Neurocomputing 612 (2025) 128714

Contents lists available at ScienceDirect

Neurocomputing

journal homepage: www.elsevier.com/locate/neucom

Survey paper

Deep learning-based image encryption techniques: Fundamentals, current trends, challenges and future directions

Om Prakash Singh [a], Kedar Nath Singh [b], Amit Kumar Singh [c,*], Amrit Kumar Agrawal [d]

[a] Deptt. of CSE, IIIT Bhagalpur, Bihar, India
[b] Deptt. of CSE & IT, JIIT Noida, U P, India
[c] Deptt. of CSE, NIT Patna, Bihar, India
[d] Deptt. of CSE, School of Engineering and Technology, Sharda University, Greater Noida, U P, India

ARTICLE INFO

Communicated by X. Wang

Keywords:
Encryption
Deep learning
Security
Healthcare
Machine learning

ABSTRACT

In recent years, the number of digital images has grown exponentially because of the widespread use of fast internet and smart devices. The integrity authentication of these images is a major concern for the research community. So, the encryption schemes that are commonly used to protect these images are an important subject for many potential applications. This paper presents a comprehensive survey of recent image encryption techniques using deep learning models. First, we explain the reasons that image encryption using deep learning models is beneficial to researchers and the public. Second, we discuss various state-of-art encryption techniques using deep learning models and offer technical summaries of popular techniques. Third, we provide a comparative analysis of our survey and existing state-of-the-art surveys. Finally, by investigating existing deep learning-based encryption, we identify several important research challenges and possible solutions including standard security metrics. To the best of our knowledge, we are the first researchers to do a detailed survey of deep learning-based image encryption for digital images.

1. Introduction

Because of fast-growing internet technology, digital images are the most common type of multimedia used for communications and entertainment [1]. People greatly enjoy the convenience of using digital images, which enable them to quickly understand and absorb information without having to read large amounts of text or process complex explanations [2]. Moreover, human beings have a very strong ability to process and memorize visual information, which can help them remember things better. Researchers are currently adopting generative AI and the ChatGPT model for text-to-image generation for various purposes such as education, research and entertainment. According to a report about AI image statistics that was published in 2023 [3], people generate more than 34 million images per day with the help of the DALL-E 2 system, which OpenAI built. The report noted that more than 4.76 billion people worldwide, or 60% of the global population, use the social media platform [4]. Digital images are vulnerable to attacks during their transmission and storage. This poses a significant challenge in protecting image privacy against leakage [5]. This leakage seriously affects the use of digital images, especially in sensitive application scenarios such as healthcare, digital forensics and facial recognition [6–8]. Image encryption is regarded as an important line of defence for privacy protection [9]. It transforms meaningful images into noisy images, making it difficult for unauthorized users to decipher the original content. As depicted in Fig. 1, some of the important applications of image encryption are healthcare social media, digital forensics, remote sensing, e-governance, military etc. [10–15].

Over the years, numerous image encryption methods [16–18] have been developed, each with merits and limitations. In general, there are two types of encryptions: symmetric and asymmetric encryption. In symmetric, user employed the $Enc()$ to transform the plain image $Plain_{img}$ into cipher image $Ciph_{img}$, and then $Dec()$ is utilized to recover the plain image using the secret key. If secret key ($Key_1 = Key_2$) is similar for both encryption and decryption purpose, then it is known as symmetric encryption. Otherwise, it is known as asymmetric encryption [19]. The computation of encryption and decryption process is described in the below Eq. (1) and Eq. (2) respectively.

$$Ciph_{img} = Enc(Plain_{img}, Key_1) \tag{1}$$

$$Plain_{img} = Dec(Ciph_{img}, Key_2) \tag{2}$$

Where, $Enc()$ and $Dec()$ are denoted as encryption and decryption function. Furthermore, the comparative analysis of symmetric and

* Corresponding author.
E-mail addresses: omprakash7667@gmail.com (O.P. Singh), knsinghait@gmail.com (K.N. Singh), amit.singh@nitp.ac.in (A.K. Singh), agrawal.amrit4@gmail.com (A.K. Agrawal).

https://doi.org/10.1016/j.neucom.2024.128714
Received 31 January 2024; Received in revised form 5 July 2024; Accepted 3 October 2024
Available online 9 October 2024

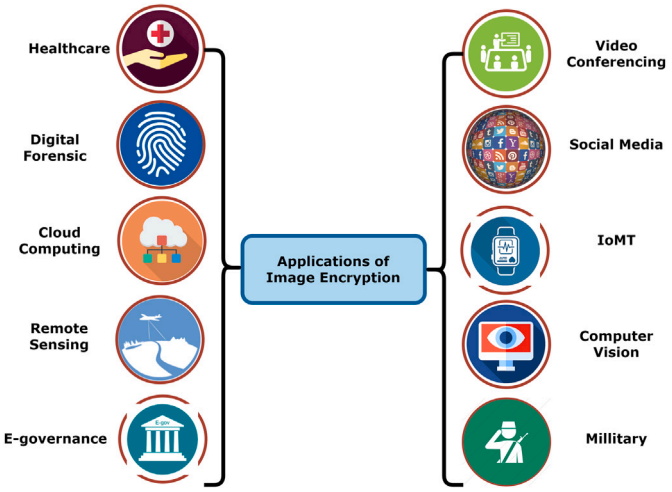

Fig. 1. Applications of image encryption.

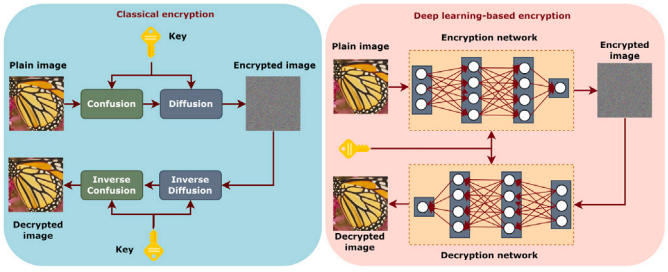

Fig. 2. Graphical representation of classical vs deep learning-based encryption.

Table 1
Comparative analysis of symmetric and asymmetric encryption.

Key points	Symmetric	Asymmetric
Key used for encryption and decryption purpose	Similar key	Different key
Distribution of secret key	Mandatory	Not required
Computational cost	Low	High
Speed	Fast	Slow
Key distribution	Easy	Difficult
Types	DES, AES	RSA, DSA, Diffie Hellman
Application	Healthcare	Multimedia
Robustness	Low	High

asymmetric based encryption is described in Table 1 in terms of merits, limitations, application, and computational cost. The graphical representation of classical vs deep learning-based encryption is listed in Fig. 2.

The key indexes of traditional encryption performance, security and cost are contradictory and are affected by factors including algorithms, key sizes, operational mode and implementations. And secret key distribution is a difficult task in symmetric encryption. However, asymmetric encryption is not ideal for real time-based applications due to high computational cost for encryption purposes. In contrast to traditional encryption methods, deep learning-based encryption is a promising means of addressing authenticity challenges [20]. It uses deep learning models for encryption and decryption, which offer better resistance and high security [21]. Deep learning models are used to enhance the quality of decrypted images and play other roles in the encryption process including key generation, encryption and decryption. Fig. 3 lists some of these roles.

Most researchers employ the deep learning framework at various stages of the encryption process for purposes such as feature extraction,

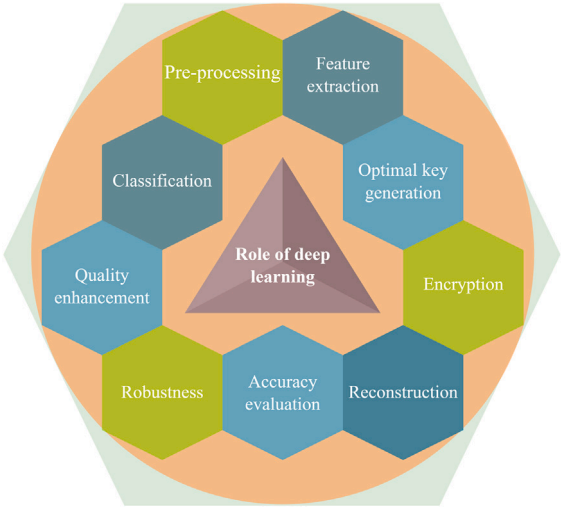

Fig. 3. Role of deep learning model in encryption.

classification, accuracy determination, optimal key generation and encryption. The researchers also use them for pre-processing, improving robustness against attacks, enhancing the quality of decrypted images and reconstructing decrypted images. Encryption in deep learning environments must meet three key criteria. First, the encryption algorithm must be secure against several kinds of attacks. Second, the secret key must be sufficiently large. Third, the encryption process must be low cost, ensure high accuracy and maintain content integrity. This comprehensive survey addresses these requirements, explains why image encryption is important, provides background information and describes recent applications. It presents several noteworthy encryption methods based on the deep learning model and provides a comparative analysis of the objectives, methodology, performance metrics and roles of different types of deep learning models in encryption strategies. A comparison with existing state-of-the-art surveys indicates that our survey offers richer technical details about deep learning-based encryption for images. Also, we identify important research challenges and possible solutions, including standard security metrics that will help researchers develop new encryption methods in deep learning environments. In recent years, surveys have used classical [20–26] and deep learning models [27–33] to provide information about encrypting and decrypting images.

Table 2 represents a comparative analysis of our survey and existing state-of-the-art survey papers. As this table indicates, a survey by Hosny et al. [20] discussed how various encryption techniques use spatial and transform domain features to preserve multimedia contents' privacy. A survey by other authors [21] provided a comprehensive review of chaotic systems and highlighted the key challenges that chaotic-based encryption techniques pose. Similarly, a survey by Zia et al. [22] focused on various chaotic map-based encryption techniques that are used to make digital images secure.

A survey by Priyanka and Singh [23] presented a detailed comparative analysis of various encryption techniques for protecting the security of medical images. It used various performance metrics to measure the effectiveness of the different encryption methods. Singh and Singh [24] did a survey on joint compression and encryption techniques for protecting the privacy of digital images. They examined each encryption technique's advantages and limitations and addressed problematic issues related to the techniques. Another paper [25] reviewed metaheuristic-based encryption techniques for ensuring digital images' authenticity and security. The paper offered a detailed analysis of the performance measures used to assess metaheuristic-based encryption methods and addressed various issues related to those methods. The authors of another survey paper [26] discussed encryption techniques

for colour images. Their work presented security and performance analyses of these techniques in tabular form.

Lata and Cenkeramaddi [27] surveyed various cryptographic techniques that keep medical images secure by using the deep learning model for denoising and enhancement as well as other applications such as classification, key generation and object detection. Their paper also focused on the limitations and future direction of encryption techniques based on the deep learning model. Similarly, other authors presented a discussion of efficient encryption techniques for digital images in a deep learning environment [28]. That survey also presented a comparative performance analysis of the deep learning model in tabular form. Kiya et al. [29] examined various learnable encryption techniques for colour images that use the deep learning model. Their study also analysed the encryption techniques' security and robustness against noise. Meraouche et al. [30] presented a survey that offered performance and security analyses of various neural network-based encryption techniques. Bao and Xue [31] did a paper on encryption techniques for keeping digital images secure by using a deep learning framework. The paper included a performance analysis of the deep learning model in encryption methods for applications such as compression, object detection, classification and key generation. The authors of [18] examined only a few encryption techniques based on machine and deep learning models. In this survey, a detail discussion on statistical, performance metric, challenges and their possible solutions are inadequate. Another work by different authors [32] comprehensively surveyed cryptography techniques that use computational intelligence to protect digital images' security. It presented a performance analysis of encryption techniques in tabular form. Another survey [33] investigated various cryptography techniques that use machine learning to keep digital content secure. This paper also discussed present and future issues related to the use of the machine learning model in encryption techniques.

Our survey aims to systematically discuss, summarize, and organize the recent trends of digital image encryption techniques using deep learning models. Our comprehensive survey's key contribution is described below:

- Our study explore the promising background knowledge of deep learning based image encryption along recent applications, evaluation metric, possible attacks, current limitations and notable suggestions
- Our survey highlights the key role of the deep learning model at different stages of encryption on the sender's side, during transmission and on the receiver's side.
- By highlighting recent challenges and opportunities, we hope to empower researchers and practitioners develop new encryption methods based on the deep learning model.
- The comparison of our survey with existing surveys in different technical prospective is provided in Tables 2 and 3.

