EFFICIENT BAR-CODE WATERMARK SYSTEM TO PROTECT AGRICULTURAL PRODUCTS INFORMATION AND COPYRIGHT

Lin Deng[1,*], Xiaoming Wen[2]

[1] *China Patent Information Center, State Intellectual Property Office of P.R.China, Beijing, P. R. China, 100088*

[2] *Shandong University Library , Jinan , Shandong Province, P. R. China, 250100*

[*] *Corresponding author, Address: Hui Zhong Bei Li 116-1-401, Chao Yang District, Beijing, P.R.China, 100012, Tel: +86-13439892596, Email: denglin1021@hotmail.com*

Abstract: In order to protect agricultural product information and copyright, this paper proposes an efficient bar-code watermark system with digital signature. The proposed system adopts digital signature to prevent a buyer from unauthorized copies and to prevent a seller from forged unauthorized copies. The proposed system also encodes the signature with bar-code and embeds the bar-code image into the original image. As long as the similarity of watermark extracts from the damaged image over a threshold, the signature can be fully recovered. It is a novel idea to bring the bar-code concept into watermark system to protect agricultural product information and copyright. Detailed simulation results show that the proposed system gets much better results than that with error correcting code scheme, and prove that the proposed system can protect agricultural product information and copyright effectively.

Keywords: bar-code, digital signature, agricultural product, copyright protection

1. INTRODUCTION

At the global level, significant progress has been made towards improved agricultural product safety and information (Fernando, et al. 2006; Clark, et al. 2005). Since then, world gross agricultural production has grown. In order to manage agricultural production effectively, many efforts have been made, such as the scheme (N., et al. 2008; Konde, et al. 2005; Anon, 2005) for information and its management for differentiation of agricultural products, and a knowledge-based intelligent e-commerce system for selling agricultural products called KIES (W., et al. 2007; Kresic, 2005; Buf, 2007). The KIES system not only provides agricultural products sales, financial analysis and sales forecasting, but also provides feasible solutions or actions based on the results of rule-based reasoning. The authors proposed a method of adopting a bar code technology which is successfully applied to a production processing information management of a grocery enterprise (X., et al. 2007). The method can real-timely be analyzed the devotion, the output and wearing off of the original materiel, burden, equipment and manpower, and the individual client cost and individual product cost by the management systems. The cryptography and the digital watermark have begun to attract more attention from the agricultural field along with the rapid growth of the Internet and electronic businesses. Robust watermark can be seen as a mean for the declaration of copyright (S. et al., 1998; R., et al., 2007), and at the same time offers a way to hide data safely. Bar code technology has widely been applied in materiel management of production processing (X. et al., 2007; R., et al., 2007), however, such schemes did not consider protecting agricultural product information and copyright.

In this paper, we show how digital signature protects agricultural product information and copyright traded in the Internet. Copyright protection is known to be a buyer-seller problem (Nasir, et al. 2001) and must meet the three following requirements. First, when we find an unauthorized copy image, we should be able to detect where the original source comes. Second, the message embedded in the image should include buyer information that the seller has no access to. This will prevent the seller from making the signature himself. The last and the most important point is that the signature should be accessed to anyone to verify the validation, but not only to those who own special information. In our method, we encode a long message into a bar-code. The maximal length of the message in our simulation is 64 bytes. It is long enough for the inclusion of identification, the object name, the object number, the price, the timestamp, and so on. Another point that obviously differentiates the method introduced in the paper from those in other watermark references is that we use bar-codes to replace meaningful logos or random sequences. We find that bar-codes can sustain various kinds of attacks and therefore are much better than any other error correcting codes. This is very useful in recovering the damaged watermark.

2. PROPOSED METHOD

2.1 Bar-code scheme

The bar-code scheme is similar to that of code 39. We expand the number of lines to present each byte from nine to twelve. The twelve lines are composed of three bold black, three thin black, two bold white and four thin white lines. So there are 300 combinations and they are enough to express all ASCII codes and the remaining 44 combinations are reserved. Assumption a black line as a start line so that it will end with a white one. The bold line must be presented in two pixels and the thin one in one pixel. That is each byte will be presented in 17 pixels.

A bar-code scheme can not only declare the ownership but also can record various information that includes the buyer, the seller, the object for sale, the object price and so on. Because the bar-code is made follow some orders, we can recover the damaged bar-code image with some recovery rules so that the bar-code has high recoverability against various attacks.

The recover rules of the proposed bar-code scheme are listed below: According to the majority rule and the average gray level, we judge the line is black or white. By the assumption, the start line representing each byte is a black one and its ending line is a white one. When we judge the line is black or white, we record the error pixels of each line and the number of error pixels can be viewed as the severity of attack. If one line and its neighboring line are of the same color, we view these two lines as a bold line. We can check if there are three bold black, three thin black, two bold white and four thin white lines for each byte. If not, we change the color of the line that has the most error pixels until the number of bold and thin lines for each byte is correct. We group every twelve lines as a set for the bar code and map a set of twelve lines to an ASCII code. If we can not map it to any ACSII code, we mark this byte to be a '?' to indicate an error. Every Chinese character is denoted as two ASCII codes.

To show the high recoverability of the bar-code scheme we do several simulations. The original bar-code image and the damaged bar-code images of these simulations are shown in Table 1. We encode a trade message to be a bar-code image. We attack the bar-code images with several kinds of image processing. In the extraction process, we use the recovery rules described above to fix the damaged bar-code images and map the recovered bar-code images to corresponding characters.

The extracted messages and the number of error characters of these simulations are listed in Table 2. The trade message is: "Richard Marks=>Tom 张 2008/3/29 $2000". It means that the seller is Richard

Marks and the buyer is Tom Smith. The transaction of \$2000 is done in 2008/3/29. These simulations prove the high recoverability of the bar-code scheme. Ever if the damage is great enough to cause some errors, we can still retrieve the rest part of the trade message from the damaged bar-code image.

Table 1. Original bar-code image and damaged bar-code images.

Processing	Image
Original bar-code image	
100% uniform noise	
JPEG compression	
Sharpening	
100% uniform noise and blurring	
120% uniform noise	

Table 2. Extracted messages and number of error characters.

Processing	Similarity	Extracted message	Error
Original bar-code image	1.0	Richard Marks=>Tom 张 2008/3/29 \$2000	0
100% uniform noise	0.503	Richard Marks=>Tom 张 2008/3/29 \$2000	0
JPEG compression	0.595	Richard Marks=>Tom 张 2008/3/29 \$2000	0
Sharpening	1.0	Richard Marks=>Tom 张 2008/3/29 \$2000	0
100% uniform noise and blurring	0.0006	Richard Marks=>Tom 张 2008/3/29 \$2000	0
120% uniform noise	0.497	R?chard Marks=>?om 张 2008/3/29 \$2000	2

2.2 Verifying procedure

The proposed bar-code watermarking system is composed of three stages: the verifying procedure, the embedding procedure and the extraction procedure.

Suppose buyer B wants to buy an object from a seller A. He must make a trade message M which includes the buyer's name, the seller's name, the kinds of objects, the trade price and the trade date. The message is signed with B's private key and buyer B encrypts the signature with A's public key to avoid the message is known to the third party. Then he tells A who he is and transmits the cipher-text to A:

$$\begin{aligned} &B: M=ID_A||ID_B||Objects||Price||Date \\ &B: S=E_{Bs}(M) \qquad (1) \\ &B\rightarrow A:T=ID_B||E_{Ap}(S) \end{aligned}$$

where E_{Bs} means encrypt with B's private key.

