Fuzzy Systems and Soft Computing
ISSN : 1819-4362

AN INVESTIGATION ON TECHNIQUES OF VARIOUS IMAGE ENCRYPTION

Mr. S. Sundaramoorthy Asst. Professor Department of Computer Science, Bharathidasan College of Arts and Science, Erode, India
Ms. M. Premavathi Asst.Professor Department of Computer Science, Bharathidasan College of Arts and Science, Erode, India
Dr. P. SureshBabu Associate Professor Department of Computer Science, Bharathidasan College of Arts and Science, Erode, India

Abstract
The advancement of modern internet technologies has led to the widespread dissemination of information across networks, particularly images that may contain sensitive data. As a result, there is an urgent need to strengthen security measures for these images. Methods used to protect information during transmission fall into two categories: encryption and concealment techniques. Encryption techniques alter the content of sensitive data, making it indecipherable to even skilled hackers. Various encryption methods enhance security by making it challenging for intruders to predict or bypass protections. This study explores the challenges faced by researchers in this field and examines the latest proposed technologies.

Keywords:
Security, Image Encryption, Challenges, Assessment Parameters, CNN

Introduction

The need for information security methods is growing due to the heightened amount of data transmission over the Internet. The procedure for incorporating confidential data intoa medium is categorized into two distinct types. The first type is the spatial domain, where the embedding operation is executed directly on the pixels. This method is straightforward and rapid; however, it is also susceptible to detection. Examples of this approach include Least Significant Bits (LSB) and Pixel Value Differencing (PVD). Secondly, frequency domains refer to the process by which the embedding operation transforms pixels into frequency representations, including techniques such as Discrete Wavelet Transform (DWT) and Discrete Cosine Transform (DCT). Conversely, the concept of encryption involves altering the original confidential information into an unintelligible format for unauthorized individuals, utilizing a key to ensure a high level of security [1]. Various encryption algorithms exist, including the Advanced Encryption Standard (AES) and the Data Encryption Standard (DES). Nevertheless, these algorithms are not appropriate for image encryption due to the high levels of redundancy and correlation present in images. Consequently, most image encryption techniques employ chaotic systems. Pseudo Random Number Generators (PRNG) that exhibit chaotic behavior are employed in image encryption to enhance the processes of confusion and diffusion. The following sections of the paper are organized as follows. Section 2 includes a review of the literature. Section 3 addresses the evaluation parameters. The conclusion of the paper is found in Section 4.

1. Literature Survey of Image Encryption

There are a variety of encryption image methods, such as encryption based on chaotic maps, Deoxyribonucleic Acid (DNA), Neural Networks, and the Substitution box. This work discusses the latest work of past 5 years for image encryption.

1.1 Chaotic Maps with Image Encryption

Chaos theory, classified as a nonlinear system, is divided into two primary categories: discrete and continuous chaos. Discrete chaotic systems are characterized by their dynamic nature, operating at specific time intervals and generated using iterative equations. In contrast, systems governed by differential equations are referred to as continuous-time chaotic systems. Discrete chaos is relatively simple in structure and easy to implement while still providing a level of randomness beneficial for security applications. On the other hand, continuous chaos has a more complex structure but offers stronger security.Chaotic systems are further categorized based on the variables in the equation,

distinguishing between one-dimensional and multi-dimensional chaos. The one-dimensional approach offers limited randomness but is highly efficient in terms of execution speed, whereas the multi-dimensional approach provides a broader range of chaos at the cost of increased processing time. Chaotic maps are defined by two key parameters: the initial condition and the control parameters. The initial seed, a confidential value known only to the sender and receiver, plays a crucial role in generating the encryption key. Control parameters determine the system's behavior and initiate the bifurcation process, with greater bifurcation leading to an expanded key space and enhanced security. Various techniques, including randomness tests and Lyapunov stability analysis, are used to evaluate the performance of chaotic encryption methods.

