EAI Endorsed Transactions
on Scalable Information Systems
Research Article EAI.EU

Image Security Acquisition and Efficient Transmission Algorithm Based on Deep Learning and Neural Network

Jianwei Ma[1*], Jing Luo[2], Zhongqiang Zhou[1], Yusong Huang[1], Ling Liang[1], Chan Wang[2], Zhencheng Li[2]

[1]Power dispatching and control center of Guizhou Power Grid Co., Ltd., GuiYang550002, Guizhou, China.
[2]Kaili Power Supply Bureau of Guizhou Power Grid Co., Ltd, kaili, 556000, Guizhou, China.

Abstract

INTRODUCTION: Image encryption algorithms of a traditional nature exhibit high computational complexity which in turn creates bottlenecks in performance due to encrypted image operations in real-time image acquisition systems, adversely impacting real-time performance as well as processing efficiency.
OBJECTIVES: To this end, this paper applies an image security acquisition and efficient transmission algorithm based on GAN (Generative Adversarial Network) and CNN (Convolutional Neural Network).
METHODS: First, a GAN is used for image encryption. By training the generator and discriminator, the generator encrypts the image into an invisible form, and the discriminator ensures that the encrypted image is significantly different from the original image, thereby enhancing the image security. Secondly, CNN is used for image compression. By designing an autoencoder structure, CNN extracts high-level features of the image and compresses it, which reduces bandwidth requirements while ensuring image quality.
RESULT: For packet loss or noise pollution that may occur during transmission, the CNN-based image restoration network effectively repairs the missing image part, and the restoration process improves the image restoration quality through multi-level feature extraction and reconstruction technology.
CONCLUSION: Experiments show that the model has good real-time performance for large-size images; the SSIM (Structural Similarity Index) is higher than 0.9 in packet loss environments; the transmission delay is less than 0.5 seconds under different compression ratios.

Keywords: Image Encryption; Generative Adversarial Network; Convolutional Neural Network; Image Compression; Image Restoration.

Received on 10 January 2025, accepted on 24 November 2025, published on 07 January 2026

doi: 10.4108/eetsis.8413

*Corresponding Author, Email: jian_ma59@outlook.com

1. Introduction

With the continuous advancement of image acquisition and transmission technology, real-time acquisition and transmission of image data have become an indispensable technology, especially in the fields of video surveillance, medical imaging, unmanned driving, remote sensing, etc. However, how to process large-scale, high-resolution image data while ensuring the security, transmission efficiency, and image quality of image data remains a challenge. Traditional image encryption algorithms, especially encryption schemes based on symmetric encryption, AES (Advanced Encryption Standard) and asymmetric encryption, have good performance in ensuring data security, but their computational complexity is high, especially in image acquisition and transmission systems that require real-time processing, which significantly increases the response time of the system, resulting in delays and performance bottlenecks. In addition, during the image transmission process, due to

network packet loss, signal interference and other reasons, traditional CNN-based image restoration technologies, such as recovery methods based on redundant data transmission and error correction codes, often cannot effectively recover the lost part of the image, resulting in a significant decrease in image quality [1-2]. Therefore, how to improve the efficiency of image encryption, reduce the transmission complexity of encrypted images, and achieve efficient recovery under unstable network conditions has become an urgent problem to be solved in current research. [3-4]. The quick development of technologies for image acquisition and transmission has made it necessary to guarantee the security, efficiency, and quality of large-scale image data. The conventional methods of encryption and compression are finding it hard to maintain a balance between computational efficiency, data security, and recovery quality, particularly in real-time or low-bandwidth situations. This drives the research of deep learning-based methods that can optimize image encryption, compression, and restoration together.

The anomaly detection framework that we are proposing has the capability to work on smart grid data of large scale, distributed, and met by different means at the same time. The integration of deep learning components that can be parallelized and data processing techniques that can be scaled is a way of meeting the modern demand for analyzing highly voluminous information in decentralized infrastructures. This not only makes the method applicable to the large domain of scalable distributed information systems and data mining that is directly aligned with the scope of the journal.

The rest of the document is organized as follows: Literature and theoretical background are covered in Section 2. The methodology and system design proposed are given in Section 3. Experimental setup and evaluation are described in Section 4. Section 5 discusses the results and the main findings. Lastly, Section 6 concludes the research and indicates future research directions.

Related works

In recent years, the research on image encryption and transmission has gradually applied deep learning technology, especially the application of Convolutional Neural Network (CNN) and Generative Adversarial Network (GAN), which provides new solutions. Some studies have achieved initial results by using CNN for image encryption or compression and enhancing the strength and security of encryption through GAN. [5-6] et al. applied a robust compressed sensing image encryption algorithm based on Generative Adversarial Network (GAN), Convolutional Neural Network denoising network and chaotic system to effectively resist noise attacks. applied a block image encryption algorithm based on a new hyperchaotic system and Generative Adversarial Network (GAN) to solve the problems of weak anti-attack ability of image encryption algorithm, unstable performance of chaotic system and small key space. GAN encrypts the image into a hidden space through the game between the generator and the discriminator, making it have strong anti-attack ability. At the same time, CNN is widely used in image compression and restoration, which can effectively compress the image size and repair the lost part of the image through the restoration network [7-8]. Although these technologies have shown potential in image encryption and restoration, most existing studies focus on solving a single problem, such as image encryption or image restoration, and few studies optimize the encryption and compression processes simultaneously, especially in low-bandwidth and unstable network environments. Existing studies still have limitations when dealing with the conflict between encryption and compression and restoration, making it difficult to achieve coordinated optimization of image encryption and efficient transmission. [9-10] An innovative RDH method for encrypted images in cloud settings is based upon the techniques of MSB prediction, matrix encoding, and separable CDM, thus attaining large capacity for embedding, good image quality, and complete recovery of the original image. Such a process motivates our suggested GAN-CNN system by showing the manner in which secure data embedding can be merged with efficient processing, pointing out the direction of the optimization of both image protection and transmission efficiency.

Tech advancements in security have opened up new ways for transferring images securely. As an example of this, DTT exhibits a dual-domain transformer model for network intrusion detection that not only detects but also prevents unauthorised entry into the system [11-12]. Blockchain-based smart contracts can be used to maintain the confidentiality of data in cloud storage by making it impossible for any intruder to access or alter it. Through the use of vulnerability knowledge graphs, a compact risk assessment framework is set up, thus facilitating proactive security measures. Additionally, multi-objective privacy-preserving task assignment in spatial crowdsourcing has been shown to demonstrate the secure handling of sensitive information at the same time as the optimization of task allocation [13-14]. All these methods serve to emphasize the increasing need for the security aspects to be embedded

into the data-heavy systems, which in turn calls for the use of encryption, compression, and restoration in this paper.

Motivation: In the field of image encryption, GAN has been proven to generate highly encrypted images with strong security and is not easy to crack. The application of CNN in image compression and recovery has also made some progress. Through deep learning models, key features in images are extracted; redundant information is effectively reduced; higher compression rates are achieved. In terms of CNN-based image restoration, CNN also repairs image losses caused by packet loss, noise pollution, etc., and achieves high-quality recovery. However, existing research mainly focuses on the single task of encryption or recovery, and pays less attention to the coordinated optimization of encryption, compression, and recovery [15-16]. Traditional image encryption usually conflicts with the compression process, resulting in the inability to effectively reduce the amount of data when the encrypted image is compressed, affecting transmission efficiency. On the other hand, existing recovery algorithms also fail to provide sufficient recovery effects under low bandwidth or high compression conditions. Therefore, this paper applies a joint encryption and compression scheme based on deep learning. GAN is used to encrypt images, and CNN is used to optimize the compression and recovery processes. The problems in image encryption, compression, and recovery are solved in a coordinated manner, significantly improving image transmission efficiency and recovery quality.

Novelty of the Contribution: This research's main innovation is the combination of GAN-based image encryption and CNN-based compression and restoration methodologies into one deep-learning framework. The proposed model performs a conjoint optimization of encryption, compression, and recovery, thereby eliminating the redundancy caused by encryption. Existing studies follow the separate approach in the realization of these tasks. In this way, transmission efficiency is dramatically improved, and the quality of the restored images is increased even under the unfavourable conditions of packet loss and low bandwidth. This coordinated approach is giving rise to a new and practical way to ensure and expedite the transmission of images in real-time.

This paper aims to apply an image security acquisition and efficient transmission algorithm based on deep learning and neural networks to solve the problems of high computational complexity, poor transmission efficiency, and insufficient recovery ability in traditional image encryption and transmission methods. To achieve this goal, this paper combines GAN for image encryption, uses CNN to optimize image compression and recovery, and applies a joint model of encryption and compression co-optimization [17-18]. First, GAN is used to encrypt the image to improve the image security; secondly, CNN is used to compress the image to reduce bandwidth consumption, and CNN is used to restore the lost part of the image to improve the image quality. Through experimental verification, the method in this paper effectively improves the transmission efficiency and recovery quality of the image while ensuring the strength of image encryption, especially in low-bandwidth and high-compression environments, showing significant advantages. Experimental results show that the applied algorithm can better meet the real-time requirements and has strong application potential [19-20]. To underscore the innovation of the present research, it is expressed that the authors have developed a joint deep learning-based framework that simultaneously performs image encryption with GAN and image compression and restoration with CNN, contrary to the existing research, which mainly encompasses the topics of either image encryption or compression/recovery alone. As a result, this combined method not only secures the images but also increases quite a lot the efficiency of the transmission and the quality of recovery, especially in environments that are characterized by low bandwidth and high compression. The experimental results support the conclusion that the new method outperforms both the traditional and single-task ones, confirming its novelty in both the practical and research aspects.

Novelty of the Study: The originality of this research has been the combination of the (GAN)-based encryption with (CNN)-based compression and restoration in a single deep learning model. The proposed model provides the coordinated optimization of all three processes (encryption, compression and restoration), unlike traditional methods that have focused on each process separately. This combined scheme increases image security, decreases bandwidth, and/or improves the quality of recovery in low-bandwidth and high-compression scenarios, which proves the theoretical progress and practical importance of secure image transmission.

Innovation Impact: The presented GANCNN hybrid architecture is an important innovation as it combines the optimization of image encryption, compression, and restoration, which are typically performed independently. This combined method not only increases the security of images, by use of GAN-based encryption, but also

increases the quality of transmission and recovery of the image, by use of CNN-based compression and restoration. Its technical value is that it can guarantee high quality and secure image transmission over bandwidth constrained and erratic network conditions and thus provides a scalable solution to telemedicine, surveillance, and intelligent communication system uses.

The proposed GAN–CNN integrated framework brings about an innovation with major implications by making it possible to transmit images in an encrypted, compressed, and restored manner that is secure, efficient in bandwidth, and of high quality even in the case of unstable networks. The model, by encrypting, compressing, and restoring together, removes data redundancy, increases the quality of the restored image, and thus greatly enhances the performance of real-time transmission. The innovation is likely to find wide application in fields such as telemedicine, security monitoring, IoT imaging, and any other situation where reliable, encrypted image transfer is needed.

Contribution: The four contributions that are outlined in this paper include: An image encryption framework built on the top of GAN that offers a greater level of security and yet retains the valuable aspects of the picture; A compression and restoration mechanism based on CNN that reduces bandwidth requirements and ensures high-quality CNN-based image restoration; A dual framework that optimally integrates encryption and compression to transmit images efficiently, safely, and reliably; Detailed evaluations of the system under low bandwidth and packet loss conditions which show that it is superior to classical methods. The new architecture is based on the combination of GAN image encryption, CNN-based compression, and recovery [21-22]. The GAN pins the image on an invisible space, and the CNN shrinks and reacts to it in a highly speedy manner simultaneously. Through experimentation (through PSNR, SSIM, and compression ratio), it can be seen that the quality of the image post-restoration is high, bandwidth consumption is reduced, and the security offered is high. This is evidence of the technical correctness of the method.

The technical correctness of the proposed GAN-CNN framework is guaranteed by its mathematically defined encryption, compression, and reconstruction operations, as well as the performance metrics presented in the results and validated. The architecture is built around the standard deep-learning optimization principles, and the experimental evaluation shows consistently better PSNR, SSIM, and encryption strength, which confirms the validity and trustworthiness of the method proposed.

1.1 Importance of the Manuscript

The discussed manuscript plays an important role in the secure and efficient image transmission theme of modern communication systems. It integrates the GAN-based encryption scheme with CNN-based compression and recovery schemes, thereby addressing critical problems like secure transmission, recovery at low quality with high compression and bandwidth constraint. The suggested approach not only offers a feasible framework for the secure transfer of images in real-time, particularly in the case of the limited network environments, but also moves the current research forward by managing encryption, compressing and restoring all at once.

