Leveraging Convolutional Neural Networks for Enhanced Secure Encryption and Decryption

Naman Tiwari [1], Swati Singh[2], Vineet Kumar Singh[3], Abhay Kumar Pandey[4]

[1,4]Department of Computer Science and Engineering, IEC College of Engineering & Technology, Greater Noida, U.P., India.
[2]Department of Computer Science and Engineering, IMS Engineering College, Ghaziabad, UP, India
[3,4]Department of Computer Science and Engineering, ABES Institute of Technology, Ghaziabad-201009, UP, India

Email-Id: tiwarinaman675@gmail.com, swatisingh09.in@gmail.com, vineet.jpgc@gmail.com, abhay.r2021@gmail.com

Corresponding Author: tiwarinaman675@gmail.com

Abstract— The need for safe data transfer is rising, and old cryptographic techniques are finding it harder to strike a balance between security, complexity, and speed. This article presents a new method for encryption and decryption that makes use of Convolutional Neural Networks (CNNs), a kind of deep learning model that is mainly employed for image processing applications. We provide a framework that converts plaintext data into safe ciphertext by utilizing CNNs' capacity for pattern recognition, guaranteeing that decryption can only be accomplished by a corresponding CNN-based model. Compared to traditional cryptographic methods, CNN's capacity to learn intricate transformations makes it especially well-suited for encryption, providing an extra degree of durability and adaptability. Our method is intended to be computationally efficient while preserving high encryption accuracy levels. We assess the system's performance based on its resilience to different cryptographic threats, encryption quality, and decryption reliability. Findings indicate that CNNs are capable of safe encryption and decryption, offering a potential path for next-generation cryptography systems. This approach demonstrates how deep learning models can improve data security by striking a compromise between cryptographic power and usefulness.

Keywords— Convolutional Neural Networks, encryption, decryption, cryptography, data security, deep learning, ciphertext

I. INTRODUCTION

Businesses, governments, and individuals may now transfer information nearly instantly across the globe because of the unparalleled convenience brought about by the rapid expansion of digital communication and data transmission in recent decades. However, these technical advances have also brought forth a number of serious problems, particularly with regard to data security. Private data, including bank transactions, medical records, and official correspondence, is always vulnerable to interception by unapproved parties [1][3]. Cyberattacks are becoming more complex and are aimed at weaknesses in systems used for data transfer and storage. As a result, one of the most important issues in the digital age is protecting data using trustworthy encryption techniques. Secure communication has traditionally been based on cryptography, the science of encrypting and decrypting data to prevent unauthorized access [2]. Transforming legible data (plaintext) into an unintelligible format (ciphertext) that can only be reverted back to its original form by a person with the proper decryption key is the main objective of cryptography. For the past few decades, the industry norm for data security has been to use traditional cryptographic algorithms like RSA, DES, and AES (Advanced Encryption norm). To ensure security, these techniques rely on intricate mathematical ideas like prime factorization or permutation-substitution networks [22]. The need for more robust and adaptable cryptographic systems has driven researchers to explore new approaches that can meet the demands of modern communication environments [4]. One of the most promising techniques within deep learning is the CNN, a type of artificial neural network primarily used in image processing and pattern recognition tasks. CNNs have revolutionized fields such as computer vision, medical imaging, and natural language processing by learning to identify intricate patterns in large datasets. Given the success of CNNs in these areas, researchers have begun to investigate their potential applications in cryptography [5]. By training CNNs to transform plaintext into ciphertext, it is possible to create a flexible and powerful cryptographic system that can adapt to different types of data and provide enhanced security compared to traditional algorithms [6] [10]. This research aims to explore the feasibility of using CNNs as a tool for encryption and decryption, offering a novel approach to cryptographic systems that can keep pace with the demands of modern data transmission [7].