Traditional encryption techniques are not well-suited for image data due to high redundancy and correlation coefficients. Consequently, most image encryption research relies on chaotic maps, which improve confusion and diffusion. In the confusion phase, chaotic maps rearrange bits or pixels to strengthen security against attacks, while the diffusion phase alters pixel values to break their correlation with the original image. Several studies have proposed image encryption methods using chaotic maps. In 2019, Wang et al. introduced a two-round encryption scheme that segments images into bits and redistributes them randomly. That same year, Khan and Ahmad developed an encryption method that divides an image into blocks and calculates correlation coefficients for each block.

The segment with the highest correlation is combined with random numbers from a skew tent map using a pixel-wise XOR operation. The entire image is then reorganized using two random sequences derived from a TD-ERCS chaotic map.Additionally, in 2019, Gan et al. presented an algorithm that decomposes color images into 24-bit planes through RGB splitting and bit-plane decomposition. The 3D Chen chaotic system generates permutation position sequences, leading to scrambled image components. In the same year, Arab et al. proposed an encryption method that integrates chaotic sequences with a modified AES algorithm. The encryption key is derived from the Arnold chaos sequence, and the image is encrypted using a modified AES process, where the chaotic system generates the round keys.

1.2 ***S-Box Image Encryption***

The S-box (Substitution Box) is a fundamental nonlinear component used in the substitution-permutation process of encryption. It converts a set of input bits (x) into a corresponding set of output bits (y), ensuring that the output values differ from the input. S-boxes function as y-bit lookup tables and are classified into three types.The first type is the straight S-box, where the input and output sizes remain identical. A well-known example is the AES S-box, which represents the standard S-box configuration. The second type is the compressed S-box, where the input size exceeds the output size, as seen in the Data Encryption Standard (DES), which maps 6-bit inputs to 4-bit outputs per block. Lastly, the expanded S-box increases the number of output bits relative to the input.

Recent research has combined S-boxes with chaotic maps to improve security by using a pseudorandom number generator (PRNG) to distribute bits within the S-box through a sorting mechanism. In 2019, Khan et al. introduced an encryption framework that generates S-boxes or Boolean functions for block ciphers using Gaussian distribution and linear fractional transformation. The following year, Liu Lidong et al. proposed a unique encryption method structured in three phases: combining, scrambling, and diffusion. The combining phase employs image compression to condense three original images, which are then merged using a stochastic matrix generated by a two-dimensional chaotic system. The scrambling phase introduces an innovative coded lock scrambling method to enhance processing efficiency. Finally, the diffusion phase applies a nonlinear component, the S-box, whose pseudo-code is provided in the study.In 2020, Qing Lu et al. developed a highly secure image encryption technique incorporating a chaotic S-box. Their approach utilizes a discrete compound chaotic system known as the Logistic-Sine system (LSS), which offers a broad chaotic range and improved security characteristics

1.3 ***Image Encryption Based on DNA***

DNA-based encryption applies DNA encoding techniques by transforming an image’s binary pixel values into corresponding DNA sequences. This approach leverages DNA coding principles to convert binary data into synthetic DNA sequences.DNA is composed of four nucleotides—adenine (A), guanine (G), cytosine (C), and thymine (T). The synthesis and sequencing of DNA require specialized

laboratory equipment. According to encoding rules, a pixel with a decimal gray value of 180 can be represented as the quaternary number "3201" (or binary "11100001"). This value can be encoded into eight different DNA sequences: "TGAC," "TCAG," "AGTC," "ACTG," "GTCA," "GACT," "CTGA," and "CAGT.

Table1. DNA rules.

Binary	1	2	3	4	5	6	7	8
00	A	A	T	T	C	C	G	G
01	C	G	C	G	A	T	A	T
10	G	C	G	C	T	A	T	A
11	T	T	A	A	G	G	C	C

In 2020, Zefreh [15] introduced an innovative image encryption technique that combines hash functions, chaotic systems, and DNA computing, utilizing a 5D chaotic framework. The DNA permutation aspect involves the random rearrangement of the components' positions within the DNA image, achieved through a mapping process based on the chaotic logistic map.

In 2021, Iqbal et al. [16] formulated a new image encryption method that integrates chaotic systems, DNA computing, and the Castle chess piece. When the original image is inputted, its pixels are relocated to a scrambled image at randomly chosen pixel positions. This scrambling process is executed using the Image Scrambler utilizing the Castle (ISUC) algorithm. In 2022, Lone et al. [17] presented a novel technique for image encryption that employs DNA and the 3D Arnold chaos system.

Image Encryption Based on Neural Networks

Neural networks can be utilized in image encryption methods to enhance both the security and efficiency of the algorithms. These networks have the capability to rearrange and/or compress the original images. Additionally, neural networks that demonstrate chaotic behavior can generate. These techniques are inspired by the convolution neural processes of the human brain through conditional training [18].

The domain of image encryption leveraging neural networks has garnered significant interest from researchers, as these networks A variety of neural techniques, including fuzzy logic, heuristic methods, genetic algorithms, particle swarm optimization, and convolutional neural networks, are employed in image encryption. In 2021, Man et al. [19] introduced a dual image encryption algorithm that integrates convolutional neural networks (CNN) with dynamic adaptive diffusion.

A chaotic map is initially employed to manage the starting values of the 5D conservative chaotic system, thereby enhancing the security of the key. Subsequently, to effectively counter known plaintext attacks and chosen-plaintext attacks, the proposed method utilizes a chaotic sequence as the convolution kernel within a convolutional neural network. This generates a chaotic pointer that is associated with the plaintext, which governs the scrambling process of two images.

In 2023, Fenget al. [20] introduced a method that integrates chaotic image encryption with a convolutional neural network (CNN) to bolster both security and performance. This approach leverages the randomness and nonlinear mapping properties of chaotic sequences, in conjunction with the advanced feature extraction capabilities of a CNN model, to produce robust image encryption. Initially, the fundamental principles of chaotic image encryption and convolution neural networks are outlined.

2. Evaluation Parameters

Various criteria are used to evaluate the performance and effectiveness of encryption and concealment processes. Table 2 presents a summary of the most essential evaluation parameters**.**

Parameters	Abbreviation	Definition	Encryption
Histogram	H(s)	This method displays the Distribution of pixel values.	Equal distribution
Entropy	$E(s)$	It quantifies the level of Uncertainty or randomness.	Must benear8 value

Correlation Coefficient	CC	Evaluating the degree of Association between pixels	Nearto-1
Mean Square Error	MSE	It measures the error ratio between the original plain image and the steganography or Encrypt image.	Increasing (near to infinite)
Peak Signal Noise Ratio	PSNR	Serves as a signal match ratio between an encrypted or steganography image and a plain image.	Decreasing (near to zero)

3. Conclusion

The methods for securing data can be categorized into two fundamental types: cryptography and steganography. Many encryption methods currently in use lack the robustness necessary to withstand attacks from hackers and intruders. To enhance unpredictability, a novel hybrid approach that combines encryption and steganography may be implemented. The proposed encryption framework is founded on hyper-chaos, characterized straightforward structure and an extensive bifurcation range, incorporating various rounds of confusion and diffusion. This study offers the following recommended summary.

References

[1]. M.KaurandV.Kumar,"Acomprehensivereviewonimageencryptiontechniques,"*Arch. Comput.MethodsEng.*,vol.27,no.1,pp.15–43,2020.DOI:10.1007/s11831-018-9298-8

[2].K.C.JithinandS.Sankar,"ColourimageencryptionalgorithmcombiningArnoldmap,DNA sequence operation, and a Mandelbrot set," J. Inf. Secur. Appl., vol. 50, no. 102428, p. 102428, 2020. DOI:10.1016/j.jisa.2019.102428

[3]. R.B.NaikandU.Singh,"Areviewonapplicationsofchaoticmapsinpseudo-random numbergeneratorsandencryption,"Ann.DataSci.,vol.11,no.1,pp.25–50,2024. DOI:10.1007/s40745-021-00364-7

[4].J. S. Muthu and P. Murali,"Review of chaos detectiontechniques performed on chaotic maps and systems in image encryption," SN Comput. Sci., vol. 2, no. 5, 2021. DOI: 10.1007/s42979-021-00778-3

