International Journal of Security and Its Applications
Vol. 9, No. 3 (2015), pp. 319-334
http://dx.doi.org/10.14257/ijsia.2015.9.3.24

Monoecism Algorithm in the Application of E-commerce Information Security

Qingjie Zhang, Jianming Zhu, Xiaoxu Wang and Yapan Li

School of Information
Central University of Finance and Economics
Beijing, P. R. China 100081
E-mail: cufe_dbzy@163.com

Abstract

With the development of e-commerce industry, the security of business information has attracted a lot of attention. The paper [1] puts forward the monoecism watermarking algorithm. The algorithm divides image into two parts: ROI (Region of interest) and RONI (Region Of Non Interest), and respectively deal with the two parts. Female watermark and male watermark are embedded into the RONI at the same time, and generate embedding watermark of the image. As is known to all, the integrity of ROI is also very important in e-commerce. This paper tries to apply the monoecism watermarking algorithm to e-commerce information security. The author gives six applications of the algorithm in electronic commerce that is graphical physical paper, electronic paper anti-counterfeiting, electronic seal, copyright protection, digital fingerprint generation, secure communication protection. This author introduced the embedding watermark and extracting watermark process and detection process of monoecism watermark algorithm. Through the analysis of simulation experiment of six application fields of monoecism watermark algorithm in the e-commerce information security, the simulation experiment has verified the validity of the algorithm. In a word, this paper has discussed the general rules of selecting ROI and the specific rules of selecting ROI in e-commerce applications. The simulation results are given, and the satisfactory results have been achieved.

Keywords: *female watermark, male watermark, monoecism watermarking, e-commerce, information security*

1. Introduction

In recent years, great changes have taken place in people's consumption way, and e-commerce industry is developing rapidly. Potential threat hides in electronic business activities, such as order price tamper, fake electronic invoice, thievery of intellectual property. In the process of flow of business information, information loss, tamper, duplicate information, and information change in the delivery order will lead to inconsistence in information transmitting and accessing between participating electronic trading parties, and result in the failure of the deal. Watermarking algorithm provides a new train of thought to solve the problem of the information security of e-commerce.

Now, the security threats about e-commerce mainly include business information interception and steal, malicious tampering and forgery of business information, trading denial behavior. The security threats bring the immeasurable loss for the providers and users of e-commerce. In addition, e-commerce activities will produce a large number of electronic files, such as electronic checks, electronic contracts and electronic seal, *etc*. These electronic

ISSN: 1738-9976 IJSIA

documents are faced with various security challenges in the process of network transmission. Because a receiver of electronic file cannot guarantee no change in the process of transmission of the documents contents, so we can't determine the authenticity of documents. At the same time, receiver cannot be sure the identity of the transfer [13].

For e-commerce security, the traditional solution is to use encryption technology. It based on the theory of the cryptography. Through controlling access to the electronic encryption file, illegal user cannot unscramble the ciphertext, in order to ensure the authenticity and integrity of the file contents.

Although encryption technology can solve the problem of security transmission and access control, but once the file content is decrypted, its protective effect also disappears. The electronic information without secret key protection will be vulnerable to illegal attacks. It could face the risk of randomly copied and spread. In addition, the encryption technology has a fatal flaw that is special remind illegal users what are the important information. In the process of transport, storage cipher is easy to attract the attention of the attacker and making illegal users more clear the targets. It greatly increases the possibility of deciphering a ciphertext.

In order to improve the security strength of the encryption algorithm, the length of key was increased. But with the processing power improvement of modern computer, this method will become more and more insecure.

The information security technology in the past is network security technology or cryptography. From the perspective of communication and transport, network security technology is the breakthrough point to solve the problem of e-commerce security; The password techniques are more focused on the protection of the file itself. Even if the password techniques are classic, modern computer has enough computing power to break the conventional password rules. With the popularity of cryptography and hacker attacks, using the password techniques to ensure the safety of the e-commerce is more and more out of puff. Digital watermarking technology as an effective way to digital product safety certification has attracted great attention at home and abroad in recent years. Because of its robustness, security, and invisibility, digital watermarking technology plays an important role in the field of e-commerce. Now, digital watermarking technology has been widely used in the certification of authenticity and copyright protection, security communications, and other fields.

Encryption is one of the main traditional technology in the field of information security technology, and it is a technology based on the shannon information theory and the cryptography theory. The existing digital content protection uses encryption methods to do more, so as to achieve the purpose of copyright protection and information security. But this does not completely solve the problem: on the one hand, the encrypted file prevents the transmission of multimedia information; On the other hand, multimedia information encrypted is easy to cause the attacker's curiosity and attention, and there is the possibility of cracking. Cryptography can only protect the contents of the transmission, and once the content is decrypted, it will no longer have a protective effect. Digital watermark technology is a kind of new technology in the open network environment for the copyright protection, the authentication source and the integrity.

