Secure News Video Transmission Using Bidirectional GAN Encoding and Honey Encryption: A Hybrid Deep Learning Approach

Xiaoguang Li[1*], Chang Duan[2], Guohua Yuan[3]

[1]Party Committee Organization Propaganda Department, Shijiazhuang Institute of Railway Technology, Shijiazhuang, 050000, China

[2]Discipline Inspection and Supervision Department, Shijiazhuang Institute of Railway Technology, Shijiazhuang, 050000, China

[3]Department of Information Engineering, Shijiazhuang Institute of Railway Technology, Shijiazhuang, 050000, China

E-mail: lxg_198807@163.com

*Corresponding author

Keywords: Bidirectional GAN, honey encryption algorithm, news videos, communication protection, algorithm optimization

Received: August 4, 2025

This study addresses the challenges of data compression and security protection during the dissemination of news videos and proposes an encryption protection method combining bidirectional generative adversarial networks and honey encryption algorithms. This method first uses a bidirectional generative adversarial network encoder to convert video frames into latent codes, and then applies the honey encryption algorithm for encryption processing. At the receiving end, the latent code is decrypted with the correct key and then restored to a video frame by the generative adversarial network decoder, and the complete video is reconstituted. The experimental results on the 50GB dataset show that after 100 iterations, this method achieves an accuracy rate of 0.9, a recall rate of over 0.8, a loss function value of below 10^{-4}, and the mean absolute error and root mean square error stabilize below 0.1. In addition, the encryption speed of this algorithm is 0.45 seconds, the decryption speed is 0.32 seconds, the compression ratio is 30.13%, and the reconstruction quality is 35.89dB, all of which are superior to the existing technologies. This research provides an efficient and reliable solution for the secure dissemination of news videos, effectively preventing the tampering and leakage of video content, and ensuring the authenticity and authority of news content.

Povzetek: Študija predlaga zaščito videov novic z dvosmernimi GAN-i in šifriranjem, kjer se okvirji kodirajo v latentne zapise za hkratno kompresijo in šifriranje, kar prinese hitrejšo, učinkovitejšo in robustnejšo varno distribucijo.

1 Introduction

Driven by the wave of digitization, news videos, as an important carrier for conveying information, are spreading faster and wider in coverage on the Internet [1]. However, the popularity of news video dissemination is also accompanied by challenges of data security and privacy protection. In the process of dissemination, news videos may encounter problems such as unauthorized access, tampering, and even malicious use, which not only undermine the authenticity and authority of news, but also may lead to a series of social problems [2-3]. Therefore, how to ensure the efficient dissemination of news videos while maintaining the security and integrity of their content is a key issue in the industry today. Artificial intelligence and machine learning technologies are developing rapidly and have achieved many results in the field of data encryption and security protection. Generative Adversarial Network (GAN) is a model with strong generative ability, which has shown its unique advantages in many fields such as image generation, data enhancement, etc [4]. GAN is capable of generating high-quality data samples through the adversarial training of generators and discriminators, which provides a new view and methods [5-6].

In the process of news video dissemination, how to balance data compression and security protection has always been the focus of the industry. khan A A and his team provided a new solution to this problem by skillfully integrating GAN with fuzzy logic. They utilized fuzzy logic to accurately control the object frequency and the generation of processing code, while effectively eliminating the adversarial loss and removing redundant data, to construct an efficient and collaborative multimedia data compression model. Experimental results showed that the model significantly outperformed other advanced models in terms of compression ratio, and the decoded video was completely consistent with the original video, with a compression rate of up to 30.13% or more, which opens up new horizons for encryption and protection of news video distribution [7]. To address the challenges of big data pattern recognition, Amiri Z et al. conducted a systematic literature review and carefully categorized 60 cutting-edge articles, covering a wide range of methods such as deep learning and machine learning, including ten categories of techniques such as Convolutional Neural Networks (CNNs), recurrent neural networks, and GANs. The results showed that these articles provide an in-depth discussion on key parameters such as accuracy, adaptability, fault tolerance, security, scalability, and flexibility, which provide valuable references for the selection of pattern recognition techniques in the encryption and protection of news video distribution [8]. Faced with the proliferation of malware variants, Maniriho et al. focused on deep learning techniques. Given the numerous variants of malicious software, deep learning algorithms have become powerful tools for building scalable and advanced malware detection models, thanks to their ability to handle large datasets. The study explored deep learning techniques suitable for malware attack detection on Windows, Linux, and Android platforms, covering different types of algorithms, network optimizers, regularization methods, as well as loss functions, activation functions, implementation frameworks, etc. It also involved a review of feature extraction methods and deep learning-based detection models, and pointed out the main research problems and future research directions in this field [9]. Badhagouni et al. proposed a hybrid feature extraction method based on CNN and Honey Badger Algorithm (HBA) for human behavior recognition in videos. By combining the CNN classifier with HBA and optimizing the weight parameters, the performance of CNN could be improved. The experiment was validated using Weizmann and KTH datasets, and the results showed that the method performed well in performance indicators such as specificity, sensitivity, and accuracy, providing an effective means for human behavior recognition in encrypted protection of news video dissemination [10].

Aiming at the privacy protection issue in network communication security, Huang P et al. proposed a chaotic random knowledge recognition model combining the log system and the configuration center. The results showed that the proposed model outperformed traditional methods in encryption speed under different data packet sizes, demonstrating its potential for secure and efficient data encryption in network communication [11]. To address the limitations of Internet of Things (IoT) devices in terms of energy, computing power and memory, Hedayati R et al. proposed a lightweight data compression algorithm for image encryption. This algorithm adopted scanning-based block compression and selective pixel encryption methods, and could complete image data encryption in just one round, thereby reducing the computational complexity and the amount of data. The results of implementing this method in the IoT test environment showed that, compared with the existing algorithms, the average energy consumption and data packet rate of the devices were reduced by 15% and 26% respectively [12]. A large amount of multimedia data was generated and exchanged in various IoT devices, systems and applications. Yang W et al. conducted a comprehensive review on the security and privacy protection of multimedia data in the IoT. Firstly, multimedia data was classified into different types and security levels based on application fields. Then, the existing multimedia data protection schemes in the IoT were analyzed and discussed, including traditional technologies such as cryptography and watermarking technology, as well as emerging technologies such as blockchain and federated learning [13]. The differences between the existing studies and this one is shown in Table 1.

Table 1: Summary of literature review

Reference number	Methods	Encryption speed (s)	PSNR (dB)	Computational complexity	Limitations
[7]	Combination of GAN and fuzzy logic	0.5	34	Medium	The compression ratio needs to be improved
[8]	Deep learning pattern recognition	/	33	High	Insufficient adaptability
[9]	Deep learning malware detection	0.7	32	High	It has a strong dependence on large datasets
[10]	Hybrid feature extraction of CNN and HBA	0.6	35	Medium	Accuracy needs to be improved
[11]	Chaotic random knowledge recognition model	0.55	35.5	Low	The applicable scenarios are limited
[12]	Lightweight image encryption algorithm	0.58	34.5	Low	Only applicable to IoT devices
This study	Bidirectional GAN and honey encryption	0.45	35.89	Low	No obvious limitations

Most of the current research is still limited to the application of a single technique, and it is often difficult to achieve the desired results in the face of data such as news videos, which are both complex and highly demanding in terms of security and timeliness. To address these limitations, the research proposes an innovative cryptographic protection method that integrates bidirectional GAN with honey encryption algorithms, aiming to provide an efficient as well as secure solution for the dissemination of news videos. The main objective of the research is to develop an encryption protection method that can simultaneously reduce latency, maintain video fidelity and enhance anti-attack capabilities. The research assumes that the bidirectional GAN combined with the honey encryption algorithm can effectively achieve these goals. The innovation of the method lies in constructing a new cryptographic protection framework that fully utilizes the powerful capabilities of bidirectional GAN in data generation, compression, and feature extraction, while taking advantage of the unique security features of the honey encryption algorithm. The honey encryption algorithm produces seemingly valid but actually incorrect results even if the wrong key is used for decryption, and this property can effectively confuse attackers, thus providing a higher level of security and confidentiality for the dissemination of news videos.

2 Methods and materials

The research integrates bidirectional GAN with honey encryption technology to protect the secure transmission of news videos. The whole scheme covers the key aspects of video preprocessing, encryption, transmission, decryption and reorganization, forming a complete and tight protection system. The specific applications of bidirectional GAN and honey encryption in the field of video encryption are analyzed in depth, demonstrating their significant advantages in improving encryption efficiency and enhancing security, thus ensuring the integrity and usability of the video content in all aspects.

2.1 News video encryption technology based on honey encryption algorithm

Honey encryption algorithm is an innovative encryption technology, whose core idea is to obtain seemingly effective results even if the wrong key is used for decryption, thereby confusing attackers and increasing the difficulty of attacks [14-15]. Firstly, the news video frame images are converted into latent code representations. Assuming the news video frame image is I and the encoder is E, the representation of the latent code is shown in equation (1). The encoder function Encode is a deep neural network that converts the input video frame image into a compact latent representation.

$$Z = E(I) \quad (1)$$

In equation (1), Z is the latent code representation of news video frames, and E is the encoder. Next, the latent code Z is honey encrypted. The honey encryption algorithm converts the latent code into an encrypted latent stream through a distributed conversion encoder. The DTE function is responsible for converting latent representations into encrypted latent code streams. The encrypted latent stream is shown in equation (2).

$$Z' = DTE(Z) \quad (2)$$

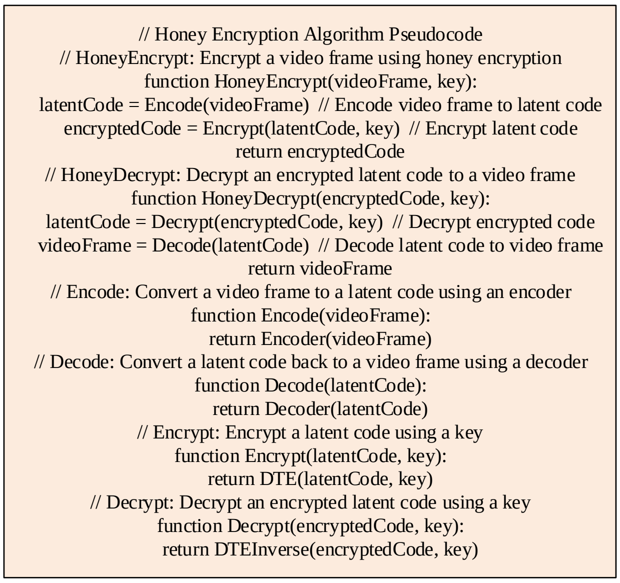
In equation (2), Z' is the encrypted latent stream, and DTE is the distributed conversion encoder. At the decryption end, the correct key K is utilized to decrypt the encrypted latent stream Z'. The decryption process is shown in equation (3).

$$Z = DTE^{-1}(Z', K) \quad (3)$$

In equation (3), DTE^{-1} is the inverse process of the distributed transform encoder, and K is the correct decryption key. Finally, the decrypted latent code is converted back into news video frame images through a decoder. If the decoder is set to G, the restored news video frame image is shown in equation (4).

$$I' = G(Z) \quad (4)$$

In equation (4), I' is the restored news video frame image. The pseudocode of the honey encryption algorithm is shown in Figure 1.



```
// Honey Encryption Algorithm Pseudocode
// HoneyEncrypt: Encrypt a video frame using honey encryption
function HoneyEncrypt(videoFrame, key):
    latentCode = Encode(videoFrame)  // Encode video frame to latent code
    encryptedCode = Encrypt(latentCode, key)  // Encrypt latent code
    return encryptedCode
// HoneyDecrypt: Decrypt an encrypted latent code to a video frame
function HoneyDecrypt(encryptedCode, key):
    latentCode = Decrypt(encryptedCode, key)  // Decrypt encrypted code
    videoFrame = Decode(latentCode)  // Decode latent code to video frame
    return videoFrame
// Encode: Convert a video frame to a latent code using an encoder
function Encode(videoFrame):
    return Encoder(videoFrame)
// Decode: Convert a latent code back to a video frame using a decoder
function Decode(latentCode):
    return Decoder(latentCode)
// Encrypt: Encrypt a latent code using a key
function Encrypt(latentCode, key):
    return DTE(latentCode, key)
// Decrypt: Decrypt an encrypted latent code using a key
function Decrypt(encryptedCode, key):
    return DTEInverse(encryptedCode, key)
```

Figure 1: Pseudocode of honey encryption algorithm

In Figure 1, the weights of the bidirectional GAN-honey encryption model include the encoder, decoder, 128-dimensional latent space parameters of honey encryption, AdaIN layer γ/β coefficients, and 256-bit key matrix. The dataset provides H.264 encoded, 1920×1080/30fps news videos and synthetic scripts. The training uses the Adam optimizer, with a learning rate of 0.001, batch size of 64,50 epochs, no dropout, weight initialization by Xavier, and a loss function composed of adversarial loss, reconstruction loss, and style consistency loss weighted λ=0.1. The bidirectional GAN encoder is trained using a deep CNN structure. The encoder optimizes its parameters by minimizing reconstruction errors and adversarial losses. The latent space is designed as a high-dimensional space capable of capturing the key features of the input data. The encryption function is implemented through a key-based hash function and a pseudo-random number generator, ensuring the security of the encryption process. First, the input video frames are converted into latent representations through the encoder; Then, the latent representation is encrypted through the encryption module; Finally, the encrypted latent representation is transmitted over the network and restored to a video frame at the receiving end through a decoder. The Encode and Decode functions are used for encoding video frames to latent code and decoding latent code to video frames, respectively [16-18]. The encryption architecture for news video dissemination based on honey encryption algorithm is shown in Figure 2.

