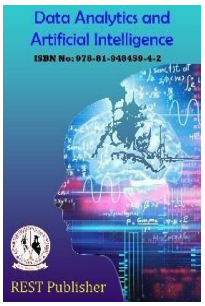
Data Analytics and Artificial Intelligence

Vol: 4(2), 2024

REST Publisher; ISBN: 978-81-948459-4-2

Website: http://restpublisher.com/book-series/daai/

DOI: https://doi.org/10.46632/daai/4/2/1



Enhancing Privacy in Social Media Image Sharing Using Advanced Encryption Technique

[*]Subham Kumar, Prasanth S, Sai Priya K, S. Durga Devi

Vel Tech High Tech Engineering College, Avadi, Chennai, Tamil Nadu, India.

[*]Corresponding Author Email: ***subhamkumar_cse21@velhightech.com***

Abstract: *As social media usage grows, protecting user privacy, especially in image sharing, is increasingly important. This paper explores enhancing privacy in social media image sharing using advanced encryption techniques based on chaotic neural networks. Chaotic neural networks, known for their complex and unpredictable behavior, offer strong encryption by transforming images into secure, unreadable formats. We discuss how these networks can effectively encrypt images during upload, store them securely, and ensure only authorized users can decrypt and view the images. This approach also includes using steganography to hide encrypted images within other files for added security. While chaotic neural networks provide robust encryption, they also introduce challenges like higher computational requirements and potential impacts on user experience. Optimizing these networks can mitigate such issues. Ensuring compliance with data protection laws like GDPR is crucial in this context. Future work may explore integrating quantumresistant encryption and AI-driven security enhancements. By leveraging chaotic neural networks, social media platforms can significantly improve the privacy and security of shared images, providing users with greater confidence in their privacy.*

Keywords: *Neural Networks, Image Encryption, Image Security, Driven Encryption, Cybersecurity, Dynamic Encryption, Financial Data Protection, User Authorization, Access Control.*

1. INTRODUCTION

In the digital age, social media platforms have become integral to daily communication, enabling users to share personal images and experiences with a broad audience. However, this convenience comes with significant privacy risks, as shared images can be vulnerable to unauthorized access, misuse, and data breaches. Protecting user privacy in social media image sharing is thus a critical concern. Traditional encryption methods, while effective, often face limitations in balancing security, performance, and user experience. Advanced encryption techniques, particularly those involving chaotic neural networks, offer a promising solution. Chaotic neural networks are known for their complex, unpredictable behavior, making them highly suitable for creating robust encryption schemes. These networks can transform images into secure, unreadable formats that are exceptionally difficult for unauthorized users to decipher. This paper explores the use of chaotic neural networks to enhance privacy in social media image sharing. By integrating these networks into the encryption process, social media platforms can ensure that images are encrypted upon upload, stored securely, and only accessible to authorized users. Additionally, the use of steganography can further protect encrypted images by embedding them within other files, adding an extra layer of security.

The adoption of chaotic neural networks for image encryption also aligns with regulatory requirements, such as the General Data Protection Regulation (GDPR), which mandates stringent data protection measures. Despite potential challenges, including increased computational demands and maintaining a seamless user experience, the benefits of this approach are substantial. This paper aims to provide a comprehensive overview of how chaotic neural networks

can be leveraged to enhance privacy in social media image sharing. We will discuss the technical aspects of implementing these networks. By addressing these issues, social media platforms can significantly improve the privacy and security of usershared images, fostering a safer digital environment.

