Nanotechnology Perceptions
ISSN 1660-6795
www.nano-ntp.com

An In-Depth Review On Enhancing Security And Data Embedding Capacity Using Deep Learning Approaches In Image Encryption

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

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

A message's content must be concealed as it traverses an unsecured channel due to the prevalent use of data digitization. Prior to transmission, the sender encrypts the message. Two things are needed for encryption to work: an algorithm and a key. When sending sensitive photos over an unprotected network like the internet, it is essential to take extra precautions to protect the recipients' privacy and confidentiality. Despite the fact that these algorithms lack standardization Use of chaos-based cryptosystems, such as Chebyshev polynomials, in conjunction with typical public key cryptosystems, such as RSA and El-gamal, can enhance security, similar to AES, DES, RSA, etc. While traditional algorithms like AES have long been the go-to, many experts now advise using chaos-based encryption methods for media files like images and videos because of how efficient they are computationally. Researchers have suggested customized algorithms for image encryption because these commonly used algorithms have slow encryption speeds and high processing requirements of safe encryption technologies make them unsuitable for real-time picture encryption.. When a picture is encrypted using chaotic technology, the cipher text displays an unpredictability that significantly reduces the potential of deciphering, making it one of the best algorithms available. As a result, chaotic technology-based digital image encryption algorithm research has emerged as a significant tool for contemporary digital image encryption. We talk about the major advancements in picture encryption. The purpose of this work is to introduce and summarize the picture encryption algorithms & metrics that are now in use, with the goal of evaluating them and providing academics and practitioners with the necessary background to comprehend the methods' present status. This paper examines the various methods of picture encryption and ranks them according to their strengths and shortcomings. In addition, comparative study has confirmed the evaluation matrices utilized to assess the performance and security of the algorithms for encryption in recent studies.In addition, the study gives the upper and lower limits for a set of efficiency, quality, and security evaluation measures for picture encryption methods and gives a thorough review of these metrics.

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

1.Introduction:

Each aspect of our commercial, industrial, and everyday lives has been profoundly impacted by the rapid evolution of the Internet and related information technology. These advancements have simplified and reduced the cost of producing massive volumes of data that we use every day. In tandem with these developments, mobile technology has grown in popularity over the past 20 years, with photos becoming the most common sort of data [1].When saving and sharing photos, it is crucial to secure their security and prevent them from unauthorized access because they contain extremely sensitive data. Researchers have taken notice of this, and it has since been cited extensively as an example of image encryption [2].

Encrypting images is a way to make sure that only authorized individuals can decipher transmitted data, even when there are security risks. Problems with data translation, authorization, and key distribution are only a few of the many that cryptographic methods must solve. Information security is of the utmost importance as internet-based systems continue to evolve. In most cases, users' information can be protected while being transmitted over public networks by using data encryption. However, there are drawbacks to using conventional techniques for data encryption in photographs. Problems such as high correlation between picture pixels, inefficient handling of huge data, etc.

Encrypting picture data has different challenges than text data. To start, text data is much smaller than visual data when it comes to real-world applications. Due to this, encrypting photos in an acceptable amount of time becomes challenging. The second scenario involves extremely strong connections between neighboring pixels in the picture data [3], which means that malicious actors can use statistical attacks to retrieve the actual photos. When encryption techniques aren't robust enough, they're useless. So, traditional methods of data encryption, such DES, TDES, AES, and RSA, which are commonly employed for text data encryption, aren't going to cut it when it comes to image data [4]. It is obvious that several methods are required to encrypt image data. Permutation, substitution, and diffusion are the three main designs used by image encryption techniques [5]. To change the locations of the image's pixels without changing their values is what the permutation step is all about. The result is a significant reduction in the correlation between neighboring pixels [6]. In order to methodically alter the statistical characteristics of picture pixels, the substitution and diffusion stage is executed [7]. What this means is that it allows for a methodical approach to changing the pixel values. Due of their inability to alter the images' histograms, permutation-only encryption techniques are insufficient [8]. The employment of both permutation and diffusion in an effective encryption scheme is highly recommended. Using encryption methods based on chaos, the permutation & propagation stages can be satisfied. Modern picture encryption often makes use of chaos-based techniques, which provide a practical mechanism to achieve diffusion and confusion simultaneously. Approaches based on chaos are highly conditional on the starting point. They have also found extensive usage in picture encryption due to their nature that the resulting values are random rather than periodic. The Basic Image encryption/Decryption Process is as shown in Figure 1.

