Image Information Hiding Processing Based on Deep Neural Network Algorithm

Zhe Zhang[1],*
School of Computer Science and Technology, Nanyang Normal University, Nanyang, Henan, 473061, China[1]

***Abstract*—In order to more effectively hide and extract image information, a deep neural network-based algorithm and computer-aided image information hiding method is proposed. The hardware design of the system includes the selection of the main control chip, the design of the parallel processing structure, and the design of the Ethernet communication circuit; Software design includes an image information hiding module, an image information extraction module, and a carrier image processing module. The operation of the image information processing system based on the reversible information hiding algorithm is realized through the system hardware and software design. The experimental results show that the carrier image processing degree of the design system is much higher than that of the traditional system, and the maximum value can reach 91%, indicating that the carrier image processing performance of the design system is better. The scheme proposed in this paper can improve the security of secret information while ensuring the quality of dense image. Follow-up studies will continue to explore the combination of adversarial learning and various traditional embedding algorithms to further improve the concealment of graph-hiding algorithms.**

Keywords—Image information hiding; neural networks; system design; image acquisition; information processing

I. Introduction

With the development of technology, people have entered the era of networking, informatization, and intelligence, and correspondingly, the requirements for various industries are also increasing. Visual information is the most direct carrier of human information, and images are the main manifestation of visual information. Images are an effective description of objective objects, mainly including their texture distribution, morphology, etc. Continuous image sequences also contain information such as the motion characteristics of objects. The combination of these information is an important basis for determining the category of objects. Therefore, image information processing has become an important research direction in the field of information processing today, and many scholars and experts have conducted in-depth research on it and achieved certain results [1-2]. At present, with the continuous improvement of the Internet and chip level, intelligent communication devices have become an important part of people's work and life, and also brought a variety of information security risks, such as personal sensitive information leakage caused by the low security transmission of information. Therefore, the research in the field of information security is of great significance. Information hiding technology is an important component of the field of information security. It mainly embeds secret information into multimedia carriers through information hiding algorithms, and the recipient extracts the secret information from the carrier through extraction algorithms [3]. Due to the insensitivity to modifications and pixel redundancy of images, they are currently widely used as hidden carriers and one of the main research directions.

In recent years, optoelectronic technology and integrated circuits have developed rapidly. Image information processing systems, which use image sensors as information acquisition methods and embedded hardware as acquisition and information processing units, have been widely applied in fields such as agriculture, military, transportation, and industry [4]. Traditional image information processing systems mainly use image sensors to obtain image information. Due to the small field of view angle of the sensors, low resolution, and limited information transmission, the image resolution is reduced, and there is significant distortion, which cannot clearly distinguish the details of the imaging target in the image. The development of network information technology has led to frequent leakage of image information, posing information risks. Traditional image steganography algorithms often rely on manually designed distortion cost functions, which are complex and highly specific. Once features are discovered, they will completely lose their security advantages, resulting in high maintenance costs for traditional image steganography algorithms. The main principle of traditional image steganography algorithms is to calculate the impact of each pixel modification on overall distortion, in order to find the optimal embedding position, reduce the modification of the carrier image by secret information, and achieve the goal of confusing the public [5]. Common methods include statistical histogram steganography and dual communication code steganography. The difference between these two types of algorithms lies in the different ways in which redundant information is filtered. Combined with the visual difference vulnerability of adjacent colors in the same color gamut of the human eye, the modification of the carrier image can be ignored when observed by the human eye. The former achieves steganography by transforming the image pixel matrix into redundant statistics that can be filtered out by histograms in different transformation domains; The latter uses the adjoint error correction code mechanism in reverse to define the encrypted carrier as a disturbed channel. Through the communication code error correction mechanism, the encrypted carrier is corrected back to the original carrier to extract secret messages. However, these schemes all have obvious specificity features. With the increasing maturity of deep learning technology in recent years, the above algorithms have limited ability to resist data-driven deep steganalysis [6].