The earliest digital watermark is embedded in the view picture carrier. But in the whole image, embedded watermark has influenced the quality of the image. For example, the part changes of the medical image will affect the doctor's diagnosis. In order to improve this situation, people proposed watermark technology based on RONI (region of non interest). In this way, the image is divided into region of interest (ROI) and region of non interest (RONI). The watermark is embedded into RONI, and ROI is full reserved.

Akiyoshi [4] use progressive coding algorithm. The signature image is compressed, and the most important information is embedded into the bit plane closest to the ROI.

Siau [5] divide image into two parts: ROI and RONI, and respectively deal with the two parts. The information of each block of ROI embeds into the corresponding RONI block.

Qingjie, *et al.*, [1] present monoecism watermark algorithm based on RONI. Combining the female watermark with ROI, the male watermark is generated. Female watermark and male watermark are embedded into the RONI at the same time, and generate embedding watermark of the image. Female watermark and male watermark are embedded into RONI at the same time. So watermarked image is generated for detecting the image credibility, and it is necessary to extract the female watermark, male watermark and ROI of the image to detect. Monoecism watermark algorithm can effectively ensure the integrity and authenticity of the ROI. As long as ROI is under attack, it can be detected.

In order to judge the reliability of the watermark algorithm, watermarked image distortion situation is usually evaluated by the image signal-to-noise ratio PSNR and the mean square error MSE, [3, 4, 9-11]; It can also through the analysis, positioning and detection efficiency of the invisibility of signature image to evaluate the accuracy of watermark algorithm, including the miss rate, the rate of false positives, *etc.* [7].

Yiwei Sun [2] put forwards digital signature technology improvement ideas and implementation model based on the combination of digital encryption and information hiding. The method emphasizes the ciphertext hidden transmission, rather than pay attention to detecting integrity of the hidden information. Youan Xiao, *et al.*, [6] put forward a new kind of electronic signature technology. This method establishes correlation between electronic seal and electronic document, and put the summary of document as the watermark embedded seal image. The watermark information is text information. Xiangwei Kong *etc.*, [8] put forward the copyright protection system for digital works based on the digital watermark, and the technology of concrete method is not involved.

Someone puts forward a method by using visual electronic seal to ensure the effectiveness of electronic files, such as the electronic contract and its legitimacy. But at present the application of electronic seal pattern usually is to insert a seal image in the electronic file, and adds passwords to control the image. Due to the password in algorithm design unable to overcome the weakness of intensity, thus this method cannot achieve file non-repudiation. And this method has no complex functions, such as file tracking. Therefore, many researchers put forward the digital watermarking technology, and use it to solve information security problems of e-commerce. [15-19]

Taking into consideration of the e-commercee information security, there are also many images need to specially pay attention to, especially protect the integrity of information. Therefore, this paper tries to apply monoecism watermarking algorithm to the e-commerce information security. Monoecism watermark algorithm can ensure the important information without interference, so as to verify the integrity of the business information and provide security for e-commerce activities.

Watermarking technology can be classified by the characteristics, load media, detection process, content, hidden location, purpose, etc. According to the purpose of the watermarking, digital watermarking can be divided into ticket anti-counterfeiting watermark, copyright protection watermark, tampering with prompt watermark and hidden logo watermark [12]. New purpose are still found in continuously. This paper will discuss six aspects about the image in the e-commerce activities, such as the graphical physical paper, electronic paper anti-counterfeiting, electronic seal, copyright protection, digital fingerprint generation, and secure communication.

The six aspects of image information contain some important information, and one of the main advantages of monoecism watermark algorithm is to give special attention to important information, to protect the integrity of important information. Hence, this paper will analyze monoecism watermark algorithm in the application of e-commerce information security from the six aspects.

2. Monoecism Watermarking Algorithm

2.1. Conceptual Framework

Several basic concepts will be used in monoecism watermark algorithm: female watermark, male watermark and monoecism watermark.

2.1.1 Female Watermark: In monoecism watermark algorithm, we refer to the original watermark signal as the female watermark, recorded as FWM (Female WaterMark).

2.1.2. Male Watermark: Corresponding to female watermark, it is male watermark. By transforming the Female Watermark (FWM) and ROI, watermark signal is generated, which is called Male Watermark (MWM). That is, MWM = f (FWM, ROI), as MWM (Male WaterMark). Among them, the f is transformation rules. In this article, transformation function f is XOR $\oplus$.