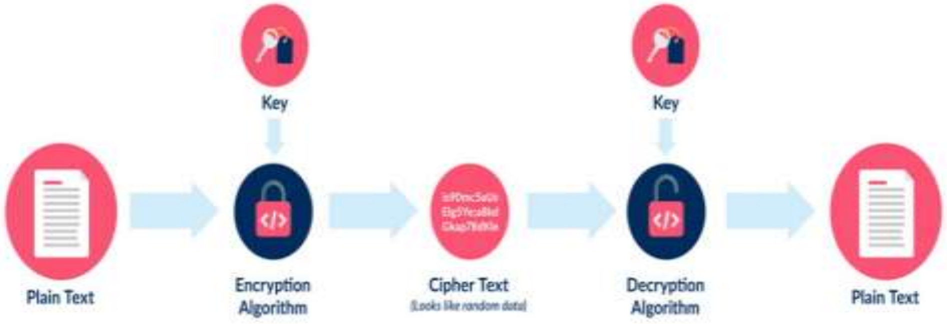

Figure 1.Basic Encryption/Decryption Procedure

The rapid growth of personal computers in the 1960s and 1970s coincides with a surge in research into chaotic dynamics. The advent of more powerful computers made it possible to study nonlinear systems of all kinds for the first time. One crucial feature of these systems is the existence of so-called strange attractions, which cause the surrounding trajectories to diverge. When these characteristics come together, the result is time series that seem random but are actually completely deterministic. Chaotic systems can be employed for encryption due of their seeming randomness. To prevent unauthorized parties from gaining access to sensitive information, cryptography defines encryption as the procedure of converting it into an unidentifiable type. Securely transferring images requires an encryption method because to the image content's critical properties, such as high redundancy, size, capacity, and correlation among bit pixels [8]. The process of converting a plain picture to a cipher picture, which effectively masks the original, important information, is accomplished by employing an encryption method. After that, the picture can be safely sent over the network without anybody else being able to decipher it. As a result, the encrypted picture is transformed back into its original format at the opposite end of the network using a decryption mechanism. In addition, a key is embedded into the original image during encryption, which is to encode the image. In contrast, a decryption method is employed during decryption in order to retrieve the original image from encrypted data. There are two primary kinds of keys used for encrypting and decrypting images: symmetrical keys (shown in Fig. 2) and asymmetric keys. When it comes to symmetric key cryptography both the methods of encryption and decryption use the same key. On the other hand, when it comes to asymmetric key cryptography, also known as public key cryptography, each process uses a different key.