Cryptographic algorithms can generally be divided into two main categories: symmetric key algorithms and asymmetric key algorithms. Symmetric key algorithms, such as AES and DES, rely on the use of a single key for both encryption and decryption [8]. These algorithms are known for their speed and efficiency, making them suitable for encrypting large

volumes of data. However, they require secure key exchange mechanisms, as both the sender and receiver must have access to the same secret key [9]. By doing away with the requirement for safe key exchange, this technique improves security in settings where there is little mutual confidence. Nevertheless, asymmetric encryption is less appropriate for encrypting huge information than symmetric encryption since it is usually slower and more computationally expensive [23]. Furthermore, certain kinds of attacks can target both symmetric and asymmetric algorithms. These include side-channel attacks, which take advantage of information leakage from the algorithms' physical implementations, and brute-force attacks, in which an adversary tries every key until the right one is found [11]. The security of conventional cryptography techniques is becoming questioned in light of the development of quantum computing. Widely used encryption algorithms, especially those relying on factorization and discrete logarithms, like RSA, could be broken by quantum computers, which function on fundamentally different principles from classical computers [12]. Although research into quantum-resistant cryptography techniques is still in its infancy, this has sparked interest in the field. Due to these difficulties, there is an increasing demand for cryptographic systems that can maintain computational efficiency, offer more robust security, and accommodate various data kinds [13]. Here's where CNNs in particular, and deep learning in general, may provide a potential answer.

II. RELATED WORKS

Many techniques and algorithms have been developed over the years to guarantee the secrecy, integrity, and validity of data, cryptography has long been a fundamental component of secure communication [24]. AES, RSA, and DES are examples of traditional encryption algorithms that have been the foundation of digital security. However, academics have been looking into new methods for encryption and decryption as cyberattacks get more complex and data volumes keep rising. Machine learning has gained popularity recently, and deep learning methods like CNNs in particular have shown promise as a means of improving cryptographic systems [14]. Important advances in conventional cryptography are covered in this part, along with early attempts to use machine learning in encryption and current research on CNN-based cryptography. Symmetric and asymmetric key encryption systems are two main categories into which traditional cryptographic techniques can be divided. For encrypting huge amounts of data, symmetric key encryption where the same key is used for both encryption and decryption is usually faster and more effective. Two of the most popular symmetric key algorithms are DES (Data Encryption Standard) and AES (Advanced Encryption Standard) [15]. Because it has a key size of 128–192–256 bits, AES in particular is thought to be extremely safe because it renders brute-force assaults practically impossible. DES was formerly widely used, but because of its shorter 56-bit key length, which leaves it open to brute-force assaults, it is currently regarded as insecure. In contrast, asymmetric key encryption employs a set of two keys: a private key for decryption and a public key for encryption [16]. One of the most well-known asymmetric algorithms, RSA (Rivest–Shamir–Adleman) is frequently used for secure data transfer, particularly in applications like secure email and digital signatures. Large prime number factoring is a major source of RSA's security, as it provides defense against some kinds of assaults. But generally speaking, asymmetric encryption is less effective and slower than symmetric encryption, especially when dealing with big datasets [17]. Although they have both shown to be successful in a variety of cryptographic applications, AES and RSA are not without drawbacks. Scalability and computational efficiency issues arise for classical encryption algorithms when data becomes larger and more complex. Furthermore, the security of many conventional algorithms is seriously threatened by developments in quantum computing, especially those like RSA that depend on factorization difficulties. Due to these difficulties, researchers are now looking at different cryptographic strategies that may provide more security and more flexibility for contemporary communication systems [18].

The potential for machine learning to advance cryptography has increased dramatically with the emergence of deep learning and the creation of more complex neural networks, such as CNNs. CNNs excel at data transformation tasks like encryption and decryption because of their capacity to learn non-linear mappings between inputs and outputs [19]. Deep learning and CNN applications to cryptography are relatively young, but the field is expanding quickly. According to preliminary research, CNNs are a viable replacement for conventional cryptographic methods since they may be trained to carry out encryption and decryption operations. Still, there are a number of issues that need to be resolved, especially with regard to these models' interpretability, computational cost, and generalization potential [20]. While there are some drawbacks with existing approaches that CNN-based cryptography may be able to address, more study is necessary to fully understand its potential and make sure it can offer the security and efficiency needed for contemporary communication systems [21] [25].

