Journal of Combinatorial Mathematics
and Combinatorial Computing
www.combinatorialpress.com/jcmcc

Application of Generative Adversarial Networks' Image Information Security Encryption Algorithm in the Behavior Management of Prison Inmates

Fei Gao[1,] ✉

[1] *Department of Information Technology, Henan Judicial Police Vocational College, Zhengzhou, Henan, 450046, China*

ABSTRACT

With the global informationization boom, information security has become a problem for all of us. In order to be able to effectively detect the physical health status of criminals in prison and ensure the data security of the process, an image encryption method is designed to effectively protect the monitoring information. The process is based on generative adversarial network with generator and discriminator for image generation and data discrimination processing respectively, and optimizes the feature transmission process of image with the help of residual network. The key is generated by chaotic sequence method during the image transmission process. The encrypted image is transmitted to the staff port and the destination image is obtained after the decryption process of data key. The results of the study indicated that the decryption accuracy of the GAN algorithm in the dataset test increases gradually with the iteration process. The accuracy of the image after the completion of the iteration reached 98.69%, indicating that the algorithm has a good restoration effect for recovering the image after transmission. The structural similarity of the data image after the GAN algorithm processing decryption can reach 0.988. The peak signal-to-noise ratio index of the image was 37.78dB, which indicates that the clarity of the image after encrypted transmission is high. The research method can provide an effective theoretical support for the encrypted transmission of video images.

Keywords: Information Security, Health States, Generative Adversarial Networks, Diffusion encryption, Residual Networks

1. Introduction

Prisons, as the state's penal enforcement organs, bear the important tasks of correctly enforcing penalties, punishing and reforming criminals, and preventing and reducing crime, so it is very important to maintain the continued safety and stability of prison supervision. Currently, with the

✉ Corresponding author.
E-mail address: Gaofeifeii0@163.com (F. Gao).
Received 01 March 2024; Revised 25 May 2024; Accepted 10 November 2024; Published Online 16 April 2025.
DOI: 10.61091/jcmcc127b-402

popularity of high-definition monitoring and supervision needs, the explosive growth of the amount of data in the field of security monitoring has given rise to the demand for intelligent technology, which requires the establishment of modern management concepts, the establishment of a scientific and effective management system, mechanism, standardization of prisons, refinement of the management, is the construction of a safe, civilized, modernized, intelligent prisons is an important guarantee [1-4]. Over the years, with the continued promotion of judicial informationization, intelligent construction and the requirements of multi-level networking for judicial security systems, security products and systems have been popularized in the field of prisons, prisons have basically established a comprehensive management of security, but in the process of the establishment of the management program, the level of security construction in prisons around the world varies [5-7]. Moreover, Tahamont [8] utilized a breakpoint regression design to assess the relationship between prison security level and violation reports from inmates, and the number of violation reports was higher at the high security level than at the medium security level. Therefore, it is urgent to strengthen the security level of prisons.

As prison informatization enters the fast track of development, each functional department puts forward higher requirements for prison security systems in terms of work safety prevention, risk assessment and internal control management. However, the existing information resources are only limited to the internal prison, lack of human, physical and technical defense, multi-channel, multi-various types of big data risk analysis and control, not to mention that it can not be shared with the higher management [9-11]. And the most important point is that, due to the intelligent and informatized nature, the system data is prone to forgery, tampering, leakage and other attacks, such as AI face change and other deep counterfeiting techniques to tamper with the monitoring screen and fake the monitoring scene, which causes misjudgment events by the prison guards and panic in the prison management [12-13]. In addition, the existing encryption strategy can not simultaneously meet the encryption security and decoding speed and execution speed, the availability and confidentiality contradiction is aggravated, it is difficult to realize the overall data encryption, and the encryption randomness and key space is insufficient [14-15]. It can be seen that the traditional information management and encryption technology needs to be optimized.

AES is the current commonly used traditional encryption algorithm, Andriani et al [16] compared the performance of AES-128, AES-192 and AES-256 algorithms, compared with the other two algorithms, the processing time of AES-128 is shorter, and the CPU utilization of AES-192 is shorter, following the increase of its key length, the security and complexity of the encryption algorithm also increases Gaur and Kaushik [17] designed an encryption method for Advanced Encryption Standard (AES) with images as input and output objects, which is effective in encrypting image data. Generative Adversarial Network (GAN) is a machine learning based generative model, which is innovative in that it shows excellent performance when used for tasks such as image synthesis, image editing, and image super-resolution reconstruction through the training of two mutually adversarial neural networks [18].

Generative Adversarial Networks (GANs) are used for encryption algorithms, which bring a larger key space for encryption algorithms. Therefore, Fang et al [19] developed a new chunked image encryption algorithm with larger key space, which was mainly designed by using GAN and newly designed hyper chaotic system.Man et al [20] formulated a random number generator by using Least Squares GAN in order to solve the problem of imbalance in the number and speed of random keys in chaotic system. Wang [21] designed an image encryption algorithm by GAN and DNA dynamic coding, GAN is learning and training the random key generated by chaotic system and DNA dynamic coding is transforming the random key.Dai et al [22] fused four methods to improve the GAN and formulated a composite loss function consisting of five loss functions and designed a two-stage chaotic system with two-stage confusion operation and in this way achieved double image encryption.Liu et al [23] designed residual self-attention mechanism-GAN by combining Wasserstein GAN and loss function

and this network was used to design color image encryption algorithm to solve randomness and security.

2. Methods and Materials

2.1. GAN Based Image Encryption Algorithm Design

With the rapid development of today's society, information technology has become a global trend. In order to be able to effectively monitor the physical condition of prison offenders, the state of offenders is usually observed by surveillance to identify whether there are any health abnormalities in offenders. The image information generated during the process is only viewed by prison staff, so the information used to observe the images needs to be encrypted to ensure the security of the information. GAN as a class of adversarial training class of deep learning algorithms can effectively deal with image data, and at the same time can be used for image information security processing. Image information security is mainly carried out by means of encryption and concealment. The principle of GAN recognition of image samples is shown in Figure 1.

