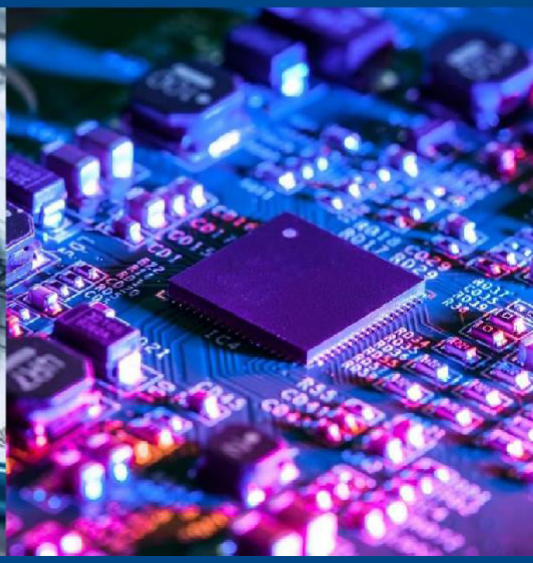
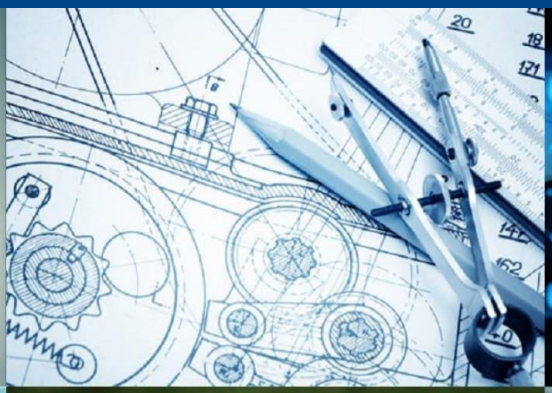
ISSN: 2582-7219

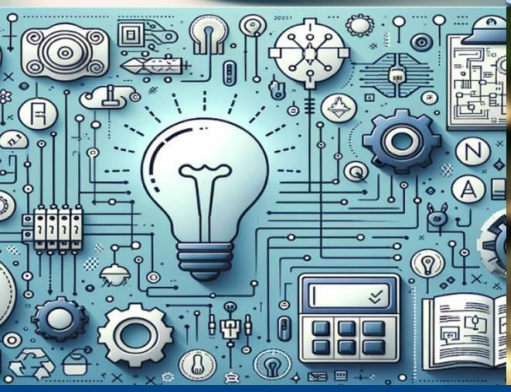




International Journal of Multidisciplinary Research in Science, Engineering and Technology

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)



Impact Factor: 8.206 **Volume 8, Issue 7, July 2025**

© 2025 IJMRSET | Volume 8, Issue 7, July 2025| DOI:10.15680/IJMRSET.2025.0807080

ISSN: 2582-7219 | www.ijmrset.com | Impact Factor: 8.206| ESTD Year: 2018|

International Journal of Multidisciplinary Research in Science, Engineering and Technology (IJMRSET)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

Advancing Image Encryption using Neural Network Architectures

Rubeena Khanum, Prof. Shanmukaswamy C.V

M.Tech (CSE) Student, Shreedevi Institute of Engineering and Technology, Tumkur, Karnataka, India

Associate Professor, Dept. of CSE, Shreedevi Institute of Engineering and Technology, Tumkur, Karnataka, India

ABSTRACT: The sense of neural networks in deep learning is being applied progressively within the domain of picture encryption as the need for data encryption and information protection intensifies, and neural network's impact on this sector is steadily expanding. The current popular network image encryption techniques fall into two categories: chaotic systems and pixel disruption. in addition to an interpretation of the algorithmic framework and an examination of the encrypted image, this paper offers a basic introduction to the four network models for image encryption chaotic neural network, CNN, cellular neural networks and generative adversarial networks. All 4 neural network models have exhibit to be impacted by the models size and parameters; if the neural network encrypted image is very noisy- resistant, the image's is distortion will be greater, and image's visual entropy will rise in a proportion. A model has relatively wide key space, low correlation of nearby pixels, good encryption, and is a more challenging to crack if it is sensitive to the beginning value.