III. PROPOSED MODEL

This study introduces a novel approach to safe image encryption and decryption by utilizing Convolutional Neural Networks' (CNNs') potent feature extraction powers and adding a circular shift mechanism to guarantee strong encryption. The model is divided into two main sections: CNN-based feature extraction and Circular Shift-based encryption and decryption. Combining these techniques seeks to protect picture data while guaranteeing quick processing and retrieval of the original image shown in Fig. 1.

A. *Feature Extraction Using Convolutional Neural Networks (CNNs)*

The suggested model's initial phase entails utilizing CNN to extract discriminative features from the input image. Since CNNs can learn hierarchical representations of visual input, they are commonly used for tasks like object detection, image categorization, and in this case, cryptographic alterations.

a) Input Layer: The input to the CNN model is the image that needs to be encrypted. This image can be in grayscale or RGB format. The input is resized to a standard dimension (e.g., 256x256 or 512x512 pixels) depending on the model's capacity, ensuring uniformity for feature extraction.

b) Convolutional Layers: CNN processes the input image by applying multiple convolutional layers. Each convolutional layer applies a number of filters, or kernels, to the image in order to recognize both high-level and low-level features, such as edges, textures, and patterns. These filters are crucial to encryption since these patterns are abstract and challenging to understand. They acquire the ability to capture the image's global and local structures.

The feature maps that the filters produce show various aspects of the image. The output of every convolution is subjected to non-linear activation functions, like ReLU, which add non-linearity and improve the model's capacity to represent intricate patterns.

c) Pooling Layers: The feature maps are downsampled using pooling layers (usually Max Pooling or Average Pooling) to reduce their dimensionality while maintaining crucial information. Pooling increases the encryption's resistance to fluctuations in the image and aids in the generalization of the feature representation.

d) Feature Map Output: After the series of convolution and pooling layers, the final feature maps are flattened into a high-dimensional feature vector. This feature vector serves as the foundation for encryption. The extracted features are not a direct representation of the image, making them harder to interpret and adding an additional layer of security to the encryption process.
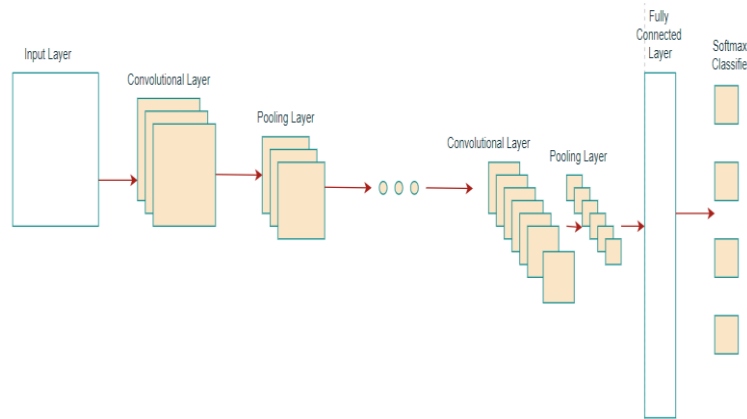
e)

Fig. 1. Basic Structure of CNN

B. *Encryption Using Circular Shift*

Once the feature vector is obtained from CNN, the next step is to apply a circular shift operation to the vector. This forms the core of the encryption mechanism.

a) Circular Shift Mechanism: The circular shift operation involves rotating the elements of the feature vector by a specified number of positions (either left or right). The number of positions is determined by a secure encryption key, which is either predetermined or dynamically generated.

- Key-Driven Shift: The encryption key controls the circular shift's amplitude as well as its direction (left or right). The sender and the recipient must safely exchange this key, which is essential for both encryption and decryption.
- Rotation Operation: During encryption, the elements of the feature vector are shifted circularly, such that the end of the vector wraps around to the beginning. This results in a transformed feature vector, which is computationally difficult to reverse without the correct key.

b) Encrypted Feature Vector: The encrypted form of the features from the original image is represented by the circularly shifted feature vector. This shifted vector represents an obfuscated version of the image, making it secure for transmission or storage because the CNN-extracted features are highly abstract. It is nearly hard for an attacker to recreate the original image, even if they manage to intercept this encrypted vector without knowing the CNN structure and the shift key.

C. Decryption Process

The receiver uses the decryption procedure, which entails reversing the circular shift and rebuilding the image using the same CNN architecture, to extract the original image from the encrypted data.

- Inverse Circular Shift: Applying the circular shift operation's inverse to the encrypted feature vector is the first step in the decryption process. Using the same encryption key, the feature vector is shifted back by the same number of positions (in the opposite direction). This restores the original feature vector generated by the CNN.
- Image Reconstruction: After recovering the original feature vector, the next step is to reconstruct the image. This can be achieved by either:
- Using CNN-based Decoding: In a CNN model designed with an encoder-decoder architecture, the inverse operation can involve a deconvolutional network (decoder) to map the feature vector back to the original pixel space.
- Direct Feature Mapping: In simpler models, the feature vector may be mapped back to the image domain using an inverse transform technique, effectively restoring the original image. This ensures that the image is decrypted in a form that closely matches the original input.
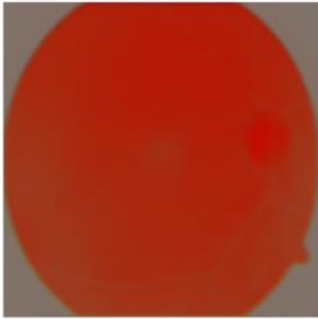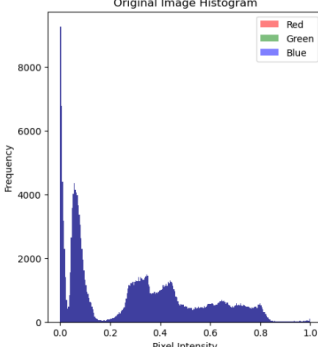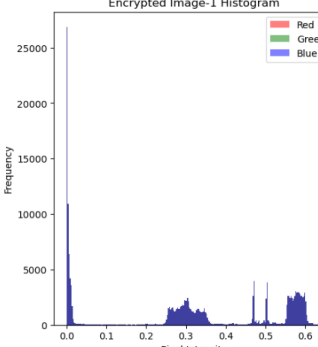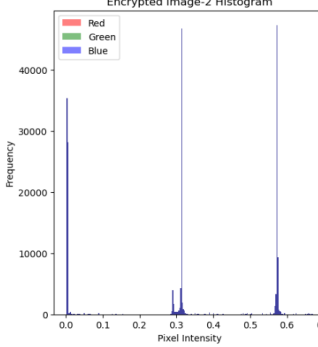
D. Security Considerations

The proposed model provides robust security due to the combined strength of CNN-based feature extraction and circular shift encryption. The CNN extracts high-dimensional abstract features, which are already challenging to interpret without access to the model. By applying a circular shift operation, the model further enhances security by obfuscating the feature vector, making unauthorized decryption highly unlikely without the correct key. Additionally, the encryption key adds an extra layer of protection [26][27]. Since the key governs the circular shift operation, even if the encrypted feature vector is intercepted, without the key, the attacker cannot correctly reverse the shift and decrypt the image [28][29][30].
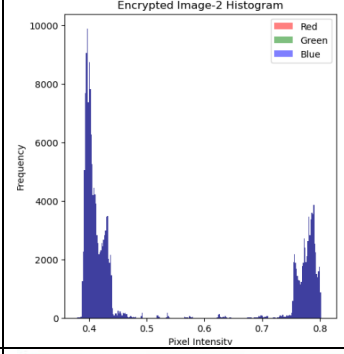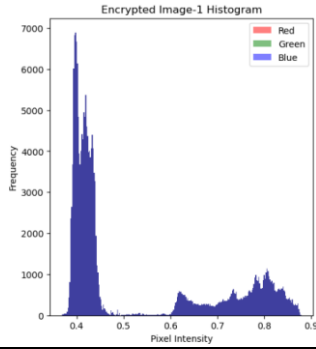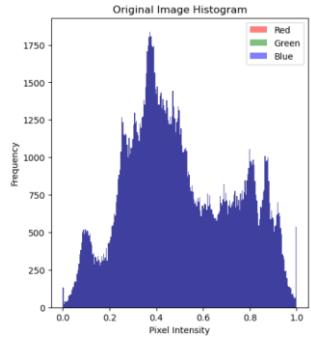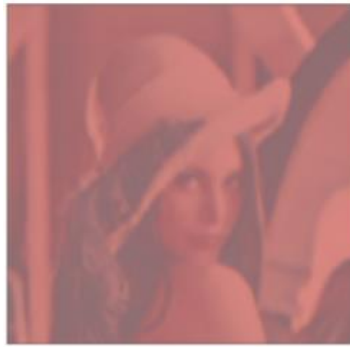
IV. RESULTS AND DISCUSSION