2.1.3. Monoecism Watermarking: The process which female watermark and male watermark are embedded into the carrier image at the same time is called monoecism watermarking.

2.2. Watermark Embedded Algorithm

Figure 1 and Figure 2 give a simplified model of monoecism algorithm respectively. This model ignores encryption keys when the watermark are embedded and extracted.

Specific watermark embedded process is as follows:

First, the original carrier image is read. Suppose the original carrier image is RGB color model. The region of interest is recorded as ROI. The Region Of Non Interest is recorded as RONI. Users can choose ROI according to their needs.

Second, the watermark image is read. The watermark image is called the female watermark, recorded as FWM; Transforming Female watermark (FWM) and ROI, male watermark (MWM) is generated. That is, MWM = f (FWM, ROI).

The original image is divided into some image blocks. The image blocks are not covered each other. Then each pixel block whether is in RONI is decided. If it is true, then the discrete cosine transform is done for the block. An element of watermark image is DCT coefficient of low frequency embedded in the image block. Finally to watermarked image block for inverse discrete cosine transform, this completed a watermark embedding. If it is in the interior of the ROI, then skipping the image block, we can determine the next image block.

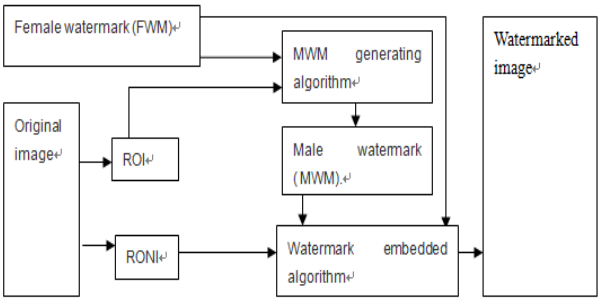

Figure 1. The Watermark Embedding Process

2.3. Watermark Extraction Algorithm

Watermark extraction algorithm is the inverse operation of watermark embedding process. The algorithm still needs to judge each non-overlapping pixels block: If the pixel block is outside of ROI, the corresponding block are respectively extracted from the watermarked image on the discrete cosine transform, and according to the result of operation watermark information can be recovered; If the pixel block is in the interior of the ROI, then the block is skipped, and the next image block will be determined.

2.4. Validity Check

Before the validity check, corresponding watermark signal needs to be extracted from the image. Using the watermark detection algorithm, we can extract female watermark and male watermark from the RONI of the detected image respectively, recorded as FWM' and MWM'. There are three ways to judge whether the image credible, this paper only uses first detection method.

The FWM' and ROI of the watermarked image (ROI') is transformed to generate male watermark (MWM") .That is MWM" = f (FWM', ROI'). Male watermark' (MWM') and male watermark" (MWM") are compared. If MWM' and MWM" are same, then the image is credible; If MWM' and MWM" are different, then the image isn't credible [1].

Watermark extraction and image reliability test process is shown in Figure 2.

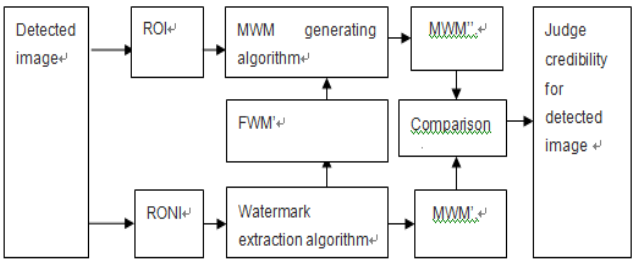

Figure 2. Watermark Extraction and Image Reliability Test Process

3. Applicability of Monoecism Algorithm in E-commerce Information Security

3.1. Characteristics of Monoecism Algorithm

Monoecism algorithm based on RONI is designed for medical image processing. This algorithm has the following features:

1) The algorithm embeds the watermark image into RONI, namely the quality of image ROI is not affected by the presence of the watermark, to ensure the integrity of the ROI.
2) The algorithm can not only detect the attack and tamper with RONI, but also can detect the attack and tamper with ROI. This is a big advantage of this algorithm.

Anyhow, monoecism watermark algorithm can solve the contradiction between image quality and ROI integrity control. For image quality and integrity of the ROI, this algorithm gives the same attention.

3.2. Applicability

Considering that graphical data storage and transmission, the information safety protection in many e-commerce activities are crucial to ensure e-commerce activities smoothly. Graphical data includes some important data, and some data are relatively unimportant. For example, the source of the funds and whereabouts are important data. Important part of data can be defined as ROI. Other data is defined as RONI. Monoecism algorithm is applied to the e-commerce information security, and important data can be given special attention and protection.

