Evidence Collection and Qualitative Analysis of Electronic Data in the Background of Artificial Intelligence

Ge Li
NorthWest Minzu University LAW SCHOOL, Lanzhou 610000, Gansu, China

*Corresponding author e-mail: lige@xbmu.edu.cn

Abstract. With the rise and rapid development of mobile communication, intelligent terminal and artificial intelligence technology, in recent years, China has made some progress in the credibility of digital forensics. This paper proposes a forensics method based on artificial intelligence, which makes use of the sequence and dependence characteristics of the previous stage of artificial intelligence to establish an ex post forensics model. When problems occur in the forensics stage, it can feed back to the previous stage and find the problem stage. This paper mainly introduces the forensics and cross examination analysis of electronic data under the background of artificial intelligence. In this paper, we use electronic data forensics and cross examination analysis under the background of artificial intelligence, use a * algorithm for indoor path planning and design, and reasonably analyze the feasibility of Dijkstra algorithm and adjacency table model. This paper analyzes the proof system of the validity of artificial intelligence forensics, uses the evolved expert system to judge the validity of forensics methods and data, and formally proves the integrity and consistency of data in the process of forensics from a theoretical point of view. The experimental results show that the forensic and cross examination analysis of electronic data under the background of artificial intelligence increases the efficiency of the algorithm by 16%. The limitations of the design and research of indoor path planning algorithm for complex environment, and the methods and ways of providing good indoor path planning for the application of ant colony algorithm are analyzed, discussed and summarized, so as to enrich the research results of the academic community.

Keywords: Artificial Intelligence, Electronic Data, Forensics Model, Data Traceability

1. Introduction
In the research of internal environment information service, internal path planning is an important research focus. For different usage, internal path planning will have different index requirements [1-2]. For example, in the case of airport hall or railway station, users are usually required to plan the shortest path to a specific goal [3-4]. In large shopping centers, users will be required to plan the best route according to their own shopping needs. Path map is the data base and calculation object for path planning. The premise of path planning on path map is to express it as the data that can be recognized
by computer, and organize and store it in a reasonable way, so that it can be used for path planning and save storage space [5-6]. This function of internal space greatly reduces the amount of data to be stored. Defending spatial data: different from external data, internal spatial data is dependent.

With the progress of science and technology and the rapid development of the Internet, the design of electronic data forensics in artificial intelligence has been enhanced. James and Q believe that starting from the general digital forensics model, integrating various existing host forensics models, network forensics models and mobile forensics models, we can conclude a general digital forensics process and model that can be widely used, focusing on the research topic [7]. Moshe a thinks that we should learn the method of marking data packets in network forensics, and develop a framework and standard that can be used to mark data traces and store them safely, so that we can query and trace the data during data traceability, ensure the credibility of data static attributes in the process of forensics, and construct a credible forensics workflow model [8]. On the basis of the previous research content, it is proved that the workflow proposed by the model can ensure the traceability of forensics operation content, forming a chain of custodial, that is, evidence integrity chain and forensics supervision chain, so as to ensure the dynamic behavior of forensics process is credible [9-10]. However, there are errors in their experimental process, resulting in inaccurate results.

The innovation of this paper is to propose the forensics and cross examination analysis of electronic data under the background of artificial intelligence. Aiming at the forensics and cross examination analysis of electronic data under the background of artificial intelligence, this paper starts from the trusted forensics and data traceability system of human-computer interaction. According to the above aspects, it starts from the research of trusted forensics of special electronic evidence carrier (such as a hard disk). After obtaining certain characteristics of forensics methods, the scope of forensics methods is expanded to general forensics process types such as host forensics and network forensics, and the common points and feasibility of forensics process and specification are studied, so as to obtain a widely trusted method and system that can be applied to all kinds of digital equipment forensics. The purpose of this study is to find a new way for the development of electronic data system in artificial intelligence.

2. Electronic Data Analysis under the Background of Artificial Intelligence

2.1 Electronic Data Analysis

Under the background of artificial intelligence, after studying the credibility of forensics tools, electronic data still need to standardize the effectiveness of forensics technology in law, and put forward some legislative suggestions on credible forensics. At the same time, the theoretical system of electronic data trusted forensics is based on the static attribute of electronic data trusted and trusted dynamic forensics behavior. The establishment of credible forensics model provides technical and legal traceability for the effectiveness of Judicial Forensics. As the name suggests, according to the existing information, we can trace the traces left by things, so as to trace the source of the initial development of things. The process of traceability also forms an interrelated "traceability chain". The correct derivation of each link can ensure the correctness of the final source.

