Research on Deep Forgery Data Identification and Traceability Technology Based on Blockchain

Ke Yang
State Grid Digital Technology Holding Co., Ltd.
State Grid Blockchain Technology (Beijing) Co., Ltd.
Beijing, China
yangke@sgdt.sgcc.com.cn

Da Li
State Grid Blockchain Technology (Beijing) Co., Ltd.
State Grid Co., Ltd. Blockchain Technology Laboratory
Beijing, China
lida@sgdt.sgcc.com.cn

Qinglei Guo
State Grid Blockchain Technology (Beijing) Co., Ltd.
State Grid Co., Ltd. Blockchain Technology Laboratory
Beijing, China
guoqinglei@sgdt.sgcc.com.cn

Hejian Wang
State Grid Digital Technology Holding Co., Ltd.
State Grid Blockchain Technology (Beijing) Co., Ltd.
Beijing, China
wanghejian@sgdt.sgcc.com.cn

Desheng Bai
State Grid Blockchain Technology (Beijing) Co., Ltd.
State Grid Co., Ltd. Blockchain Technology Laboratory
Beijing, China
baidesheng@sgdt.sgcc.com.cn

Xiukui Pan
State Grid Blockchain Technology (Beijing) Co., Ltd.
State Grid Co., Ltd. Blockchain Technology Laboratory
Beijing, China
panxiukui@sgdt.sgcc.com.cn

2022 IEEE 2nd International Conference on Data Science and Computer Application (ICDSCA) | 978-1-6654-7200-5/22/$31.00 ©2022 IEEE | DOI: 10.1109/ICDSCA56264.2022.9988274

***Abstract*—With the acceleration of the digital transformation of the power system, the electronic data in the power production operation has shown an explosive growth. However, the increasing proliferation of deep forgery technology has brought huge hidden dangers to the electronic data management of power grid enterprises, and it is urgent to build a trusted management system for electronic data. This paper proposes a blockchain-based deep forgery data identification and traceability framework. Firstly, a method of trusted identification of electronic data based on blockchain is proposed, which constructs the unique identification of data and embeds it in the electronic data as a digital watermark. Second, introduce blockchain-based electronic data forensic appraisal technology to conduct authenticity and similarity analysis of electronic data. Finally, a deep forgery data traceability mechanism based on digital identification is designed to realize deep forgery data traceability and dissemination supervision. After comparative analysis, the framework is more secure and efficient in deep forgery data supervision, and can provide key support for building a trusted content system in cyberspace.**

Keywords—deep forgery, blockchain, data identification, forensic appraisal, data traceability

I. INTRODUCTION

"Deep forgery" refers to combining and superimposing existing images and videos into new images and videos by means of deep learning, so as to achieve the effect of being fake as real [1]. Deep forgery has had a disruptive impact on trust systems based on "seeing is believing". In recent years, deep forgery technology has developed rapidly, especially the introduction and deepening application of generative adversarial network technology, deep forgery audio and video has achieved the effect of being difficult to distinguish between true and false. Although deep forgery technology can play a positive role in film and television production, social networking, and entertainment, its negative abuse has created a huge challenge to the credibility of cyberspace information content. It will not only pose a threat to global political security, public trust and personal property security, but also cause certain difficulties to the trusted management of enterprise electronic data. When carrying out foreign-related businesses such as line equipment inspection, power grid construction, and marketing and electricity theft inspection, power grid companies usually use electronic data such as video and audio recordings to prove the authenticity of relevant power production activities. These electronic data serve as electronic evidence for power safety production accidents and power theft disputes when needed. However, deep forgery technology has had a serious negative impact on the credibility of electronic evidence. Power grid companies urgently need to improve their ability to credibly collect and store electronic data such as video and audio recordings, so as to provide support for protecting the legitimate rights and interests of power grid companies.