The rest of the article is arranged as follows: Section 2 discusses performance evaluation criteria; Section 3 presents the comprehensive literature of deep learning-based encryption algorithms; Section 4 discusses the challenges and potential solutions to deep learning-based encryption; and Section 5 concludes the article. The complete road map of this comprehensive survey is highlighted in Fig. 4.

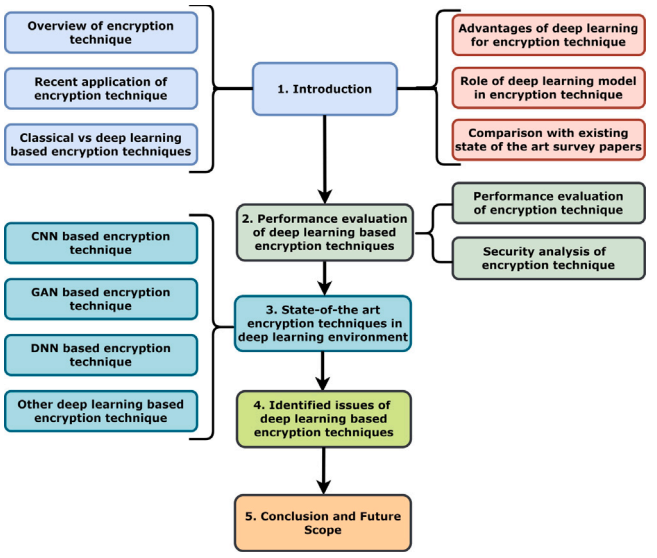

Fig. 4. Roadmap of this survey.

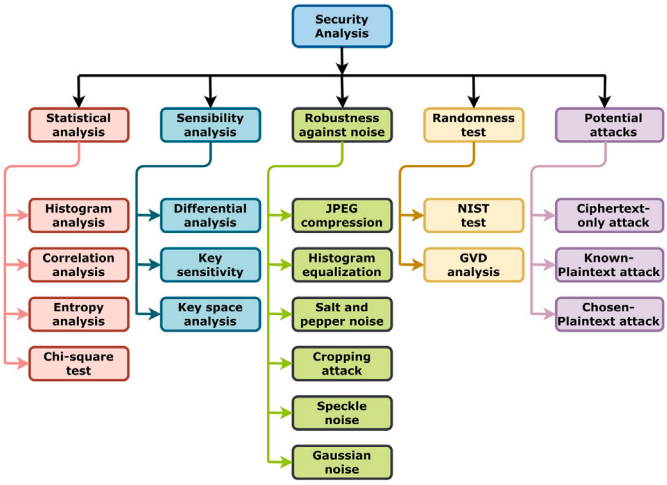

Fig. 5. Security analysis of encryption scheme.

2. Performance evaluation of encryption technique

In this section, security analysis of encryption schemes introduced, particularly for digital images. It is necessary to measure the effectiveness of encryption technique in terms of statistical, differential, robustness against noise, randomness test, and potential attacks. The detailed security analysis of encryption technique is listed in Fig. 5.

The histogram, correlation coefficient (CC), and chi-square test analysis are evaluated to identify adjacent pixels in cipher image to claim the robustness performance of encryption technique against the statistical attacks [34]. The differential analysis is utilized to examine the strength and diffusion performance in the encryption method [35]. It used to measure the strength of encryption technique, while change single pixel in the original image. The number of pixel change rate (NPCR) and unified average changing intensity (UACI) are two standard metrics to examine the robustness against the differential attacks [35]. The key sensitivity and key space analysis are evaluated to identify the robustness against the brute-force attacks [36]. The larger key size of encryption technique provides the randomness, and also offers the better robustness against the brute-force attacks. The ideal encryption method should be resisting against the various type of noise. Hence, the standard performance metrics such as peak signal to noise-ratio (PSNR), structural similarity index (SSIM), mean-squared error (MSE), and normalized correlation (NC) are utilized to measure the robustness performance against the noise [37,38]. The chaotic sequence generated through the chaotic map is measured the randomness performance through the national institute of standards and technology (NIST) test [39]. The entropy performance is evaluated to measure the randomness in the cipher image. It can be also utilized to provide the robustness against the cipher-text only attack. Some notable standard metric is used to measure the performance of encryption techniques are listed in Table 4.

Table 2
Comparative analysis existing state-of-the-art survey.

Ref	Year	Objective	Classification of survey	Total discussed methods	Type of content
[20]	2023	Secure the multimedia data using encryption schemes	Spatial, and transform domains	25	Digital Images
[21]	2023	Demonstrate the chaotic based image encryption	Chaotic system	57	Digital Images
[22]	2022	Introduce the chaotic-map based image encryption	Spatiotemporal, spatial, and transform domains	43	Digital images
[23]	2022	Discuss the encryption schemes for healthcare	Spatial domain	34	Medical images
[24]	2022	Study the encryption-and-compression scheme for digital image	CTE, ETC, SCE	35	Digital images
[25]	2020	Protect the digital images using encryption techniques	Meta-heuristic, spatial, and transform domain	49	Digital images
[26]	2019	Investigate the encryption method using computational schemes for colour image	Spatial, and transform domain	52	colour images
[27]	2023	Secure the medical image using deep learning model	Deep Learning	27	Medical images
[28]	2023	Introduce the efficient encryption scheme using deep learning	Deep Learning	13	Digital Images
[29]	2022	Demonstrate the colour image encryption using deep learning	Deep Learning	32	colour images
[30]	2021	Demonstrate the cryptography techniques using neural network	Artificial intelligence	12	Digital images
[31]	2021	Investigate encryption method to secure digital image using Deep Learning	Deep Learning	24	Digital images
[18]	2021	Introduce the encryption methods using machine and deep learning	Machine and deep learning	11	Digital images
[32]	2020	Introduce the encryption methods to secure the digital image using computational intelligence	Computational intelligence	24	Digital images
[33]	2019	Investigate the encryption method using machine learning	Machine Learning	16	Digital images
Our Survey		Secure the digital image using deep learning based encryption	Classical and deep Learning model	58	Digital images

Table 3
Statistical analysis existing survey on deep learning-based encryption.

Ref	Comparative analysis in tabular form	Deep Learning Models considered for surveys	Performance analysis	Statistics for popular images for encryption	Security analysis	Description of encryption performance metric	Existing challenges and research directions
[18]	×	✓	×	×	×	×	×
[27]	✓	✓	×	×	×	×	✓
[28]	✓	✓	✓	×	×	×	✓
[29]	×	✓	✓	×	×	×	×
[30]	✓	✓	×	×	×	×	×
[31]	✓	✓	✓	×	×	×	×
[32]	×	✓	✓	×	×	×	×
[33]	×	✓	×	×	×	×	✓
Our survey	✓	✓	✓	✓	✓	✓	✓

3. State-of-the-art encryption techniques in deep learning framework

Presently, deep learning models are widely used in many digital image applications such as segmentation, classification and image recognition [40], due to their excellent performances. In addition to conventional applications, this model is widely used for encryption [41]. Fig. 6 offers a schematic diagram of the deep learning-based encryption technique. As this figure indicates, the use of the deep learning framework results in optimal key generation (pseudo-random number sequences (PRNS)), and it ensures better security. An input image, and noise are fed into an encryption network to obtain a cipher image. After the cipher image is transmitted, the only people who can apply the decryption network to extract the original content are authorized users. They use the content for research, education, and entertainment purposes.

Currently, researchers employ deep learning models at different stages of image encryption [42,43]. This section offers a detailed analysis of recent work based on image encryption using convolutional neural network (CNN), the generative adversarial network (GAN), deep neural network (DNN) and other deep learning methods. The popular word cloud through keyword of literature survey paper is depicted in Fig. 7.

3.1. CNN-based image encryption

The CNN model is used primarily in encryption techniques for extracting features, optimizing the chaotic sequence, encrypting input images, reconstructing decrypted images and providing greater robustness against common attacks. What follows is a discussion of some popular CNN-based encryption techniques.

Raghuvanshi et al. [43] presented a encryption scheme for colour image using CNN architecture. In this work, they employ logistic map and CNN architecture to generate private and public key respectively for encryption purpose. This method offers high resistance against statistical and differential attacks. In similar direction, Bigdeli et al. [44]

Table 4
Performance metrics used in encryption techniques.

Metric	Description	Formula
MSE	It computes the average square error between the each pixel of two different images	$MSE = \frac{1}{A \times B} \sum_{i=1}^{A} \sum_{j=1}^{B} [O(i,j) - D(i,j)]^2$ Where $O(i,j)$ and $D(i,j)$ is denoted as pixel value of the plain and decrypted image, respectively. $A \times B$ is termed as size of image.
PSNR	It is used the measure the similarity between plain and decrypted image. PSNR value greater than 28 dB (Acceptable)	$PSNR = 10log_{10} \frac{R^2}{MSE}$ Where R indicates the maximum pixel intensity value in plain image.
Compression ratio (CR)	CR is the ratio of total number of bits in original and compressed data.	$CR = \frac{Size\ of\ Uncompressed\ bits}{Size\ of\ compressed\ bits}$
SSIM	It computes the similarity between two different images. SSIM values lie between [0, 1].	$SSIM = f(I(x,y)J(x,y)K(x,y))$ where, $I(x,y) = (2\alpha_x\alpha_y + E_1)/(\alpha_x^2\alpha_y^2 + E_1)$; $J(x,y) = (2\beta_x\beta_y + E_2)/(\beta_x^2\beta_y^2 + E_2)$; $.K(x,y) = (\beta_{xy} + E_2)/(\beta_x\beta_y + E_2)$. Where, $I(x,y)$, $J(x,y)$ and $K(x,y)$ are termed as luminance, contrast, and structure functions. E_1, E_2, and E_3 are known as positive constant value.
NPCR and UACI	NPCR: It measures the rate of change of pixel value in the cipher image when one pixel is ultered in the plain image. UACI: It measures the average intensity change value between the two cipher images when corresponding images change by one pixel. The ideal value of NPCR and UACI for grayscale image is 0.9960, and 0.3340 respectively.	$NPCR = \frac{\sum_{a,b} O(a,b)}{A \times B}$; $UACI = \frac{\sum_{a,b} \lvert C(a,b) - C'(a,b) \rvert}{255 \times A \times B}$. where, $O(a,b) = \begin{cases} 0 & \text{if } C(a,b) = C'(a,b) \\ 1 & \text{if } C(a,b) \neq C'(a,b) \end{cases}$ Here, $C(a,b)$: cipher image, $C'(a,b)$: 1 bit changed in cipher image, and $A \times B$: is termed as size of image.
CC	It evaluates the diffusion quality of the encryption algorithm. The ideal value of CC is nearer to 0.	$R(a,b) = \frac{P(a,b)}{\sqrt{Q(a)} \cdot \sqrt{Q(b)}}$ where, $P(a,b) = \frac{\sum_{i=1}^{T}(a_i - A(a))(b_i - A(b))}{T}$; $Q(a) = \frac{1}{K} \sum_{i=1}^{T}(a_i - A(a))^2$; $Q(b) = \frac{1}{K} \sum_{i=1}^{T}(b_i - E(b))^2$. $P(a,b)$: Covariance of sample a, b. T : Number of pixel pairs (a_i, b_i). $Q(a)$, $Q(b)$: Standard deviations of a and b. $A(a)$: Average of p_i pixel values.
Information Entropy	It computes the randomness of encryption technique. The ideal entropy value of cipher image is close to 8.	$Entropy = -\sum_a (C(x_a) \times \log_2 C(x_a))$ Where, $C(x_a)$ is the probability of x_a
Key Analysis		It shows the impact of minor changes in the key on the decrypted image. Size of key ∞ Security. The size of key $\geq 2^{100}$, then it can resist against the brute force attacks.
Computational Time		The total time required for encrypt the image. Computational cost of encryption scheme must be low for real time based applications.
Histogram Analysis		Histogram of cipher image is distributed in uniform manner. Hence, nobody can extract the information about that image. It also measure the quality of encryption techniques.