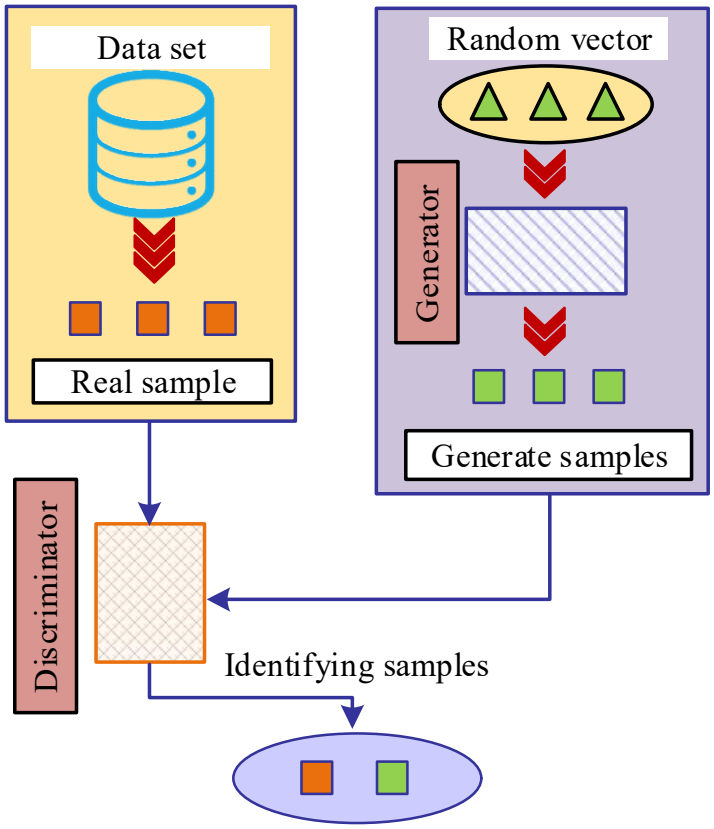

Fig. 1. Generative Adversarial Network

In Figure 1 it is shown that the GAN trains the generator with inputs of random variables so that the generator produces a set of trained spurious samples. The discriminator, on the other hand, discriminates between true and false samples by extracting the correct samples from the real dataset. The discriminative feedback of the samples strengthens the generator's generative ability and the discriminator's discriminative ability, and accurately determines the truth and falsity of the image samples. The game length of the GAN training process depends on whether the generator's false samples can fool the discriminator's judgment. The discrimination process is shown in Equation (1).

$$\begin{cases} \min\limits_{G}\max\limits_{D} V(D,G) = E_{x\sim P_{data}}\left[\log D(x)\right] \\ +E_{x\sim P_{data}}\left[\log\left(1-D\left(G(z)\right)\right)\right] \end{cases} \tag{1}$$

In Equation (1), D denotes the discriminator in GAN and G denotes the generator in GAN. x denotes the true data in GAN and P_{data} denotes the distribution of true data in GAN. z denotes the fake data generated by the generator, and P_z denotes the distribution for the generated sample data. E denotes for the expected value in GAN. The iterative process of GAN on image data is mainly implemented through the convolutional neural network layer, which nonlinearizes the algorithm through the activation function and strengthens the algorithm's feature extraction capability with the iterative learning process. The pooling process amplifies the feature saliency of the image through a numerical retention process to ensure the accuracy of the received surveillance images. In order to optimize the image stability of the network process, residual network is added to the transmission process, and the working process of residual is shown in Figure 2.

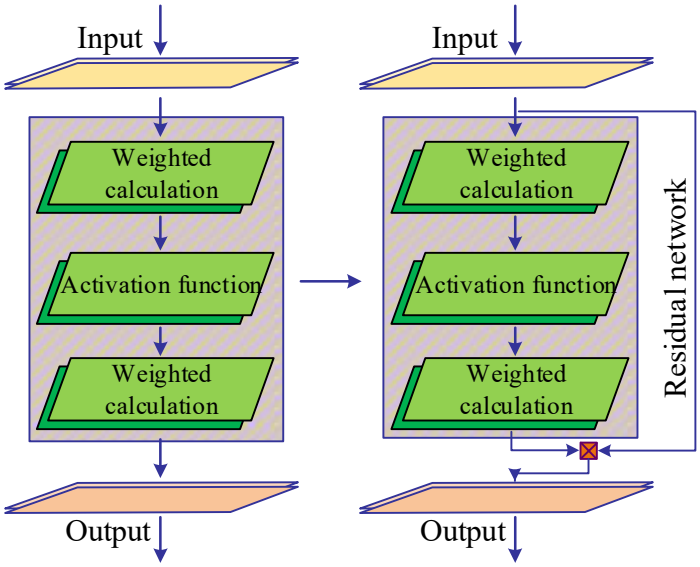

Fig. 2. Residual Network

In Figure 2, the network structure with the inclusion of residual blocks connects the input and output of the network. The GAN network model optimized by residual network is able to avoid the feature degradation problem caused by too deep network layers, and effectively reduces the missing data of features in the transmission process. The encryption process of GAN builds the base of the model module with an autoencoder. The data is encoded to transform the received input vectors and the data is hidden inside the encoder. The process associates the input vectors with the hidden vectors through weight reconstruction. The loss minimization reconstruction method is attempted through iterative learning to achieve the transformation and transmission of the dynamic information of the image. Asymmetric encryption is used for image processing. The encrypted content is data hidden so that only commands with a decryption password can view the real data transmitted from the image. The specific image encryption method is shown in Figure 3.