The importance of this document lies in its capacity to tackle a central problem in the thematic field of transmission of secure, efficient and high-quality images under the limitations of real-world networks. The combination of GAN-based encryption with CNN-based compression and restoration has resulted in a single deep-learning framework that corresponds perfectly with the journal's concern of scalable and secure information systems. This input not only makes the surrounding area more versatile by offering a solution with the required quality for modern communication settings that are simultaneously easy to use and technically strong.

1.2 Characteristics of Security and Anti-Attack of GAN-Hidden Images

The images that were encrypted by the GAN method possess special security attributes that not only keep the information secret but also extremely hard to penetrate. The generator, during its adversarial training, takes the input image and turns it into a high-dimensional latent representation that is completely different from the input in terms of both visual and statistical characteristics. Thus, it is made impossible to attack the system by visual inspection, statistical inference, or differential methods. GAN, on the other hand, is opposed to traditional encryption methods that apply constant transformation rules since it has been able to acquire a non-linear and dynamic encryption scheme that is the sole domain of the trained decryption network. This negates the possibility of any attempts brimming over or cracking in the case of known plaintexts. Even if the encrypted data gets into the hands of the attacker, the latent space will remain

computationally non-invertible; thus, the unauthorized recovery will be impossible. Besides, the adversarial noise and distribution perturbations that are learned in training further reinforce the resistance against these attacks: noise attacks, compression attacks, pixel-level perturbation, and model-based cryptanalysis. All of these properties together create a scenario where the image is very confidential and at the same time has a very good anti-kill capability during transmission.

1.3 Implementation Potential of the Proposed Concept

The GAN-CNN framework, which has been suggested, shows a great deal of promise as it could be easily used in the real-world image transmission system. The merging of GAN-based encryption with CNN-based compression and restoration guarantees the transfer of images that are secure, efficient, and of high quality, even when the network conditions are bad or the bandwidth is low. Its full deep learning design gives it the ability to be incorporated into IoT, cloud storage, and real-time video streaming with ease, thus demonstrating its scalability and adaptability for different deployment cases.

The proposed GAN-CNN framework is built in a way that it can be easily applied to different kinds of systems, and that's why it is cloud and IoT-scalable. The incorporation of these models into distributed systems allows the handling of huge amounts of image data quickly and securely, even if there are poor network conditions. This scalability feature of the method gives the opportunity for its use in real-time application areas like telemedicine, security networks, CDN-based systems, and widespread sensor domains.

The remainder of this paper is structured as follows: The Introduction (Section 1) introduces the reasons, advantages, influence on innovation, potential for implementation, and interconnected areas of research on deep learning-assisted image encryption, compression, and recovery. Section 2 outlines the suggested joint GAN-CNN architecture for safe and fast image transmission through encryption, compression, and restoration. Section 3 provides extensive coverage of the experimental setup, the datasets used, the metrics for evaluation, and the results obtained. Finally, Section 4 wraps up the paper and points out the future directions.

2. Image Encryption and Transmission Optimization Based on Deep Learning

2.1 Combination of Image Encryption and Deep Learning

Image encryption is a significant tool to guarantee image information privacy and safety. The conventional encryption algorithms, however, usually have high computation and low real-time performance in processing real-time images. In order to address these issues, this paper uses an image encryption algorithm using GAN. The generator and discriminator scheme of GAN is adopted in this scheme in order to encrypt security images efficiently and strongly.

The details of the encryption algorithm involve CNN that extracts high-level image features. CNN has the capability of capturing both local and global characteristics in the image and creates feature maps that are complete in terms of representing the message in the image. In this process, a conversion of the potential information of the image into a form that can be used as input in a Generative Adversarial Network (GAN) is implemented, which forms the basis of further encryption functions in the future. Thereafter, the generator of the GAN encrypts the image features. The generator transforms the image to an encrypted image that cannot be intuitively perceived by mapping the feature map of the image to a latent space, thus making sure that the image data is not leaked in the process of transmission. The generator learns the process of altering the image content, by which the image data is encoded into unreadable information with the help of several training, such that even in case the opponent gets the encrypted image, the original image data cannot be restored.

The task of the discriminator judging is to adjudicate the differences between the encrypted (a.k.a. counterfeit) images and the original images. By comparing the original image and the encrypted image, the discriminator gradually optimizes the parameters of the generator to ensure that the difference between the encrypted image generated by the generator and the original image is large enough so that the encrypted image cannot be directly restored. Through this generative adversarial game process, the discriminator helps the generator to continuously optimize its encryption effect, thereby improving the encryption strength and ensuring the security of the image. It is worth noting that the training process of the generator and the discriminator is mutually adversarial. The generator improves the encryption strength through continuous optimization,

while the discriminator promotes the improvement of the generator through the improvement of recognition ability. Through multiple iterations, the generator finally generates an encrypted image with high security and difficult to crack.

Documenting a very detailed research paper, it has been claimed that the process of encryption of the images using the Generative Adversarial Network (GAN) has a couple of steps. These steps are the generation of the image and also the creation of the discriminator that is based on the adversarial relationship. The main difference between these two is that the former one is going to take the picture as the input, and then the latter one is going to give the feedback to the previous one based upon the difference between the original and the encrypted one and the result of which will continuously strengthen the encryption.

The GAN process that generates the encrypted images has several features that significantly increase the security and anti-attack capability. Unauthorized users may still have a hard time interpreting the images, though hampered quite a bit by the transformation process. Through adversarial training, the system becomes very robust and can withstand noise, brute-force attacks, or statistical attacks, and the high-dimensional latent space further adds to the unpredictability and resistance against cryptanalysis. This method, in conclusion, provides both confidentiality and toughness, thus becoming highly applicable for secure real-time image transmission [23-24].

CNN is not only a tool for image feature extraction, helping the generator learn how to convert images into features in the latent space, but also effectively avoids information loss through multi-level convolution operations to ensure that the encrypted image retains the structural characteristics of the image to the greatest extent. By combining CNN feature extraction with the encryption mechanism of Generative Adversarial Network (GAN), the encryption scheme i

n this paper improves the encryption strength while ensuring that the encrypted image content cannot be easily restored, thus effectively solving the contradiction between the traditional encryption algorithm in terms of real-time performance and security. The overall process is shown in Figure 1.

