Chinese Journal of Electronics
vol. 33, no. 4, pp. 886–898, July 2024
https://doi.org/10.23919/cje.2023.00.382

Special Focus on Multi-Dimensional QoS Provision of Intelligent Edge Computing for IoT

RESEARCH ARTICLE

Blockchain Meets Generative Behavior Steganography: A Novel Covert Communication Framework for Secure IoT Edge Computing

Yuanlong CAO[1,3], Junjie LI[2,3], Kailin CHAO[2,3], Jianmao XIAO[2,3], and Gang LEI[2,3]

1. *School of Computer Information Engineering, Jiangxi Normal University, Nanchang 330022, China*
2. *School of Software, Jiangxi Normal University, Nanchang 330027, China*
3. *Jiangxi Blockchain Data Security and Governance Engineering Research Center, Jiangxi Normal University, Nanchang 330027, China*

Corresponding author: Yuanlong CAO, Email: ylcao@jxnu.edu.cn
Manuscript Received December 1, 2023; Accepted March 26, 2024

Abstract — The rapid development of Internet of things (IoT) and edge computing technologies has brought forth numerous possibilities for the intelligent and digital future. The frequent communication and interaction between devices inevitably generate a large amount of sensitive information. Deploying a blockchain network to store sensitive data is crucial for ensuring privacy and security. The openness and synchronicity of blockchain networks give rise to challenges such as transaction privacy and storage capacity issues, significantly impeding their development in the context of edge computing and IoT. This paper proposes a reliable fog computing service solution based on a blockchain fog architecture. This paper stores data files in the inter planetary file system (IPFS) and encrypts the file hash values used for retrieving data files with stream cipher encryption. It employs a steganographic transmission technique leveraging AlphaZero's Gomoku algorithm to discretely transmit the stream cipher key across the blockchain network without a carrier, thus achieving dual encryption. This approach aims to mitigate the storage burden on the blockchain network while ensuring the security of transaction data. Experimental results demonstrate that the model enhances the transmission capacity of confidential information from kilobytes (KB) to megabytes (MB) and exhibits high levels of covert and security features.

Keywords — Internet of things, Edge computing, Blockchain, Covert communication, Communication security, Generative behavior steganography.

Citation — Yuanlong CAO, Junjie LI, Kailin CHAO, *et al.*, "Blockchain Meets Generative Behavior Steganography: A Novel Covert Communication Framework for Secure IoT Edge Computing," *Chinese Journal of Electronics*, vol. 33, no. 4, pp. 886–898, 2024. doi: 10.23919/cje.2023.00.382.

I. Introduction

The number of Internet of things (IoT) networked devices is expected to grow exponentially with the advent of the 5G era [1]. Addressing the challenges of the quality of communication (QOC) and security in IoT communication using edge computing technology poses new challenges for researchers. Numerous studies have indicated that the integration of edge computing into the IoT creates a vast network encompassing multiple domains. Therefore, in such an extensive communication network, researching the security of communication and data holds significant importance [2], [3]. Many scholars have recognized the limitations of single-domain attack defenses, prompting the exploration of cross-domain solutions. Leveraging blockchain technology, which provides tamper-resistant data records without centralized authorization and ensures data integrity and authenticity [4], has become a widely adopted approach in cross-domain solutions [5].

As illustrated in Figure 1, the architecture of the Internet of things and blockchain network is built upon a specific data structure – chained blocks [6]. Each block

Associate Editor: Prof. Jiwei HUANG, China University of Petroleum, Beijing.

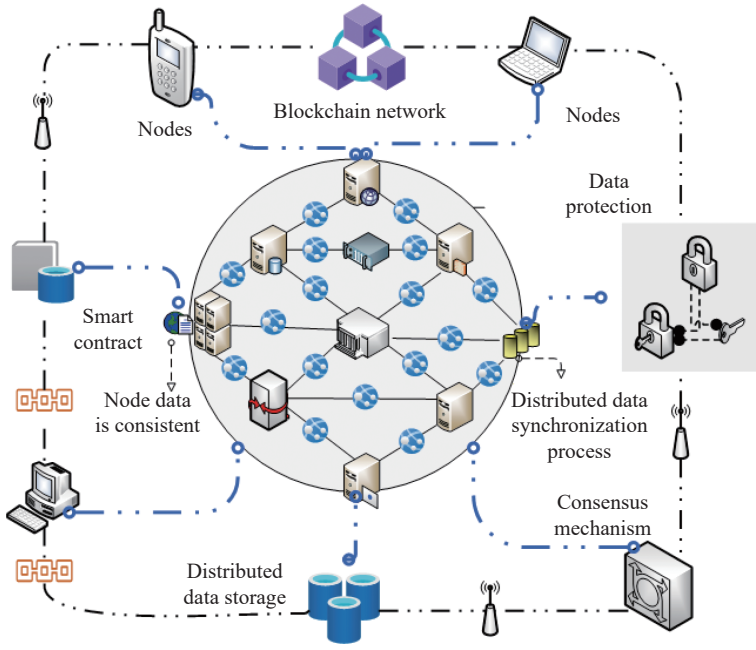

Figure 1 Architecture of the Internet of things and blockchain network.

contains a certain number of transaction records and is linked to the preceding block, forming an encrypted and verified chain structure that ensures data integrity. In this system, each smart device functions as a self-maintaining and self-regulating independent network node. These nodes can exchange information or verify identities with the assistance of smart contracts. This not only provides a high level of security and resilience [7], but also has lower computing and storage costs compared to centralized network architectures.

Despite various advantages demonstrated by blockchain technology, it still faces numerous challenges in practical applications [8]. Particularly in terms of data security, with the explosive growth of data, a significant amount of private information is transmitted within data streams. Publicly visible blockchain networks lack the ability for covert transmission and storage of this type of information [9]. In such scenarios, steganography provides a potential solution for blockchain in this predicament. The basic principle of steganography is to embed information into another carrier without attracting the attention of the outside world, so as to realize the covert transmission of information. For example, embedding secret information in digital images [10], audio [11], video [12], and other multimedia files makes it difficult for ordinary observers to detect. Its high level of covert makes it applicable in military, communication, and security fields [13]. Unlike traditional encryption techniques, steganography not only encrypts information but also completely conceals the existence of the information. However, it has its limitations [14]. Although this technology offers good covert in certain information communication scenarios, it still has some inherent flaws. For instance, once steganography is detected, the carrier itself may be regarded as a suspicious object. Furthermore, with the increase in computing capabilities, numerous steganography detection methods are gradually emerging, making the security of traditional steganography methods challenging [15].

In current research, some scholars have focused on empowering blockchain with steganography techniques to further enhance the security and privacy of the blockchain. Through the integration of steganography techniques, the blockchain achieves not only data encryption but also data covert [16]. Similarly, the application of steganography techniques in blockchain provides a public, immutable, and distributed platform. Simultaneously, it enhances the anonymity of steganography techniques, making the carriers of steganographic information more secure and resilient [17]. However, the traditional embedded steganography schemes currently used in research inevitably alter the statistical characteristics of the carriers, causing distortion in the carrier content. This distortion provides crucial detection evidence for steganalysis, making it challenging to resist steganalysis.

Therefore, this paper proposes and verifies a new steganography method without carrier information through a large number of experiments, which integrates steganography, stream cipher technology and various encryption strategies [18]. We utilize blockchain as a platform for information transmission and storage. This comprehensive, multi-layered security framework not only provides security through multiple encryption strategies but also significantly enhances the reliability and traceability of data through the distributed ledger and smart contract mechanisms of blockchain. In the experimental validation section, we demonstrate the high advantages of this integrated method in terms of covert, security, and reliability. In summary, the main contributions of this research include:

1) We proposed a ternary carrier-less steganography method based on the moves of Gomoku (Five in a Row).

2) We constructed a blockchain dual encryption system that integrates carrier-less steganography techniques to achieve highly secure information transmission and enhance system robustness.