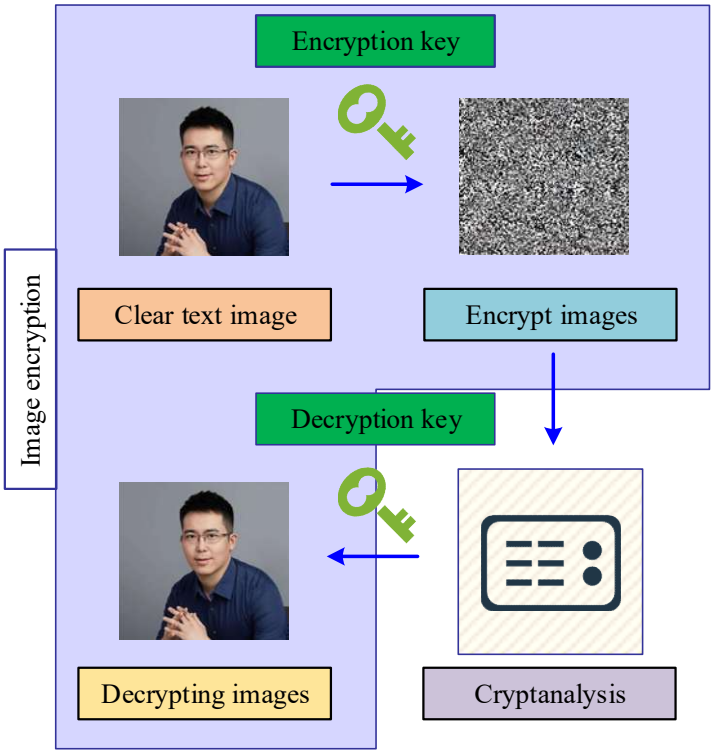

Fig. 3. Image Encryption Process

In Figure 3, the transmitted plaintext image is exposed in the network without encryption. The image data is hidden by encryption, and what is presented in the network is the processed ciphertext image. The encrypted image reduces the risk of exposure during transmission. The decryption passphrase is synchronized to the staff member in order to allow the staff member who receives the image to view the surveillance image. The staff member can open the real surveillance image with the correct passphrase.

2.2. Construction of GAN Encryption Algorithm with Chaotic Encryption Algorithm Module Included

Image data contains more information than text data in the actual process, and image data is very easy to be exposed in the network, so it is more important to have a sense of confidentiality for image management in some non-public places. The main content of prison images is to monitor the behavioral changes and physical health status of criminals. Therefore the network model also needs to ensure the real-time and integrity of the image information in the encryption process. The encryption process generates chaotic sequences with chaotic image encryption and diffusion encrypts the image through logical relations. The GAN encryption method by adding the chaotic system module can optimize the encryption strength of the image. The dual encryption parameter setting of chaotic system extends the space of cipher text and sparsely connects the transmitted image with wavelet transform method which reduces the amount of computation in the network process. The parameter setting of chaotic sequence in the system is shown in Equation (2).

$$x_{i+1} = a x_i \left(1 - x_i\right) \tag{2}$$

In Equation (2), x_{i+1} denotes as the newly generated chaotic system. x_i denotes as the initial value of the system. a denotes as the chaotic control parameters. Chaotic systems take values between 0 and 1. The limitation of the chaotic parameters on the values of the chaotic system results in the generation of chaotic sequences as a set of discontinuous distribution values. To ensure the generation of chaotic sequences arranged in a uniform structure, the study optimizes the computation of the chaotic system by taking the mode operator function, and the optimization process improves

the processing performance of the chaotic system by expanding the parameter range. As the processing process of plaintext image is to cover the ciphertext image with small regions of altered values by diffusion obfuscation in order to achieve the purpose of graphical information hiding. To avoid the obfuscation way of the obfuscation process of GAN network is captured, the depth of the encryption method is strengthened with diffusion algorithm, and the specific process is shown in Figure 4.

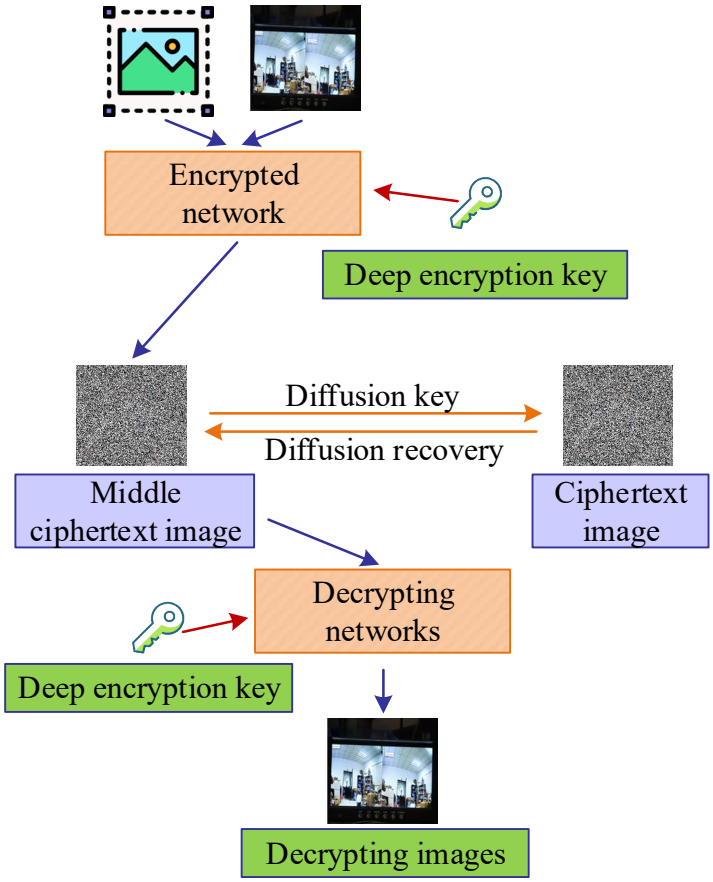

Fig. 4. Image Depth Encryption

In Figure 4, the random image and the ciphertext image are simultaneously processed by an encryption network, and a set of deep encryption keys are set in the encryption network. The processed ciphertext image is used as a set of intermediate values, and a set of diffusion keys are added to form the processed ciphertext image by bitwise heterodyne diffusion. The decryption process of the image needs to go through the double-layer parsing of the diffusion key and the deep encryption key. The reverse decoded image is then transmitted to the staff. The random generation of the diffusion key is shown in Equation (3).