Therefore, monoecism algorithm is applied in the field of e-commerce information security, which is different from the traditional practice of watermarking on the whole image. It provides a new thought and method for the information security in e-commerce.

3.3. Application Fields

Monoecism algorithm in the application of e-commerce information security including: graphical physical paper, electronic paper anti-counterfeiting, electronic seal, copyright protection, digital fingerprint generation, secure communication. Monoecism algorithm is applied to the six aspects. It also faces the question how to determine the ROI of the image. The next section will discuss the rules of selecting ROI in detail.

4. Rules of Selecting ROI

4.1. General Rules

RONI method of digital watermark is mainly used in medical image processing. ROI refers to sensitive data of medical images, such as lesions reflected in image. Now monoecism algorithm is introduced into e-commerce information security field, and selecting ROI should follow the three rules:

4.1.1. Selecting ROI Should Combine with Domain Knowledge;

4.1.2. Selected ROI Should be the Very Important Data Area in the Image, Which is More Likely to be Tampered.

4.1.3. The Selected ROI Should be Smaller than the RONI.

4.2. Specific Rules

According to the general rule, the following rules of selecting ROI for monoecism algorithm are given in the application of e-commerce.

4.2.1. Selecting ROI for the Graphical Physical Paper: Graphical physical paper can be divided into three categories: promissory notes, checks and drafts. Generally speaking, the

source of the funds and whereabouts are the core content, because it is related to the flow of capital risk. For bank acceptance, however, the acceptor is the bank, so the source of money is reliable. There is no acceptance risk problem. So, key information of the whole paper is only a payee account. The payee account shows the money whereabouts. For payee account, bank determines which account to accept the money. Once there was an error, it will bring trouble to both sides of bank and the payee. So the information becomes the main tampering goal of the attackers. In order to prevent account information, the payee account location should be defined as ROI. As shown in Figure 3. (a)

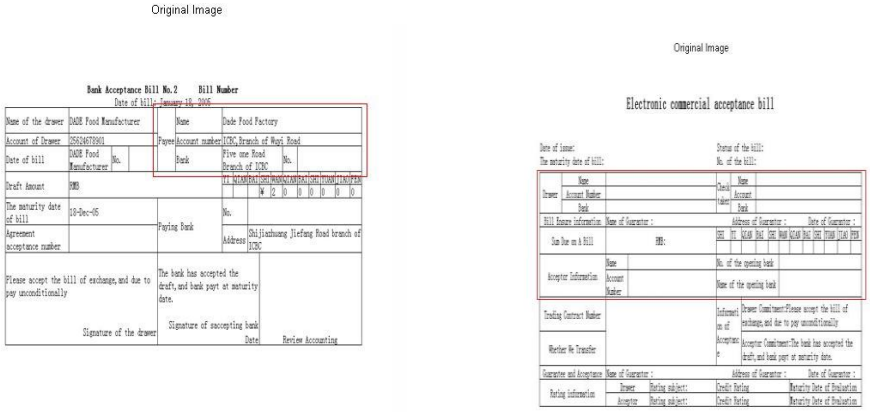

Figure 3. (a) The Original Bank Acceptance Bill (b) The Original E-commerce Acceptance Bills

4.2.2. Selecting ROI for Electronic Paper Anti-counterfeiting: Electronic paper is a kind of bills in order to meet the needs of the market. It has the same information with the traditional paper bill. E-commercial acceptance bills, for example, the source of the funds and the whereabouts is still the most key content, which embodies in the drawer information bar. For e-commercial acceptance bills, the drawer information, the acceptor information and the amount of the instrument should be defined as ROI. As shown in Figure 3(b).

4.2.3. Selecting ROI for Electronic Seal: Electronic seal is divided into visible seal and invisible seal. Visible electronic seals show the effectiveness of signed documents and the integrity. The authenticity of electronic seal directly determines the credibility of the file. Only real and effective seal has the force of law, thus for visible electronic seal, protecting seal originality is a vital problem. Based on the above reason, seal image should be as ROI. As shown in Figure 4(a).

Invisible electronic seal technology is to put the seal image itself as a watermark embedded into the electronic file. For the type of application, verifying the validity of the file is a key problem. Only the real file can display the seal image properly. ROI can be selected as the important data section of the file. The important degree of each part can also be randomly selected. As shown in Figure 4(b).