3) We utilized an AlphaZero-based Gomoku game model [18] as the key generation model for stream cipher, addressing the challenge of sharing stream cipher keys with redundancy while ensuring randomness.

The subsequent sections of this paper are organized as follows: Section II reviews relevant prior work and provides a theoretical background, laying the foundation for the subsequent methodology and experimental design. Section III introduces the structure of the proposed framework. Section IV details the experimental design. Finally, Section V discusses the experimental results and their significance. We firmly believe that this study will provide new perspectives and directions for security research in the field of information communication.

II. Related Work

Since the widespread applications of blockchain technology in various fields such as supply chain, healthcare, finance, and the Internet of things [19]–[21], research on blockchain technology has entered a period of rapid development. Currently, numerous researchers are actively investigating the scalability, security, privacy protection, and integration with other technologies [22] (such as artificial intelligence, secure multi-party computation, federated learning) of blockchain. Especially, strengthening the data security of blockchain network has become the focus of current research [23].

Some researchers have focused on introducing new technologies to ensure data integrity and tamper resistance. For example, Wei *et al.* [24] proposed a modifiable blockchain framework for secure federated learning in industrial IoT, presenting a "security-enhanced solution". Similar studies include Qahtan *et al.*'s work [25], who introduced a multidimensional security and privacy benchmarking framework for blockchain-based IoT healthcare systems in Industry 4.0. Mothukuri *et al.* [26] integrated federated learning with blockchain technology to address the challenges in data security sharing encountered by existing federated learning methods. However, the current research on these types of methods still leans towards the academic realm. The "security-enhanced solution" proposed by Wei *et al.* exhibits certain vulnerabilities to model update attacks by malicious agents, and its robustness in secure transmission is not entirely flawless. Although the "multi-dimensional evaluation scheme" proposed by Qahtan *et al.* shows remarkable practical results, it is difficult to apply in practice because of its complex structural design.

Similarly, some researchers focus on integrating new cryptographic techniques with deep learning to ensure data privacy and security. For instance, Kumar *et al.* [27] proposed a blockchain and deep learning-based framework for privacy protection and threat identification in networks. Kumar *et al.* [28] presented a privacy-preserving security framework using blockchain-based deep learning to provide privacy and security in cooperative intelligent transportation systems. Dang *et al.* in [29] designed a blockchain and cryptography-based power business data sharing system to address issues such as the lack of dynamics in data transmission encryption, long data file download times, and poor security in the presence of multiple user nodes. However, the current research in this category still remains largely theoretical, with the primary limitation being computational resources. For example, in the "comprehensive security solution" proposed by Kumar *et al.*, the deep learning module requires substantial computational resources, making it challenging to fully configure the resources during actual network transmission and synchronization processes. Similarly, Kumar *et al.* achieve intelligent transmission and uploading through the construction of a "multilayer security solution", but its complexity affects real-time performance and cannot be practically applied due to computational resource limitations.

A significant amount of research has made valuable contributions to enhancing the data security of blockchain networks. However, current studies exhibit certain limitations, including reliance on specific encryption algorithms, lack of defense against various types of attacks, and issues related to the flexibility and scalability of data in different application scenarios. These limitations not only limit the wide application of blockchain technology, but also provide researchers with a new exploration direction. Therefore, recent research has increasingly focused on the integration of steganography techniques to enhance the data covert and operability of blockchain networks from various perspectives, addressing the protection of data as a noteworthy and exploratory problem.

Some studies have explored the integration of steganography techniques to enhance the covert and operability of blockchain data. For example, Mohsin *et al.* in [30] proposed a novel method based on blockchain and steganography for securely updating and sharing the COVID-19 data between hospitals. This method effectively improves the security of medical data transmission. Xu *et al.* [31] introduced a new steganography method that broadcasts secret data in the blockchain to enhance data security. This "data broadcast security enhancement method" increases the security of data transmission to some extent. Rede *et al.* [32] used steganography combined with blockchain technology to address security vulnerabilities that may arise when sharing hash values of identity documents, significantly enhancing the security of personal identity authentication. However, the existing research in this field still faces challenges, mainly reflected in low efficiency or limited applicability to different data types. For instance, the method proposed by Mohsin *et al.* is primarily limited to the healthcare

data domain, lacking universal applicability to other fields. Xu *et al.* did not consider optimization for the blockchain network situation and steganographic carrier capacity, raising doubts about its practical application effects and environments. Rede *et al.*'s work is constrained by the efficiency limitations of the method, making it challenging for practical applications.

Although the work conducted by the aforementioned researchers in the research area of "integrating steganography techniques to enhance blockchain data security" still presents certain challenges, existing research demonstrates that this direction is an effective approach to improving the security of blockchain data and exploring new avenues for steganography techniques. Steganography can effectively prevent data tampering or theft, while blockchain can provide a fair and anonymous platform under smart contracts for steganography techniques. Hence, this paper focuses on using Gomoku move actions as a generative behavioral steganography method, enhancing the capacity of steganographic carriers using a ternary approach, overcoming the transmission limitations of small batches of data in steganography techniques. The blockchain is optimized by using stream cipher to achieve security, thus realizing anonymity of steganography carrier and flexibility of data transmission. This not only addresses the capacity limitations of traditional steganography techniques but also enhances the security of data transmission and the non-traceability of steganographic carriers under a multi-layered encryption strategy.

III. Methodology

This paper introduces a generative steganographic method for Gomoku integrated with AlphaZero in ternary representation (AGSM) and stream cipher technology into the blockchain network, and proposes a highly robust blockchain covert communication model (BCCM). The framework of BCCM is as depicted in Figure 2, consists of an integrated stream cipher embedding module and an integrated stream cipher extraction module, both combined with AlphaZero-based ternary Gomoku behavioral generative steganography.

- In the stream cipher embedding module integrated with AGSM:

Step 1: Alice uploads a file through the IPFS system. The file's hash is encrypted using a key with stream cipher encryption.

Step 2: The key is embedded in the Gomoku board through generative steganography.

Step 3: Alice sends the encrypted file hash to Bob and stores the Gomoku board in the blockchain network.

- In the stream cipher extraction module integrated with AGSM:

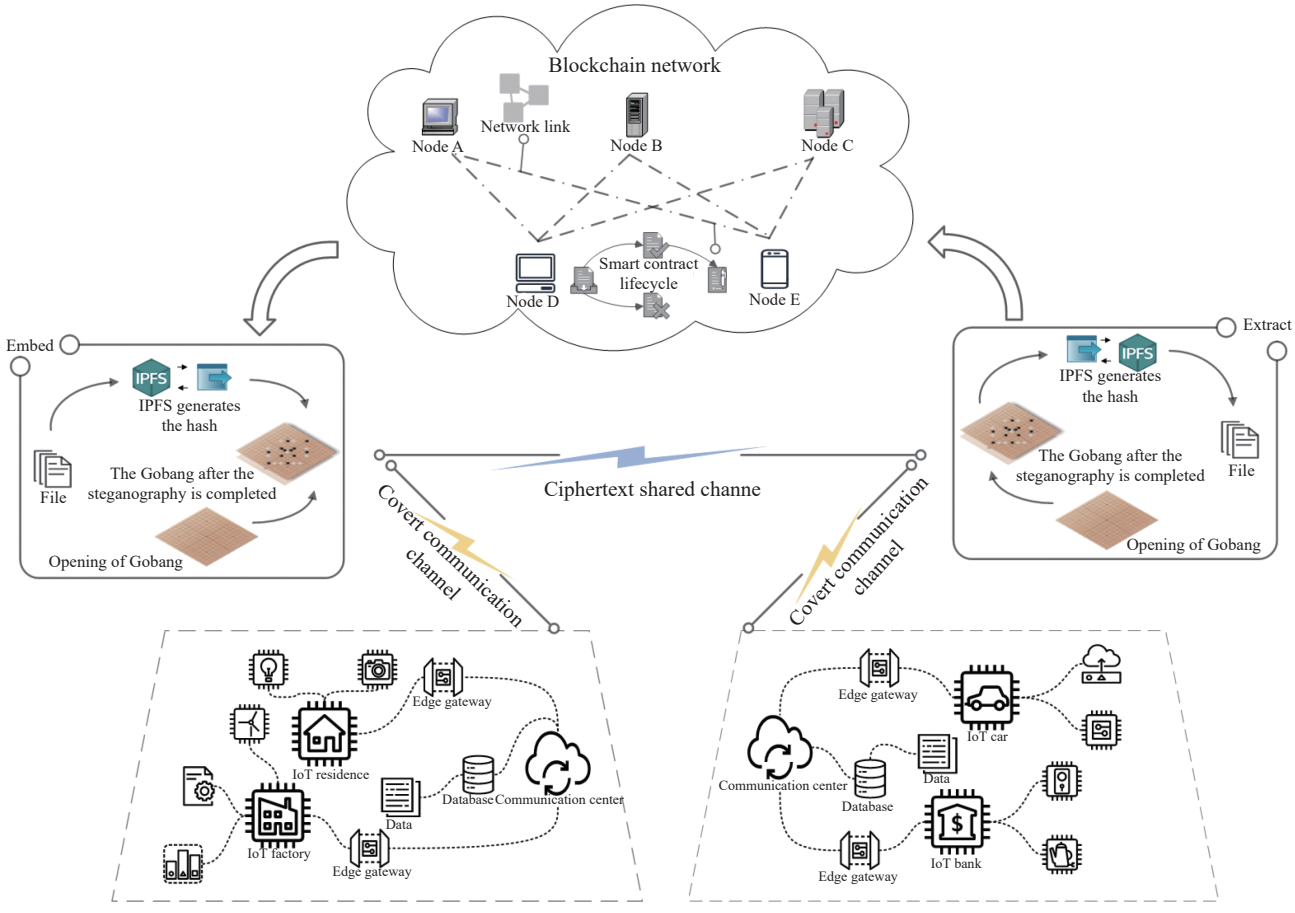

Figure 2 Overview of the methodology.

Step 1: Bob acquires the encrypted file hash through a ciphertext-sharing channel.

Step 2: Bob retrieves the Gomoku board from the blockchain network, extracts the key using generative steganography, and utilizes the key to obtain the file hash value.

Step 3: Bob downloads the file from the IPFS system using the obtained file hash value.

By combining the tamper-resistant nature of blockchain with the imperceptibility of Gomoku behavioral steganography, BCCM is optimized in terms of covert and security.

1. AGSM and stream cipher

The Gomoku move model based on AlphaZero is similar to AlphaGoZero [33]. It primarily consists of a Monte Carlo tree search (MCTS) and a reinforcement learning network, requiring no expert dataset. However, AlphaZero has a faster training speed compared with AlphaGoZero. Specifically, the reinforcement learning network is a neural network denoted as f_θ with parameters θ. This network takes the game state and model parameters as input and outputs probabilities and values. The relationship is as follows:

$$(p, v) = f_\theta(s) \tag{1}$$

$$p_a = \Pr(a|s) \tag{2}$$

the move probability vector p represents the probability of choosing each move action a, while the value v is the predicted evaluation value of the current player winning the game in the game state s. MCTS can be viewed as a self-play algorithm that, given neural network parameters θ and game state s, calculates the move vector recommended by the search probability. The formula is as follows:

$$\pi = \alpha_\theta(s) \tag{3}$$

$$\alpha_a \propto N(s, a)^{\frac{1}{T}} \tag{4}$$

where T is the temperature parameter. The reinforcement network uses MCTS to calculate each move action. Initially, the neural network is initialized with random weights θ. In each subsequent iteration $i \geq 1$, self-play is performed. For the t-th time step, the neural network f_θ utilizes the network from the previous iteration $f_{\theta_{-1}}$ to execute MCTS search. Moves are then sampled using the probability distribution π_t. The game terminates at step y when both players pass, the search value is below a threshold, or the game exceeds the maximum length. The match is then scored, and a reward $r_y \in \{-1, 1\}$ is assigned.

The data for each time step t is stored as (S_t, π_t, Z_t), where $Z_t = \pm r_y$. The new network parameters θ' are trained using data (s, π, z) uniformly sampled from all time steps in the previous iteration. The neural network is updated to minimize the error between the predicted value v and the winner z in self-play, maximizing the similarity between the neural network move probabilities p and search probabilities π. Specifically, the loss function l, which is the sum of mean squared error and cross-entropy losses, is used. Gradient descent is employed to adjust the parameters θ. The formula can be expressed as follows:

$$l = (z - v)^2 - \pi^y \log p + c\,||\theta||^2 \tag{5}$$

After AlphaZero completes the moves on the initial chessboard, the final chessboard will be output, and this chess record is encoded by a ternary encoder. Specifically, for a Gomoku board with dimensions of 15×15, the top-left corner is marked with coordinates (1,1), and the bottom-right corner is marked with coordinates (15,15). For each grid x, if a white piece is placed, it is marked as 1; if no piece is placed, it is marked as 0; and if a black piece is placed, it is marked as 2. This results in the chessboard matrix $\boldsymbol{M}$, represented as follows:

$$\boldsymbol{M} = \begin{bmatrix} x_{1,1} & \cdots & x_{1,15} \\ \vdots & \ddots & \vdots \\ x_{15,1} & \cdots & x_{15,15} \end{bmatrix},\ x_{i,j} \in \{0, 1, 2\} \tag{6}$$

Transforming this matrix into a one-dimensional vector yields the ternary-encoded data m as below:

$$m = x_{1,1} \ldots\ x_{1,15} \ldots\ x_{15,1} \ldots\ x_{15,15} \tag{7}$$

Convert the ternary encoded data to binary data, which can be used as the key S input for a stream cipher encryptor. Encrypt the binary hash H of the file using the stream cipher, resulting in ciphertext Q:

$$Q = S \oplus H \tag{8}$$

Since the stream cipher is a symmetric and reversible encryption method, inputting the key S into the stream cipher encryptor and decrypting the ciphertext Q yields the encrypted binary hash H' of the file:

$$H = S \oplus Q \tag{9}$$

As Gomoku is a game played on a 15×15 board. In Gomoku, each position can be empty (without a piece), occupied by a white piece, or occupied by a black piece. Therefore, for each position, there can be three states: empty, white, or black. If we consider each position on the chessboard as a point, then the combination of the states of these points constitutes the position combination of a five piece chessboard. For each position, there can be three states, so the total number of possible position combinations is $3^{15\times15}$. This number is far greater than the number of atoms in the universe, so there are many combinations of positions on the Go board that are almost inexhaustible. In theory, AlphaZero's falling habits

have extremely high randomness. In summary, the theoretical collision probability of m is $\frac{1}{3^{225}}$, indicating that the key S possesses sufficient randomness. Assuming the encryption of a 128-bit plaintext using the above stream cipher, the brute-force attack space complexity is 2^{128}, which is considered relatively secure given the current computational capability.

2. Fusion of AGSM stream cipher embedding module

At this stage, Alice and the recipient Bob establish an IPFS cluster and upload the file using IPFS to obtain the file hash. As shown in Figure 3, Alice uses the initial chessboard as the seed for generative steganography and the final chessboard as the key. The hash value is encrypted into ciphertext using a stream cipher. In addition, this article can only upload the state matrix of the opening game of Gomoku to the blockchain network, rather than uploading images to the blockchain network. This methodology guarantees a balance between covert operation and security, mitigating the risk of uploading sensitive privacy data in plaintext to the blockchain.

The specific steps of this embedding process are as follows:

1) Alice uploads the file to IPFS and obtains the file hash returned by IPFS.

2) Alice selects an opening move in a Gomoku game.

3) Alice inputs the Gomoku opening move into the AlphaZero model to obtain the final state of the Gomoku game. The moves in this chess record are encoded as ternary data.

4) Alice converts the ternary chessboard data to binary data and inputs it, along with the file hash value, as the key and plaintext into the stream cipher model to obtain the ciphertext.

5) Alice uploads the opening chess record to the blockchain network and sends the blockchain address where the record is located along with the ciphertext to Bob.

Algorithm 1 Information embedding process

Require:
Input: DataFile F, Gomoku opening move B.
Output: Ciphertext M, Gomoku endgame E.

if (File is of the correct file type) **then**
  if (File passes required checks) **then**
    fileHash ← UploadFileToIPFS(F);
  else
    File is not compliant;
  end if
else
  File is not of the correct file type;
end if
if (fileHash not exists) **then**
  Return;
end if
B ← [15][15];
for (i=1 to 15) **do**
  // Choose a game opening for the gobang
  for (j=1 to 15) **do**
    Pieces ← GenerateChessPieces(); //Randomly choose to generate black pieces, white pieces, or no pieces
    while (Not comply with the rule) **do**
      Pieces ← GenerateChessPieces();
    end while
    $B[i][j]$ ←Pieces;
  end for
end for
E ← AlphaZeroModel(B);
ternaryData ← EncodeToTernary(E);
binaryData ← ConvertTernaryToBinary(ternaryData);
M ← StreamCipherModel(fileHash, binaryData);
uploadToBlockchain(B); // Upload the game opening to the blockchain
sendToBob(M).

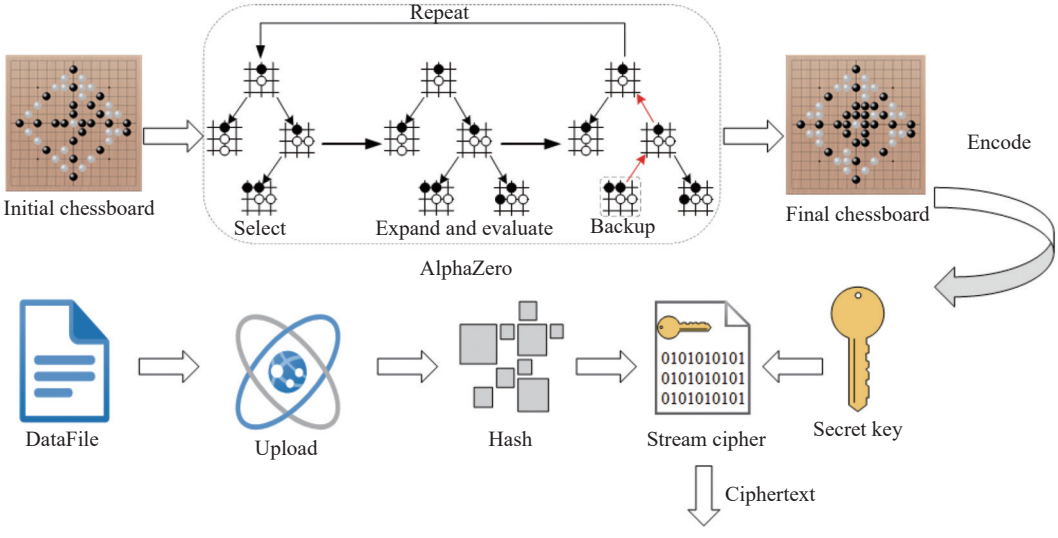

Figure 3 Embedding process diagram.

3. Fusion of AGSM stream cipher extraction module

Upon receiving the ciphertext from Alice, Bob downloads the Gomoku opening chessboard from the agreed-upon blockchain network. As shown in Figure 4, Bob uses the opening chessboard as the seed for generative steganography, the endgame chessboard as the key, and decrypts the ciphertext into the file hash using a stream cipher. Bob then uses the hash value to download the file from IPFS.

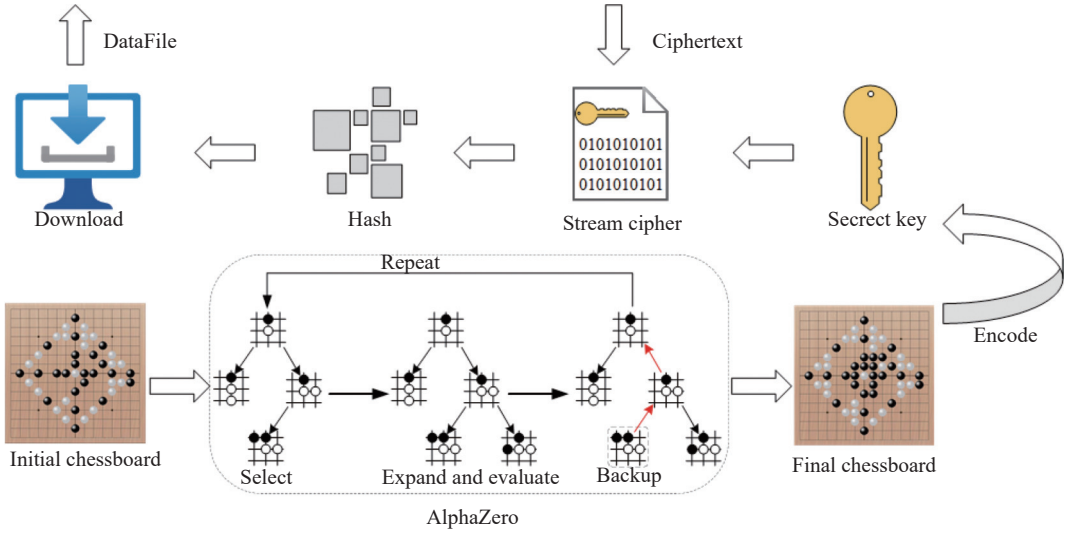

Figure 4 Extraction Process Diagram.

The specific steps of this embedding process are as follows:

1) Bob receives the ciphertext sent by Alice.

2) Bob downloads the Gomoku opening from the blockchain network.

3) Bob inputs the Gomoku opening into the AlphaZero model to obtain the final state of the Gomoku game. The moves of this chess game are encoded as ternary data.

4) Finally, Bob converts the ternary data to binary data and inputs it along with the ciphertext into the stream cipher model to obtain the file hash value.

5) Bob inputs the file hash value into IPFS to retrieve the file.

Algorithm 2 Information extraction process

Require:

Input: Ciphertext M, Gomoku opening B.

Output: DataFile F, Gomoku endgame E.

while (Connection is open) **do**
  if (Message is received) **then**
    messageDelivered ← true;
  else if(Timeout occurs) **then**
    handle timeout as needed;
  else if (Connection is closed) **then**
    handle closed connection;
  end if
  if (messageDelivered) **then**
    if (Message status is confirmed) **then**
      B ← DownloadChessBoardFromBlockchain();
      E ← AlphaZeroModel(B); // Apply AlphaZero model to get the game result
      ternaryData ← EncodeToTernary(E);
      binaryData ← ConvertTernaryToBinary(ternary Data);
      fileHash ← StreamCipherModel(M, binaryData);
      F ← FetchFileFromIPFS(fileHash); // Retrieve the file from IPFS using the hash value
    else
      messageDelivered ← false;
    end if
  end if
end while

