The Application of Information Hiding Technology in Network Accounting

Yan-Ling HU
Jilin Teachers Institute of Engineering and Technology
Changchun, Jilin, China
1104909735@qq.com

Keywords: Information Hiding Technology, Network Accounting, Application Introduction.

Abstract. With the rapid development of network technology, network environment brings unprecedented opportunities for the development of network accounting, but at the same time, the information security provided by network accounting has become the focus of people’s concern, because of the complexity of the economic environment, self-quality of the accountants, the inherent limitations of computer network and so on, it brings some problems for network accounting security, this paper explores the application of information hiding technology in network accounting which is safer than data encryption.

Information Hiding Technology is the Key Technology in Network Accounting System

Acquisition, storage, transmission of information security has become the focus of people’s concern, encryption and access restriction is not enough to guarantee the safety of information and decoding technology, decoding technology, hackers and other technologies make people feel that the Internet is less secure and reliable, “crisis without limit” of the Internet makes people feel regret about the “commercial opportunities” As a result, information hiding technology which is more secure than data encryption comes into being.

The early stage of the accounting computerization makes accounting method from the abacus to the keyboard, from books to disk. And network accounting will make the media continue to change, move rapidly to the electronic, such as all kinds of invoices documents of settlement are presented in the form of electronic accounting data. The circulating process of the signature and seal and other traditional means have lost their power.

With the development of electronic commerce, electronic money will also replace the notes or coins into circulation, complete the settlement function. Network accounting environment is a set of network system which includes suppliers, manufacturers, distributors, customers, banks and other institutions as a whole, there is no direct transaction payment, on the contrary, it is the online settlement by electronic money. The concentration and automatic control of the computer information processing make traditional authority segmentation disappear, the changes of information carrier and improvement of sharing degree make manual accounting system as the core of the control system ineffective, Therefore, modern information technology gives a new meaning to the enterprise's internal control, such as password control, data encryption, authority management, access rights to the time management, log management operation, etc.

People traditionally love and agree to regard all invoices and settlement documents as proof of purchase and sale of the two sides, when they come in the form of electronic, how reliable,
safe transfer accounting vouchers, purchase and sales invoices (especially seal information) is the core problem of the network accounting and electronic commerce needs to solve, information hiding technology for solving this problem will have a key role, which is a very practical and effective technology in network accounting system in a very practical and effective technology.

The Origin of Information Hiding Technology

The openness, internationalism and freedom of the Internet, on the one hand increase the degrees of freedom of the application, improve work efficiency and the response capacity of the market, on the other hand they must face the new challenge and the new danger, that is the higher requirements for the information security proposed. Therefore, information security in the information age is a related to national security, economic development and personal interests of the major issues. Information security requires a complete system to protect, this involves legislation, technology, management, application and many other aspects, which information security technology is an indispensable link, advanced security technology is the fundamental guarantee of the information security[1].

Information hiding is an old and interesting information security technology; information hiding and history are examples of information camouflage. Such as in order to avoid suspicion of others, poets use hiding the beginning, the end and leakage form of the poem, to express the meaning hidden at a particular position in the poem. The majority only pay attention to the surface meaning of the poem, and do not explore the hidden meaning in the poem. In WWI and WWII, steganography ink, hollow coins and micro photographs and other means make information hiding technology obtain significant development.

Modern information hiding can be more strictly known for information hiding (steganography). It provides a non-cryptographic security approach, using a new idea: use of digital audio and video signal for people's visual, auditory redundancy, spatial domain and transform domain information hiding, so as to realize covert communication. The technique combines multidisciplinary theory and technology as a whole, the mathematical statistics theory, cognitive psychology, cryptography, communication theory, coding theory, spread spectrum technology, signal processing technology, data compression technology and noise theory, audio-visual perception theory can play a part in this new field.

The basic idea of digital watermark (Digital Watermarking) technology is the result of ancient Steganography. The Spartans in ancient Greece had the military intelligence on ordinary wood, using paraffin fill and level up, the receiving party as long as they roast hot board, melting wax, can be seen. During World War II, the use of steganography method to calculate chemical steganography, milk, alum, fruit juice, etc. have been used as steganography potions. That is to say, the early human use of secret communication means belongs to steganography rather than a password. However, compared with the password techniques, because of the lack of necessary theoretical foundation, steganography technique has not developed into an independent discipline.

Nowadays, the development of digital technology has injected new vitality, also brought new opportunities for ancient steganography. In the study of digital watermarking process, researchers use the idea of steganography as a reference. Especially in recent years, the rise of information hiding technology, steganography has become a rigorous science. There is no doubt, steganography technology will revive in the digital age.
The Definition and Classification of Information Hiding and Digital Watermarking

The Definition of Information Hiding

Information hiding is to use different data redundancy existing digital media itself, as well as the human physiological and psychological sensory organs which are not sensitive to certain information, the secret information hiding in another carrier, Cover Signal (Cover Signal) in the (this) Coverage can be still images, audio, text, video and other digital media). Due to external characteristics of the external performance is the first signal, does not change the basic characteristics and use value, so the information hiding with password encryption method has its own advantages of secret communication.