Figure 4. (a) The Original Seal Documents (b) The Original Announcement File

4.2.4. Selecting ROI for Copyright Protection: In order to ensure the digital works presented in the form of original, the most colorful or the most iconic place of work can be chosen for ROI, while the watermark image should be embedded into other section. In this experiment, a flash effects works is as a carrier image. It can be seen that the image has three very obvious bright spots. The red flare part can be selected as ROI. As shown in Figure 5(a).

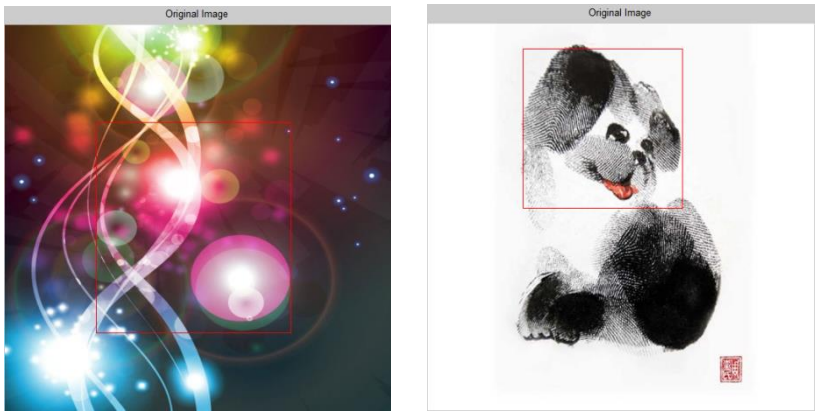

Figure 5. (a)The Original Flash Digital Works (b) The Original Digital Works Image

4.2.5. Selecting ROI for Digital Fingerprint Generation: Digital fingerprint can be a digital works ID number or serial number. It is used to determine the source of the digital works, in the form of the watermark itself. Digital fingerprint generation process is actually the watermark embedding process. The representative area of the digital works can be chosen as ROI. As shown in Figure 5(b).

4.2.6. Selecting ROI for Secure Communication Protection: The core of secure communication is hiding secret information without trace in the carrier image. By the carrier image, the information can be successfully delivered to the receiver. The only requirement is that the embedding position has high concealment, so the information can be transmitted to the destination safely. In order to achieve this goal, we deliberately chose a flower image. In this image, the white flowers are shark contrast to green leaves around them. According to the sensitivity of the human eye to color and common sense, white flowers in the centre of the

image is the focus of the whole image, which is the most eye-catching place. On the contrary, due to the large area of green leaf, the color of leaf is similar and easy to be overlooked, which provide the best location for information hiding. Therefore, white flowers in the middle of the image can be selected as ROI, while the other parts are selected as RONI of the watermark algorithm. As shown in Figure 6.

Figure 6. The Original Carrier Image

5. Simulation and Evaluation

This section introduces simulation experiment of six application fields of monoecism watermark algorithm in the e-commerce information security. The simulation experiment has verified the validity of the algorithm.

5.1. Simulation Settings

The simulation experiment used MALAB software, to test the ROI quality of watermarked image, and its detection ability to be tampered with.

5.1.1. Experimental Environment: Hardware environment: Intel (R) Core (TM) 2 Duo CPU P6700 @2.53GHz 783MHz, 2.98GB memory.

Software environment: Operating system: Windows 7.

Simulation software: MATLAB Version 7.4.0.287 (R2007a)

Experimental data: the original images have seven images that respectively from six aspects: the graphical physical paper, electronic paper anti-counterfeiting, electronic seal, copyright protection, digital fingerprint generation, secure communication. As shown in Figure 3 to Figure 6.

Considering the intercommunity of monoecism algorithm applied to the graphical physical paper, electronic paper anti-counterfeiting, electronic seal, copyright protection, digital fingerprint generation and secure communication, as well as restriction of the article length, here the original watermark image are only given both the visible seal document and secure communication carrier, namely female watermark. As shown in Figure 7.

Figure 7. (a) FWM Embedded into Visible Seal Document (b) FWM Embedded Secure Communication Carrier

5.1.2. Experimental Contents

The ROI of the original image is selected, and the corresponding male watermark is generated.

The male watermark and female watermark respectively are embedded into the corresponding original image at the same time. The watermarked images are generated.

Artificially tampering with watermarked image respectively, testing the effectiveness of the detection.

Then decide the credibility of the watermarked image.

5.2. Experimentation

The red rectangular box is respectively ROI of the original image, as shown in Figure 3 to Figure 6.