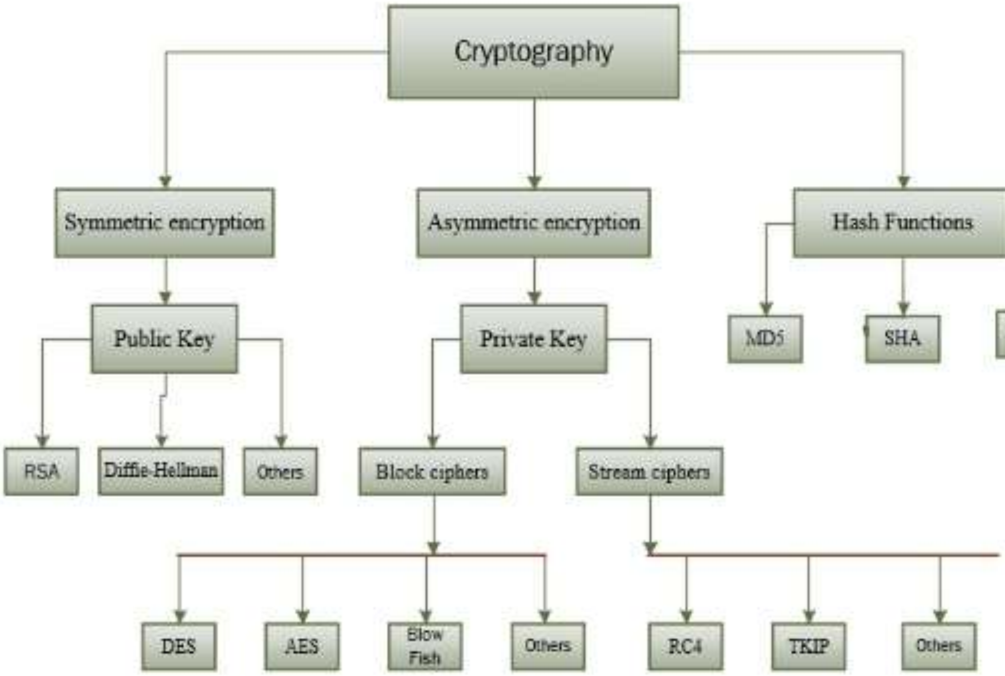

Figure 2. General Classification of image encryption algorithms

Recent years have seen academics paying special attention to the correlation between cryptography and chaotic systems, with the goal of developing cryptographic algorithms based on chaos to encrypt and communicate securely even when an attacker is present [9]. Thus, chaotic cryptography is the result of fusing chaos theory with cryptography research. Unlike chaotic systems, which are defined on real numbers, cryptosystems are defined on a finite set of integers. The main difference between the two is this. Classical ciphers such as AES and DES are inadequate for picture encryption since they display repetitive information pixels in similar images. Encryption approaches based on chaos theory tackle this problem by producing encrypted versions of images with keys that are randomly dispersed, thus hiding the original data [10]. Confusion and diffusion are the two main phases in creating a chaos-based image cryptosystem. The schematic of the building's system is shown in Figure 3. During the confusion phase, sometimes known as pixel permutation, the image is made into an unrecognizable shape by shifting the positions of the pixels over the entire image while maintaining the values of the pixels constant. Since the initial phase lacks enough security and is readily hackable, the dispersion step is then implemented. Because it produces a sequence that sequentially alters the values of all the image's pixels, a chaotic map is helpful for the diffusion phase. Iteratively repeating the confusion-diffusion process is necessary to attain an appropriate level of safety.

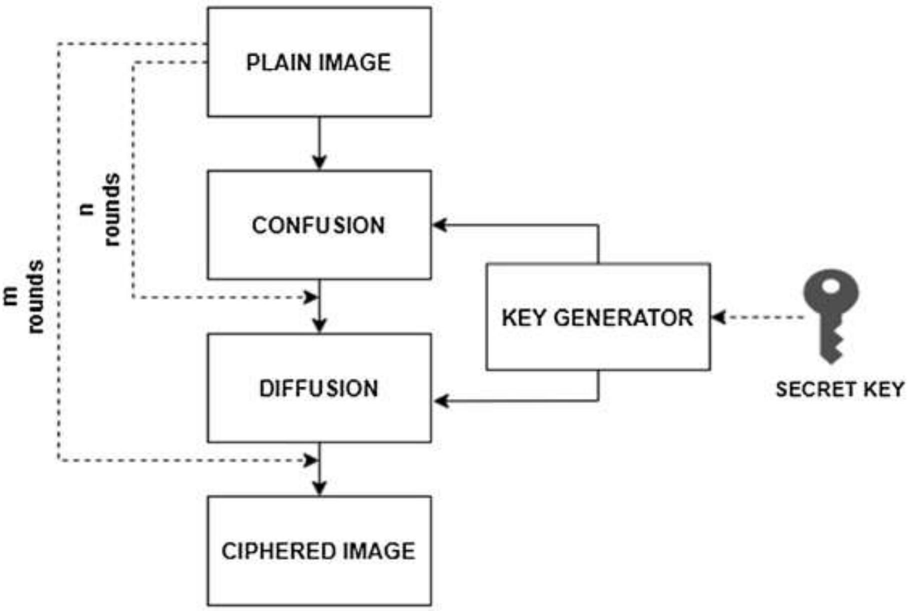

Figure 3. Chaos-based image cryptosystem architecture [11]