$$K = random\left[k_1, k_2, \ldots, k_{m\times n\times h}\right] \tag{3}$$

In Equation (3), K denotes the generated diffusion key. $random$ denotes the random number generating function. k denotes the value of the random key. h indicates the number of data rows after textualization of the process image. n indicates the number of data columns after textualization of the process image. m denotes the number of data rows after textualization of the process image. The image data of the conversion process generates elements in a matrix manner. The recovery process decodes the pixel data of the image elements and the total pixels generated after combining are the first pixel. Since the key is the key way to decode the image, it is very important to fight against the attacker's key interception or data corruption during the image transmission process. The security

of the key is mainly determined by the encryption space and encryption method of the key. The encryption of the image can be made difficult to crack by extending the value space of the key and the difficulty of key generation. To reflect the operation flow between the user side and the encryption process of GAN network, the workflow of encrypted image transmission is elaborated as in Figure 5.

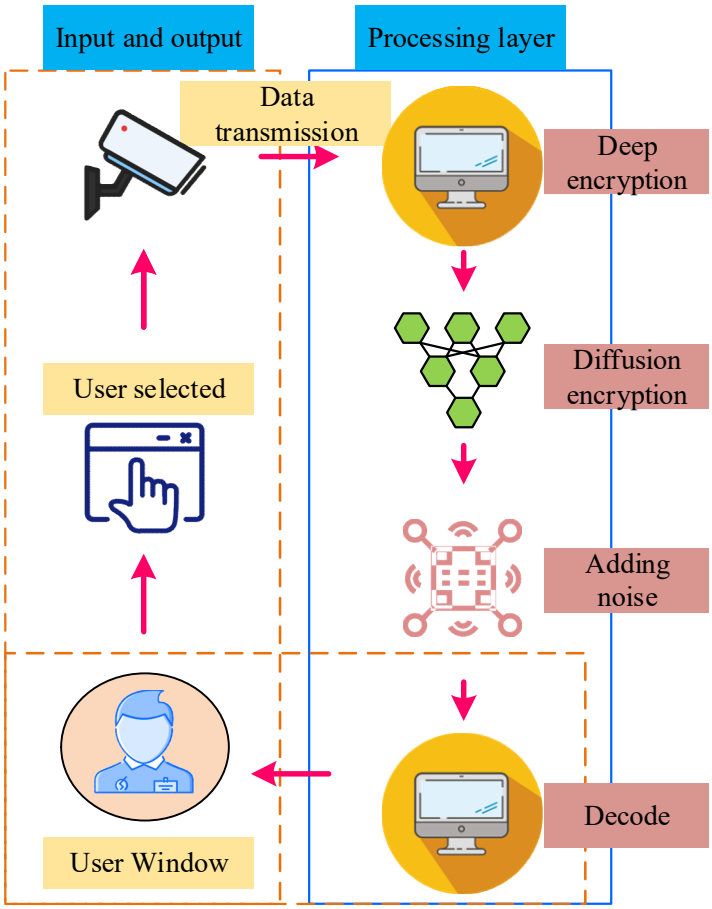

Fig. 5. Image Encryption Transmission Flowchart

In Figure 5, the user interaction process with the image takes place only in the input layer. The user selects the image through the interaction interface and the image is encrypted by the monitoring side with deep and diffusion encryption. The encrypted image is transmitted during the process, and the transmitted data is displayed in front of the display interface with key decryption. To ensure stable transmission of images during the process, the staff needs to monitor the health status of prison inmates in a step-by-step manner. Firstly, the depth key of the image is set with a chaotic sequence, and the image data is adversarial updated by GAN to ensure that the image is difficult to recognize in the transmission process. However, in order for the staff to effectively monitor the state of the criminal, the image needs to be made computationally fast in the decryption process and the accurate original image needs to be obtained. To further ensure the key security of the process the data is diffusely encrypted by displacement or diffusion algorithm to ensure that the surveillance data is not leaked by double encryption.

3. Result

3.1. Performance Tests of Image Information Security Protection Algorithms

Due to the complexity and large number of people in prisons, the monitoring process requires accurate surveillance images to identify personnel behavior. In order to test the screen transmission accuracy

of the encryption algorithm, the image dataset of multiple personnel is selected as the test sample set. The number of iterations of the algorithm is set to 120 times. The statistical study of the image transmission accuracy and error values of the algorithm during the test set iterations are shown in Figure 6.

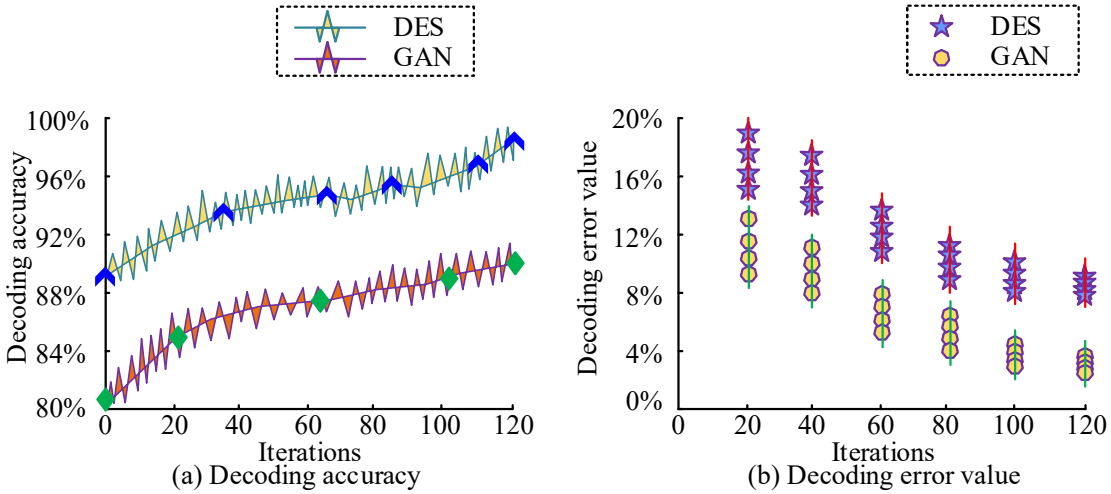

Fig. 6. Image Processing Accuracy and Error

In Figure 6(a), the image decryption accuracy of GAN algorithm in the process of image encryption rises gradually with data iteration, and the accuracy of decrypted image can reach 91.83% when the number of iterations is carried out to 20 times. After 120 iterations, the accuracy of the processed image can be increased to 98.69%. The data encryption standard (DES) algorithm also shows a gradual increase in image accuracy during the data iteration process. When the number of iterations is carried out up to 120, the image accuracy of the data can reach 89.93%. The image accuracy of the research algorithm is 8.76% higher as compared to DES method. In Figure 6(b) with data iteration GAN algorithm shows a gradual decrease in the error value during image encryption. After 120 iterations the error value of the image decreases to 2.73%-4.51%. While the trend of error value of DES algorithm is consistent with GAN algorithm, but the final error value shows 8.07%-10.83%. It indicates that the iterative changes in the dataset show that the GAN algorithm has a better image processing accuracy in the testing process, and the decoded image has a higher clarity. Moreover, compared to DES algorithm, the image processing error value of the research method is lower. To further test the encryption ability of the algorithm, the correlation of the image is calculated with the test set data as shown in Figure 7.

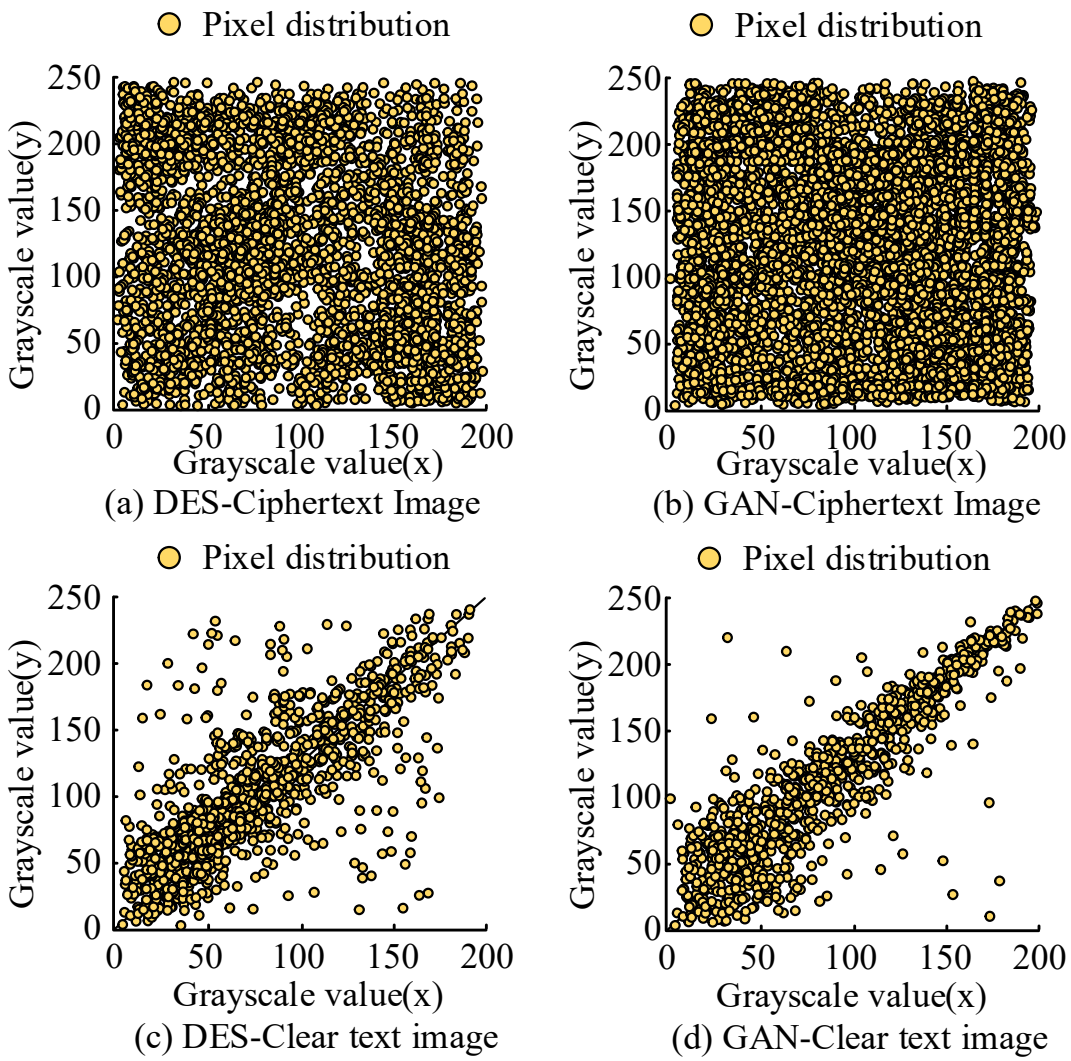

Fig. 7. Image Correlation Analysis

In Figure 7(a), the picture encrypted with DES method gets uniformly distributed pixel points, but there are gaps at the site locations. In Figure 7(b), the pixel points of the image encrypted with GAN method are more uniformly distributed and there is no obvious clustering. In Figure 7(c), the decoded image encrypted with DES has obvious correlation. The pixel points are concentrated in the diagonal position and some pixel points are scattered in other regions. The data statistic of image correlation is 78.6%. In Figure 7(d), the distribution of decoded images encrypted by the method is more clustered, and the image correlation is significantly higher than that of the DES method. The final image correlation statistics is 93.71%. The GAN method has a more uniform range of data distribution in the encryption method, while the encryption strength is higher. Moreover, the decoding clarity of the image is higher when receiving the data, and the image quality obtained is better, which is more conducive for the staff to observe the health condition of the criminals in the prison.

3.2. Application Effectiveness Test of Image Information Security Protection Algorithm

In order to test the encryption algorithm for monitoring the health status and abnormal behavior of criminals in a real prison environment, the prison scenario is selected as the test site. The data monitoring probes encrypted by the research algorithm are set up in the prison dormitory and

infirmary environments to further evaluate the encryption effect of the research algorithm on the monitoring images and the transmission picture quality. The chaos coefficient control parameter of the algorithm is set to 25. The learning rate of the training process is 0.001, with $b = 3$, $c = 28$. The image evaluation indexes of the monitoring screen are obtained as shown in Figure 8.

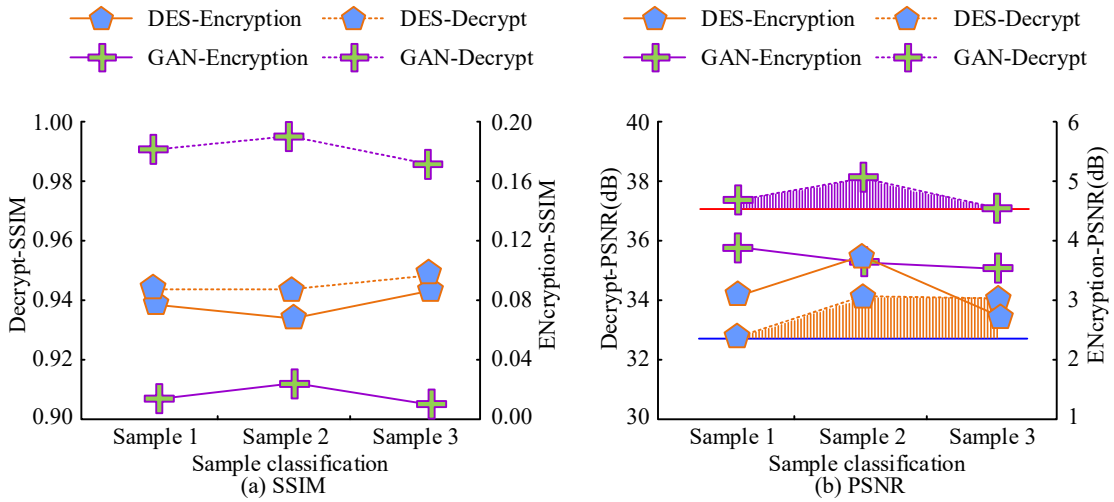

Fig. 8. Analysis of Image Similarity and Clarity

In Figure 8(a), the mean value of structural similarity (SSIM) of the image under encryption with DES algorithm is 0.078. The mean value of SSIM of the image under encryption with GAN algorithm exhibits 0.024, and the study algorithms have a lower value of SSIM as compared to DES algorithm. For the decrypted data image, the mean value of SSIM under DES algorithm processing is 0.945. The SSIM value of the image under GAN algorithm processing is 0.988. The similarity of the decrypted image under GAN algorithm is more. In Figure 8(b), the peak signal-to-noise ratio (PSNR) performance of the image data encrypted by DES algorithm process is 3.04 dB, while the mean value of PSNR value of the image data encrypted by GAN algorithm is 3.74 dB. There is no significant difference between the two. After image encryption, the average value of PSNR of the image processed by DES method is 33.29dB, and the average value of PSNR of the image processed by GAN method is 37.78dB. It indicates that the image data encrypted by GAN algorithm cannot observe the original image information, and it has better encryption effect. Moreover, the decrypted image data is closer to the original image. To determine the image processing efficiency of the algorithm in the application process, the processing time of the statistical algorithm under different number of images is shown in Figure 9.

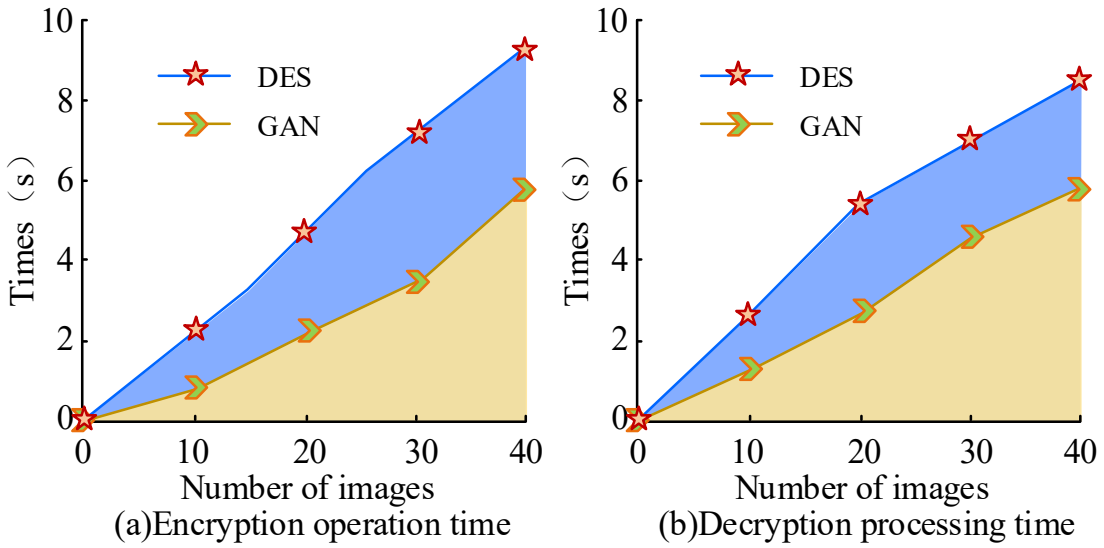

Fig. 9. Image Processing Efficiency of Algorithms

In Figure 9(a), during the encryption of images, the computing time of the DES algorithm grows as the number of processed images increases. The time required when the algorithm encrypts 40 images reaches 9.61 s, and the actual encryption speed is 0.240 s/image. The trend of encryption time of GAN algorithm for images is the same as DES algorithm, but the required encryption time is shorter. When the GAN algorithm handles the encryption of 40 images, the computing time is 5.98s and the encryption speed of the process is 0.149 s/sheet. Compared to DES algorithm research method is 41.6% more computationally efficient. In Figure 9(b), the change in the operation time of the DES algorithm during the decryption of the data in the image is consistent with the encryption. When decrypting 40 images, the operation time of DES algorithm is 8.76s and the decryption speed is 0.219s/sheet. Whereas the GAN algorithm takes less time in the process of decrypting the images. When the GAN algorithm handles the encryption of 40 images, the operation time is 5.96s and the encryption speed of the process is 0.149 s/sheet. It shows that the GAN algorithm is more efficient for image processing, compared to DES algorithm research method takes less time in both encryption and decryption process of images. To visualize the processing effect of the image, the comparison of the processed image is shown in Figure 10.

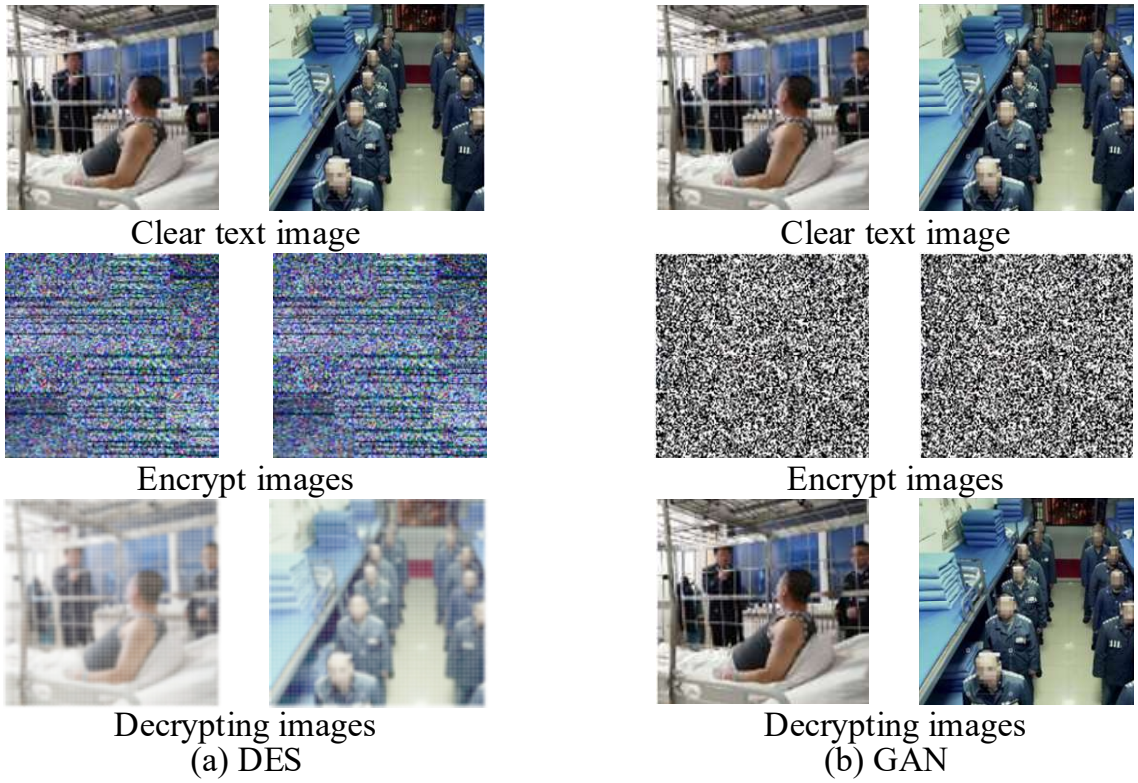

Fig. 10. The Image Effect after Algorithm Processing

In Figure 10(a), the plaintext image, encrypted image and decrypted image under DES algorithm are shown. The two sets of images after encryption of the display image shows only the noise image, and the algorithm performs image decryption after the image is basically restored to the original image content. However, the color difference and clarity of the images are partially affected and the final image similarity is only 86.42%. In Figure 10(a), the image that has been encrypted under the GAN algorithm is uniformly covered by noise, and the content in the plaintext image is no longer shown in the image. The accuracy and color gamut change of the image and the original image after performing the algorithm decryption are basically the same, and the similarity is as high as 99.26%. The results demonstrate that the GAN algorithm has an effective image encryption effect in the security protection of image information, while maintaining the clarity of the transmitted image data at a high level. This has the advantage of providing a better visualization effect for monitoring and observing the health status of prisoners.