The biggest advantage of information hiding methods to realize covert communication is except the two sides of communication any third party do not know of the existence of the fact of secret communication, that means adding a layer of protection to simple password encryption method, making network encryption mechanism from “see don't understand” to “invisible”, so as not to become the target of the attacker.

The Classification of Information Hiding

According to the different processing methods and application fields, information hiding technology can be divided into two categories: hidden communication technology and digital watermarking technology:

Hiding Communication Technology

Hiding communication technology refers to the secret information hidden in some public digital media, make secret information be transmitted in the communication network security technology of secret communication. For the implementation of the communication of both sides, secret data is embedded by the information of interest, but the appearance is just a secret information hiding carrier, its content does not have any practical significance.

Digital Watermarking Technology

Digital watermarking technology refers to methods of signal processing of digital multimedia data in embedded hidden marker. The marker is usually unaware of the information, only through a special detector or reader to extract. It tries to identify and protect the copyright of digital media. The value at this time is the appearance of digital media, people do not need the specific content of the watermark information, and only care about its existence, will be changed, whether be deleted. Digital watermarking technology is widely used in copyright protection for digital products, online data transmission and storage of data integrity verification (whether it was tampered with), network business transaction behavior authentication and bill anti-counterfeiting. Due to the digital watermarking technology is a safeguard in the normal order of the network society the study of its technology has become the focus of people’s attention. [2].

As a branch of information hiding, digital watermarking has been developed rapidly in recent years, and the following we will focus on the digital watermarking technology.

Classification of Digital Watermarking

According to different characteristic of digital watermarking, it can be divided into three categories: robust digital watermarking, (fragile digital watermarking) and annotating a digital watermark (annotation digital watermarking). Digital watermarking for copyright protection
is generally called robust digital watermarking, for multimedia content authentication
watermarking is commonly known as fragile watermark, to be used only for multimedia
assisted marking watermark information about multimedia content is commonly known as
annotation watermark. The fragile watermark and the robust watermark are most common.

The robust watermark is embedded the owner’s information in the multimedia content, or
embedded in the label (i.e., serial number) of the buyer, in order to realize the purpose of
copyright protection. In the event of disputes, the information of the creator or the owner is
used to identify the data of the copyright owner, and the serial number is used to track the
users who violate the agreement and provide multimedia data. Digital watermarking for
copyright protection requirement has very strong robustness and security, in addition to the
requirements in general image processing such as filtering, adding noise, compression, etc.) to
survive outside, it still needs to resist malicious attacks. The robust watermark is a hot topic of
current research, but there is still a long way to go for the practical application.

Fragile watermarking is also in the record multimedia content data (not in the file format)
that embeds the invisible information. When a change occurs in the contents, the watermark
information will change corresponding to identify whether the original data has been
tampered with. Fragile watermark has strong ability of immune to common image processing
(robustness), at the same time it requires a strong sensitivity, namely, it allows a certain
degree of distortion, and distortion can be detected. Robust and fragile watermarks in many
aspects are different:

First of all, different purposes. Judgment data distortion is the purpose of fragile
watermark, and pay attention to under the premise of security as possible report distortion.
Robust watermark is used in copyright Robust watermark is used for copyright protection, the
request can withstand the general image processing.

Second, fragile watermarking needs to have label ability. Fragile watermarking can not
only detect the watermark, but also as for the distortion of the data, detection algorithm could
be pointed out the distortion region and even indicate the frequency domain, makes an
analysis of the causes of the distortion.

Third, the vulnerable watermark pay more attention to the use value of the original data
than the robust watermark.

Fourth, fragile watermark is sensitive to rounding errors and overflow, and the robustness
of digital watermarking is the opposite.

Fifth, attack on the difference. Robust watermark to resist attacks can be divided into: basic
attack, attack robust, expression attacks, interpretation attack, and the implementation process
of the attack.

Comparison between Information Hiding and Traditional Encryption Technology

Information hiding technology and the traditional encryption technology has obvious
difference.

Traditional cryptography (Cryptography) regards hiding the secret information as its
purpose, the content of the traditional method is the method to encrypt data in cryptography,
the result is characterized by a chaotic encrypted information.

Difficult to understand, do not read the state of (state) look not to understand, to protect this
information at the same time, also easy to cause others to doubt, snoop attack was intercepted
and cracking. It is by increasing the key length so that it can not be deciphered, along with the
computer computing power multiplied, the encryption method is more and more insecure.
Due to the defects of encryption in the communication and the limitation of multimedia content protection, it leads to the development of information hiding technology. It becomes one of the sensitive information security communication ways after the cryptography. Information hiding communication external performance is the content and features of the signal coverage, covered by the information disclosure and the third party will not feel secret information (can not see), and basic characteristics and clinical value of secret information did not change at all, so information hiding has a stronger information security and information security.