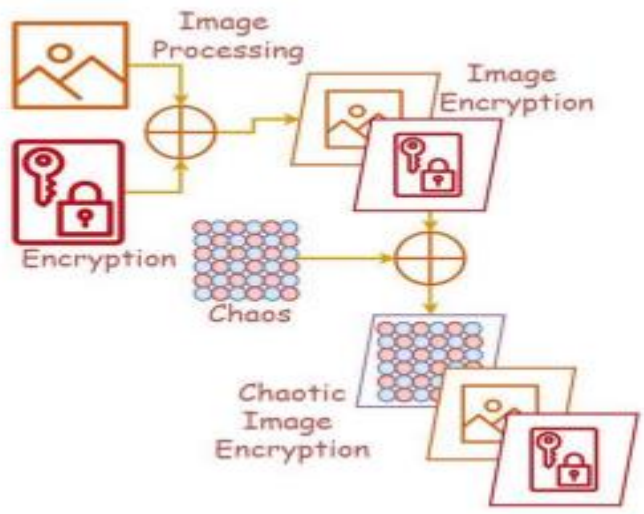


FIGURE 1. Image Encryption

2. LITERATURE REVIEW

[1] The literature survey by Xingyuan Wang, Shengnan Chen, and Yingqian Zhang explores an innovative image encryption approach that integrates a chaotic system with dynamic mixing of pixel values, pixel bits, and binary bits encryption algorithms. The process begins by converting the original plain text image into an initial key using the SHA-512 algorithm. This key is then used in the Delayed Feedback Dynamic Mixed Linear-Nonlinear Coupled Mapping Lattices (DFDMLNCML) to generate a chaotic matrix for encryption. The encryption involves manipulating mixed pixel values, pixel bits, and binary bits, and employs scrambling and diffusion techniques to enhance security. Experimental results show an average NPCR of 99.6075 and an average UACI of 33.4795, indicating the system's efficacy. Security analyses confirm its robustness against common attacks like plaintext selection, cropping, and noise attacks. [2] In this paper by Yuqin Luo, Jin Yu, Wenrui Lai, and Lingfeng Liu, a novel image encryption algorithm leveraging double chaotic systems is introduced. The approach addresses limitations and vulnerabilities in single chaotic maps by combining a two-dimensional Baker chaotic map and a logistic chaotic map. This dual system enhances control and randomness, making the logistic sequence non-stationary for improved unpredictability. The algorithm involves shuffling and substituting processes to enhance security through added complexity and unpredictability. Statistical tests and security analyses demonstrate the algorithm's robustness and competitiveness with other image encryption methods, confirming its efficacy in protecting visual data from potential threats. [3] The survey by Shima Ramesh Maniyath and Thanikaiselvan V covers image encryption and security trends, including cryptography's growth with AES and RC techniques. It notes persistent challenges in existing methods and highlights neural networks as an optimization avenue, despite their complexity and limitations. The integration of chaotic maps like logistic and Baker maps with traditional encryption is a rising trend for enhanced security. The survey underscores deep learning's role in refining encryption, merging with chaotic maps to bolster security while maintaining image quality. Overall, it offers a comprehensive view of current research and sets directions for future exploration in image security. [4] This study by Prashant Verma and Khushboo Badli introduces a robust and secure image encryption scheme incorporating a chaotic logarithmic map and key generation using a deep convolutional neural network (CNN). The CNN model generates a sensitive key, providing initial values and control parameters for the chaotic log-map, resulting in a diverse chaotic sequence for encryption. The encryption process involves four operations: permutation, DNA encoding, diffusion, and bit reversion, which together scramble and manipulate image pixels. The scheme is rigorously evaluated through various cryptoanalyses, including key space analysis, key sensitivity, information