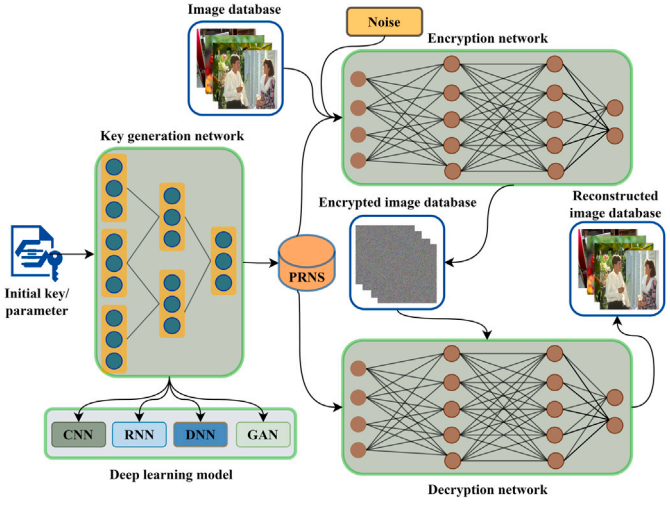

Fig. 6. Schematic diagram of deep learning based encryption technique.

Fig. 7. World cloud obtained through keyword of literature survey paper.

introduced a CNN-based encryption scheme for covert communications. In this work, selected component of plain image was given input into a CNN model, which produced a cipher image with the help of an activation function. A chaotic tent map was used as an activation function to maintain the relationship between the plain image and the cipher image. This scheme was robust against brute-force attacks. The authors did not do a security analysis of this encryption technique. In another work [45], the authors proposed a fractional-order discrete chaotic neural network (FODCNN)-based encryption approach for colour images. In this approach, SHA-256 is used to obtain a secret key from a plain image. Then, a FODCNN is used to generate a random sequence, which can scramble the pixel values in each component of a plain image. After that, deoxyribonucleic acid (DNA) encoding rules are used for diffusion purposes.

Ratnavelu et al. [46] proposed a fuzzy cellular neural network (FCNN)-based encryption framework for colour images. This process would apply FCNN to a chaotic system to generate a chaotic key sequence for encryption. The process would be highly resistant to brute-force attacks because of its large key space. In [47], Chen et al. combined deep learning and a 2D sin-linear-cos (SLC) hyper-chaotic map to develop a meaningful encryption scheme for grayscale and colour images. In the pre-processing stage of this scheme, a CNN model is used to compress plain images to ensure their high-quality

Table 5
Comparative analysis of CNN-based image encryption.

Ref	Objectives	Techniques and deep learning models	Role of deep learning	Datasets	Remarks
[43]	Secure the colour image using CNN architecture	CNN, logistic map, DNA encoding	Generate of secret key	-	It satisfies NIST test. It offers high resistance against various attacks.
[44]	CNN based encryption scheme for covert communication	CNN, Chaotic tent map	Generate of chaotic sequence for encryption	SIPI	Resist against brute force attacks
[45]	FODCNN based encryption approach for colour image	FODCNN, SHA-256, DNA	Scrambles pixel value of plain image	–	Secure and more robustness against occlusion attack
[46]	Increase the robustness against brute force attacks using FCNN	FCNN, chaotic system	Generate the chaotic sequence	UCID	It satisfies NIST test. It offers better resistance against various attacks.
[47]	Secure encryption scheme for both colour and grayscale image	CNN, 2D-SLC map, LSB, compression-reconstruction network	Compress the plain image to ensure better reconstruction	set11, set5	It passes the NIST test. It resist against plain text, cipher text attacks also.
[48]	Increase the robustness of encryption scheme using deep CNN model	Deep-CNN, FrFT, image scrambling	Improve the resolution of the decrypted image	–	It delivers better robustness against the listed attacks. However, security analysis is missing.
[49]	Secure the grayscale image using CNN model	Deep-CNN, Logistic map, XOR operation	Reconstruct the decrypted image	STL-10	Better accuracy for detect the cancer disease.
[50]	Discuss the encryption method for disease detection	CNN, DWT, CLMM, Substitution box	Feature extraction and classification	CIFAR-10, Caltech Faces	Security analysis is missing in this work
[51]	To secure transmission of multimedia data	CNN, 5D chaotic map	Generate the chaotic sequence	SIPI	The computational complexity is less. Robust against various attacks.
[52]	Feature extraction based encryption scheme	CNN, RS code, XOR operation	Feature extraction, key generation	CASIA iris image	It did not measure the differential, key sensitivity, and robustness analysis
[53]	Secure the multiple image using CNN and CS	CNN, CS, logistic map	Reconstruct the decrypted image	–	It did not evaluate the differential, entropy, computational time analysis
[54]	Secure the colour image using CNN and DNA	CNN, DNA encoding	Generate the chaotic sequence	–	It offers better resistance against statistical, and brute force attacks.
[55]	Secure digital image using Deep-CNN	CNN, chaotic log map, DNA encoding	Key generation	SIPI	It provides the better security.
[56]	Secure the CT image using CNN based encryption approach	CNN, CMT, 2D-SLMM, and TLT map	Control the initial parameter of chaotic sequence	FERET	It offers better resistance differential, statistical attacks due to robust key
[57]	Secure the Chest X-ray image using CNN based encryption scheme	CNN, Paillier encryption	Classification purpose	COVID-19	It did not evaluate the security analysis of encryption technique
[58]	Secure digital image using deep learning model	CNN, U-net, 5D hyper chaotic map	Reconstruct the secret cipher image	–	It generates the robust key using 5D hyper chaotic system, which ensure the better security

reconstruction. A hyper-chaotic map is used to encrypt compressed images to improve their security. This process passes the randomness test, which also enhances security.

Chen et al. [48] introduced a deep CNN-based encryption model that aims for enhanced robustness against attacks. In this work, the authors scrambled the input image, and fractional fourier transform (FRFT) transformed the scrambled image into an encoded image. To improve this method's robustness, a CNN model was used to enhance the reconstructed image's resolution. This method resists blur and occlusion attacks, too. The authors did not do a detailed security analysis of encryption method, though. Bai et al. [49] developed the encryption approach using a deep learning framework for reconstructing images. The approach the authors devised integrates a lorenz map, and chaotic map to generate the random sequence, which can improve the process's security. The authors adopted a CNN-based residual network to train and learn between the plain and cipher images. Their method can reconstruct original images with improved visual quality. These authors did not do a detailed security analysis of their encryption method. Rehman et al. [50] presented an encryption approach that uses a deep learning framework to preserve privacy. This approach deploys a cubic logistic chaotic map to obtain a random sequence. Discrete wavelet transform (DWT) decomposes a plain image, and the confusion process is used in a selected coefficient of DWT for encryption purposes. The CNN model can be adopted to predict cancer and is highly accurate (98.9%) in doing so. Man et al. [51] presented a double-image encryption scheme using CNN and a chaotic system to secure the transmission of multimedia data. The authors used the chaotic map to control the initial parameters of a 5D chaotic system, which enhance the proposed method's security. They used the chaotic sequence as a kernel of CNN to encrypt both images.

This method provides enhanced resistance against plaintext and chosen plaintext attacks. In another work, Li et al. [52] proposed a CNN-based encryption scheme for iris images. In the pre-processing stage, a normalization process is performed on iris image datasets. The iris image is extracted using a deep learning model, which is also used in the key generation process. Furthermore, the XOR operation is performed between a plain image's key matrix and pixel matrix to obtain an encrypted image. The authors of this work did not measure the effectiveness of the proposed method's security, differential or key sensitivity or analyse its robustness. Different authors introduced a multiple-image encryption [53] based on deep learning and compressed sensing (CS). They applied CS to compress the images up to eight times and used a logistic map to scramble the compressed images' pixel value. They used CNN to recover the decrypted images. This scheme was robust against attacks. A paper by Wang et al. [54] described a CNN-based encryption approach that secures colour images by using DNA rules. The authors transform the colour image into three matrices and then apply DNA encoding rules to convert the matrices into DNA matrices. A CNN model is used to generate a chaotic sequence that can be used to scramble the DNA matrix. Finally, this scheme's DNA decoding rule is used to obtain the cipher image. This process is highly resistant to statistical and brute-force attacks. Erkan et al. [55] presented a deep-CNN-based encryption approach for securing digital images. In their work, the authors used a chaotic log map to generate the chaotic sequence. They obtained the final key by performing the XOR operation between the initial secret key and the random key, which is obtained from a VGG-16 of deep CNN. They used a permutation and diffusion process to generate the cipher image using DNA rules. Their scheme was highly robust against various types of attacks. Abdellatef et al. [56] introduced a CNN-based encryption framework to protect the privacy of computer tomography (CT) images, which can be used to diagnose COVID-19. The authors employed CNN architecture to extract the features from patients' facial images and then used the extracted features to control the initial parameter of a two-dimensional sine logistic modulation map and a tent logistic tent map. They used Chaotic Magic Transform and two chaotic sequences to obtain the cipher images. This process was highly secure and resistant to attacks. To provide privacy protection for chest X-rays, Boulila et al. [57] devised an encryption process using a deep learning framework. They encrypted a COVID-19 dataset using the Paillier encryption scheme and input the

Table 6
Performance analysis of CNN-based image encryption.

Ref	NPCR	UACI	PSNR	SSIM	Entropy	Accuracy	Computational time		Correlation coefficient		
							Enc.	Dec.	H	V	D
[43]	99.76	33.36	–	–	7.9996	96.00	–	–	0.0011	0.0011	0.0003
[44]	–	–	–	–	7.9972	–	12.06	11.85	0.0012	0.00183	0.0011
[45]	99.60	33.41	–	–	7.9893	–	–	–	0.0001	0.0091	−0.0023
[46]	99.95	33.34	85.49	0.9699	7.9940	–	–	–	−0.0407	−0.0239	0.0345
[47]	98.45	33.74	40.9292	0.9976	–	–	0.35	–	−0.0055	−0.0396	0.0034
[48]	–	–	28.18	0.8885	–	–	–	–	–	–	–
[49]	–	–	35.42	1.000	–	–	–	–	–	–	–
[50]	–	–	–	–	7.9920	98.92	–	–	–	–	–
[51]	99.61	33.45	9.6351	–	7.9870	–	0.2346	–	0.0015	−0.0034	0.0007
[52]	–	–	–	–	–	–	–	–	–	–	–
[53]	–	–	32.95	0.8661	–	–	–	–	−0.0019	0.0474	−0.0068
[54]	99.45	33.28	–	–	7.9914	–	–	–	−0.0219	0.0326	−0.0098
[55]	99.60	33.46	21.37	–	7.9994	–	0.4146	0.3662	−0.0029	0.0021	0.0003
[56]	99.45	34.48	–	0.900	7.9993	–	–	–	0.005	0.009	0.006
[57]	–	–	–	–	–	93.20	–	–	–	–	–
[58]	99.56	–	40.23	0.9989	7.9884	–	–	–	−0.0034	−0.0027	0.0065

results in CNN architecture to train the datasets in a secure manner. A trained deep learning model can easily classify different types of encrypted images. Their process was highly accurate in determining different classes of COVID-19 datasets. The authors did not do a security analysis of the encryption scheme.

Himthani et al. [58] used 5D chaotic map-based image encryption in a deep learning environment. They deployed the 5D chaotic system to generate the random key sequence for encryption purposes, which enhanced its security. They hid the cipher images inside multimedia objects using a U-Net framework and reconstructed the secret images with CNN architecture. Their scheme produced high-quality images. The authors did not assess he process's robustness against various types of attacks.

The comparative analysis of CNN-based encryption techniques are listed in tabular form, and it is listed in Table 5. Further, the performance analysis of CNN-based encryption is also listed in Table 6.

3.2. GAN based image encryption

GAN [59], which is one of the most popular deep learning algorithms is used in various types of image processing such as hiding data and denoising, encrypting and enhancing images [60–63]. Because of its generative and discriminative features, GAN's architecture is used in encryption techniques for secret key generation and decrypted-image reconstruction and verification and increases the encryption system's robustness [64]. For example, Singh et al. [65] devised a scheme that used GAN and a customized super resolution network (CSRNet). They adopted GAN to generate the random sequence number, which they used for encryption purpose. They integrated cross-coupled logistics and a henon map to encrypt plain images into cipher images by using a secret key. They compressed the cipher image using down sampling to save bandwidth and minimize the use of storage. They applied the CSRNet on the extraction side to improve the decrypted image's visual quality. Their process takes very little time to encrypt, so it is suitable for real-time applications.