KEYWORD: *Image Encryption, Neural Networks. Cellular Neural Networks (CeNN), Chaotic Neural Networks (ChNN), Convolutional Neural Networks (CNN).*

I. INTRODUCTION

Strong and secure data encryption technology is now essential in the quickly changing digital world. traditional encryption techniques are becoming a more and more difficult to use as a technology develops and opponents computing power increases. This has caused scholars and professionals to start looking at a different encryption techniques. Neural network contain a chaotic complexities because they are a highly nonlinear system[25]. furthermore neural network are a perfect candidates for the creation of novel encryption algorithms due to their intrinsic nonlinear characteristics, which include a sensitive to beginning values, randomness, and unpredictability[9]. The significance of safeguarding private images, private documents, and other graphic information obtained through illegal access has increased as people continue to post and distribute these types of things online. This situation is made worse by a rise in because shared media are so widely used in today's communication environment, they are frequently the subject of cyber attacks, identity theft, and privacy concerns. The high degree of redundancy in images, which result from the innate connection between the nearby pixels is among the greatest important problems[1]. Image encryption is used in many fields, including telemedicine, business, medical imaging biometric authentication, and military communication, among others [6]. Technique for securing digital images include such as encryption, watermarking, and stenography. The most efficient of this is encryption, which uses a secret key to change the original image into an unintelligible format. No one could retrieve the original image without this key. Diffusion and confusion are the two processes that the picture encryption process depends on [10]. The fundamental encryption Figure 1 shows how it works. Because every type of data has different characteristics, Pictures and Images aren't as well-suited to traditional encryption methods as text or other types of data.

© 2025 IJMRSET | Volume 8, Issue 7, July 2025| DOI:10.15680/IJMRSET.2025.0807080

ISSN: 2582-7219 | www.ijmrset.com | Impact Factor: 8.206| ESTD Year: 2018|

International Journal of Multidisciplinary Research in Science, Engineering and Technology (IJMRSET)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

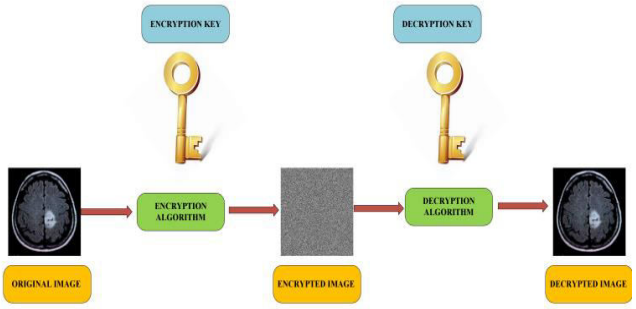


Figure 1: Image Encryption and Decryption

Consequently, a variety of tactics were used put in place to guarantee that private image data is shielded from unauthorized access [23]. To maintain the accuracy of pictures when they are processed sent, cryptographic technologies are employed [2]. The first step in ensuring that any electronic images are secure is frequently to use conventional encryption methods, that are well known due to their advanced level of security, to encrypt the image data. As a consequence, the discipline of cryptography has been advancing steadily in recent years with the introduction of whole new neural network models. Many models of neural networks are available at the moment, including the Hopfield neural network [7-20], cellular convolutional neural networks [11,3], adversarial neural networks [12,13], neural networks [24–22], etc., which have produced several iterations and outcomes in the field of cryptography, including image encryption and cryptographic method.

The focus of this paper is to evaluate the state of encryption research and applications based on various neural network models. This study will explain the use of neural network architectures by analyzing their advantages, disadvantages, and distinctiveness. picture encryption and the related security consequences. The basic for comprehending the working of neural network encryption will be laid by this papers Introduction to the Principles of Neural Networks.

