Communications on Applied Nonlinear Analysis
ISSN: 1074-133X
Vol 32 No. 1s (2025)

# An Extensive Analysis of Deep Learning Techniques for Improving Picture Encryption's Security & Data Embedding Capability

**Mr. Yandapalli Venkata Sree Vaishnava Reddy[1], Dr. D. Ganesh[2]**

[1]Research Scholar, Department of CSE, Mohan Babu University, (Erstwhile Sree Vidyanikethan Engineering College (Autonomous)),Tirupati, Andhra Pradesh, India. yvreddy008@gamil.com

[2]Associate Professor of CSE, Mohan Babu University, (Erstwhile Sree Vidyanikethan Engineering College(Autonomous), Tirupati, Andhra Pradesh , India. ganesh.d@vidyanikethan.edu

***Article History:***

***Received:*** *14-08-2024*

***Revised:*** *27-09-2024*

***Accepted:*** *15-10-2024*

**Abstract:**

Because data digitisation is so common, it is necessary to encrypt messages while they travel over unprotected channels. The communication is encrypted before it is sent. Encryption cannot function without both a technique and a key. It is crucial to take additional measures to safeguard the privacy and confidentiality of the receivers when transmitting sensitive images over an unsecured network such as the internet. Regardless of the fact that there is no standardisation for these algorithms Combining standard public key cryptosystems like RSA and El-gamal with chaos-based cryptosystems like Chebyshev polynomials can improve security in a manner similar to AES, DES, RSA, etc. Although AES and other classical algorithms have been standard for some time, many security experts now recommend chaos-based encryption approaches for media files due to their computational efficiency. Because existing algorithms are unsuited for real-time picture encryption due to their poor encryption speeds and the high processing needs of secure encryption methods, researchers have proposed bespoke algorithms for image encryption. One of the better techniques is chaotic encryption, which uses cypher text that is unpredictable enough to greatly decrease the likelihood of decipherment when applied to images. Consequently, research into digital picture encryption algorithms based on chaotic technology has become an important tool for modern digital image encryption. We go over all the new features and improvements in picture encryption. With an eye towards evaluating them and giving academics and practitioners the context they need to understand the methods' current position, this study aims to introduce and summarise the currently used photo encryption algorithms and metrics. This study rates the different photo encryption algorithms based on their strengths and weaknesses after examining them. Furthermore, the assessment matrices used to evaluate the performance and security of the encryption algorithms in recent studies have been validated by comparative analysis.The article also reviews these metrics in detail and provides upper and lower bounds for a set of efficiency, quality, and security evaluation criteria for image encryption algorithms.

Keywords: image encryption; chaotic system, Security and privacy, Logistic mapping, Digital image.

## 1.Introduction:

The exponential growth of the Internet and associated information technologies has had a significant influence on every facet of our business, industrial, and daily life. We rely on these improvements every day because they have made the production of large amounts of data easier and cheaper.

Concurrent with these changes, mobile technology has exploded in the last 20 years, with images surpassing all other types of data in terms of usage [1].Photos include very personal information, so it's important to take precautions to keep them safe when saving and sharing them. Academics have noticed this, and it has been referenced frequently as an illustration of picture encryption since then [2].

Even when security is at danger, encrypted photos can be sent so that only authorised recipients can read them. Among the numerous problems that cryptographic approaches must resolve are issues related to data translation, authorisation, and key distribution. With the ever-changing nature of internet-based systems, information security has become paramount. Data encryption can usually keep consumers' information safe when it's being sent over public networks. Traditional methods of image data encryption can have their limitations, though. Various issues, such as excessive correlation between image pixels, ineffective management of massive datasets, etc. When compared to text data, the difficulties of encrypting image data are distinct. To begin, in terms of practical uses, text data is substantially more compact than visual data. This makes it difficult to encrypt photographs in a reasonable length of time. Malicious actors can utilise statistical assaults to recover the actual photographs in the second case, which entails extraordinarily strong associations between neighbouring pixels in the picture data [3]. Inadequately strong encryption methods render them ineffective. Therefore, standard data encryption techniques that are often used for text data, like DES, TDES, AES, and RSA, will not work for picture data [4]. Encrypting image data obviously requires a number of different approaches. Image encryption approaches mostly employ permutation, substitution, and diffusion schemes [5]. The goal of the permutation step is to rearrange the pixels in the image in a different order without altering their values. As a result, the association between nearby pixels is drastically reduced [6]. A systematic approach to changing the statistical properties of image pixels is taken by carrying out the substitution & diffusion stage [7]. This paves the way for a systematic method of adjusting the pixel values. Methods that rely solely on permutations for encryption are inadequate since they cannot change the images' histograms [8]. It is strongly advised that an efficient encryption system employs both diffusion and permutation. To complete the permutation and propagation steps, one can use chaos-based encryption algorithms. In order to accomplish both diffusion and confusion at the same time, chaos-based techniques are commonly used in modern photo encryption. The beginning point is crucial for chaos-based approaches. Their random, rather than periodic, resultant values have also made them very useful in image encryption. In Figure 1 we can see the fundamental steps of the image encryption and decryption process.

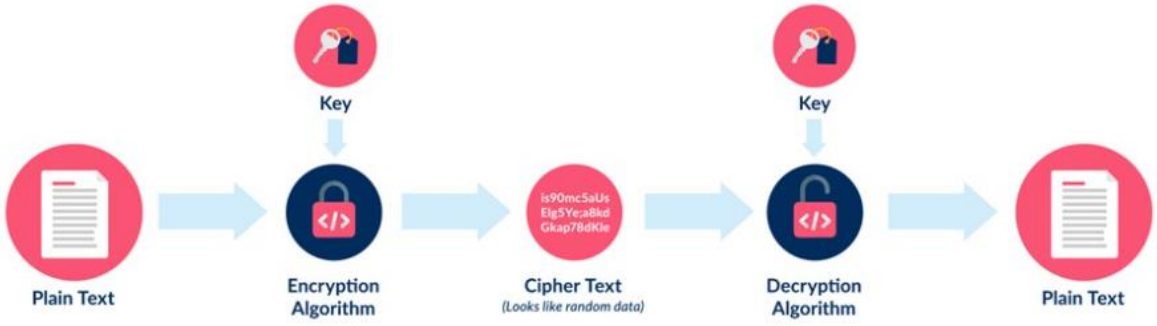


Figure 1.Basic Encryption/Decryption Procedure

Research into unpredictable behavior experienced a spike during the 1960s and 1970s, coinciding with the rapid expansion of personal computers. For the first time, nonlinear systems of any kind could be studied with the arrival of more powerful computers. Strange attractions, which cause nearby trajectories to diverge, are an essential component of these systems. The combination of these features produces what appear to be random time series, but which are, in fact, entirely deterministic? Since chaotic systems appear to be random, they can be used for encryption. Cryptography describes encryption as the process of changing data into an unrecognisable type in order to prevent unauthorised individuals from accessing sensitive information. The crucial features of image content, including high redundancy, size, capacity, and correlation among bit pixels, necessitate an encryption approach for secure image transfer [8]. The use of an encryption method allows for the transformation of a plain picture into a cypher picture, which successfully conceals the original meaningful information. Subsequently, the image can be securely transmitted over the network without compromising its decipherability. Consequently, a decryption method is used at the other end of the network to convert the encrypted picture back to its original format. Encryption also involves inserting a key into the original image so that it can be encoded. On the other hand, decryption is the process of using a way to get the original picture out of encrypted data. Figure 2 shows two common types of keys used for image encryption and decryption: symmetrical keys and asymmetric keys. The encryption and decryption processes of symmetric key cryptography share a single key. Asymmetric key cryptography, sometimes called public key cryptography, differs in that it employs a unique key for each process.

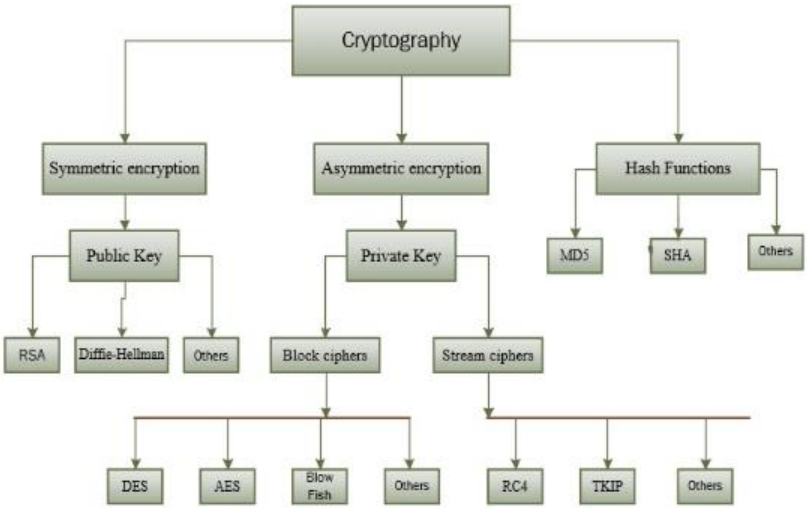


Figure 2. General Classification of image encryption algorithms

In order to create cryptographic algorithms that can encrypt and interact securely even in the presence of an attacker, scholars have recently focused on the association between cryptography with chaotic systems [9]. As a result of combining chaos theory with encryption research, chaotic cryptography was born. Cryptosystems are defined on a finite set of integers, in contrast to chaotic systems that are defined on real numbers. Here is where the two vary primarily. Due to their inability to distinguish between unique and similar images, classical cyphers like AES and DES fail miserably when it comes to photo encryption. A solution to this difficulty is provided by chaos theory–based

encryption methods, which encrypt images using randomly distributed keys and so conceal the underlying data [10]. Building a chaos-based picture cryptosystem primarily entails two stages: confusion and dispersion. Figure 3 shows the building's system schematic. The image is transformed into an unrecognizable shape during the disorientation phase, which is also called pixel permutation, by moving the pixels throughout the whole picture while keeping their values constant. The implementation of the dispersion stage follows the initial phase's lack of sufficient security, making it easily hackable. An advantageous feature of a chaotic map during the diffusion phase is the sequence it generates, which sequentially changes the value of all the pixels in the image. To achieve a suitable degree of safety, the confusion-diffusion process must be repeated iteratively.

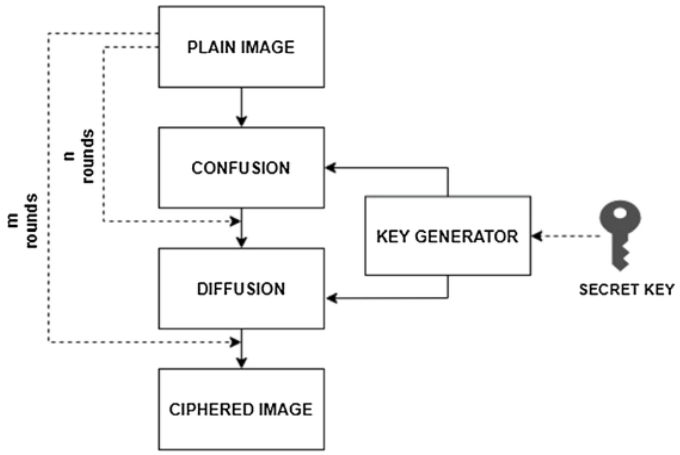


Figure 3. Chaos-based image cryptosystem architecture [11]

Chaos theory-based picture encryption algorithms are highly favoured because to its non-linearity, sensitivity to initial parameters, speed, and robustness [12]. Algorithms based on chaos can distribute and permute a plaintext picture using pseudorandom chaotic sequences from the chaotic system [8]. Picture encryption methods frequently make use of chaotic maps, such as logistic maps[13–14], Baker maps[15–16], Arnold maps[17–18], tent maps[19–20], hyper chaotic maps[21], etc. Multiple disordered system-based images A number of different encryption techniques have been proposed by industry leaders. The outline for the rest of the paper is as follows: Section 2 explores the inspiration behind the work, Section 3 analyses the literature review, Section 4 proposes the main objectives, and Section 5 concludes.

## 2. Motivation:

Recent advances in algorithmic capability have made feasible both lossless extraction and increased data embedding. Digital watermarking, content authentication, and encrypted data transmission are just a few of the many successful uses of these approaches. Despite these advancements, problems with embedding capacity, information security, and maintaining image quality persist. The increasing significance of secure data transmission and storage in the modern digital ecosystem has made reversible data hiding methods vital. Reversible data hiding is essential in multimedia and data security applications because it enables additional data to be hidden into digital media while ensuring the lossless extraction of the original material. When data must be embedded into media yet doing so permanently affects its integrity, data privacy, degradation-free recovery, and integrity of the data are

of the utmost importance. A must-have feature is reversible data concealing because existing methods of data hiding aren't always reversible.

Limitations in embedding capacity pose a significant challenge to reversible data concealment. It is crucial to enhance the host media's quality while incorporating large volumes of data. It can be difficult for current systems to achieve high embedding capacities while preserving the media's integrity & perceptual quality. Striking a good equilibrium in this trade-off is a challenging task. Another major issue is the security of reversible data concealing. Ensuring the security and dependability of the embedded data is of the utmost importance due to the vital nature of data-hiding applications. Data manipulation, unlawful extraction, or embedded data identification could be possible using current technologies. In order to ensure the privacy and security of embedded information, reliable and secure methods for reversible information concealing must be developed.

To add insult to injury, reversible data hiding systems need various forms of digital media to be compatible. Audio, video, & image files all have their own unique formats and characteristics. In order to ensure their general usability and compatibility, it is crucial to create flexible algorithms that are capable of storing and retrieving data from many forms of media. Incorporating ML and DL techniques into an adaptive strategy could solve issues with embedded capacity, data security, or preserving picture quality. Integrating the benefits of algorithms for machine learning and deep learning can enhance the efficiency and effectiveness of reversible data concealment techniques.

## 3.Literature Survey:

Image Security has numerous applications. It is required by nearly every other sector of the economy. Many other approaches are suggested in the literature, some of which use sequences and others common transformations. In the realm of image protection, two broad classes exist. Full and partial encryption are the two approaches used for images. We have performed a comprehensive literature review, as shown in figure 4.