*Corresponding author

II. Literature Review

Advancements in information technology and hardware have led to remarkable increases in computer processing capabilities. Consequently, deep learning, which heavily relies on substantial computing power, has garnered significant attention in research circles. Convolutional Neural Networks (CNNs) have emerged as a prominent tool in machine vision, yielding impressive achievements and widespread adoption in various applications [7]. Object detection serves as the cornerstone for a multitude of advanced visual tasks, including image semantic segmentation, instance segmentation, image annotation, and video comprehension. Its importance cannot be overstated, as it lays the groundwork for complex visual tasks like image scene recognition and content comprehension. Moreover, it plays a pivotal role in constructing image retrieval systems, facial recognition, object identification, pedestrian detection, video surveillance, and facilitating advancements in autonomous driving technology [8]. Information hiding technology is a method of hiding secret information in multimedia information. Images are the most suitable data carrier for information hiding. The main methods of information hiding include digital watermarking technology, steganography, etc. Information hiding can be divided into lossy information hiding and reversible information hiding techniques, with the difference being whether the receiving end can recover the carrier without distortion. Lossy information hiding technology can be applied to copyright protection scenarios of multimedia data, and the receiver cannot fully recover the carrier after extracting secret data. Reversible information hiding can be applied to the illegal tampering of multimedia data, which can verify its integrity and restore it without loss, such as medical diagnostic information. After extracting secret information at the receiving end, the carrier can be restored without distortion.

Lai et al. proposed method, a generative image steganalysis algorithm is introduced, leveraging a focused feedback residual convolutional neural network. This approach enables the simultaneous detection and extraction of concealed information within images. Initially, a preprocessing network, comprising multiple convolutional layers and two novel focus modules, is employed to preprocess candidate stego images, producing enhanced feature maps. Subsequently, these enhanced feature maps are fed into both the classification network and the reconstruction network [9]. Khan, A. A. and others introduced a steganography technique utilizing the least significant bit (LSB) method to conceal secret data within an original image. Initially, lightweight stream encryption cryptography encrypts the confidential information within the cover image, safeguarding it throughout transmission from source to destination. The encrypted cover data is then embedded into the carrier of the steganographic image, employing the LSB technique for transmission [10]. Jun, M. et al. introduced an innovative dual-stream convolutional neural network tailored for single image dehazing. This network architecture comprises two distinct flows: the spatial information feature flow and the high-level semantic feature flow. The spatial information feature flow focuses on retaining intricate details within the dehazed image, while the high-level semantic feature flow specializes in extracting multi-scale structural features from the dehazed image [11].

Image encryption and information hiding are research directions for protecting information security. Cryptography ensures the security of data content through encryption. Information hiding technology verifies the integrity of multimedia data by embedding secret data. The reversible information hiding of encrypted images can play a dual role in ensuring information security during data processing. Encryption protects the content of image data, while embedded secret data can monitor whether multimedia data has been tampered with during transmission after decryption, verify its integrity, and achieve lossless recovery of the original carrier. It can be applied in scenarios such as remote medical diagnosis, encrypted data annotation in cloud environments, and digital forensics in the judiciary. In order to solve the problems existing in traditional systems, the author designs a reversible image information hiding system, applies reversible information hiding algorithms to image information processing systems, improves image processing speed and transmission speed, and ensures the security of image information processing.

III. Method

A. Hardware Design of Image Information Processing System

The system hardware mainly includes the selection of the main control chip, the design of parallel processing structure, and the design of Ethernet communication circuit. The specific design process is as follows:

1) Selection of main control chip: The main control chip adopts an FPGA chip, which is the core of image information processing and has the advantages of fast processing speed, simple operation structure, and large amount of data involved. The performance of the FPGA chip determines the effectiveness of image information processing. After research and comparison, it was found that the XC5VLX110T chip produced by Xilix Company was chosen. The XC5VLX110T chip has 110000 equivalent logic units, 16 transceivers, 64 DSP48E logic chips, 5328Kb ARM, and six clocks [12].

2) Parallel processing architecture design: Parallel processing is mainly implemented by buses, therefore, the design of parallel processing architecture mainly involves designing bus interfaces. The system bus interface connection diagram is shown in Fig. 1.

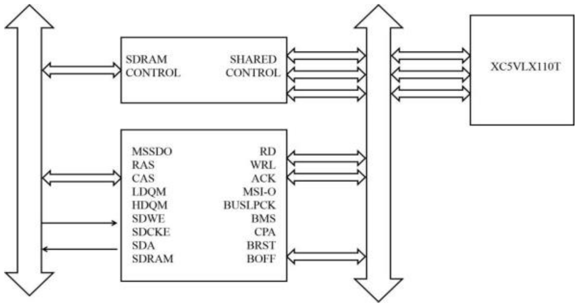

Fig. 1. Bus interface connection diagram.

The bus interface has multiple pins, as defined in Table I.

TABLE I. DEFINITION OF BUS PINS

grouping	types	Describe
External port bus control	I/O	Burst
	O	Host space chip selection signal
	O	Memory selection
	I/O	Response
External port arbitration	I	Revoke
	O	Bus lock indication
	I/O	Kernel Access Priority
	I	Host bus grant
External port DMA/Flyby	I	DMA request pin
	O	I/O read
	O	I/O device output enable
	O	I/O write

3) Ethernet communication circuit design: The image information processing system requires good network communication support. In order to design an Ethernet communication circuit, the independent interface of the processor needs to be connected to the Ethernet transceiver, and the IEEE802.3 network transmission protocol needs to be set. The circuit should be set to work mode to ensure the normal operation of the image information processing system.

The design diagram of the Ethernet communication circuit is shown in Fig. 2.

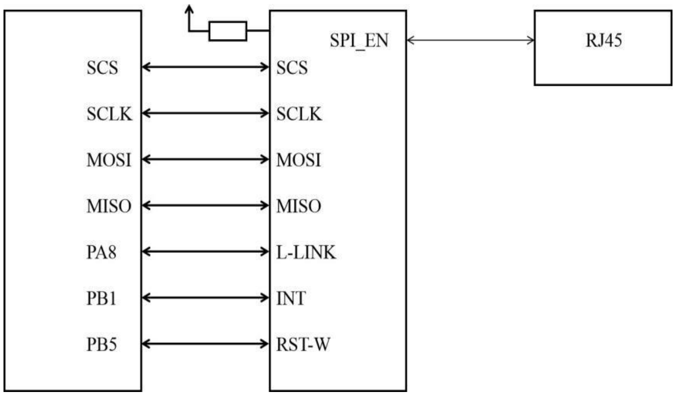

Fig. 2. Ethernet communication circuit design diagram.

The above process has completed the design of the system hardware, providing hardware support for the following system software design.

B. Software Design of Image Information Processing System

The system software mainly includes an image information hiding module, an image information extraction module, and a carrier image processing module. The specific design process is as follows:

1) Image information hiding module: The image information hiding module mainly uses reversible information hiding algorithms to hide image information, achieving the goal of protecting image information. Firstly, the carrier image is divided into non overlapping blocks, with a block size of 2 × 2. Secondly, each image block is processed sequentially, paying attention to hiding image information. The specific steps for hiding image information are as follows:

Step 1: Generate a reference matrix of 256 x 256 based on n x n matrix blocks, with n optional values including 4, 8, 16, and 32.

Step 2: The image block mainly consists of 4 pixels, denoted as $C(i,j)$， $C(i,j+1)$， $C(i+1,j)$, and $C(i+1,j+1)$. Construct them into three pixel pairs and convert them into planar coordinate points, denoted as $P_1(C(i,j)，C(i,j+1))$, $P_2(C(i,j)，C(i+1,j))$, and $P_3(C(i,j)，C(i+1,j+1))$. Among them: $C(i,j)$ represents the pixels of the carrier image; $C(i,j+1)$， $C(i+1,j)$, and $C(i+1,j+1)$ represent the pixels obtained by interpolation calculation.

Step 3: Convert the reference matrix into a planar region, map P_1, P_2, and P_3 to the reference matrix, and find the corresponding coordinate positions.

Step 4: Scan in the left and right directions with P_1 as the center in the reference matrix. Form a pixel group G with n scanned pixels, convert their information into hidden information using decimal, find the corresponding position in G, replace the vertical coordinate of P_1 point, and complete the information hiding of P_1 point.

Step 5: Process P_2 and P_3 information according to the method in Step 4, and complete the hiding of P_2 and P_3 information.

Step 6: Repeat steps 2 to 5 until all image information is hidden.

2) Image information extraction module: Based on the hidden images mentioned above, embed a decoding program to extract image information. The specific process is shown below.

The decoding program refers to the decoding algorithm of reversible information hiding algorithms, which converts hidden information into raw information and extracts it [13-14]. Under normal circumstances, only personnel with image ownership rights can have decoding programs, and outsiders cannot extract image information. This can greatly ensure the security of image information and avoid the harm caused by image information leakage. The decoding key is mainly represented by k_1 and k_2, and the image information extraction process is shown in Fig. 3.