The main differences between the information hiding and the traditional encryption technology can be summarized as follows:

**Hidden Objects are Different**

Encryption is hidden content, and information hiding mainly hides the very existence of the hidden information. Covert communication is more secure than communication encryption, because it hides the receiver and transmitter of the communication, and the existence of the communication process, it is not easy to arouse suspicion.

**The Effective Range of Protection is Different**

Traditional encryption method for content protection is only confined to the encrypted communication channels or other encrypted state, once decrypted, without protection; information hiding, does not affect the use of the host data, only needs to be tested when detecting the hidden data, later it does not affect the role of the access and hide information.

In general, robust watermarking for copyright protection requires a longer protection effect.

**The Degree of Tolerance of the Data Distortion is Different**

The copyright protection of multimedia content and authenticity are often required to tolerate a certain degree of distortion, and the encrypted data do not allow for a bit of change, otherwise it is impossible to decrypt. Therefore, digital watermarking technology is even regarded as the last line of defense for multimedia content protection. The password in a lot of thought could be used in data hiding (such as security of digital watermarking system should be established on the basis of key, does not obtain through the algorithm confidential security), And the application systems of information hiding, (such as digital watermarking) tend to depend on the password system to achieve, we could combine the hidden communication technology and the password technology together, using the traditional cryptography to make encryption processing of secret information hidden in other coverage, in order to achieve both the existence of hidden information and the double security role of the content of the hidden information.

**The Basic Principle of Digital Watermarking Technolog**

Digital products including images, video, audio, text, etc., are all in order to meet the demand of people's visual, auditory sensory (business or law enforcement), which requires the watermark not undermine its ornamental value and use value, require watermark should not compelling. As we all know, any digital information to analog signals, has its inherent error range, the noise of the so-called, because it is analog signal approximation; The making process of the digital watermarking can be considered to incorporate information such as property right as the additive noise in the original digital products, but does not affect the
person's sensory perception of digital works appreciation, it is using the redundancy on the feeling. This is not easy to perceive the premise of digital watermarking[3].

The key performance of digital watermarking is not easy to perceive. First, people don't know its existence; Second, even if its existence, people don't know where it is hidden, difficult to be removed. Can cite an example: A needle fell into the sea not carefully, do you want to find it is very difficult, why? On the one hand, because the needle is relative to the size of the sea is too small, on the other hand the needle from your hands drop off when where is uncertain. Digital watermarking technology is using this principle, namely unspectacular and randomness. This ensures that the digital watermark hidden deep in the digital works, can't be found and removed.

The Basic Requirements of Digital Watermarking Algorithm

A mature digital watermarking algorithm must be able to resist various attacks that mentioned above. of course, different types of digital watermarking may get different attacks, therefore, different watermarking has different technical performance, but in general, it should have the following features[4].

The Security of the Hiding Place

Watermark should be embedded directly in the data, rather than on the file head or tail and other locations, the file format of the transformation should not lead to the loss of the watermark data.

The Security of the Algorithm

A watermarking system want to be applied in business field, the algorithm must be public. The security of the algorithm depends entirely on the key, rather than on the algorithm in order to obtain security. Therefore, the key space need be large enough, and must be evenly distributed.

Randomness

Depend on different methods of deposit and random location to ensure that, by using cryptography in the password encryption (including public key and secret key) system to strengthen.

To Extract the Watermark Does not Need to the Original Data

Don't have to get full data, only can be detected from the data stream digital watermarking. Many applications can not make sure the original data (such as: to search a lot of illegal copies of some images on the Internet), or no original data (such as: can be used for most digital cameras). But there are also a number of occasions can use the original data to improve the accuracy of watermark extraction.

Low failure probability can embed a number of robust watermarking, and can distinguish the different join order of robust watermarking (may require third party notarization)

The Hiding Capacity

That is the maximum number lies in the digital media, which reflects the ability to hide secret information.

Obviously, in the digital watermarking technology, there are some contradictions between
the size of the information hiding capacity and the level of robustness, that is, the larger the hidden capacity, the worse the robustness, and vice versa, so in the application, it needs to be weighed according to the requirements.

From the subjective perspective, the ideal watermarking algorithm should not only hide a lot of data, but also resist channel noise and signal distortion. However, in practice, these two indicators cannot be realized at the same time, but this does not affect the application of digital watermarking technology, because the practical application only emphasizes one aspect of it. If it is for covert communication, the amount of data is clearly the most important, because the means of communication is extremely subtle, it is unlikely to encounter the enemy's attack, thus it doesn’t require high robustness. But to ensure the safety of data, on the contrary, all kinds of confidential data at any time is facing the danger of being stolen and tampered with, so the robustness is very important, the hidden requirements on the quantity of the data.

References:


