International Journal of
INTELLIGENT SYSTEMS AND APPLICATIONS IN ENGINEERING
ISSN:2147-6799 www.ijisae.org Original Research Paper

Revolutionizing Image Encryption: Data Hiding Model Based on Optimized Neural Network

Ms. Pallavi S. Chakole[1], Siva Rama Krishna T.[2], Rahul Mishra[3], Beemkumar Nagappan[4], Dr. Sachin S. Pund[5], Dr. Jasneet Kaur[6]

Submitted: 03/02/2024 **Revised:** 11/03/2024 **Accepted:** 17/03/2024

Abstract: Information security researchers are currently focusing on Revolutionizing Image Encryption in data hiding for safe digital data movement. Preserving information that has been hidden in a system is one of the core concepts of data hiding. For image encryption, data hiding is the process of embedding private data into images to ensure it is hidden from perceptions by other people. In this research, the hidden data is retrieved by our proposed Multi-rate Salient Gated Recurrent Neural Network (MSG-RNN) and it employs a dependent classification method to recover images from encrypted images. We gathered a data of various kinds of image data. Following the encryption of the original image, we established the Elliptic Curve Cryptography (ECC) method and created an innovative image encryption technique to improve security by data hiding. We calculated our proposed method's bit error rates. The comparison evaluation is performed with various methods to estimate proposed technique. Using the MSG-RNN approach on a number of images produced superior outcomes and they include the results for boats (0.0714), peppers (0.0712), baboons (0.0716) and airplanes (0.0719). The experimental outcomes offered that the proposed MSG-RNN technique performed better than other existing methods in data hiding process to enhance image encryption.

Keywords: *Data Hiding, Elliptic Curve Cryptography (ECC), Image Encryption, Information security Multi-rate Salient Gated Recurrent Neural Networks (MSG-RNN).*

1. Introduction

Data hiding is the process of hiding sensitive information in a different kind of cover material and minimizing the amount of inconsistencies that are present in data. Machine hackers should be able to avoid digital steganalysis tools including StegExpose and the latest deep learning-based ones by making the distortions invisible. For individual hackers, the detected distorting can be consistent with individual conclusions, penalizing errors that can be most perceptively or cognitively apparent [1]. The environment is evolving very rapidly caused by technological advancements. Every aspect of existence can be changed and changed significantly by the internet and multimedia. The modern generation of systems is intelligent, flexible, decentralized, self-organizing and well-connected. The utilization of IoT to connect different system components and modify CPS to track and control the devices has made it possible [2]. The primary objective has been to protect the data and information from strangers by employing data security techniques like cryptography and steganography. Using an encryption key with an algorithm for encryption an ensemble of methods known as cryptography are utilized to transform data into a format that can't be accessed. Steganography hides the message within a different medium [3]. The unique qualities of the internet are the vast potential for development in both the ability and availability. The relevant mathematical

1Assistant Professor, Department of Civil Engineering, Yeshwantrao chavan college of engineering,Nagpur, Maharashtra, India. chakole121pallu@gmail.com, https://orcid.org/0000-0001-5300-0897
2Assistant Professor, Computer Science and Engineering, Jawaharlal Nehru Technological University Kakinada, India. srktummalapalli@gmail.com. orcid id: 0000-0003-3351-4393.
3Centre of Research Impact and Outcome, Chitkara University, Rajpura, Punjab, India. rahul.mishra.orp@chitkara.edu.in
4Professor, Department of Mechanical Engineering, Faculty of Engineering and Technology, JAIN (deemed to be University), Bangalore, Karnataka, India, Email Id-beemkumar@jainuniversity.ac.in
5Assistant Professor, Department of Mechanical Engineering, Shri Ramdeobaba College of Engineering and Management, Nagpur, Maharashtra, India. pundss@rknec.edu, https://orcid.org/0000-0002-5616-2469
6Symbiosis International Deemed University, lavale pune, India
jasneetkaur@scon.edu.in, 0000-0001-6897-9137

frameworks have the ability to produce enormous amounts of information that can be utilized as pseudorandom generated keys in the framework of image encryption and they are required for seed-based encryption methods [4]. Steganography promotes imperceptibility that is different from cryptography in that it involves hiding information without raising concerns. Given that secure communication is needed, steganography is utilized [5]. The concept of multimedia refers to the combination of several media components, each of which is a different type. The process of digital storage, transmission and processing of various types of information is called computer-controlled integration of content [6]. Block-chain employs a distributed ledger to store data. Block-chain technology offers integrity and availability, enabling users of the network to make perspective and validate transactions stored in a distributed ledger [7]. The objective of this research is to implement our new MSG-RNN image encryption technique to provide more privacy protection and revolutionize image encryption in data-hiding applications.

The following are the organizations of the remaining portion: phase 2 contains representations of related works. A description of the proposed MSG-RNN framework is given in phase 3. The experiment's results are shown in phase 4. Conclusions are provided in phase 5.

2. Literature Review

The study [8] utilized an innovative cryptographic framework and optimization techniques to investigate the Internet of Things (IoT) security for hidden medical images. The evaluation revealed that in comparison with various existing frameworks, their recommended technique offered greater privacy. To hide, retrieve and identify digital data in images, they introduced the StegYou technique [9] in that work. They utilized an original crypt-steganography technique for several images to secure their implementation of data hiding and retrieval. They provided an innovative composition-aware image steganography (CAIS) [10] that used self-generated supervision to ensure both visual privacy and resistance to deep steganalysis. To endure extensive steganalysis, the recommended CAIS can accomplish improved security and better information hiding. The research [11] demonstrated that the declared security offered by this encryption technique cannot be maintained. The complex DNA encryption processes were first represented utilizing substitution boxes (s-boxes) and the entire encryption method was subsequently removed to form an s-box-then-permutation cipher of sorts. It was anticipated that security assessment could benefit from the proposed approach by expanded the Deoxyribonucleic acid (DNA) encrypted as an s-box alternative. They provided an innovative separate encrypted image-based reversible data hiding [12] method. Considered an image, the edge generated encrypted variations of it and subsequently offered it to intermediate nodes that create encrypted variations of the images that contain messages and the cloud can extract that message from the original image. Experimental findings were presented to demonstrate the efficacy and efficiency of that approach. Steganography and Cryptography were integrated into the article [13] to boost security and to make the device harder for hackers to break into. Both an objective and subjective analysis of the generated stego-image that was expressed revealed no cause for concern, consequently performed an initial objective of steganography. They developed an updated universal embedding model (UEM)--based visually meaningful image encryption (VMIE) [14] method by UEM. The proposed VMIE method can get an improved visual quality than conventional VMIE algorithms based on simulation outcomes and performance comparisons. The discrete wavelet transforms (DWT) [15] technique was primarily employed in the article to convert the original image into an arrangement for storage in a separate image that has to be protected. An image that was completely encrypted was the end product of that procedure.

3. Materials and Methods

The study of image encryption methods has increased the need for secure image transformation that can be performed in real time utilizing wireless networks and the web. Several methods have been explored and proposed. This section provides an explanation of the proposed methodology.

3.1 Data Collection

A collection of digital images can be found in the USC-SIPI (https://sipi.usc.edu/database/) image data. The main objective is to facilitate the

processing of images, evaluation of images and machine vision research. Several more images have been stored since the USC-SIPI image database's initial version. A simple character analysis of the images is employed to categorize the database into portions. Each volume of images has various pixel dimensions like 256x256, 512x512, or 1024x1024. Each pixel in black and white color images is 8 bits and each pixel in a color image is 24 bits.

3.2 Elliptic Curve Cryptography (ECC) for Data Hiding

Elliptic curve cryptography (ECC) is frequently employed in IoT to provide privacy as well as security features such as digital signatures and key transmission. The Weierstrass equation (1) defines an elliptic curve on prime field $HE(q)$:

$$x^2 = y^3 + by + a \ (mod\ q) \quad (1)$$

The elements $a\ and\ b$ which are the integers in the basic field $HE(q)$, provide $4a^3 + 27b^2 \neq 0\ (mod\ q)$. A Weierstrass ellipse F in $HE(q)$ is composed of by combining an extra point O, frequently referred to a point at infinity and a group of points $q = (y, x)$ having $y, x\ HE(q)$. The points at infinity and the total number of ellipse points together form a collection that allows the group equation (2) can be established. Point Addition (PA) is defined as $P_1(x_1, y_1) + P_2(x_2, y_2) = P_3(x_3, y_3)$.

$$y_3 = \left(\frac{x_2 - x_1}{y_2 - y_1}\right)^2 - y_1 - y_2 \quad (2)$$

$$x_3 = \left(\frac{x_2 - x_1}{y_2 - y_1}\right)(y_1 - y_3) - x_1 \quad (3)$$

Point Doubling (PD) is defined as $2P_1(x_1, y_1) = P_3(x_3, y_3)$,

$$y_3 = \left(\frac{3y_1^2 + b}{2x_1}\right)^2 - 2y_1 \quad (4)$$

$$x_3 = \left(\frac{3y_1^2 + b}{2x_1}\right)(y_1 - y_3) - x_1 \quad (5)$$

The two points of the elliptic curve are denoted by $P_1(x_1, y_1)$ and $P_2(x_2, y_2)$. It is essential to remember that the prime field $HE\ (q)$ provides the framework for all calculations, including additions, subtractions, multiplications and divisions.

3.3 Image Recovery Using Multi-rate Salient Gated Recurrent Neural Networks (MSG-RNN)

The essential component of MSG-RNN is sequential information. It is assumed that every input and output in common neural networks are independent of one another. The issue of the explosion of gradients and gradient disappearance causes MSG-RNN to appear backward in time and it can utilize sequence information of any length. The i^{th} value's path direction is displayed in equation (1). When the machine goes straight forward at Ω, Ω becomes zero and it is utilized to calculate one lateral stability index.

$$\Omega = \frac{\sum_{j=j}^{i+M-1} |\psi_{j+1} - \psi_j|}{M-1} \quad (6)$$

W[d] and x[d] are the inputs and outputs of a Gated recurrent units (GRU) unit. To calculatex|[d − 1], y[c] is also utilized. In the following equations (2–7), the exact computation is demonstrated.

$$K = \sigma(U_K W[d] + Y_K x|[d-1] \quad (7)$$

$$K = \sigma(U_h W[d] + Y_h x|[d-1] \quad (8)$$

$$\hat{x} = tang\ (Uw[d] + Y(K \odot x[d-1] \quad (9)$$

$$x[d] = (1 - h) \odot x[d-1] + h \odot \hat{x} \quad (10)$$

$$\sigma(w) = \frac{1}{1 + \exp(-w)} \quad (11)$$

$$Sil = \frac{1}{n} \sum_{j=1}^{p} \sum_{w \in U_j} \frac{r(w) - e(w)}{\max(e(w), r(w))}, \quad (12)$$

The units $(U_K, U_h, U_w, and\ U)$ are defined by four criteria that maintain previous information and need more features than the fundamental unit. Since its outputs and inputs are independent, this unit performs calculations in an approach similar to that of the conventional connection. Utilizing an appropriate hidden layer neural network design, the model analyzes input data that indicates the degrees of involvement and disengagement. As its output, this neural network forecasts that can range from engagement to indifference to uncertainty. The hidden layers within the network that identify intricate patterns and relationships in the input data allow for the identification and classification of

complicated states based on their levels of involvement in data hiding.

4. Performance Evaluation

This section describes the experimental setting utilized by the given image encryption framework. The outcomes of the simulations used to test the proposed approach are explained. Python version 2.7 was utilized to construct the proposed encryption technique. The system included a 1TB drive and an Intel Core i7 central processing unit (CPU) running at 2.40 GHz with 8 GB of Random Access Memory (RAM). Utilizing a variety of images such as peppers, boats, airplanes and baboons, the efficiency of both the proposed and traditional approaches is contrasted. Existing methods consist of Reversible Data Hiding (RDH) [16], Encrypted Image RDH (EIRDH) [18] coupled with RDH and Convolutional Neural Network (RDH-CNN) [17]. The estimation of the bit error rate and entropy for encrypted as well as embedded data images was determined.

The amount of inaccurately retrieved bits of the hidden information that was obtained is shown by the bit error rate. It has the potential to be retrieved utilizing the MSG-RNN method that has a zero-bit error rate and indicates in which the embedded information is extracted effectively. Table 1 and Fig 1 show more information on the demonstrated MSG-RNN technique's bit error rate and embedding capacity.

Table 1. Images of the airplane, peppers, boat, baboon and have several bit error rate

Methods	Image Name (Bit Error Rate)			
	Baboon	**Boat**	**Airplane**	**Peppers**
RDH [16]	0.0625	0.0625	0.0625	0.0625
MSG-RNN [Proposed]	0.0513	0.0516	0.0511	0.0517