II. RELATED WORK

Traditional research that is exclusively focused on image security are included in this section. In addition the literature employs chaotic approaches for photo encryption[7]. with these approaches, it is challenging to strike an appropriate balance between the encryption relevance and security effectiveness. To tackle various challenges, neural networks with multiple layers are often used to extract important features from raw images. Convolutional Neural Networks (CNNs), in particular, have gained a lot of attention for their success in computer vision tasks and image domain transfer [17]. These models help us understand how to transform an input image into a corresponding output image by learning from pairs of matched images. This process, often viewed as a form of texture transfer, involves transferring visual patterns and styles from one image domain to another. The cycle-reliable adversarial system [5] is one of the most commonly used techniques for image-to-image translation. It works by transforming an image from one domain to another and then reconstructing it back to its original form, ensuring reliability over two cycles of conversion. The image denoising issue is handled by the DL approach [18]. Image noise refers to unwanted random variations or disturbances in image data, often caused by interference during acquisition or transmission, which can obscure or degrade important visual information. Picture restoration is the procedure of picture denoising[19]. A novel rotation domain, dual image encryption method based on pixel scrambling and cross-images was proposed by authors of[4]. The previous authors proposed a dual image encryption technique in[5] that uses DNA spatiotemporal chaos, deletion, and insertion to increase the efficiency of encryption process security, jumble and imaginary data segments created by each encrypted cycle[21]. The technology combines scrambling and diffusion techniques with DNA sequence insertion and deletion techniques to encrypt two images at once. A novel dual image compression encryption technique that enhance the dual-image encryption approaches Robustness and secrecy was presented in references[14].These methods can encrypt to photos independently using the same encryption approach, requiring two decryptions to retrieve the two images[15], In their paper the authors of[16] suggested a technique for medical image cryptography that combines a chaotic and neural networks. The main objective of the suggested approach is to use a less complex technique than

ISSN: 2582-7219 | www.ijmrset.com | Impact Factor: 8.206| ESTD Year: 2018|

International Journal of Multidisciplinary Research in Science, Engineering and Technology (IJMRSET)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

existing ones to confirm the security of medical photos. Test results shows the effectiveness and performance of the suggested approach, which satisfies requirements for medical digital interaction and recording.

III. METHODOLOGY

The proposed research examines how many models of neural networks are applied to picture encryption and common models of neural networks for images encryption, including cellular, convolutional, and chaotic neural networks. Finding the artificial neural network models most commonly utilized in the field of picture encryption is the principle purpose of the first stage. Four different models—Chaotic Neural Networks (ChNN), Cellular Neural Networks (CeNN), and Convolutional Neural Networks (CNN), were chosen because of their strong performance in managing nonlinearity, randomness, and adaptive learning. Chaotic Neural Networks create pseudo-random encryption sequences by utilizing the chaotic characteristics of nonlinear systems. Cellular neural networks operate well in real-time encryption situations because of their dynamic updates and local connections. The research focuses on three widely adopted models of neural networks for images encryption:

A. Chaotic Neural Network (CNN)

Combining the features of artificial neural networks and chaos theory, chaotic neural networks may produce extremely complicated and unpredictable pseudo-random patterns suitable for picture encryption in the key generation and perturbation operation, which is most commonly used in the Hopfield neural network, the widely accepted classification as of right now:

1. Chaotic neural network based on weights perturbation: this method makes the network state uncertain by dynamically adjusting the neural network weights using chaotic sequences.
2. Input perturbation-based chaotic neural network: pictures are encrypted by chaotic input data mapping.
3. Hybrid chaotic neural networks, which contain chaotic perturbations in convolutional layers, are a deep fusion of neural network models with chaotic mapping. Figure 2 shows a standard structure for encryption algorithms.

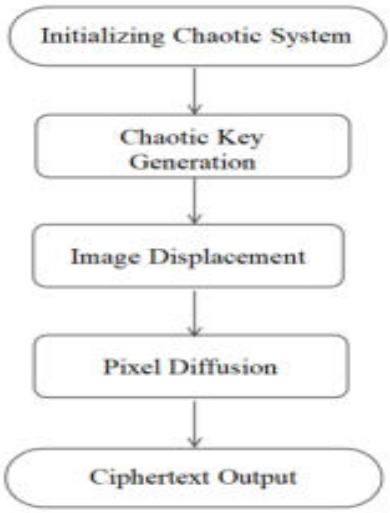


Figure 2: Typical chaotic neural network encryption algorithm

Several chaotic systems can serve as the foundation for the initial Unorganized framework that might then be utilized to create initial chaotic sequences, dynamic keys utilizing picture features, chaotic sequences to shift the ranks of the image pixels, and lastly chaotic sequences using the original pixel values for arithmetic element by element.