Ding et al. [66] wrote a paper that presented a deep learning based encryption and decryption network (DLEDNet) framework for internet of medical things (IoMT) applications. Their process used GAN to learn the network architecture for encryption purpose. They deployed a neural network to generate a robust key, which enhances the security. They employed reconstruction architecture to transform encrypted images into plain images. Adversaries and attackers would be unable to extract the decrypted images even if they knew about this process's hidden factors and network architecture. Dev Singh et al. [67] came up with another GAN-based encryption approach, which aims be highly secure and resistant to attacks. The authors used GAN to generate the secret key, which can produce high randomness. They passed input images through three stages (substitution, permutation and diffusion) to obtain cipher images. Because of its large key space, their scheme was highly resistant to occlusion, geometric and brute-force attacks.

Fang et al. [68] combined a hyper-chaotic system and GAN to secure multimedia content against attackers and adversaries. They improved the chaotic system's initial parameter by using the hyper-chaotic system and thereby enhanced this method's security. They used GAN and a chaotic sequence model to encrypt plain images. Their scheme had a large key space, which made it resistant to well-known types of attacks. Bao et al. [69] wrote about an asymmetric encryption approach for colour images that deployed an autoencoder and cycle-consistent adversarial networks (CycleGAN) to secure multimedia content. It used the autoencoder–decoder network to scramble plain images and employed CycleGAN to generate the public and private key for encoding and decoding purposes. This scheme did a good job of protecting the reconstructed images against well-known types of attacks. The authors did not examine the process's computational cost. Man et al. [70] devised the least squares GAN (LSGAN)-based encryption technique, which generated a random key for encryption purposes. The authors used six different chaotic systems to generate a pseudorandom sequence then, they used the LSGAN to tune the sequence and generate the random chaotic key sequence, which satisfied the randomness test. They used the random chaotic key to scramble the plain images, which enhances the process's security and made it resistant to common types of attacks. Ding et al. [71] introduced an encryption scheme for medical images that used a deep learning model. In their work, the authors used GAN to obtain a robust secret key for encryption and decryption. Thanks to the large key space obtained by using GAN, their scheme was secure from attacks. The authors did not do a randomness test and computational cost analysis on their scheme.

Panwar et al. [72] came up with a GAN-based encryption system that secure the multimedia information when it was transmitted over insecure media. They applied a stochastic gradient descent for training the dataset, which optimized the model. They used the loss function of the proposed network architecture to reconstruct the decrypted images and enhance their visual quality. And they deployed GAN architecture to obtain their scheme's secret key. Their encryption system was highly resistant to plaintext attacks. Fang et al. [73] combined a hyper-chaotic system and a deep convolutional GAN (DCGAN) to keep multimedia content secure from brute-force and plaintext attacks. The authors used plain images to obtain the chaotic system's initial parameter and then deployed a hyper-chaotic system to enhance the additional their process's security. They used the DCGAN model to generate the

pseudorandom sequence and obtained the cipher images with the help of the chaotic key matrix. This scheme had a large key space, which made it highly resistant to attacks. Sirichotedumrong and Kiya [74] used a deep learning environment to create an encryption method with enhanced robustness against ciphertext attacks. They deployed a DNN model and a canadian institute for advanced research (CIFR-10 dataset) for training and testing purposes, which resulted in better classification. They employed residual network (ResNet-18) architecture to determine accuracy and applied the GAN model to obtain cipher images with acceptable visual quality. The authors did not analyse the effectiveness of their scheme's security. Authors examined a study that focused on the use of GAN-based encryption in a cloud environment to keep medical information secure [75]. The study's authors used deep GAN to perform a key generation process and obtain a large key space, which ensured better randomness. They used a robust secret key to perform a permutation and diffusion procedure and obtain the cipher images. They used a blockchain framework to enhance the cipher images' security and provide authenticity. The study did not include a robustness analysis. Mulkiah et al. [76] presented a GAN-based encryption framework for securing the digital images in the encryption-then-compression (ETC) domain. The authors used the GAN model to compress the plain images and deployed the logistic map for encryption to improve security and save bandwidth. They did not do a security analysis of their proposed method but it is noticed did that its computational cost is prohibitively high.

The authors of [77] devised a scheme that used the GAN model to keep medical images secure. They used a U-Net model to extract the region of interest (RoI) portions of plain images and then input the RoI portions' seed value into the GAN model to generate the secret key. They used the secret key to encrypt the images, thereby making them more secure from listed attacks. Their scheme passed the NIST test, which ensured the better randomness. Tables 7 and 8 contains the summary of popular GAN-based encryption and performance analysis, respectively.

3.3. DNN based image encryption

A deep learning framework can be used to take a large dataset as input and extract its relevant features to improve a proposed model's accuracy [78]. In this subsection, we focus on various DNN-based encryption schemes that keep image content secure. To enhance the encryption system's security performance, Maniyath and Thanikaiselvan [79] employed a deep learning framework to compute the random secret keys. Then, they used the diffusion approach in an XOR operation. Their scheme had very little resistance to attacks because it used a traditional diffusion approach for image encryption. Man et al. [80] developed an encryption method that used a bidirectional activation deep neural network (BADNN) model and a 5D chaotic system to secure cloud data. They applied the 5D chaotic system to generate the initial chaotic sequence and then used the BADNN model to generate the random key sequence for encryption. They obtained the cipher images by using the permutation process. This method was highly resistant to against plaintext attacks. In another study, Huang et al. [81] introduced the use of deep learning architecture for medical image encryption. They used RGB channels to transform the images. Then, they employed negative positive transformation on each channel's pixel value using the random key and applied the colour shuffling procedure to produce the encrypted images. This method had an F1 score of 93.66 using Xception, which ensures better results. The authors did not investigate the statistical, differential, key sensitivity, histogram or robustness analyses of their proposed technique. Similarly, the authors of another study [82] deployed encryption and a DNN model to preserve privacy. They used data augmentation process on a large dataset to train the DNN model. In the testing phase, they employed the deep residual network to classify plain and encrypted images. Their classifications were very accurate. Their proposed method was resistant to ciphertext attacks. The authors did not do a security analysis of their proposed scheme. Gao and Tian [83] introduced an encryption approach using deep learning for digital images. The authors used a sensitive logistic map and a henon map to generate a random chaotic sequence. The chaotic sequence served as input into the back propagation neural network, which produced the robust key. It was used to transform plain images into cipher image. The use of the robust key for encryption improved the process's resistance to most types of attacks. The authors did not do differential, statistical or robustness analyses to examine the effectiveness of their encryption approach. Rupa et al. [84] developed an encryption method that used a DNN model and a logistic map. They used a ResNet model to classify the fake multimedia data during the pre-processing stage. They deployed the logistic map to obtain random sequences during key generation and performed an XOR operation on two random sequences to obtain the secret key for encryption. They used the robust key to encrypt each channel of the colour images and then produced the encoded images. Their method secured medical data against cyberattacks.

Iqbal et al. [85] combined a chaotic system, DNA and a deep learning model to implement encryption techniques that keep digital information secure. The authors used the VGG-16 of a deep CNN model to generate the random key for encryption. They employed DNA encoding rules and the secret key to obtain the cipher images. Their scheme satisfied the randomness test, which means it was highly secure. Ito et al. [86] developed a DNN-based encryption framework that preserves privacy. They trained the image datasets by using a DNN model that transformed the plain images into cipher images. Their scheme used ResNet and VGG architecture to classify the network, with accuracy scores of 91.56 and 91.59, respectively for CIFAR-10 datasets. The authors did not do differential, statistical or robustness analyses of their encryption technique. Similarly, authors of [87] introduced a novel encryption approach for keeping digital images secure. They used a DNN model for training purposes to generate the cipher images. It determined the classification of plain and cipher images during testing. Their scheme was resistant to ciphertext attacks. The authors did not do a security analysis of the proposed method. A study by Lee et al. [88] devised a homomorphic-based encryption framework that used deep learning framework to secure the images. In this work, authors utilized a ResNet-20 model and plain images to train a CIFAR-10 dataset and then employed homomorphic encryption to obtain the cipher image. Further, they employed the ResNet-20 architecture of a DNN model to classify the network. Their accuracy score for CIFAR 10 datasets was 91.89. The authors did not do differential, statistical or robustness analyses of their encryption technique. Tables 9 and 10 contain the summary of popular DNN-based encryption and performance analysis, respectively.

3.4. Other deep learning based image encryption scheme

In this subsection, we will discuss other deep learning-based encryption schemes that are used to keep images secure. Singh et al. [89] devised one such scheme by integrating encryption and compression to keep multimedia data secure in a deep learning framework. The authors used a novel 3D chaotic map to generate the random key, which made the process more secure. They employed the confusion and diffusion procedures on the plain images to obtain the cipher images using the circular shift operation. Before transmitting the cipher images, the authors used down sampling concept to compress the cipher images, which reduced storage use and saved bandwidth. Finally, they used the concept of residual dense spatial network (RDSN) to reconstruct the decrypted images with better visual quality.

Similarly, Selvi et al. [90] used deep learning to create a novel encryption-compression scheme for healthcare. Their encryption process generated the cipher images with a signcryption scheme at a hidden layer. The authors employed an entropy encoding algorithm to compress the cipher images, which saved bandwidth and reduce

Table 7
Comparative analysis of GAN-based image encryption.

Ref.	Objectives	Techniques and deep learning models	Role of deep learning	Datasets	Remarks
[65]	Secure the multimedia data, using GAN	GAN, CSRNet, logistics, and henon map	Generate the random key sequence	COCO2017	It satisfies the NIST test, which ensure better randomness.
[66]	Develop a secure encryption framework using GAN for IoMT	GAN, ResNet-50, Pixel-level segmentation	Encryption purpose	Chest X-ray	Adversary could not extract decrypted image even they know hidden factor, architecture.
[67]	Introduce the DNN based encryption scheme for colour image	GAN, logistic map, Substitution box	Generate the secret key	SETs	Security analysis is missing.
[68]	Improve the resistance against well-known attacks using encryption approach	Hyper chaotic system, GAN	Encryption purpose	–	It satisfies the NIST test, which ensure better randomness.
[69]	Secure the colour image, using Cycle-GAN based encryption	Cycle-GAN, auto encoder	Scrambling purpose	Corel-1000	It did not evaluate computational cost of encryption scheme
[70]	Generate robust key for encryption purpose using LSGAN	LSGAN, Chaotic system	Robust key generation	–	This scheme achieves better security due to robust key generation using GAN
[71]	Secure the medical image using GAN based image encryption	GAN, Generator-Discriminator network	Robust key generation	Ultrasonic, chest Xray, BraTS18	It evaluate the security performance on three different medical datasets
[72]	Secure the transmitted data over insecure channel using GAN based encryption	GAN, SGD	Generation of secret key	skin cancer	Loss function of this architecture is utilized to enhance the visual quality of decrypted image.
[73]	Improve the resistance against brute force attack using encryption approach	Hyper chaotic system, DCGAN	Generation of secret key	–	It resist against the brute force and plain text attack, due to large key space.
[74]	To improve the robustness using GAN based encryption	VGG-13, GAN, ResNet-18	Encryption purpose	CIFAR-10, CIFAR-100	It offers better accuracy. However, it did not investigate the security analysis.
[75]	Secure the medical image using GAN based encryption	GAN, SHA-1, PRNG, Blockchain	Generation of secret key	BraTS18	Blockchain system is employed to enhance the additional security
[76]	Secure digital images using GAN in ETC domain	GAN, logistic map	Encryption purpose	–	The detailed security analysis is not investigated in this work
[77]	To secure the medical images using GAN and AES	GAN, AES, and U-net Model	Generation of secret key	Chest X-ray	It offers better randomness. However, the security analysis is missing.

Table 8
Performance analysis of GAN-based image encryption.

Ref	NPCR	UACI	PSNR	SSIM	Chi-square	Entropy	Computational time		Correlation coefficient		
							Enc.	Dec.	H	V	D
[65]	99.60	33.46	34.62	0.9068	256.88	7.9993	0.3772	0.3774	0.0007	0.0017	0.0018
[66]	–	–	35.0	0.930	–	7.9700	0.273	0.272	–	–	–
[67]	99.60	33.45	24.48	0.9915	–	–	–	–	−0.0001	0.0003	−0.0002
[68]	99.60	33.51	–	–	–	7.9902	22.706	–	0.0104	−0.0063	0.0127
[69]	99.42	13.84	26.81	0.9799	–	7.9770	–	–	0.0044	0.0172	0.0151
[70]	99.60	33.45	9.64	–	–	7.9975	0.9437	–	−0.0019	0.0474	−0.0068
[71]	99.56	20.87	–	0.9983	–	7.9807	–	–	0.0627	0.2557	0.0203
[72]	–	–	39.97	0.9972	–	7.4000	–	–	0.4812	0.4584	0.2169
[73]	99.69	33.42	–	–	213.24	7.8091	1.822	–	0.0003	0.0009	0.0019
[74]	–	–	–	0.9460	–	–	–	–	–	–	–
[75]	99.60	33.86	–	0.9720	–	7.980	0.2500	0.2500	–	–	–
[76]	99.70	36.48	30.75	0.9772	–	7.9957	1.8500	1.9200	–	–	–
[77]	99.59	–	–	–	–	7.9974	2.8600	–	–	–	–

Table 9
Comparative analysis of DNN-based image encryption.