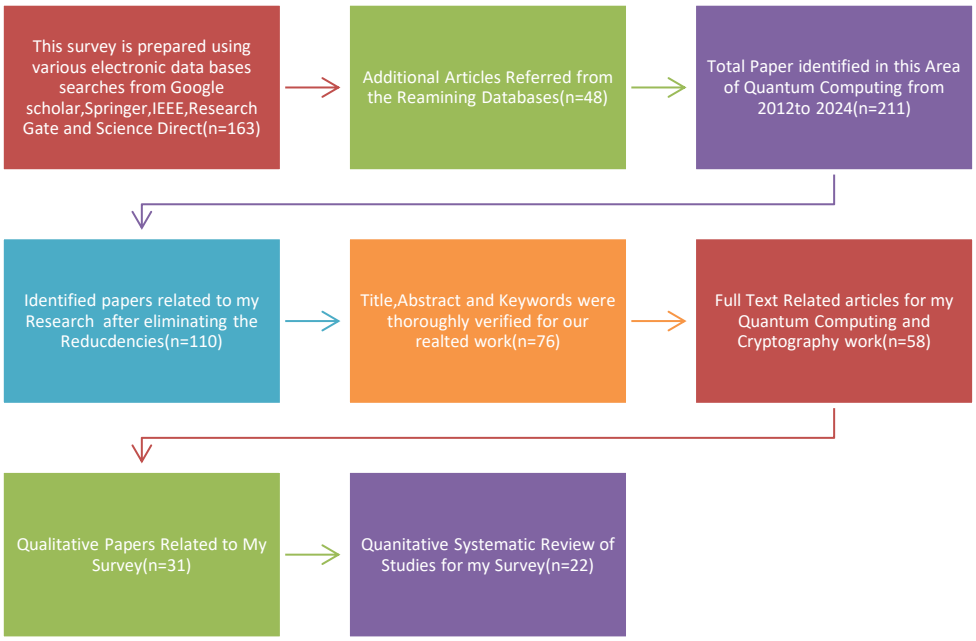


Figure 4.Literature Survey on My proposed Research

Hazem Mohammed et al. demonstrated the time-based multi-chaotic encrypting scheme [22]. An alternative method for image encryption is proposed, which makes use of a vast array of chaotic functions. Cryptographic algorithms used by the cryptosystem get increasingly intricate as a result of this. Som et al. [23] employed a chaos-theory-based pseudorandom binary generator for picture encryption. Bit planes are considered crucial because of their role in the creation of pixels. We do not encrypt minor bit planes. A faster way is to partially encrypt photos. Bit plane encryption protects sensitive information and ensures the algorithm's trustworthiness.

Raj et al. [24] proposed an encryption method that makes use of structures in long-term and short-term memory. The image has been provided to the theme memory structure in its component components. For key generation, a two-dimensional mixed lattice system with chaos has been used. To provide a more random key 1, an enhanced chaotic logistic sequence is employed. For chaos key 2, the hyper chaos system is employed. The approach is based on two rounds of photo encryption using a double key. When it comes to statistical data and picture encryption, the results of the simulations show that it is very efficient and accurate.

Tian et al. [25] proposed a method for encrypting palm print photos. Investigating DNA coding as a potential new avenue for picture encryption research seems hopeful. With a one-of-a-kind mapping of the four possible DNA base permutations to the pixel values, pixel diffusion can be achieved. The current methods for choosing the eight principles of DNA coding are largely static. A conventional scrambling diffusion encrypting framework was used in tandem with DNA coding in the five-dimensional hyperchaotic system. A chaotic mixed-map-based strategy may accommodate critical distance, confusion, and diffusion. There are a lot of chaos maps utilised. The encryption technique is impenetrable across any known attack vector.

In order to guarantee that transmitted data is correlated, Muhammad Asif et al. [26] detailed a picture encryption method that employs a nonlinear chaotic algorithm. If you believe the IEA, you should test UACI and NPCR close to the closest optima. One way to create prime numbers for the RSA method is to use the chaotic sequence obtained from the first two phases of the 3D chaotic system. Finally, the chaotic series is XORed with the pixel intensities. We use the RSA method to re-encrypt the output. The proposed approach creates asymmetric cryptography keys by means of a chaotic system, utilizing characteristics of asymmetric cryptography. In addition to producing better results, the proposed approach is easy to implement. By combining logic and sine graphs, Hannah et al. [27] proposed a 2D chaos graph. There is a hyper chaotic character to the end result. Images are encrypted using obfuscation and diffusion techniques. Use the Chaos Magic Transformation to simultaneously align horizontally and vertically. Diffusion is achieved by exchanging the pixels in each column and row with a chaotic matrix derived from a predefined hyper chaos map. To improve the algorithm's performance, two operations are required. This method is sturdy and resistant to multiple assaults, and its temporal complexity is small.

