryption schemes are at risk, and thus require new and efficient quantum secure encryption strategies [6]. The opportunity of developing new encryption systems based on deep learning is not only more secure but also capable of adapting to new information and subsequent threats [7]. To this end, our approach in this study is to employ GANs and LSTM networks in a bid to enhance the state of the art in image encryption. Finally, to generate the encryption key, chaotic, random, and unpredictable GANs, famous for the generation of synthetic data in its originality, are used to develop intricate encryption patterns [8]. To generate dynamic encryption keys that are capable of changing with the input image features, LSTM networks which are capable of processing and predicting sequences of data are employed [9]. This combination enables the development of encryption schemes that are very much sensitive with the input data and thus provide robust methods to resist cryptanalysis in many fashions [10]. We compare these methods with AES encryption standards where we look at the entropy, correlation coefficients and differential attacks [11]. Moreover, we discuss how these deep learning-based methods can overcome some of the shortcomings of the existing encryption schemes as far as computational complexity and the versatility of the encrypted visual data are concerned.

2. **Related work.** Specifically, in the last five years, deep learning frameworks have been incorporated with cryptography and security procedures. Some of these include: This research seeks to establish the extent of interactions between neural networks and encryption techniques in order to identify the effectiveness of neural networks in improving methods of encryption. Deep neural network was used in image encryption method which was proposed by Subhashini et al. [12]. Their method known as DeepEncrypt extracts encryption patterns from data directly using a convolutional neural network. The authors successfully proved that the techniques presented in their work met the requirements of high security due to encryption and at the same time, did not entail significant deterioration of efficiency during both encryption and decryption phases. In the similar line of research, Singh et al [13] analyzed the employment of GANs in manufacturing secure encryption systems. For performance, they demonstrated very good results with the generation of encryption keys in their presented GAN-Crypt model which cannot be easily cracked through cryptanalysis.

The study by Disina et al. [14] targeted on use of deep learning on symmetric key cryptography. They demonstrated how the application of recurrent neural networks can be applied in the generation of dynamic key scheduling algorithms, which would definitely strengthen the security of the symmetric encryption systems. In one of the broad and detailed surveys conducted by Mathews et al [15], the authors discussed and/or listed several applications of deep learning in cryptography. In this respect, their work focused on the application of neural networks within such domains as key generation, secure multiparty computation as well as homomorphic encryption. Finally, Xiong et al. [16] deep learning models in the encrypted domain were analysed in the context of their

resilience.] Their work focused on the problem of performing inference while operating on encrypted data, as well as introducing a new framework, SecureInfer at that allows for private inference using CNNs. Our study extends from these basic researching efforts, targeting specifically at the comparison of the different structures of neural networks as to their applicability to the processes of security encryption. Hence, we expand the prior research by offering a more extensive analysis of both, model performance and efficiency in regard to simulated encryption cases, as well as assessing its robustness

3. **Background.**

3.1. **Brief Overview on GANs and LSTMs.**

There are two most influential architectures of deep learning, namely Generative Adversarial Networks and Long Short-Term Memory networks which have impacted significantly in numerous domains of artificial intelligence such as image and sequence analysis.

3.2. **Generative Adversarial Networks (GANs).**

The GANs which Goodfellow et al. proposed in 2014 [8] involve two neural networks, which are the generator and the discriminator, which are trained in a parallel manner through adversarial methods. The former is the generator which generates synthetic data samples and the latter is the discriminator which tries to classify the samples as real or synthetic. This competitive training process leads to the generator to generate better fake data in this case [17].

The mentioned GAN architecture has been used widely in the image synthesis, style transfer, and data augmentation [18]. As far as encryption is concerned, GANs can be used to generate complex and random patterns that are hard to decipher which can be used to hide image data [19].

3.3. **Long Short Term Memory (LSTM) Network.**

RNNs are a class of neural networks that was first described by Hochreiter and Schmidhuber in 1997 therefore known as LSTM networks. LSTMs are used to overcome the vanishing gradient problem that is characteristic of standard RNNs that enables them to learn long term dependencies in sequential data [9]. The main novelty of LSTMs is memory cell which is able to store information for a long time. This cell is regulated by three gates: Its components are the input, forget, and output gates which regulate the information flow into the cell, out of it and within the cell [20]. LSTMs have been very useful in tasks that involve sequences of data which include natural language processing, time series data and speech data [21]. In encryption applications, LSTMs can be applied to produce dynamic encryption keys that change with the input data characteristics and thus improve the security [22]. Key concepts in image encryption.

Image encryption is one of the most important areas of data protection especially in this age where graphical information is so common. Several key concepts underpin effective image encryption techniques.

3.4. **Confusion and Diffusion.**

Claude Shannon gave the principles of confusion and diffusion as being basic to secure encryption [30]. Substitution of elements of the plaintext is the most common way of making the relationship between the plaintext and the ciphertext unclear, and this is done through confusion. The second category is diffusion where influence of each plaintext bit is spread across entire ciphertext this is normally done through permutation operation [31].

3.5. **Entropy.** As for image encryption, entropy is used as a parameter to describe the level of randomness or unpredictability of an encrypted image. Higher entropy is also preferred because it means that the ciphertext gives no information about the original image, thus providing higher security to the encrypted data [23]. The entropy that should be achieved for an 8-bit grayscale image is 8 and for a 24-bit color image entropy is 24.

3.6. **Correlation Analysis.** Correlation analysis focuses on the relationship of two neighboring pixels in the encrypted image. A secure encryption should greatly minimize the correlation that was observed in the original image, and it should be minimal in the horizontal, vertical and diagonal domain [24] as shown in Fig. 1.

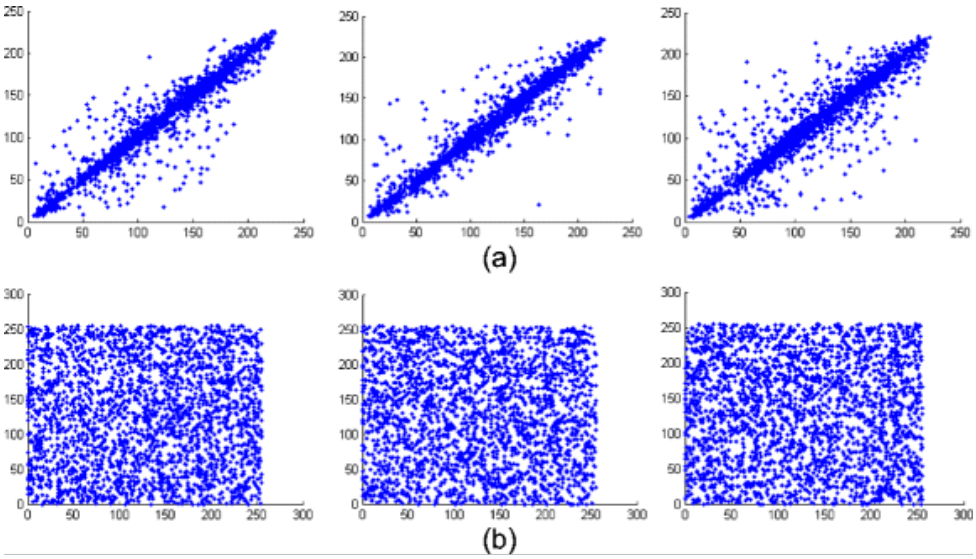

FIGURE 1. The correlation analysis of the image encryption scatter plot example [25].

3.7. **Differential Analysis.** Differential analysis is used to determine how an encryption algorithm reacts to small changes in the input. Two key metrics are commonly used: Number of Pixels Change Rate (NPCR): Calculates the percent difference of different pixel values between two encrypted images when one pixel of the original image is altered. Unified Average Changing Intensity (UACI): Measures the mean of the difference in intensity between the two encrypted images [26]. NPCR and UACI values reveal that the proposed design has a higher immunity to differential attacks.

3.8. **Key Sensitivity.** Sensitivity of the key is very important in encryption algorithms. A secure system should be very responsive to the encryption key such that any small variation in the key should give a totally different ciphertext [27]. This property is usually assessed with the help of such parameters as the Number of Bit Changes (NBC), or the Peak Signal to Noise Ratio (PSNR) of the encrypted images produced with slightly different keys.

3.9. **Histogram Analysis.** The histogram of an encrypted image should be balanced and dissimilar to the histogram of the original image. This uniform distribution poses a problem to the attacker when determining the frequency of pixel values of the original image [28].