Picture encryption methods based on chaos theory are among the most preferred options because of their non-linearity, sensitivity to starting parameters, speed, and robustness [12]. Using the chaotic system's pseudorandom chaotic sequences, chaos-based algorithms can permute and distribute a plaintext picture [8]. Logistic map[13–14], Baker map[15–16], Arnold map[17–18], tent map[19–20], hyper chaotic map[21], etc. are some of the chaotic maps often used in picture encryption methods. Numerous chaotic system-based picture Various methods of encryption have been suggested by experts.Here is the structure of the remaining paper: Section 2 delves into the work's motivation, Section 3 examines the literature survey, Section 4 suggests the work's primary goals, and Section 5 wraps things up.

2. Motivation:

Increased data embedding and lossless extraction are both made possible by algorithms that have come a long way in the past few years. Several uses have found success with these methods, such as digital watermarking, content authentication, and secure data transmission. There are still issues with embedding capacity, security of information, and preserving image quality, even with these improvements. Nowadays, reversible data hiding techniques are crucial due to the growing importance of safe data transit and storage in the digital ecosystem. Because it allows new data to be embedded into digital media while guaranteeing the original material's lossless extraction, reversible data hiding is crucial in data security and multimedia applications. Data integrity, secrecy, and degradation-free recovery are critical in situations where embedding data within media is essential, yet doing so irreversibly compromises the data's integrity. Because traditional data hiding methods aren't always reversible, reversible data hiding is a must-have feature.

Reversible data concealing faces a major obstacle in the form of embedding capacity limitations. Improving the quality of the host media while embedding massive amounts of data is of utmost importance. Maintaining the media's integrity and perceptual quality while achieving high embedding capacity is sometimes a challenge for existing systems. Finding the right balance in this trade-off is still quite difficult. The safety of reversible data concealment is another important concern. The criticality of data-hiding applications makes it all the more important to guarantee the safety and reliability of the embedded data. Current approaches could be vulnerable to data manipulation, illegal extraction, or embedded data detection. The creation of trustworthy and secure techniques for reversible data concealing is crucial for protecting the confidentiality and safety of embedded information.

Furthermore, different types of digital media must be compatible with reversible data hiding schemes. The structures and traits of audio, video, and image files are distinct from one another. It is of the utmost need to develop versatile algorithms that can include and retrieve data from various media types, all the while guaranteeing their universal utility and compatibility. Problems with embedding capacity, data security, and picture quality preservation may be amenable to an adaptive strategy that makes use of ML and DL methods. Reversible data hiding approaches can be made more efficient and effective by combining the advantages of ML and DL algorithms.

3.Literature Survey:

Image Security is useful in many different contexts. Just about every other industry has a need for it. The literature proposes a variety of methods, some of which rely on sequences and others on common transformations. There are two main categories for picture security. Two methods of image encryption: full and partial. As may be seen in figure 4, we have conducted a systematic literature review.