B. Cellular Neural Networks (CNN)

Neural network that operates in cells are primarily linked in neural networks that are effective at processing signals in real time and can handle picture data. The prevalent classification as of right now:

1. Cellular neural networks operating in continuous time: modeling a continuous dynamic system and applications differential equations to explain how the network state changes over time. Because it uses continuous dynamic

ISSN: 2582-7219 | www.ijmrset.com | Impact Factor: 8.206| ESTD Year: 2018|

International Journal of Multidisciplinary Research in Science, Engineering and Technology (IJMRSET)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

properties to produce high complexity encryption procedures, it is appropriate for dynamic encryption processes, such as the encryption of real-time image streams.

2. Cellular Neural Networks in discrete time: Differential equations are utilized to characterize the network state update to discrete time increments. It has the benefits of easy implementation and effective computation making it appropriate for encrypting static digital images.

3. Adaptive Cellular Neural Networks: To improve the randomness and security of encryption, network parameters (such as template parameters) are dynamically changed depending on the input image or external key.

Figure 3 shows a standard structure for encryption algorithms.

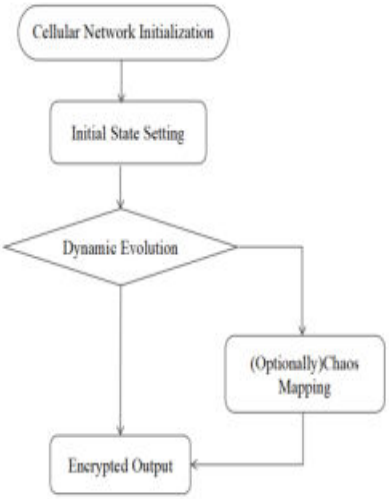


Figure 3: Cellular neural network encryption algorithm

C. Convolutional Neural Network (CNN)

Convolutional neural networks, which emphasize nonlinear mapping and feature extraction skills to increase the complexity and security of pictures, can automatically learn and extract features from them thanks to their variable parameter convolution, pooling, and fully connected layers. algorithms for cryptography. The classification used by the mainstream today:

1. Single-Layer Convolution Encryption: A single convolutional layer is used to carry out fundamental cryptographic operations on images, including diffusion and permutation.

2. Multi-Layer Convolution Encryption: By employing deep CNNs; multilevel feature extraction capability, multilayer convolutional operations improve the robustness and security of picture encryption.

3. Hybrid Convolution Encryption: The total security and complexity of cryptographic systems are increased by combining convolutional neural networks with other cryptographic approaches (such as chaotic mapping and conventional encryption algorithms). Figure 4 depicts a standard structure for encryption algorithms.

ISSN: 2582-7219 | www.ijmrset.com | Impact Factor: 8.206| ESTD Year: 2018|

International Journal of Multidisciplinary Research in Science, Engineering and Technology (IJMRSET)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

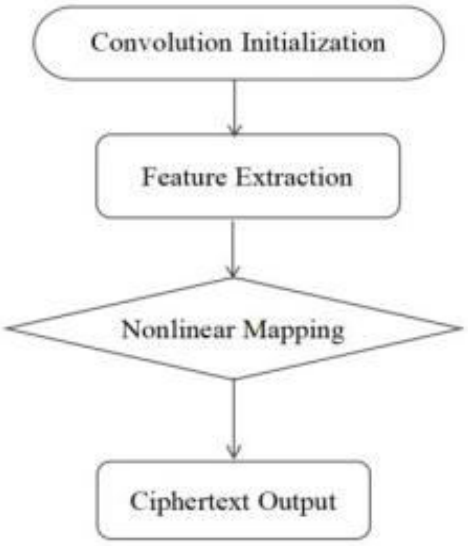


Figure 4: Typical convolutional neural network encryption algorithm

The convolutional neural system should be constructed, and the number of convolutional layers, pooling layer, and activation function should be determined. The convolutional layer should be employed to extract and distinguish the image, and the activation function and chaotic mapping should be introduced to facilitate the nonlinear encryption of image

