Frontiers in Health Informatics
ISSN-Online: 2676-7104
www.healthinformaticsjournal.com
2024; Vol 13: Issue 3
Open Access

Enhanced Deep Learning Based Cryptographic Digital Optical Chaotic Mapping Method for Image Encryption

[1] V.Jayabharathi, [2] Dr.S.Sukumaran

[1] Ph.D., Research Scholar, Department of Computer Science, vjayabharathimca@gmail.com,
Erode Arts and Science College (Autonomous), Erode-638009, Tamilnadu, India

[2] Associate Professor, Department of Computer Science, prof_suumar@yahoo.com
Erode Arts and Science College (Autonomous), Erode-638009, Tamilnadu, India

Cite this paper as: V.Jayabharathi,S.Sukumaran (2024). Enhanced Deep Learning Based Cryptographic Digital Optical Chaotic Mapping Method for Image Encryption. *Frontiers in Health Informatics, 13*(3), 940-949.

Abstract

In multimedia, assume a significant part for transmission as well as this is vital to safeguard the image information while sending over network. One of the most crucial things in the next scenario is the transmission of images to multimedia material. Images are crucial for multimedia transmission, and it's critical to safeguard picture data when it's being transmitted across a network. Image encryption and decryption can be used to do this, and a variety of strategies should be applied to safeguard private image data from unwanted access. In this work, the suggested approach Digital Chaotic Mapping based on digital image encryption is contrasted with previous studies that have used various techniques for picture encryption through the utilize the related deep learning methods are to be simplify the exploration of a variability of image. The suggested approach was utilised to assess other image-related measures, including F1-score, recall, and precision. The proposed approach yields the best results in terms of the accuracy of the encrypted image, whereas accuracy values compare the methods that are currently in use.

keywords: *Image Encryption Image Steganography ECC Logistic Regression Digital Optical Chaotic Mapping Digital Security*

1 INTRODUCTION

Image protection can be classified into various categories, one of which is image encryption. In the global digital computer industry, protection is the most important concern. These measures of safety include encryption, steganography, and watermarking [1]. Numerous applications that are associated with the phrases physical safety, virtual security, and factual safety can benefit from image processing. When it comes to image safety in particular, these words are closely related to statistics protection. They have to do with identity authentication, surveillance packages, national security, and other things. Therefore, it is safe to use contemporary technology, such as deep learning and the neural community set of rules, which employ education to forecast the upcoming chances for image encryption. While steganography and watermarks use imperceptibility to hide the game's name, encryption is a specific phrase that refers to its ability to make hackers difficult to defeat. This ensures that the wrong hands will no longer handle exclusive statistics. Images are the most important media to encrypt since they are harder to hide and more reliable. Pictures are regarded as one of the most significant assets of information security because to the quick advancements in internet technology and security [3].

One approach to define image graph encryption is as the act of encrypting a secret image so that unauthorised users are unable to access it. Encryption is mostly used to protect the privacy of digital information stored on laptops or sent over the internet or any other computer network. Image encryption is essential for providing the user with safety and privacy by preventing unauthorised users from accessing the data. Applications for image and video encryption can be found in many domains, such as army communications, clinical imaging, multimedia systems, internet

communication, and tele-remedy [2]. Usually, the encryption approach is the opposite. Because decryption requires a secret key or password, it decodes the encrypted statistics so that only a licenced consumer can decrypt them. This work aims to analyse and identify the encrypted image as its subject is related classification of encrypted image graphs using deep learning of the era with the ResNet 50 version.Despite the fact that this analysis only assesses one of the encryption techniques used in those images, the effectiveness of those designs utilising deep learning techniques allows the total technique to be used to an algorithmic diffusion. Sports are now smaller, faster, and simpler to analyze on a large scale as a result of the integration of encryption and artificial intelligence. This kind of machine is special as, to the extent that the creators know, nobody has at any point dealt with a multi-name type with an encoded picture. Some exiting methods rely on a single key, while the remaining ways rely on two keys for encryption. The confusion and diffusion processes, which are crucial to all picture encryption techniques. Image, after which pre-processing is applied to normalize the image and get it ready for the confusion process.