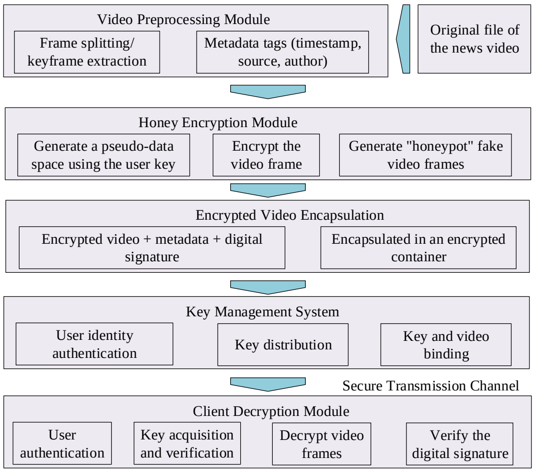

Video Preprocessing Module
Frame splitting/ keyframe extraction
Metadata tags (timestamp, source, author)
Original file of the news video
Honey Encryption Module
Generate a pseudo-data space using the user key
Encrypt the video frame
Generate "honeypot" fake video frames
Encrypted Video Encapsulation
Encrypted video + metadata + digital signature
Encapsulated in an encrypted container
Key Management System
User identity authentication
Key distribution
Key and video binding
Secure Transmission Channel
Client Decryption Module
User authentication
Key acquisition and verification
Decrypt video frames
Verify the digital signature

Figure 2: Encryption architecture diagram for news video dissemination based on honey encryption algorithm

In Figure 2, a mechanism combining Advanced Encryption Standard (AES) and Honey Encoding is introduced to return a "honeypot" fake video when decryption fails, effectively deceiving attackers. Combining digital signatures, Transport Layer Security (TLS) transmission, and Public Key Infrastructure (PKI) system, it comprehensively enhances content security and traceability, suitable for secure distribution scenarios of highly sensitive news videos.

2.2 Optimization of news video encryption efficiency and security based on bidirectional GAN

The study introduces a news video encryption protection method based on honey encryption algorithm. Next, the research uses bidirectional GAN to improve encryption efficiency and security, while ensuring the integrity and availability of video content. The encryption protection algorithm for news video dissemination based on bidirectional GAN mainly consists of a video segmentation module, bidirectional GAN encoder, encryption module, encrypted transmission module, bidirectional GAN decoder, and video reassembly module [19-21]. The architecture of the encryption protection algorithm for news video dissemination based on bidirectional GAN is shown in Figure 3.

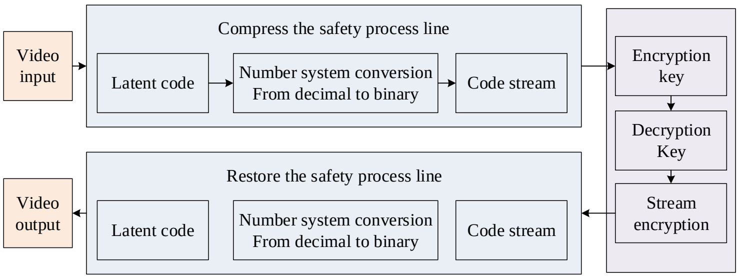

Video input
Compress the safety process line
Latent code
Number system conversion From decimal to binary
Code stream
Encryption key
Decryption Key
Stream encryption
Video output
Restore the safety process line
Latent code
Number system conversion From decimal to binary
Code stream

Figure 3: Architecture of encryption protection algorithm for news video propagation based on bidirectional GAN

In Figure 3, the video input is then segmented into individual frames through a preprocessing module. Subsequently, each frame of the image is converted into a latent feature representation through a bidirectional GAN encoder. The structure of the bidirectional GAN generator model is shown in Figure 4.

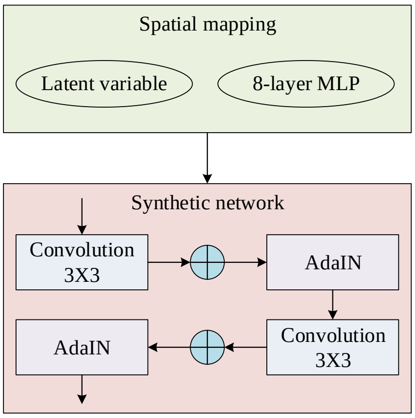


Figure 4: Structure of bidirectional GAN generator model

In the bidirectional GAN generator model structure shown in Figure 4, the generator consists of an encoder and a decoder. The encoder consists of multiple convolutional layers, each of which uses a 3×3 kernel with a step size of 2 and a fill size of 1. The feature mapping dimension gradually increases from 64 to 256, and the activation function adopts LeakyReLU (with a negative slope of 0.2). The decoder is composed of multiple deconvolution layers, with a kernel size of 3×3, a step size of 2, a fill size of 1, a feature mapping dimension gradually decreasing from 256 to 64, an activation function of ReLU, and the final output layer uses the Tanh activation function. During the training, the Adam optimizer is adopted, with a learning rate of 0.0002, a batch size of 64, and 200 training epochs. To balance the quality of compression and reconstruction, a weighted combination of perceptual loss and reconstruction loss is introduced as the optimization objective. By adjusting the weight parameters, the quality of the reconstructed video is optimized while maintaining a low bit rate, thereby achieving a better balance between compression efficiency and video quality. In addition, noise is added after each convolutional layer to increase the stability of the model during training [22-23]. This generator adopts an improved architecture, in which the AdaIN layer is used to implement style transfer, allowing the network to dynamically adjust the style of the feature map during the generation process, thereby enhancing the diversity and authenticity of the generated images. The AdaIN layer achieves style transfer by normalizing the feature map and multiplying it by the style vector, and then adding the mean of the style vector. During the training, a combined loss function is employed, including adversarial loss, reconstruction loss, and style consistency loss, to ensure that the generator could learn effective latent spatial representations and generate high-quality images corresponding to the input. The AdaIN operation process is shown in equation (5).

$$\mathrm{AdaIN}(f_l, s) = \sigma(s) \cdot \frac{f_l - \mu(f_l)}{\sigma(f_l)} + \mu(s) \quad (5)$$

In equation (5), $\mu(s)$ and $\sigma(s)$ respectively represent the mean and standard deviation of the feature map, f_l is the feature map of the l th layer, and s is the style vector. A multi-scale discrimination mechanism is introduced into the discriminator to enhance its ability to recognize forged features, as shown in equation (6).

$$\mathrm{L}_D = \sum_i \mathrm{E}_{x\sim p_{\mathrm{data}}}[\log D_i(x)] + \mathrm{E}_{z\sim p_z}[\log(1 - D_i(G(z)))] \quad (6)$$

In equation (6), D_i is the output of the discriminator on the i th scale and L_D is the discriminative loss function. The objective of the generator is to minimize the generation loss while maximizing the misclassification rate of the discriminator with the loss function shown in equation (7).

$$\mathrm{L}_G = \sum_i \mathrm{E}_{z\sim p_z}[\log(1 - D_i(G(z)))] \quad (7)$$

In equation (7), L_G is the generator loss function. Bidirectional GAN can effectively improve the attack resistance and reconstruction quality of the encryption system while maintaining the integrity of the video content.

2.3 Encryption protection for news video dissemination based on bidirectional GAN-honey encryption algorithm

The study introduces the application of honey encryption algorithm in news video encryption and the implementation mechanism of bidirectional GAN in improving encryption efficiency and security. Next, the study will organically integrate bidirectional GAN with honey encryption algorithm to construct a complete, efficient, and robust encryption protection framework for news video dissemination. The bidirectional GAN-honey encryption algorithm flow is shown in Figure 5.

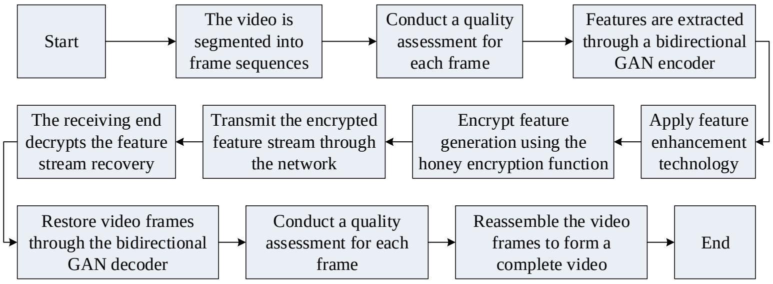

Start
The video is segmented into frame sequences
Conduct a quality assessment for each frame
Features are extracted through a bidirectional GAN encoder
Apply feature enhancement technology
Encrypt feature generation using the honey encryption function
Transmit the encrypted feature stream through the network
The receiving end decrypts the feature stream recovery
Restore video frames through the bidirectional GAN decoder
Conduct a quality assessment for each frame
Reassemble the video frames to form a complete video
End

Figure 5: Process of bidirectional GAN-honey encryption algorithm

In Figure 5, feature enhancement is used to improve the robustness and expressiveness of encryption features. This process involves preprocessing the latent features extracted from video frames, including feature standardization, noise injection, and nonlinear transformation, to enhance the model's decoding ability for encrypted data. During the training, the encoder converts news video frame images into latent code, and then encrypts the latent code through the honey encryption algorithm. The encrypted latent code stream is then decoded by the decoder to reconstruct the video frames. Throughout the entire process, the encoder, decoder, and honey encryption-related modules jointly participate in the training, optimizing the model parameters by minimizing the reconstruction error and adversarial loss. This end-to-end joint training method ensures the collaborative optimization between the encoding process from video frames to latent codes and the decoding process from latent codes to video frames, thereby preserving the integrity and availability of video content to the greatest extent while providing encryption protection, and providing a guarantee for the high performance of the model. In the honey encryption algorithm, the distribution-transform encoder adopts a multi-round iterative design based on confusion and diffusion. In each round, the latent code is processed through nonlinear transformation and permutation operations to ensure that the encrypted latent code stream has a high degree of randomness and complexity. The decoder restores the original latent code through reverse operation. Assuming that the latent code follows a Gaussian distribution, when decrypted with an incorrect key, by deliberately introducing bias and noise, the decryption output deviates from the true distribution, resulting in seemingly effective but actually erroneous outcomes, thereby confusing the attacker. The key length is 256 bits and adopts the AES-256 format. The key management strategy includes dynamic generation of the key, regular update and secure storage to ensure the uniqueness and security of the key. The encryption protection framework for news video dissemination is shown in Figure 6, which includes five main parts: video preprocessing, encryption module, transmission module, decryption module, and video reassembly module.

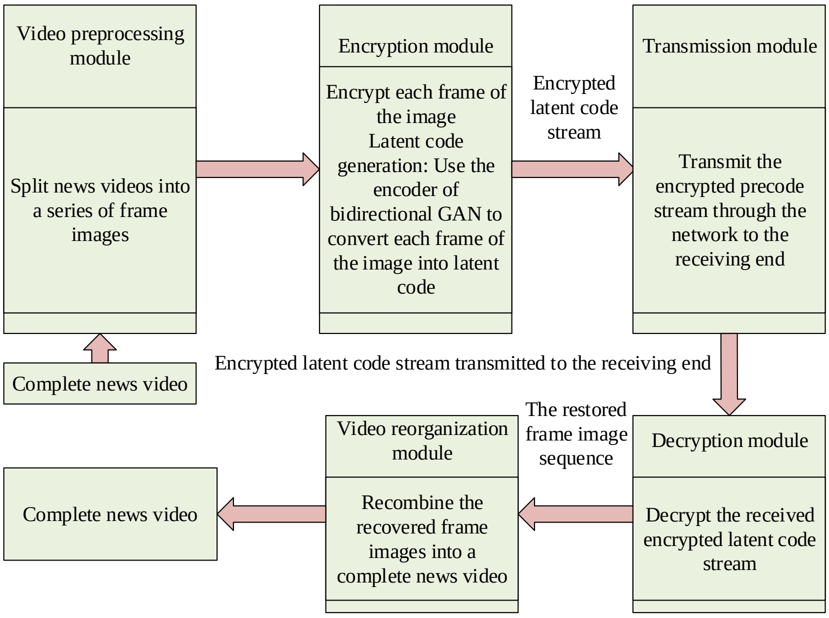

Video preprocessing module
Split news videos into a series of frame images
Complete news video
Encryption module
Encrypt each frame of the image Latent code generation: Use the encoder of bidirectional GAN to convert each frame of the image into latent code
Encrypted latent code stream
Transmission module
Transmit the encrypted precode stream through the network to the receiving end
Encrypted latent code stream transmitted to the receiving end
Decryption module
Decrypt the received encrypted latent code stream
The restored frame image sequence
Video reorganization module
Recombine the recovered frame images into a complete news video
Complete news video

Figure 6: Encryption protection framework for news video dissemination

In Figure 6, the video preprocessing module is responsible for segmenting the complete news video into a series of individual frame images, providing basic data for subsequent encryption steps. The encryption module utilizes the encoder part of bidirectional GAN to convert each frame of image into latent code, and then applies a distributed transformation encoder to honey encrypt these latent codes to enhance security. Then, the transmission module securely sends these encrypted latent streams over the network to the receiving end. At the receiving end, the decryption module uses the correct key to decrypt these encrypted latent streams, recovers the original latent codes, and uses the decoder part of the bidirectional GAN to convert the latent codes back into video frames. Finally, the video reassembly module reassembles these recovered frame images into a complete news video, ensuring that authorized users can view unaltered news content and ensuring the security and confidentiality of the news video during transmission. The research adopted Peak Signal-To-Noise Ratio (PSNR) and Structural Similarity Index (SSIM) indicators to quantify the quality of the decrypted video. PSNR is used to evaluate the pixel-level quality of videos, and the calculation is shown in equation (8).

$$\mathrm{PSNR} = 10 \cdot \log_{10} \frac{\mathrm{MAX}^2}{\mathrm{MSE}} \quad (8)$$

In equation (8), MAX represents the maximum possible value of the video pixel, and MSE is the mean square error. SSIM is used to evaluate the structural information of a video, and its calculation is shown in equation (9).

$$\mathrm{SSIM}(x,y) = \frac{\left(2\mu_x\mu_y + c_1\right)\left(2\sigma_{xy} + c_2\right)}{\left(\mu_x^2 + \mu_y^2 + c_1\right)\left(\sigma_x^2 + \sigma_y^2 + c_2\right)} \quad (9)$$

In equation (9), x and y represent the original video frame and the decrypted video frame respectively, μ represents the mean, σ represents the standard deviation, σ_{xy} is the covariance of x and y, and c_1 and c_2 are small constants added to avoid the denominator being zero.