Wang et al. [28] proposed a new way to encrypt colour images that are associated with genetic modification and chaotic systems. In order to overcome the one-dimensional chaotic limitation, improve data image encryption using DNA rules, and generate fresh values for CML repetitions by increasing the Hamming distance, we use a mixed map network. It is more secure, encrypts data faster, and is resistant to attacks than competing approaches. Combining enhanced Logistic mappings

with wavelet transform, Arnold mapping, and Kent mapping, Xiao Chen et al. [29] propose a novel encryption method. We use wavelet transforms and Arnold maps to shuffle the picture pixels around randomly, and we construct the Arnold maps' control parameters with Kent maps. To create pseudorandom numbers, the modified logistic map XORs the key value with the pixel value. In 2017, Chen et al. [30] presented a directional confined predictor to identify locations where LC does not impact PE. In order to further improve RDH's efficiency, a DEPE (directionally-enclosed forecasting and expansion) system was deployed. Only pixels that had a proportionate LC to PE connection could DEPE embed data into. Wu et al. proposed an RDHEI approach in 2018 [14] that relies on Secret Sharing. The encrypted file was twice the size of the original, though. Because of its increased size relative to the original, the encrypted image necessitates more room for storage and more bandwidth for transmission. This constraint might be an issue for resource-constrained or massively-scaled applications, as well as for scenarios where data storage or network bandwidth is scarce or costly.

Using a 2D sinusoidal correction model, Natick et al. (2019) proposed an approach to picture and hyperchaotic graph encryption. The performance analysis indicates that a complicated method with a low-cost deployment is feasible. Wu et al. (2019) showed an approach that included breaking the cover photo into blocks of different sizes and then labelling them after three rounds of segmentation. Within the given block, every pixel has its Least Significant Bits (LSBs) set aside. Following that, the standard deviation and average of the block's pixels are shown here as supplementary data. The method is impacted by the picture block sizes and the predefined threshold, and the area can be improved.
Liu et al. (2020) describe an effective way to encrypt photos utilising a message transfer technique and an outside chaotic message.

The method of connecting with neighboring pixels is called a message-passing strategy. Logic diagrams in two dimensions are used to make the keys. It quickly produces highly pseudo-random numerical sequences. A 2D logic map is employed to produce the collection of edge pixel pictures, which serve as a pseudorandom pattern generator. The approach and outcomes demonstrate that the algorithm is resilient against numerous existing low-cost attacks. In 2020, Zhao et al. proposed a technique called histogram displacement [12]. A message containing solely the numbers 1, 0, and 1 is created during the encoding process by converting sensitive data into this format. When creating the displacement histogram, the next step is to select the middle segment bin. You can use these containers to insert a message with 1, 0, or 1 by arranging them horizontally. The Threshold approach is used to alter the band size, and the Chess Board Projection approach is used to generate the histogram. Because it is so predictable, attackers can simply detect the Chess Board Predictions technique and remove it or inadvertently change it using image manipulation. If a competitor has enough information, they can utilise the method's predictability to uncover secret data or delete it totally. This restriction puts the reliability and accuracy of the embedded data at risk.

Using compression sensors and a memristive chaotic system, Haiying Hu et al. (2021) presented an encryption system. This technique applies a twofold compression on the image in order to decrease storage expenses. Two layers of encryption—block encoding and the zigzag transform—protect the pixel array. Using diffuse image matrices and chaotic pseudo-random sequences, the final

cypher image is formed. Finally, the system maintains good decompression performance even with a compression ratio of 0.25, as supported by simulation and performance research results. The scheme is quite secure and resistant to several types of attacks, according to the security study. An strategy to block encryption was used by Chen et al. [11] in 2021. After halving the encrypted image, we utilised lossless compression techniques, such as Huffman coding, to reduce the bit plane and free up more space. Finally, the combined MSBs were able to recover the original cover image. Because the block was too small, the embedding capacity was limited.

In 2022, data was encrypted and compressed using picture blocks by Kim et al. [31] using Hamming coding. The quantisation process also regulated the maximum amount of embedded data. Some bits in the host media need to be changed so that more data can be encoded in RDH using Hamming codes. The overall quality or perception of the host media may be affected if these alterations generate noticeable distortions or changes to the medium. The trade-off between embedding depth and distortion becomes critical, therefore Hamming codes might not be the optimal solution for decreasing distortion. In 2022, Chen and colleagues developed RDHEI, a new way to share secrets. This method outperforms its predecessor by making use of a plethora of information hiders. Because Chen et al.'s technique maintains a fixed overall embedding volume, the embedding rate drops as the number of photo shares increases. A constant total embedding volume distributes the data over several shared images. As the quantity of photos that are shared increases, so does the rate at which each image is embedded. If there are a lot of shared photos, the method might not be able to fit all the necessary data into each one.

In 2023, Shaiju and colleagues created a novel Ensembled Learning method that utilises the Fibonacci Transform. In this case, the receiver explores all possible Fibonacci transformations in an effort to decode the blocks. The computational intensity of this approach is a major negative. Processing time and complexity might increase dramatically when doing numerous Fibonacci conversions [33].

Table 1. Gap Identification through literature review

| S. No | Technique used with its reference | Publication Details | Year of publication | Observations | Gaps |
|---|---|---|---|---|---|
| 1. | Ensembed Learning using Fibonacci Transform [33] | Panchikkil, Shaiju, et al. "An Ensemble Learning Approach for Reversible Data Hiding in Encrypted Images with Fibonacci | 2023 | The Method uses Fibonacci transforms for decryption of encrypted image blocks. | The approach is computationally intensive due to the need to perform numerous Fibonacci transformations, leading to |

| | | | | | |
|---|---|---|---|---|---|
| | | Transform" Electronics 12, no. 2: 450. | | | increased processing time and complexity. |
| 2. | employed Hamming code [31] | Appl. Sci. 2022, 12, 8225 | 2022 | Code for encrypting and compressing image blocks in order to conceal data | may not provide the best balance for reducing distortion |
| 3. | a novel secret-sharing RDHEI technique [34] | IEEE Trans. Dependable Secur. Comput. 2022, 19, 978–991. | 2022 | increases the number of information hiders from one to many. | The embedding rate decreases as the quantity of shared images grows. |
| 4. | employed block encryption Method [35] | Connection Science. Volume 33, 2021 | 2021 | After that, the encrypted picture was split into two halves, and to make more room, lossless compression methods like Huffman coding were used to shrink the bit plane. | The block, however, was too small, limiting the embedding capacity. |
| 5. | histogram Shifting [36]. | *Signal Process. Image Commun.* 2020, *81*, 1–9 | 2020 | Results of the Chess Board Prediction method's prediction errors | is vulnerable to detection and removal by attackers or unintended image manipulation |

| | | | | | |
|---|---|---|---|---|---|
| 6. | based on scalable blocks [37] | Multimed. Tools Appl. 2019, 78, 25349–25372. | 2019 | After three rounds of segmentation, the cover photo was divided into blocks of varying sizes and tagged. | The image block size and fixed threshold have an effect on the method, and the space has to be improved further. |
| 7. | Secret Sharing [38] | *Signal Process.* 2018, *1 43*, 269–281 | 2018 | RDHEI approach based on Secret Sharing | concerning the size of the encrypted image, which is more than twice the size of the original image. |
| 8. | directional enclosed predictor [30] | , *IEEE Signal Process. Lett.*, 2017, 24, (5), pp. 574–578 | 2017 | Put to use in locating instances where LC has no bearing on PE | Pixels where LC had a proportionate relationship with PE were the only ones that could have data embedded via DEPE. |
| 9. | encrypting color images pertaining to DNA sequence manipulation [28] | Bio systems, vol. 144, pp. 18-26,2016 | 2016 | combined map network, extend the Hamming distance to generate new values for CML iterations, and use DNA rules to enhance data image encryption | faster encryption speeds so that chance of missing the information |
| 10. | Novel image encryption method with | Appl. Math. Inf. Sci, vol. 9, no. 6, pp. 2991- | 2015 | Image Encryption technique that | Requires better performance and easy |

| | | | | | |
|---|---|---|---|---|---|
| | numerous chaotic functions [27] | 2995,2015 | | employs a nonlinear chaos method | implementation |

## 4.Objectives:

The suggested methodology and anticipated outcomes informed the following four research aims:

1. In Order to Acquire a Stronger Ensembled Deep Learning Model for the Prediction of MSBs

- **Objective:** Establish a cutting-edge deep learning model utilising adversarial training, mechanisms of attention, transfer learning, and other approaches to improve the precision of image Most Significant Bit (MSB) plane predictions.
- **Motivation:** Reducing prediction errors and increasing the capacity and quality of information embedding are both made possible by enhancing the precision of MSB predictions.

2. **To Implement a Reversible Data Hiding Technique Utilizing Prediction Errors:**

- **Objective:** Develop and implement a data-hiding mechanism that can be undone, preserving high image quality while supplementing the MSB prediction module's inaccurate predictions with more data.
- **Motivation:** Using prediction errors as carriers for data immersion increases the data's capacity to embed and guarantees the process's reversibility. The overall picture quality is less affected by this.

3. **To Enhance Security through Image Encryption:**

- **Objective:** Put a robust encryption mechanism into the watermarked photos to make the encoded data unreadable by anyone trying to decipher it.
- **Motivation:** Encrypting pictures securely is crucial for maintaining the privacy and integrity of embedded data, especially while transferring or storing them.

4. **To Validate the Proposed Scheme through Accurate Data Extraction and Original Data Recovery:**

- **Objective:** Make that your extraction method can decipher the watermarked image, restore it to its intended MSB plane, and retrieve the contained data without causing any damage or loss.
- **Motivation:** Precise extraction and recovery of the hidden data is crucial to prove that the proposed reversible data hiding approach is effective and reliable.

## 5.Conclusion:

This research investigation takes a close look at picture encryption methods that are utilised in numerous industries. We have meticulously examined and categorised the most recent studies released in the previous twelve years to help you understand them better. Reviewing the literature on the subject, it is evident that picture encryption is still in its early stages and has much room for

improvement in terms of processing efficiency, parameter tuning, and security. According to the results of the assessment procedures for encryption methods, the majority of publications do not use all of the standard checks to validate an algorithm's performance. Having a standardized approach to test the effectiveness of new photo encryption algorithms would be helpful. The importance of multimedia file encryption has grown in the last several decades. Along with discussing the challenges of existing chaos-based picture encryption methods, this chapter provides a thorough examination of multiple techniques that can aid in future research.

## References:

[1] Ben Slimane, N., Aouf, N., Bouallegue, K., & Machhout, M. (2018). A novel chaotic image cryptosystem based on DNA sequence operations and single neuron model. *Multimedia Tools and Applications*,*77*(23), 30993–31019.

[2] Li, C., Zhao, F., Liu, C., Lei, L., & Zhang, J. (2019). A hyperchaotic color image encryption algorithm and security analysis. Security and Communication Networks, 2019, 1–9.

[3] Abduljabbar, Z. A., Abdul jaleel, I. Q., Ma, J., Al Sibahee, M. A., Nyangaresi, V. O., Honi, D. G., Ibrahim, A.,& Jiao, X. (2022). Provably secure and fast color image encryption algorithm based on s-boxes and hyperchaotic map. IEEE Access, 10, 26257–26270.

[4] K. Rajendra Prasad, Santoshachandra Rao Karanam, D. Ganesh, Kazi Kutubuddin Sayyad Liyakat, Vamsidhar Talasila, P. Purushotham, "AI in public-private partnership for IT infrastructure development", The Journal of High Technology Management Research, Volume 35, Issue 1,2024,100496,https://doi.org/10.1016/j.hitech.2024.100496

[5] Güvenoğlu, E., & Tunalı, V. (2023). ZigZag transform with Durstenfeld shuffle for fast and secure image encryption. Connection Science, 35(1), 1–23.

[6] M. B. Mukesh Krishnan and D. Ganesh, "Hybrid Machine Learning Approaches for Predicting and Diagnosing Major Depressive Disorder" International Journal of Advanced Computer Science and Applications(IJACSA), 15(3), 2024. http://dx.doi.org/10.14569/IJACSA.2024.0150363

[7] Turukmane, A. V. ., Tangudu, N. ., Sreedhar, B. ., Ganesh, D. ., Reddy, P. S. S. ., & Batta, U. . (2023). An Effective Routing Algorithm for Load balancing in Unstructured Peer-to-Peer Networks. International Journal of Intelligent Systems and Applications in Engineering, 12(7s), 87–97Mondal, B., & Singh, J. P. (2022). A lightweight image encryption scheme based on chaos and diffusion circuit. Multimedia Tools and Applications, 81, 34574–34571.

[8] Kumar, T. P., & Kumar, M. S. (2021). Optimised Levenshtein centroid cross-layer defence for multi-hop cognitive radio networks. *IET Communications*, *15*(2), 245-256.

[9] T. Pavan Kumar, and M. Sunil Kumar. "Efficient energy management for reducing cross layer attacks in cognitive radio networks." *Journal of Green Engineering* 11 (2021): 1412-1426.

[10] Zia, Unsub, et al. "Survey on image encryption techniques using chaotic maps in spatial, transform and spatiotemporal domains." *International Journal of Information Security* 21.4 (2022): 917-935.

[11] Luo, Y.; Yu, J.; Lai, W.; Liu, L. A novel chaotic image encryption algorithm based on improved baker map and logistic map. Multimed. Tools Appl. 2019, 78, 22023–22043.

[12] Zhang, B.; Rahmatullah, B.; Wang, S.L.; Liu, Z. A plain-image correlative semi-selective medical image encryption algorithm using enhanced 2D-logistic map. Multimed. Tools Appl. 2022, 82, 15735–15762 .

[13] Elashry, I.F.; El-Shafai,W.; Hasan, E.S.; El-Rabaie, S.; Abbas, A.M.; Abd El-Samie, F.E.; El-sayed, H.S.; Faragallah, O.S. Efficient chaotic-based image cryptosystem with different modes of operation. Multimed. Tools Appl. 2020, 79, 20665–20687.

[14] Mondal, B.; Kumar, P.; Singh, S. A chaotic permutation and diffusion based image encryption algorithm for secure communications. Multimed. Tools Appl. 2018, 77, 31177–31198.

[15] Rachmawanto, E.H.; De Rosal, I.M.S.; Sari, C.A.; Santoso, H.A.; Rafrastara, F.A.; Sugiarto, E. Block-based arnold chaotic map for image encryption. In Proceedings of the 2019 International Conference on Information and Communications Technology (ICOIACT), Yogyakarta, Indonesia, 24–25 July 2019; pp. 174–178.

[16] Shalaby, M.A.W.; Saleh, M.T.; Elmahdy, H.N. Enhanced Arnold's cat map-AES encryption technique for medical images. In Proceedings of the 2020 2nd Novel Intelligent and Leading Emerging Sciences Conference (NILES), Giza, Egypt, 24–26 October 2020; pp. 288–295.