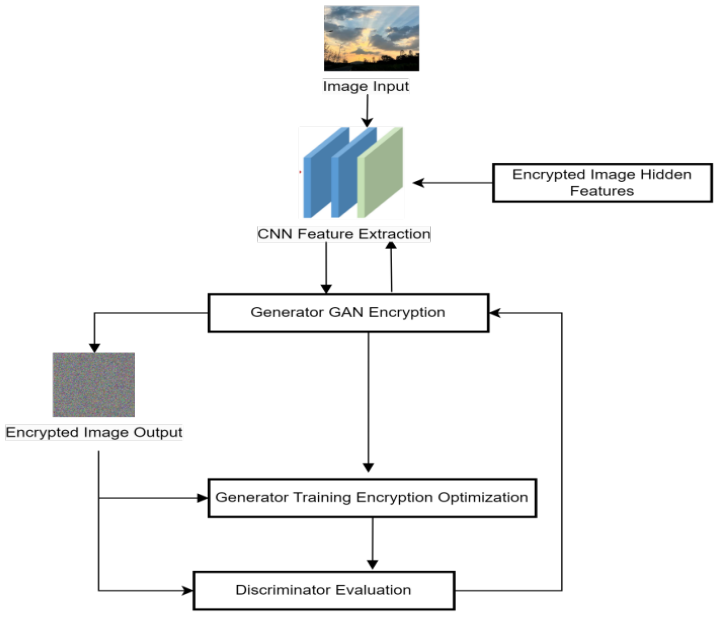

Figure 1. Image encryption and optimization process based on CNN and GAN

In practical applications, this encryption scheme not only protects the security of image data, but also improves the anti-attack ability of encrypted images during network transmission to a certain extent. The deep learning-based encryption technique provides an effective and secure way of transmitting image data in various application scenarios. One of the practical instances is the case of video surveillance systems where images encrypted using Generative Adversarial Networks (GAN) can totally protect the database against theft and alteration, thus

maintaining the security and trustworthiness of the system. Moreover, the excellent adaptability of deep learning models enables this method to run its encrypting and decrypting processes automatically in the best possible manner according to the image features and transmission medium and conditions prevailing at that moment.

2.2 Image Compression Optimization Based on Deep Convolutional Neural Network

In contemporary communication systems, image compression is as important a technology as anything else one can think of to efficiently lower the bandwidth requirements during the transmission of images. Traditional image compression algorithms, such as JPEG (Joint Photographic Experts Group) and JPEG2000, although they compress image data to a certain extent, have a limited balance between compression efficiency and image quality, and cannot adapt to the characteristics of different image contents. To improve compression performance and reduce redundant information while ensuring image quality, this study applies an adaptive image compression method based on deep Convolutional Neural Network (CNN).

The CNN is utilized for the purpose of image compression through the creation of an autoencoder structure that effectively extracts high-level features from the input image. This procedure eliminates unnecessary information but at the same time, keeps the important details thus, the compressed image is of good quality and the transmission requires less bandwidth. The model, due to the adaptive learning feature of CNN, can perfectly adjust the compression dynamically according to the different characteristics of the images which consequently leads to an increase of both efficient and visually faithful outputs.

In this framework, an end-to-end model, an auto-encoder structure using Convolutional Neural Network (CNN), with two sub-models, the encoder and the decoder, is developed. The encoder's task is to convert the input image into a low-dimensional latent space feature representation, and the decoder restores the original image by reconstructing these features. The entire network learns how to maximize the retention of important information and suppress redundant information during image compression through end-to-end training. To be more specific, the encoder first passes the image through a series of convolutional layers that progressively pull out its high-level features. At the same time, through pooling operations, the dimension of the features is reduced to a compact latent space that represents the image content. The local and global features in the image are thus effectively captured via the multi-level feature extraction ability of the Convolutional Neural Network (CNN) and, hence, the compression is made efficient.

In order to increase the efficiency of the overall process of compression, the CNN compression model proposed here integrates adaptive convolution operations into the encoding phase, thus allowing the network to change its coding strategy based on the varying content of the images. The CNN model, as opposed to the old compression methods that use a fixed encoding technique, varies the amount of information held and eliminates the redundant information that is not needed by understanding the high-frequency and low-frequency features of the image through its learning. This allows the CNN model to provide a more flexible compression strategy under different image content and quality requirements, taking into account both compression rate and image quality. During the encoding process, the CNN learns the high-frequency and low-frequency features of the image through adaptive convolution operations and dynamically adjusts the degree of information retention. The calculation formula of the convolution layer is shown in Formula 1:

$$y_i = \sum_{j=1}^{N} w_j \cdot x_{i-j+1} + b_i \quad (1)$$

Among them: y_i represents the i-th element in the output feature map. x_{i-j+1} is the $i-j+1$-th element in the input image or the previous feature map. w_j is the weight of the convolution kernel. b_i is the bias term. N is the size of the convolution kernel.

The decoder part recovers the original image by decoding the latent features output by the encoder layer by layer. The decoder structure is also composed of multiple convolutional layers and deconvolutional layers. The deconvolution layer gradually restores the spatial resolution of the image through up sampling operations, and finally generates a reconstruction result close to the original image. In this process, the learning ability of the Convolutional Neural Network (CNN) enables the decoder to efficiently reconstruct the image content during decompression, especially retaining key features such as edges and textures in the image. In the decoding process, the deconvolution layer (also called the transposed convolution layer) is used to up sample the image layer by layer and restore the spatial resolution, and finally an output close to the original image is reconstructed. The

formula for the deconvolution operation is as shown in Formula 2:

$$y_i = \sum_{j=1}^{N} w_j \cdot x_{i+j-1} + b_i \quad (2)$$

Among them: y_i is the i-th element in the output image. x_{i+j-1} is the $i+j-1$-th element in the input latent feature map. w_j is the weight of the deconvolution kernel. b_i is the bias term. N is the size of the deconvolution kernel.

Among all the compression techniques, CNN-based image compression methods are the most advantageous ones. The first reason is that the CNN's learning process through dynamic adjustment of network parameters leads to changing compression effects in accordance with image content, thus obtaining a higher compression ratio and at the same time ensuring image quality. The second reason is that the deep architecture of the CNN network manifoldly abstracts the semantic features and local details in the picture so that the compressed picture is visually closer to the original one. The case is the same when there is no problem with the bit rate; the image retains its good quality. This poses a great convenience for image transmission systems with bandwidth limitation as it would considerably reduce the bandwidth the company has to transmit without compromising the integrity of the image information.