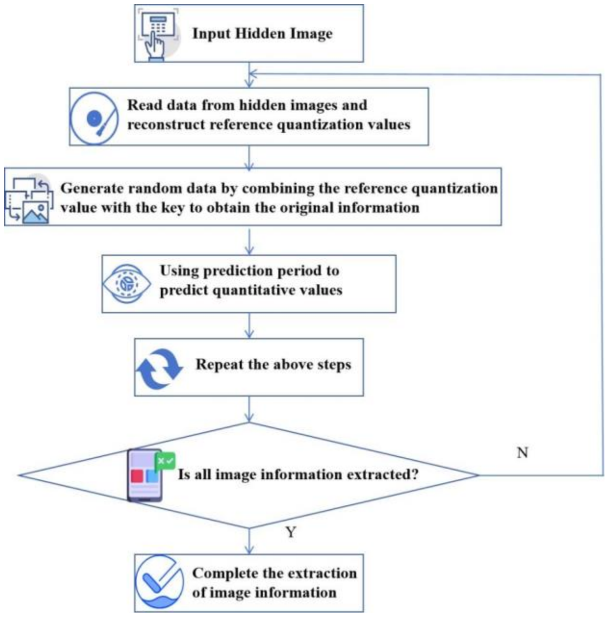
Input Hidden Image
Read data from hidden images and reconstruct reference quantization values
Generate random data by combining the reference quantization value with the key to obtain the original information
Using prediction period to predict quantitative values
Repeat the above steps
Is all image information extracted?
N
Y
Complete the extraction of image information

Fig. 3. Image information extraction process diagram.

3) Carrier image processing module: After extracting image information, it is necessary to process the carrier image, which is the inverse process of image information hiding. The specific program is shown in Fig. 4.

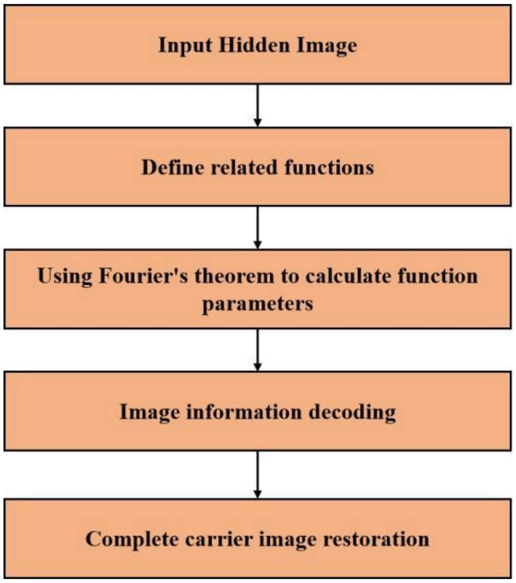
Input Hidden Image
Define related functions
Using Fourier's theorem to calculate function parameters
Image information decoding
Complete carrier image restoration

Fig. 4. Carrier image processing program diagram.

The carrier image processing function is represented as:

$$H = \sum_{i=1}^{n} \alpha k_1 * \beta k_2 \tag{1}$$

In the formula α, β represents the carrier image processing parameters.

Through the design of the hardware and software of the above system, the operation of an image information processing system based on reversible information hiding algorithm has been achieved, providing more effective support for image information security.

C. Similarity of Semantic Information

By applying probability functions to analyze the similarity of semantic information between images, propose image and semantic sets for a given query image.

The representation method for image sets:

$$I = \{I_1,\ I_2,\ \cdots I_n\} \tag{2}$$

The representation method of semantic sets:

$$X = \{x_1,\ x_2,\ \cdots x_m\} \tag{3}$$

Based on the given set expansion analysis, when the image I_i has semantic x_j, it can be represented by $x_j(I_i) \in \{0,\ 1\}$. In order to further clarify the similarity between the two images, it is necessary to measure the distance between the indicator functions. There is a relationship where the decrease in this value leads to an increase in similarity. The categories of natural semantic information are diverse and have significant uncertainty, so even with the same semantics, there may be multiple categories. Considering this situation, a probability based semantic level information similarity method is adopted. Assuming that I_i has semantic x_j, it is represented by $p = \left(x_j(I_i) = 1|I_i\right)$. This can further clarify the semantic labels of the image, specifically:

$$x_j:\ max_{xj} p = \left(x_j(I_i) = 1|I_i\right) \tag{4}$$

The query image I_q maintains a relatively independent relationship with the dataset image I_i. Under this condition, there is $p = \left(I_q,\ I_i|x_j\right) = p\left(I_q|x_j\right)\left(I_i|x_j\right)$. Based on the image I_q and I_i, the correlation features of the image can be obtained through joint probability, which can be expressed as follows:

$$p = \left(I_q I_i\right) = \sum_{x_j \in X} p\left(I_q,\ I_i|x_j\right) = \sum_{x_j \in X} p\left(I_q|x_j\right) p\left(I_i|x_j\right) p\left(x_j\right) \tag{5}$$