The corresponding male watermark is generated, as shown in Figure 8

Figure 8. (a) Male Watermark (Visible Seal) (b) Male Watermark (Secure Communication)

The watermarked images are as shown in Figure 9(a) and Figure 9(b)

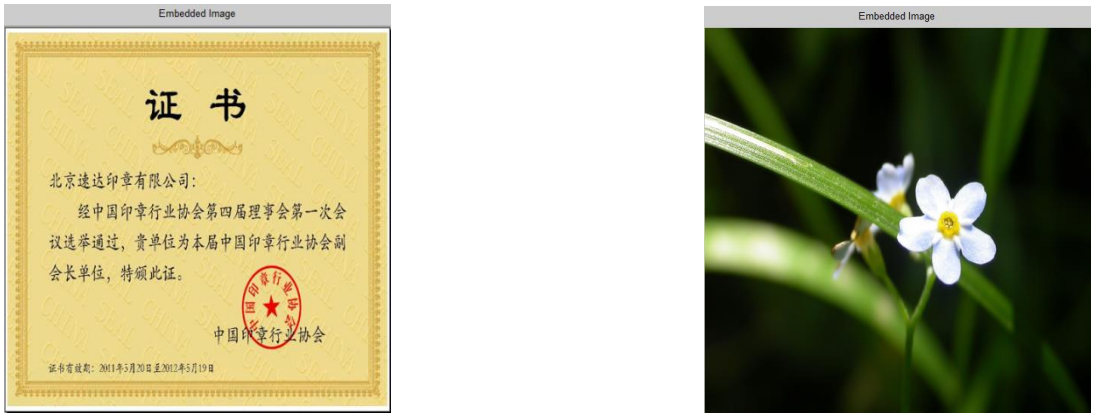

Figure 9. (a) Watermarked File (Visible Seal) (b) Watermarked File (Secure Communication)

Tampering with watermarked image, such as changing the payee account of the bank acceptance, seals, secure communication carrier, *etc.* The images tampered with, as shown in Figure 10 (a) and Figure 10 (b).

Figure 10. (a) The Image Tampered with (Visible Seal) (b) The Image Tampered with (Secure Communication)

The female watermark (FWM') and the male watermark (MWM') are respectively extracted from the detected image. Because of the female watermark (FWM') and male watermark (MWM') extracted from the Figure 10(a) are consistent with Figure 8(a) and Figure 8(b), so this article is no longer shown. The female watermark (FWM') and the male watermark (MWM') extracted from Figure 10(b) are respectively as shown in Figure 11(a) and shown in Figure 11(b).

Figure 11. (a) (FWM') Extracted from the Tampered Image (b) (MWM') Extracted from the Tampered Image

Using the extracted female watermark (FWM') and the ROI of detected image, we can generate male watermark (MWM''). The male watermarks (MWM'') are respectively generated as shown in Figure 12.

Figure 12. MWM'' Generated of Using (FWM') and the Detected ROI

5.3. Experimental Results

Simulation experiments show that, when the detected images are not tampered with, result is reliable. And when the detected images are tampered with, the detection results are

incredible. Watermark signal has no effect on ROI. This ensured the ROI quality of the image. Details are shown in Table 1.

Table 1. The Simulation Results

serial number	application fields	Area of watermark embedded	Method of embedding watermark	watermark signal whether ROI affected by	Whether the detected image is tampered with	The detected image whether is credible
1-7	All six applications	RONI	DCT (discrete cosine transform)	no	no	credible
		RONI	DCT (discrete cosine transform)	no	yes	incredible

5.4. Experimental Results Analysis

5.4.1. Effectiveness: From the experiment, monoecism watermark algorithm can not only detect change of ROI, but also detect the change of RONI embedded watermark. The experimental results show that the monoecism watermark can safely protect graphical physical paper, electronic paper, electronic seal, digital fingerprinting, copyright protection and secure communications. This can illustrate monoecism watermark algorithm is effective.

5.4.2. Invisibility of Watermark: As can be seen from the experimental images, from the bank acceptance image embedded watermark to secure communication carrier image embedded watermark, the image quality didn't fall in the case of watermark embedding. We cannot identify the location of the watermark by the eye alone. The watermark is invisible.

5.4.3. Security: Monoecism watermark algorithm has high security. Embedded watermark is divided into two parts, the female watermark and male watermark. There is a strong correlation between them. Unauthorized people can't copy watermark, and also can't extract the information carried by watermark. So watermark is unlikely to be forged. It can ensure the security of algorithm

5.4.4. Applicability: From the experimental results and analysis, monoecism watermark algorithm is as a digital watermarking technique based on RONI. This approach will divide graphical physical paper into two parts, important area (ROI) and unimportant area (RONI). Division of important area can maximally protect the sensitive data from the watermark interference. Monoecism watermark can provide reliable security performance, uniqueness of security products, automatic detection function and low cost four conditions. It aims to provide electronic paper anti-counterfeiting technology. Monoecism watermark method can provide good service for electronic paper anti-counterfeiting.