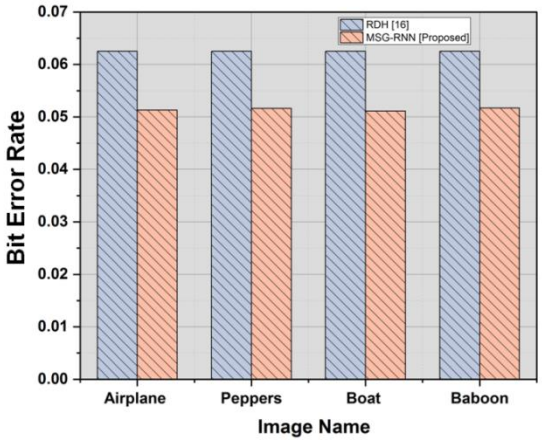

Fig 1. Comparison of Bit Error Rate Outcomes in images

Visual programming with a lot of unpredictable behavior is appropriate for the message as its pixels appear effectively similar. An encrypted image in which there is no tendency for the pixels to be matched in any manner could contribute to the desired patterns created by the encryption method. Entropy is an arithmetical calculation of uncertainty, which is able to utilize and determine the appearance of the original image. The encrypted images have increased entropy compared to the images. The entropy values for the data embedded and encrypted images such as the boat, baboon, airplane and pepper were displayed in Table 2 and Fig (2a) and (2b).

Table 2. Measured entropy on images Outcomes

Methods	Entropy (Encrypted Image)			
	Airplane	**Peppers**	**Boat**	**Baboon**
RDH [16]	7.9992	7.9992	7.9993	7.9994
MSG-RNN [Proposed]	8.19	8.24	8.15	8.11
Methods	**Entropy (Image with Data Embedded)**			
RDH [16]	7.9992	7.9992	7.9993	7.9994
MSG-RNN [Proposed]	8.19	8.24	8.15	8.11

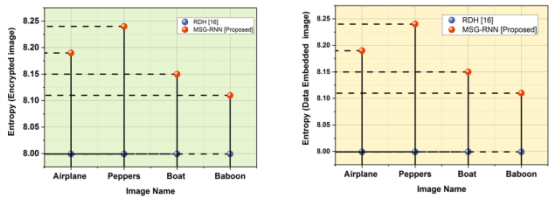

Fig 2. Comparison outcomes of Entropy (a) encrypted image, (b) embedded image

We evaluated the effectiveness of MSG-RNN integration in comparison with various RDH, RDH-CNN and EIRDH methods of similar features. In Table 3 and Fig 3, the comparison is shown. The basic objective of embedding the data and preserving the encrypted image's pixel distribution was accomplished.

Table 3. Comparing images of peppers, boats, baboons, and airplanes using various techniques

Methods	Values			
	Peppers	**Boat**	**Baboon**	**Airplane**
RDH [16]	0.0625	0.0625	0.0625	0.0625
RDH-CNN [17]	0.0547	0.0547	0.0547	0.0547
EIRDH [18]	0.0047	0.0072	0.0072	0.0011
MSG-RNN [Proposed]	0.0712	0.0714	0.0716	0.0719

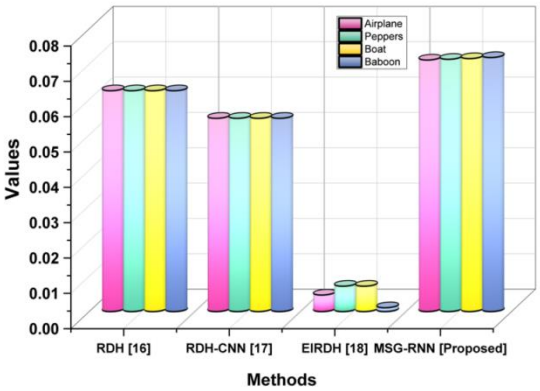

Fig 3. Comparison of proposed and existing methods outcomes

The majority of RDH [16] technique has limitations in the area of embedded capability and security. Data visibility coupled with effectiveness can be limited and it can have an impact on the speed and efficacy of data analysis as well as processing. Numerous issues with RDH-CNN [17] include a large memory footprint, an impulse of performance significantly slower, interpretability issues and a potential to process much slower. EIRDH possesses certain disadvantages including the requirement for extra money, assets for implementation and maintenance along with the integration of hazards as well as complications in managing data. Our proposed method shows an improved performance in airplanes, peppers, boats and baboons than other methods in image encryption and data hiding. For the analysis of sequential and repetitive information such as text, videos and images, MSG-RNNs are more effective. Its rapid convergence and efficiency in identifying global solutions are its main benefits.

5. Conclusion

We created an innovative independent information hiding technique in encrypted images utilizing the MSG-RNN method. The original image's data are fully encrypted using an encryption. By modifying an amount of the encrypted data, Extra data can be embedded in the encrypted image by hiding the data, which cannot be used for the original data. USC-SIPI image database is employed for the evaluation of experimental validation of the proposed method and the outcomes are evaluated through the use of a variety of images. For hiding the data ECC encryption technique was determined. More significant outcomes have been obtained by our proposed method's performance for data-embedded images, encrypted images and bit error rates. The comparison evaluation demonstrated the higher performance of the MSG-RNN methodology over other existing techniques. The MSG-RNN technique provided superior outcomes in various images like Boat (0.0714), Airplane (0.0719), Pepper (0.0712) and Baboon (0.0716). The proposed MSG-RNN is effective in revolutionizing image encryption and data hiding, based on a privacy investigation of the obtained experimental outcomes. Further study in this field could investigate more possibilities to enhance the use of available images for privacy in communication. It has been determined that the proposed image encryption techniques have the potential to be used in hardware in the future to enable efficiency.