[17] Li, C.; Luo, G.; Qin, K.; Li, C. An image encryption scheme based on chaotic tent map. Nonlinear Dyn. 2017, 87, 127–133.
[18] Vishwas, C.; Kunte, R.S. An image cryptosystem based on tent map. In Proceedings of the 2020 Third International Conference on Smart Systems and Inventive Technology (ICSSIT), Tirunelveli, India, 20–22 August 2020; pp. 1069–1073.
[19] Gao, X. Image encryption algorithm based on 2D hyperchaotic map. Opt. Laser Technol. 2021, 142, 107252.
[20] Li, Y.; Wang, C.; Chen, H. A hyper-chaos-based image encryption algorithm using pixel-level permutation and bit-level permutation. Opt. Lasers Eng. 2017, 90, 238–246.
[21] Hazem Mohammad Al-Najjar & Asem Mohammad AL-Najjar 2012, 'Multi-Chaotic Image Encryption Algorithm Based on One Time Pads Scheme', International Journal of Computer Theory and Engineering, vol. 4, no. 3.
[22] Som, S & Sayani, S 2013, 'A non-adaptive partial encryption of grayscale images based on chaos', vol. 10, pp. 663-671.
[23] Raj, V, Janakiraman, S, Rajagopalan, S & Amirtharajan, R 2021, 'Security analysis of reversible logic cryptography design with LFSR key on 32-bit microcontroller', Microprocess. Microsyst., vol. 84, no. August 2020, p. 104265.
[24] Ganesh, D., Rao, K. J., Kumar, M. S., Vinitha, M., Anitha, M., Likith, S. S., & Taralitha, R. (2023, March). Implementation of Novel Machine Learning Methods for Analysis and Detection of Fake Reviews in Social Media. In 2023 International Conference on Sustainable Computing and Data Communication Systems (ICSCDS) (pp. 243-250). IEEE.
[25] Kumar, M. Sunil, et al. "Prediction of Heart Attack from Medical Records Using Big Data Mining." International Journal of Intelligent Systems and Applications in Engineering 11.4s (2023): 90-99.
[26] Kumar, M. Sunil, et al. "Reinforcement Based Concrete Modelling in Commercial Buildings Using Machine Learning Simulations." International Journal of Intelligent Systems and Applications in Engineering 11.4s (2023): 118-126.
[27] Godala, S. and Kumar, M.S., 2023. Intrusion Detection by Stacked Deep Ensemble Model with Entropy and Correlation Feature Set. International Journal of Intelligent Systems and Applications in Engineering, 11(4s), pp.07-21.
[28] Ramadevi, J., et al. "AI enabled value-oriented collaborative learning: Centre for innovative education." The Journal of High Technology Management Research 34.2 (2023): 100478.
[29] Jana, S., et al. "Plant Leaf Disease Prediction Using Deep Dense Net Slice Fragmentation and Segmentation Feature Selection Using Convolution Neural Network." International Journal of Intelligent Systems and Applications in Engineering 11.6s (2023): 76-85.
[30] Shanthi, T., et al. "A Novel approach Secure Routing in Wireless Sensor Networks for Safe Path Establishment of Private IoT Data Transmission." International Journal of Intelligent Systems and Applications in Engineering 11.9s (2023): 455-460.
[31] Neelima, P. & Reddy, Dr. (2019). Hybrid Algorithm using the Advantage of Krill Herd Algorithm with Opposition-Based Learning for Dynamic Resource Allocation in Cloud Environment. International Journal of Engineering and Advanced Technology. 8. 306-311. 10.35940/ijeat.F1064.0886S19.
[32] Madhuri, T. Sirisha, et al. "Big-data driven approaches in materials science for real-time detection and prevention of fraud." Materials Today: Proceedings (2021).
[33] Girinath, S., et al. "Deep Learning-based Segmentation and Computer Vision-based Ultrasound Imagery Techniques." 2023 Fifth International Conference on Electrical, Computer and Communication Technologies (ICECCT). IEEE, 2023.
[34] P. Venkateswarlu, et al. "Implementation of Latest Deep Learning Techniques for Brain Tumor Identification from MRI Images." 2023 8th International Conference on Communication and Electronics Systems (ICCES). IEEE, 2023.Peng, F.; Zhao, Y.; Zhang, X.; Long, M.; Pan, W.Q. Reversible data hiding based on RSBEMD coding and adaptive multi-segment left and right histogram shifting. Signal Process. Image Communication 2020, 81, 1–9
[35] Wu, H.B.; Li, F.Y.; Qin, C.; Wei, W.W. Separable reversible data hiding in encrypted images based on scalable blocks. Multimedia Tools Appl. 2019, 78, 25349–25372.
[36] Wu, X.; Weng, J.; Yan, W. Adopting secret sharing for reversible data hiding in encrypted images. Signal Process. 2018, 143, 269–281.