2. RELATED WORK

Safety in bometric records was redefined by Gatouillat et al. [8]. They discussed the issues with several biometric approaches, including face, fingerprint, and retinal scanning. This unique biometrics have also been utilised to encrypt data using popular image steganography techniques like pixel value differencing (PVD), transform area strategies (DCT/DWT), spatial domain strategies (LSB-Steganography), and hybrid techniques like singular value decomposition (SVD). Binarization was introduced to handle records including biometric data.

A new set of rules for pix based entirely on Quantum Steganography was proposed by Ding et al. [6]. The two algorithms that were given were amazing because they didn't require any conventional computers to operate and they were completely blind. The Hilbert picture scrambling set of rules was used to finish the image preparation process, rearranging the pixels into different places.

A summary of several steganography techniques and tools was provided by Tang et al. [15]. unique steganalysis methods to break down the previously stated steganographic approaches, such POV-based total Chi-square check Pallette Checking, standard Blind Detection, and so on. had been briefly explained. For facial element portrayal, Deng et al. [7] recommended a PCA (chief component assessment eigenface) with solid rotating versatility; nonetheless, its presumed generally speaking execution is fundamentally lessened while the light and mindset trade are enormous. The previously mentioned set of rules shows that it is so hard to really communicate complex properties when tests and figuring gadgets are restricted, uncovering the constraints of shallow organizations. As indicated by Tortorella et al. [17], this study analyzes what 10 H4.0 virtual advancements mean for four powerful framework qualities in the setting of medical clinics. With 109 H4 and resilient healthcare No experts from both ascending of clinics, we directed a review for this reason. 109 strong medical care and H4.

The poll had no professionals taking part. The gained information was inspected utilizing both univariate and multivariate measurable procedures. Our outcomes recommend four H4.0 virtual advancements that will essentially impact the four flexibility abilities: computerized stages for helpful sharing of impacted individual information and measurements; far off discussions and upgrade of the consideration plan continuously virtual harmless consideration; and incorporated clinical crisis guides.

As indicated by Brindha et al. [5], records picture that pass on phenomenal enlightening styles should be scrambled with uncommon security. This article makes sense of how the capability extraction is utilized to take conceal snap pictures for the image class. The okay-Nearest Neighbor (ok-NN) method of the picture type method is used to classify the query document using a sophisticated collection of attributes pulled from the record database. The optical person acknowledgment (OCR) approach is utilized to recognize the record type and to look into text or numbers in reports as well as affirming their area. The archive type decides the priority level. The files with extraordinary priority levels are distributed using novel methods. Reports with a higher

priority are encrypted with the highest level of security, while documents in lower priority categories are encrypted with lower levels of security.

The proposed work was tested for various report types with a wider range of image attributes for a substantial educated database. The findings indicate that compared to a standard encryption method for all document types, a high rate of encryption for a set of report pages with priorities is more effective in evaluation. The utilization of the Chaotic Neural Community (CNN) to create, carry out, and dissect scratched hash abilities is finished by Abdoun et al. [2]. These frameworks produce two forms of hash cost lengths, 256 and 512 pieces, and are totally founded on Wipe development. While the subsequent design is made utilizing a blend of nonlinear qualities and one-layered CNN, the principal structure is comprised of two-layered CNN. Without a doubt, the recommended structures utilize strong nonlinear frameworks, explicitly a brain network framework and a turbulent gadget. Furthermore, the proposed study is a clever methodology that consolidates Wipe creation with turbulent brain organizations, which has been demonstrated to be secure against known attacks. The overall performance of the two suggested systems is subjected to security and speed analyses. To guarantee security, the two recommended strategies' joined hits can't surpass two for 256-bit hash values and three for 512-cycle hash values.

3. PROPOSED METHODOLOGY

The process of accessing data in cryptography is referred to as encryption. Historically, cryptography has been supported by a range of encryption techniques. Early on, military communications were encrypted by a robot. Since then, fresh methods have emerged and proliferated throughout every aspect of modern computing. The concepts of symmetric key and public key are used in modern encryption schemes.