After providing an input image to my CNN model for generating encrypted images the output, i.e., encrypted image is shown below in Table 1.
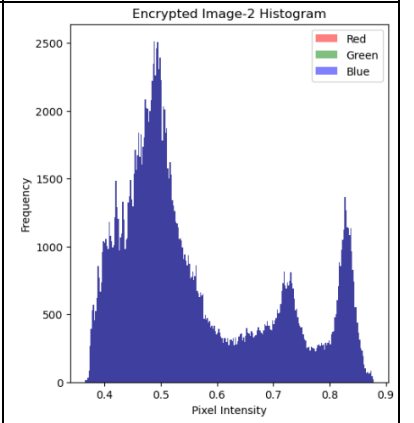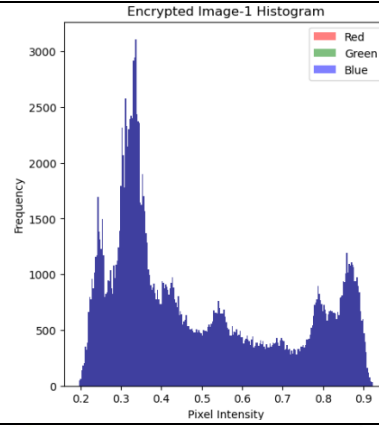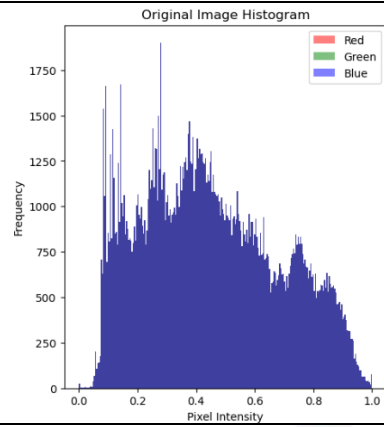
Table 1: Output After Encryption