IV. THE PROCESS OF ENCRYPTION AND DECRYPTION ALGORITHM

A. Encryption Algorithm

In neuron network based image encryption, an original image is transformed into an incomprehensible format in order to prevent the unwanted access. This start with preparing the image, such as scaling or normalizing a pixel value, to make sure it conforms to the input format needed by the neural network model. The encryption process is then driven by a the secret key or starting parameter, which is frequently created from the chaotic system or image specific properties. Whether it is a CNN, CeNN or ChNN, these selected neural network architecture applies a number of interact changes to the image.

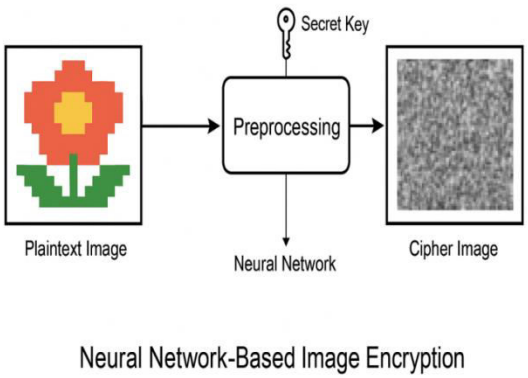


Figure 5: Neural Based Image Encryption

ISSN: 2582-7219 | www.ijmrset.com | Impact Factor: 8.206| ESTD Year: 2018|

International Journal of Multidisciplinary Research in Science, Engineering and Technology (IJMRSET)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

These changes included diffusion, which modifies the pixel intensity values to eliminate any visual patterns, and confusion, which confuses pixel positions. These neural models are able to provide extremely safe, pseudo-random outputs because of their inherent nonlinearity, randomness, and sensitivity to initial condition. These procedures a cipher image that is visually identical to original but has low pixel correlation and high entropy, providing robust defense against the statistical or a brute-force attacks. After encryption, this image can be safety stored or sent over unprotected channels.

Algorithm: Encrypt_Image

Input: Original_Image, Secret_Key

Output: Encrypted_Image
function Encrypt_Image (Original_image, Secret_Key):

#Step 1: preprocess the original image
Preprocessed_image= Preprocess_image(Original_image)

#Step 2: Generate key-based parameters using the Secret Key
Key_parameters=Generate Parameters From Key(Secret_Key)

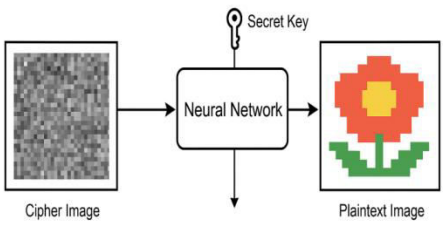
#Step 3: Use Neural Network with Key-Based parameters to transform image
Neural_Net=Initialize_Neural_Network (Parameters=Key_Parameters)
Encrypt_Image=Neural_Net.Transform (Preprocessed_Image)

#Step 4: store the result
Save_Image (Encrypted_Image)

#Step 5: return Encrypted_Image
Return Encrypted_Image

B. Decryption Algorithm

The goal of the decryption that is the opposite of the encryption process, is to return the encrypted image to its original State but only if the right key or a parameters are supplied. First the same architecture of neural networks utilized for encryption is fed to the encrypted image. The same secret key, chaotic sequence, or neural parameters used for encryption or used to establish the decryption model. With the help of these, the neural networking gradually undoes the images modification by reconstructing the original pixel values and unscrambling pixel position. Due to the extreme sensitivity of these procedures, the original image cannot be recovered even with the slight alteration in the key or in neural setup.



Neural Network-Based Image Decryption

Figure 6: Neural Based Image Decryption

ISSN: 2582-7219 | www.ijmrset.com | Impact Factor: 8.206| ESTD Year: 2018|

International Journal of Multidisciplinary Research in Science, Engineering and Technology (IJMRSET)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

The accuracy of the initial key and model configuration determines how well the decryption works, guaranteeing the original image can only be recovered by the authorized users with the right credentials. The outcome of reversing all modification is the reconstructed Plaintext image. Which to be structurally and similar to the input image before encryption. The resilience and dependability of neural network based encryption solution in processing the sensitive visual data are confirmed by the safe and accurate reversal.