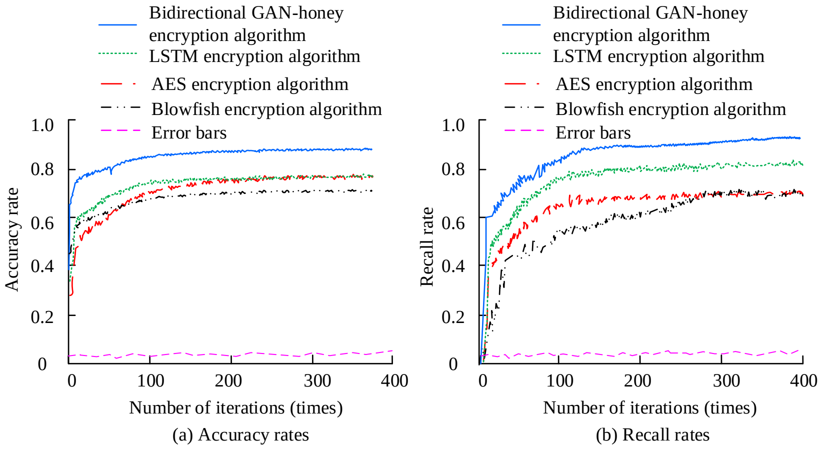
3 Results

The dataset used in the experiment was 50GB in size. The news videos were sourced from high-definition news videos released by multiple news organizations and public online video platforms. The video duration ranged from 1 minute to 10 minutes, with resolutions covering 1920×1080, 1280×720, 800×600, 640×480, 480×360, etc. The frame rates included 24fps, 30fps, and 60fps. Before inputting the data into the model, a preprocessing step was carried out, including splitting the video into individual frame images and evaluating the quality of each frame to ensure the effectiveness of subsequent processing. The hardware environment of the experiment consisted of an Intel Core i7 processor, 16GB RAM, NVIDIA GeForce GTX 1080 Ti GPU and a 1TB solid-state drive. The software environment was built on Python version 3.8. The deep learning framework selected was TensorFlow 2.4.0. Meanwhile, libraries such as NumPy, Pandas and Matplotlib were called to complete data processing and visualization tasks. To ensure the reliability and robustness of the results, cross-validation and multiple test experiments were adopted. The dataset was divided into a training set, a validation set and a test set, with proportions of 70%, 15% and 15% respectively. A 5-fold cross-validation was used to evaluate the generalization ability of the model. Different random seeds were used to initialize the model parameters in each experiment, ensuring the repeatability of the experimental results. The reported values were based on the average of multiple runs, which reflect the performance of the model on different data splits. In addition, different data splitting strategies were adopted, including random splitting and hierarchical splitting, to verify the model's adaptability to different data distributions. The specific experimental parameters and configurations are shown in Table 2.

Table 2: Experimental parameter configuration table

Parameter name	Parameter value
Dataset size	50GB
Training set ratio	70%
Verification set ratio	15%
Test set ratio	15%
Processor	Intel Core i7
Memory	16GB
GPU	NVIDIA GeForce GTX 1080 Ti
Hard disk	1TB solid-state drive
Deep learning framework	TensorFlow 2.4.0
Programming language version	Python 3.8
Batch size	64
Learning rate	0.001
Number of iterations	50
Encryption algorithm	Honey Encryption

In Table 2, the learning rate was set to 0.001. After multiple experiments, it was verified that this value could ensure the rapid convergence of the model while avoiding overfitting. The iteration count was set to 50 times. This choice was based on experimental observations. Under this number of iterations, the model could achieve better performance and the loss function tends to be stable. Sensitivity analysis of hyperparameters showed that minor adjustments in the learning rate may lead to significant changes in the model's convergence speed and final performance, while the contribution of an increase in the iteration count to performance improvement gradually decreased after exceeding a certain threshold. Therefore, the selected hyperparameters play a crucial role in ensuring the validity and efficiency of the model. In this experiment, the study analyzed the newly proposed bidirectional GAN-honey encryption algorithm in comparison with three widely recognized encryption algorithms, which are the AES algorithm, Blowfish algorithm, and Long Short-Term Memory Artificial Neural Network (LSTM)-based encryption algorithm. The main indicators for research evaluation were as follows: Accuracy was measured by calculating the ratio of the number of correctly decrypted video frames to the total number of video frames, reflecting the performance of the encryption algorithm in maintaining the integrity of video content. Recall rate was evaluated by calculating the ratio of the number of correctly decrypted video frames to the actual number of video frames that should be decrypted to assess an algorithm's ability to restore all original video frames. The Mean Absolute Error (MAE) was obtained by calculating the average of the absolute values of the pixel value differences between the decrypted video frame and the original video frame, and was used to measure the closeness of the decrypted video to the original video. The Root Mean Square Error (RMSE) was derived by calculating the square root of the average square of the difference in pixel values between the decrypted video frame and the original video frame, and was used to measure the degree of difference between the decrypted video and the original video. These indicators are applicable in measuring security and reconstruction quality because they can quantitatively assess the impact of the encryption-decryption process on video content, ensuring the security and availability of the video during transmission. The accuracy and recall of several algorithms are shown in Figure 7.



(a) Accuracy rates
(b) Recall rates

Figure 7: Accuracy and recall of several algorithms

In Figure 7 (a), the accuracy of the bidirectional GAN-honey encryption algorithm grew the fastest, approaching 0.9 after approximately 100 iterations and remaining stable thereafter until reaching 1.0 at the end of 400 iterations. In Figure 7 (b), the recall rate of the bidirectional GAN-honey encryption algorithm also performed well, rapidly rising above 0.8 after 100 iterations and continuing to increase in subsequent iterations, ultimately approaching 1.0. The bidirectional GAN-honey encryption algorithm outperformed the other three algorithms in two key performance indicators, accuracy and recall, demonstrating its superior performance and potential in news video transmission encryption protection. The convergence of several algorithms is shown in Figure 8. Dataset A consists of high-definition news videos released by multiple news organizations, ranging in length from 1 minute to 10 minutes, with a resolution of 1920 × 1080, covering multiple fields such as politics, economy, and society. Dataset B comes from publicly available online video platforms, containing video clips of different resolutions and frame rates, with diverse content covering emergencies, on-site reporting, and more. These video contents were processed by specific codecs and the H.264 encoding standard was used to ensure a balance between video quality and compression efficiency. Both datasets A and B are publicly available and can be obtained from the corresponding news organizations and online video platforms, providing replicable experimental conditions for research.