3.1 Digital Optical Chaotic Mapping based Digital Image Encryption Method (DOCM)

Within the picture processing method, there are three types of image protection: steganography, which aims to conceal methods and secrets within the picture in a way that the thief may not always observe [10]. Second, a watermark increases a picture's imperceptibility in order to conceal secrets within it. Steganography and watermark should not display the game message's name [12]. The image is encrypted in the remaining 0.33 kind. In this case, the image itself may represent the name of the game, making it difficult for the hacker to decode [13].

Algorithm of Proposed Digital Optical Chaotic Mapping based Digital Image Encryption Method

The Authenticated Encryption function CNN Cipher Image − AEAD[C f , Pad,r, ρ]	
Step 1:	**ρ ≤ ρmax(Pad,r) − 1**
Step 2:	**CNND = CNNDuplex[C f , Pad,r]**
Step 3:	**CNNDAEAD.initilalize(K, IV) with K ∈ Z |K| 2 and IV ∈ Z b 2 HM0 = CNND.initialize(K, IV)**
Step 4:	**for i = 1 to I − 1 do CNND.duplexing(ADi ||1, 0) end for**
Step 5:	**HM = CNND.duplexing(ADI ||0, |M1|) C = M1 ⊕ bHMc|M1 |**
Step 6:	**for j = 1 to J − 1 do HM = CNND.duplexing(Mj ||0, |Mj+1 |) C = C||(Mj+1 ⊕ bHMc|Mj+1 |) end for**
Step 7:	**HM = CNND.duplexing(MJ ||1, ρ)**
Step 8:	**while |HM| <Tlen do HM = HM||CNND.duplexing(0, ρ) end while**
Step 9:	**T = bHMcTlen**
Step 10	**Return (C, T).**

One needs to consider the most important encryption issues caused by randomly jumbled pixels when generating a random key. A pixel's placement can be adjusted to modify how an image is observed, but the information stays the same. A pixel is made up of the intensity of the value and two distinct variable positions that are coordinated (X, Y). Although altering the coordinates results in altering the position, the value's intensity remains constant. The go back worth at the receiver side must be taken into account because it is designed for uncertainty. This goal led to the creation of the following algorithm, which is utilized for encryption by the transmitter and decryption by the receiver. The proposed method allows one to select the row and column in a given representation [6]. Each repetition of a feature produced from a column and row will select the next column or row, and each feature will save the vector for manipulation.

