Research of key technical issues based on computer forensic legal expert system

Li Song [1, a]

[1] *Liaoning province,Jinzhou city, Taihe district ,keji road 19, Bohai university, China*

[a] *82325235@qq.com*

Abstract.

The research field of legal profession includes related legal features of computer evidence and its recognition process thereof. Evidence technical features and acquisition techniques thereof are researched and calculated from technical angle in computer field. Since forensic discipline belongs to an inter-discipline established on the basis of law and computer science. It should be researched from the perspective of the two disciplines and specialty embodied on the derived disciplines thereof. In the paper, effectiveness of economic contract and risk consultation during performance are proposed, and legal expert system design model for legal retrieval is established with limited natural language. The system is realized with blackboard model. A knowledge expression method applicable for legal field is also proposed. Law is combined with computer technology for researching computer forensics. Related legal issues of computer forensics are described. Technical methods and tools for computer forensics are mainly researched, and a technical process of computer forensics experiment is provided. Current related laws and regulations of computer forensics and disadvantages of computer forensics technology are proposed. Keys of exchange safety under network environment are discussed with information exchange theory. Existing information laws are analyzed. Establishment of new network safe legal system is proposed from the perspective of information exchange. Finally, the system is designed and realized, and key issues are studied.

Keywords: law; JS structure; expert system; strategy tree; Manual manipulation

Introduction

As we all know, there are two major trends for information revolution: digitization and networking. Digitalization refers that information is fixed in the electronic digital form, thereby forming massive information resources. Digitalized information is characterized by extremely high reproducibility and diffusibility[1,2]. Existing internet with rapid development just provides a platform for digital information dissemination and exchange. Information

exchange is the most basic representation form of information activity. Digital information can realize purposes of exchanging and sharing through network. The state has successively formulated a series of laws and regulations aiming at network security. Domestic scholars have also raised many quite thoughtful comments and suggestions aiming at the issue in the aspect of legal regulation[3,4]. However, since network security is involved in wide range, network itself has characteristics of high scientific content and rapid development, legal systems related to the above two aspects are not sound enough, actual implementation is much difficult, etc., therefore there is no recognized ideal solution. The economic contract legal analysis consulting expert system regards economic contract law as research field, which serves main body of the contract. Some work of legal advisers can be completed by the system; it can assist contract establishers to analyze contract legal validity of contract from the perspective of law[5]. Risk during contract implementation process can be analyzed and estimated according to information provided by contract establisher, expert experience and economic contract law, and reference economic contracts can be drafted. Meanwhile, users can check related articles of contract law, national policies and administrative regulations related with the article of the contract law at any time, thereby assisting users to work and learn. In the paper, exchange safety under network environment is discussed again from the perspective of information exchange. Possible methods for solving the difficulty in legal regulation are proposed.

1 Knowledge Representation and Knowledge KS Structure

Economic contract law analysis consulting expert system is an expert system based on blackboard model[6]. Its overall structure is shown in Fig 1. Legal norm has three basic elements: assumption, processing and sanction specification. Assumption part includes conditions applicable to laws and regulations. Processing refers to model of behavior main body action when assumption conditions are met, and it is main part of laws and regulations. Sanction part refers to national attitude on the subsequence of the part meeting assumption after certain action, such as punishment, reward and so on. Legal specification describes the allowable behaviors, prohibited behaviors, necessary behaviors and behooved behaviors of people[7]. China economic contract law belongs to arbitrary legal norms in accordance with manifestation form of legal regulation. Knowledge of general engineering and technical expert system is only related with knowledge in the area, which is not involved in knowledge of other aspects. Moreover, general engineering and technical expert system can directly express, reason and research the knowledge without comprehension of knowledge semantics. Legal knowledge is not the case. It not only demands knowledge in the above two aspects, but also should analyze semantics of law articles and facts, thereby increasing difficulty in developing legal expert systems.

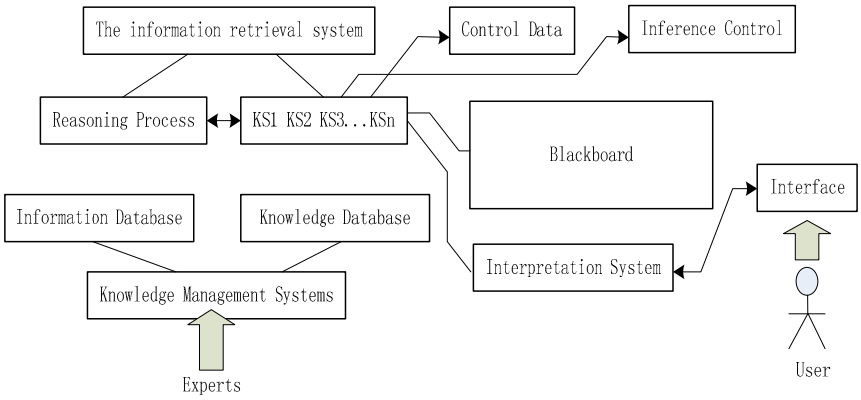

Figure 1 General structure of legal expert system

Features of Computer Evidence

Material carriers of computer evidence include electronic components, magnetic materials, etc. Only integrated circuit electronic matrix positive and negative levels or magnetic material magnets, etc. are changed from the aspect of physical representation. Special means are demanded for obtaining evidence of these behaviors, which is completely different from acquisition of other evidences. Calculation technology, storage technology, network communication technology, etc. in computer science must be adopted for computer evidence generation, storage, transmission, collection, analysis and judgment. Vulnerability: since computer information can easily be modified, and no traces can be left after actual modification, therefore computer information is fragile and unreliable. Manual manipulation of data and program destroy are universal at certain degree. Treatment of computer system on data is characterized by multiple links and complicated technology and equipment. In addition, data can be modified instantly due to faster and faster processing speed of computer. Therefore, the computer evidence is not always reliable. In addition, it also has human-computer interaction characteristic, namely formation of computer evidence is participated by different computer operators in different links. They can affect operation of computer system at different degrees. In addition, the influence level and degree are related with work property of these employees. Man-machine system should be strictly controlled in the aspects of technology and management in order to ensure evidence reliability and authenticity.

Former Knowledge Representation of Economic Contract

Economic contract law representation should reflect the above characteristics. Characteristics of contract law can be accurately mastered by meeting the above features, which is beneficial for acquisition and reasoning efficiency of legal knowledge. Hierarchical characteristics of legal knowledge can be reflected by

tree structure. Parent node and child node can have corresponding relation with elements of legal regulations. Features of legal regulations, morality and ambiguous performance, can be reflected by determinacy of logic relation among the two aspects. Applicable strategy of related legal regulation also can be described by mesh of legal knowledge. Meanwhile, the strategy also reflects contractual relationship of contract rights and obligations. Expert experience and contract law can be included, summarized and abstracted into strategy tree as shown in figure 2. Method for describing strategy tree can be adopted in the system in order to increase flexibility of reasoning, and improve interpretation and reasoning efficiency. Therefore, strategy tree knowledge representation method based on rules can be formed. In the method, strategy is described by a group of rules. Strategy tree can become a virtual form. The conceptual structure can play a role of restricting production rule application environment.