Ref. No.	Objectives	Techniques and deep learning models	Role of deep learning	Datasets	Remarks
[79]	Secure the multimedia data, using DNN based encryption scheme	DNN, Auto-encoder, Chaotic map	Secret key generation	SIPI	Robustness analysis was not evaluated against the attacks
[80]	Secure the cloud data, using deep learning concept	5D chaotic system, BADNN	Chaotic key stream for encryption purpose	–	It resist against plain-text attacks only.
[81]	Introduce DNN based encryption scheme for colour image	DNN, negative-positive transformation	Classification purpose	MRI brain tumor, COVID19	It did not examine the security analysis of encryption scheme
[82]	Discuss the pixel based image encryption using DNN	DNN, colour shuffling, ResNet-18	Reconstruction of decrypted image	CIFAR-10	It offers better robustness against cipher-text attacks only.
[83]	Improve the security using DNN	BPNN, SLM, and Henon map	Generate robust key	SIBI	It did not examine the differential, statistical, and robustness analysis.
[84]	Secure the multimedia content using DNN based encryption scheme	DNN, ResNet model	Classification of fake image	PHIL	This scheme is applicable for image and video also.
[85]	Introduce DNA based hybrid encryption approach	DCNN, DNN, 5D chaotic system	Generation of secret key	–	It satisfies the randomness test, which ensure better security.
[86]	Privacy preserving based encryption approach using DNN	DNN, U-Net architecture, ResNet-20, VGG16	Encryption the plain image	CIFAR-10, CIFAR-100	It did not investigate security analysis
[87]	Privacy preserving using ResNet architecture	DNN, ResNet negative-positive transformation	Classification, and encryption purpose	CIFAR-10	It offers better robustness against cipher-text attacks only.
[88]	Image encryption using DNN, and homomorphic based encryption	DNN, ResNet-20, homomorphic encryption	Classification, and encryption purpose	CIFAR-10	It did not investigate security analysis

Table 10
Performance analysis of DNN-based image encryption.

Ref	NPCR	UACI	PSNR	SSIM	Entropy	Accuracy	Computational time		Correlation coefficient		
							Enc.	Dec.	H	V	D
[79]	99.87	33.61	Inf	0.0032	7.9854	–	0.420	–	−0.0064	0.0222	0.0163
[80]	99.60	33.45	7.11	–	7.9971	–	0.508	–	0.0024	0.0092	0.0007
[81]	–	–	–	–	–	–	–	–	–	–	–
[82]	–	–	–	–	–	86.99	–	–	–	–	–
[83]	–	–	–	–	–	–	–	–	–	–	–
[84]	99.98	33.57	–	–	7.890	88.83	8.33	–	–	–	–
[85]	99.60	33.40	31.86	–	7.997	–	–	–	−0.0136	−0.0121	0.0204
[86]	–	–	–	–	–	91.56	–	–	–	–	–
[87]	–	–	10.73	0.1732	–	92.97	–	–	–	–	–
[88]	–	–	–	–	–	91.89	–	–	–	–	–

storage use. The authors did not analyse their encryption scheme's security. In another work, Wang et al. [91] employed deep learning to keep multimedia images secure in the encryption-then-compression domain. The authors used the Modulo addition 256 rule to produce the cipher images. They deployed down sampling to compress those images before their transmission. This procedure reduced storage and saved bandwidth. They used RDSN on the receiver's side to reconstruct the decrypted images, which resulted in better visual quality. The outcomes this scheme indicated that its compression performance was very good. The authors did not analyse the scheme's security. Efficient encryption techniques are needed to secure traffic data from adversaries and attackers. To achieve this goal, Kumar and Dua [92] implemented an intelligent transport scheme based on a chaotic system and a gated recurrent unit (GRU). They used a sine-cosine map to generate the chaotic sequence, which they combined with an initial key to make a robust key for permutation. They employed a GRU to generate another intermediate key for diffusion. He et al. [93] integrated a two-dimensional coupled map lattice (2DCML) and a once forward long short-term memory structure (OF-LSTMS) to design a robust encryption scheme for digital images. They transformed the image into different blocks and then directly input each block's pixel value into the OF-LSTMS model during the encryption process by using a chaotic sequence obtained with a 2DCML. The outcomes of this scheme produced better performance than other chaotic-based encryption techniques. Zhu et al. [94] devised a federated deep learning-based encryption scheme for preserving privacy by using CNN for image classification. The authors used federated learning without involving trusted third parties for key generation and deployed secret sharing techniques for decryption. Their process required a considerable amount of time for training the database to handle classification work. The authors did not analyse their encryption technique's security. Feixiang et al. [95] implemented the chaotic restricted boltzmann machine (CRBM) method for colour images in a blockchain environment. The authors integrated two

chaotic maps (Henon and zigzag) to create a pseudorandom sequence, which enhance their scheme's security. They used a CRBM and three pseudorandom sequences to scramble the plain images' pixel value. Further, they employed a blockchain system is employed to enhance their scheme's security. Liu et al. [96] created another deep learning-based encryption method for colour images. The authors used the chen chaotic system to generate the initial chaotic sequence, which they used as input into a bidirectional long short-term memory (Bi-LSTM) model to obtain three chaotic sequences for encryption purpose. Their scheme was highly secure and resistant to a few types of attacks but not differential ones. Gupta and Vijay [97] implemented a compression-then-encryption (CTE) scheme using a stacked autoencoder (SAE) model to secure the transmission channel. The authors used the SAE framework to compress the plain images and created a secret key for encryption by deploying a logistic map. Their scheme produced high-quality reconstructed images, was robust and had a good compression ratio. However, the computational cost is very high. Pan et al. [98] came up with an ANN-based encryption scheme for financial systems. The authors integrate logistic, sine and tent maps to create a hybrid chaotic system, which gave their system better security against differential and statistical attacks. They employed ANN to obtain a random chaotic sequence for encryption. Their method was highly secure and resistant to most types of attacks.

Zhou et al. [99] devised an LSTM-based encryption method for colour images using a 4D hyper-chaotic lorenz system (HCLS). The authors developed a novel map for their system, which satisfied the randomness test. They employed HCLS to create the chaotic sequence, which they fine-tuned using an LSTM-based model for improving the security. Then, they used the novel chaotic sequence and performed the permutation process to produce the cipher image. Wang and Li [100] introduced the hopfield chaotic neural network (HCNN)-based encryption approach for colour images. The authors integrate the logistic and tent map to create the initial key sequence, and then scrambled the plain image using the Arnold transform. During the diffusion process, they employed the HCNN to obtain a chaotic key matrix. Finally, they used the chaotic key and performed an XOR operation on the scrambled images to create the cipher images. Their scheme passed the randomness test, which indicates that it was highly secure. The authors did not assess their scheme's visual quality assessment. Cheng et al. [101] wrote about an aggregate deep convolutional neural network (ADCNN) model that uses hashing and a DNA mechanism to protects users' privacy. The authors used ADCNN and VGG-16 model to extract features and then deployed principal component analysis (PCA) to reduce the dimensions. They integrated the hyper-chaotic system and DNA to secure the data. Their method is highly secure and resistant to a wide range of attacks. In their work, Sang et al. [102] introduced an autoencoder-based encryption framework to keep digital images secure. The authors used a logistic map to scramble the plain images and deployed an autoencoder to transform them into cipher images, which improved the randomness. Their method could resist a wide range of attacks and was highly secure. Singh et al. [103] implemented a deep learning framework for image encryption using hybrid chaotic map. In this work, authors employ the UNet3+ architecture to detect ROI part of medical image, and then it is encrypted using secret key which is obtained through hybrid chaotic map. This method is more robust and secure against the various attacks.

A deep learning-based encryption then compression method is introduced by Priyanka et al. [104] for healthcare system. First, author integrates three different chaotic map to generate the robust key for permutation purpose, which ensure the better security. Prior to disseminating encrypted image over transmission channel, it employs lossy compression on encrypted image to reduce storage overhead. Lastly, original image is recovered through the reconstruction network without losing the visual quality. In another study, Priyanka et al. [105] developed a joint encryption-then-compression framework for healthcare application. In this work, they employ the you only look once (YOLO)v7 model to detect ROI part of medical image, which offers the better security. Further, they perform the 3D chaotic map to obtain secret key for encryption purpose. Lastly, super resolution (SR) network is utilized at the receiver side to recover the ROI image for better diagnosis purpose. Wang and Lo et al. [106] presented a joint compression-then-encryption framework for colour image using autoencoder. First, they compress the original image using autoencoder, and then it is encrypted using logistic map, that provides the high resistance against statistical and differential, and robustness attack. Chai et al. [107] implemented an encryption methodology that secure the colour image using deep reconstruction network (DRN). In this work, they employ the sine chaotic map to generate secret key encryption purpose, which enhance additional security. Further, DRN architecture is employed at receiver side to extract the decrypted image, without losing the visual quality.

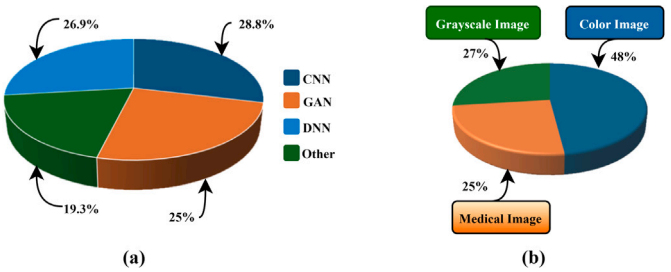

Fig. 8. (a): Popular deep learning model for image encryption (b): Encryption technique used in various application.

Tables 11 and 12 contain the summary of popular encryption techniques in deep learning environments and performance analysis, respectively.

4. Challenges and possible solution

Thanks to its strong learning ability and superior results, deep learning-based encryption is an effective method for protecting the privacy and security of digital content, especially images [108,109]. As our survey demonstrates, CNN and GAN-based encryption techniques are very popular. (See Fig. 8a.) Most deep learning-based encryptions are designed for colour and medical images. (See Fig. 8b.) Once image content is encrypted, it no longer contains meaningful information, and each image sounds almost identical until its decryption. These images are at risk of being intercepted by attackers after their decryption, which may lead to copyright violations and the misuse of the original content. In certain scenarios, larger key sizes are used for strong encryption, which increases the computational speed of the encryption and decryption processes. So, utilizing only encryption technique is an insufficient measure to provide a high level of security. Also, it is very difficult to address deep-learning models' security and privacy issues.

This survey identified some key issues and their potential solutions (Refer to Fig. 9) of deep-learning-based encryption technique are described as follows:

- Researchers employed the deep learning model for key generation purpose, which enhances the randomness performance. However, it increases the computational cost. Hence, computational cost can be reduced using the concept of parallel processing [110].
- It can be observed that robustness/security of images in deep learning model based encryption technique is not much sufficient. Hence, multiple security techniques [111,112] can be applied to enhance the media security.
- In general, researchers utilize the deep learning model for media protection. But the copyright protection of deep learning network is equally important. Hence, watermarking techniques [113] can be used to protect the copyright violation of the network.

Table 11
Comparative analysis of other deep learning-based image encryption.