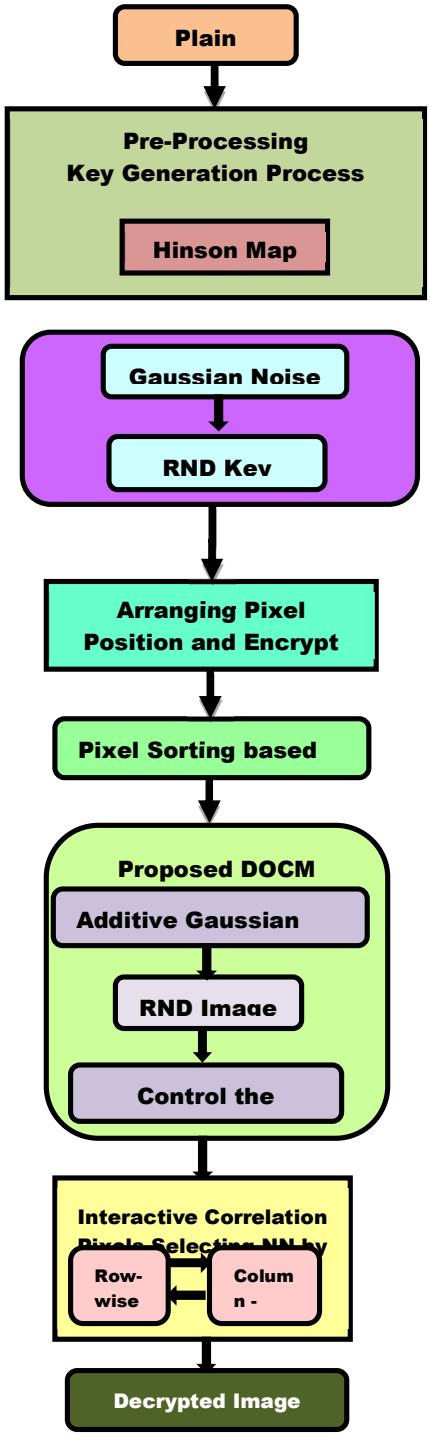
3.2 Dataset

Experiments are carried out on five popular image datasets: Cifar-10, MNIST, SVHN, Fashion-MNIST, and Flower images to confirm the efficacy of our suggested algorithm. Ten different item kinds are included in the 60 thousand images that make up the Cifar-10 dataset. Each image is a color, 32 by 32 by 3. 70,000 28 × 28 pixel setting pixels make up the MNIST dataset. The dataset is divided into ten categories, with 10,000 images serving as the test set and 60,000 images as the training set. The Google Street View number is the source of the Street View House Number (SVHN) dataset. The dataset we picked comprises of 73257 pictures in the preparation set and 26032 pictures in the test set. The picture charts are trimmed to a size of 32×32×3, and the variety pictures range from 0 to 9. 70,000 dress pictures in ten classes, 60,000 preparation pictures and 10,000 test pictures with foundation pixels of 28 by 28 make up the Design MNIST dataset. Day, dandelion, rose, sunflower, and tulip are the four classifications into which the 3670 photographs in the Blossom photographs assortment are isolated.

The floral image databases' sample images are three-dimensional color image graphs of varying sizes. The excess 500 pictures are leaned toward from the test set, while the leftover 3126 pictures are browsed the preparation set. Assessment is done on the sender's end using data from both plain and encrypted pictures before the information is sent to the recipient. As represented in figure 1.2, the plain picture is handled and scrambled utilizing keys that are like those

Fig.1.1 Flow Diagram of Digital Optical Chaotic Mapping based Digital Image Encryption Method

utilized in the collector's activity, yet entirely in switch. Using the data in the key, a plain image initiates the encryption process, creates a cipher image, and sends it to the other party to complete the process in the opposite direction. Color and grayscale images, as well as images from a standard dataset for benchmarking and evaluation, can all be encrypted using the suggested method. At the point when irregular factors with an ordinary conveyance with a mean of nothing and a standard deviation (σ) are added to standard information, the subsequent commotion is known as Gaussian clamor. It's a profound learning approach that adds flightiness to the loads and information. In deep learning, it is a method for making the weights and input data unpredictable.



The Gaussian noise is additive in nature. This suggests that one should simply apply the noise from the original image after creating a noisy image. Following that, the image saves the parts that show the standard deviation and harvests the parts that are homogeneous. Given the current ascent in data breaks, getting media applications has turned into a basic concern. Elliptic Bend Cryptography (ECC) related to the High level Encryption Standard (AES) in CTR counter mode is utilized to complete this encryption cycle. In order to generate an arbitrary number sequence based on the curve in the cryptographic system, we have suggested utilizing ECRG. Then, erratic keys are utilized to direct the AES-CTR on these groupings to scramble pictures. The cipher and plain image come from a typical collection called Tiffany. Utilizing the logistic map equation, a Hinson map, and the suggested random function to evaluate the randomness of the proposed method.

The histogram modification process uses the pixel sorting method to carry out the secret data in binary form. An innovative artificial neural network-based system is trained to determine the best way to sort the prediction errors in order to embed the neural networks. The method provides a more ideal way to insert pixels.

The encrypted pixel picture will be split into black and white pixels using a checkerboard pattern. The distinct random integer sequences S, whose values fall between 0 and 255 and which constitute the data keys, are sent during the data concealment phase.