IV. Experiment

This section conducted experiments and analysis on the covert capacity, robustness, and covert of the proposed method, comparing it with existing methods. Inspired by Cao [34] and SHE [35], this study follows a similar experimental approach, and some results are referenced. AlphaZero is employed for Gomoku game move prediction, using the Paddle-2.0.2 deep learning framework and an RTX 3060 12GB GPU for 1100 training rounds. During training, after each game, the sample data is stored in the experience replay pool, and samples are collected from it for training the reinforcement learning network. The reinforcement learning network comprises a value network and a policy network. As the policy and value functions improve, the training samples are continually enhanced, gradually improving the capabilities of the trained agent. Mean squared error loss and cross-entropy loss are used to optimize the value network and

policy network, respectively. The formulas can be expressed as follows:

$$l_v = (z - v)^2 \tag{10}$$

$$l_p(\pi_t, p_t) = -\pi_t^T \log p_t \tag{11}$$

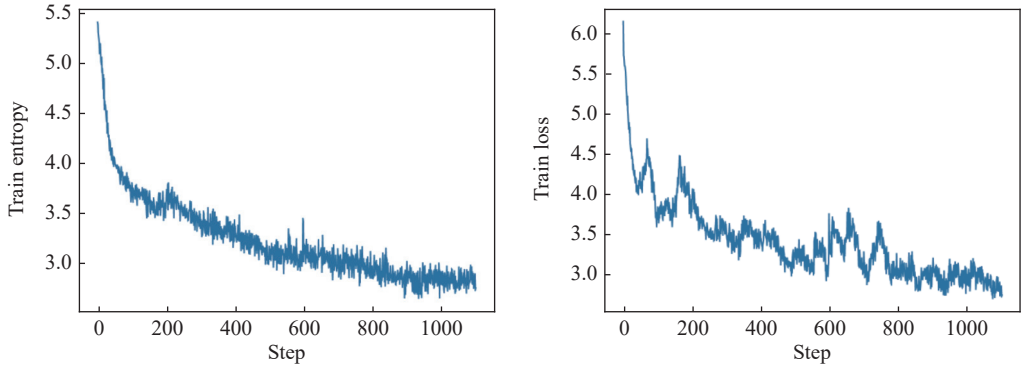

Figure 5 Extraction process diagram.

From Figure 5, it can be observed that the cross-entropy and mean squared error of the model gradually decrease. This indicates that the model's accuracy in predicting neural network outputs is gradually improving, and the difference between the output policy of the neural network and the policy output by MCTS is decreasing.

1. The capacity of covert

This paper conducted simulation experiments on sensitive documents of different sizes, encrypting these sensitive documents and uploading them to IPFS. The resulting hash values from IPFS were successfully embedded into Gomoku game boards for covert transmission. The comparison of the transmitted secret information quantities among different methods in the blockchain covert communication model is shown in Table 1.

Table 1 Transmission of secret information scale

Methods	Capacity
Literature [36]	Bit
Literature [37]	Kb
Literature [38]	Bit
Literature [39]	Bit
BCCM	Mb

From Table 1, it can be observed that compared to traditional methods, the proposed method in this study achieves a significant improvement in the order of magnitude of transmitted secret information, reaching MB. This is mainly because the study integrates blockchain and IPFS to achieve collaborative storage on-chain and off-chain. IPFS is used for off-chain storage of sensitive files, while the blockchain stores Gomoku game boards with embedded IPFS hash values. This collaborative approach effectively addresses the storage capacity issue of the blockchain, ensuring the integrity, authenticity, and security of the Gomoku game openings.

2. Robustness

This paper first simulates the potential attacks, such as noise, filtering, etc., that encrypted Gomoku game records may encounter during the communication process, as described in Table 2. Subsequently, the robustness of the proposed method is evaluated using the bit error rate (BER) as a robustness assessment metric. The BER formula is as follows [40]:

$$\mathrm{BER} = \frac{\sum_{i=1}^{m} p_i \oplus q_i}{m} \tag{12}$$

Table 2 Simulated noise attacks

Attacks	Parameter	Literature [41]	BCCM
Rotation	50°	53.6%	0
Gaussian noise	σ (0.01)	28.2%	0
Salt and pepper noise	σ (0.01)	14%	0
Mean filter	3×3	14%	0
Median filter	3×3	22.8%	0
Gaussian filter	3×3	10.4%	0

As shown in Figure 6 and Table 2, the test results indicate that the proposed method exhibits high robustness against common attacks in communication channels. This is primarily attributed to the substantial color contrast between black and white pieces in Gomoku, allowing the game records to remain distinguishable even when subjected to attacks. Moreover, Gomoku gameplay does not rely on the specific order of moves in the record; it only requires the current state of the game board for deduction. Consequently, the recipient retains the ability to accurately deduce the final state of the Gomoku game, even when confronted with partially compromised game records.

3. Covert

Covert refers primarily to the imperceptibility of the steganographic process, with mean-square error (MSE)

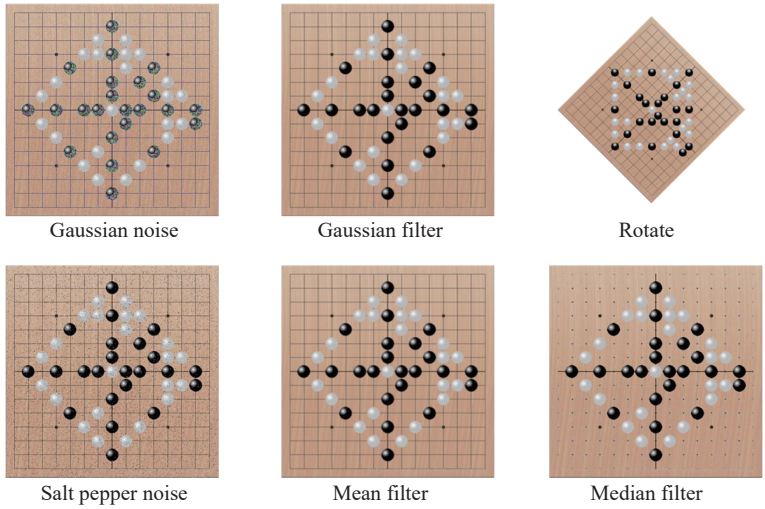

Figure 6 Illustration of noise attacks.

and structural similarity index (SSIM) serving as the primary metrics for evaluation. MSE primarily reflects the degree of difference between the cover image and the stego image. This metric is employed to assess the quality of the stego image obtained after embedding secret information. MSE is calculated by summing the squared differences of all pixel values between the cover image and the stego image, divided by the total number of pixels. A smaller MSE value indicates a better steganographic method. The formula for MSE is expressed as follows [42]:

$$\mathrm{MSE} = \sum_{i=1}^{M}\sum_{j=1}^{N} \frac{\left(I\left(i,\ j\right) - I'\left(i,\ j\right)\right)^2}{M^*\ N} \tag{13}$$

where i and j respectively denote the rows and columns of the image. $I(i,j)$ represents the pixel at the i-th row and j-th column in the cover image, while $I'(i,j)$ represents the pixel at the i-th row and j-th column in the stego image.

Structural similarity index (SSIM) is a measure of similarity between two images. A higher SSIM value indicates a greater similarity between the cover image and the stego image. The formula for SSIM is expressed as follows [42]:

$$\mathrm{SSIM}\left(x,y\right) = \frac{\left(2\mu_x\mu_y + C_1\right)\left(\sigma_{xy} + C_2\right)}{\left(\mu_x^2 + \mu_y^2 + C_1\right)\left(\sigma_x^2 + \sigma_y^2 + C_2\right)} \tag{14}$$

where μ_x represents the mean of x, μ_y represents the mean of y, σ_x^2 represents the variance of x, σ_y^2 represents the variance of y, σ_{xy} represents the covariance between x and y, and C_1 and C_2 are constants used to maintain stability.

From the experimental results in Table 3, it can be observed that, compared to classic steganographic methods such as SUNI [43], WOW [44], HUGO [45], MiPOD [46], etc., the proposed method in this paper, due to the absence of a steganographic carrier, does not modify the chessboard containing the secret, and the monitoring party in the communication process cannot detect any traces of chessboard modification. Consequently, the model achieves a higher level of covert.