[5].M. Z. Talhaoui, X. Wang, and M. A. Midoun, "A new one-dimensional cosine polynomial chaotic map and its use in image encryption," Vis. Comput., vol. 37, no. 3, pp. 541–551, 2021.DOI: 10.1007/s00371-020-01822-8

[6].X. Wang, S. Gao, L. Yu, Y. Sun, and H. Sun, "Chaotic image encryption algorithm based ont-combinationscramblingindecimalsystemanddynamicdiffusion,"IEEEAccess,vol.7, pp.103662–103677,2019.DOI: 10.1109/ACCESS.2019.2931052

[7]. K. J. Sher and J. Ahmad, "Chaos-based efficient selective image encryption," Multidimensional Systems and Signal Processing, vol. 30, pp. 943–961, 2019.DOI:10.1007/s11045-018-0589-x

[8].Z.-H. Gan, X.-L. Chai, D.-J. Han, and Y.-R. Chen, "A chaotic image encryption algorithm based on 3-D bit-plane permutation," Neural Comput. Appl., vol. 31, no. 11, pp. 7111–7130, 2019. DOI:10.1007/s00521-018-3541-y

[9].A. Alireza, M. Rostami, and B. Ghavami, "An image encryption method based on chaossystemandAESalgorithm,"TheJournalofSupercomputing,vol.75,pp.6663–6682,2019.DOI:10.1007/s11227-019-02878-7

[10].D.Lambić,"Anewdiscrete-spacechaoticmapbasedonthemultiplicationofinteger numbers and its application in S-box design," Nonlinear Dyn., vol. 100, no. 1, pp. 699–711, 2020.DOI: 10.1007/s11071-020-05503-y

[11].C. Easttom, "s-box Design," in Modern Cryptography, Cham: Springer InternationalPublishing, 2022, pp. 193–212.DOI:10.1007/978-3-031-12304-7_8

[12].K.M.Fahad,A.Ahmed,andK.Saleem,"Anovelcryptographicsubstitutionboxdesign using Gaussian

distribution," IEEE Access, vol. 7, pp. 15999–16007, 2019. DOI: 10.1109/ACCESS.2019.2893176
[13].L. Lidong, D. Jiang, X. Wang, L. Zhang, and X. Rong, "A dynamic triple-image encryption scheme based on chaos, S-box and image compressing," IEEE Access, vol. 8, pp. 210382–210399, 2020. DOI: 10.1109/ACCESS.2020.3039891
[14].Q.Lu,C.Zhu,andX.Deng,"AnefficientimageencryptionschemebasedontheLSS chaotic map and single S-box," IEEE Access, vol. 8, pp. 25664–25678, 2020. DOI: 10.1109/ACCESS.2020.2970806
[15].E. Z. Zefreh, "An image encryption scheme based on a hybrid model of DNA computing, chaotic systems, and hash functions," in Multimedia Tools and Applications 79, 2020, pp. 24993–25022.DOI: 10.1007/s11042-020-09111-1
[16].N. Iqbal et al., "On the image encryption algorithm based on the chaotic system, DNA encoding, and castle," IEEE Access, vol. 9, pp. 118253–118270, 2021. DOI: 10.1109/ACCESS.2021.3106028
[17].P. N. Lone, D. Singh, and U. H. Mir, "Image encryption using DNA coding and three-dimensionalchaoticsystems,"Multimed.ToolsAppl.,vol.81,no.4,pp.5669–5693,2022. DOI:10.1007/s11042-021-11802-2
[18].B. Han, Y. Jia, G. Huang, and L. Cai, "A medical image encryption algorithm based onHermite chaotic neural network," in 2020 IEEE 4th Information Technology, Networking, Electronic and Automation Control Conference (ITNEC), 2020. DOI: 10.1109/ITNEC48623.2020.9085079
[19].Z. Man, J. Li, X. Di, Y. Sheng, and Z. Liu, "Double image encryption algorithm based on neural network and chaos," Chaos Solitons Fractals, vol. 152, no. 111318, p. 111318, 2021.DOI: 10.1016/j.chaos.2021.111318
[20].Feng, "Image encryption algorithm combining chaotic image encryption and convolutional neural network," Electronics, vol. 12, 2023.DOI: 10.3390/electronics12163455