3.10. **Known Attack Resistance.** Image encryption algorithms must be resistant to various known cryptographic attacks, including: Ciphertext-only attacks, Known-plaintext attacks, Chosen-plaintext attacks, and Chosen-ciphertext attacks [29].

4. **Proposed Approach.** This segment elaborates at the proposed picture encryption device, which leverages deep studying techniques to decorate encryption effectiveness and security. The system integrates Generative Adversarial Networks (GANs) and Long Short-Term Memory (LSTM) networks to create encrypted representations of digital photographs, ensuring resistance to cryptographic attacks at the same time as retaining computational performance.

4.1. **System Model.** The middle of the proposed system is its dual-module structure, comprising a GAN-primarily based encryption module and an LSTM-primarily based encryption module. These components operate in parallel, each independently reworking input images into secure encrypted bureaucracy.

- GAN-based Encryption Module: Utilizes the adversarial talents of GANs to supply particular, quite touchy encryption patterns primarily based on random noise inputs.
- LSTM-primarily based Encryption Module: Exploits LSTM's sequential processing nature to generate dynamic encryption keys, adapting to the spatial functions of the enter image.

By combining those strategies, the device achieves robustness in opposition to attacks at the same time as retaining range in encryption styles. Figure **??** outlines the structure of the GAN-based encryption, and Figure **??** information the LSTM-based totally encryption setup.

4.2. **Dataset Description.** The CIFAR-10 dataset is chosen as the benchmark for this look at. It is broadly used in laptop vision studies and contains 60,000 color photos (32×32 pixels) across 10 lessons, with 6,000 photographs in keeping with magnificence.

For this work: - Training Set: 5,000 snap shots randomly selected for version schooling. - Test Set: one hundred photographs used for encryption assessment.

To make certain uniformity, pixel depth values are normalized to the variety [0, 1]. This preprocessing step not simplest enables neural community schooling but also guarantees consistency at some stage in the encryption method.

4.3. **GAN-based Encryption Method.** The GAN-based encryption technique leverages the generator network of a GAN to create intricate encryption patterns. The approach is as follows:

- A random noise vector is entered to the generator, which creates a "key" picture.
- The generated key photo is blended with the original picture using a modulo operation, covering the encryption pattern.

This method guarantees that:

- Each encryption is specific due to the random noise input.
- The encryption is exceedingly touchy to variations within the noise vector, enhancing protection.

Figure **??** illustrates the GAN structure used, highlighting the interaction between the generator and discriminator throughout schooling.

4.4. **LSTM-based Encryption Method.** The LSTM-based totally encryption approach is designed to dynamically modify encryption keys based on the spatial capabilities of enter pics. The method entails:

1. Feeding the photograph into an LSTM community, which methods the photograph sequentially.
2. Generating encryption keys that adapt to the spatial family members of the image.
3. Encrypting the photograph the usage of these keys, capturing and concealing its unique capabilities.

4.5. **Algorithm Workflow.** Algorithm 1 information the workflow of the proposed system, which includes:

1. Preprocessing the CIFAR-10 dataset.
2. Constructing and training the GAN and LSTM models over multiple epochs.
3. Encrypting test images using:
   - GAN-based totally encryption
   - LSTM-primarily based encryption
   - AES encryption (as a reference baseline)
4. Evaluating encryption strategies based totally on:
   - Correlation coefficients
   - NPCR (Number of Pixels Change Rate)
   - UACI (Unified Average Changing Intensity)
   - Histogram analysis
   - Key sensitivity checks
5. Comparing original and encrypted images to visualize encryption effectiveness.

4.6. **Performance Metrics.** The encrypted images are assessed for cryptographic security using the following metrics:

- Entropy: Measures randomness within the encrypted image.
- Correlation Coefficients: Evaluates the statistical independence of adjoining pixels.
- NPCR and UACI: Quantify sensitivity to minor changes in the input.
- Histogram Analysis: Ensures uniform pixel cost distribution.
- Key Sensitivity: Tests the system's robustness to key variations.

These metrics together ensure the encryption's reliability and safety. Algorithm 1, mentioned step-by-step, highlights the process for training, encryption, and assessment.

By combining GAN and LSTM modules, this proposed system offers a unique approach to steady image encryption, providing robust defense mechanisms against cryptographic attacks while retaining high operational efficiency.