Table 3 Results of MSE and SSIM

	MSE (%)		SSIM (%)	
	0.4 bpp	0.04 bpp	0.4 bpp	0.04 bpp
HUGO	9.05	0.68	99.98	99.99
S-UNIWARD	7.65	0.56	99.98	99.99
WOW	14.79	1.91	99.95	99.99
MiPOD	8.61	0.5	99.97	99.99
BCCM	N/A	N/A	N/A	N/A

Steganalysis tools can detect steganographic activities, thereby compromising the covert of communication models. In this study, conventional steganalysis algorithms, SRNet [47] and Zhu-Net [48], were employed to analyze the aforementioned embedded steganographic methods and the proposed method in this paper, yielding detection accuracy results (Acc). Acc represents the detection accuracy of the steganalysis method, and a value closer to 50% indicates stronger resistance to steganalysis. The formula for Acc is as follows [42]:

$$\mathrm{Acc} = \frac{T_p + T_n}{T_p + F_n + F_p + T_n} \tag{15}$$

where T_p represents the number of samples correctly predicted as containing hidden information by the steganalysis method, F_p represents the number of samples incorrectly predicted as not containing hidden information, T_n represents the number of samples correctly predicted as not containing hidden information, and F_n represents the number of samples incorrectly predicted as containing hidden information. The steganalysis results are shown in Figure 7. It is apparent that the aforementioned embedded steganographic techniques, which entail modifying the carrier to incorporate clandestine in-

formation, unavoidably induce alterations in the statistical attributes of the carrier. As a result, they are difficult to resist detection by various steganalysis tools. In contrast, the method proposed in this paper integrates steganographic behavior seamlessly with regular Gomoku game behavior, without modifying the chessboard or causing distortion in the game records. This approach effectively withstands steganalysis.

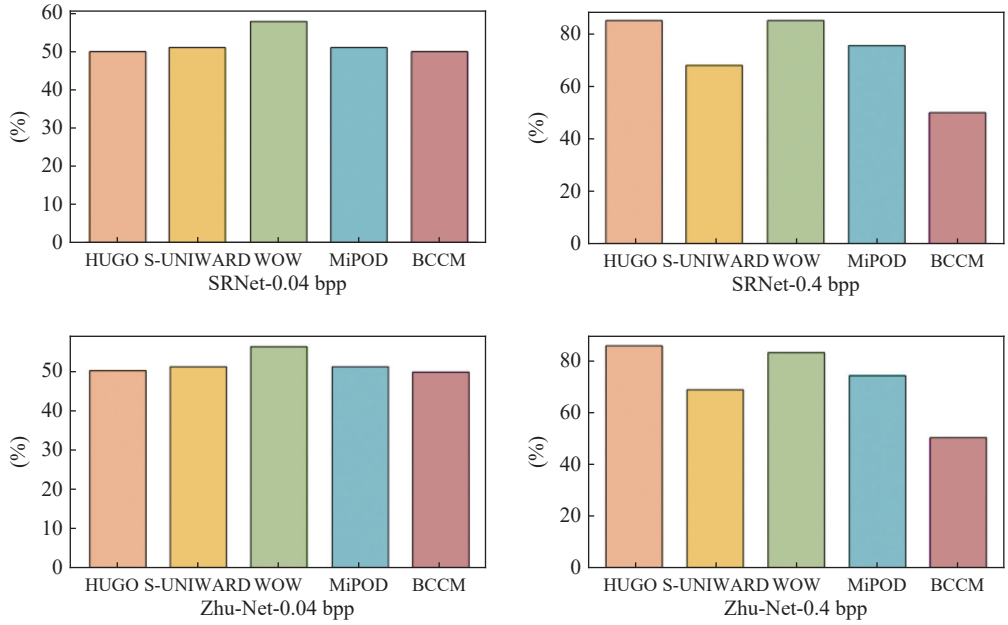

Figure 7 Steganalysis resistance chart.

As this paper utilizes Gomoku as the steganographic behavior, the rationality of the Gomoku records becomes particularly important. Since placing a stone in the center of the board is more advantageous than at the edges, conventional Gomoku strategies often involve the first move placed at the center, followed by spreading moves around it. Therefore, the stone placement pattern in the game records is more in line with a normal distribution. This paper establishes a Cartesian coordinate system with the center of the board as the origin. The distance between intersections located in the same row or column on the board is set to 1. In a 15×15 board, the coordinate ranges for the x-axis and y-axis are both $[-7, +7]$. The x and y coordinates follow independent normal distributions $N(\mu, \sigma)$, and their probability density function is given by

$$f(x) = \frac{1}{\sqrt{2\pi}\sigma} \exp\left(-\frac{(x-\mu)^2}{2\sigma^2}\right) \tag{16}$$

So, when $\mu = 0$, the larger the σ is, the more dispersed the stone placements, and the smaller the σ is, the more concentrated the stone placements in the center of the board. In this paper, when generating the opening moves for Gomoku records, the first move is specified to be at the center of the board. Subsequent moves follow a random placement strategy that conforms to a normal distribution. The normal distribution model is set with $\mu = 0$ and $\sigma = 7$, resulting in $\sigma = 7$.

Following the above-mentioned method, this paper generated 10000 pairs of coordinates, and their distribution pattern is illustrated in Figure 8. It is evident that coordinates have a probability of over 99% of falling within the chessboard, adhering to the standard Gomoku stone placement pattern. During the Gomoku record generation process, if the stone coordinates fall outside the board's boundaries or overlap with previously placed stones, new coordinates are obtained.

V. Conclusion and Future Prospects

This paper proposes a highly robust blockchain covert communication model (BCCM), to achieve covert transmission of sensitive files within a blockchain. The model employs stream cipher technology to encrypt file hash values for security assurance. Additionally, it utilizes a generative steganographic method that integrates AlphaZero's ternary Gomoku behavior to embed the key within a Gomoku game, enhancing the covert of the transmission. The performance of the model is evaluated by comparing metrics such as MSE and SSIM with traditional methods. Experimental results indicate a significant improvement in the transmission of secret information, coupled with high levels of covert and security. However, the model has certain limitations, requiring a reanalysis of the game records during the extraction of secret information. In the future, we will extend the proposed steganography method to consider more practical application scenarios. The research will explore carrier-free covert communication methods based on behavioral protocols. Within the framework of adhering to estab-

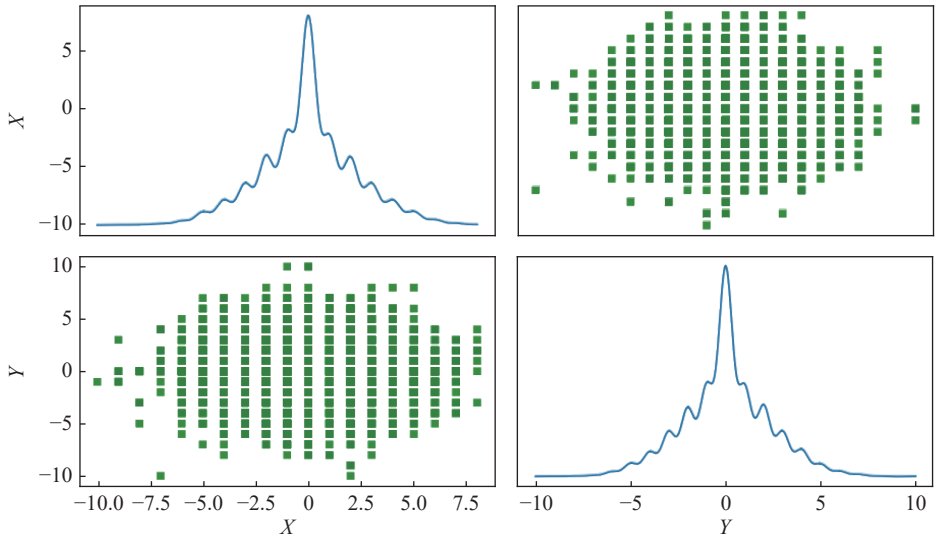

Figure 8 Stone placement pattern chart for coordinates.

lished game rules, communication parties seek to promptly deduce actions that directly convey confidential information, relying on pre-established protocols, thereby obviating the necessity for computer-assisted calculations. In the future, we will extend the proposed steganography method to consider more practical application scenarios. In addition, this article will also use BCCM to optimize asymmetric encryption methods, embed public keys into chessboards, and use steganography for hiding. To facilitate the implementation of public key authentication and encryption in special military scenarios, achieving the effect of resisting man in the middle hijacking attacks without the need for third-party notarization.

