Eng Int Syst (2026) 2: 149–157


**Engineering**
***Intelligent Systems***

# Anti-Tampering Simulation Algorithm for Supply Chain Financial Big Data Based on Artificial Intelligence and Blockchain

**Xiaoqing Wu**[1,a] **and Hongli Wu**[2,b*]

[1] *College of Economics and Management, Chongqing Vocational and Technical University of Mechatronics, BiShan402760, Chongqing, China*
[2] *Guangdong Innovative Technical College, Dongguan 523000, Guangdong, China*

Social development and the progress of science and technology have driven the rapid advancement of computer technology. As an important research direction at this stage, computer vision multimodal learning of human-computer interaction has attracted the research interest of many scholars. Artificial intelligence (AI) and blockchain in terms of the multi-mode computer vision of human-computer interaction have also received a lot of attention. At present, AI has been widely used in various fields. Blockchain is mostly used for the prevention of data tampering and the protection of data security. Blockchain supply chain finance has encountered many problems in actual tamper proof applications. Many scholars have proposed corresponding countermeasures against the anti-tampering problem of blockchain. However, most of them focus on the identity of users and the privacy of transactions. There are few tamper proof studies on financial big data. On the basis of previous scholars' research on blockchain, this paper proposes the anti-tampering algorithm of supply chain financial big data of artificial intelligence and blockchain and conducts empirical research. The research on AI and blockchain of computer vision multimodal learning of human-computer interaction showed that this method was feasible. When the number of pieces of information was 3050, the number tampered with after the application of the proposed method was 226 lower than that of traditional methods for counter attack. Regarding the security of data transmission, the number of pieces of information that had been tampered with was 101 lower than that secured by traditional methods. For the reliability of data storage, this method had 224 fewer tampered information than traditional methods. This showed that the algorithm proposed in this paper was more resistant than traditional methods to attacks on the security of financial big data information of the supply chain, the protocol security during data transmission, and the reliability during data storage. At the same time, the research on AI and blockchain contributes to the development of computer vision multimodal learning for human-computer interaction.

Keywords: supply chain, financial big data, artificial intelligence and blockchain, tamper-proof simulation algorithm

## 1. INTRODUCTION

With the rapid development of a digital society and computer vision multi-mode learning, data publishing is already a basic data service. In general, the distribution of data depends on the trusted third party of the central server. Given the emergence of big data, the Internet of Things, artificial intelligence (AI), blockchain and other technologies, it is particularly important to prevent the tampering of the big data of supply chain finance. At present, the relationship between major global supply chain companies is becoming increasingly stronger, and a greater number of companies are beginning to pay

*Corresponding Author. [a] wuxiaoqing257@163.com, [b] whlpwf009@163.com

more attention to their relationships with partners. The rapid development of the Internet has seen numerous websites appearing online, with many companies setting up their own websites. Unfortunately, many of these websites have security issues that potential attackers can exploit. However, the existing algorithms have conversion difficulties and the encryption and encoding processes are inefficient. On the basis of previous research, this paper introduces a simulation method that combines artificial intelligence with blockchain technology to ensure that data is tamper-proof, and compares the results with those of traditional anti-tampering algorithms. Through the research on AI and blockchain of computer vision multimodal learning under human-computer interaction, this paper finds that this method can not only optimize and improve the research and application of blockchain technology in the supply chain financial big data anti tampering, but also meet the continuous expansion of AI computing needs of IoT devices under computer vision multimodal learning under human-computer interaction, which has important research significance and application value.

Many scholars have conducted research in different directions on big data anti tampering. Liang, Wei studied the safe data storage and recovery in the industrial blockchain network environment. He said that the large-scale redundant data storage and communication in the network 4.0 environment had the problems of low integrity, high cost and easy tampering. The proposed scheme could improve the repair rate and data storage rate of multi node data, and had good security and real-time performance [1]. Yang, Jiachen studied the blockchain based big data network sharing and anti tampering framework. He said that the continuous growth of data led to difficulties in data sharing. To solve the problem of distributed secure storage of big data in the blockchain, he proposed an encryption algorithm to prevent transaction data from being tampered with during user storage, so as to ensure transaction security and data reliability when conducting transactions in the blockchain [2]. Sivaganesan, D studied the storage of blockchain industrial data based on smart contracts. He said that blockchain helped to build a tamper proof network, which was built according to the contract signed in the system. It provided inviolable authentication for the transmitted industry data by providing security protection for anonymous authentication information [3]. Yang, Wenhui studied a lightweight car mounted social network blockchain. He said that the emerging blockchain technology, with its high security and irreversible characteristics, was a good catalyst for the development of mobile social networks. It could also be a data management tool for quickly generating vehicle mounted social network data with tamper proof function [4]. These scholars have their own views on data security and anti tampering issues and propose to protect data tampering through blockchain. Their research on data anti tampering and blockchain can provide a theoretical basis for anti tampering of financial big data. However, there are still some deficiencies in their research.