entropy, histogram analysis, correlation analysis, differential attack assessment, noise attack examination, and cropping attack evaluation. Both visual and numerical results are compared with state-of-the-art encryption methods, demonstrating superior performance. The study confirms the proposed scheme's effectiveness, robustness, and reliability in safeguarding images against various cryptographic analyses, positioning it as a credible solution for secure image encryption. [5] This paper by Shuying Wang, Ling Hong, and Jun Jiang introduces an image encryption scheme where pixel values are bit-level shuffled using sequences from a complex network and pixel positions are scrambled using chaotic sequences from a time-delayed neural network. This dual-layer approach combines a highdimensional multistable hyper-chaotic system and a time-delayed neural network, significantly enlarging the key space. The scheme includes selecting different nodes for generating encryption and decryption sequences and determining the necessary node count for accurate synchronization. The algorithm shows superior security, enhanced key sensitivity, and resilience against attacks, proving effective in securing image data with increased complexity and robustness. [6] This paper by Liping Chen, Yin Hao, Tingwen Huang, Liguo Yuan, Song Zheng, and Lisheng Yin introduces a three-dimensional fractional-order (FO) discrete Hopfield neural network (FODHNN) for image encryption. The FODHNN exhibits rich nonlinear dynamics, verified through phase portraits, bifurcation diagrams, and Lyapunov exponents. A control scheme based on the stability theorem of FO discrete linear systems is designed to achieve synchronization within the FODHNN. The chaotic dynamics of the FODHNN are applied to develop a novel image encryption system. Security analyses, including key space analysis, key sensitivity, information entropy, and resistance to differential, noisy, and cropping attacks, confirm the system's robustness and efficacy. This research contributes significantly to cryptographic methodologies in image encryption. [7] This paper by Esteban Tlelo-Cuautle, Jonathan Daniel Díaz-Muñoz, Astrid Maritza González-Zapata, Rui Li, Walter Daniel León-Salas, Francisco V. Fernández, Omar Guillén-Fernández, and Israel CruzVega explores image encryption using chaotic systems with Hopfield and Hindmarsh–Rose neurons. Suitable coefficient values for these neurons are identified using bifurcation diagrams to achieve high positive Lyapunov exponent and Kaplan–Yorke dimension values. The randomness of generated sequences is assessed using NIST tests. Both neurons are implemented on field-programmable gate arrays (FPGAs) to develop an encryption system for RGB images. Tests including correlation, histogram, variance, entropy, and Number of Pixel Change Rate (NPCR) validate the system's success. The study demonstrates the practicality and efficacy of using chaotic neural networks in cryptographic applications, reinforcing their potential through comprehensive evaluations. [8] This paper presents a double image encryption algorithm using Convolutional Neural Network (CNN) and dynamic adaptive diffusion. It employs a chaotic map to enhance the encryption key's security and uses a chaotic sequence in the CNN to control image scrambling. The algorithm includes a dual-channel approach for secure transmission and a novel image fusion method based on information content in the images, improving encryption efficiency and resistance to attacks. [9] This project introduces the Fractal Sorting Matrix (FSM) concept for enhancing encryption algorithm security in chaotic image encryption. The FSM, characterized by fractal properties, provides an irregular and self-similar foundation. The paper outlines an iterative FSM calculation method and proposes global pixel diffusion using two chaotic sequences for high security and efficiency. Experimental comparisons demonstrate the proposed algorithm's advantages, including faster processing, higher pass rates in entropy tests, closer data proximity to theoretical values with reduced fluctuation, and resilience against cropping and noise attacks, positioning it as a promising advancement in chaotic image encryption. [10] This paper by Luoyin Feng and Xin Chen addresses the security risks in image recognition technologies by proposing a method using a high-dimensional chaos Henon Map and a one-dimensional chaos Logistic Map to generate encryption keys for face image encryption. The approach enhances key complexity and capacity, strengthening security. Additionally, a BP neural network is used for face image recognition. The algorithm's robustness is verified against conventional, geometric, and occlusion attacks, ensuring its effectiveness and reliability against various threats.

3. METHODOLOGY

In developing an image encryption and decryption system using chaotic neural networks for enhanced image sharing with MATLAB, we start by clearly defining the problem and identifying the specific requirements for image sharing. Then, we conduct a thorough review of existing techniques and best practices through literature analysis. Representative sample images are carefully chosen to ensure the effectiveness of our development process. We proceed to design and implement a chaotic neural network in MATLAB, incorporating chaotic elements and training it on a dataset containing chaotic sequences and relevant features for image sharing. Next, we develop an encryption algorithm utilizing the chaotic neural network and implement it in MATLAB. A corresponding decryption algorithm is also designed to reverse the encryption process. Throughout this process, we ensure seamless integration of the system with images, addressing any security concerns that may arise. Performance evaluation is conducted using

metrics like speed, security robustness, and resistance to attacks. Based on the evaluation results, optimization and finetuning of the system are performed. Comprehensive documentation of the entire methodology, including algorithms, parameters, and results, is maintained. Continuous improvement is emphasized, with regular consultations with security experts to ensure compliance with evolving security standards in image sharing.