Table 1. Performance Comparison of Image Type and Compression Techniques

Image Type	Compression Ratio	Traditional Compression PSNR (dB)	CNN Compression PSNR (dB)	Traditional Compression SSIM	CNN Compression SSIM
Natural Landscape	10:01	38.5	42.1	0.85	0.92
Portrait	8:01	35.7	39.8	0.8	0.88
Indoor Scene	12:01	40.3	44.2	0.87	0.94
Medical Imaging	6:01	30.2	34.9	0.75	0.83
Street Scene	9:01	37.1	41.6	0.82	0.89

Table 1 shows that the CNN model can achieve higher quality of image restoration than the classical method at the same compression ratio. In the case of portrait image, the PSNR (Peak Signal-to-Noise Ratio) of the classic method is 35.7 dB; the PSNR of the CNN compression method gets to 39.8 dB; the SSIM (Structural Similarity Index) also goes up from 0.80 to 0.88, indicating that the CNN model can retain details in the image and cause less deterioration in image quality. In complex images such as natural landscapes and medical images, the advantages of the CNN

method are also obvious, which can not only obtain a high compression ratio but also maintain high image quality.

To further improve the compression performance, this paper also adopts a quantization strategy. In the output layer of CNN, the amount of compressed data is further reduced by quantizing the features. The network's training process is not only accelerated, but the size of the compressed data is also cut down even more with this operation. Through quantization, the network can lower the network's bandwidth even more without losing image quality, hence, the image compression process is made more efficient.

In practical applications, the advantage of the CNN compression model lies in its high adaptability and flexibility, which dynamically adjust the compression strategy according to different types of images. In addition, due to its end-to-end training method, the CNN model automatically learns the optimal encoding and decoding methods during the compression and decompression process, without the need to manually set complex parameters, reducing the difficulty of model tuning. Thus, the CNN model is not only fit for the compression of still images but also adept at the video sequence compression necessities with remarkable versatility and scalability. The design of the model is made in such a way that it can be easily integrated into cloud-based processing and thus is prepared for handling larger datasets without dropping performance.

The CNN-based method of restoring images beats the conventional error correction techniques in conditions of high packet loss because of its capacity to learn intricate spatial and contextual features from images. CNN, unlike traditional techniques, which are based on fixed rules or interpolation, is capable of estimating the missing or damaged areas of an image by utilizing the patterns it has already learned during training. The model thus can successfully reconstruct the lost information, retain the overall form, and blend in the texture details, giving higher PSNR and SSIM values even in the case of extreme network packet loss. As a result, the CNN-based method offers stronger and more trusted CNN-based image restoration in a real high-loss transmission environment.

2.3 Intelligent Recovery during Transmission

During the image transmission process, due to factors such as network packet loss, transmission delay, and noise pollution, the image may suffer from partial data loss or image quality degradation. Traditional error repair techniques usually rely on redundant data and fixed error correction algorithms, but these methods are often limited in image quality recovery, especially in low-bandwidth or high compression conditions. To solve this problem, this paper uses a CNN-based image restoration method to effectively repair damaged images and reduce quality loss during transmission.

To be more precise, a CNN-based image restoration system which is to learn dynamically how to recover content from damaged or incomplete images during the transmission of the images has been constructed. The network takes as input a photo that got its part missing or was distorted by noise, and it then outputs an unblemished photo as the result of the restoration. In the course of the restoration, the CNN model takes advantage of its multi-level feature extraction and reconstruction powers to discover hidden spatial and semantic features of the damaged images and on the basis of these features predicts and reconstructs the parts that were missing.

The architecture of the CNN image restoration network starts with the convolution layer that is responsible for feature extraction of the image at both local and global levels. The convolution layer sorts out the information of texture, edges, and color distribution in the image, which is very important for getting a hold of the overall structure and local details of the image. In order to augment the network's restoration capabilities, the deep architecture of the network contains several convolutional layers and pooling layers that successively project the image from the original space to the latent space and capture high-level semantic information. The pooling operation in this process enables the network to lower the resolution of the image and thus concentrate on the high-level features of the image. This not only helps the network to retain important image information but also boosts the quality of the restored images during the whole restoration period.

To address the packet loss problem during transmission, the CNN restoration network uses an effective feature fusion mechanism and contextual information to predict the lost image parts. The Convolutional Neural Network (CNN) identifies the context structure in the image and infers the content of the missing area through the relationship between adjacent pixels. Especially in low-bandwidth and high-compression environments, the network infers the lost area from some known areas, thereby achieving higher-quality image restoration. This restoration model not only relies on intuitive information

in the image, but also supplements and restores the lost details by learning the potential patterns of the image. The restoration process is shown in Figure 2.

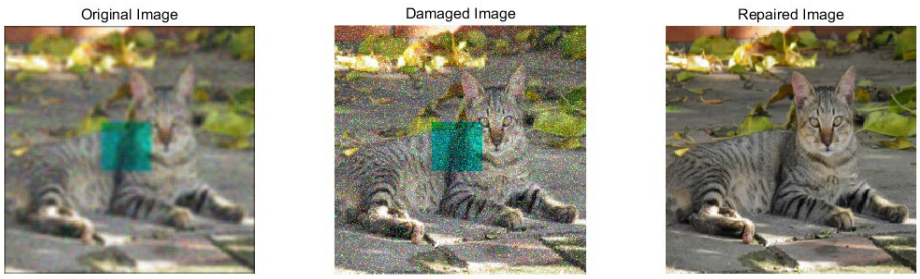

Figure 2. CNN image restoration process

To improve the restoration effect, the image restoration network in this paper adopts a residual learning strategy. Residual learning reduces the complexity of network training in the prediction process and improves the restoration accuracy. During the network training process, the residual block helps the network better learn the details of image restoration by calculating the residual information of the difference before and after image restoration. This method can quickly adapt to different types of damaged images with fewer training samples and improve the restoration effect.

Compared with traditional error restoration methods, the advantages of CNN image restoration networks lie in their powerful adaptive learning ability and efficient feature extraction ability. The CNN model automatically adjusts parameters through a large number of training samples and learns the best strategy for image restoration without relying on artificial feature design or redundant data. This makes this method show strong robustness and high-quality restoration capabilities in multiple types of damage and low-bandwidth environments. In addition, the restoration method based on deep learning also effectively handles complex problems such as noise pollution and image blur, significantly improving the visual quality of the restored image.