By bit XORing one integer sequence from each of the eight keys with the white pixels in an image block, data concealment can be achieved. A three-piece grouping from the encoded message relates with each key. Both the original image and the hidden message must be retrieved, and the recipient must select the data keys and decryption key. While confusion is used to create ignorant cipher text, diffusion is used to increase the plain text's repetition over the most important part of the cipher text, making it more opaque. The stream cipher relies solely on confusion, whereas the block cipher uses diffusion. Utilizing the key stream components delivered by a one-layered turbulent guide, pixel values are progressively changed all through the dispersion step. The modification to a single pixel typically depends not only on the corresponding key stream element but also on the cumulative effect

of all previous pixel values, where p(n), k(n), c(n), and c(n-1) denote the current plain pixel, key stream element, output cipher-pixel, and previous cipher-pixel, respectively.

$$c(n) = k(n) \emptyset p(n) \emptyset c(n-1) \ldots\ldots (1)$$

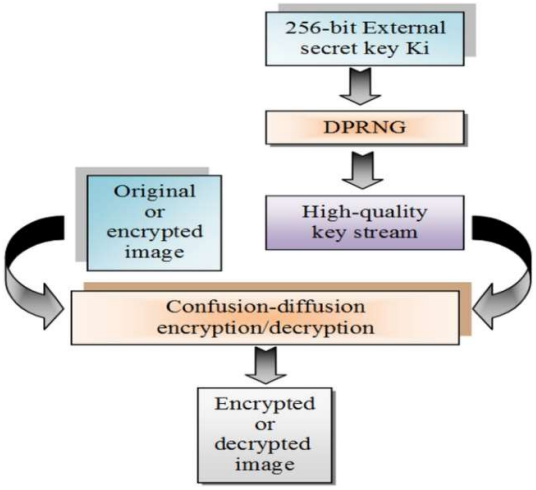


Fig.1.2 Image Encryption Processing

This diffusion method, which can spread small differences in the plain image to large pixels in the ciphered image, may render differential attack virtually useless. The underlying pixel, c(- 1) should be put as a seed together to encode. Taking everything into account, present status of the tumultuous guide emphasis can yield k(n), the key stream component. The suggested hash function is robust and satisfies the properties of hash algorithms, including random-like (non-periodic) behaviour, ideal sensitivity to the original message and secret key, one-way property, and optimal diffusion effect, as shown by the security analysis in figure 1.3. Since images are easier to process than text, they are frequently used in communication. In the event that the user communicates over a compromised network, information security becomes critical. In order to preserve the security of the information being transmitted, encryption, or the system used to change an image into another image that is difficult to understand, is crucial. Applications for image encryption can be found in many domains, such as the military and security services, or anywhere sensitive or confidential data is stored. The following three concepts form the basis of image encryption techniques or algorithms: Pixel substitution: changing the value of each pixel; Pixel permutation: shuffling the pixels; Visual Alteration. One of the security factors taken into account for encryption techniques is an image histogram. The frequency distribution is shown on the histogram, which also offers information on the frequency of each pixel value. The Advanced Encryption System (AES) is one of the encryption techniques that uses pixel value modification to produce a uniform image histogram that protects against plain text attacks while requiring no loss of data during the decryption process. This is not helpful in this instance because the quantity of hidden data depends on the neural network that is used to hide images in other images, which in turn depends on the redundant area in the cover images.

4. RESULTS AND DISCUSSIONS

The usefulness of the proposed algorithm is evaluated using many datasets, and its overall performance is studied using four evaluation metrics: Precision (Pre), Take into account (Rec), F1, and mean average Precision (mAP), in that order. In the end, the three components of the experimental system are delivered in a methodical manner. First, a training network model is used to extract image features. Second, the encrypted image incorporates the extracted capabilities to achieve the information hiding characteristic. Thirdly, the retrieval characteristic is recognized by extracting the concealed capabilities from the cipher text.