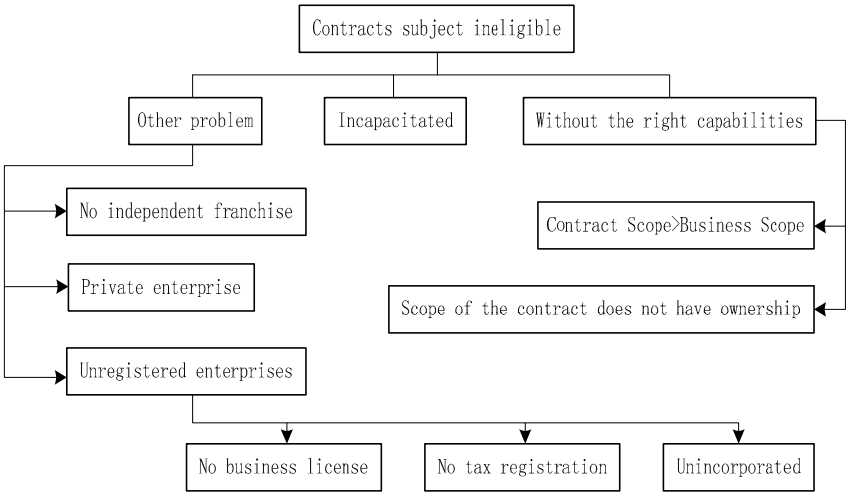

Figure 2 Strategy tree structure

Information Exchange Based on Network

Information exchange belongs to transmission and exchange behavior between information sender and recipient, which is realized through utilizing some delivery channel with some symbol system. Information exchange is different from information dissemination mainly in that information exchange belongs to two-way interaction behavior. That is, the information sender and information receiver are corresponding, and their roles can be interchanged. Information exchange pays more attention to subjective initiative of information exchange main body compared with transmission. Information transmission receiver only can receive passively with weak interaction and continuity. Network is the fourth largest media following newspapers, radio and television. Network inherits many advantages thereof compared with the former three media. It has unique advantages. Information can be exchanged freely by the advantage. Information

exchange based on network environment has new characteristics of exchange mode integrity, environmental dependency, exchange theme uncertainty, etc. These features belong to aspects that must be considered for managing network information exchange.

Survey Forensic System of Computer Operating Environment

The system integrates network scanning technology, system scanning technology and network monitoring technology. Chinese character graphical interface is adopted with convenient and rapid operation. Original running state of system environment is protected. Cross-platform network communication can be realized through multi-level network protocols under the precondition. Dynamic vulnerability knowledge base is utilized to achieve vulnerability check of systems and networks. Model check can be utilized for realizing security protocol analysis. Effective algorithm can be utilized for realizing network topology information search on the basis of existing ICMP protocol tool. Key technologies adopted in the system include the follows: network equipment; automated scanning and analysis technique configured on the host machine; analysis technique based on network management protocol; automatic development and analysis technique of network topological structure, automatic acquisition and expression technology of application, services and other information in network, visualization technology of operating environment and topological structure. Model checking techniques are utilized for realizing system vulnerability analysis. The system structure is shown in Figure 1. Vulnerability rule base is utilized; dynamic link library technology is combined for scanning vulnerability, which is convenient for system upgrading and expansion. System scanning technique based on plug-in technology can uniformly solve multi-version problem of system scanning. The system structure is shown in figure 3.

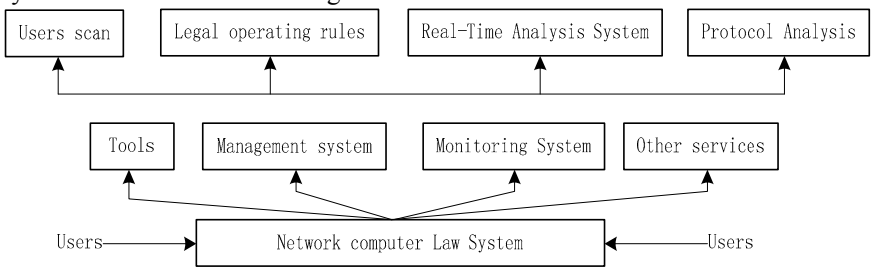

Figure 3 Forensic system overall structure diagram

Legal Regulatory System Structure

Law system structures can be firstly constructed in order to assist people to better understand content of information exchange safety laws. Research achievements