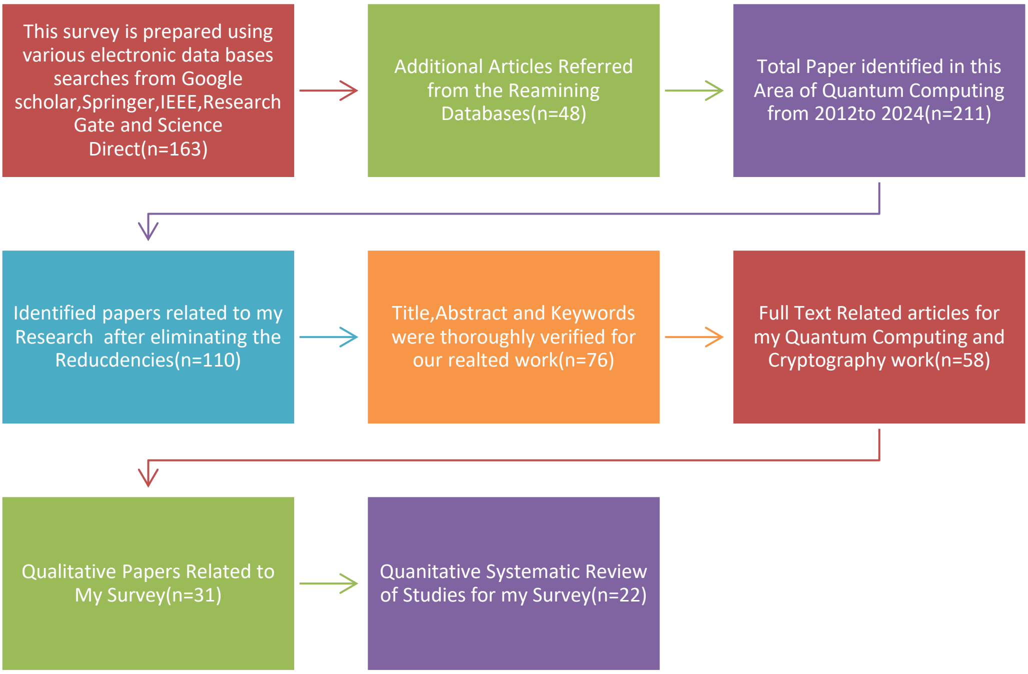
This survey is prepared using various electronic data bases searches from Google scholar,Springer,IEEE,Research Gate and Science Direct(n=163)
Additional Articles Referred from the Reamining Databases(n=48)
Total Paper identified in this Area of Quantum Computing from 2012to 2024(n=211)
Identified papers related to my Research after eliminating the Reducdencies(n=110)
Title,Abstract and Keywords were thoroughly verified for our realted work(n=76)
Full Text Related articles for my Quantum Computing and Cryptography work(n=58)
Qualitative Papers Related to My Survey(n=31)
Quanitative Systematic Review of Studies for my Survey(n=22)

Figure 4.Literature Survey on My proposed Research

The time-based multi-chaotic encryption method was shown by Hazem Mohammed et al. [22]. Using a plethora of chaotic functions, a new approach to picture encryption is suggested. Because of this, the cryptosystem's cryptographic algorithms become more complicated. To encrypt images, Som et al. [23] used a pseudorandom binary generator based on chaos theory. According to their relative importance in pixel formation, bit planes are classified as essential. Unimportant bit planes are not encrypted. Partially encrypting images speeds up the method. The algorithm's dependability is preserved due to the encryption of bit planes that hold sensitive information.

An encryption technique based on long-term short-term memory structures was suggested by Raj et al. [24]. The theme memory structure has been given the image in its component parts. A mixed lattice chaotic system in two dimensions has been employed for key generation. An improved chaotic logistical sequence is used to produce a key 1 that is more haphazard. The hyper chaos system is used to create chaos key 2. Using a double key for picture encryption in two rounds forms the basis of the algorithm. The picture encryption technique has excellent efficiency, accurate statistical data, and good accuracy, according to the findings of the simulations.

An approach of encrypting images of palm prints was suggested by Tian et al. [25]. A promising new area for research in the field of image encryption is DNA coding. Pixel diffusion is obtained by uniquely mapping the four base permutations of DNA coding to the values of picture pixels. Presently used approaches for selecting the eight DNA coding principles are mostly static. The five-dimensional hyperchaotic system employed DNA coding in conjunction with a traditional scrambling diffusion encryption framework. Critical space, confusion, and diffusion can all be accommodated by a chaotic mixed map-based approach. Many chaos maps are used in the process. There is no attack vector that can break the encryption scheme.

An image encryption approach that uses a nonlinear chaotic algorithm to ensure transmitted data correlation was described by Muhammad Asif et al. [26]. Assess UACI and NPCR near the nearest optima, according to the IEA. Using the chaotic sequence gathered from the initial two stages of the 3D chaotic system, prime numbers can be generated for the RSA method. In the last step, the pixel intensities are XORed with the chaotic series. We re-encrypt the result with the RSA technique. Using asymmetric cryptography features, the suggested method generates keys for asymmetric cryptography using a chaotic system. The suggested method is simple to execute and yields superior results. A 2D chaos graph that is derived from logic plus sine graphs was suggested by Hannah et al. [27]. A hyperchaotic quality permeates the final product. By utilizing obfuscation and diffusion techniques, it encrypts images. Get into a vertical and horizontal alignment at the same time with the Chaos Magic Transform. Column and row pixels are substituted with a chaotic matrix taken from a planned hyper chaos map to create diffusion. Two operations are necessary for the algorithm to get better performance. The temporal complexity of this approach is modest, and it is resistant to several attacks.

A novel method for encrypting color images related to genetic manipulation and chaotic systems was been forward by Wang et al. [28]. We employ a combined map network to circumvent the limitation of one-dimensional chaos, increase the data picture encryption through the usage of DNA rules, and produce new values for CML iterations by extending the Hamming distance. Compared to other methods, this one is more secure, has quicker encryption speeds, and can withstand any attack. An innovative encryption method is suggested by Xiao Chen et al. [29] that combines improved Logistic mapping with wavelet transform, Arnold mapping, plus Kent mapping. We employ wavelet transformations and Arnold maps to randomly rearrange the pixels in the image, and we build control parameters for the Arnold maps using Kent maps. By XORing the key value with the improved logistic map pixel value, pseudorandom numbers are generated by the enhanced logistic map. To find places where LC has no effect on PE, Chen et al. [30] provided a directional contained predictor in 2017. In addition, a DEPE (directionally-enclosed forecasting and expansion) system was put in place to make RDH more efficient. Pixels with a proportionate relationship between LC and PE were the only ones that DEPE allowed data embedding into. An RDHEI method based on Secret Sharing was suggested by Wu et al. in 2018 [14]. But the encrypted version of their image was twice as big as the original. The encrypted image requires more storage space and more bandwidth to transmit due to its larger dimensions compared to the original image. Applications with limited resources or those operating on a massive scale may find this limitation problematic, as may situations where storage space or network bandwidth is expensive or otherwise limited.

A method for encrypting images and hyperchaotic graphs was suggested by Natick et al. (2019) using a 2D sinusoidal corrective model. A low-cost implementation is possible, according to the performance analysis, however the method is complex. After three rounds of segmentation, Wu et al. (2019) presented a method that involved dividing the cover photo into blocks of varying sizes and then labeling them. Each pixel in the provided block has its least significant bits (LSBs) reserved. After that, as supplemental data, The block's pixel average and standard deviation are displayed here. The approach is affected by the size of the picture blocks and the predetermined threshold, and there is space for enhancements to the region.

An efficient method for encrypting images using a message transfer algorithm and an externally chaotic message is detailed by Liu et al. (2020). A message-passing approach is utilized for communicating with pixels that are nearby. The keys are made using two-dimensional logic diagrams. It rapidly generates extremely pseudo-random sequences of numbers. As a pseudorandom sequence generator, a 2D logic map is used to generate the set of edge pixel images. Both the method and the results show that the algorithm can withstand many low-cost attacks that are already out there. In 2020, a method known as histogram displacement was suggested by Zhao et al. [12]. The process of encoding involves transforming sensitive data into a message that only contains the numbers 1, 0, and 1. After that, we choose the middle segment bin to insert into the displacement histogram. These containers can all be used for incorporating a message consisting of the numbers 1, 0, or 1 by horizontally rearranging them. Band size is adjusted using the Threshold method, while the histogram is constructed employing the prediction error values produced by the Chess Board Projection Method. Attackers can easily identify and delete the Chess Board Prediction approach or accidentally alter it using image manipulation because of how predictable it is. Competitors with enough knowledge can use the predictability of the method to find hidden data or even remove it entirely. The integrity and trustworthiness of the embedded data are jeopardized by this limitation.

An encryption system that relies on compression sensors and is built on a memristive chaotic system was proposed by Haiying Hu et al. (2021). To reduce storage costs, this method applies a double compression to the image. The pixel array is encrypted twice using block encoding and the zigzag transform. The final cipher image is generated using chaotic pseudo-random sequences and diffuse image matrices. Lastly, the scheme continues to exhibit good decompression performance even when the compression ratio is set to 0.25, according to simulation and performance study. Security analysis confirms that the scheme is highly secure and can survive a variety of attacks. In 2021, a block encryption approach was employed by Chen et al. [11]. To make additional room, we used lossless compression methods like Huffman coding to shrink the bit plane after splitting the encrypted picture in half. In the end, the original cover image was successfully restored by the collective MSBs. The capacity for embedding was constrained since the block was inadequately sized. Using Hamming coding, Kim et al. [31] encrypted and compressed picture blocks in 2022 to hide data.

The amount of data that could be embedded was also controlled through the implementation of quantization. In order to encode more data in RDH utilizing Hamming codes, some bits in the host media need to be modified. These changes may cause the host medium to change or distort in a way that is easy to see, which could impact its overall quality or how well it is perceived. Hamming codes might not provide the best compromise for reducing distortion, as the trade-off between embedding depth and distortion becomes critical. Chen[32] and colleagues came up with RDHEI, a novel secret-sharing method, in 2022. By utilizing numerous information hiders, this strategy improves upon the prior one. The embedding rate decreases with increasing photo shares because the method developed by Chen et al. keeps the overall embedding volume constant. The data is spread out among a number of shared images, with a constant overall embedding volume. The rate at which each image is embedded grows in direct proportion to the number of shared photographs. So, when dealing with a huge number of shared photographs, the approach can struggle to incorporate all the data needed in each one.

The innovative Ensembled Learning approach, developed by Shaiju and colleagues in 2023, makes use of the Fibonacci Transform. Here, the receiver tries to decipher the blocks by executing every conceivable Fibonacci transformation. One big drawback of this strategy is how computationally intensive it is. Doing many Fibonacci conversions can make processing time and complexity go up tremendously [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 Transform" Electronics 12, no. 2: 450.	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 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, 143, 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 numerous chaotic functions [27]	Appl. Math. Inf. Sci, vol. 9, no. 6, pp. 2991-2995,2015	2015	Image Encryption technique that employs a nonlinear chaos method	Requires better performance and easy implementation

4.Objectives:

The following are the four study objectives derived from the proposed approach and expected results:

1. **To Develop an Enhanced Ensembled Deep Learning Model for MSB Prediction:**
   - **Objective:** To enhance the accuracy of image Most Significant Bit (MSB) plane predictions, build a state-of-the-art deep learning model that uses adversarial training, attention mechanisms, transfer learning, and other techniques.
   - **Motivation:** Improving the accuracy of MSB predictions is crucial for reducing prediction mistakes and improving the capacity and quality of data embedding.
2. **To Implement a Reversible Data Hiding Technique Utilizing Prediction Errors:**

- **Objective:** Create and execute a method for reversible data hiding that maintains high picture quality while inserting extra data into the forecasting errors produced by the MSB prediction module.
- **Motivation:** To increase the data ability to embed and guarantee the process's reversibility, prediction errors are used as carriers for data embedding. This helps to reduce the effect on the overall image quality.

3. **To Enhance Security through Image Encryption:**
   - **Objective:** Secure the watermarked photographs by incorporating a strong encryption scheme; this will make the encoded data impenetrable to prying eyes.
   - **Motivation:** Encrypting images securely is essential for keeping embedded data private and undamaged, particularly during transmission or storage.
4. **To Validate the Proposed Scheme through Accurate Data Extraction and Original Data Recovery:**
   - **Objective:** Create and test an extraction method that successfully decodes the watermarked picture, recreates the expected MSB plane, and safely retrieves the actual embedded data without corruption or loss.
   - **Motivation:** Proof of the efficacy and dependability of the suggested reversible data hiding strategy relies on precise extraction & recovery of the embedded data.

5.Conclusion:

Image encryption techniques used in many sectors are thoroughly examined in this research. The most up-to-date studies published in the last twelve years have been systematically reviewed and organized into appropriate categories to facilitate comprehension. It is clear from the reviewed literature that picture encryption is an emerging topic that has a long way to go before it reaches maturity in terms of security, computing efficiency, and parameter adjustment. In order to validate the performance of an encryption algorithm, most publications do not employ all of the standard checks, based on the findings of the evaluation procedures for encryption methods. It would be helpful to have a standardized way to measure how well new picture encryption methods work. Encryption of multimedia files has become more important in recent decades. Additionally, this chapter details the extensive analysis of several algorithms to help with future research and talks about the difficulties of current chaos-based image encryption algorithms.

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. Burada, S., Manjunathswamy, B.E. & Kumar, M.S. Deep ensemble model for skin cancer classification with improved feature set. Multimed Tools Appl (2024). https://doi.org/10.1007/s11042-024-19039-5
24. Girinath, S., et al. "Real-Time Identification of Medicinal Plants Using Deep Learning Techniques." 2024 International Conference on Trends in Quantum Computing and Emerging Business Technologies. IEEE, 2024.
25. Kumar, M. Sunil, et al. "Use of Blockchain for Fake Product Detection." 2024 IEEE International Conference on Computing, Power and Communication Technologies (IC2PCT). Vol. 5. IEEE, 2024.
26. Sreedhar, B., et al. "Moving Vehicle Registration Plate Detection Using Machine Learning." 2024 International Conference on Trends in Quantum Computing and Emerging Business Technologies. IEEE, 2024.
27. Burada, Sreedhar, Manjunathswamy Byranahalli Eraiah, and M. Sunil Kumar. "Optimal hybrid classifier with fine-tuned hyper parameter and improved fuzzy C means segmentation: skin cancer detection." International Journal of Ad Hoc and Ubiquitous Computing 45.1 (2024): 52-64.
28. M. Sunil Kumar. "AI technologies, tools, and industrial use cases", book Toward Artificial General Intelligence, De Gruyter 2024. https://doi.org/10.1515/9783111323749-002
29. Venkata Ramana Saddi, Dynamic Scheduling Algorithms for Serverless Computing Solutions in the Cloud", 2024 International Conference on E-mobility, Power Control and Smart Systems (ICEMPS), DOI: 10.1109/ICEMPS60684.2024.10559356. 2024
30. Venkata Ramana Saddi," Reducing loss for Brain tumour detection and classification in MRI using deep learning techniques",Communications on Applied Nonlinear Analysis,Vol 31 No. 6s, PP.330-341.(2024)
31. .Venkata Ramana Saddi, "Exploring the Quality of Service Impacts of Cloud Computing over Wireless Networks", 2024 International Conference on E-mobility, Power Control and Smart Systems (ICEMPS), DOI: 10.1109/ICEMPS60684.2024.10559341, 2024.
32. Panchikkil, Shaiju, Siva Priya Vegesana, V. M. Manikandan, Praveen Kumar Donta, Praveen Kumar Reddy Maddikunta, and Thippa Reddy Gadekallu. 2023. "An Ensemble Learning Approach for Reversible Data Hiding in Encrypted Images with Fibonacci Transform" Electronics 12, no. 2: 450.
33. Chen, B.; Lu, W.; Huang, J.; Weng, J.; Zhou, Y. Secret sharing based reversible data hiding in encrypted images with multiple data-hiders. IEEE Trans. Dependable Secur. Comput. 2022, 19, 978–991.
34. Chen, M.K.; Chang, C.C. High-capacity separable reversible data hiding method in encrypted images based on block-level encryption and Huffman compression coding. Connect. Sci. 2021, 33, 975–994.

35. 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
36. 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.
37. Wu, X.; Weng, J.; Yan, W. Adopting secret sharing for reversible data hiding in encrypted images. Signal Process. 2018, 143, 269–281.