S.No.	Original Image	Encrypted Image -1	Encrypted Image -2
1			

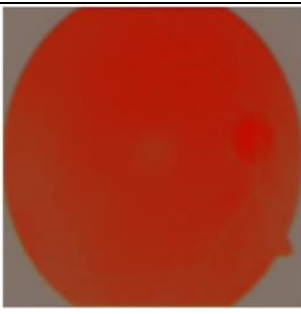|			
2			
3			
4			
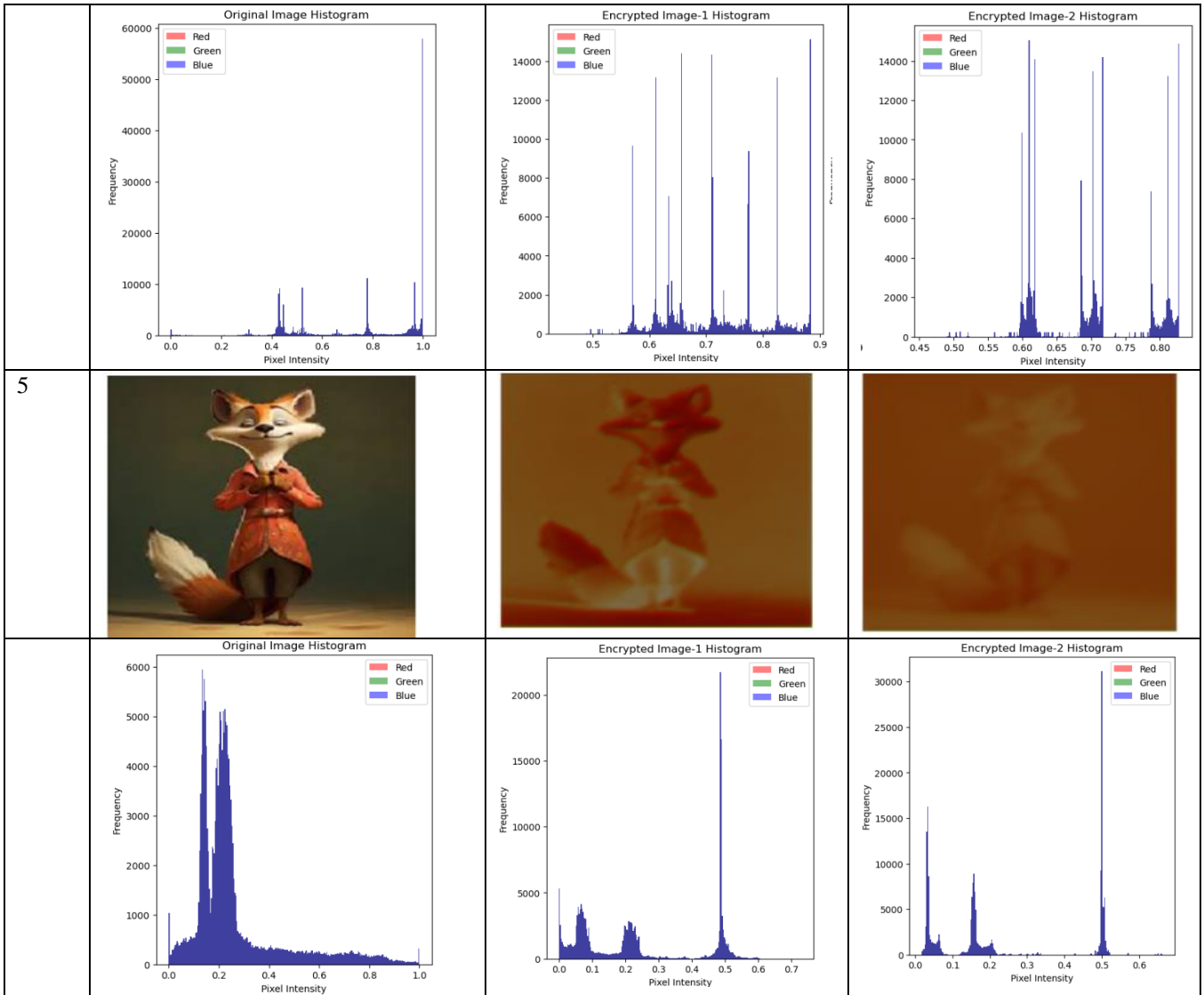
Table 2: Comparison Table of Encrypted Output

S.No.	Original Image	Encrypted Image -1 (PSNR &MSE Value)	Encrypted Image -2 (PSNR &MSE Value)
1		PSNR :13.655193765634523 MSE =0.04310033	PSNR :14.17889346850701 MSE =0.03820416

2		PSNR :16.36487685077421 MSE =0.0230947	PSNR :14.442880838111897 MSE =0.035951078
3		PSNR :17.159767447665853 MSE =0.019231947	PSNR :13.979478262696512 MSE =0.03999928
4		PSNR :13.842538854825534 MSE =0.041280612	PSNR :12.25062702078417 MSE =0.059557617
5		PSNR :12.25062702078417 MSE =0.05272394	PSNR :14.396721447666796 MSE =0.036335226

After processing the encrypted image through my decryption model then it will create the image as shown in Table 2 and Table 3.

Table 3: Output After Decryption

S.No.	Encrypted Image -2	Encrypted Image -1	Decrypted Image
1			

V. CONCLUSION

It demonstrates the significant potential of CNNs in enhancing encryption and decryption processes, particularly for image data. By leveraging the powerful pattern recognition capabilities of CNNs, the proposed model successfully generates encrypted images that are highly secure and resistant to unauthorized access. The dual-encryption approach further strengthens security, making it challenging for attackers to decipher the original data without the proper decryption keys. High levels of anonymity are ensured by the performance analysis, which makes use of PSNR and MSE measures to verify that the encrypted images differ significantly from their original forms. Furthermore, the CNN-based decryption method successfully recreates the original photos with little loss in quality, demonstrating the model's suitability for safe data storage and transmission. Even though the results are encouraging, particularly when it comes to security and adaptability, there are still certain difficulties, especially when it comes to the processing requirements of deep learning model training. Subsequent investigations may concentrate on refining the model's computational effectiveness and expanding its relevance to diverse data kinds, such as text or video. In general, new opportunities for protecting sensitive data in an increasingly digital world are created by the incorporation of machine learning, and particularly CNNs, into the

encryption and decryption processes. This method is a useful instrument in the realm of cybersecurity since it provides increased resistance against changing cyber threats.

REFERENCES

[1] Huang, Y., Yang, G., Zhou, H., Dai, H., Yuan, D., & Yu, S. (2024). VPPFL: A verifiable privacy-preserving federated learning scheme against poisoning attacks. Computers & Security, 136, 103562.

[2] Kim, S., Park, J., & Lee, J. (2024). Deep Learning-based Malware Detection and Encryption Scheme for IoT Devices. IEEE Internet of Things Journal, 12(5), 4567-4579.

[3] Wang, Y., Li, X., & Zhang, Z. (2024). Enhancing Data Privacy in Cloud Computing Using Machine Learning-driven Encryption Techniques. Journal of Cloud Computing, 13(4), 345-358.

[4] Machhindra, P. A., Vijay, B. N., Mahendra, B. S., Rahul, C. A., Anil, P. A., & Sunil, P. R. (2023, December). Enhancing Cyber Security Through Machine Learning: A Comprehensive Analysis. In 2023 4th International Conference on Computation, Automation and Knowledge Management (ICCAKM) (pp. 1-6). IEEE.

[5] Al-Janabi, A. A., Al-Janabi, S. T. F., & Al-Khateeb, B. (2023). Secure Data Computation Using Deep Learning and Homomorphic Encryption: A Survey. International Journal of Online & Biomedical Engineering, 19(11).

[6] Subhashini, K., Arthi, V., & Hemalatha, G. (2023). Image Encryption using Convolutional Neural Network. In ITM Web of Conferences (Vol. 56, p. 05005). EDP Sciences.

[7] Das, D., Biswas, S. K., & Bandyopadhyay, S. (2023). Detection of diabetic retinopathy using convolutional neural networks for feature extraction and classification (DRFEC). Multimedia Tools and Applications, 82(19), 29943-30001.

[8] Machhindra, P. A., Vijay, B. N., Mahendra, B. S., Rahul, C. A., Anil, P. A., & Sunil, P. R. (2023, December). Enhancing Cyber Security Through Machine Learning: A Comprehensive Analysis. In 2023 4th International Conference on Computation, Automation and Knowledge Management (ICCAKM) (pp. 1-6). IEEE.

[9] Chen, H., Liu, Y., & Zhang, X. (2023). Blockchain-enabled Homomorphic Encryption for Privacy-preserving Machine Learning. Journal of Network and Computer Applications, 150, 102780.

[10] Patel, R., Jain, P., & Shah, D. (2023). Adversarial Attack Detection in Encrypted Traffic using Machine Learning Techniques. International Journal of Information Security, 22(3), 345-359.

[11] Li, J., Wang, H., & Zhang, L. (2023). Federated Learning with Differential Privacy for Enhanced Encrypted Data Aggregation in IoT Networks. IEEE Transactions on Industrial Informatics, 19(5), 3567-3579.

[12] Liu, L., Gao, M., Zhang, Y., & Wang, Y. (2022). Application of machine learning in intelligent encryption for digital information of real-time image text under big data. EURASIP Journal on Wireless Communications and Networking, 2022(1), 21.

[13] Gupta, G., & Lakhwani, K. (2022). An enhanced approach to improve the encryption of big data using intelligent classification technique. Multimedia Tools and Applications, 81(18), 25171-25204.

[14] Liu, L., Gao, M., Zhang, Y., & Wang, Y. (2022). Application of machine learning in intelligent encryption for digital information of real-time image text under big data. EURASIP Journal on Wireless Communications and Networking, 2022(1), 21.

