

Research on Construction of the Information Content Security Curriculum System

Zhuang Miao

College of Command & Control Engineering
PLA Army Engineering University,
Nanjing, China
E-mail: emiao_beyond@163.com

Honglong Gao

Institute of the PLA Army Armored Engineering,
Bengbu, China
E-mail: honglong40889@126.com

Bo Wu

College of Command & Control Engineering
PLA Army Engineering University,
Nanjing, China
E-mail: wubo@163.com

Yang Li

College of Command & Control Engineering
PLA Army Engineering University,
Nanjing, China
E-mail: solarleon@outlook.com

Jiabao Wang

College of Command & Control Engineering
PLA Army Engineering University,
Nanjing, China
E-mail: jiabao_1108@163.com

Zhijie Zhao

Unit No.31700 of PLA
Liaoyang, China,
E-mail: zzj765413@qq.com

Abstract-Information content security refers to the selective blocking of information in the flow of information space, so as to ensure the reliable and controllable flow of information. Information content security is of great significance and application value to national security and military information secrecy. In this paper, the significance and necessity of opening the course of information content security are analyzed. The knowledge system of information content security is discussed. The curriculum system of information content security is put forward. The applicability of the curriculum system to communication, command automation, computer, network and other related majors is analyzed simply.

Keywords-component; information content security; knowledge system; curriculum system; information hiding; information retrieval

I. INTRODUCTION

With the development and popularization of information technology, the variety and quantity of information content rapidly expand. In particular, the widespread application of the Internet has caused reactionary speech, secret information and bad content to fill up, which poses new challenges to information security. In military, government, commercial and other industries, the disclosure of information content will lead to serious consequences [1]. Therefore, the importance of information content security, or information security based on content, is becoming more and more important. It is a new problem in the new situation of information development. However, it is difficult to strictly limit the scientific definition of confidential content and the

classification of information content security level. In addition to the traditional text information, a large number of multimedia information such as voice, image, video and so on make the difficulty of information content security rating, marking, monitoring and other problems increasing, information content The security situation is not optimistic..

II. RELATED MAJORS AND COURSES

Since twenty-first Century, information security education has been gradually developed in China's higher education. Following the approval of the Ministry of education in 2001, the undergraduate program of information security was approved in Wuhan University, and several universities have been approved to set up a bachelor's degree in information security. Many universities and scientific research institutes have set up a master's and a doctoral degree in the direction of information security. In 2005, the Ministry of Education issued a document "on Further Strengthening the information security disciplines, professional construction and personnel training," and will establish a national information security system as one of the basic strategic goals of national development.

Many famous universities in China have set up relevant courses on information security, such as cryptography, network information security and so on [2]. Some colleges have set up information security specialties, such as Beijing University of Posts and Telecommunications, University of Science and Technology of China and so on. As the foundation of each university is different, the emphasis of the teaching of information security is different. For example,

Beijing University of Posts and Telecommunications and Wuhan University mainly teach the network information security. The Southeast University has set up information security related courses based on the information processing of wireless system. The Xi'an Jiaotong University has opened a letter in the mathematics major. Information security courses mainly focus on cryptography. Information Engineering University involves information security in the course of undergraduate teaching, and cryptography is one of the main teaching contents. In 2017, the Academic Degrees Committee of the State Council and the Ministry of Education decided to set up a Cyberspace Security level discipline under the category of Engineering to award engineering degrees. At present, the Institute of information engineering of the Chinese Academy of Sciences has set up a Ph.D. degree in this field.

III. THE KNOWLEDGE SYSTEM OF INFORMATION CONTENT SECURITY

Information content security is not a single technique. It is integrated into a variety of technologies, such as information retrieval, digital signal processing, information hiding, content reasoning and analysis. Each of them contains many theories, methods and means to form a separate research direction.

At present, there is still a lack of unified understanding of the definition of information content security and the understanding of its connotation and extension, and there is no authoritative knowledge system on information content security. Although many technologies can be included in the scope of information content security at present, some conferences are subject to the subject of information content security, but there are also some conferences on the subject of information content security. There are few textbooks on information content security. According to the connotation of information content security, its possible knowledge system mainly includes the following contents.

A. Information Hiding and Digital Watermarking

In real life, people tend to resort to cryptography for the protection of information. Cryptography is a discipline that studies communication security and secrecy. Its basic idea is to disguise confidential information. That is, the user changes the confidential information that needs to be camouflaged and gets another expression that seems unrelated to the original information. The legitimate user can restore the original confidential information from the information, and if the illegal user tries to analyze the original confidential information from the camouflaged information, either the analysis process is simply impossible, or the cost is too great to carry out.

With the development of computer hardware and software technology, the ability of password decoding is getting stronger and stronger, which forces people to put forward higher and higher requirements for the strength of encryption algorithm. In many areas, cryptography has

shown its limitations. Ciphertext is easy to cause attackers' attention, which is a significant weakness of cryptography. Therefore, it is not enough for some applications to encrypt information content only.

The purpose of information hiding is to hide confidential information in a general file and then transmit it [3]. The information intercepted from the network by the illegal interceptor seems to be the same as other general information that is not confidential. Therefore, the probability of avoiding attack is high. At present, it is mainly realized by using digital watermarking technology [4].

Cryptography and information hiding technology are different from the perspective of information security technology, combining the two, can further enhance the security of information. For example, the encrypted message is encrypted first and then the ciphertext is hidden into the carrier. In order to get the message, the attacker should first detect the existence of the message, and know how to extract the ciphertext from the secret carrier and how to decrypt the ciphertext to restore the message, which greatly increases the difficulty of the attack. Cryptography and information hiding are two effective ways to ensure information security. They promote each other and develop together.

B. Network Information Retrieval and Filtering

Network information retrieval and filtering is a technology to analyze, identify, judge and classify the content of the acquired information, determine whether it is the required target content, and filter and control the target content which has been determined. From a technical point of view, information filtering is the opposite process of information retrieval [5]. It needs to search for relevant information before deciding whether to return to the requestor. According to the format of search information, it can be divided into text and multimedia information retrieval and filtering.

The text information filtering technology is based on the simple method of keyword filtering, by using various methods and techniques such as Natural Language Processing, artificial intelligence, data mining and so on, according to the semantic features and text elements, such as theme, internal capacity, format and context, which are presented by some contents of bad information. Information filtering technique is to identify and filter target information by analyzing and understanding the semantics of text content [6]. The filtering analysis of this content semantic analysis is not an absolute judgment. It can't be filtered by one or two keywords, and it is also dependent on the semantic meaning of the text content. It has the characteristics of high fitness and high accuracy, and can effectively solve the problems that can't be handled well by grading tags, address library and keyword filtering technology [7]. With the increasing number of multimedia information such as images and videos on the Internet, it has become the main object of information retrieval and filtering.

According to the principle of information retrieval and filtering technology and the characteristics of information content, its key technical work can be summed up in two aspects. One is that content preprocessing, which is to preprocess the content of the information source, and extract the explicit and recessive characteristics that can reflect or help distinguish the nature of the content, so that the retrieval or over is to be retrieved or passed. The content of the filter is effectively expressed by the feature item. The other is that the content matching is matching and sorting the information template with the content to be retrieved or filtered according to a certain matching rule and method, then the information source is processed according to the matching result, and the processed result is returned to the user who submits the application request.

C. Information Content Recognition and Reasoning

Information content identification refers to identifying, judging and classifying the content of information obtained, determining whether it is the required target, and the accuracy and speed of recognition is an important index. It is mainly divided into text, voice, image and pattern recognition [8]. Word recognition includes keyword, feature word, attribute word recognition, grammar, semantics, pragmatic recognition, theme, position and attribute recognition, including rules matching, string matching, natural language understanding, classification algorithm, clustering algorithm and so on. The current network intrusion detection products, anti-virus products, anti-spam products, and staff online filtering products are basically based on the text based identification method. The research of audio content recognition technology belongs to the category of audio information retrieval. The research work on audio cords began in the late 90s of last century. At present, speech recognition technology has entered the practical stage. In recent years, the gradual maturity of deep learning has made the image recognition technology move towards practical stage.

Based on information content identification, the knowledge base is established according to the specific information security rules, and the related information is connected and reasoning to prevent the recessive leakage of key information [9]. It is of great significance and broad application prospect for military and national security.

IV. TEACHING CONTENT OF INFORMATION CONTENT SAFETY COURSE

Information content security is based on deep theoretical knowledge, including computer application, computer software, digital signal processing, network and communication and other professional knowledge. At present, because our university has not specially set up the information security undergraduate major, it lacks the complete curriculum system of information content security, some related professional courses involve some knowledge, but it is not comprehensive; some contents are scattered in

the teaching content of many courses, and the content is not involved in the existing curriculum system.