When A receives the cipher-text from B, he can decrypt it to E_{Bs}(M) with his private key and decrypt E_{Bs}(M) to M with B's public key. So, he can confirm the content of the trade message. If the seller A accepts the deal, he calculates SHA-1(Bp) and concatenates it with E_{Bs}(M) to be the information encoded into a bar-code, otherwise the seller would reject the trade and notify the buyer.

A: S= EBs(M)=DAs(EAp(S))
A: M=DBp(EBs(M))
If A accepts the deal, (2)
A: I=SHA-1(Bp)||EBs(M);
Otherwise the trade is rejected.

2.3 2.3 Watermark embedding procedure

The second stage of the proposed bar-code watermarking system is the embedding procedure. We encode the information I to be a bar-code image. Each byte takes 17 pixels width of bar-code image. The default bar-code height is 21 pixels. So, the bar code image is a bitmap, whose size is 64*17 by 21, equal to 22848 pixels. We decompose the original image with 8*8 block Integer DCT and obtain 4096 blocks of 8*8 pixels from the images of 512*512 pixels. In our simulation, we hide 21 pixel height bar-code image into the 4096 blocks. In average, we must embed each pixel height bar-code image into every 195 block and give up the last one block. One pixel height bitmap includes 64*17=1088 bits. As a result the front 82 blocks out of 196 blocks should choose 5 positions to embed the watermark and the rest 113 blocks should choose 6 positions. We show the relationship in the equation (3) and (4).

$$\lfloor 4096/21 \rfloor = 195,\ 4096 \text{ mode } 21 = 1 \tag{3}$$

$$\lfloor (64*17)/195 \rfloor = 5,\ 64*17 \text{ mode } 195 = 113 \tag{4}$$

For the reason we want the watermark embedded algorithm can be public and the watermark still can maintain its robustness. We choose the embedded position according to the coefficients in the frequency domain and the seller's private key. Therefore, each image will have different embedded point list.

Suppose we want to choose five positions to embed the watermark each block. We sort the 63 AC terms by their absolute values in a descending order first. Then we pick out the top ten terms and encrypt them with A's private key. We sort the value after encryption in a descending order again. The five large ones are the positions where we want to embed the watermark.

Expression (5) is the watermarking equation.

$$\begin{cases} C_i^{'} = C_i(1+\alpha), if \quad W_i = 255 \\ C_i^{'} = C_i(1-\alpha), if \quad W_i = 0 \end{cases} \tag{5}$$

Where C_i is the original coefficient and $C_i^{'}$ is the embedded coefficient. W_i is a sequence of gray levels of bar-code bitmap composed of 0 and 255. α is an unfixed scaling factor varying with the DCT coefficients. The rule of adjusting a value is shown in equation (6).

$$\alpha = \begin{cases} 0.15, if \quad C_i > 35 \\ 0.3, if \quad C_i \in (20,35] \\ 0.6, if \quad C_i \in (10,20] \\ 0.8, if \quad C_i \in (5,10] \\ 0, C_i = C_i + 12, if \quad C_i < 5 \quad and \quad W_i = 255 \\ 0, C_i = C_i - 12, if \quad C_i < 5 \quad and \quad W_i = 0 \end{cases} \tag{6}$$

After watermark embedded, we do the inverse DCT to get a watermark embedded image.

2.4 Watermark embedding procedure

The third stage of the proposed bar-code watermarking system is the extraction procedure. In the embedding procedure, we decompose the original image by using the 8*8 block DCT. Then we choose the embedded positions according to the coefficients in the frequency domain and the seller's private key. In the extraction procedure, we use the same two steps to find the positions where the watermark is embedded.

Expression (7) denotes to retrieve the watermark sequences.

$$\begin{cases} T_i = C_i^{'} / C_i \\ If \quad T_i \le 1, W_i^{'} = 0 \\ If \quad T_i > 1, W_i^{'} = 255 \end{cases} \tag{7}$$

Where C_i is the original coefficient and $C_i^{'}$ is the watermarked image coefficient. $W_i^{'}$ is the extracted watermark sequence.