The steps followed for achieving the image encryption by using the chaotic neural networks are:

1. Collection of Images: The data that have to be transferred securely have to be collected at earlier stage. Later that is to be classified into the security concerns and priorities.

2. Segmentation: As the collecting part is done, further a particular image is selected from the entire image which have to be encrypted and protected. The classification of the images is always as important as the encryption and decryption process for the image security.

3. Image Selection: Further select the specific image and encrypt the data as per the particular requirement.

4. Key generation: The secret key is generated using key generation technique. That secret key should be shared between the sender and receiver for the security concerns. And sent to the other end to decrypt that specific data.

5. Image Decryption: And the final stage of this is to Decrypt the data that had received by the receiver on another end. That will be decrypted by using that secretive key given by the sender. Thus, the data can be read by only by the people that sender allows by giving the secretive key. Hence by using these techniques we can protect the sensitive images.

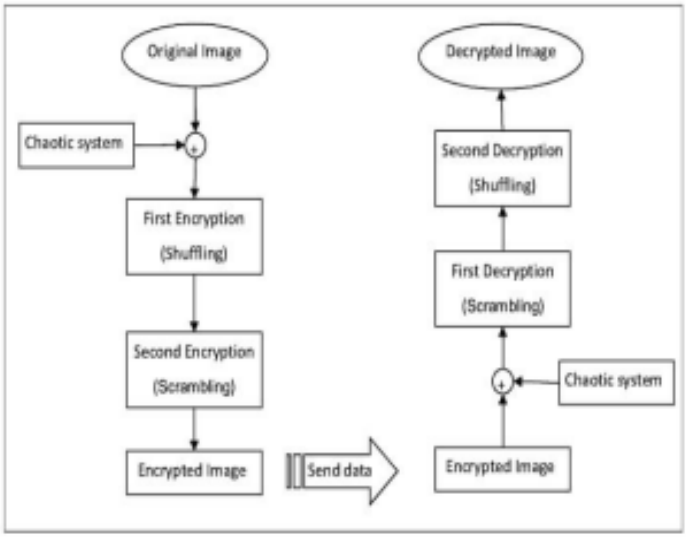


FIGURE 2. Block Diagram

4. MODEL ANALYSIS AND RESULTS

Dataset and Experimental Setup: The experimentation was conducted using MATLAB on a dedicated system. MATLAB leveraged various Toolboxes, including image pre-processors, Deep Learning Toolbox, and Statistical Machine Learning Toolbox, to facilitate image encryption and decryption processes.

FIGURE 3. Input Module

FIGURE 4. Key Generation

FIGURE 4. Encryption Process

5. RESULTS AND DISCUSSION

The developed system exhibits proficiency in safeguarding sensitive images, such as bank transactions, effectively shielding it from security breaches and attacks. Consequently, the outcome of the process yields encrypted images, necessitating decryption using a pregenerated secret key for access and utilization.

FIGURE 4. Decryption Process

This structured approach, leveraging MATLAB's diverse Toolboxes, demonstrates the system's capability to enhance data security, particularly in sensitive contexts like banking transactions. By employing advanced encryption techniques and leveraging MATLAB's extensive capabilities, the system ensures robust protection for critical data, offering heightened security and peace of mind for users.

6. ACKNOWLEDGEMENT

We are immensely grateful to the Department of Computer Science and Engineering (CSE) for granting us the opportunity to undertake our project, "Enhancing Privacy in Social Media Image Sharing Using Advanced Encryption Techniques." Special thanks to Dr. S. Durga Devi for her invaluable coordination and guidance throughout. With the department's support, we aim to explore innovative encryption techniques to safeguard privacy in social media image sharing, contributing to the advancement of digital security and knowledge in the field of computer science.