Blockchain technology has the characteristics of decentralization, non-tampering, openness, transparency and traceability, which is of great help in improving the credibility of electronic data. Supervision of deep fake data through blockchain technology has good applicability. At present, many countries, including China, have legally recognized the effectiveness of blockchain for storing electronic evidence [2,3]. The research on the integration of blockchain and electronic evidence mainly focuses on two aspects. One is to improve the immutability of existing electronic evidence platform data through blockchain storage [4,5], and the other is to directly realize decentralized electronic evidence extraction and trusted storage through the blockchain platform [6,7]. Reference [4] designed a blockchain-based chain of custody for electronic evidence to achieve auditability and traceability of the entire process from the collection of evidence to the use of evidence in court in digital forensics. Reference [5] builds a blockchain-based electronic evidence storage system, which saves blockchain storage space and time by using a batch packaging mechanism on the basis of ensuring the

authenticity of the evidence.Reference [6] proposes an electronic forensics model based on blockchain, which realizes decentralized forensics and storage in cloud computing environment, and solves the problem of low reliability caused by centralized forensics of cloud service providers. Literature [7] proposes a blockchain-based IoT electronic forensics framework. By uploading the data of all IoT devices to the chain, it can achieve more comprehensive data preservation and improve the transparency of the judicial investigation process. The above literature provides a reference for deep forgery data forensics. However, most of the deep forgery data is disseminated through public media, which has pain points such as difficulty in source supervision, fast dissemination, and difficulty in identification. The existing electronic forensics framework cannot be directly applied.

At the same time as the development of deep forgery technology, deep forgery identification technology has been produced, which has become the key to combating the abuse of deep forgery technology. At present, deep forgery identification technology has received a lot of attention in cademia and industry at home and abroad, and has become a research hotspot [8-10]. Literatures [8] and [9] combed deep forgery technology and detection technology, summed up the main technical directions of the opposing parties. And pointed out that the current deep forgery new technologies emerge in an endless stream, the detection technology has serious defects in generalization and robustness, and it is almost impossible to deal with the new forgery technology. Reference [10] analyzed the key risks of deep synthetic data to the legal acceptance of electronic evidence, and proposed an identification mechanism that combines source containment and expert identification. The current deep forgery detection technology lags behind the deep forgery technology as a whole, and it is basically unrealistic to realize the deep forgery data identification only through the deep forgery detection technology. Therefore, it is necessary to build a new deep forgery detection framework, which organically combines laws and regulations [11], blockchain traceability and deep forgery detection technology, which is a feasible solution.

In view of the above problems, this paper proposes a blockchain-based deep forgery data identification and traceability framework. First, an electronic data identification method based on blockchain is proposed. By constructing the unique identification of any image, audio and video, and embedding it into the electronic data as a digital watermark, the source control of electronic data is realized. Secondly, the electronic data forensic appraisal technology based on blockchain is introduced, and the authenticity and similarity identification of data is realized by means of legal means, and the whole process can be audited through blockchain technology. Finally, a deep forgery data traceability mechanism based on trusted data identification is designed to realize deep forgery data traceability and dissemination supervision. This framework provides key support for building a trusted management system for electronic data.

The remaining chapters of this paper are organized as follows. The second part is the identification and traceability technology of deep forgery data based on blockchain. The third part is the safety and efficiency analysis. The fourth part is the summary and outlook.

II. Blockchain-based Deep Forgery Data Identification and Traceability Technology

A. Blockchain-based deep forgery data identification and traceability framework

The process of deep forgery data synthesis and dissemination is shown in Figure 1 below, including the stages of real data generation, deep forgery data synthesis, publishing and reprinting. For deep forgery data supervision, proactive control at the source is more beneficial than relying solely on late-stage deep forgery detection.

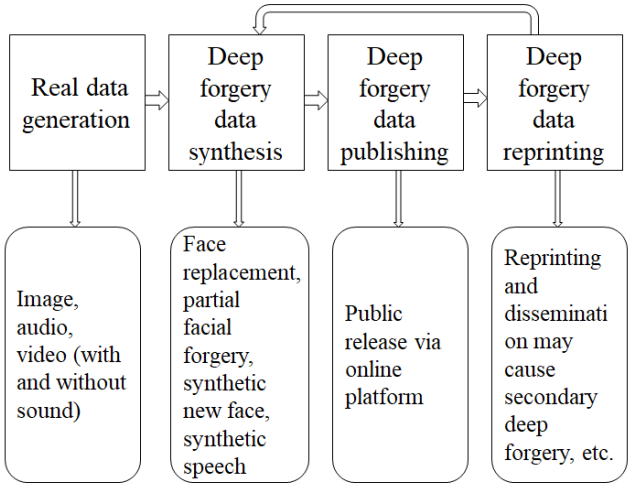

Fig. 1. Deep forgery data synthesis and dissemination process

With the goal of establishing a full-life-cycle supervision system for deep forgery data, and supported by technologies such as blockchain, deep forgery detection, electronic data forensics, and forensic appraisal, this paper proposes a blockchain-based deep forgery data identification and traceability framework, as shown in Figure 2. Starting from the source data protection, the deep forgery data supervision is divided into three stages: original data identification, deep forgery data forensics and appraisal, and deep forgery data traceability.