As can be seen from the experiment, the seal image as an important area can ensure it will not damaged by the embedded watermark. The experimental results also explain that the monoecism watermark algorithm can be used to identify the file authenticity. Monoecism watermark algorithm provides a new technical support for invisible seal. Seal image is no longer single image information. Seal image and the male watermark generated by seal image constitute the file protection barriers.

Watermark technology which has the function of copyright protection should not only have the general characteristics of information hiding technology, but also its inherent characteristics, including invisibility, safety and certainty. As a watermark technology, monoecism watermark method has good ability of information hiding. By adjusting the size

of the pixel block in the RONI, the watermark capacity has been greatly improved. Using monoecism watermark method to protect copyright has fairly strong invisibility. Monoecism watermark algorithm meets all the conditions required for copyright protection.

The watermark applied in the digital fingerprint can locate the digital works, to distinguish the tagged digital document and stolen reproductions. For this application, watermark not only need strong robustness, but also can resist malicious erasure or forging. Monoecism watermark method built a good platform for digital fingerprint generation. It has more watermark space than the average watermark technology. Monoecism watermark creates favorable conditions for the formation of digital fingerprint. When we need to identify information, we can read the hidden fingerprint information to help track the source of the product through the special reading program.

Monoecism watermark method is used to put the secret information hidden in the image in the form of watermark. Receiver extracts the watermark signal from the file through the watermark detection algorithm, and complete message transfer. Monoecism watermark algorithm also meets the requirements of secure communication.

We may draw a conclusion: as a kind of innovative watermark technology, monoecism watermark algorithm has good applicability in graphical physical paper, electronic paper anti-counterfeiting, electronic seal generation, digital fingerprint generation, copyright protection and secure communication.

6. Superiority

The traditional watermark technology applied to the e-commerce embed watermark signal in the carrier image. But embedding watermark in the whole image, it do not highlight the protection of important information, at the same time watermark image interfere with important information. Simple watermark embedding method is easy to be cracked. Aiming at the shortcomings, the use of monoecism watermark method to protect e-commerce information security has the following advantages:

6.1. Highlight Safety Protection of Important Information

This paper introduces RONI technology which is mainly used in medical images safety protection to e-commerce information security area. Compared with traditional watermark algorithm, monoecism watermark method pays more emphasis on the protection of ROI information.

6.2. Improve Security

Monoecism watermarking algorithm has high security. Embedded watermark is divided into two parts：the female watermark and male watermark. There is a strong correlation between them. Unauthorized people can't copy watermark, and also can't extract the information carried by watermark. To judge the authenticity of electronic bills need to follow two conditions: First, complete female watermark and male watermark can be extracted from the electronic bills; Second, the new male watermark (MWM") generated by male watermark (FWM') and ROI must be completely consistent with the extracted male watermark (MWM') . In this paper electronic papers which only satisfy the two conditions at the same time can be considered to be true. As long as there is one condition that paper can't conform to, the source of the paper is questionable.

6.3. Expand the Watermark Capacity

RONI technology still only embeds a watermark signal each time. The watermark capacity is small, so the ability of the image to hide information is limited. To store more effective information, on the design of experiment, the corresponding adjustment to the size of RONI pixel block was made. It made full use of the non important area of the image, and embedded as much as possible authentication information within the limited space. Watermark capacity has been fully extended.

6.4. Improve the Efficiency of Extraction and Detection

To supplement the traditional watermarking techniques, monoecism watermark algorithm is a leap in RONI technology. It divides the RONI into several parts. That is, different watermark signal corresponds to different embedding position, and there is the certain corresponding relationship between the two. Therefore, when we extract the watermark, we just need to apply the watermark extraction algorithm to the specific areas without traversing the whole image, greatly improving the efficiency of extraction and detection.

7. Summary

Monoecism watermark algorithm pay attention to the protection of important information. This paper combined the advantages of monoecism watermark algorithm with the characteristics of e-commerce graphic information, and applied monoecism watermark algorithm in e-commerce information security. This paper discussed the monoecism watermark algorithm in the application of the e-commerce information security from six aspects, including graphical physical paper security protection, electronic paper anti-counterfeiting, electronic seal generated, copyright protection, digital fingerprint generation and secure communication. This paper introduced the embedding watermark and extracting watermark process and detection process of monoecism watermark algorithm, and elaborated the general and specific rules to select ROI.