4.1 Evaluation Metrics

We believe tests with a similar mark to be tantamount and tests with special names to be different to use the marks of the factual examples completely. Within the check set, experiments for evaluation are carried out. The scope of equivalent and different examples that were successively separated from the dataset is addressed by TP and FP. Meanwhile, the dataset's immense range of comparative and various examples that could never again be recovered is displayed as FN, TN. Precision, which is the percentage of similar samples in the back seek effects, is represented by pre. Rec is used to indicate Remember, which is the percentage of comparable samples among all similar samples in the

again search consequences. Precision and remember are distinct in that the former uses the range of all comparable samples as its denominator, while the latter uses the quantity of all search effects.

$$Precision = TPX\ TP + FP \ldots\ldots\ldots\ldots(1)$$
$$Recall = TPX\ TP + FN \ldots\ldots\ldots\ldots(2)$$

Accuracy and memory on their own are insufficient to assess retrieval performance in a thorough and unbiased manner. As a result, we continued to compute the mAP and F1, respectively. The formula (4) is used to calculate the F1 value, which is the harmonic common of recall and precision. Formula (eight) illustrates how the mAP, or mean average precision, can be used to solve the unmarried-factor cost challenge of the above indicators and increase the display of the global performance indicators. As shown in formula (2). The labels of the query image and the image graph in the lookup set are denoted by lq and lt, respectively, in procedure (3).

$$F1=\frac{PrecisionXR}{Precision+Recall} \quad \ldots\ldots\ldots\ldots(3)$$

$$MAP=\frac{1}{num\_query}\sum_{i=1}^{num\_query}\sum_{j=1}^{threshold} index\ lq_{num(index)}^{i,k}..(4)$$

Numerous evaluation criteria can be applied to compare different approaches for image encryption. There are more than five evaluation criteria for the suggested technique. The majority of assessments on this challenge focus on unpredictability and vulnerability to assaults; correlation within the image and between its pixels is crucial. Additionally, the hash function's speed performance is examined and contrasted with a hash feature that was developed using CNN and sponge creation.

In this section, it is explained the results of research and at the same time is given the comprehensive discussion. Results can be presented in figures, graphs, tables and others that make the reader understand easily [14], [15]. The discussion can be made in several sub-sections.

Table 1.1Performance Evaluation of Digital Optical Chaotic Mapping based Digital Image Encryption Method

Algorithms	Accuracy	Recall	Precision	F1-Score
Logistic Regression	**92.61**	**91.41**	**91.65**	**92.58**
ECC	**93.31**	**92.91**	**92.81**	**93.23**
ML-ELM	**91.91**	**91.14**	**92.82**	**91.91**
DOCM	**94.75**	**94.12**	**94.23**	**94.71**

The digital level optical Chaotic Mapping principally based Digitized image Encryption method's overall performance is explained in Table 1.1, which also compares the results to current methods in terms of image correctness, recall, precision, and f1-rating.

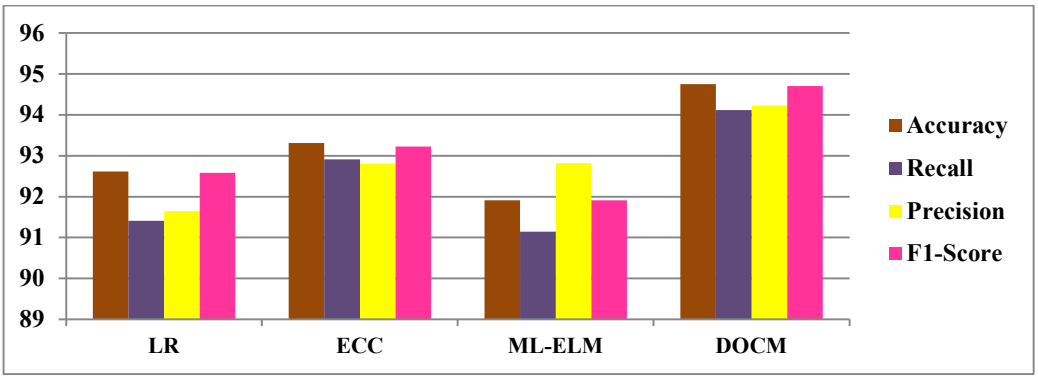


Fig 1.3 Evaluation of Digital Optical Chaotic Mapping based Digital Image Encryption Method

The performance of the digital level optical Chaotic Mapping based Digitized Image Encryption method is explained in Figure 1.3. Image accuracy, recall, precision, and F1-score are analysed and compared with those of current and suggested methods for accuracy, precision, recall, and F1-score. The Digital Optical Chaotic Mapping approach, when compared to the current methods, yields the best results.