We use the watermark sequences gotten in (7) to reconstruct the bar-code image and fix the bar-code with the recovery rules describing in section 2.1. Then we translate the content of the recovered bar-code image into bytes. These bytes can be taken to compose an information which equals to SHA-1(Bp)||E_{Bs}(M). These steps are shown in Fig.1.

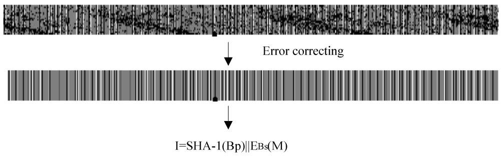

Fig.1: Steps of reconstructing bar-code and using to compose a signature

The decryption process is shown in expression (8). The information I can be clipped into two parts. The first part is SHA-1(Bp) and the second part is EBs(M). SHA-1(Bp) can help us quickly find the buyer in the masses of the buyers. And we can decrypt the cipher-text EBs(M) with B's public key to obtain the trade message M.

$$\begin{aligned}&I=\text{SHA-1}(Bp)\|EBs(M)\\&DBp(EBs(M))=M\\&M=IDA\|IDB\|Objects\|Money\|Date\end{aligned} \tag{8}$$

3. EXPERIMENT RESULTS

In the simulation, we encrypt a trade message with 1024-bits RSA [6] and confirm the ciphertext by both the buyer and the seller. Then we encode it as a signature with the buyer's private key. Then, the signature is encoded into a bar-code to be a watermark to embed in the original image. The embedded point list is decided by SHA-1 hash function with the seller's private key as a random seed. In the watermark detection, only the seller can extract the watermark because nobody has his private key. However, after the signature is extracted everyone can verify the message with the buyer's public key. So we can make certain who the real buyer and the real seller are. In this experiment, four 512*512 test images are used to be the original images. The trade message hided into each original image is different. We encode these messages to the bar-code images that are watermarks we will embed into the original images. The PSNR of the watermarked image is computed to show its image quality.

The similarity is to measure the degree of damage between the original bar-code watermark W and the extracted bar-code watermark W*. It equals to the number of pixels that are the same gray level between two bar-code watermarks divided by the number of total pixels. These image processing include JPEG compression, blurring, sharpening, uniform noise and cropping. We should define some keywords we will use lager. "Jpeg4" means that we do Jpeg compression with image quality level 4(low) to the image and "Jpeg6" means compressing with image quality level 6(medium). We should list the image sizes after compressing below the tables. "Noise5" means we add 5% uniform noise into the watermarked image and so on. The number of errors in the result table presents the different characters between the original trade message and the extracted message. The trade message we presuppose for the test image is: &Alice &Bob &2007\5\18 &4,000,000. When the ciplier text the seller receive from the buyer, the seller will decrypt the cipher text with B's public key and verify the trade message. If the message is correct, the seller produces the bar-code watermark image as shown in Fig.2.

Fig.2: Bar-code watermark image embedded in test images

The image quality, the extracted message and the number of errors of the test images are shown in Table 3 and Table 4.

Table 3. Experiment results of image “Scene”.

Processing	PSNR	Similarity	Extracted message	Error
WMKed	39.28	1	&John &K.J.陈&2007\6\1 &12,345	0
Jpeg6	34.68	0.921	&John &K.J 陈&2007\6\1 &12,345	0
Jpeg4	33.00	0.869	&John &K.J. 陈&2007\6\1 &12,345	0
Blur	35.41	0.755	?J??? ?K????? ???0??6??????,345	21
Sharpen	29.05	0.905	&John &K.J. 陈&2007\6\1 &12,345	0
Noise5	29.81	0.860	&John &K.J. 陈&2007\6\1 &12,345	0
Noise10	24.30	0.716	&John &K.J. 陈&200??6\1 &12,345	2
Crop0.25	10.49	0.739	&John &K.J. 陈&2007\6\1 &12,345	0

Table 4. Experiment results of image “Lena”.