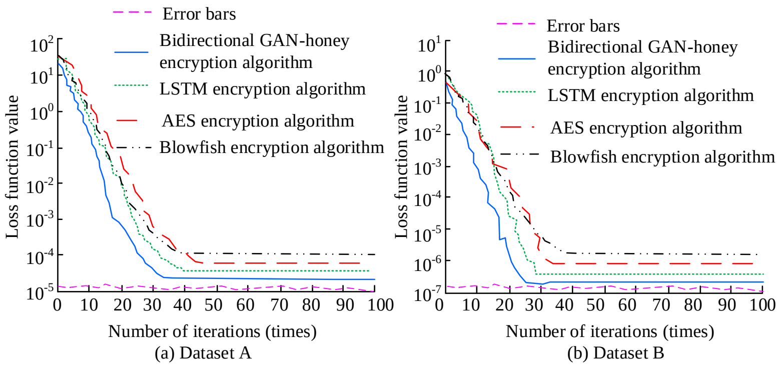


Figure 8: Convergence of several algorithms

In Figure 8 (a), the loss function value of the bidirectional GAN-honey encryption algorithm decreased the fastest, dropping below 10^{-4} after about 20 iterations, and further dropping to 10^{-5} after 30 iterations, finally reaching the lowest value of 10^{-6} at 100 iterations. In Figure 8 (b), the bidirectional GAN-honey encryption algorithm also exhibited the fastest convergence speed, dropping below 10^{-6} after approximately 15 iterations, and further dropping to 10^{-7} after 30 iterations. Finally, it reached its lowest value of nearly 10^{-7} at 100 iterations. It has been confirmed that the bidirectional GAN-honey encryption algorithm has superior convergence performance on different datasets, and can achieve lower loss function values in fewer iterations, demonstrating better generalization ability and robustness. The MAE and RMSE of several algorithms are shown in Figure 9.

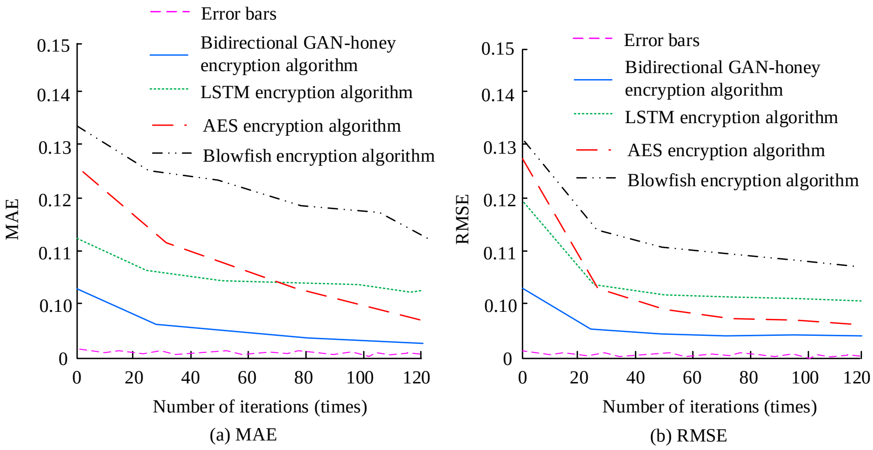


Figure 9: MAE and RMSE of several algorithms

In Figure 9 (a), the MAE value of the bidirectional GAN-honey encryption algorithm rapidly decreased from an initial value of 0.10, dropped to 0.09 after 20 iterations, and further decreased to 0.08 after 40 iterations, finally stabilizing at 0.07 after 120 iterations. In Figure 9 (b), the RMSE value of the bidirectional GAN-honey encryption algorithm rapidly decreased from an initial value of 0.10, dropped to 0.09 after 20 iterations, further decreased to 0.08 after 40 iterations, and finally stabilized at 0.07 after 120 iterations. The bidirectional GAN-honey encryption algorithm had significant advantages in improving encryption accuracy and reducing errors, especially in the early iteration stage, where its performance improvement was more significant.

3.2 Evaluation of encryption protection effect for news video communication

To comprehensively evaluate the practical application effect of encrypted protection in news video dissemination and its scalability in different scenarios, multiple key indicators were selected for comparative analysis. The anti-attack capability was quantified by simulating attack scenarios to evaluate the resistance of encryption algorithms to attacks such as brute-force cracking. Measured by the success rate of cracking and the required computing resources, a low success rate and high resource demand indicated strong anti-attack capability. The complexity of key management measured the ease of generating, distributing, storing and updating keys. It involved aspects such as key length, distribution mechanism and storage security. Low complexity means that the management process is simple, secure and low-cost. The actual application effects of different encryption algorithms in news video dissemination are shown in Table 3.

Table 3: Actual application effects of different encryption algorithms in news video dissemination

Algorithm type	Bidirectional GAN-honey encryption algorithm	AES encryption algorithm	Blowfish encryption algorithm	LSTM encryption algorithm	*p* value	Variance bar (standard deviation)
Encryption speed (s)	0.45	0.56	0.67	0.78	<0.001	±0.05
Decryption speed (s)	0.32	0.43	0.54	0.65	<0.001	±0.04
Encrypted video size (MB)	25.67	26.78	27.89	29.01	<0.01	±1.20
Video quality after decryption (PSNR)	35.89	34.56	33.23	32.12	<0.001	±0.50
Key management complexity	2.34	2.56	2.78	3.01	<0.01	±0.20
Anti-attack ability	4.56	3.45	3.23	3.01	<0.001	±0.30
Algorithm stability	0.98	0.92	0.89	0.85	<0.001	±0.03
Resource consumption (CPU %)	15.23	16.78	18.34	20.45	<0.01	±1.50
Memory usage (MB)	120.5	135.2	150.3	165.7	<0.001	±10.00
Encryption throughput (Mbps)	85.4	78.3	72.1	68.9	<0.001	±5.00
Error rate (%)	0.12	0.25	0.34	0.45	<0.001	±0.05

In Table 3, the bidirectional GAN-honey encryption algorithm outperformed the other three algorithms in terms of encryption and decryption speed, being approximately 0.11 seconds faster than the AES encryption algorithm, approximately 0.22 seconds faster than the Blowfish encryption algorithm, and approximately 0.33 seconds faster than the LSTM encryption algorithm, respectively. This indicates that the bidirectional GAN-honey encryption algorithm can more efficiently complete the encryption and decryption process of news videos, reduce user waiting time, and improve the timeliness of news video dissemination. In terms of encrypted video size, the bidirectional GAN-honey encryption algorithm generated the smallest encrypted video size, which was 25.67MB. In terms of key management complexity, the bidirectional GAN-honey encryption algorithm had the lowest key management complexity, which was 2.34. In terms of anti-attack ability, the bidirectional GAN-honey encryption algorithm had the strongest anti attack ability at 4.56. The bidirectional GAN-honey encryption algorithm had the highest stability, at 0.98. The high stability ensures that the algorithm can run stably in different environments and conditions, reducing interruptions or errors in news video dissemination caused by algorithm failures. In terms of resource consumption, the bidirectional GAN-honey encryption algorithm had the lowest resource consumption, at 15.23%. The lower resource consumption means that the algorithm requires less system resources and will not excessively occupy CPU and other resources, which is beneficial for running on resource limited devices and improving the compatibility and scalability of news video broadcasting. The *p* values were all less than 0.05, indicating that these differences were statistically significant. The variance bar showed the standard deviations of each indicator, further verifying the superiority and stability of the bidirectional GAN-honey encryption algorithm in multiple key performance indicators. The scalability evaluation results under different scenarios are shown in Table 4.

Table 4: Comparison of scalability evaluation in different scenarios

Scene type	High-definition live streaming scene				Mobile network scenarios			
Algorithm type	Bidirectional GAN-honey	AES encryption	Blowfish encryption	LSTM encryption	Bidirectional GAN-honey	AES encryption	Blowfish encryption	LSTM encryption
Length of news video (min)	30	25	20	15	20	15	10	5
Video resolution (px)	1920×1080	1280×720	800×600	640×480	1280×720	800×600	640×480	480×360
Network bandwidth (Mbps)	50	40	30	20	20	15	10	5
Number of users	1000	800	600	400	800	600	400	200
The number of encrypted videos	500	400	300	200	400	300	200	100
Multi-device compatibility	9.87	9.23	8.56	7.89	9.12	8.76	8.12	7.56
Cross-platform support	9.56	9.12	8.67	8.12	9.23	8.89	8.45	7.89
Concurrent processing capability	8.76	8.23	7.65	6.78	8.45	7.98	7.34	6.67

In Table 4, in high-definition live streaming scenarios, the bidirectional GAN-honey encryption algorithm supports up to 30 minutes of video, 1920 × 1080 resolution, 50Mbps bandwidth, and 1000 concurrent users, demonstrating strong processing capability and adaptability. In the mobile network scenario, although the overall performance has declined, the bidirectional GAN-honey encryption algorithm still maintained a high level, supporting 20-minute videos, 1280 × 720 resolution, 20Mbps bandwidth, and 800 concurrent users, which was significantly better than AES, Blowfish, and LSTM algorithms. This algorithm also demonstrated higher stability and scalability in terms of multi device compatibility, cross platform support, and concurrent processing capabilities. The study evaluated the resistance of the bidirectional GAN-honey encryption algorithm to brute-force cracking, selected plaintext attacks and pure ciphertext attacks through quantitative methods. For brute-force attacks, since the honey encryption algorithm used a 256-bit key length and the key space size was 2^{256}, this made brute-force attacks computationally infeasible. Even if it is assumed that the attacker has the computing power to try 10^{12} keys per second, the time required to crack it still exceeded the age of the universe. For plaintext attacks, honey encryption algorithms deceive attackers by generating seemingly valid but erroneous decryption results. Even if an attacker can select a specific plaintext and obtain its corresponding ciphertext, due to the distribution transformation and noise introduction during the decryption process, the attacker cannot obtain useful information about the original plaintext or key from the incorrect decryption result. In a simulated attack scenario, even if the attacker selects 1,000 different plaintexts for the attack, the probability of successfully restoring the original plaintext is still lower than 10^{-6}. For pure ciphertext attacks, since the ciphertext generated by the honey encryption algorithm will produce seemingly valid random results when mistakenly decrypted, attackers cannot infer any information about the plaintext from the ciphertext. In a simulated attack, even if the attacker has 1,000 ciphertext samples, they cannot recover the plaintext or key through statistical analysis or pattern recognition, and the attack success rate is close to zero. When facing selective ciphertext attacks, the "honeypot" mechanism of the algorithm deliberately introduces misleading information, making it impossible for attackers to infer the key or the original plaintext content even if they obtain part of the ciphertext. In side-channel attacks, algorithms reduce the possibility of attackers obtaining keys by analyzing the leaked information during the algorithm's execution by increasing the randomness and complexity of the operation. For statistical attacks, the algorithm utilizes a highly randomized encryption process to ensure that the statistical characteristics of the encrypted data cannot be distinguished from random noise, thereby effectively resisting such attacks.

To more comprehensively evaluate the performance of the proposed bidirectional GAN-honey encryption algorithm in the encryption protection of news video dissemination, the study made a side-by-side comparison of it with the current most advanced deep learning-based encryption methods, as shown in Table 5 specifically.

Table 5: Performance comparison of different encryption algorithms

Indicator	Encryption speed (s)	Decryption speed (s)	Compression ratio (%)
Bidirectional GAN-honey encryption	0.45	0.32	30.13
Variational autoencoder (VAE)	0.58	0.45	28.00
Watermarking method based on GAN	0.62	0.48	27.50
Neural Crypto model	0.55	0.40	29.00
p value	<0.001	<0.001	<0.01
Variance bar (standard deviation)	±0.05	±0.04	±1.20

In Table 5, the bidirectional GAN-honey encryption led with an encryption speed of 0.45 seconds. In terms of decryption speed, bidirectional GAN-honey encryption was also the fastest, taking 0.32 seconds. In terms of compression ratio, the bidirectional GAN-honey encryption reached 30.13%. The bidirectional GAN-honey encryption algorithm outperformed the other three algorithms in terms of encryption and decryption speed as well as compression ratio, demonstrating its advantages in efficiency and compression performance.

4 Discussion

The research conducted an in-depth analysis of the performance of the news video dissemination encryption protection method based on bidirectional GAN and honey encryption. The experimental results showed that this method outperformed the existing technologies in multiple key performance indicators. Compared with the multimedia data compression model combining GAN and fuzzy logic proposed by Khan A A et al. in reference [7], this method improved the encryption speed by 0.11 seconds, achieved a compression ratio of 30.13%, and maintained a relatively high video quality at the same time. Compared with the deep learning pattern recognition technology proposed by Amiri Z et al. in reference [8] and the hybrid feature extraction method based on CNN and HBA proposed by Badhagouni S K et al. in reference [10], this method also showed better performance in terms of adaptability and security. The possible reasons for the performance differences include the advantage of bidirectional GAN in potential code representation, which helps to capture the features of video content more effectively, as well as the enhanced encryption strength of the honey encryption algorithm, which improves security. Parameter sensitivity research further revealed the impact of different compression levels or encryption parameters on video quality and security, indicating that by adjusting these parameters, video quality can be optimized while maintaining security.

The limitations of the research lie in the fact that the scalability of high-resolution video or live streaming scenarios has not been fully verified. If attackers can understand the potential code distribution, there may be potential vulnerabilities, as well as resource constraints that may be faced in the deployment of low-power devices. These limitations point to the directions for future research, including testing the performance of algorithms in a wider range of application scenarios, enhancing the algorithms' defense capabilities against potential code distribution leaks, and further optimizing the algorithms to adapt to resource-constrained environments.