2.4 Simultaneous Optimization of Encryption and Compression

In traditional image encryption and compression methods, encryption and compression are usually independent and conflicting processes. Traditional encryption technologies, such as AES, based on symmetric encryption algorithms, often apply redundant data, resulting in low image compression efficiency. When compressing images, the lossy compression processing of image content by the compression algorithm may also affect the security and recoverability of the encrypted image. Therefore, how to effectively combine the two processes of encryption and compression to ensure the security of the image and optimize the compression effect has become an important research topic. This study applies a joint encryption and compression model based on deep learning, which aims to achieve simultaneous optimization of encryption and compression through the collaborative work of deep neural networks.

The core idea of the joint model is to simultaneously process the encryption and compression tasks of the image through a joint deep learning framework, thereby avoiding the mutual interference between encryption and compression in traditional methods. In terms of model design, the joint model mainly consists of two modules: an encryption module (based on GAN) and a compression module (based on CNN). These two modules work together under the same framework. Through the end-to-end training process, the encryption and compression processes cooperate with each other, thereby reducing the redundant data brought by encryption while ensuring the encryption strength and improving the compression efficiency.

First, in the encryption part, this paper uses a GAN for image encryption. GAN consists of a generator and a

discriminator, where the generator encrypts the input image into an invisible form, and the discriminator is used to determine whether the encrypted image is sufficiently concealed. Unlike traditional encryption algorithms, the Generative Adversarial Network (GAN) learns how to encrypt through a generative adversarial process, and by continuously optimizing the generator's capabilities, ensures that the generated encrypted image is visually difficult to distinguish from the original image, thereby improving the encryption security. During the training process, the error feedback from the discriminator guides the generator to improve the encryption strategy, so that the encrypted image has both high encryption strength and minimizes the redundant information generated during the encryption process.

The encrypted image usually contains a lot of redundant information, which affects the subsequent compression efficiency. To avoid this problem, this paper closely combines the image encryption process and the compression process. The compression module uses a Convolutional Neural Network (CNN) to adaptively learn image features and compress the image. In the traditional CNN compression method, the network extracts key features in the image through the encoder and reconstructs the image through the decoder. In the joint model, since the encrypted image may contain a lot of redundant information that is difficult to compress, the compression module needs to learn on the encrypted image and automatically adjust the compression strategy. Through end-to-end joint training, the CNN model learns how to process encrypted images and compress them efficiently, avoiding redundant information of encrypted images from interfering with the compression process, and ensuring a balance between compressed image quality and compression ratio.

The collaborative work of joint encryption and compression is optimized by sharing network weights. During the training process, the objective functions of the two modules are not optimized independently, but jointly optimized. Through the mutual influence between encryption and compression, the encryption and compression processes complement and promote each other. The output of the encryption module is used as the input of the compression module. After training, the compression module automatically adapts to the characteristics of the encrypted image and adjusts the compression strategy, thereby effectively reducing information loss during the compression process. In this way, the joint model minimizes the redundant data generated by the encryption process, while ensuring that the encrypted image still maintains a high compression effect when compressed.

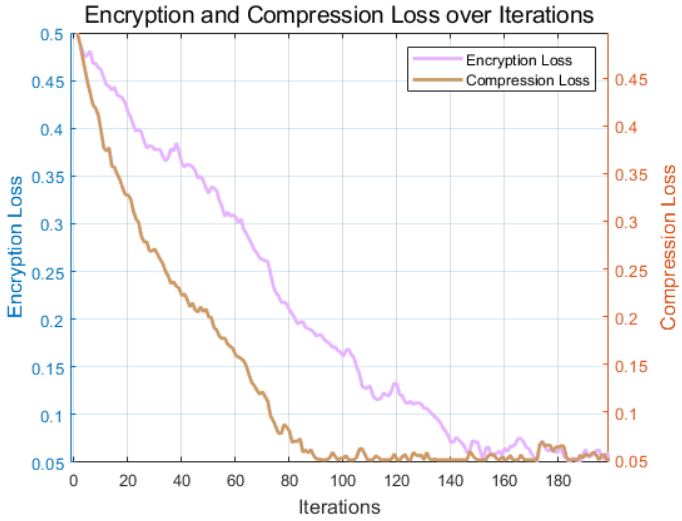

Figure 3. Encryption loss and compression loss

Figure 3 shows the change of encryption loss and compression loss with the number of iterations. In the early stage, the two loss values are high, indicating that the encryption and compression processes have not yet been effectively coordinated. The training progression shows that the errors in encryption and compression gradually reduced, revealing that the mutual optimization model gradually improves. The compression error gets down to

about 0.05 at the 90th iteration, and the encryption error stays more or less the same for 150 iterations, thus signalling that the compromise between encryption and compression has been tuned to perfection, which in turn means that the model has successfully discarded unnecessary data during training and yet has kept the large data compression ratio.

The joint model's benefit is that it employs the flexible deep learning capability to optimally carry out both the encryption and compression processes at the same time and does not stick to the strict encryption and compression strategies determined by traditional methods. The joint model is able to handle the data reduction with a great deal of certainty in terms of encryption security and image transmission quality in the case of low-bandwidth and high-compression ratio application scenarios. In addition, the joint training method avoids the conflict between encryption and compression, allowing the two to cooperate better, ultimately achieving the goal of both ensuring image security and improving transmission efficiency.

3. Performance Evaluation and Effect Verification

3.1 Encryption and Decryption Performance

Traditional encryption algorithms such as AES and RSA (Rivest-Shamir-Adleman) are secure, but the computational complexity is high, resulting in a long encryption and decryption process. This paper adopts an image encryption model based on a Generative Adversarial Network (GAN), and uses computational complexity and processing delay as evaluation indicators to analyze the efficiency of the model in the encryption and decryption process. GAN encrypts images through a generator, and the discriminator ensures encryption strength, but its encryption process consumes a lot of time. Compared with traditional methods, although the encryption time of the GAN model is longer, after parallel optimization, it can show higher encryption efficiency when processing large-scale image data. Although the decryption process has a high computational complexity, the decryption time is significantly reduced through optimized training and hardware acceleration to meet real-time requirements.