Algorithm: decrypt_Image

Input: Encrypted_Image,Secret_Key

Output: Decrypted_Image
function Decrypt_Image (Encrypted_Image, Secret_Key):
#Step 1: Load the encrypted image
Load_image= Load_image(Encrypted_Image)
#Step 2: Generate key-based parameters using the Secret Key
key_parameters = Generate_Parameters_From_Key (Secret_Key)
#Step 3: Use Neural Network To reverse the transformation.
Neural_Net= Initialize_Neural_Network (Parameters= Key_Parameters)
Decrypted_Image=Neural_Net.Reverse_Transform (Loaded_Image)
#Step 4: store the result
Save_Image (Decrypted_Image)
#Step 5: return Decrypted_Image
Return Decrypted_Image

V. CONCLUSION

The study demonstrates the productiveness of mathematical Cognitive network designs for picture encryption solve the security issues with conventional cryptographic techniques. With unique benefits including increased unpredictability, real-time adaptation, and robust feature extraction, Chaotic the field of neural networks, Artificial in cells, and Convolutional Neural Networks greatly increase the strength and resilience of encryption against attacks. Higher security for digital images is ensured by the development of complicated key spaces and minimal pixel correlation made possible by these models' intrinsic nonlinearity and sensitivity to initial conditions. Neural network-based encryption techniques offer a flexible and scalable answer to the growing need to protect sensitive data in fields like online media, military communications, and medical imaging. Future developments should concentrate on combining hybrid models for better performance, minimizing distortion while preserving noise resistance, and optimizing computational efficiency.

REFERENCES

[1]. Y. Alghamdi, and A. Munir, (2024). Image encryption algorithms: A survey of design and evaluation metrics.Journal of Cybersecurity and Privacy, 4(1), 126-152, https://doi.org/10.3390/jcp4010007.
[2]. M. Sun, J. Yuan, X.Li, D.Liu, and X.Wei,(2024, July). A Novel Color Image Encryption based on Chaos and DNA Mutation. In 2024 9th International Conference on Signal and Image Processing (ICSIP), (pp. 717-725). IEEE, DOI: 10.1109/ICSIP61881.2024.10671465.
[3]. Taye, M. M. (2023). Theoretical understanding of convolutional neural network: Concepts, architectures, applications, future directions. Computation, 11(3): 52.
[4]. Feng, F.; Hu, J.; Guo, Z.; Gan, J.-A.; Chen, P.-F.; Chen, G.; Min, C.; Yuan, X.; Somekh, M. Deep Learning-Enabled Orbital Angular Momentum-Based Information Encryption Transmission. ACS Photon. 2022, 9, 820–829.
[5]. Wang, X.; Wei, H. Cryptanalysis of compressive interference-based optical encryption using a U-net deep learning network. Opt. Commun. 2022, 507, 127641.
[6]. U.Zia, M.Mc Cartney, B.Scotney, J.Martinez, M. AbuTair, J.Memon, and A.Sajjad,(2022). Survey on image encryption techniques using chaotic maps in spatial, transform, and spatiotemporal domains. International Journal of Information Security, 21(4), https://doi.org/10.1007/s10207- 022-00588-5.
[7]. Lai, Q., Wan, Z., Zhang, H., et al. (2022). Design and analysis of multiscroll memristive hopfield neural network with adjustable memductance and application to image encryption[J]. IEEE Transactions on Neural Networks and

ISSN: 2582-7219 | www.ijmrset.com | Impact Factor: 8.206| ESTD Year: 2018|

International Journal of Multidisciplinary Research in Science, Engineering and Technology (IJMRSET)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