5 Conclusion

The study proposed a novel encryption protection method for the data security and privacy leakage risks faced by news videos in the dissemination process, which integrates the technical advantages of bidirectional GAN and honey encryption algorithm. With the excellent data processing capability of bidirectional GAN and the unique security features of honey encryption algorithm, this scheme was committed to protect the dissemination of news videos and realize efficient and solid encryption protection. Experimental results showed that the bidirectional GAN-honey encryption algorithm had excellent performance in terms of precision and recall. After 100 iterations, the precision rate approached 0.9 and stabilized, while the recall rate rapidly rose to over 0.8 and approached 1.0. The loss function value of the algorithm dropped to less than 10^{-4} after 20 iterations, demonstrating its excellent convergence performance. The algorithm encrypted and decrypted video files 0.11 seconds faster than the AES encryption algorithm, 0.22 seconds faster than the Blowfish encryption algorithm, and 0.33 seconds faster than the LSTM encryption algorithm. The size of the encrypted video file was also effectively compressed, with a minimum of 25.67MB, which was 1.11MB smaller than AES encryption algorithm, 2.22MB smaller than Blowfish encryption algorithm, and 3.34MB smaller than LSTM encryption algorithm.The bidirectional GAN and honey encryption algorithms had the highest stability, which reached 0.98, and the lowest resource consumption, which was only 15.23%. The proposed encryption protection method for news video distribution based on bidirectional GAN and honey encryption was effective. However, in practical application scenarios, the method still needs to be further optimized to adapt to diverse network environments and device conditions. Future research will be devoted to optimizing this problem and exploring the application potential of the method in other types of multimedia data to promote the further development of news video dissemination encryption.

References

[1] Hosny K M, Zaki M A, Lashin N A, Hamza H M. Fast colored video encryption using block scrambling and multi-key generation. The Visual Computer, 2023, 39(12): 6041 - 6072. DOI:10.1007/s00371 - 022 - 02711 - y.

[2] Hadjadj M A, Sadoudi S, Azzaz M S, Bendecheche H, Kaibou R. A new hardware architecture of lightweight and efficient real - time video chaos - based encryption algorithm. Journal of Real - Time Image Processing, 2022, 19(6): 1049 - 1062. DOI:10.1007/s11554 - 022 - 01244 - w.

[3] Dua M, Makhija D, Manasa P Y L, Mishra P. 3D chaotic map - cosine transformation-based approach to video encryption and decryption. Open Computer Science, 2022, 12(1): 37 - 56. DOI:10.1515/comp - 2020 - 0225.

[4] Qin L, Zhang G, You L. Application of CSK encryption algorithm in video synergic command systems. Journal of Organizational and End User Computing (JOEUC), 2022, 34(2): 1 - 18. DOI:10.4018/JOEUC.20220301.oa1.

[5] Dhingra D, Dua M. Medical video encryption using novel 2D Cosine - Sine map and dynamic DNA coding. Medical & Biological Engineering & Computing, 2024, 62(1): 237 - 255. DOI:10.1007/s11517 - 023 - 02925 - 9.

[6] Yolanda L. Pasia. Online News Stories on the 2022 Presidential Candidates. Acta Informatica Malaysia. 2023; 7(1): 63-66. DOI:10.26480/aim.01.2023.63.66.

[7] Khan A A, Laghari A A, Elmannai H, et al. Gan - iotvs: A novel internet of multimedia things - enabled video streaming compression model using gan and fuzzy logic. IEEE Sensors Journal, 2023, 23(23): 29434 - 29441. DOI:10.1109/JSEN.2023.3316088.

[8] Amiri Z, Heidari A, Navimipour N J, Unal M, Mousavi A. Adventures in data analysis: A systematic review of Deep Learning techniques for pattern recognition in cyber - physical - social systems. Multimedia Tools and Applications, 2024, 83(8): 22909 - 22973. DOI:10.1007/s11042 - 023 - 16382 - x.

[9] Maniriho P, Mahmood A N, Chowdhury M J M. A survey of recent advances in deep learning models for detecting malware in desktop and mobile platforms. ACM Computing Surveys, 2024, 56(6): 1 - 41. DOI:10.1145/363824.

[10] Badhagouni S K, ViswanadhaRaju S. HBA optimized Efficient CNN in Human Activity Recognition. The Imaging Science Journal, 2023, 71(1): 66 - 81. DOI:10.1080/13682199.2023.2176804.

[11] Huang P, Liu W. Chaotic Random Knowledge Recognition Model for Secure Data Encryption in Network Communication. Informatica, 2025, 49(20). DOI:10.31449/inf.v49i20.6625.

[12] Hedayati R, Mostafavi S. A lightweight image encryption algorithm for secure communications in multimedia IoT. Wireless Personal Communications, 2022, 123(2): 1121-1143. DOI:10.1007/s11277-021-09173-w.

[13] Yang W, Wang S, HuHu J, Karie N M. Multimedia security and privacy protection in the IoT: research developments and challenges. International Journal of Multimedia Intelligence and Security, 2022, 4(1): 20-46. DOI:10.1504/IJMIS.2022.121282.

[14] Lin C H, Hu G H, Chen J S, Yan J J, Tang K H. Novel design of cryptosystems for video/audio streaming via dynamic synchronized chaos - based random keys. Multimedia Systems, 2022, 28(5): 1793 - 1808. DOI:10.1007/s00530 - 022 - 00950 - 6.

[15] El Ogri O, Karmouni H, Sayyouri M, Qjidaa H. A new image/video encryption scheme based on fractional discrete Tchebichef transform and singular value decomposition. Multimedia Tools and Applications, 2023, 82(22): 33465 - 33497. DOI:10.1007/s11042 - 023 - 14573 - 0.

[16] Wen W, Tu R, Zhang Y, Fang Y, Yang Y. A multi - level approach with visual information for encrypted H. 265/HEVC videos. Multimedia Systems, 2023, 29(3): 1073 - 1087. DOI:10.1007/s00530 - 022 - 01037 - y.

[17] Geetha N, Mahesh K. An efficient enhanced full homomorphic encryption for securing video in cloud environment. Wireless Personal Communications, 2022, 123(2): 1553 - 1571. DOI:10.1007/s11277 - 021 - 09200 - w.

[18] Liu P, Wang X, Su Y. Image encryption via complementary embedding algorithm and new spatiotemporal chaotic system. IEEE Transactions on Circuits and Systems for Video Technology, 2022, 33(5): 2506 - 2519. DOI:10.1109/TCSVT.2022.3222559.

[19] Gao S, Liu S, Wang X, et al. New image encryption algorithm based on hyperchaotic 3D - IHAL and a hybrid cryptosystem. Applied Intelligence, 2023, 53(22): 27826 - 27843. DOI:10.1007/s10489 - 023 - 04996 - 5.

[20] Farri E, Ayubi P. A robust digital video watermarking based on CT - SVD domain and chaotic DNA sequences for copyright protection. Journal of Ambient Intelligence and Humanized Computing, 2023, 14(10): 13113 - 13137. DOI:10.1007/s12652 - 022 - 03771 - 7.

[21] Jiang B, He Q, Liu P, Maharjan S, Zhang Y. Blockchain empowered secure video sharing with access control for vehicular edge computing. IEEE Transactions on Intelligent Transportation Systems, 2023, 24(9): 9041 - 9054. DOI:10.1109/TITS.2023.3269058.

[22] Alsoliman A, Rigoni G, Callegaro D, et al. Intrusion detection framework for invasive FPV drones using video streaming characteristics. ACM Transactions on Cyber - Physical Systems, 2023, 7(2): 1 - 29. DOI:10.1145/3579999.

[23] Salem R B, Aimeur E, Hage H. A Multi - Party Agent for Privacy Preference Elicitation. Artificial Intelligence and Applications. 2023, 1(2): 98 - 105. DOI:10.47852/bonviewAIA2202514.