Ref. No.	Objectives	Techniques and deep learning models	Role of deep learning model	Datasets	Remarks
[89]	Introduce the 3D chaotic map to secure colour image	3D Chaotic map, RDSN, Down sampling	Reconstruct the decrypted image	BSDS100, Urban100, Set15	Encryption time can be reduced.
[90]	Design encryption-compression scheme for healthcare system	Signcryption, entropy encoding algorithm	Encrypt the plain image	Chest X-ray-pneumonia	The security analysis of this scheme is missing.
[91]	Introduce DNN based encryption method for colour image	RDSN, Down sampling, Modulo addition 256	Reconstruct the decrypted image	BSDS100, Urban100, Set15	It did not evaluate the security analysis.
[92]	Secure transport images using GRU and chaotic encryption	sine-cosine map, GRU	Key generation for diffusion purpose	flickr website	Computational time of encryption scheme can be reduced.
[93]	Secure the multimedia content using LSTMS	OF-LSTMS, 2DCML	Encrypt the plain image	–	It delivers better robustness against the listed attacks.
[94]	Secure the multimedia content using DNN	GAN, DNN, LSTM, ResNet, Paillier system	key generation purpose	MNIST, CIFAR10	This scheme is applicable for image and video also.
[95]	Secure the multimedia data using encryption and blockchain	CRBM, blockchain, SHA-256, henon, and zigzag map	Generation of pseudo random sequence	Ultrasonic, BraTS18	It evaluate the security performance on three different medical datasets
[96]	Secure the colour image using BiLSTM model	BiLSTM, Chen chaotic map	Predict key sequence of chaotic system	SIPI Image	Low resistance against differential attacks.
[97]	Introduce the SAE encryption scheme for digital image	Logistic map, SAE,	Compress the plain image	–	Better visual quality of reconstructed image.
[98]	Design encryption scheme for financial system	ANN, logistic, sine, tent map	Generation of pseudo random sequence	–	Hybrid chaotic map ensure the better randomness and security.
[99]	Secure the colour image using DNN	LSTM, HCLS, Scrambling	Generation of pseudo random sequence	USC-SIPI	It satisfies randomness test, which enhance the better security
[100]	Secure the colour image using HCNN based encryption	HCNN, logistic and tent map	Generation of chaotic key matrix	–	It passes the randomness test, that ensure better security.
[101]	Protect the user privacy using deep learning procedure	ADCNN, DNA, PCA, Hyper-chaotic map	Encrypt the plain image	CIFAR10	Hyper-chaotic map ensure the better randomness and security.
[102]	Secure the image using auto encoder	Auto encoder, logistic map, scrambling	Obtain the cipher image	–	The complete security analysis is missing.
[103]	Secure the medical image using chaotic map	UNet3+, chaotic map,	ROI segmentation	MSD, LiTS	It passes the randomness test, that ensure better security.
[104]	Secure the medical image using Reconstruction model	RDSN, lorenz, tent, and logistic map	Reconstruct the decrypted image	HAM-10000, BBBC041	Robustness analysis is missing.
[105]	Joint encryption-compression method for medical images	SR, YOLOv7, chaotic map, huffman encoding	Reconstruct the decrypted image	LiTS	Differential and robustness test is not examined.
[106]	Joint compression-encryption approach for colour image	Autoencoder, logistic map	Compress original image	Kodak	Robustness analysis is missing.
[107]	Secure the colour image using Reconstruction model	DRN, hashing, sine chaotic map	Reconstruct the decrypted image	DIV2K	Differential and robustness analysis is missing.

- Most of the deep learning-based encryption techniques require to share the sensitive information about model to the target domain/model for encryption purpose, which may lead to privacy leakage and misuse of the original content. Further, the computational cost of deep learning based encryption is high. Hence, hybrid of split and federated learning [114,115] model can be applied to make the model efficient and provide the privacy protection of original content.
- Most of techniques required larger training time for encryption purpose. Hence, it can be further reduced by applying the concept of transfer learning and high performance computing [116,117].
- If adversary can be able to access the hidden factor of deep learning model, then it can easily extract the secret information. The techniques like dynamic deep model watermarking [118] can be applied to protect the hidden factor of deep learning model.
- It can be identified that very few encryption techniques are developed for multi-resolution and 3D/4D type of images. Due to, their higher dimensionality/depth which requires higher computational cost. Hence, deep networks like GAN [119] can be used.
- Most of the deep learning based encryption techniques require larger training datasets. Hence techniques like data augmentation, pre-training model [120,121] can be the effective solution.

Table 12
Performance analysis other deep learning-based image encryption.

Ref	NPCR	UACI	PSNR	SSIM	Chi-square	Entropy	Computational time		Correlation coefficient		
							Enc.	Dec.	H	V	D
[89]	99.40	32.46	39.44	0.972	247.49	7.9987	0.335	0.341	0.0056	−0.002	0.0001
[90]	–	–	52.46	–	–	–	0.20	–	–	- -	
[91]	–	–	32.72	0.904	256	–	–	–	–	–	–
[92]	99.62	33.34	–	–	–	7.9882	–	–	−0.0003	0.0045	0.0034
[93]	99.59	33.54	79.69	–	–	7.9990	–	–	0.0012	0.0037	0.0001
[94]	–	–	–	–	–	–	0.002	0.001	–	–	–
[95]	99.69	33.43	–	–	–	7.9921	–	–	0.0103	0.0049	0.0072
[96]	–	–	–	–	–	7.9916	–	–	−0.0046	0.0072	0.0009
[97]	99.60	33.44	80.64	0.9956	–	7.9992	4.15	3.73	−0.0016	0.0010	0.0011
[98]	96.60	35.50	–	–	–	7.9975	–	–	0.0009	0.0015	0.0026
[99]	99.60	33.46	–	–	–	7.9970	–	–	0.0018	0.0000	−0.0108
[100]	99.65	33.43	–	–	–	7.9993	–	–	−0.0131	0.0142	−0.0044
[101]	99.63	33.46	37.67	–	–	7.9994	–	–	−0.0037	0.0031	−0.0056
[102]	–	–	–	–	–	7.9961	–	–	−0.0280	0.0385	−0.0092
[103]	99.60	33.46	28.81	0.9591	255.87	7.9983	0.076	0.104	−0.0011	−0.0320	−0.0039
[104]	99.58	33.47	41.44	0.9209	–	7.9998	1.7917	1.6899	−0.0014	−0.0005	−0.0003
[105]	–	–	30.42	0.9400	–	7.9992	1.235	1.292	–	–	–
[106]	99.61	33.47	40.27	0.9976	–	–	–	2.78	−0.0392	−0.0026	0.0002
[107]	–	–	30.44	0.9060	–	–	0.01	0.15	0.001	−0.0089	0.0165

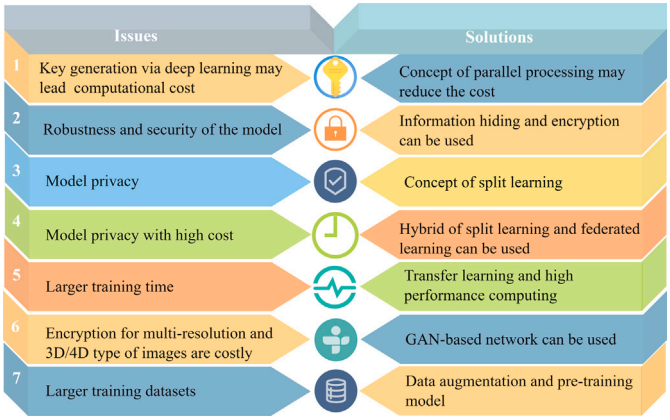

Fig. 9. Identified issues and their potential solution of deep learning based encryption technique.

5. Conclusion

This article examined various state-of-the-art encryption techniques that are based on deep learning models for multimedia information. In it, we reviewed classical encryption techniques and their attendant issues and discussed the important role that deep learning models play in encryption. We investigated numerous state-of-art-encryption processes that are based on deep learning models and summarized the results in tabular form. We analysed different performance metrics to measure the effectiveness of existing encryption techniques. Lastly, we identify the existing issues of deep learning based encryption techniques, along with some potential research directions that could fill the gaps in these domains for both researchers and developers, and discuss the improvement.

CRediT authorship contribution statement

Om Prakash Singh: Writing – review & editing, Writing – original draft, Visualization, Validation, Supervision, Methodology, Investigation, Funding acquisition, Formal analysis, Data curation, Conceptualization. **Kedar Nath Singh:** Writing – review & editing, Writing – original draft, Visualization, Validation, Supervision, Resources, Methodology, Investigation, Formal analysis, Data curation, Conceptualization. **Amit Kumar Singh:** Writing – review & editing, Writing – original draft, Visualization, Validation, Supervision, Resources, Project administration, Methodology, Investigation, Formal analysis, Data curation, Conceptualization. **Amrit Kumar Agrawal:** Writing – review & editing, Writing – original draft, Visualization, Validation, Supervision, Methodology, Investigation, Formal analysis, Conceptualization.

Declaration of competing interest

I certify that they have NO affiliations with or involvement in any organization or entity with any financial interest, or non-financial interest in the subject matter or materials discussed in this manuscript.

Data availability

No data was used for the research described in the article.

Acknowledgement

All authors approved the version of the manuscript to be published.

References

[1] M. Agiwal, A. Roy, N. Saxena, Next generation 5G wireless networks: A comprehensive survey, IEEE Commun. Surv. Tutor. 18 (3) (2016) 1617–1655.
[2] A.L. Buczak, E. Guven, A survey of data mining and machine learning methods for cyber security intrusion detection, IEEE Commun. Surv. Tutor. 18 (2) (2015) 1153–1176.
[3] AI image statistics: How much content was created by ai, 2023, https://journal.everypixel.com/ai-image-statistics. (Accessed 18 December 2023).
[4] S. Kemp, Digital 2023: Global overview report, 2023, DataReportal – Global Digital Insights. (Accessed 18 December 2023).
[5] O.P. Singh, A.K. Singh, G. Srivastava, N. Kumar, Image watermarking using soft computing techniques: A comprehensive survey, Multimedia Tools Appl. 80 (2021) 30367–30398.
[6] A. Anand, A.K. Singh, Watermarking techniques for medical data authentication: A survey, Multimedia Tools Appl. 80 (2021) 30165–30197.
[7] M.R. Bloch, Covert communication over noisy channels: A resolvability perspective, IEEE Trans. Inform. Theory 62 (5) (2016) 2334–2354.
[8] X. Chen, J. An, Z. Xiong, C. Xing, N. Zhao, F.R. Yu, A. Nallanathan, Covert communications: A comprehensive survey, IEEE Commun. Surv. Tutor. 25 (2) (2023) 1173–1198.
[9] O. Singh, A.K. Singh, Data hiding in encryption–compression domain, Complex Intell. Syst. 9 (3) (2023) 2759–2772.
[10] O.P. Singh, A.K. Singh, H. Zhou, Multimodal fusion-based image hiding algorithm for secure healthcare system, IEEE Intell. Syst. 38 (4) (2023) 53–61.

[11] Priyanka, N. Baranwal, K. Singh, O.P. Singh, A. Singh, HIDDEn: Robust data hiding for medical images with encryption and local binary pattern, Circuits Systems Signal Process. (2024) 1–21.

[12] B. Zhang, L. Liu, Chaos-based image encryption: Review, application, and challenges, Mathematics 11 (11) (2023) 2585.

[13] O.P. Singh, A.K. Singh, A robust information hiding algorithm based on lossless encryption and NSCT-HD-SVD, Mach. Vis. Appl. 32 (4) (2021) 101.

[14] K.N. Singh, O.P. Singh, A.K. Singh, Ecis: encryption prior to compression for digital image security with reduced memory, Comput. Commun. 193 (2022) 410–417.

[15] X. Tian, P. Zheng, J. Huang, Robust privacy-preserving motion detection and object tracking in encrypted streaming video, IEEE Trans. Inf. Forensics Secur. 16 (2021) 5381–5396.

[16] K.N. Singh, O. Singh, A.K. Singh, A.K. Agrawal, EiMOL: A secure medical image encryption algorithm based on optimization and the Lorenz system, ACM Trans. Multimed. Comput. Commun. Appl. 19 (2s) (2023) 1–19.

[17] O.P. Singh, K.N. Singh, N. Baranwal, A.K. Agrawal, A.K. Singh, H. Zhou, HIDEmarks: hiding multiple marks for robust medical data sharing using IWT-LSB, Multimedia Tools Appl. 83 (8) (2024) 24919–24937.

[18] T.N. Lakshmi, S. Jyothi, M.R. Kumar, Image encryption algorithms using machine learning and deep learning techniques—A survey, in: Modern Approaches in Machine Learning and Cognitive Science: A Walkthrough: Latest Trends in AI, vol. 2, Springer, 2021, pp. 507–515.

[19] B. Halak, Y. Yilmaz, D. Shiu, Comparative analysis of energy costs of asymmetric vs symmetric encryption-based security applications, IEEE Access 10 (2022) 76707–76719.

[20] K.M. Hosny, M.A. Zaki, N.A. Lashin, M.M. Fouda, H.M. Hamza, Multimedia security using encryption: A survey, IEEE Access (2023).