In addition, considering the development needs of scalability, a matrix $\Lambda = I \times X$ is introduced to conduct calculations and analysis, exploring the correlation between two images. If the joint distribution of the images exceeds the cutoff threshold t, it is reasonable to indicate that there is correlation between the two images:

$$\Lambda = \left(I_q I_i\right) = p\left(I_q I_i\right) \geq t \tag{6}$$

On the contrary, it indicates that the two are not related. By applying the probability function of semantics between images, it is possible to effectively determine the semantic correlation of images. If the threshold is exceeded, it indicates significant semantic correlation, otherwise there is no significant correlation [15].

D. System Implementation Process

Write a reversible image information hiding system using callable functions to achieve image information hiding processing. The image information hiding system based on reversibility uses FIFO memory to collect image information, applies grayscale stretching processing to the image, threshold segmentation processing to the image after stretching processing, and uses ARM processor to hide image information through reversible information hiding algorithm. After reverse operation, the hidden image information is extracted and output to achieve image information processing in the image information processing system [16].

E. Data Communication Module

The image data transmission is achieved through a data communication module, which can achieve multi chip communication. The data communication of the image information processing system is achieved through Ethernet data transmission interface and high-speed serial interface. The data communication module utilizes PCI interface to achieve information exchange between the image information processing system and the computer. The PCI interface is the data exchange and control center of the system hardware, which receives commands and data from the image information processing system and various device drivers through the communication interface module. The communication interface module completes the coordination work of various modules in the system, achieving system image information processing. The PCI communication interface module sends the collected image information and system processed data to a general-purpose PC using the PCI bus, and selects PLX's PCI9030 as the interface chip of the communication data module [17].

IV. Results and Discussion

A. Experimental Analysis

The experiment mainly uses Ethernet communication, and in order to ensure the smooth progress of the experiment, the experimental network is tested. After testing, the changes in Ethernet traffic are shown in Fig. 5. The significant changes in traffic indicate that Ethernet communication is normal and effective.

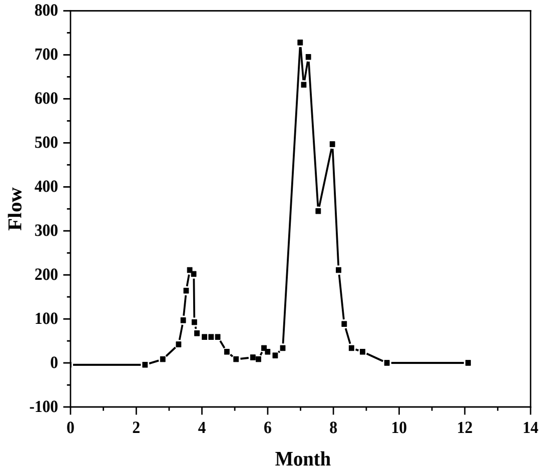

Fig. 5. Changes in Ethernet traffic.

B. Analysis of Experimental Results

The comparison of carrier image processing levels obtained through experiments is shown in Table II.

TABLE II. Comparison of Carrier Image Processing Levels %

Number of experiments	Traditional systems	design system
10	45	66
20	40	68
30	41	67
40	39	70
50	50	72
60	50	73
70	53	76
80	50	78
90	39	88
100	41	91

As shown in Table II, the carrier image processing level of the designed system is much higher than that of traditional systems, with a maximum value of 91%, indicating that the carrier image processing performance of the designed system is better [18]. The experimental results show that compared with traditional image information processing systems, the image information processing system designed by the author greatly improves the processing performance of carrier images, fully demonstrating that the designed image information processing system has better processing effects.

V. Conclusion

The author proposes an image information hiding processing based on deep neural network algorithms. Image information processing is an extremely important part of the field of image processing. The proposed solution can improve the security of secret information while ensuring the quality of encrypted images. Design a reversible image information hiding system and apply the reversible information hiding algorithm to the image information processing system. Through experimental results, it has been verified that using this system to process image information can achieve high image information processing efficiency at a lower cost, and has good processing performance, which can be applied to practical processing requirements of different types of image information.