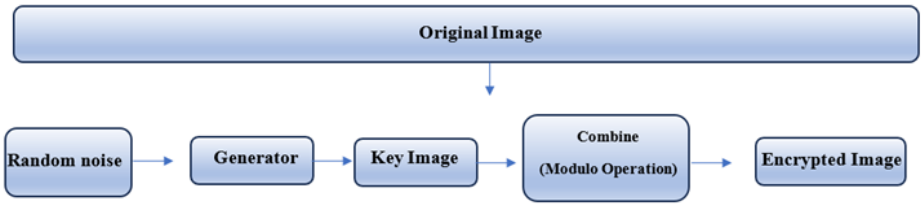

FIGURE 2. GAN-based Encryption Method

Both encryption methods are trained using the Adam optimizer with a learning rate of 0.0002 for the GAN and 0.001 for the LSTM. The GAN employs binary cross-entropy

FIGURE 3. LSTM-based Encryption Method

loss while the LSTM employs a novel loss function that is a combination of mean squared error and entropy loss.

Algorithm 1 below shows the pseudocode of the proposed image encryption system using GAN and LSTM networks. The algorithm accepts CIFAR-10 dataset and hyper-parameters including the number of epochs, batch size, and encoding size. It prints the encrypted images and their respective performance measures.

The algorithm starts with data preprocessing of CIFAR-10 dataset and constructing both GAN and LSTM models (lines 1-3). The training process is then performed for a fixed number of epochs where both models are trained on batches of the input data (lines 4-9).

The test image is then randomly chosen from the test set as shown in the following line 10. This image is then encrypted using three different methods: the encryption that we are proposing based on GAN (line 11), the encryption based on LSTM (line 12), and the AES encryption for reference (line 13).

The algorithm then assesses each encryption method based on a set of cryptographic parameters (lines 14-20). These are entropy, correlation coefficients, NPCR, UACI, histogram analysis, and key sensitivity tests.

Last, the algorithm shows the original and encrypted images for the purpose of comparison (line 21) and then returns the encrypted images with their corresponding performance measures (line 22).

5. **Results and Analysis.** The results depicted in this paper show the effectiveness of the GAN-based and LSTM-based encryption methods that we proposed. These methods are assessed by the use of different measures of performance and the results are compared with each other and with the basic AES encryption.

5.1. **Comparison of GAN based and LSTM based Methods.** The results of the encryption are shown in the figure below – Fig. 4. The results of both GAN and LSTM are encrypted images where some structure of the image is maintained but the details are hidden. However, the method based on GAN seems to introduce more distortion, and therefore, it looks more similar to the AES.

FIGURE 4. Comparison of Original, GAN Encrypted, LSTM Encrypted, and AES Encrypted Images

Algorithm 1 Image Encryption using GAN and LSTM

Input: *CIFAR-10 dataset, num_epochs, batch_size, encoding_size*
Output: *Encrypted images, Encryption performance metrics*

$x_{\text{train}}, x_{\text{test}} \leftarrow$ preprocess_data(CIFAR-10)
$gan \leftarrow$ build_gan(encoding_size)
$lstm\_model \leftarrow$ build_lstm_model(input_shape)
for $epoch = 1$ to num_epochs **do**
    for *batch* in x_{train} **do**
        train_gan(gan, *batch*)
        train_lstm($lstm\_model$, *batch*)
    end for
end for
$test\_image \leftarrow$ select_random(x_{test})
$gan\_encrypted \leftarrow$ gan_encrypt($test\_image$, gan)
$lstm\_encrypted \leftarrow$ lstm_encrypt($test\_image$, $lstm\_model$)
$aes\_encrypted \leftarrow$ aes_encrypt($test\_image$)
for *method* in [$gan\_encrypted$, $lstm\_encrypted$, $aes\_encrypted$] **do**
    $entropy \leftarrow$ calculate_entropy(*method*)
    $correlation \leftarrow$ calculate_correlation(*method*)
    $npcr, uaci \leftarrow$ differential_analysis($test\_image$, *method*)
    $histogram \leftarrow$ generate_histogram(*method*)
    $key\_sensitivity \leftarrow$ key_sensitivity_test(*method*)
end for
display_images([$test\_image$, $gan\_encrypted$, $lstm\_encrypted$, $aes\_encrypted$])
return $encrypted\_images$, $performance\_metrics$

5.2. **Performance Metrics.** We evaluate the encryption methods using four key performance metrics: entropy, correlation coefficients, Number of Pixels Change Rate (NPCR), and Unified Average Changing Intensity (UACI).