5. CONCLUSION

This paper presents an encryption technique for images using a random key and deep neural network. The three random factors that contributed to the increase in the chaotic picture are the logistic map, the Henon map, and the key thing region of unpredictability. To put it another way, encryption has been used to alter the image's pixel region as well as the relationship between a single pixel and its neighbours. The deep neural network community is responsible for selecting the pixel area that follows. A histogram is the ideal size for picture cryptography, and the strength of the suggested method is demonstrated by its consistency. Grayscale and colored snapshots are the two types of images that are utilized to compare the suggested method with the Cifar-10, MNIST, SVHN, style-MNIST, and Flower images datasets. The results achieved have been satisfactory, and the system's effectiveness serves as evidence of the suggested method's dependability. The suggested approach, known as the digital optical chaotic mapping methodology, provides best-in-class results in all metrics overall performance even when it is linked to the current techniques.

REFERENCES

[1]Albatish, I.M., et al. Modeling and controlling smart traffic light system using a rule based system. Proceedings - 2019 International Conference on Promising Electronic Technologies, ICPET 2019, pp. 55–60, 2019, 8925318

[2] Abdoun N S. El Assad, T. Manh Hoang, O. Deforges, R. Assaf, and M. Khalil, “Designing two secure keyed hash functions based on sponge construction and the chaotic neural network,” Entropy, vol. 22, no. 9, p. 1012, 2020.

[3] Aceto, G.; Persico, V.; Pescapé, A. Industry 4.0 and Health: Internet of Things, Big Data, and Cloud Computing for Healthcare 4.0. J. Ind. Inf. Integr. 2020, 18, 100129.

[4] Dr.S.Brindha, Dr.S.Sukumaran, Dr.S.Ravichandran, “Effective Taxonomy of Advanced Mobile Edge Computing of Long-Term Evolution for 5G”, International Journal of Science and Research (IJSR), Volume 11, Issue 3, March 2022.

[5] Dr.S.Brindha,Dr.S.Sukumaran,Dr.S.Ravichandran, “Deployment Liabilities of Deep Learning Based on 5G Mobile Applications Using Advanced Mobile Edge Computing Taxonomy”, International Journal Of Creative Research Thoughts (IJCRT), ISSN:2320-2882, Volume 9, Issue 11, Pp: 567-571,UGC Approved Journal No: 49023(18), 30thNovember 2021.

[6] Ding, Y., Wu, G., Chen, D., Zhang, N.: DLEDNet: a deep learning-based image encryption and decryption network for internet of medical things. IEEE, arXiv: 2004.05523v1, 2020.

[7] Deng W, Hu J, Lu J, et al. Transform-Invariant PCA: A unified approach to fully automatic face alignment, representationand recognition [J]. IEEE TransonPattern Analysis and Machine Intelligence, 2014, 36 (6): 1275-1284.

[8] Gatouillat, A., Badr, Y., Massot, B., Sejdić, E.: Internet of medical things: a review of recent contributions dealing with cyber-physical systems in medicine. IEEE Internet Things J. 5(5), 3810–3822 (2018)

[9] Hazra, T.K., Chowdhury, S.R., Chakraborty, A.K.: Encrypted image retrieval system: a machine learning approach, January 31, 2019, Digital Object Identifier, https://doi.org/10.1109/ACCESS.2019.2894673

[10] J. Fei and Y. Chen, "Fuzzy double hidden layer recurrent neural terminal sliding mode control of single-phase active power filter," IEEE Transactions on Fuzzy Systems, vol. 29, no. 10, pp. 3067–3081, 2020.