Other scholars also put forward other views on data tamper prevention. Li, Weiweil studied the data security of 6G network artificial intelligence applications based on blockchain. He said that intelligent services inevitably needed to process a large amount of data, such as storage, calculation and analysis, so the data might be easily tampered with or contaminated by attackers. The blockchain was more effective in data security, so the integration of AI and blockchain aimed to evaluate and optimize the quality of intelligent services [5]. Liu, Yanhui studied fog computing based on blockchain and data privacy protection of the Internet of Things. He said that the security of sensitive IoT data was a big problem. Blockchain was a distributed book technology with application prospects, which could effectively prevent the tampering of malicious data and provide users with reliable data storage. To this end, he proposed a distributed access control system based on blockchain technology, which could effectively protect the privacy of IoT data [6]. These scholars have different views on data protection and anti tampering. Some scholars have focused on data security and protection through artificial intelligence and blockchain, which to some extent broadens the way of data anti tampering. However, because scholars' views are limited to theoretical research, there is no good practical verification. Therefore, this idea only stays at a shallow level, and can not provide a good reference for the effectiveness of anti tampering for actual data. Therefore, there is a gap in big data regarding tamper-proof technology of AI and blockchain, which requires more research to fill in the gaps.

On the basis of previous scholars' research on data tamper prevention, in this paper, artificial intelligence and blockchain are proposed to optimize data tamper-proofing. The research shows that this method is feasible. It improves the attack resistance and security of data, which has certain market application and promotion value.

## 2. AI AND BLOCKCHAIN SUPPLY CHAIN FINANCIAL BIG DATA

### 2.1 Overview of Blockchain Based Supply Chain Finance

As a strong support for the real economy, finance in the supply chain has become an important way to help SMEs innovate in the context of the integration of industry and finance [7]. The advantage of supply chain finance is that it provides a convenient and fast way for SMEs to finance, and also opens up a new development path for its core enterprises and commercial banks. Driven by policies, the participants in supply chain finance are no longer limited to traditional commercial banks. Supply chain finance is a thread of social economy, which can be accessed through commercial banks, factoring companies and other capital channels. Through the channels of transaction and financing, the customer's trust and fair distribution of interests are realized, thus obtaining financial support from commercial banks and factoring companies [8]. It is a capital optimization for the core business of the financial institution or enterprise. To maximize the functionality and enhance the efficiency of supply chain finance, it must be realized through collaboration with various stakeholders to reduce costs and default risks and increase new financing opportunities [9]. In the whole supply chain, the logistics, capital and information flow of products

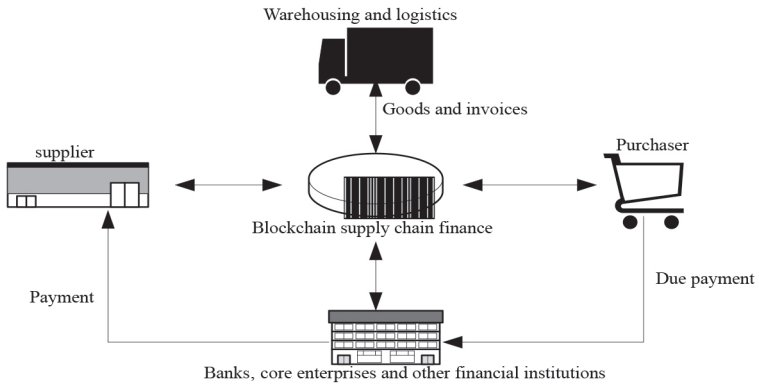


**Figure 1** Multi user transaction process of blockchain supply chain finance.

are combined to achieve the optimal management of three flows. At this stage, supply chain finance also faces various problems.

Blockchain is a network security platform based on distributed network, digital certificate, privacy protection and other technologies without relying on a third party. Due to the development of blockchain technology, the advantages of data centralization, tamper proof and other technologies can link key data with data, thus solving the problem of information asymmetry between enterprises. Blockchain technology has the opportunity to solve the trust problem in the future. It can support the information exchange between logistics and supply chain that does not rely on trust, security and authentication on the supply chain. In the blockchain, in order to ensure the synchronization and confirmation of account books, it is necessary to share data among nodes in the distributed network [10]. In addition, in the transaction process, some private information cannot be opened to all users, and technical means must be used to protect users' data security. Therefore, data security is one of the key topics.

In the alliance chain of supply chain finance, there are many participants, mainly suppliers, purchasers, financial institutions, core enterprises, warehousing, transportation, etc. Therefore, in supply chain finance, the business of blockchain applications is very complex, and must be split according to the business functions to separate the data between various services [11]. At present, the mature application of blockchain still stays on the single chain architecture, and the single chain architecture is difficult to adapt to the large-scale blockchain system built under the supply chain financial environment. The supply chain finance multi user transaction process of the blockchain is shown in Figure 1.