Nowadays, traceability is mostly used in food safety. From plant cultivation, raw material processing to food production, the environment, quality, quantity and other attribute information in the whole process are recorded in detail and stored safely for query. In case of major food safety accidents, the complete production and processing process can be traced step by step according to the stored information, So as to find out the source of the problem and solve it. Now the traceability of food or agricultural products mainly depends on the RFID based wireless sensor network system. By adding the relevant attribute information in the links of planting, production, processing, logistics and sales to the RFID tag, the information content is synchronized to the central database in real time, Through the management platform connected with the database, the stable operation and safe development of the whole process can be supervised and managed. We can design an effective algorithm in electronic data, which has the following forms.
\[ K = \exp(- (u - v) / 2 \times p l^2) \]  

The calculation value of the electronic data algorithm is, and the formula is as follows;  
\[ K = (U \times V + 1)^{n1} \]  

The following formula shall be used for the test:  
\[ 3I_{02} = I_{a2} + I_{b2} + I_{c2} = 3U_{01} \sigma C_{02} \]  

2.2 Application of Electronic Data Forensics

Evidence collection is also a process of reconstructing the criminal process, and the investigation and evidence collection of evidence also needs to ensure the whole process of credibility, so as to strengthen the legal effect of the investigated evidence. In the process of reducing crime through various kinds of evidence collected, there will be data generated related to evidence constantly, and these data need to be recorded one by one. The general steps of network traceability method are information marking method and the marked information is used to reconstruct path query. The following steps are generally included. The tracing information is recorded to record certain traceability information in the process of continuous forwarding of packets in the network. The recording method adopts the probability packet marking technology that the forwarding node marks the path information in the packet field. The traceability query request is sent by the method of tracing based on log record. Once the node is attacked, the network traceability query request will be issued. The router that records the attack data information in the network will forward the tracing message to the destination. After collecting enough trace information, the method based on probability packet tag can reconstruct the complete path information according to the path information in the packet.

3. Data Traceability Analysis under Artificial Intelligence

3.1 Data Traceability Analysis

The digital forensics process is a process of abstracting effective evidence from ordinary data. A series of steps of obtaining evidence are like taking the forensic equipment as a raw material of products, and finally converting it into a finished product after passing through production lines one by one according to the demand. As the current product traceability, it is to make the relevant data of each link controllable, and the problem link can be quickly found once the finished product has problems. The objective of credible evidence collection is also traced back to the production of products. Relevant data including forensics environment are recorded in each forensics link. Once the legal institutions doubt the evidence obtained, it can find out the detailed information of each step of discovery, fixation, extraction and analysis of evidence, which provides a strong basis for refuting the raised query points. In some special cases, the conditions for obtaining evidence at that time may be limited, which may lead to the unsatisfactory results of forensics. Sometimes, when the technology develops to a certain extent, the data will be taken out for reanalysis. At this time, because every step of forensics at that time is reliable and traceable, it can be based on the information at that time, in the case of the previous step, we choose to save time from one step to improve the efficiency of forensics.

3.2 Electronic Data Forensics System

The forensics model is divided into five steps, including trusted discovery, trusted fixed, trusted extraction, credible analysis and credible representation. The operation and data to be recorded in different stages are different. Therefore, corresponding data record format and method should be developed for each stage. Each link should have their own identification information to facilitate the fast query and location attack mode when tracing the source to guide the search evidence forensics. This also helps to identify and identify all the collected components during the data collection phase, determine the priority of the data, the location of the components being searched, and collect data for each block during the investigation. In general, attack patterns are important in providing a way to protect the system from any potential attack.
As a forensics workflow, the data driven mode is adopted. The operation taken in each step is only related to the previous processing results. In case that each level of processing is not necessarily in logical order, the previous processing is usually recorded in tuple form when recording information. It is used to describe the concept of metadata when describing data attributes. In some cases, the data is used to describe the data attributes, the internal and metadata that traceability wants to express are consistent. When a traceability system is executed, it will carry out the information marked for traceability data in the process. After the execution, it can trace the original process according to the marking information recorded in the traceability data. This paper uses these elements contained in traceability information to describe each link content in the dynamic behavior of electronic data forensics, so that once a step in the process of tracing and collecting evidence can quickly query all the traceability information about the electronic data in this step, which is the complete description of the whole process. The whole traceability chain is closely linked, so the results derived from the data traceability method should be objective and trustworthy. The specific results are shown in Table 1.

| Table 1. The concept of metadata |
|----------------------------------|
| Client a                        | System end protection | survival time | Gprs            |
| Account information             | Database operation    | Protocol header | Full Duplex    |
| contacts                        | Log operation         | check sum value | Extremely High |
| Group information               | Intrusion judgment    | Source IP      | High           |
| Communication record            | Intrusion operation   | Address target | Medium         |

4. Forensics Model under Artificial Intelligence

4.1 Forensics Model
In this paper, the model is divided into forensics workflow implementation module, process management module, data generation and storage module. Among them, data generation and storage module data are metadata information and workflow information generated in the process of forensics. Here, the signature and storage of workflow information are no longer repeated. The process module is the entity description of a series of forensic activities for electronic data in the same way as metadata. Trusted digital forensics is generally divided into five steps: trusted discovery, trusted fixed, trusted extraction, trusted analysis and trusted representation. These five steps are human operation, and software analysis. These operations will be decomposed into multiple forensic activities, and each activity has direct relationship of sequence and concurrency. The specific results are shown in Figure 1. Under the forensics model, the value of trusted digital forensics tends to be stable.
4.2 Forensic Application in Electronic Data

The characteristics of AI are the sequence and dependence of the stages. The first mock exam is the first mock exam. The first mock exam is the first mock exam. When a module is in question and the module is verifiable, it will go back to the previous module to investigate. If there is still a problem, go back to the next level until the root of the problem is found. Then we start to investigate and collect evidence layer by layer until the current level. The model is divided into six steps: authorized investigation, investigation preparation, investigation and evidence collection, data analysis, evidence identification Association and evidence presentation. The step classification is similar to the five steps of credible digital forensics, but the trusted discovery is divided into two parts: investigation and preparation, while the credible fixation corresponds to the investigation and evidence collection link. In the process of forensics of artificial intelligence, a credible electronic forensics model consists of several stages. To achieve the dynamic behavior of the electronic data collection process, it is necessary to ensure that the operation of electronic data in every link of forensics can be queried and verified. The specific results are shown in Table 2.

Table 2. Statistical table of sample library

| Number of Transformers | Standard features | Ageing | behavior        |
|------------------------|-------------------|--------|-----------------|
| Total Sample           | Context model     |        | Context analysis|
| Training Samples       | Context model     | Malfunction | information analysis |
| Validation Sample      | Feature           |        | Operation analysis |

The comparison between general forensics process and improved forensics process Petri net forensics model only establishes the description of the forensics process, which is used to analyze the business process, but does not have independent description of organization and data. In this model, the data and process are organized independently, which can not only improve the flexibility of the model work, but also facilitate the interaction between the models, such as the same metadata structure can be used in another form of forensics process. The organization model can clearly view the structure relationship of all personnel involved in the forensics, which will not cause transparency of work, facilitate supervision and management, and make evidence collection more objective. Data module can make clear the change and direction of data in the process of forensics implementation, make the process of electronic data from evidence to data to evidence more clear and enhance persuasion. The
specific results are shown in Figure 2. Process management is the focus of the model. At the same time, the rules, tools and methods used to execute these processes are also formulated to make each forensics operation follow the rules.

5. Conclusions
In this paper, although in the background of artificial intelligence, electronic data forensics and cross examination analysis, there are still many shortcomings. Tracing all the forensic information of an electronic evidence needs to restore the whole forensic process. The tuple information saved in the workflow model saves the information generated in each step, forming a "forensic chain" in which each step is only related to the previous step. The design of electronic data forensics and cross examination not only needs extensive theoretical knowledge, but also has a solid theoretical foundation and ability literacy. Under the background of artificial intelligence, electronic data forensics and cross examination analysis still have a lot to study. There are still many steps in the research of indoor path design and analysis, which are not involved due to space and personal ability. In addition, the experimental results of the algorithm design can only be compared with the traditional model in theory and simulation.

References
[1] A, M, Baikulova, et al. The System of Development Programmes on Pre-School and School Education in the Republic of Kazakhstan. Interchange, 2016, 48(2), 13-15.
[2] Prof. Dr. Hüseyin Uzunboylu, Gundogdu E G. A Content Analysis Study on Pre-School Education and Instructional Technologies. International Journal of Innovative Research in Education, 2018, 5(4):119-128.
[3] Sandra, B, Ward, et al. An Investigation of Intervention Assistance Teams at a Preservice Level. School Psychology International, 2016, 19(3):279-286.
[4] Donaldson, A. L. Pre-Professional Training for Serving Children With ASD: An Apprenticeship Model of Supervision. Teacher Education & Special Education, 2015, 38(1):58-70.
[5] Lamis D A , Underwood M , D'Amore N. Outcomes of a Suicide Prevention Gatekeeper Training Program Among School Personnel. Crisis, 2016, 38(2):89-99.
[6] Nelson J , Bennewitz L. Special Education Teacher Training and Knowledge of Behavior Assessment and Intervention Practices. Estuarine Coastal & Shelf Science, 2015, 81(4):544-554.
[7] James, Q, Affleck, et al. Expanding the Resource Concept: The Resource School. Exceptional Children, 2016, 39(6),18-23.
[8] Moshe A. Inclusion Assistants in General Education Settings - A Model for In-service Training.
Universal Journal of Educational Research, 2017, 5(2):209-216.

[9] Sandra, B, Ward, et al. An Investigation of Intervention Assistance Teams at a Preservice Level. School Psychology International, 2016, 19(3):279-286.

[10] Kumral O, Sahin A. Farabi Exchange Program in Higher Education with its Purpose and Functionality: An Investigation through the Eyes of Pre-service Teachers. Journal of Higher Education and Science, 2017, 7(1):41-42.