References

[1] J. W. Huang, C. X. Zhang, and J. B. Zhang, "A multi-queue approach of energy efficient task scheduling for sensor hubs," *Chinese Journal of Electronics*, vol. 29, no. 2, pp. 242–247, 2020.

[2] M. L. Dai, S. Y. Xu, S. J. Shao, *et al.*, "Blockchain-based reliable fog-cloud service solution for IIoT," *Chinese Journal of Electronics*, vol. 30, no. 2, pp. 359–366, 2021.

[3] J. W. Huang, H. Gao, S. H. Wan, *et al.*, "AoI-aware energy control and computation offloading for industrial IoT," *Future Generation Computer Systems*, vol. 139, pp. 29–37, 2023.

[4] Y. Q. Liu, K. Qian, K. Wang, *et al.*, "BCmaster: A compatible framework for comprehensively analyzing and monitoring blockchain systems in IoT," *IEEE Internet of Things Journal*, vol. 9, no. 22, pp. 22529–22546, 2022.

[5] J. Su and M. N. Jiang, "A hybrid entropy and blockchain approach for network security defense in SDN-based IIoT," *Chinese Journal of Electronics*, vol. 32, no. 3, pp. 531–541, 2023.

[6] S. L. Xu, C. L. Guo, R. Q. Hu, *et al.*, "Blockchain-inspired secure computation offloading in a vehicular cloud network," *IEEE Internet of Things Journal*, vol. 9, no. 16, pp. 14723–14740, 2022.

[7] D. X. Liu, A. Alahmadi, J. B. Ni, *et al.*, "Anonymous reputation system for IIoT-enabled retail marketing atop PoS blockchain," *IEEE Transactions on Industrial Informatics*, vol. 15, no. 6, pp. 3527–3537, 2019.

[8] Y. J. Han, Y. W. Zhang, and S. H. Vermund, "Blockchain technology for electronic health records," *International Journal of Environmental Research and Public Health*, vol. 19, no. 23, article no. 15577, 2022.

[9] M. Naz, F. A. Al-zahrani, R. Khalid, *et al.*, "A secure data sharing platform using blockchain and interplanetary file system," *Sustainability*, vol. 11, no. 24, article no. 7054, 2019.

[10] X. J. Liu, W. B. Wang, D. Niyato, *et al.*, "Evolutionary game for mining pool selection in blockchain networks," *IEEE Wireless Communications Letters*, vol. 7, no. 5, pp. 760–763, 2018.

[11] M. Massaro, "Digital transformation in the healthcare sector through blockchain technology. insights from academic research and business developments," *Technovation*, vol. 120, article no. 102386, 2023.

[12] S. Ghimire, J. Y. Choi, and B. Lee, "Using blockchain for improved video integrity verification," *IEEE Transactions on Multimedia*, vol. 22, no. 1, pp. 108–121, 2020.

[13] P. Gao, P. X. Chai, and J. Lang, "Behavior steganography in social networks based on 0–1 knapsack algorithm," *Acta Electonica Sinica*, vol. 50, no. 3, pp. 753–758, 2022. (in Chinese)

[14] A. Cheddad, J. Condell, K. Curran, *et al.*, "Digital image steganography: Survey and analysis of current methods," *Signal Processing*, vol. 90, no. 3, pp. 727–752, 2010.

[15] M. S. Rathore, M. Poongodi, P. Saurabh, *et al.*, "A novel trust-based security and privacy model for internet of vehicles using encryption and steganography," *Computers and Electrical Engineering*, vol. 102, article no. 108205, 2022.

[16] O. Torki, M. Ashouri-Talouki, and M. Mahdavi, "Blockchain for steganography: Advantages, new algorithms and open challenges," in *Proceedings of the 18th International ISC Conference on Information Security and Cryptology*, Isfahan, Iran, Islamic Republic of, pp. 1–5, 2021.

[17] S. Y. Zheng, C. Q. Yin, and B. Wu, "Keys as secret messages: Provably secure and efficiency-balanced steganography on blockchain," in *Proceedings of the 2021 IEEE Intl Conf on Parallel & Distributed Processing with Applications, Big Data & Cloud Computing, Sustainable Computing & Communications, Social Computing & Networking*, New York City, NY, USA, pp. 1269–1278, 2021.

[18] D. Silver, T. Hubert, J. Schrittwieser, *et al.*, "Mastering chess and shogi by self-play with a general reinforcement learning algorithm," *arXiv preprint*, arXiv: 1712.01815, 2017.

[19] F. Zhang and Y. Ding, "Research on the application of internet of things and block chain technology in improving supply chain financial risk management," in *Proceedings of the 2021 International Conference on Computer, Blockchain and*