4. Conclusions

In order to ensure the information security of the image while receiving the image information clearly, a dual-key image processing algorithm based on GAN is researched and designed. The process encrypts the video image in layers by segmentation processing of image data. The construction of the encryption module is carried out with a self-coder, the image is encrypted through the coding conversion of the image, and the reconstruction of dynamic data is carried out with iterative learning. The study also performs deep encryption of data with the help of bitwise heterogeneous or diffusion. The generation of encryption key for chaotic system is optimized by mode-taking operation, so that the image has higher strength encryption effect. The results of the study indicated that the research algorithm processed images encrypted and decrypted with less loss during transmission. The error value of the image can be reduced to 2.73%-4.51% during the iteration process. Whereas the pixel correlation of the image indicated low correlation of the encrypted image and better correlation of the

decrypted image and better encryption as compared to DES method. When the processing efficiency of the image was examined, the average speed of the GAN method for data encryption can reach 0.240 s/sheet, which is 41.6% higher compared to the DES method. As for the decryption process of the image, the processing time of the research method for the image was 0.149 s/sheet, which also showed high processing efficiency compared to the DES method. Given that the surveillance images of prison facilities are all dynamic type maps, and that the monitoring of the health status of personnel requires more sophisticated image information capture capabilities, the research method for the subtle movements of the monitored personnel requires the assistance of staff to recognize. Consequently, subsequent research can be conducted in the direction of subtle motion capture technology, with the objective of developing a robust theoretical model for the efficient and safe transmission of video images.

References

[1] Liang, W., Li, W., & Feng, L. (2021). Information security monitoring and management method based on big data in the internet of things environment. IEEE Access, 9, 39798-39812.

[2] Pan, T. (2022). Intelligent Monitoring System for Prison Perimeter Based on Cloud Intelligence Technology. Wireless Communications and Mobile Computing, 2022(1), 2517446.

[3] Imandeka, E., Hidayanto, A. N., Putra, P. O. H., Suhartanto, H., & Pidanic, J. (2024). Unlocking the Potential of Smart Security and Surveillance Technology in Prisons: A Brief Review. Revue d'Intelligence Artificielle, 38(3).

[4] Button, M. (2021). Professionalising prison security: developing a model and agenda rooted in research to enhance the delivery of security in prisons. Prison Service Journal, 252, 3-8.

[5] Yang, X. (2023). Security imperative, reformation and compliance: Understanding the prison system in China. International Journal for Crime, Justice and Social Democracy, 12(3), 54-63.

[6] Jurgilewicz, O., Hydzik, P., Malec, N., & Itrich-Drabarek, J. (2020). MANAGEMENT OF PROTECTIVE INFRASTRUCTURE IN PRISONS AS AN ELEMENT INCREASING SAFETY OF PENITENTIARY EMPLOYEES. Journal of Security & Sustainability Issues, 9(3).

[7] Chisari, C. (2023). Transitioning from dynamic security in italian prisons: assessing the influence of perceived insecurity on prison management. RASSEGNA ITALIANA DI CRIMINOLOGIA, (3), 240-251.

[8] Tahamont, S. (2019). The effect of facility security classification on serious rules violation reports in California prisons: a regression discontinuity design. Journal of Quantitative Criminology, 35, 767-796.

[9] Rahman, M. M., & Ali, A. (2018). An analysis on the real barriers of prison administration in Bangladesh. International Journal of Innovative Research and Advanced Studies, 15(4), 289-293.

[10] Purwito, A., Sitanggang, D. W. F., Suprayitno, S., & Marbandi, A. (2018). Design Of Prison Security Information System Using Rfid. JOURNAL ASRO, 9(1), 129-135.

[11] Joseph, J. (2025). Technoprison: Technology and prisons. Criminal Justice in the 21st Century, 95.

[12] Yasmeen, G., & Afaq, S. A. (2024). The Rising Threat of Deepfake Technology. Effective Strategies for Combatting Social Engineering in Cybersecurity, 307.

[13] Raher, S. (2024). Data privacy in carceral settings: The digital panopticon returns to its roots. Nw. UL Rev. Online, 119, 73.

[14] Briongos, S., Malagón, P., de Goyeneche, J. M., & Moya, J. M. (2019). Cache misses and the recovery of the full AES 256 key. Applied Sciences, 9(5), 944.

[15] Salami, Y., Khajevand, V., & Zeinali, E. (2023). Cryptographic algorithms: A review of the literature,

weaknesses and open challenges. J. Comput. Robot, 16(2), 46-56.

[16] Andriani, R., Wijayanti, S. E., & Wibowo, F. W. (2018, November). Comparision of AES 128, 192 and 256 bit algorithm for encryption and description file. In 2018 3rd International Conference on Information Technology, Information System and Electrical Engineering (ICITISEE) (pp. 120-124). IEEE.

[17] Gaur, P., & Kaushik, A. (2021). AES image encryption (Advanced encryption standard). Int. J. Res. Appl. Sci. Eng. Technol, 9(12), 1357-1363.

[18] Cai, Z., Xiong, Z., Xu, H., Wang, P., Li, W., & Pan, Y. (2021). Generative adversarial networks: A survey toward private and secure applications. ACM Computing Surveys (CSUR), 54(6), 1-38.

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

[20] Man, Z., Li, J., Di, X., Liu, X., Zhou, J., Wang, J., & Zhang, X. (2021). A novel image encryption algorithm based on least squares generative adversarial network random number generator. Multimedia Tools and Applications, 80, 27445-27469.

[21] Wang, X. (2024). GAN-DNADE: Image encryption algorithm based on generative adversarial network and DNA dynamic encoding. Computer Science and Information Systems, (00), 53-53.

[22] Dai, L., Lei, H., Chen, L., Wang, C., & Feng, L. (2024). An Image Double Encryption Based on Improved GAN and Hyper Chaotic System. IEEE Access.

[23] Liu, T., Chen, Z., Wu, X., Long, B., He, C., Wang, L., ... & Deng, H. (2024). RESAKey GAN: Enhancing Color Image Encryption through Residual Self-Attention Generative Adversarial Networks. Physica Scripta.