[11] Koutras, D.; Stergiopoulos, G.; Dasaklis, T.; Kotzanikolaou, P.; Glynos, D.; Douligeris, C. Security in IoMT Communications: A Survey. Sensors 2020, 20, 4828.

[12] Manikandana, V.M., Masilamania, V.: Reversible data hiding scheme during encryption using machine learning, Procedia Computer Science Volume 133, 2018, Pages 348-356.

[13] Revanna, C.R., Keshavamurthy, C.: A novel priority based document image encryption with mixed chaotic systems using machine learning approach. FactaUnivSer Electron Energetics 32(1), 147–177 (2019).

[14] S. R. Maniyath and V. Tanikaiselvan, "An efficient image encryption using deep neural network and chaotic map," Microprocessors and Microsystems, vol. 77, Article ID 103134, 2020.

[15] Tang, F., Wu, E., Liu, J., Wang, H., Xian, M.: Privacy preserving distributed deep learning via homomorphic re-encryption. e Creative Commons Attribution (CC BY) license. https://creativecommons.org/licenses/by/4.0/, Electronics 2019, 8(4), 411, https://doi.org/10.3390/electronics8040411, 9 April 2019.

[16] Tanwar V.K, B. Raman, A. S. Rajput, and R. Bhargava, "SecureDL: a privacy preserving deep learning model for image recognition over cloud," 2021.

[17] Tortorella, G.L.; Saurin, T.A.; Fogliatto, F.S.; Rosa, V.M.; Tonetto, L.M.; Magrabi, F. Impacts of Healthcare 4.0 Digital Technologies on the Resilience of Hospitals. Technol. Forecast. Soc. Change 2021, 166, 120666.

[18] P. G. Mante, H. R. Oswal, D. Swain, and D. Deshpande, "A symmetrical encryption technique for text encryption using randomized matrix based key generation," Advances in Data Science and Management, Springer, Singapore, pp. 137–148, 2020.

[19] Y. Zhang, "The fast image encryption algorithm based on lifting scheme and chaos," Information Sciences, vol. 520, pp. 177–194, 2020.

[20] Y. Ding, "DeepEDN: a deep learning-based image encryption and decryption network for internet of medical things," IEEE Internet of INGS Journal, vol. 8, no. 3, pp. 1504–1518, 2020.

[21] Y. Wu, L. Zhang, T. Qian, X. Liu, and Q. Xie, "Contentadaptive image encryption with partial unwinding decomposition," Signal Processing, vol. 181, Article ID 107911, 2021.

[22] Y. Liu, S. Liu, Y. Wang, H. Zhao, and S. Liu, "Video steganography: a review," Neurocomputing, vol. 335, pp. 238–250, 2019.BIOGRAPHIES OF AUTHORS

	V.jayabharathi was born in Erode, Tamil Nadu (TN), India, in 1990. She received the Bachelor of Computer Science (B.Sc.) degree from the Bharathiar University, Erode, TN, India, in 2010 and the Master of Computer Applications (M.C.A.) degree from the University of Madras, Chennai, TN, India, in 2013. She also recieved the M.Phil degree from the Bharathiar University, Coimbatore, in 2014. She is pursuing Ph.D degree in computer science at Bharathiar University.His research interests include Cryptography.
	**Dr. S. Sukumaran** graduated in 1985 with a degree in Science. He obtained his Master Degree in Science and M.Phil in Computer Science from the Bharathiar University. He received the Ph.D degree in Computer Science from the Bharathiar University. He has 35 years of teaching experience starting from Lecturer to Associate Professor. At present he is working as Associate Professor of Computer Science in Erode Arts and Science College, Erode, Tamilnadu. He has guided for more than 55 M.Phil research Scholars in various fields and guided 13 Ph.D Scholars. Currently he is Guiding 3 M.Phil Scholars and 6 Ph.D Scholars. He is member of Board studies of various Autonomous Colleges and Universities. He published around 80 research papers in national and international journals and conferences. His current research interests include Image processing, Network Security and Data Mining.