Blockchain technology has a good ability to solve current problems. However, due to the complexity of the entire industrial chain and more and more supply chains, its data security has been greatly threatened [12]. In blockchain, data security protection is a very critical link, which can provide security guarantee for the promotion of blockchain and the use of users. The current blockchain security protection is mainly anonymous, such as zero knowledge proof. Although these technologies can protect users' privacy and transaction data security to a certain extent, they do not involve the processing of big data such as machine learning. Therefore, privacy problems such as consistency attack and background knowledge attack occur [13]. In addition, in the practical application of supply chain finance, a large number of data statistics and analysis are needed to provide better application services. In the supply chain financial environment, banks and other financial institutions need higher privacy and higher data utilization. In this kind of business, it is generally characterized by large amount of data and high dimension. These data characteristics are directly related to the privacy and ultimate usability of the algorithm, thus bringing new challenges to users' privacy security.

## 2.2 Anti Tampering of AI and Blockchain Technology

### 2.2.1 Data Anti Tampering Principle

SQL (Structured Query Language) injection is an attack against database tampering. It provides users with specific code to collect data on programs and servers and obtain corresponding data [14]. SQL injection is carried out through a common website interface, which looks no different from the visit of a common web page. Therefore, in the current market, no firewall reminds SQL injection. If the administrator does not have the habit of checking the Internet Information Service (IIS) logs, the network database has not been tampered with for a long time [15]. The anti tampering method mainly introduced in this paper is the combination of artificial intelligence and blockchain.

### 2.2.2 Overview of Blockchain

The connotation of blockchain can be divided into two categories: broad sense and narrow sense. In the narrow sense, blockchain refers to a chain structure that continuously arranges several digital blocks in time sequence. The blockchain link uses encryption technology to ensure that data cannot be tampered with or forged. Therefore, it can also be considered as a distributed book system [16]. However, in a broader sense, it refers to a design paradigm of a distributed computing infrastructure that uses a variety of technologies, which is rich in value creation. Its data structure, distributed consensus algorithm and encryption algorithm also include the preservation and verification, generation and update of information, which guarantees data security and tamper resistance [17].

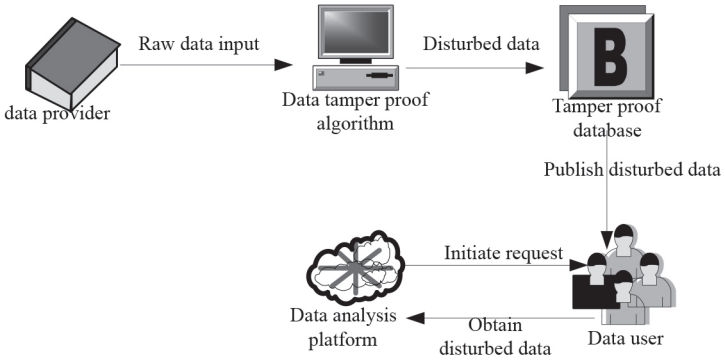


**Figure 2** Flow chart of non interactive data publishing.

### 2.2.3 Overview of Artificial Intelligence

Artificial intelligence based on multi-mode learning of human-computer interaction computer vision is a new computer science. The purpose of AI is to enable machines to have a certain degree of intelligence and help people analyze and solve complex problems [18]. The research of artificial intelligence mainly focuses on expert system, pattern recognition, machine learning, etc. Expert system is an artificial intelligence program that can handle complex problems in some special fields [19]. The system can make intelligent judgments on complex problems according to the professional knowledge of the specialty. Compared with the conventional computer program, the system can output the decision results only when there is no accurate input data. Pattern recognition refers to the use of machinery to imitate animals, through the perception of the external environment to carry out cognition. The main research direction of pattern recognition is the recognition of two-dimensional images, especially text. With the continuous development of technology, the discrimination of complex scenes and dynamic objects has become an important topic in the field of pattern recognition. Machine learning is to input data into the computer, learn and obtain its inherent laws through the computer, so as to obtain new rule knowledge. It can improve the intelligence of the computer and make it have the ability of human judgment. Machine learning can be divided into supervised learning, unsupervised learning and semi supervised learning.

### 2.2.4 Anti Tampering of AI and Blockchain Data Release

The design of a reasonable and efficient publishing mechanism can reduce users' restrictions on data. It is an important method to study data security protection. At present, data protection and publishing technologies can be divided into two types according to their manifestations in different application environments: interactive and non interactive data publishing.

Non interactive publishing technology based on human-computer interaction under multimodal learning of computer vision, noise conforming to the definition of differential privacy is added to the original data set at one time, so that it can handle all queries [20]. The advantage of this method is that the noise that meets the differential privacy definition once can be directly added to the original data, so that data users can only make statistics and analysis on the data after interference. Because there is no need to process queries in real time, the non interactive publishing technology does not have problems such as query restrictions. However, in practice, non interactive publishing technology also has its shortcomings. The non interactive data publishing process is shown in Figure 2.