[21] P. Fang, H. Liu, C. Wu, M. Liu, A survey of image encryption algorithms based on chaotic system, Vis. Comput. 39 (5) (2023) 1975–2003.

[22] U. Zia, M. McCartney, B. Scotney, J. Martinez, M. AbuTair, J. Memon, A. Sajjad, Survey on image encryption techniques using chaotic maps in spatial, transform and spatiotemporal domains, Int. J. Inf. Secur. 21 (4) (2022) 917–935.

[23] Priyanka, A.K. Singh, A survey of image encryption for healthcare applications, Evol. Intell. 16 (3) (2023) 801–818.

[24] K.N. Singh, A.K. Singh, Towards integrating image encryption with compression: A survey, ACM Trans. Multimed. Comput. Commun. Appl. (TOMM) 18 (3) (2022) 1–21.

[25] M. Kaur, V. Kumar, A comprehensive review on image encryption techniques, Arch. Comput. Methods Eng. 27 (2020) 15–43.

[26] H.M. Ghadirli, A. Nodehi, R. Enayatifar, An overview of encryption algorithms in color images, Signal Process. 164 (2019) 163–185.

[27] K. Lata, L.R. Cenkeramaddi, Deep learning for medical image cryptography: A comprehensive review, Appl. Sci. 13 (14) (2023) 8295.

[28] K. Panwar, S. Kukreja, A. Singh, K.K. Singh, Towards deep learning for efficient image encryption, Procedia Comput. Sci. 218 (2023) 644–650.

[29] H. Kiya, A.P.M. Maung, Y. Kinoshita, S. Imaizumi, S. Shiota, et al., An overview of compressible and learnable image transformation with secret key and its applications, APSIPA Trans. Signal Inf. Process. 11 (1) (2022).

[30] I. Meraouche, S. Dutta, H. Tan, K. Sakurai, Neural networks-based cryptography: A survey, IEEE Access 9 (2021) 124727–124740.

[31] Z. Bao, R. Xue, Survey on deep learning applications in digital image security, Opt. Eng., Bellingham 60 (12) (2021) 120901–120901.

[32] T.T. Ramanathan, J. Hossen, S. Sayeed, J.E. Raja, Survey on computational intelligence based image encryption techniques, Indonesian J. Electr. Eng. Comput. Sci. 19 (3) (2020) 1428–1435.

[33] M.M. Alani, Applications of machine learning in cryptography: A survey, in: Proceedings of the 3rd International Conference on Cryptography, Security and Privacy, 2019, pp. 23–27.

[34] H. Jin, Y. Luo, P. Li, J. Mathew, A review of secure and privacy-preserving medical data sharing, IEEE Access 7 (2019) 61656–61669.

[35] O. Singh, A.K. Singh, A.K. Agrawal, H. Zhou, SecDH: security of COVID-19 images based on data hiding with PCA, Comput. Commun. 191 (2022) 368–377.

[36] H.M. Ghadirli, A. Nodehi, R. Enayatifar, An overview of encryption algorithms in color images, Signal Process. 164 (2019) 163–185.

[37] O.P. Singh, C. Kumar, A.K. Singh, M.P. Singh, H. Ko, Fuzzy-based secure exchange of digital data using watermarking in NSCT-RDWT-SVD domain, Concurr. Comput.: Pract. Exper. 35 (16) (2023) e6251.

[38] D.K. Mahto, O.P. Singh, A.K. Singh, Fusiw: fusion-based secure rgb image watermarking using hashing, Multimed. Tools Appl. 83 (2022) 61493–61509.

[39] I. Makhdoom, M. Abolhasan, J. Lipman, A comprehensive survey of covert communication techniques, limitations and future challenges, Comput. Secur. 120 (2022) 102784.

[40] Y. Sun, B. Xue, M. Zhang, G.G. Yen, Evolving deep convolutional neural networks for image classification, IEEE Trans. Evol. Comput. 24 (2) (2019) 394–407.

[41] H.K. Singh, N. Baranwal, K.N. Singh, A.K. Singh, H. Zhou, GAN-based watermarking for encrypted images in healthcare scenarios, Neurocomputing 560 (2023) 126853.

[42] M. Singh, N. Baranwal, K. Singh, A. Singh, H. Zhou, Deep learning-based biometric image feature extraction for securing medical images through data hiding and joint encryption–compression, J. Inf. Secur. Appl. 79 (2023) 103628.

[43] K.K. Raghuvanshi, S. Kumar, S. Kumar, S. Kumar, Image encryption algorithm based on DNA encoding and CNN, Expert Syst. Appl. 252 (2024) 124287.

[44] N. Bigdeli, Y. Farid, K. Afshar, A novel image encryption/decryption scheme based on chaotic neural networks, Eng. Appl. Artif. Intell. 25 (4) (2012) 753–765.

[45] L.-p. Chen, H. Yin, L.-g. Yuan, A.M. Lopes, J.T. Machado, R.-c. Wu, A novel color image encryption algorithm based on a fractional-order discrete chaotic neural network and DNA sequence operations, Front. Inf. Technol. Electron. Eng. 21 (6) (2020) 866–879.

[46] K. Ratnavelu, M. Kalpana, P. Balasubramaniam, K. Wong, P. Raveendran, Image encryption method based on chaotic fuzzy cellular neural networks, Signal Process. 140 (2017) 87–96.

[47] W. Chen, Y. Wang, Y. Xiao, X. Hei, Explore the potential of deep learning and hyperchaotic map in the meaningful visual image encryption scheme, IET Image Process. 17 (11) (2023) 3235–3257.

[48] J. Chen, X.-W. Li, Q.-H. Wang, Deep learning for improving the robustness of image encryption, Ieee Access 7 (2019) 181083–181091.

[49] X. Bai, J.-X. Li, Z. Yu, Z.-Z. Yang, Y.-J. Wang, X.-Y. Chen, X. Zhou, Reconstruction of chaotic grayscale image encryption based on deep learning, in: 2021 IEEE International Conference on Imaging Systems and Techniques, IST, IEEE, 2021, pp. 1–6.

[50] M.U. Rehman, A. Shafique, Y.Y. Ghadi, W. Boulila, S.U. Jan, T.R. Gadekallu, M. Driss, J. Ahmad, A novel chaos-based privacy-preserving deep learning model for cancer diagnosis, IEEE Trans. Netw. Sci. Eng. 9 (6) (2022) 4322–4337.

[51] Z. Man, J. Li, X. Di, Y. Sheng, Z. Liu, Double image encryption algorithm based on neural network and chaos, Chaos, Solitons Fractals 152 (2021) 111318.

[52] X. Li, Y. Jiang, M. Chen, F. Li, Research on iris image encryption based on deep learning, EURASIP J. Image Video Process. 2018 (1) (2018) 1–10.

[53] R. Ni, F. Wang, J. Wang, Y. Hu, Multi-image encryption based on compressed sensing and deep learning in optical gyrator domain, IEEE Photonics J. 13 (3) (2021) 1–16.

[54] J. Wang, F. Long, W. Ou, CNN-based color image encryption algorithm using DNA sequence operations, in: 2017 International Conference on Security, Pattern Analysis, and Cybernetics, SPAC, IEEE, 2017, pp. 730–736.

[55] U. Erkan, A. Toktas, S. Enginoğlu, E. Akbacak, D.N. Thanh, An image encryption scheme based on chaotic logarithmic map and key generation using deep CNN, Multimedia Tools Appl. 81 (5) (2022) 7365–7391.

[56] E. Abdellatef, E.A. Naeem, F.E.A. El-Samie, DeepEnc: deep learning-based CT image encryption approach, Multimedia Tools Appl. (2023) 1–21.

[57] W. Boulila, A. Ammar, B. Benjdira, A. Koubaa, Securing the classification of covid-19 in chest x-ray images: A privacy-preserving deep learning approach, in: 2022 2nd International Conference of Smart Systems and Emerging Technologies, SMARTTECH, IEEE, 2022, pp. 220–225.

[58] V. Himthani, V. Singh Dhaka, M. Kaur, A visually meaningful image encryption scheme based on a 5D chaotic map and deep learning, J. Imaging Sci. 69 (1–4) (2021) 164–176.

[59] A.S. Fard, D.C. Reutens, V. Vegh, From CNNs to GANs for cross-modality medical image estimation, Comput. Biol. Med. 146 (2022) 105556.

[60] T. Qiao, Y. Ma, N. Zheng, H. Wu, Y. Chen, M. Xu, X. Luo, A novel model watermarking for protecting generative adversarial network, Comput. Secur. 127 (2023) 103102.

[61] Z. Chen, Z. Zeng, H. Shen, X. Zheng, P. Dai, P. Ouyang, DN-GAN: Denoising generative adversarial networks for speckle noise reduction in optical coherence tomography images, Biomed. Signal Process. Control 55 (2020) 101632.

[62] D. Zhang, C. Wu, J. Zhou, W. Zhang, C. Li, Z. Lin, Hierarchical attention aggregation with multi-resolution feature learning for GAN-based underwater image enhancement, Eng. Appl. Artif. Intell. 125 (2023) 106743.

[63] T. Nithya, P.R. Kanna, S. Vanithamani, P. Santhi, An efficient PM-multisampling image filtering with enhanced CNN architecture for pneumonia classfication, Biomed. Signal Process. Control 86 (2023) 105296.

[64] H. Emami, M.M. Aliabadi, M. Dong, R.B. Chinnam, Spa-gan: Spatial attention gan for image-to-image translation, IEEE Trans. Multimed. 23 (2020) 391–401.

[65] M. Singh, N. Baranwal, K.N. Singh, A.K. Singh, Using GAN-based encryption to secure digital images with reconstruction through customized super resolution network, IEEE Trans. Consum. Electron. 70 (1) (2024) 3977–3984.

[66] Y. Ding, G. Wu, D. Chen, N. Zhang, L. Gong, M. Cao, Z. Qin, DeepEDN: A deep-learning-based image encryption and decryption network for internet of medical things, IEEE Internet Things J. 8 (3) (2020) 1504–1518.

[67] O.D. Singh, S. Dhall, A. Malik, S. Gupta, A robust and secure immensely random GAN based image encryption mechanism, Multimedia Tools Appl. 82 (13) (2023) 19693–19743.

[68] P. Fang, H. Liu, C. Wu, M. Liu, A block image encryption algorithm based on a hyperchaotic system and generative adversarial networks, Multimedia Tools Appl. 81 (15) (2022) 21811–21857.

[69] Z. Bao, R. Xue, Y. Jin, Image scrambling adversarial autoencoder based on the asymmetric encryption, Multimedia Tools Appl. 80 (18) (2021) 28265–28301.