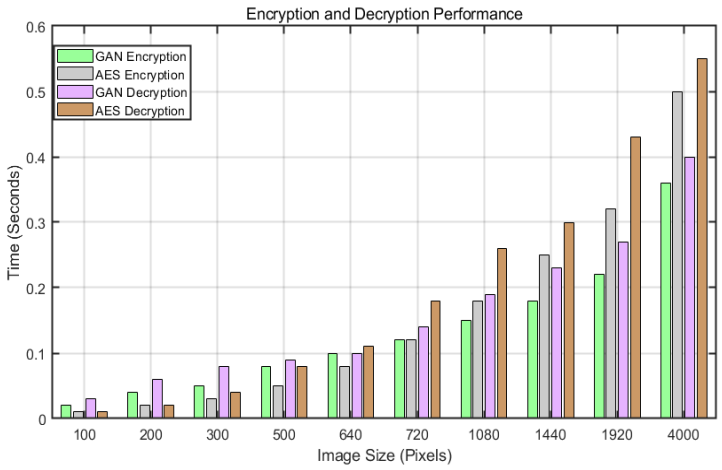

Figure 4. Performance comparison of GAN and AES encryption and decryption

Figure 4 shows the performance comparison of GAN and AES encryption and decryption in this paper under different image sizes. The data shows that as the image size increases, the time for all encryption and decryption processes increases. For a 100-pixel image, the GAN encryption time is 0.02 seconds, while the AES encryption time is only 0.01 seconds. However, when the image size reaches 4000 pixels, the GAN encryption time reaches 0.36 seconds, while the AES encryption time is 0.5 seconds. In the same decryption process, as the image size increases, the GAN encryption time gradually becomes smaller than the AES encryption time. This shows that when processing large images, although GAN provides stronger encryption security, the real-time requirements are better.

3.2 Image Restoration Quality

The image restoration quality is evaluated using PSNR and SSIM, which reflect the similarity between the restored image and the original image. Traditional error correction methods, such as Huffman coding and LDPC code (Low-Density Parity-Check Code), have limited recovery effects when packet loss is severe. In contrast, the restoration method based on a deep Convolutional Neural Network (CNN) can effectively repair lost information by adaptively learning image features, especially in low-bandwidth environments. Experimental results show that the deep learning method is significantly better than the traditional method in terms of PSNR and SSIM indicators, with higher quality of restored images, especially in packet loss environments.

Table 2. Comparison of packet loss rates

Loss Rate (%)	Method	PSNR (dB)	SSIM
0%	CNN	48.2	0.98
0%	Huffman Coding	43.5	0.95
0%	LDPC	42.8	0.94
5%	CNN	40.2	0.94
5%	Huffman Coding	36.5	0.89
5%	LDPC	35.2	0.88
10%	CNN	36.1	0.91
10%	Huffman Coding	32	0.84
10%	LDPC	30.5	0.82

Table 2 shows that the CNN-based image restoration method is superior to Huffman coding and LDPC code at different packet loss rates. When the packet loss rate is 0%, the PSNR of CNN is 48.2 dB, the SSIM is 0.98, and the restoration effect is close to the original image. As the packet loss rate increases to 10%, the PSNR of CNN drops to 36.1 dB, and the SSIM is 0.91, which still maintains a high quality. This shows that CNN can effectively restore images in a packet loss environment and has more advantages than traditional methods.

The CNN-based restoration model has better performance in high packet loss situations since it knows how to detect spatial patterns and contextual relationships from training images, thus allowing it to infer lost areas even in cases of large data loss. On the other hand, conventional error-correction techniques like Huffman and LDPC rely on

predetermined redundancy and get stuck when the loss is more than their correction capacity. The CNN network, through multi-level feature extraction, has reconstructed edges, textures, and semantic details more accurately, which has led to outstanding PSNR and SSIM performance even under extreme packet-loss conditions.

3.3 Transmission Efficiency

Image transmission efficiency is evaluated by compression ratio and transmission delay. Although traditional compression methods have advantages in compression ratio, the image quality is seriously degraded. The deep learning compression method adaptively learns key features through CNN, while ensuring high quality, improving compression ratio and transmission efficiency. Experimental results show that the CNN model achieves a higher compression ratio in a low-bandwidth environment and reduces transmission delay when restoring images, thereby improving overall transmission efficiency. Compared with traditional methods, deep learning compression technology significantly improves the real-time and stability of network transmission while ensuring image quality.

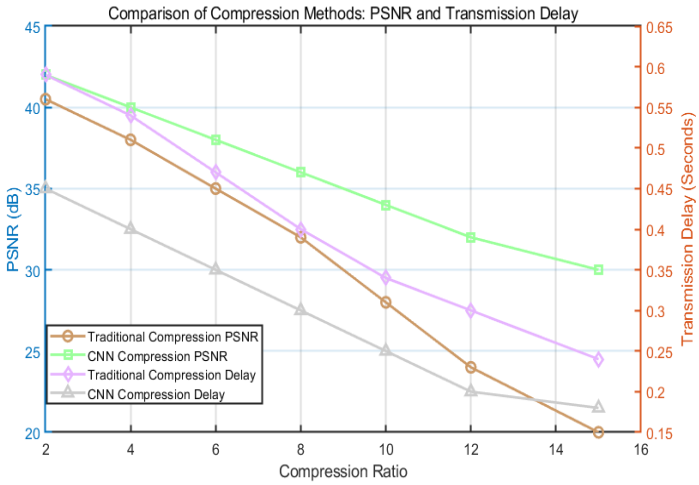

Figure 5. PSNR and transmission delay of traditional compression and CNN compression methods at different compression ratios

Figure 5 shows the PSNR and transmission delay of traditional compression and CNN compression methods at different compression ratios. The PSNR of the traditional method drops significantly at high compression ratios and drops to 20 dB when the compression ratio is 15, and the image quality is reduced. In contrast, the CNN method maintains a high PSNR with a compression ratio of 30 dB, showing better image quality. In terms of transmission delay, the CNN method performs better. When the compression ratio is 10, the delay of the traditional method is 0.34 seconds, while that of CNN is 0.25 seconds, indicating that the CNN method can more effectively improve the transmission efficiency in a low-bandwidth environment.