The interactive data publishing technology based on human-computer interactive computer vision multimodal learning requires users to submit query tasks to the database and process each request in real time. Users can access the database through the preset query interface. After the original data is disturbed, the noise results that meet the differential privacy definition are fed back to the data user. Because of the real-time requirements of the query, the interference results consume the user's privacy and generate random noise when answering the query. In the case of a large number of queries, due to the huge consumption of privacy, the user's privacy loss is great. On the premise of ensuring the differential privacy, the subsequent query results are subject to a lot of interference, which leads to the reduction of the effectiveness of the data. When the user's privacy budget is exhausted, the system returns the user's query to ensure that the user's data is still under the protection of differential privacy. Therefore, the core of the research on interactive data distribution technology is to solve the excessive personal information cost of users, and thus solve the user access restrictions caused by it. Although the design and application of interaction mode are more complex, it can provide better privacy protection in many situations, and also plays a key role in dynamic privacy. The specific flow chart of interactive data publishing is shown in Figure 3.

## 2.3 Data Anti Tampering Algorithm Combined with Artificial Intelligence and Blockchain

The blockchain using the PoW (Proof of Work) consensus algorithm is wasting a lot of computing power. In artificial intelligence, there is also a problem of insufficient computing power, and the two just complement each other. In the learning and training of artificial intelligence, if the computing power consumed by the blockchain can be used, it can not only solve the loss of blockchain computing power, but also solve the problem of insufficient computing power of artificial intelligence [21].

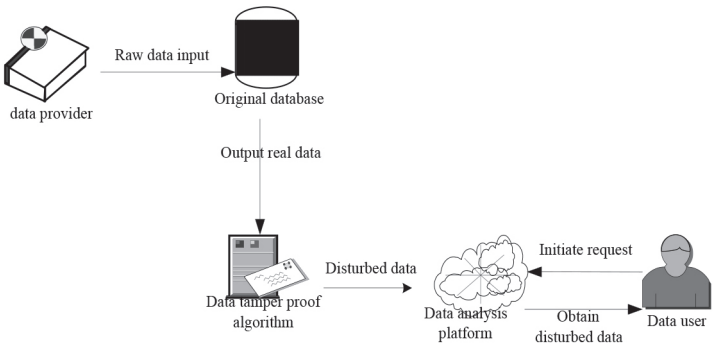


**Figure 3** Interactive data publishing process.

For the big data of supply chain finance based on artificial intelligence and blockchain technology under the multi-modal learning of computer vision based on human-computer interaction, before extracting the key characteristics of distributed big data in the database, the characteristic judgment standard of distributed data is established, so that it can be recognized while evaluating its importance. First, the important information from scattered databases is mapped and transformed into multidimensional data. T is represented as multidimensional space and marked with spatial dimensions. The corresponding set is expressed by the following formula:

$$\{(a_i, b_i)|a_i \in T^n, b_i \in \{1, 2, \cdots, m\}\} \tag{1}$$

Among them: $m \geq 2$.

$$i = 1, 2, \cdots, k.$$

It can be seen that the formula of feature subset difference degree $DFS_j$ of distributed data is:

$$DFS_j = \frac{\sum_{c=1}^{m} \|\overline{a}_j^{(c)} - \overline{a}_j\|^2}{\sum_{c=1}^{m}} \frac{1}{k_c - 1} \sum_{c=1}^{m} \|\overline{a}_{i,j}^{c} - \overline{a}_j^{(1)}\|^2 \tag{2}$$

Among them: $j = 1, 2, \cdots, n$.

$\overline{a}$ - Average vector of feature subsets in all data sets.

$a_j^{(c)}$-Average vector of feature subset in sampled data.

$a_{i,j}^{(c)}$-Vector of subset in the first group of samples.

In this formula, the numerator represents the sum of data vectors in one center, while the denominator represents the internal distribution of each type. In the corresponding data set, its value is reduced and the difference in characteristics of each data is also reduced. If the absolute value of $DFS_j$ is larger, the characteristics of a set of data can be well determined.

In selecting the important features of the data, the idea of minimizing the R1 parametric number is used to optimize the data scattered in the database, which makes the sparse representation and reconstruction coefficients of the data effectively solved. Assuming that the distributed data set is $\{A_j\}_{j=1}^{k}$ and $A_j \in T^n$, and the formula corresponding to the data vector of the data set and each matrix is as follows:

$$A = [A_1, A_2, \cdots, A_k] \in T^{\text{nak}} \tag{3}$$

In calculating the sparsity of the data, the coefficient matrix is first combined and then transformed into a minimum linear programming under the L1 model. The formulas are:

$$B = \min_{z_j} \|Z_j\| \tag{4}$$

$$\overrightarrow{A}_j = A' \tag{5}$$

Among them: $z_j$ - required calculation function.