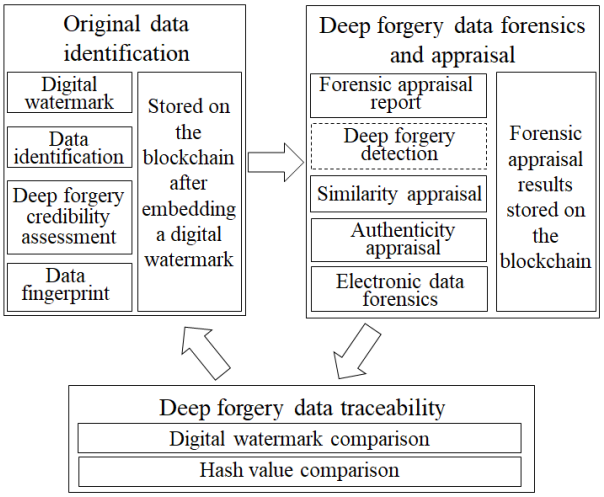

Fig. 2. Blockchain-based deep forgery data identification and traceability framework

In the original data identification stage, when the network platform receives any image or audio and video data, it first extracts its data fingerprint, and splices the data fingerprint

with the digital identity of the data submitter as the unique ID of the data. Secondly, through the deep forgery data detection algorithm, the data credibility value is obtained. Thirdly, the ID and credibility value are implicitly annotated as digital watermarks in the data submitted by the user, and the hash value of the data after adding the implicit annotation is calculated. Finally, the hash value is stored on the blockchain and the digitally watermarked data is used in network publications.

In the stage of deep forgery data forensics and appraisal, first forensics of a single electronic data is obtained in accordance with relevant specifications, and its hash value is calculated, and the data and its hash value are bound to form an inspection material to complete the data fixation. Secondly, compare the hash value on the blockchain. If it already exists, it means that the data has not been modified, and the data forensic appraisal conclusion can be directly obtained. Otherwise, carry out further authenticity and similarity identification of the data, and analyze the modification of the data and the degree of similarity with the existing data. Finally, when it is identified that the data has no similarity with the existing data, the data is input into the deep forgery data detection algorithm to obtain its credibility value, and the credibility value and other forensic appraisal results are combined as the final appraisal opinion and stored on the blockchain.

In the deep forgery data traceability stage, according to the results of the forensics and appraisal stages, if there is a clear correlation conclusion with the existing data, the correlation between the data is extracted to form a traceability record and stored on the blockchain. Otherwise, use the digital watermark extraction technology to extract the implicit label information of the data. If it can be extracted, the source of the data can be obtained according to the digital watermark, and it can be determined that the data has been tampered with, and the traceability relationship of the data is recorded in the blockchain. When the digital watermark cannot be extracted, the data is regarded as new original data and processed according to the data identification stage flow.

B. Blockchain-based electronic data forensics and appraisal technology

Before the original data such as images, audios, and videos are released on the Internet platform, a unique identifier is first generated for the data and embedded in the original data. Raw data is divided into two categories, one is real data and the other is deep synthetic data. For real data, we add data identification through implicit embedding. For deep synthetic data, in addition to the implicit addition of data identification, it is also necessary to display the word “synthesis” in accordance with regulations.

In order to verify the authenticity of the data, deep forgery detection is carried out on any submitted original data with the help of the deep forgery detection algorithm. Select the corresponding deep forgery detection algorithm according to the type of original data to obtain the credibility of the data. We concatenate the algorithm name and the credibility, and denote it as R. Set the credibility judgment threshold of deep forgery data. When it is less than the threshold, it is determined that the data is deep forgery, and the word “synthesis” must be marked.

The data identification is generated based on the data fingerprint, the identity of the data owner and the credibility, and is unique. Data identification can not only determine data sovereignty, but also correlate original data. The data fingerprint is generated by the hash algorithm, as follows: DF=Hash(RD), where DF represents the data fingerprint, RW represents the original data, and Hash() represents the hash algorithm. The identity of the data owner is represented by UID, which can be the identity in the user's digital certificate issued by a third-party authority. Considering the privacy protection requirements of the user identity, the distributed digital identity technology can also be used to generate an autonomous identity. The identification of the original data is marked as DI, which is composed of data fingerprint, identity identification, and credibility, that is, DI=DF+UID+R.

Secondly, the data identification is embedded in the original data in the form of implicit labeling through digital watermarking technology. In view of the characteristics of face and voice that are tampered with by deep forgery technology, the mapping relationship between face or voice in the original data and the data identification is constructed, and the data identification is embedded in the original data by using the quantization index modulation (QIM) method [12]. Store the hash value of the original data, the data ID, the hash value of the data after the ID is embedded, and the relationship between the three on the blockchain. Through blockchain technology, data sovereignty is further recorded and data is prevented from being tampered with.

C. Blockchain-based deep forgery data identification method

There is a risk of deep forgery in the electronic data of power production and operation, which may lead to public opinion incidents or judicial disputes. Forensic appraisal of power images, audio and video data related to the case is an effective way to resolve disputes.

First, rely on the blockchain platform to extract and fix case-related electronic data [13]. Extract the electronic data that needs to be forensic appraisal from the target network platform, uniquely number the data according to the forensic authentication specification, calculate its hash value as the basis for data integrity, and store the data, its number and hash value on the blockchain. When extracting data, use a digital camera or screen recording software to record the entire process of data extraction, record the data source and every step of the operation, and store the recorded video on the blockchain.

Secondly, data authenticity and similarity appraisal are required for deep forgery identification. Data authenticity appraisal is mainly to identify the modification of electronic data. Data similarity appraisal is mainly to identify the degree of similarity between electronic data and existing data. According to the electronic data authenticity appraisal standard or specification, identify the generation and modification of the data, and obtain the authenticity identification result. According to the electronic data similarity appraisal standard or specification, identify the consistency, homology and content similarity between the data and the recorded data, and obtain the similarity identification result.

Thirdly, when the above steps fail to obtain a clearly oriented data authenticity and similarity appraisal conclusion,

further use the deep forgery detection algorithm to evaluate the authenticity of the data and obtain the credibility of the data.

Finally, all appraisal processes and results are aggregated to form an forensic appraisal report for this data. The report is encrypted and stored on the blockchain, or its hash value is stored on the blockchain, and the original report is stored on the off-chain electronic evidence platform to ensure that the report cannot be tampered with.

D. Deep forgery data traceability mechanism based on trusted data identification

Through data traceability, the relationship between the dissemination and modification of data is constructed, and the ability to detect deep forgery data is improved. The traceability of power production and operation data is mainly divided into two steps. One is to determine whether it is recorded data by comparing the hash value. The second is to discover the source of deep forgery data by extracting data identifiers.

For suspected deep forgery data, its attributes are firstly analyzed based on the results of forensic appraisal. Through the authenticity appraisal results, the generation time and modification of the suspected deep forgery data can be determined. For the generation time attribute, find out whether there is data on the blockchain with the exact same generation time as the suspicious data. If it exists, the two are likely to be related, and the relationship between the two is marked. Then, through the similarity appraisal results, the degree of consistency or similarity between the suspected deep forgery data and the existing data on the blockchain is determined. When the appraisal result is consistent, that is, the hash value of the suspected deep forgery data is the same as the hash value of a certain data already on the blockchain, then the source of the data has been found. If the same hash value does not exist, the data is not recorded. Then, based on the similarity conclusion, the homology analysis is carried out. If similar existing data is found, the relationship between the two will be marked.

Secondly, by extracting the data identifier of the data to determine whether it is a deep forgery of a certain recorded data. The data identification of suspicious data is obtained by using the quantitative embedding method, and the Hamming distance between the suspicious data identification and the existing data identification is calculated. Set the distance threshold. When the distance is less than the threshold, it is determined as deep forgery data, and the corresponding relationship between deep forgery data and existing data is marked. If it is different from all recorded data identification, the data is recorded on the blockchain according to the electronic data identification method.

III. Safety and efficiency analysis

The blockchain-based deep forgery data identification and traceability framework organically combines blockchain, forensic appraisal and digital watermarking technologies, and has better performance in terms of security and efficiency than traditional deep forgery detection methods.

A. Security Analysis

By embedding traceable identifiers in the source data and storing them on the blockchain, it ensures that the original data cannot be deleted or tampered with, and realizes the trusted management of source data. In the process of deep forgery data appraisal and traceability, the appraisal results and traceability relationship are stored on the blockchain to ensure the credibility of the forensic appraisal report and correlations between deep forgery data.

B. Efficiency Analysis

For the identification of deep forged data, on the one hand, the post-event evidence collection mode is improved to pre-store evidence, which significantly reduces the time for evidence collection and improves the efficiency of forensic appraisal. On the other hand, by improving the existing forensic appraisal technology to make it more suitable for deep forgery data appraisal, so as to improve the law enforcement efficiency of related judicial disputes. This framework establishes a set of electronic data trusted management ecosystem, which can continuously accumulate the correlation between deep fake data and help improve the traceability efficiency.

IV. Conclusion and outlook

In view of the problems of the existing deep forgery detection, such as weak identification ability, difficulty in tracking and tracing, and lack of judicial supervision, this paper proposes a blockchain-based deep forgery data identification and traceability framework, and constructs a deep forgery data full life cycle supervision system from the perspective of active defense, helping to create a trusted electronic data ecosystem. The framework of this paper can improve the existing deep forgery data management methods in terms of security and efficiency, and provide an important reference for related theory and practice. Forensic appraisal technology for deep forgery data still needs in-depth research and improvement. How to judge the legal validity of the results obtained by the deep forgery detection algorithm is also an important research direction in the future.

Acknowledgment

This work was financially supported by State Grid Digital Technology Holding Co., Ltd. Science and Technology Project “Research on deep forgery investigation, evidence collection, identification and traceability technology of power production and operation data”(1200/2022-72001B).

References

[1] W. Li. "From ‘Deep Synthesis’ to ‘Deep Forgery’," Procuratorate Fengyun. China, vol. 12, pp. 11-12, February 2021.

[2] Opinions of the Supreme People’s Courton. “Strengthening Blockchain Application in the Judicial Field,” (2022-07-15). https://www.court.gov.cn/fabu-xiangqing-360271.html.

[3] D. Xie. “Technical authentication of electronic data,” Legal Research, China, vol.44, pp. 209-224, February 2022.

[4] S. Bonomi, M. Casini, C. Ciccotelli. “B-CoC: A Blockchain-based Chain of Custody for Evidences Management in Digital Forensics,” // 2018.https://arxiv.org/pdf/1807.10359.pdf.

[5] Y. Hou, X. Liang, X. Zhan. “Block Chain Based Architecture Model of Electronic Evidence System,” Computer Science. Chain, vol. 45, pp. 348-351, June 2018.

[6] X. Huang, L. Xu, Q. Yang. “A blockchain-based cloud computing electronic forensics model ”. Journal of Beijing University of Posts and Telecommunications. China, vol.40, pp. 120-124, June 2017.

[7] J. Ryu, P. Sharma, J. Jo, et al. “A blockchain-based decentralized

efficient investigation framework for IoT digital forensics," The Journal of Supercomputing. Springer, vol.75, pp. 4372–4387, August 2019.

[8] X. Li, S. Ji, C. Wu, et al. "Review of Deep Forgery and Detection Technology," Journal of Software. China, vol.32, pp. 496-518 February 2021.

[9] W. Zhou, W. Zhang, N. Yu, etc. "A review of face video deep forgery and defense technology," Journal of Signal Processing. China, vol. 37, pp. 2338-2355, December 2021.

[10] S. Zhang, B. Peng, W. Wang, et al. "Deep forgery detection based on hole convolution and attention mechanism," Modern Electronic Technology. China, vol. 45, pp. 42-48, May 2022.

[11] S. Cai. "The technical logic and legal reform of 'deep forgery'," Journal of Political Science and Law. China, pp. 131-140, March 2020.

[12] J. Chen, L. Zhang, M. Jiang. "An anti-collusion vector space data fingerprint scheme," Surveying and Mapping Science. China, pp. 149-156, January 2020.

[13] J. Sun. "Research on scalable electronic forensics model based on blockchain," Computer Application Research. China, vol.38, pp. 671-675,679, March 2021.