Through the simulation experiment, it was validated that the effectiveness of the monoecism watermark algorithm applied in the e-commerce information security. Experimental results showed that monoecism watermark algorithm can ensure that the ROI of carrier image without the watermark signal interference. It can provide effective protection for the e-commerce information security.

Digital watermarking technique is applied to e-commerce information security, but there are many issues need to be researched. Our future research tasks are to apply monoecism algorithm to the protection of the text information, as well as the database data protection.

ACKNOWLEDGEMENTS

This research is supported by National Natural Science Foundation of China (Grant No. 61272398, 61273293).

References

[1] Q. Zhang, J. Zhu and X. Wang, “Monoecism Watermarking Algorithm”, The International Symposium on Parallel Architectures, Algorithms and Programming (PAAP’12), **(2012)**, pp. 52-59.
[2] Y. Sun and W. Yang,” Research on information hiding in the digital signature, Journal of UEST of China, vol. 38, no. 1, **(2009)** November, pp. 49-52.
[3] J. Li, W. Du, Y. Bai and Y.-W. Chen, “3D-DCT Based Zero-Watermarking for Medical Volume Data Robust to Geometrical Attacks”, Proceeding of the First International Conference on Wireless Communications and Applications, **(2011)**.

[4] A. Wakatani, "Digital Watermarking for ROI Medical Images by Using Compressed Signature Image", System Sciences, **(2012)**, pp. 2043-2048.
[5] S.-C. Liew, S.-W. Liew and J. M. Zain, "Reversible Medical Image Watermarking for Tamper Detection and Recovery With Run Length Encoding Compression", Computer Science and Information Technology (ICCSIT), vol. 5, **(2010)**, pp. 417-420.
[6] Y. Xiao and J. Liu," A new type of electronic signature technology", Journal of wuhan university of science and technology, vol. 31, no. 13, **(2009)** July, pp. 123-126.
[7] I. F. Kallel, M. S. Bouhlel and J.-C. Lapayre, "Improved Tian's Method for Medical Image Reversible Watermarking", Graphics, Vision and Image Processing (GVIP), vol. 7, **(2007)**.
[8] X. Kong, D. Yangm and X. Hu," copyright protection of digital watermarking and digital products", Management of marketing resource center, http://www.mmrc.net.
[9] A. Giakoumaki, S. Pavlopoulos and D. Koutsouris, "Secure and Efficient Health Data Management Through Multiple Watermarking on Medical Images", Medical and Biological Engineering and Computing, vol. 44, no. 8, **(2006)**, pp. 619-631.
[10] M. Li, S. Narayanan and R. Poovendran, "Tracing Medical Images Using Multi-Band Watermarks", Engineering in Medicine and Biology Society, vol. 2, **(2004)**, pp. 3233-3236.
[11] K. A. Navas, M. Sasikumar and S. Sreevidya, "A Benchmark for Medical Image Watermarking", System, Signals and Image Processing, **(2007)**, pp. 237-240.
[12] http://baike.baidu.com/view/39205.htm.
[13] X. Chen, "Digital watermarking technology application in the field of e-commercee", Journal of fujian financial management cadre institute, no. 2, **(2008)**, pp. 50-53.
[14] X. Zhao, "Digital watermarking technology and its application in e-commercee", Communication and broadcasting television, no. 4, **(2002)**, pp. 37-43.
[15] L. Zhou and L. W. Y. Zhang, "e-commercee security and digital watermarking technology analysed", DA ZHONG KE JI, (Cumulatively No.115), no. 3, **(2009)**, pp. 15-16.
[16] H. Huanng, "e-commercee data security model based on digital watermark", Journal of shandong province agricultural management cadre institute, no. 4, **(2009)**, pp. 164-165.
[17] Q. LI, "Application of digital watermarking in e-commercee" Journal of hebei academy of sciences, no. 3, **(2007)** pp. 27-30.
[18] W. Sheng, "Digital watermarking technology in the application of the electronic ticketing", Journal of Qingdao Technological University, vol. 28, no.6, **(2007)**, pp. 89-92.
[19] D. Ying and B. Li, "Copyright protection of digital image products and tracking In e-commerce using digital watermark", Journal of sichuan university (engineering science), vol. 36, no. 5, **(2004)**, pp. 103-107.

Authors

Qingjie Zhang, Associate professor, School of Information, Central University of Finance and Economics, China

Jianming Zhu, Professor, School of Information, Central University of Finance and Economics, China

Xiaoxu Wang, Yapan Li, Graduate student, School of Information, Central University of Finance and Economics, China.