$A'$-matrix obtained by deleting data vector.

The $k'$-dimensional coefficient vector can be represented by $z_j$, so the formula is:

$$z_j = [z_{j1},\ z_{j2}, \cdots, z_{jj-1}, 0, \cdots, \overline{z}_k]^H \tag{6}$$

During reconstruction, $z_{jc}(c \neq j)$ can be used to represent the first vector contribution of the dataset. In this way, a set of diluted reconstruction matrices are obtained:

$$Z = (\overrightarrow{z_{jc}})\text{kak} \tag{7}$$

After the reconstruction factors are derived, the differences between the reconstructed attributes and each feature in the original data are then analyzed. The reconstructed features are integrated to obtain the analysis results of each feature. The results show that the smaller the difference between these features, the better the performance can be maintained. Through the above analysis and calculation, an objective function Z (q) that can well meet the expected requirements is obtained. The formula is:

$$Z(q) = \frac{\sum_{j=1}^{k}(a_{jq} - (A_{zj}^{-})_q)^2}{Var(A(q:))} \tag{8}$$

Among them, $Var(A(q:))$ represents the dispersion of the dimensional characteristics of the dataset.

To determine whether the characteristics of the data have changed, the distributed big data can be collected in the database in real time by monitoring the code. The monitoring code is embedded in an appropriate location to ensure that the overall structure of the data does not change. By encrypting each characteristic function, the anti tamper mechanism is improved. After the function decoding is obtained, each function is decoded to modify the data function. An appropriate key generation function is selected according to different encryption methods of each part, as shown in the following formula:

$$W2_j = R_j(V_j, T_j, G_j(DR)) \tag{9}$$

Among them: $R_j$ - first characteristic key generation function;

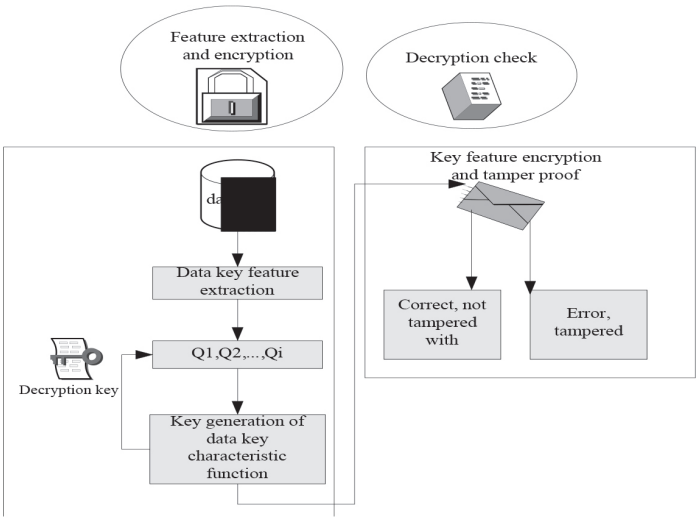


**Figure 4** Data anti tampering process of artificial intelligence and blockchain.

**Table 1** Comparison of data processing results of two inspection methods.

| Category | Period (month) | 1 | 2 | 3 | 4 | 5 |
|---|---|---|---|---|---|---|
| Number of tampered information(piece) | Algorithm in this paper | 1452 | 152 | 2578 | 25909 | 1891 |
| | | 3 | 46 | 9 | 9 | 9 |
| | Traditional algorithm | 9725 | 114 | 1898 | 2025 | 1652 |
| | | 14 | 2 | 1 | 5 | |
| Error message data(piece) | Algorithm in this paper | 6 | 8 | 9 | 5 | 4 |
| | Traditional algorithm | 15 | 17 | 15 | 9 | 11 |
| Error rate (%) | Algorithm in this paper | 0.04 | 0.05 | 0.03 | 0.01 | 0.02 |
| | | 1 | 2 | 5 | 9 | 1 |
| | Traditional algorithm | 0.41 | 0.14 | 0.07 | 0.04 | 0.06 |
| | | 5 | 9 | 9 | 4 | 7 |

$W2_j$ - first characteristic decoding key generation function;
$T_j$ - first value for decoding the registration code;
$V_j$ - first value for decoding user code;
$G_j(DR)$ - the first characteristic function value displayed;
$DR$ - array, the generated hash value.

In this function, each unit is decoded by the data function calculated by the steganographic secret key generation function. The previous functions are performed according to a series of functions. Usually, the performance of the specified data key is changed, making it unable to complete the work as usual, resulting in incorrect answers to the decoding key and incorrect decoding. Because it is difficult to decrypt the diversity of key generation functions, it can further protect distributed data functions in the database. The data anti tampering flow chart of AI and blockchain is shown in Figure 4.