of all aspects to information law are integrated. We believe that network information exchange safety regulations, network information property rights and network information resource management method are listed as three parts of network information laws. Concrete contents include the follows. 1) Information content safety regulations: flowing information in network is mostly related to economic organization development and survival trade secrets, which is also related to national secrets of national safety. If the information is not protected properly, very serious consequences can be generated on the state, society, organizations and individuals. 2) Information channel safety regulation: information channel is a platform to realize information exchange. The platform can be classified according to software and hardware. Network information system is a platform to achieve information exchange. Behaviors of illegally intruding network system and damaging computer information system should be cracked down in order to protect it. Information equipment belongs to hardware platform of information exchange. Management legislation should be generally implemented on the information equipment, and standardized management system should be established. 3) Information safety evaluation legal system: information regulation will encounter many difficulties during implementation. Information safety evaluation system not only provides a safety standard for determining safety rating of evaluated objects, but also can indicate development strategy direction for information safety, thereby preventing safety accidents

Reasoning Control Structure

Reasoning is controlled by blackboard monitoring procedures and scheduling procedures. State changes on the blackboard should be observed by monitoring procedures. Interested rules of the change can be searched according to the change, namely rules in activating state and triggering state can be selected. They are respectively sent to activity queue and waiting queue, thereby composing control data structure, and providing necessary information for schedule procedure. Schedule procedure can necessarily modify the state on the blackboard. Rules under activation state in activity queue can be acted on the blackboard each time, thereby realizing some propositions, and causing changes of blackboard state. New evidence is provided for reaching ultimate decomposition state. After blackboard action is completed, the rules can be retreated from activity queue. However, blackboard is changed due to their role. Some new rules are also in activated or triggered states. The monitoring procedure can reselect rules in activated and triggered states. Rules in triggered state can be recorded in the waiting queue. The rules are characterized in that they hope to become activated state, or the preconditions may be consistent with conclusion.

Conclusions

In the paper, knowledge representation and knowledge KS structure are proposed by analysis firstly. Computer evidence features are analyzed, therefore economic contract original legal knowledge representation methods are combined for integrating network information exchange technology into the system. Computer forensic legal expert system is designed and implemented. The system also proposes legal regulation system structure and reasoning control mechanism. Legal recognition and computer forensic procedures and principles of computer evidence as well as computer forensic application technology are studied in details. On the basis, it is proposed that computer forensic science should be studied in the aspects of law and technology. Disadvantages and future development trends in the two aspects are proposed. It is beneficial for clarifying vague awareness in the field, and promoting perfection of computer forensic laws and regulations as well as further improvement of computer forensic technology. The paper has the following shortcomings: practical application model of the system is not established in details, it is not sufficient to further prefect the system by practical case, therefore combination of actual application case will be considered in next step, thereby verifying advantages and practicality of the system with fact

References

[1] Dj.M. Maric, P.F. Meier and S.K. Estreicher: Mater. Sci. Forum Vol. 83-87 (2011), p. 119

[2] M.A. Green: *High Efficiency Silicon Solar Cells* (Trans Tech Publications, Switzerland 2005).

[1] Corey .V, Peterman.C and Shearins.S: IEEE Internet Computing Vol.6(2010),p.60−66.

[2] Zhang.J, Gong.J : Computer Science Vol.30 (2003),p.155−166.

[3] Reith.M, Carr.C: Int'l Journal of Digital Evidence Vol.1 (2002), p .1−12.

[4] Zhao.X:*Teaching Material Writing and Editing Council in Ministry of Public Security*(The Mass Press , Beijing 2012).

[5] Zhang YJ: *Network Security and Detection Technologies on Computer Crime*(Tsinghua University Press, Beijing 2010).

[6] Wang.L, Qian.H.L: Journal of Software Vol.14 (2003), p. 1635−1644.

[7] Zhang. P: *Internet Law Review* (Law Press China, Beijing 2010).