References

[1] Liu X .Analysis on the Development of Cigarette Packaging in the Era of Intelligence[J]. Electronic Research and Applications, 2023, 7(3):1-6.

[2] Ballesteros, M. , & Garro, G. . (2022). A model and a numerical scheme for the description of distribution and abundance of individuals. Journal of Mathematical Biology, 85(4), 1-37.

[3] FengXU, XiaopengYANG, & YiZHAO. (2022). Beamspace mimo radar tensor modeling and 2-d doa estimation. Journal of Signal Processing, 38(1), 1-8.

[4] Liu, D. , Chen, N. , Song, Y. , Song, X. , Sun, J. , & Tan, C. , et al. (2023). Mechanical and heat transfer properties of aln/cu joints based on nanosecond laser-induced metallization. Journal of the European Ceramic Society, 43(5), 1897-1903.

[5] Zhou, L. , Zhigao, L. U. , You, W. , & Fang, X. . (2023). Reversible data hiding using a transformer predictor and an adaptive embedding

strategy. Frontiers of Information Technology & Electronic Engineering, 24(8), 1143-1155.

[6] Zhang, Q. , Jiang, N. , Zhang, Y. , Li, A. , Xiong, H. , & Hu, G. , et al. (2024). On-chip spiking neural networks based on add-drop ring microresonators and electrically reconfigurable phase-change material photonic switches. Photonics Research, 12(4), 755.

[7] LI Shanhai, WU Yanxiong, WANG Bei, XU Yan, & LIU Yulong. (2022). Prediction of enterprise growth in information technology listed campanies based on ga-bp network. Journal of Systems Science and Mathematical Sciences, 42(4), 854-866.

[8] Gupta, S. , & Garg, N. K. . (2023). Data hiding in the optimal keyframes using circular shifting and mutation operations for improvement in imperceptibility. International Journal of Information and Computer Security, 20(1/2), 158.

[9] Lai, Z. , Zhu, X. , & Wu, J. . (2022). Generative focused feedback residual networks for image steganalysis and hidden information reconstruction. Applied Soft Computing, 39(1), 14-27.

[10] Khan, A. A. , Shaikh, A. A. , Cheikhrouhou, O. , Laghari, A. A. , Rashid, M. , & Shafiq, M. , et al. (2022). Img-forensics: multimedia-enabled information hiding investigation using convolutional neural network. IET image processing,13(11), 3543-3554.

[11] Jun, M. , Yuanyuan, L. , Huahua, L. , & You, M. . (2022). Single-image dehazing based on two-stream convolutional neural network. Journal of Artificial Intelligence Technology (English), 82(3), 3459-3484.

[12] Sahin, M. E. . (2023). Image processing and machine learning-based bone fracture detection and classification using x-ray images. International Journal of Imaging Systems and Technology, 33(3), 853-865.

[13] Nagai, S. , & Tomioka, A. . (2022). Information needs of adolescent with cancer who returning to social life. Journal of AYA Oncology Alliance, 2(1), 8-15.

[14] Guy, T. S. , & Edwards, K. . (2022). Military-civilian cardiothoracic surgery affiliations: a potential solution for low clinical volume in military medical facilities. The Annals of thoracic surgery, 114(3), 625.

[15] Jayasekara, S. , Karunasekera, S. , & Harwood, A. . (2022). Optimizing checkpoint-based fault-tolerance in distributed stream processing systems: theory to practice. Software: Practice and Experience, 52(1), 296-315.

[16] Lilian, H. , Yi, S. , Jianhong, X. , & Linyu, W. . (2022). Image encryption based on a novel memristive chaotic system,grain-128a algorithm and dynamic pixel masking. Systems Engineering and Electronic Technology: English Version, 33(3), 17.

[17] Gao, Z. , Deng, Z. , Zhang, L. , Gao, X. , An, Y. , & Wang, A. , et al. (2024). 10 gb/s classical secure key distribution based on temporal steganography and private chaotic phase scrambling. Photonics Research, 12(2), 321.

[18] Rahman, Z. , Yi, X. , Billah, M. , Sumi, M. , & Anwar, A. . (2022). Enhancing aes using chaos and logistic map-based key generation technique for securing iot-based smart home. Electronics, 11(7), 1083.