Processing	PSNR	Similarity	Extracted message	Error
WMKed	39.08	1	&Catherine &Serlina &2007\6\11 &5,000	0
Jpeg6	36.53	0.942	&Catherine &Serlina &2007\6\11 &5,000	0
Jpeg4	35.11	0.870	&Cather??e &Serlina &2002\???1? &5,000	6
Blur	38.07	0.869	&Catherine &?erlina &?007\6\11 &5,000	2
Sharpen	31.16	0.955	&Catherine &Serlina &2007\6\11 &5,000	0
Noise5	29.93	0.861	&Catherine &Serlina &2007\6\11 &5,000	0
Noise10	24.31	0.718	&Ca??erine &Ser?ina &2007\6\11 &5,000	3
Crop0.25	11.64	0.726	&Catherine &Serlina &2007\6\11 &5,000	0

4. CONCLUSION

In this paper, we have successfully combined the applications of cryptology and watermark to protect agricultural product information and copyright traded in the Internet. Cryptography is used not only for choosing embedded positions but also for encrypting and decrypting to protect the trade messages. We use asymmetrical encryption algorithm, RSA, to avoid the buyer from distributing the unauthorized copies and to prevent the seller himself from generating the signature. This is the key point in protecting agricultural product information and copyright. The bar-code watermark also offers a high recoverability to against the damage caused by image processing. For the future studies, we will select another watermark embedding method to replace the integer DCT used in our study. The spatial distribution and the neighboring pixels will be taken into considerations to adjust the weights of embedding watermark. We believe that it may get better results to protect agricultural product information and copyright.

ACKNOWLEDGEMENTS

The authors would like to thank the anonymous reviewers for the invaluable comments that have significantly improved the paper quality.

REFERENCES

Anon. Water-efficient agriculture key to China's food supply security. International Water and Irrigation, 2005, 25(3): 44-46.

Buf J. M. H.. Improved grating and bar cell models in cortical area V1 and texture coding. Image and Vision Computing, 2007, 25(6): 873-882.

Clark J. Peter. Food plant security. Food Technology, 2005, 59(11): 66-68.

Fernando P. Carvalho. Agriculture, pesticides, food security and food safety. Environmental Science & Policy, 2006, 9(7): 685-692

Konde Victor. Industrial biotechnology applications for food security in Africa: Opportunities and challenges. International Journal of Biotechnology, 2005, 7(1): 95-112.

Kresic-Juric S. Edge detection in bar code signals corrupted by integrated time-varying speckle. Pattern Recognition, 2005, 38(12): 2483-2493.

N. Niederhausera, T. Oberthu, S. Kattnigb, et al. Information and its management for differentiation of agricultural products: The example of specialty coffee. Computers and Electronics in Agriculture, 2008, 61(2): 241-253

Nasir Memon, Ping Wah Wong. A Buyer-Seller Watermarking Protocol. IEEE Transactions on Image Processing, 2001, 10(4): 643-649

R. Rivest, A. Shamir, and L. Strawczynski. A method for Obtaining Digital Signature and Public-Key Cryptosystem. Communication of the ACM, 1978, 21(2)

R. Shams, P. Sadeghi. Bar Code Recognition in Highly Distorted and Low Resolution. IEEE International Conference on Images Acoustics, Speech and Signal Processing, 2007, 1: 737-740

S. Craver, N. Memon, B.L and M. M Yeung. Resolving rightful ownerships with invisible watermarking techniques: limitations, attacks, and implications. IEEE Journal of Selected Areas in Communications, 1998, 16(4): 573-586

W. Wen. A knowledge-based intelligent electronic commerce system for selling agricultural products. Computers and Electronics in Agriculture, 2007, 57(1): 33-46

X. Liu, C. Lin. Information Management System of Grocery Production Processing Based on a Bar Code Identification Technology. IEEE International Workshop on Anti-counterfeiting, Security, Identification, 2007, 164-168