7. CONCLUSION

The integration of a chaotic algorithm for image encryption within the context of social media image sharing presents a promising approach for bolstering security and safeguarding users' privacy. Through this mini project, we have successfully demonstrated the viability of employing chaotic systems to encrypt images, thereby mitigating the risks associated with unauthorized access and potential breaches of sensitive information. While our implementation showcases notable advancements in image security, certain limitations such as computational overhead and algorithm robustness warrant further investigation. Future iterations could focus on optimizing the algorithm for real-time performance and enhancing its resilience against sophisticated attacks. Overall, this endeavor underscores the significance of leveraging innovative encryption techniques to fortify social media platforms against malicious activities, ultimately fostering a safer digital ecosystem for all users. In conclusion, our mini project illustrates the efficacy of integrating a chaotic algorithm for image encryption in social media image sharing. While successful in enhancing security and protecting user privacy, further optimization and robustness improvements are necessary. Nevertheless, this endeavor highlights the importance of innovative encryption methods in fortifying social media platforms against malicious activities, promoting a safer digital environment for all users.

REFERENCES

[1]. Xingyuan Wang, Shengnan Chen, Yingqian Zhang,A chaotic image encryption algorithm based on random dynamic mixing,Optics & Laser Technology,Volume 138,2021,106837,ISSN00303992.
[2]. Luo, Y., Yu, J., Lai, W. et al. A novel chaotic image encryption algorithm based on Improved baker map and logistic map. Multimed Tools Appl 78, 22023–22043 (2019).
[3]. Shima Ramesh Maniyath , Thanikaiselvan V , An Efficient Image encryption using Deep Neural Network and Chaotic Map, Microprocessors and Microsystems (2020).
[4]. Erkan, U., Toktas, A., Enginoğlu, S. et al. An image encryption scheme based on chaotic logarithmic map and key generation using deep CNN. Multimed Tools Appl 81, 7365–7391 (2022).

[5]. Shuying Wang, Ling Hong, Jun Jiang,An image encryption scheme using a chaotic neural network and a network with multistable hyperchaos,Optik,Volume 268,2022,169758,ISSN 0030-4026.
[6]. L Chen, Y. Hao, T. Huang et al., Chaos in fractionalorder discrete neural networks with application to image encryption. Neural Networks (2020).
[7]. Tlelo-Cuautle E, Díaz-Muñoz JD, González-Zapata AM, Li R, León-Salas WD, Fernández FV, GuillénFernández O, Cruz-Vega I. Chaotic Image Encryption Using Hopfield and Hindmarsh–Rose Neurons Implemented on FPGA. Sensors. 2020; 20(5):1326.
[8]. Zhenlong Man, Jinqing Li, Xiaoqiang Di, Yaohui Sheng, Zefei Liu,Double image encryption algorithm based on neural network and chaos,Chaos, Solitons & Fractals,Volume 152,2021,111318,ISSN 0960-0779.
[9]. Yongjin Xian, Xingyuan Wang,Fractal sorting matrix and its application on chaotic image encryption,Information Sciences,Volume 547,2021,Pages 1154-1169,ISSN 0020-0255.
[10]. Luoyin Feng, Xin Chen, "Image Recognition and Encryption Algorithm Based on Artificial Neural Network and Multidimensional Chaotic Sequence", Computational Intelligence and Neuroscience, vol. 2022, Article ID 9576184, 9 pages, 2022.
[11]. Zhang, B.; Liu, L.Chaos-Based Image Encryption:Review, Application, and Challenges. Mathematics 2023, 11, 2585.
[12]. K.M. Hosny, S.T. Kamal, M.M. Darwish, A color image encryption technique using block scrambling and chaos, Multimed. Tools Appl. (2021)
[13]. D.S. Malik, T. Shah, Color multiple image encryption scheme based on 3D-chaotic maps, Math. Comput. Simula 178 (2020) 646–666.
[14]. K.M. Hosny, S.T. Kamal, M.M. Darwish, G.A. Papakostas, New image encryption algorithm using hyperchaotic system and Fibonacci q-matrix, Electronics 10 (9) (2021) 1066.
[15]. Y.Q. Zhang, H.F. Huang, X.Y. Wang, H.X. Huang, A secure image encryption scheme based on genetic mutation and MLNCML chaotic system, Multimed. Tools Appl. 80 (2021) 19291–19305.
[16]. X.Y. Wang, M.C. Zhao, An image encryption algorithm based on hyperchaotic system and DNA coding, Opt. Laser Technol. 143 (14) (2021), 107316.