References

[1] Chen, H., Song, L., Qian, Z., Zhangtrew, X. and Ma, K., (2022). Hiding images in deep probabilistic models. Advances in Neural Information Processing Systems, 35, pp.36776-36788.

[2] Jan, A., Parah, S.A., Malik, B.A. and Rashid, M., (2021). Secure data transmission in IoTs based on CLoG edge detection. Future Generation Computer Systems, 121, pp.59-73.

[3] Al-Jarah, A.I.H. and Arjona, J.L.O., (2021), December. Secret Key Steganography: improve security level of LSB algorithm. In 2021 IEEE 12th Annual Ubiquitous Computing, Electronics & Mobile Communication Conference (UEMCON) (pp. 0215-0220). IEEE.

[4] Gabr, M., Alexan, W., Moussa, K., Maged, B. and Mezar, A., (2022), July. Multi-stage rgb image encryption. In 2022 International Telecommunications Conference (ITC-Egypt) (pp. 1-6). IEEE.

[5] Chai, H., Li, Z., Li, F. and Zhang, Z., (2022). An end-to-end video steganography network based on a coding unit mask. Electronics, 11(7), p.1142.

[6] Gohil, J., Patel, J. and Shah, M., (2021). Content watermarking and data hiding in multimedia security. In Advanced Security Solutions for Multimedia (pp. 3-1). Bristol, UK: IOP Publishing.

[7] Chaudhary, A., Sharma, A. and Gupta, N., (2023). Designing A Secured Framework for the Steganography Process Using Blockchain and Machine Learning Technology. International Journal of Intelligent Systems and Applications in Engineering, 11(2s), pp.96-103.

[8] Selvaraj, J., Lai, W.C., Kavin, B.P. and Seng, G.H., (2023). Cryptographic Encryption and Optimization for Internet of Things Based Medical Image Security. Electronics, 12(7), p.1636.

[9] Tasevski, I., Nikolovska, V., Petrova, A., Dobreva, J., Popovska-Mitrovikj, A. and Dimitrova, V., (2022), October. StegYou: model for hiding, retrieving and detecting digital data in images. In Proceedings of the Future Technologies Conference (pp. 467-485). Cham: Springer International Publishing.

[10] Zheng, Z., Hu, Y., Bin, Y., Xu, X., Yang, Y. and Shen, H.T., (2022). Composition-Aware Image Steganography Through Adversarial Self-Generated Supervision. IEEE Transactions on Neural Networks and Learning Systems.

[11] Chen, J., Chen, L. and Zhou, Y., (2020). Cryptanalysis of a DNA-based image encryption scheme. Information Sciences, 520, pp.130-141.

[12] Chen, Y.C. and Shiu, C.W., (2021). Distributed encrypted image-based reversible data hiding. Journal of Internet Technology, 22(1), pp.101-107.

[13] Naman, H., Hussien, N., Al-dabag, M. and Alrikabi, H., (2021). Encryption System for Hiding Information Based on Internet of Things.

[14] Yang, Y.G., Wang, B.P., Yang, Y.L., Zhou, Y.H., Shi, W.M. and Liao, X., (2021). Visually meaningful image encryption based on universal embedding model. Information Sciences, 562, pp.304-324.

[15] ALRikabi, H.T.S. and Hazim, H.T., (2021). Enhanced data security of communication system using combined encryption and steganography. iJIM, 15(16), p.145.

[16] Panchikkil, S., Vegesana, S.P., Manikandan, V.M., Donta, P.K., Maddikunta, P.K.R. and Gadekallu, T.R., (2023). An ensemble learning approach for reversible data hiding in encrypted images with fibonacci transform. Electronics, 12(2), p.450.

[17] Panchikkil, S., Manikandan, V.M. and Zhang, Y.D., (2022). A convolutional neural network model based reversible data hiding scheme in encrypted images with block-wise Arnold transform. Optik, 250, p.168137.

[18] Bhardwaj, R. and Aggarwal, A., (2020). An improved block based joint reversible data hiding in encrypted images by symmetric cryptosystem. Pattern Recognition Letters, 139, pp.60-68.