## 3. DEMONSTRATION OF ARTIFICIAL INTELLIGENCE AND BLOCKCHAIN DATA TAMPER PROOF SIMULATION ALGORITHM

In order to verify the performance of the anti tampering simulation algorithm of supply chain financial big data based on artificial intelligence and blockchain under the multi-modal learning of computer vision based on human-computer interaction, this design experiment is specifically explored empirically. This paper draws the corresponding conclusions by comparing the anti attack, protocol security and data storage reliability of data anti tampering algorithms of AI and blockchain with those of traditional data anti tampering algorithms.

### 3.1 Anti Tamper Simulation Algorithm Experiment Process

Validation of data tamper-proof algorithms under multimodal learning of computer vision for human-computer interaction can first be performed to verify the data tamper-proof performance of distributed networks. This study can be carried out on two personal computers. The network server is IIS 5.0, and the operating system is Windows 2016 serber, Microsoft Visual C++6.0. The standard information database is SWS Server 2016, and the computational data required for the experiment are derived from the simulation, which is divided into two phases.

### 3.2 Anti Tamper Simulation Algorithm Experimental Results

Table 1 shows the comparison of data processing results between the anti tamper algorithm of artificial intelligence and

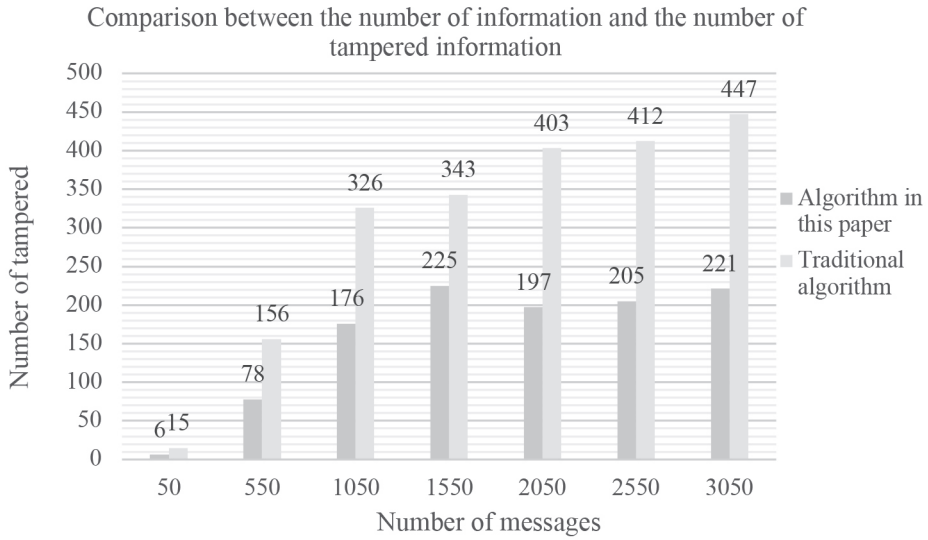


**Figure 5** Comparison of anti attack performance of two data tamper prevention algorithms.

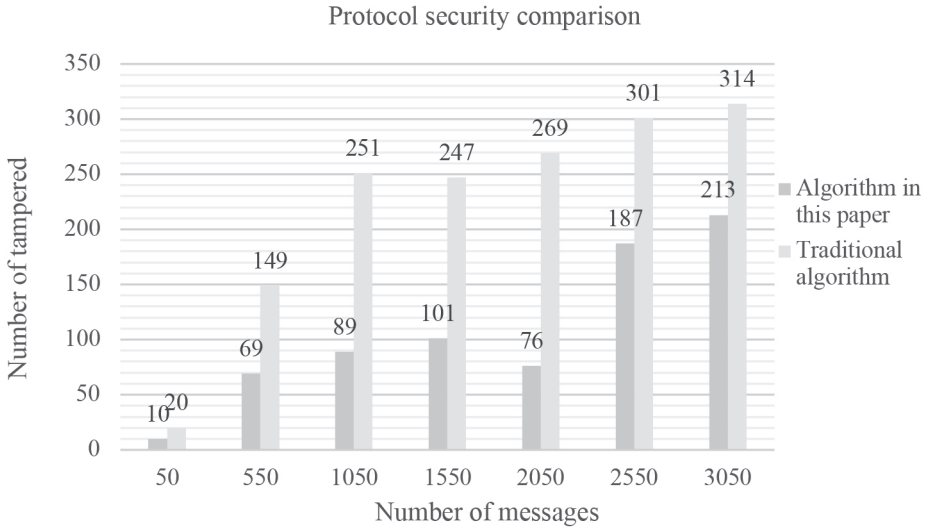


**Figure 6** Comparison of data transmission protocol security in two modes.

blockchain and the overall inspection method of traditional anti tamper algorithm under the multi-modal learning of computer vision based on human-computer interaction.