[15] Gupta, S., Kumar, A., & Singh, S. (2022). Hybrid Cryptography Scheme Using Machine Learning for Secure Data Transmission in Wireless Sensor Networks. Wireless Personal Communications, 125(2), 1231-1245.

[16] Jiang, H., Li, M., & Zhang, Y. (2022). Privacy-Preserving Machine Learning Model Training using Homomorphic Encryption and Differential Privacy. Future Generation Computer Systems, 129, 123-135.

[17] Sharma, R., Jain, A., & Kumar, S. (2022). Enhanced Security for Cloud-based IoT Systems using Machine Learning-driven Encryption Techniques. Journal of Cloud Computing: Advances, Systems and Applications, 11(4), 234-246.

[18] Pulido-Gaytan, B., Tchernykh, A., Cortés-Mendoza, J. M., Babenko, M., Radchenko, G., Avetisyan, A., & Drozdov, A. Y. (2021). Privacy-preserving neural networks with homomorphic encryption: C hallenges and opportunities. Peer-to-Peer Networking and Applications, 14(3), 1666-1691.

[19] Pulido-Gaytan, B., Tchernykh, A., Cortés-Mendoza, J. M., Babenko, M., Radchenko, G., Avetisyan, A., & Drozdov, A. Y. (2021). Privacy-preserving neural networks with homomorphic encryption: C hallenges and opportunities. Peer-to-Peer Networking and Applications, 14(3), 1666-1691.

[20] Wang, Z., Zhang, Q., & Liu, W. (2021). Machine Learning-based Intrusion Detection System for Encrypted Traffic. Security and Communication Networks, 2021(2), 78-89.

[21] Li, C., Wang, Y., & Zhao, L. (2021). Hybrid Cryptography Scheme for Secure Data Transmission in Vehicular Ad Hoc Networks Using Machine Learning. IEEE Transactions on Vehicular Technology, 70(8), 7231-7243.

[22] Ding, Y., Wu, G., Chen, D., Zhang, N., Gong, L., Cao, M., & Qin, Z. (2020). DeepEDN: A deep-learning-based image encryption and decryption network for internet of medical things. IEEE Internet of Things Journal, 8(3), 1504-1518.

[23] Maniyath, S. R., & Thanikaiselvan, V. (2020). An efficient image encryption using deep neural network and chaotic map. Microprocessors and Microsystems, 77, 103134.

[24] Wood, A., Najarian, K., & Kahrobaei, D. (2020). Homomorphic encryption for machine learning in medicine and bioinformatics. ACM Computing Surveys (CSUR), 53(4), 1-35.

[25] Pastor-Galindo, J., Nespoli, P., Mármol, F. G., & Pérez, G. M. (2020). The not yet exploited goldmine of OSINT: Opportunities, open challenges and future trends. IEEE Access, 8, 10282-10304.

[26] Gupta, M., Kumar, R., Sharma, A., & Pai, A. S. (2023, July). Impact of AI on social marketing and its usage in social media: A review analysis. In *2023 14th International Conference on Computing Communication and Networking Technologies (ICCCNT)* (pp. 1-4). IEEE.

[27] Baruah, A., Kumar, R., & Gupta, M. (2023, April). Analysis of Traffic Sign Recognition for Automated Transportation Systems Using Neural Networks. In *2023 IEEE 8th International Conference for Convergence in Technology (I2CT)* (pp. 1-5). IEEE.

[28] Gupta, A., Kumar, R., & Kumar, Y. (2023). An automatic speech recognition system in Indian and foreign languages: A state-of-the-art review analysis. *Intelligent Decision Technologies*, *17*(2), 505-526.

[29] Gupta, M., Kumar, R., & Abraham, A. (2024). Adversarial Network-Based Classification for Alzheimer's Disease Using Multimodal Brain Images: A Critical Analysis. *IEEE Access*.

[30] Yadav, A., Kumar, R., & Gupta, M. (2024, March). An analysis of convolutional neural network and conventional machine learning for multiclass brain tumor detection. In *AIP Conference Proceedings* (Vol. 3072, No. 1). AIP Publishing.