Financial Development, Nanjing, China, pp. 347–350, 2021.
[20] V. Hassija, V. Chamola, V. Gupta, *et al.*, "A survey on supply chain security: Application areas, security threats, and solution architectures," *IEEE Internet of Things Journal*, vol. 8, no. 8, pp. 6222–6246, 2021.
[21] Q. Q. Huang, R. Wen, Y. Han, *et al.*, "Intelligent fault identification for industrial internet of things via prototype-guided partial domain adaptation with momentum weight," *IEEE Internet of Things Journal*, vol. 10, no. 18, pp. 16381–16391, 2023.
[22] P. Zhang, C. Cui, D. Liu, *et al.*, "Data security sharing and interaction method of regulation system based on blockchain," in *Proceedings of the IEEE 10th Joint International Information Technology and Artificial Intelligence Conference*, Chongqing, China, pp. 1071–1074, 2022.
[23] Z. Zhou, Y. L. Tian, J. B. Xiong, *et al.*, "Blockchain-enabled secure and trusted federated data sharing in IIoT," *IEEE Transactions on Industrial Informatics*, vol. 19, no. 5, pp. 6669–6681, 2023.
[24] J. N. Wei, Q. C. Zhu, Q. M. Li, *et al.*, "A redactable blockchain framework for secure federated learning in industrial internet of things," *IEEE Internet of Things Journal*, vol. 9, no. 18, pp. 17901–17911, 2022.
[25] S. Qahtan, K. Y. Sharif, A. A. Zaidan, *et al.*, "Novel multi security and privacy benchmarking framework for blockchain-based IoT healthcare industry 4.0 systems," *IEEE Transactions on Industrial Informatics*, vol. 18, no. 9, pp. 6415–6423, 2022.
[26] V. Mothukuri, R. M. Parizi, S. Pouriyeh, *et al.*, "FabricFL: Blockchain-in-the-loop federated learning for trusted decentralized systems," *IEEE Systems Journal*, vol. 16, no. 3, pp. 3711–3722, 2022.
[27] P. Kumar, R. Kumar, G. P. Gupta, *et al.*, "P2TIF: A blockchain and deep learning framework for privacy-preserved threat intelligence in industrial IoT," *IEEE Transactions on Industrial Informatics*, vol. 18, no. 9, pp. 6358–6367, 2022.
[28] R. Kumar, P. Kumar, R. Tripathi, *et al.*, "A privacy-preserving-based secure framework using blockchain-enabled deep-learning in cooperative intelligent transport system," *IEEE Transactions on Intelligent Transportation Systems*, vol. 23, no. 9, pp. 16492–16503, 2022.
[29] Q. Dang, W. B. Shang, L. Yan, *et al.*, "Power business data sharing system based on blockchain and cryptography technology," in *Proceedings of the 2021 International Conference on Networking, Communications and Information Technology*, Manchester, UK, pp. 382–386, 2021.
[30] A. H. Mohsin, A. A. Zaidan, B. B. Zaidan, *et al.*, "PSO–blockchain-based image steganography: Towards a new method to secure updating and sharing COVID-19 data in decentralised hospitals intelligence architecture," *Multimedia Tools and Applications*, vol. 80, no. 9, pp. 14137–14161, 2021.
[31] M. T. Xu, H. Z. Wu, G. R. Feng, *et al.*, "Broadcasting steganography in the blockchain," in *Proceedings of the 18th International Workshop on Digital Watermarking*, Chengdu, China, pp. 256–267, 2020.
[32] P. Rede, S. Iyer, S. Sharma, *et al.*, "Blockchain based identity management system using cryptography and steganography," in *Proceedings of the 2023 International Conference on Information Technology*, Amman, Jordan, pp. 173–177, 2023.
[33] D. Silver, J. Schrittwieser, K. Simonyan, *et al.*, "Mastering the game of go without human knowledge," *Nature*, vol. 550, no. 7676, pp. 354–359, 2017.
[34] Y. Cao, "Research on carrierless steganography methods for secure covert communication," *Ph. D. Thesis*, Nanjing University of Information Science and Technology, Nanjing, China, 2022. (in Chinese)
[35] W. She, L. J. Huo, W. Liu, *et al.*, "A blockchain-based covert communication model for hiding sensitive documents and sender identity," *Acta Electonica Sinica*, vol. 50, no. 4, article no. 1002, 1013.
[36] J. Partala, "Provably secure covert communication on blockchain," *Cryptography*, vol. 2, no. 3, article no. 18, 2018.
[37] A. I. Basuki and D. Rosiyadi, "Joint transaction-image steganography for high capacity covert communication," in *Proceedings of the 2019 International Conference on Computer, Control, Informatics and its Applications*, Tangerang, Indonesia, pp. 41–46, 2019.
[38] S. Liu, Y. X. Liu, C. Feng, *et al.*, "Blockchain privacy data protection method based on HEVC video steganography," in *Proceedings of the 3rd International Conference on Smart BlockChain*, Zhengzhou, China, pp. 1–6, 2020.
[39] W. She, L. J. Huo, Z. Tian, *et al.*, "A double steganography model combining blockchain and interplanetary file system," *Peer-to-Peer Networking and Applications*, vol. 14, no. 5, pp. 3029–3042, 2021.
[40] D. Mitic, A. Lebl, B. Trenkić, *et al.*, "An overview and analysis of BER for three diversity techniques in wireless communication systems," *Yugoslav Journal of Operations Research*, vol. 25, no. 2, pp. 251–269, 2015.
[41] D. Chicco, M. J. Warrens, and G. Jurman, "The coefficient of determination r-squared is more informative than SMAPE, MAE, MAPE, MSE and RMSE in regression analysis evaluation," *PeerJ Computer Science*, vol. 7, article no. e623, 2021.
[42] Y. J. Luo, J. H. Qin, X. Y. Xiang, *et al.*, "Coverless image steganography based on multi-object recognition," *IEEE Transactions on Circuits and Systems for Video Technology*, vol. 31, no. 7, pp. 2779–2791, 2021.
[43] V. Holub and J. Fridrich, "Digital image steganography using universal distortion," in *Proceedings of the First ACM Workshop on Information Hiding and Multimedia Security*, Montpellier, France, pp. 59–68, 2013.
[44] V. Holub and J. Fridrich, "Designing steganographic distortion using directional filters," in *Proceedings of the 2012 IEEE International Workshop on Information Forensics and Security*, Costa Adeje, Spain, pp. 234–239, 2012.
[45] T. Pevný, T. Filler, and P. Bas, "Using high-dimensional image models to perform highly undetectable steganography," in *Proceedings of the 12th International Workshop on Information Hiding*, Calgary, Canada, pp. 161–177, 2010.
[46] V. Sedighi, R. Cogranne, and J. Fridrich, "Content-adaptive steganography by minimizing statistical detectability," *IEEE Transactions on Information Forensics and Security*, vol. 11, no. 2, pp. 221–234, 2016.
[47] M. Boroumand, M. Chen, and J. Fridrich, "Deep residual network for steganalysis of digital images," *IEEE Transactions on Information Forensics and Security*, vol. 14, no. 5, pp. 1181–1193, 2019.
[48] R. Zhang, F. Zhu, J. Y. Liu, *et al.*, "Depth-wise separable convolutions and multi-level pooling for an efficient spatial CNN-based steganalysis," *IEEE Transactions on Information Forensics and Security*, vol. 15, pp. 1138–1150, 2020.

Yuanlong CAO received the B.S. degree in computer science and technology from Nanchang University, China, in 2006, the M.S. degree in software engineering from the Beijing University of Posts and Telecommunications (BUPT), Beijing, China, in 2008, and the Ph.D. degree in communication and information system from the Institute of Network Technology, BUPT, in 2014. He was an In-

tern/Software Engineer with BEA TTC, IBM CDL, and DT Research, Beijing, China, from 2007 to 2011. He is currently a Professor with the School of Computer and Information Engineering, Jiangxi Normal University, Nanchang, China. His research interests include multimedia communications, network security and next-generation Internet technology. Dr. Cao serves as the Editor for *KSII Transactions on Internet and Information Systems*. He has served as the Lead Guest Editor for Mobile Networks and Applications, Intelligent Automation and Soft Computing, *International Journal of Distributed Sensor Networks*, *Electronics*, *Future Internet*, *Wireless Communications and Mobile Computing*, *Security and Communication Networks*, and the Guest Editor for *IEICE Transactions on Information and Systems, Computers, Materials & Continua*. He serves as the Co-General Chair of EAI MONAMI 2022, EAI DIONE 2023, and the Co-Chair of IEEE 9th WFIoT Workshop on Advancements in Metaverse and IoT, respectively. He has also served as the Technical Reviewer for several journals, including the *IEEE Transactions on Industrial Informatics*, *IEEE Transactions on Network and Service Management*, *IEEE Transactions on Cognitive Communications and Networking*, etc.
(Email: ylcao@jxnu.edu.cn)

Junjie LI received the B.S. degree in software engineering from the School of Software, Jiangxi Normal University, Nanchang, China, in 2023. He is currently working toward the M.S. degree in management science and engineering with Jiangxi Normal University, Nanchang, China. His research interests include image and signal processing, Internet technology, information security, and information management.
(Email: lijunjie@jxnu.edu.cn)

Kailin CHAO graduated in 2022 with a B.S. degree in information management and information systems from Lanzhou University of Finance and Economics. Currently he is pursuing a M.S. degree in management science and engineering at Jiangxi Normal University. His main research interests include blockchain, federated learning, and information security.
(Email: chaokailin@jxnu.edu.cn)

Jianmao XIAO received the Ph.D. degree from the College of Intelligence and Computing, Tianjin University. He is an Assistant Professor at Jiangxi Normal University, is the Deputy Director of the Jiangxi Provincial Engineering Research Center of Blockchain Data Security and Governance. He is a Member of the CCF TCSC. His main research interests include blockchain, service computing, intelligent software engineering. Dr. Xiao has authored more than 30 high-level academic papers, served as MONAMI 2022 Web Chair and ICSS 2022 PC Member. He also served as a reviewer for many domestic and international high-level journals and conferences in related fields.
(Email: jm_xiao@jxnu.edu.cn)

Gang LEI is currently an Associate Professor and the Vice Chairman of the School of Software, Jiangxi Normal University, China, where he is also serving as the Associate Director of the Academic Committee. His research interests include big data technology, computer network management, and information systems.
(Email: leigang@jxnu.edu.cn)