Table 1 shows that the test results based on the algorithm in this paper are better. The algorithm in this paper is superior to the traditional anti tampering algorithm in terms of both the inspection of tampered information of financial big data and the inspection of the number of error messages. Similarly, the error rate of the algorithm in this paper is also lower than that of the traditional algorithm. This shows that the security and integrity of information and data in the decentralized supply chain financial network under AI and blockchain are better protected, and the performance of tampering detection is better.

The above compares the overall verification capability of the algorithm for the data under the two methods, which additionally needs to be tested for its tamper resistance. In addition, its anti tampering performance shall be tested. For the test of anti attack performance, the anti attack performance of this paper is mainly measured by the number of tampered information in two specific ways, as shown in Figure 5.

From Figure 5, the number of tampered information in this algorithm is lower than that in the traditional algorithm when the amount of information is the same. When the number of information is 50, the number of tampered information in this algorithm is 9 less than that in the traditional algorithm. When the number of information is 1050, the number of tampered information in this algorithm is 150 less than that in the traditional algorithm. When the number of information is 3050, the number of tampered information in this algorithm is 226 lower than that in the traditional algorithm. This means that the anti tampering algorithm of AI and blockchain can provide more secure protection for the security of supply chain financial big data distributed network information, and its anti attack performance is better.

While processing the data, the protocol security in the data transmission process is also tested. The specific security performance of the data transmission protocol in the two modes is shown in Figure 6.

From Figure 6, under the same amount of information, the number of information tampered by this algorithm in the process of network data transmission is less than that

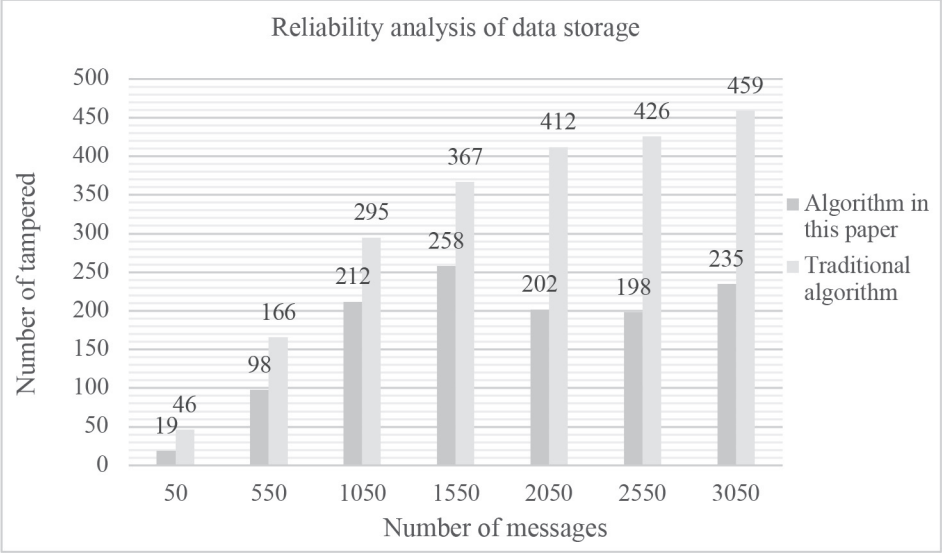


**Figure 7** Comparison of data storage reliability under two modes.

of the traditional anti tamper algorithm. When the number of information is 50, the number of tampered information in this algorithm is 10 lower than that in the traditional algorithm. When the number of information is 1050, the number of tampered information in this algorithm is 162 lower than that in the traditional algorithm. When the number of information is 3050, the number of tampered information in this algorithm is 101 lower than that in the traditional algorithm. This shows that the anti tampering algorithm based on artificial intelligence and blockchain proposed in this paper can provide better protection for data transmission in the supply chain financial big data distributed network than traditional algorithms, with higher protocol security performance and less tampered data.

After analyzing the anti attack capability and protocol security of the algorithm in two different ways, the reliability of the algorithm in data storage needs to be analyzed finally. The data storage reliability results under the two modes are shown in Figure 7.

In Figure 7, it can be seen that the amount of information tampered with by the algorithm in this paper is less than that of the traditional anti tamper algorithm when storing data. When the number of information is 50, the number of tampered information in this algorithm is 27 lower than that in traditional algorithms. When the number of information is 1050, the number of tampered information in this algorithm is 83 lower than that in the traditional algorithm. When the number of information is 3050, the number of tampered information in this algorithm is 224 lower than that in the traditional algorithm. This shows that the anti-tampering algorithm of artificial intelligence and blockchain can provide more reliable protection for the data storage in the supply chain financial big data distributed network. Its data storage is more reliable and the number of tampered information is less.

To sum up, this paper explores tamper-proof algorithms based on artificial intelligence and blockchain in the context of computer vision multimodal learning. The research shows that the algorithm proposed in this paper provides more effective protection for the anti attack of information security in the supply chain financial big data distributed network, the protocol security during data transmission and the reliability of data storage compared with the traditional algorithm. When the number of messages is 3050, the number of tampered messages is 226 lower than that of traditional ones for anti attack. For the security of data transmission, the number of tampered information is 101 lower than that of traditional information. For the reliability of data storage, the number of tampered information is 224 lower than that of traditional information.