4. Conclusions

This paper applies an image security acquisition and efficient transmission algorithm based on deep learning and neural networks, which solves the shortcomings of traditional image encryption and compression methods in terms of efficiency and security. By combining GANs for image encryption and CNNs for image compression and recovery, this paper designs a joint model for simultaneous encryption and compression optimization. Experimental results show that the algorithm has significant advantages over traditional methods in terms of image encryption strength, recovery quality, compression ratio, and transmission efficiency, especially in low-bandwidth environments, effectively improving the stability and real-time performance of image transmission. The SIGANN-based extraction and classification framework suggested is naturally scalable for huge newspaper archives and high-throughput digital repositories. Its gel-like performance aids parallel processing and cloud-based deployment, hence it is applicable to environments having huge documents for ingestion, indexing, and retrieval. This placement not just corresponds to the area of scalable

information systems but also brings in automated, high-capacity text extraction and semantic processing in the ever-growing digital collections. However, this study still has certain limitations. For example, the computational complexity of the GAN encryption process is high, and the decryption process needs to be further optimized. Future research can further improve the real-time and adaptability of the model by improving model training efficiency, applying hardware acceleration, and enhancing the robustness of the algorithm. In addition, combining more practical application scenarios and exploring the performance of the algorithm in a variety of network environments is still a research direction worthy of further in-depth study. Every instance of the technical terms like Convolutional Neural Network (CNN) and Generative Adversarial Network (GAN) has been uniformly treated with the same capitalization in the entire manuscript.

Declarations

Funding
Guizhou Power Grid Science and Technology Project, research on an automatic verification platform for monitoring information of the distribution network based on Beidou positioning image push technology (GZKJXM20232355)

Conflict of Interest
The authors declare that they have no conflicts of interest regarding this work.

Data Availability
All data generated or analyzed during this study are included in the manuscript.

Author Contributions
All authors contributed to the design and methodology of this study, the assessment of the outcomes, and the writing of the manuscript.

References

[1] Paul RK, Misra D, Sen S, Chandran S. Optimization of microscopy image compression using convolutional neural networks and removal of artifacts by deep generative adversarial networks. Multimedia Tools and Applications. 2024;83(20):58961–58980.

[2] Wang Y, Wang F, Liu F, Zhang M. Securing content-based image retrieval on the cloud using generative models. Multimedia Tools and Applications. 2022;81(22):31219–31243.

[3] Liu Z, Xue R. Visual image encryption based on compressed sensing and Cycle-GAN. The Visual Computer. 2024;40(8):5857–5870.

[4] Neela KL, Kavitha V. Blockchain based chaotic deep GAN encryption scheme for securing medical images in a cloud environment. Applied Intelligence. 2023;53(4):4733–4747.

[5] Chai X, Tian Y, Gan Z, Chen Y. A robust compressed sensing image encryption algorithm based on GAN and CNN. Journal of Modern Optics. 2022;69(2):103–120.

[6] Fang P, Liu H, Wu C, Zhang Y. A block image encryption algorithm based on a hyperchaotic system and generative adversarial networks. Multimedia Tools and Applications. 2022;81(15):21811–21857.

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

[8] Wu J, Xia W, Zhu G, Zhang X. Image encryption based on adversarial neural cryptography and SHA controlled chaos. Journal of Modern Optics. 2021;68(8):409–418.

[9] Nagarajan H, Alagarsundaram P, Sitaraman SR, Alanda A. Enhanced RDH in encrypted image with high embedding efficiency using MSB prediction, matrix encoding, and separable CDM for non-volatile memory cloud services. International Journal of Advances in Computer Science & Engineering Research. 2025;1(1).

[10] Xu C, Sun W, Li M. DTT: A dual-domain transformer model for network intrusion detection. EAI Endorsed Transactions on Scalable Information Systems. 2024;11(6).

[11] Bhurani K, Dogra A, Agarwal P, Shrivastava P, Singh TP, Bhandwal M. Smart contracts for ensuring data integrity in cloud storage with blockchain. EAI Endorsed Transactions on Scalable Information Systems. 2024;11(6).

[12] Yin J, Hong W, Wang H, Cao J, Miao Y, Zhang Y. A compact vulnerability knowledge graph for risk assessment. ACM Transactions on Knowledge Discovery from Data. 2024;18(8):1–17.

[13] Ge YF, Wang H, Bertino E, Cao J, Zhang Y. Multiobjective privacy-preserving task assignment in spatial crowdsourcing. IEEE Transactions on Cybernetics. 2025.

[14] Liu X, Meng X, Wang Y, Zhang Y. Known-plaintext cryptanalysis for a computational-ghost-imaging cryptosystem via the Pix2Pix generative adversarial network. Optics Express. 2021;29(26):43860–

43874.
[15] Li Z, Zhang M, Liu J. Robust image steganography framework based on generative adversarial network. Journal of Electronic Imaging. 2021;30(2):023006.
[16] Li J, Li Y, Li J, Zhang Y. Single-pixel compressive optical image hiding based on conditional generative adversarial network. Optics Express. 2020;28(15):22992–23002.
[17] Chun D, Kim TS, Lee K, Kim CS. Compressed video restoration using a generative adversarial network for subjective quality enhancement. IEIE Transactions on Smart Processing & Computing. 2020;9(1):1–6.
[18] Goudjil A, Benyoucef A, Hamadouche MH, Riahla MA. Efficient DNA-based logistic mapping algorithm for color image encryption. EAI Endorsed Transactions on Scalable Information Systems. 2025;12(2).
[19] Chai X, Tian Y, Gan Z, Lu Y, Wu XJ, Long G. A robust compressed sensing image encryption algorithm based on GAN and CNN. Journal of Modern Optics. 2022;69(2):103–120.
[20] Cheng J, Wu J, Leng C, Wang Y, Hu Q. Quantized CNN: A unified approach to accelerate and compress convolutional networks. IEEE Transactions on Neural Networks and Learning Systems. 2017;29(10):4730–4743.
[21] Cheng J, Wu J, Leng C, Wang Y, Hu Q. Quantized CNN: A unified approach to accelerate and compress convolutional networks. IEEE Transactions on Neural Networks and Learning Systems. 2017;29(10):4730–4743.
[22] Mallick B, Parida P, Nayak C, Ali N, Panda MK, Prasad B, Palai G. Secure real-time transmission of multi-spectral satellite images inducing a 6D hyper-chaotic system and BB84 QKD protocol. Alexandria Engineering Journal. 2025;122:364–384.
[23] Khan PW, Byun Y. A blockchain-based secure image encryption scheme for the industrial Internet of Things. Entropy. 2020;22(2):175.