Based on the analysis of information content security knowledge system, we propose the following curriculum system. It is shown in Figure 1.

A. Prerequisites

It refers to information representation and processing courses, computer and communication basic courses, etc. they are the basic principles of computer, communication and information processing. It mainly includes computer organization principle, algorithm and data structure, introduction to program design, computer hardware foundation, digital communication principle, digital signal processing and so on.

B. Professional Courses

It refers to the content directly involved in the information content security knowledge system, including cryptography, information hiding and digital watermarking, Natural Language Processing, artificial intelligence, data mining, information retrieval and so on. These courses can be taught individually, and can also be integrated into the content of information content security course.

C. Extended Courses

It refers to courses related to the frontiers of information content security, including information security technology lectures, information security and privacy regulations.

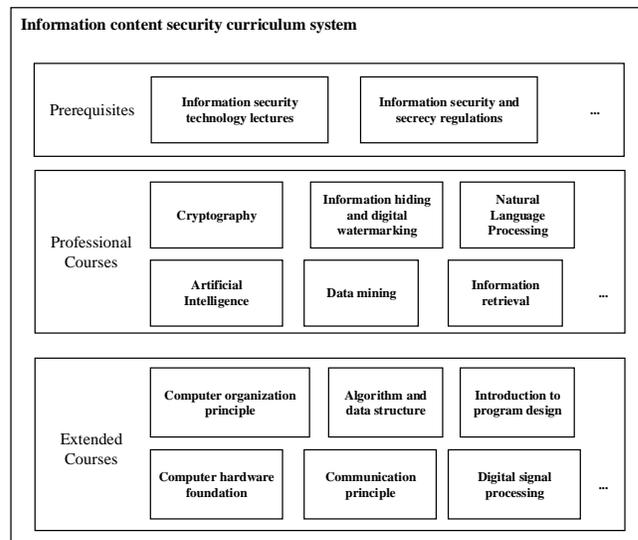


Figure 1. Information content security curriculum system.

V. APPLICABILITY OF INFORMATION CONTENT SECURITY COURSE TO RELEVANT MAJORS

Information content security is widely applied in many aspects. For example, web page filtering, short message filtering, personalized service and so on. Different from mail filtering is mainly content acquisition module, and the real

function part can be based on the development of information content security. In addition, the security of information content is increasingly needed for the society, for example, for the government to prevent illegal, reactionary, and pornographic information; for enterprises, to prevent the disclosure of internal confidential documents; for individuals, it is necessary to obtain the most necessary information in the vast ocean of information; for the army, not only In order to prevent the leakage of confidential documents, many times, we need to prevent the leakage of sensitive information from seemingly unrelated information, that is, counterintelligence collection.

At present, the importance of information security is constantly improving, and the input of information security construction has been constantly increasing in the process of informatization. For the training of talents in Colleges and universities, the students of communication, command automation, computer and network need to know some theories, methods and means of information security in different degrees. Therefore, the information content security course is not only important for the information security

profession, but also has certain applicability for other related majors such as computer and communication.

REFERENCES

- [1] K Wrona, S Oudkerk, "Integrated content-based information security for future military systems," Military Communications Conference, pp. 1230-1235, 2015.
- [2] B Xiong, L Jiang, L Xiang, "Research on curriculum system of network security and management," Computer Era, 2013 (10) :62-64.
- [3] F Petitcolas, R Anderson, M Kuhn, "Information hiding-a survey," Proceedings of the IEEE, 1999 , 87 (7) :1062-1078.
- [4] CI Podilchuk, EJ Delp, "Digital watermarking: algorithms and applications," IEEE Signal Processing Magazine, 2001, 18 (4) :33-46.
- [5] C Faloutsos, DW Oard, "A survey of information retrieval and filtering methods," University of Maryland at College Park, 1995.
- [6] W Zhang, "Content-Based Information Security Technique for Chinese Text," Springer Berlin Heidelberg , 2006, 4223 :650-659.
- [7] S Loeb, D Terry, "Information filtering," ACM , 1992 , 35 (12) :26-28.
- [8] A Nigrin, "Neural Networks for Pattern Recognition," Agricultural Engineering International the Cigr Journal of Scientific Research & Development Manuscript Pm, 1995 , 12 (5) :1235 – 1242.
- [9] R Fagin, JY Halpern, Y Moses, MY Vardi, "Reasoning About Knowledge," MIT Press, , 2003 , 67 (2) :503-525.