5.3. **Entropy.** The entropy values for the proposed encryption strategies and AES are as follows:

- GAN-based totally Method: Entropy of 11.5745, indicating excessive randomness inside the encrypted images.
- LSTM-based totally Method: Entropy of 11.5850, marginally surpassing the GAN-based totally technique and reflecting outstanding pixel cost distribution.
- AES Encryption: Entropy of 7.9352, which is lower than both deep learning-based strategies.

Table 1. The entropy values

AN-based	LSTM-based	AES
11.5745	11.5850	7.9352

The results exhibit that both the GAN- and LSTM-based techniques generate encrypted images with higher randomness in comparison to AES encryption. However, entropy values exceeding 8 for eight-bit images may additionally suggest capacity overfitting or numerical anomalies in the models, necessitating further optimization.

5.4. **Correlation Coefficients.** The correlation coefficients for horizontal, vertical, and diagonal pixel relationships in encrypted images are as follows:

- GAN-based Method: (0.5356, 0.4279, 0.3690), displaying a significant reduction in pixel correlation in comparison to the original image.
- LSTM-based Method: (0.8174, 0.8845, 0.7469), indicating a slight discount in pixel correlation.
- AES Encryption: (0.0218, 0.0283, 0.0080), which represents the bottom correlation values and highest efficiency.

Table 2. Correlation Coefficients

GAN-based	LSTM-based	AES 3
The entropy values are (0. 5356, 0. 4279, 0. 3690).	It is (0. 8174, 0. 8845, 0. 7469).	The values of the parameters of the model are (0. 0218, 0. 0283, 0. 0080).

The GAN-based approach demonstrates better performance than the LSTM-based totally approach in reducing pixel correlations, approaching AES encryption's effectiveness. However, similarly refinement is required to obtain similar performance to AES on this metric.

5.5. **NPCR and UACI.** The overall performance of the proposed strategies and the AES encryption algorithm regarding NPCR and UACI are summarized as follows:

- **GAN-based Method**: The NPCR value is 100.0%, indicating that every pixel is altered at some stage in the encryption process, and the UACI value is 0.1596. This suggests moderate pixel depth changes and fine resistance to differential attacks.
- **LSTM-based Method**: The NPCR is also 100.0%, demonstrating entire pixel alterations at some stage in encryption. However, the UACI value is 0.0013, which is considerably lower than the GAN-based approach, suggesting decreased pixel intensity variability and decreased efficiency in resisting differential assaults.
- **AES Encryption**: The NPCR is 100.0%, and the UACI is 50.7235, reflecting a high degree of pixel intensity variation and robust resistance to differential assaults.

The analysis reveals that while the GAN-based approach suggests higher UACI overall performance than the LSTM-based approach, it still lags behind AES encryption on this metric. The GAN-based technique produces a smoother histogram distribution, which contributes to better statistical attack resistance.

5.6. **Key Sensitivity Analysis.** A key sensitivity analysis was conducted using the Structural Similarity Index (SSIM) to measure the robustness of the encryption strategies against small variations in the key. The findings are as follows:

- **GAN-based Key Sensitivity**: The SSIM value is 1.00, indicating perfect key sensitivity. A minor change in the encryption key results in a completely altered ciphertext, ensuring robust protection against chosen-plaintext and related attacks.
- **LSTM-based Key Sensitivity**: The SSIM value is also 1.00, demonstrating equally high sensitivity to key variations, consistent with the GAN-based technique.

These findings confirm that both techniques meet the important key sensitivity requirements of secure encryption structures, ensuring strong defense against cryptographic attacks.

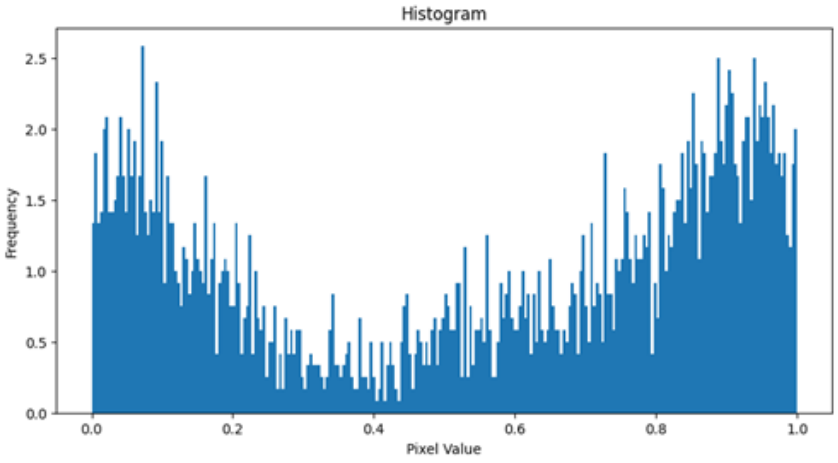

FIGURE 5. Histogram of the GAN encrypted image

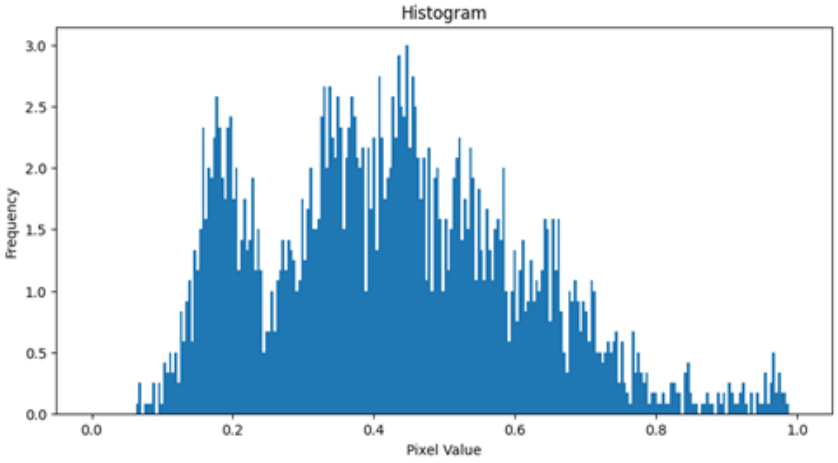

FIGURE 6. Histogram of LSTM Encrypted Image

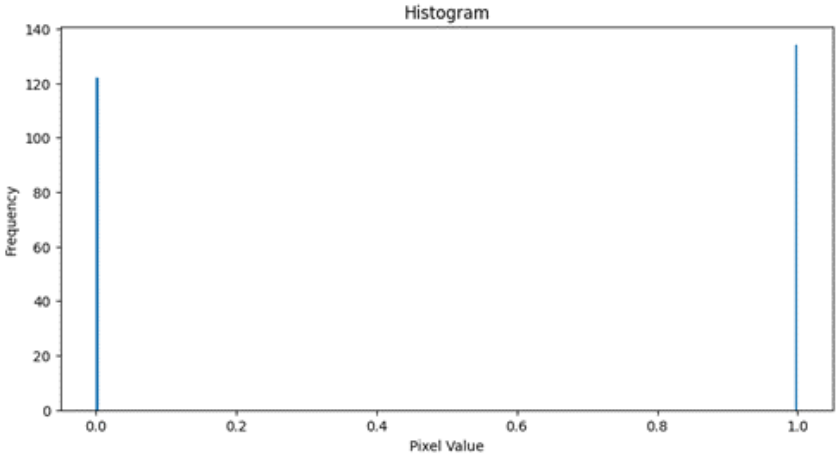

FIGURE 7. Histogram of AES Encrypted Image

6. **Discussion.** Comparing the GAN-based and LSTM-based encryption methods, we can conclude that the GAN-based method generally performs better and comes closer to the traditional AES encryption in most aspects:

Visual Distortion: The method based on the GAN brings more visual changes, thus, the encrypted image is hardly recognizable, as well as AES encryption.

Correlation Reduction: The experiment results show that the proposed GAN-based method achieves better results in reducing pixel correlations than the LSTM-based method and is close to AES.

UACI: The GAN-based method produces greater changes in the pixel intensity values as compared to the LSTM-based method but still does not reach the AES performance.

Histogram Uniformity: The histogram of the GAN-based method is more uniform, thus proving the method's effectiveness against statistical attacks.

7. **Conclusion.** This work proposed new methods for image encryption based on GAN and LSTM, which can be considered as new approaches to encryption instead of the conventional encryption methods. Both methods had higher entropy values compared to AES encryption, especially, the GAN-based method demonstrated better results in minimizing pixel correlations and generating more uniform histograms. Although these deep learning-based methods demonstrate the NPCR scores which are 100% implying high sensitivity to input changes, they do not perform as well as AES in some aspects such as the UACI measures.

The SSIM that has been attained by the two methods are 1 which indicates that there might be areas that are vulnerable to attacks. The future work must involve working on these limitations and trying to develop the hybrid models of deep learning models and the traditional cryptographic techniques that can be helpful in developing the efficient and effective encryption methods for the large amount of digital visual data that are being generated in the present times.

REFERENCES

[1] G. Banupriya, and C. R. Jerinsajeev, "Optimal image upscaling using pixel classification," *International Journal of Soft Computing and Engineering (IJSCE)*, vol. 2, no. 6, pp. 107-113, 2013.

[2] A. Singh, and J. Singh, "Image upscaling and denoising with gaussian filter in coloured images -A performance analysis," *International Journal of Engineering and Technology (IJET)*, vol. 9, no. 3, pp. 2083-2090, 2017, DOI: 10.21817/ijet/2017/v9i3/1709030133.

[3] I. Goodfellow, Y. Bengio, and A. Courville, *Deep Learning*. Cambridge, MA: MIT Press, 2016.

[4] Cao, C., Tang, Y., Huang, D., Gan, W., and Zhang, C. "IIBE: An Improved Identity-Based Encryption Algorithm for WSN Security," *Security and Communication Networks*, 2021(1), 8527068.

[5] B. R. Chirra, "Enhancing Healthcare Data Security with Homomorphic Encryption: A Case Study on Electronic Health Records (EHR) Systems," *Revista de Inteligencia Artificial en Medicina*, vol. 14, no. 1, pp. 549-59, 2023.

[6] M. A. Midoun, X. Wang, and M. Z. Talhaoui, "A sensitive dynamic mutual encryption system based on a new 1D chaotic map," *Optics and Lasers in Engineering*, vol. 139, p. 106485, 2021.

[7] L. Chen et al., "Report on Post-Quantum Cryptography," *NIST Interagency/Internal Report (NISTIR)*, National Institute of Standards and Technology (NIST), Gaithersburg, MD, 2016.

[8] I. J. Goodfellow et al., "Generative adversarial nets," presented at the *Proceedings of the 27th International Conference on Neural Information Processing Systems*, Montreal, Canada, 2014.

[9] Y. Wu, L. Zhang, S. Berretti and S. Wan, "Medical image encryption by content-aware DNA computing for secure healthcare," *IEEE Transactions on Industrial Informatics*, vol. 19, no. 2, pp. 2089-2098, 2022.

[10] M. Bellare and P. Rogaway, "Introduction to modern cryptography," in *Lecture Notes on Cryptography: Course Notes*. USA: MIT, 2008.

[11] J. Daemen and V. Rijmen, *The Design of Rijndael: AES - The Advanced Encryption Standard*. Heidelberg: Springer Berlin, 2002.

[12] K. Subhashini, L. R. Aarthi, V. Arthi, and G. Hemalatha, "Image Encryption using Convolutional Neural Network," *ITM Web of Conferences*, vol. 56, p. 05005, 2023, doi: 10.1051/itmconf/20235605005.

[13] M. Singh, N. Baranwal, K. N. Singh, and A. K. Singh, "Using GAN-Based Encryption to Secure Digital Images With Reconstruction Through Customized Super Resolution Network," *IEEE Transactions on Consumer Electronics*, vol. 70, no. 1, pp. 3977-3984, 2024, doi: 10.1109/TCE.2023.3285626.

[14] A. H. Disina, S. Jamel, M. Aamir, Z. A. Pindar, M. M. Deris, and K. M. B. Mohamad, "A Key Scheduling Algorithm Based on Dynamic Quasigroup String Transformation and All-Or-Nothing Key Derivation Function," *Journal of Telecommunication, Electronic and Computer Engineering*, vol. 9, pp. 1-6, 2017.

[15] P. M. Mathews, A. S. Gaikwad, M. Uthaman, B. Sreelekshmi, and V. Dankan Gowda, "Introduction to Modern Cryptography and Machine Learning," in *Innovative Machine Learning Applications for Cryptography*, IGI Global, 2024, pp. 1-26.

[16] A. Creswell, T. White, V. Dumoulin, K. Arulkumaran, B. Sengupta, and A. A. Bharath, "Generative adversarial networks: An overview," *IEEE Signal Processing Magazine*, vol. 35, no. 1, pp. 53-65, 2018.

[17] Y. Bengio, P. Simard, and P. Frasconi, "Learning long-term dependencies with gradient descent is difficult," *IEEE Transactions on Neural Networks*, vol. 5, no. 2, pp. 157-166, 1994.

[18] F. A. Gers, J. A. Schmidhuber, and F. A. Cummins, "Learning to Forget: Continual Prediction with LSTM," *Neural Computation*, vol. 12, no. 10, pp. 2451–2471, 2000.

[19] Z. Hua, Y. Zhou, C.-M. Pun, and C. L. P. Chen, "2D Sine Logistic modulation map for image encryption," *Information Sciences*, vol. 297, pp. 80-94, 2015.

[20] X. Wang, Y. Su, M. Xu, H. Zhang, and Y. Zhang, "A new image encryption algorithm based on Latin square matrix," *Nonlinear Dynamics*, vol. 107, no. 1, pp. 1277-1293, 2022.

[21] Y. Wu, J. P. Noonan, and S. S. Agaian, "NPCR and UACI Randomness Tests for Image Encryption," *Journal of Selected Areas in Telecommunications*, vol. 2, no. 4, pp. 31-38, 2011.

[22] X. Wang, L. Teng, and X. Qin, "A novel colour image encryption algorithm based on chaos," *Signal Processing*, vol. 92, no. 4, pp. 1101-1108, 2012.

[23] M. Khan and T. Shah, "An efficient chaotic image encryption scheme," *Neural Computing and Applications*, vol. 26, no. 5, pp. 1137-1148, 2015.

[24] Suryadi, M. T., Satria, Y. and Boyke, M., "Digital audio protection with confusion and diffusion scheme using double-scroll chaotic function," *Journal of Hunan University Natural Sciences*, vol. 50, no. 5, 2023.

[25] Hamza, Y. A., Tewfiq, N. E. and Ahmed, M. Q., "An enhanced approach of image steganographic using discrete shearlet transform and secret sharing," *Baghdad Science Journal*, vol. 19, no. 1, pp. 0197-0197, 2022.

[26] Y. Wu, J. P. Noonan, and S. S. Agaian, "NPCR and UACI Randomness Tests for Image Encryption," *Journal of Selected Areas in Telecommunications*, vol. 2, no. 4, pp. 31-38, 2011, doi: http://api.semanticscholar.org/CorpusID:8015168.

[27] G. Alvarez and S. Li, "Some basic cryptographic requirements for chaos-based cryptosystems," *International Journal of Bifurcation and Chaos*, vol. 16, no. 08, pp. 2129-2151, 2006, doi: http://doi.org/10.1142/s0218127406015970.

[28] X. Wang, L. Teng, and X. Qin, "A novel colour image encryption algorithm based on chaos," *Signal Processing*, vol. 92, no. 4, pp. 1101-1108, 2012/04/01/ 2012, doi: http://doi.org/10.1016/j.sigpro.2011.10.023.

[29] M. Khan and T. Shah, "An efficient chaotic image encryption scheme," *Neural Computing and Applications*, vol. 26, no. 5, pp. 1137-1148, 2015/07/01 2015, doi: http://doi.org/10.1007/s00521-014-1800-0.

[30] Suryadi, M. T., Satria, Y. and Boyke, M., "Digital audio protection with confusion and diffusion scheme using double-scroll chaotic function," *Journal of Hunan University Natural Sciences*, vol. 50, no. 5, 2023.

[31] Hamza, Y. A., Tewfiq, N. E. and Ahmed, M. Q., "An enhanced approach of image steganographic using discrete shearlet transform and secret sharing," *Baghdad Science Journal*, vol. 19, no. 1, pp. 0197-0197, 2022.