## 4. CONCLUSION

With the rapid development of modern society and science and technology, computer vision multimodal learning for human-computer interaction has become more widespread and increasingly available to more people because of its unique algorithm advantages. This study conducted in-depth research on an anti-tampering algorithm applied to AI and blockchain to safeguard the financial big data of supply chains.. First, the relevant background of the topic was presented. Then, a review of previous studies on the the shortcomings of blockchain anti-tampering methods again, and proposed an anti-tampering algorithm combining artificial intelligence and blockchain through theoretical analysis of blockchain and artificial intelligence. The feasibility of this method was verified by experiments. It was shown that the algorithm proposed in this paper performed better than traditional methods in terms of attack resistance, protocol security and data storage reliability. This method has an effective anti-tampering effect on the distributed network information data of supply chain finance.

## REFERENCES

1. Wei, L. “Secure data storage and recovery in industrial blockchain network environments”. IEEE Transactions on Industrial Informatics 16.10 (2020): 6543–6552.

2. Yang, J. C. “Blockchain-based sharing and tamper-proof framework of big data networking”. IEEE Network 34.4 (2020): 62–67.
3. Dhandapani, S. “Smart contract based industrial data preservation on block chain”. Journal of Ubiquitous Computing and Communication Technologies (UCCT) 2.1 (2020): 39–47.
4. Yang, W. H. “LDV: A lightweight DAG-based blockchain for vehicular social networks”. IEEE Transactions on Vehicular Technology 69.6 (2020): 5749–5759.
5. Li, W. W. “Blockchain-based data security for artificial intelligence applications in 6G networks”. IEEE Network 34.6 (2020): 31–37.
6. Liu, Y. H., Zhang, J. B. and Zhan, J. “Privacy protection for fog computing and the internet of things data based on blockchain”. Cluster Computing 24.2 (2021): 1331–1345.
7. Sravani, C., and Murali, G. “Secure electronic voting using blockchain and homomorphic encryption”. International Journal of Recent Technol and Engineering. 8.2 (2019): 1002–1007.
8. Kong, Q. L., Su, L. and Ma, M. “Achieving privacy-preserving and verifiable data sharing in vehicular fog with blockchain”. IEEE Transactions on Intelligent Transportation Systems 22.8 (2020): 4889–4898.
9. Dhawan, S. and Rashmi, G. “Analysis of various data security techniques of steganography: A survey”. Information Security Journal: A Global Perspective 30.2 (2021): 63–87.
10. Esposito, C. “Blockchain: A panacea for healthcare cloud-based data security and privacy?”. IEEE Cloud Computing 5.1 (2018): 31–37.
11. Yazdeen, A. A. “FPGA implementations for data encryption and decryption via concurrent and parallel computation: A review”. Qubahan Academic Journal 1.2 (2021): 8–16.
12. Xu, G. W. “Data security issues in deep learning: attacks, countermeasures, and opportunities”. IEEE Communications Magazine 57.11 (2019): 116–122.
13. Kaushik, S. and Charu, G. “Ensure hierarchal identity-based data security in cloud environment”. International Journal of Cloud Applications and Computing (IJCAC) 9.4 (2019): 21–36.
14. Gai, K. K., Qiu, M. K. and Zhao, H. “Privacy-preserving data encryption strategy for big data in mobile cloud computing”. IEEE Transactions on Big Data 7.4 (2017): 678–688.
15. Mulyati, M. “Blockchain Technology: Can Data Security Change Higher Education Much Better?”. International Journal of Cyber and IT Service Management 1.1 (2021): 121–135.
16. Sollins, K. R. “IoT big data security and privacy versus innovation”. IEEE Internet of Things Journal 6.2 (2019): 1628–1635.
17. Li, Y. “Crowdsensing multimedia data: security and privacy issues”. IEEE MultiMedia 24.4 (2017): 58–66.
18. Bhatia, T. and Verma, A. K. “Data security in mobile cloud computing paradigm: a survey, taxonomy and open research issues”. The Journal of Supercomputing 73.6 (2017): 2558–2631.
19. Yi Chen, Shuai Ding, Zheng Xu, Handong Zheng, Shanlin Yang. Blockchain-Based Medical Records Secure Storage and Medical Service Framework. J. Medical Syst. 43(1): 5:1–5:9 (2019).
20. Kara, M., Merzeh, H. R. J., Aydin, M. A., & Balik, H. H. (2024). Blockchain-based group signature for secure authentication of IoT systems in smart home environments. Cyber-Physical Systems, 10(4), 362–386.
21. Ma, X.and Zhang,Y. “Blockchain data privacy protection mechanism for enterprise finance anddata mining algorithms”, Engineering Intelligent Systems, 32. 5(2024): 435–443.