[70] Z. Man, J. Li, X. Di, X. Liu, J. Zhou, J. Wang, X. Zhang, A novel image encryption algorithm based on least squares generative adversarial network random number generator, Multimedia Tools Appl. 80 (2021) 27445–27469.
[71] Y. Ding, F. Tan, Z. Qin, M. Cao, K.-K.R. Choo, Z. Qin, DeepKeyGen: A deep learning-based stream cipher generator for medical image encryption and decryption, IEEE Trans. Neural Netw. Learn. Syst. 33 (9) (2021) 4915–4929.
[72] K. Panwar, A. Singh, S. Kukreja, K.K. Singh, N. Shakhovska, A. Boichuk, Encipher GAN: An end-to-end color image encryption system using a deep generative model, Systems 11 (1) (2023) 36.
[73] P. Fang, H. Liu, C. Wu, A novel chaotic block image encryption algorithm based on deep convolutional generative adversarial networks, IEEE Access 9 (2020) 18497–18517.
[74] W. Sirichotedumrong, H. Kiya, A gan-based image transformation scheme for privacy-preserving deep neural networks, in: 2020 28th European Signal Processing Conference, EUSIPCO, IEEE, 2021, pp. 745–749.
[75] K. Neela, V. Kavitha, Blockchain based chaotic deep GAN encryption scheme for securing medical images in a cloud environment, Appl. Intell. 53 (4) (2023) 4733–4747.
[76] A.K. Sari, et al., Compression-encryption model for digital images based on GAN and logistic map, in: 2021 International Seminar on Intelligent Technology and Its Applications, ISITIA, IEEE, 2021, pp. 319–324.
[77] A.A. Krishna, V. Arikutharam, K.V. Ramnan, H. Bharathi, T. Chandar, Dynamic image encryption using neural networks for medical images, in: 2022 IEEE IAS Global Conference on Emerging Technologies, GlobConET, IEEE, 2022, pp. 739–745.
[78] J. Zhang, X.-Y. Zhang, C. Wang, C.-L. Liu, Deep representation learning for domain generalization with information bottleneck principle, Pattern Recognit. 143 (2023) 109737.
[79] S.R. Maniyath, V. Thanikaiselvan, An efficient image encryption using deep neural network and chaotic map, Microprocess. Microsyst. 77 (2020) 103134.
[80] Z. Man, J. Li, X. Di, R. Zhang, X. Li, X. Sun, Research on cloud data encryption algorithm based on bidirectional activation neural network, Inform. Sci. 622 (2023) 629–651.
[81] Q.-X. Huang, W.L. Yap, M.-Y. Chiu, H.-M. Sun, Privacy-preserving deep learning with learnable image encryption on medical images, IEEE Access 10 (2022) 66345–66355.
[82] W. Sirichotedumrong, T. Maekawa, Y. Kinoshita, H. Kiya, Privacy-preserving deep neural networks with pixel-based image encryption considering data augmentation in the encrypted domain, in: 2019 IEEE International Conference on Image Processing, ICIP, IEEE, 2019, pp. 674–678.
[83] Y. Gao, Y. Tian, et al., An improved image processing based on deep learning backpropagation technique, Complexity 2022 (2022).
[84] C. Rupa, M. Harshitha, G. Srivastava, T.R. Gadekallu, P.K.R. Maddikunta, Securing multimedia using a deep learning based chaotic logistic map, IEEE J. Biomed. Health Inf. 27 (3) (2022) 1154–1162.
[85] N. Iqbal, M. Khan, K. Khurshid, I. Hussain, An efficient hybrid encryption model based on deep convolutional neural networks, deoxyribonucleic acid computing and chaotic system, Multimedia Tools Appl. 82 (9) (2023) 13881–13903.
[86] H. Ito, Y. Kinoshita, M. Aprilpyone, H. Kiya, Image to perturbation: An image transformation network for generating visually protected images for privacy-preserving deep neural networks, IEEE Access 9 (2021) 64629–64638.
[87] W. Sirichotedumrong, Y. Kinoshita, H. Kiya, Pixel-based image encryption without key management for privacy-preserving deep neural networks, Ieee Access 7 (2019) 177844–177855.
[88] J.-W. Lee, H. Kang, Y. Lee, W. Choi, J. Eom, M. Deryabin, E. Lee, J. Lee, D. Yoo, Y.-S. Kim, et al., Privacy-preserving machine learning with fully homomorphic encryption for deep neural network, IEEE Access 10 (2022) 30039–30054.
[89] K.N. Singh, N. Baranwal, O.P. Singh, A.K. Singh, SIELNet: 3D chaotic-map-based secure image encryption using customized residual dense spatial network, IEEE Trans. Consum. Electron. (2022).
[90] C.T. Selvi, J. Amudha, R. Sudhakar, Medical image encryption and compression by adaptive sigma filterized synorr certificateless signcryptive levenshtein entropy-coding-based deep neural learning, Multimedia Syst. (2021) 1–16.
[91] C. Wang, T. Zhang, H. Chen, Q. Huang, J. Ni, X. Zhang, A novel encryption-then-lossy-compression scheme of color images using customized residual dense spatial network, IEEE Trans. Multimed. (2022).
[92] A. Kumar, M. Dua, A GRU and chaos-based novel image encryption approach for transport images, Multimedia Tools Appl. 82 (12) (2023) 18381–18408.
[93] Y. He, Y.-Q. Zhang, X. He, X.-Y. Wang, A new image encryption algorithm based on the OF-LSTMS and chaotic sequences, Sci. Rep. 11 (1) (2021) 6398.
[94] H. Zhu, R. Wang, Y. Jin, K. Liang, J. Ning, Distributed additive encryption and quantization for privacy preserving federated deep learning, Neurocomputing 463 (2021) 309–327.
[95] Z. Feixiang, L. Mingzhe, W. Kun, Z. Hong, Color image encryption via hénon-zigzag map and chaotic restricted Boltzmann machine over blockchain, Opt. Laser Technol. 135 (2021) 106610.
[96] Y. Liu, G. Cen, B. Xu, X. Wang, Color image encryption based on deep learning and block embedding, Secur. Commun. Netw. 2022 (1) (2022) 6047349.
[97] N. Gupta, R. Vijay, Hybrid image compression-encryption scheme based on multilayer stacked autoencoder and logistic map, China Commun. 19 (1) (2022) 238–252.
[98] S. Pan, J. Wei, S. Hu, A novel image encryption algorithm based on hybrid chaotic mapping and intelligent learning in financial security system, Multimedia Tools Appl. 79 (2020) 9163–9176.
[99] S. Zhou, Z. Zhao, X. Wang, Novel chaotic colour image cryptosystem with deep learning, Chaos Solitons Fractals 161 (2022) 112380.
[100] X.-Y. Wang, Z.-M. Li, A color image encryption algorithm based on hopfield chaotic neural network, Opt. Lasers Eng. 115 (2019) 107–118.
[101] S.-L. Cheng, L.-J. Wang, G. Huang, A.-Y. Du, A privacy-preserving image retrieval scheme based secure kNN, DNA coding and deep hashing, Multimedia Tools Appl. 80 (2021) 22733–22755.
[102] Y. Sang, J. Sang, M.S. Alam, Image encryption based on logistic chaotic systems and deep autoencoder, Pattern Recognit. Lett. 153 (2022) 59–66.
[103] K.N. Singh, N. Baranwal, O.P. Singh, A.K. Singh, DeepENC: Deep learning-based ROI selection for encryption of medical images through key generation with multimodal information fusion, IEEE Trans. Consum. Electron. (2024) 1–1.
[104] Priyanka, N. Baranwal, K. Singh, A. Singh, Using chaos to encrypt images with reconstruction through deep learning model for smart healthcare, Comput. Electr. Eng. 114 (2024) 109089.
[105] Priyanka, N. Baranwal, K.N. Singh, A.K. Singh, et al., YOLO-based ROI selection for joint encryption and compression of medical images with reconstruction through super-resolution network, Future Gener. Comput. Syst. 150 (2024) 1–9.
[106] B. Wang, K.-T. Lo, Autoencoder-based joint image compression and encryption, J. Inf. Secur. Appl. 80 (2024) 103680.
[107] X. Chai, S. Song, Z. Gan, G. Long, Y. Tian, X. He, CSENMT: A deep image compressed sensing encryption network via multi-color space and texture feature, Expert Syst. Appl. 241 (2024) 122562.
[108] M. Mahmud, M.S. Kaiser, A. Hussain, S. Vassanelli, Applications of deep learning and reinforcement learning to biological data, IEEE Trans. Neural Netw. Learn. Syst. 29 (6) (2018) 2063–2079.
[109] H. Ali, D. Chen, M. Harrington, N. Salazar, M. Al Ameedi, A. Khan, A.R. Butt, J.-H. Cho, A survey on attacks and their countermeasures in deep learning: Applications in deep neural networks, federated, transfer, and deep reinforcement learning, IEEE Access (2023).
[110] E. Fernando, D.F. Murad, B.D. Wijanarko, Classification and advantages parallel computing in process computation: A systematic literature review, in: 2018 International Conference on Computing, Engineering, and Design, ICCED, IEEE, 2018, pp. 143–147.
[111] H.L. França, C. Teixeira, N. Laranjeiro, Techniques for evaluating the robustness of deep learning systems: A preliminary review, in: 2021 10th Latin-American Symposium on Dependable Computing, LADC, IEEE, 2021, pp. 1–5.
[112] J. Liu, Y. Jin, A comprehensive survey of robust deep learning in computer vision, J. Autom. Intell. (2023).
[113] Y. Li, H. Wang, M. Barni, A survey of deep neural network watermarking techniques, Neurocomputing 461 (2021) 171–193.
[114] S. Otoum, N. Guizani, H. Mouftah, On the feasibility of split learning, transfer learning and federated learning for preserving security in ITS systems, IEEE Trans. Intell. Transp. Syst. 24 (7) (2023) 7462–7470.
[115] L. Zhang, J. Xu, P. Vijayakumar, P.K. Sharma, U. Ghosh, Homomorphic encryption-based privacy-preserving federated learning in IoT-enabled healthcare system, IEEE Trans. Netw. Sci. Eng. 10 (5) (2023) 2864–2880.
[116] L. Shao, F. Zhu, X. Li, Transfer learning for visual categorization: A survey, IEEE Trans. Neural Netw. Learn. Syst. 26 (5) (2014) 1019–1034.
[117] X. Zhang, F. Reveriano, J. Lu, X. Fu, T. Zhang, The effect of high performance computer on deep learning: A face expression recognition case, in: 2019 IEEE International Conference on Computational Science and Engineering (CSE) and IEEE International Conference on Embedded and Ubiquitous Computing, EUC, IEEE, 2019, pp. 40–42.
[118] S. Szyller, B.G. Atli, S. Marchal, N. Asokan, Dawn: Dynamic adversarial watermarking of neural networks, in: Proceedings of the 29th ACM International Conference on Multimedia, 2021, pp. 4417–4425.
[119] P. Amrit, A.K. Singh, M.P. Singh, A.K. Agrawal, Embedr-net: Using cnn to embed mark with recovery through deep convolutional gan for secure ehealth systems, IEEE Trans. Consum. Electron. 69 (4) (2023) 1017–1022.
[120] A. Mumuni, F. Mumuni, Data augmentation: A comprehensive survey of modern approaches, Array 16 (2022) 100258.
[121] O.A. Cárdenas, L.M.F. Nava, F.G. Castañeda, J.A.M. Cadenas, ECG arrhythmia classification for comparing pre-trained deep learning models, in: 2022 19th International Conference on Electrical Engineering, Computing Science and Automatic Control, CCE, IEEE, 2022, pp. 1–5.

Om Prakash Singh is currently working as assistant professor in CSE department at Indian Institute of Information Technology (IIIT) Bhagalpur, Bihar, India. He pursued his Ph.D. degree at NIT Patna. He received his M. Tech. degree in computer science and engineering from NIT Hamirpur, H.P., India in 2018, and his B. E. in computer science and engineering from the Technocrats Institute of Technology, Bhopal, M.P., India, in 2015. His research interests include data hiding techniques, cryptography, and image watermarking.

Kedar Nath Singh is currently working as Assistant Professor in the Department of CSE and IT, JIIT Noida. He has done his Ph.D. from NIT Patna. He completed his M.Tech from AIACTR, New Delhi in 2011 and B.Tech from UPTU, Lucknow in 2008. His research interest includes Image Cryptography, Image processing and Multimedia security.

Amit Kumar Singh is currently working as an Associate Professor in the Computer Science and Engineering Department, National Institute of Technology Patna, Bihar, India. He has authored over 250 peer-reviewed journals and conference publications. Dr. Singh has been recognized as "WORLD RANKING OF TOP 2% SCIENTISTS" in the area of "Biomedical Research" (for Year 2020) and "Artificial Intelligence & Image Processing" (for Year 2020–2024), according to the survey given by Stanford University, USA. Dr Singh is currently member of editorial advisory board, IEEE Spectrum and Associate Editor of IEEE Trans. Cybern., IEEE Trans. On Multimedia, ACM Trans. Multimedia Comput. Commun. Appl., IEEE Trans. Computat. Social Syst., IEEE Trans. Ind. Informat., IEEE J. Biomed. Heal. Informatics, Eng. Appl. Artif. Intell., Elsevier, IEEE Technology Policy and Ethics Newsletter etc. He is the series editor of The IET International Book Series on Multimedia Information Processing and Security. His research interests include multimedia data hiding, image processing, biometrics, & cryptography.

Amrit Kumar Agrawal is currently working as an Associate Professor in the Department of Computer Science and Engineering at Sharda School of Engineering & Technology, Sharda University, Greater Noida, Uttar Pradesh. He received his Ph.D. in Computer Science & Engineering from Dr. APJ Abdul Kalam Technical University, Lucknow, UP, M.Tech. in Computer Science & Engineering from Jaypee University of Information Technology (JUIT), Waknaghat, Solan, Himachal Pradesh in 2010 and B. Tech. degree in Computer Science & Engineering from VBS Purvanchal University, Jaunpur, Uttar Pradesh in 2005. He has to his credit for various research articles published in International Journals/ Conferences of repute. Dr. Agrawal is interested in the areas of Image security and analysis, Biometrics, Pattern Recognition and Machine Learning.