Learning Systems, 34(10): 7824-7837.
[8].Chai, X.; Tian, Y.; Gan, Z.; Lu, Y.; Wu, X.-J.; Long, G. A robust compressed sensing image encryption algorithm based on GAN and CNN. J. Mod. Opt. 2022, 69, 103–120.
[9]. Ge, Z. C., Hu, H. P. (2021). Confluence of neural networks and cryptography: A review Journal of Cryptologic Research, 8(2): 215–231.
[10]. S.T.Kamal, K.M. Hosny, T.M. Elgindy, M.M. Darwish, and M.M. Fouda,(2021). A image encryption algorithm for grey and color medical images. Ieee Access, 9, 37855-37865, DOI 10.1109/ACCESS.2021.3063237.
[11]. Li, Z., Liu, F., Yang, W., et al. (2021). A survey of convolutional neural networks: analysis, applications, and prospects. IEEE transactions on neural networks and learning systems, 33(12): 6999-7019.
[12]. Park, S. W., Ko, J. S., Huh, J. H., et al. (2021). Review on generative adversarial networks: focusing on computer vision and its applications. Electronics, 10(10): 1216.
[13]. Gui, J., Sun, Z., Wen, Y., et al. (2021). A review on generative adversarial networks: Algorithms, theory, and applications[J]. IEEE transactions on knowledge and data engineering, 35(4): 3313-3332.
[14]. Jin, M.; Wang, W.; Wang, X. Optical color image cryptosystem based on interference principle and deep learning. Optik 2021, 251, 168474.
[15]. Song, W.; Liao, X.; Weng, D.; Zheng, Y.; Liu, Y.; Wang, Y. Cryptanalysis of phase information based on a double random-phase encryption method. Opt. Commun. 2021, 497,127172.
[16]. Wang, X.; Wang, W.; Wei, H.; Xu, B.; Dai, C. Holographic and speckle encryption
using deep learning. Opt. Lett. 2021, 46, 5794–5797.
[17]. Ding, Y.; Tan, F.; Qin, Z.; Cao, M.; Choo, K.-K.R.; Qin, Z. DeepKeyGen: A Deep Learning-Based Stream Cipher Generator for Medical Image Encryption and Decryption. IEEE Trans. Neural Networks Learn. Syst. 2021, 33, 4915–4929.
[18]. Wu, C.; Chang, J.; Xu, X.; Quan, C.; Zhang, X.; Zhang, Y. Cryptoanalysis of the modified diffractive-imaging-based image encryption by deep learning attack. J. Mod. Opt. 2020, 67, 1398–1409.
[19]. Zhou, L.; Xiao, Y.; Chen, W. Vulnerability to machine learning attacks of optical encryption based on diffractive imaging. Opt. Lasers Eng. 2020, 125, 105858.
[20]. Hu, Y., Yu, S., Zhang, Z. (2020). On the Security Analysis of a Hopfield Chaotic Neural Network-Based Image Encryption Algorithm. Complexity, 2020(1): 2051653.
[21]. Chen, J.; Li, X.-W.; Wang, Q.-H. Deep Learning for Improving the Robustness of Image Encryption. IEEE Access 2019, 7, 181083–181091.
[22]. Norouzi, B., Mirzakuchaki, S. (2017). An image encryption algorithm based on DNA sequence operations and cellular neural network[J]. Multimedia Tools and Applications, 76:13681-13701.
[23]. P.R. Sankpal, and P.A. Vijaya,(2014, January). Image encryption using chaotic maps: a survey. In 2014 fifth international conference on signal and image processing, (pp. 102-107). IEEE, DOI:10.1109/ICSIP.2014.80.
[24]. Peng, J., Zhang, D., Liao, X. (2009). A digital image encryption algorithm based on hyper chaotic cellular neural network. Fundamenta Informaticae, 90(3): 269-282.
[25]. Van Vreeswijk, C., Sompolinsky, H. (1996). Chaos in neuronal networks with balanced excitatory and inhibitory activity. Science, 274(5293): 1724-1726.

INTERNATIONAL STANDARD SERIAL NUMBER INDIA

INTERNATIONAL JOURNAL OF MULTIDISCIPLINARY RESEARCH

IN SCIENCE, ENGINEERING AND TECHNOLOGY

| Mobile No: +91-6381907438 | Whatsapp: +91-6381907438 | ijmrset@gmail.com |

www.ijmrset.com