IIETA International Information and Engineering Technology Association
Advancing the World of Information and Engineering

Traitement du Signal
Vol. 38, No. 1, February, 2021, pp. 127-133
Journal homepage: http://iieta.org/journals/ts

An Electronic Bill Encryption Algorithm Based on Multiple Watermark Encryption

Chuan Lin, Xinpeng Xu*

College of Finance and Economics, Sichuan International Studies University, Chongqing 400031, China

Corresponding Author Email: xinpengxu@cqu.edu.cn

https://doi.org/10.18280/ts.380113

Received: 25 November 2020
Accepted: 12 January 2021

Keywords:
digital image watermarking, multiple watermark encryption, electronic bill

ABSTRACT

Digital image watermarking can authenticate and protect images through image processing and cryptography. The encryption of digital watermarks helps to effectively improve the performance of digital watermarking, thereby meeting the needs of bill image authentication in the actual financial system. This paper firstly proposes a method to resist JPEG compression attack. The proposed method enhances the anti-attack ability of watermarks by constructing the wavelet coefficient matrix and binary sequence for chaotic encryption, and effectively improves the security of electronic bills in transmission. Considering the special needs of financial bills, the authors presented a method to detect the key information area of bills, and encrypt multiple watermarks. Application results show that the proposed method can identify and encrypt the key area of each bill, as well as detect and curb tampering and forgery, providing a guarantee to the security of financial bills.

1. INTRODUCTION

Data encryption is a key research field in information science. From the perspective of information security, data stealing and forging are the leading threats. Information authentication can effectively deal with these threats. One of the most important information authentication technologies is digital watermarking. By the principle of information hiding, digital watermarking embeds the watermark information into the target carrier, in a manner that embedded information cannot be detected by the naked eyes.

The watermark information could be destroyed through tampering and copying the carrier. This poses a growing risk to the authentication and protection of the carrier. During digital watermarking, special technology should be adopted to encrypt the watermark information, laying a solid basis for authentication. Information authentication based on digital watermarking has broad application prospects. It can effectively protect data security, especially in terms of tamper resistance.

The early watermarking algorithms for digital images mostly refer to spread spectrum communication, and transform the data from one domain to another. For example, the digital watermarking algorithm based on block discrete cosine transform (DCT) can embed binary information effectively, but it is too sensitive to geometric and multi-document attacks.

The encryption of electronic bills is a basic requirement in banking, finance, e-government, and other fields. Compared with traditional paper documents, electronic bills face high risks of leakage, tampering and forgery. To solve the problem, this paper introduces the tamper-proof digital watermarking information into electronic bills, and proposes an electronic bill encryption algorithm based on multiple watermark encryption.

2. LITERATURE REVIEW

Komatsu's review of digital watermarking [1] has aroused great interest of many researchers, and significantly promoted the development of this technology. Verma et al. [2] pointed out many shortcomings of the classical watermarking algorithm, especially the instability of the embedded watermark signal in the carrier image. Särkkä and Renshaw [3] embedded watermark information into the character space of the document, making the encryption algorithm more robust. Karthigaikumar and Baskaran [4] encoded and embedded the watermark information into the connected domain of binary image in the form of circles or strips, shedding new light on the watermarking of binary images.

Qin et al. [5] applied digital watermarking algorithm to JPEG compression, and enhanced the anti-compression ability of digital watermark algorithm through the improvement of M sequence. The numerous classical encryption algorithms are all significantly affected by image compression and noise, both of which undermine their stability. Pathak and Bansal [6] proposed the spatial least significant bit (LSB) algorithm, which greatly enhances the anti-compression ability. Azmi et al. [7] introduced swarm intelligence algorithm to encryption. Bin and Sun [8] applied the encryption algorithm into transform domain. Despite their good encryption effect, the robustness of these algorithms needs to be further improved. In addition, special attention should be paid to the loss and dislocation of bit information in the JPEG compression.

Li et al. [9] combined the compressed sensing algorithm with digital watermarking, making the algorithm more robust and secure. Ganic and Eskicioglu [10] designed the watermark embedding algorithm of wavelet transform, and applied it to image compression. Li and Wang [11] created a robust watermark embedding algorithm based on image contents. Chen et al. [12] presented a robust watermark embedding algorithm based on discrete wavelet transform (DWT) and discrete Fourier transform (DFT), and verified its robustness

on JPEG compression. Cao et al. [13] improved the vector image compression algorithm, such that the algorithm can effectively handle JPEG compression; however, the improved algorithm cannot embed too many information in watermarks.

Albeit their successful application in different fields, the existing digital watermarking algorithms generally have a limited robustness. This is the major bottleneck in the promotion of digital watermarking. To solve the problem, this paper comes up with a stable and secure digital watermarking algorithm, which takes advantage of the robustness of image DCT coefficients to JPEG compression.

3. ANTI-COMPRESSION IMAGE WATERMARK ENCRYPTION

3.1 Basic features of JPEG images

JPEG can compress grayscale images or color images in continuous tones. For color images, they are converted into the hue-saturation-value (HSV) space, according to our visual features. The first step of JPEG compression is to divide the input image into blocks. If the size of the image is not an integer multiple of eight, the original image needs to be enlarged, before cropping the compressed image to restore the original size. Discrete cosine transform (DCT) is adopted by JPEG, and its compression process is shown in Figure 1.

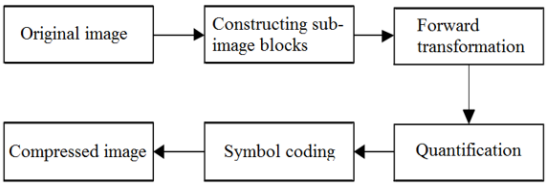

Figure 1. Block diagram of JPEG image compression

Two-dimensional discrete cosine transform (DCT) can be defined as a matrix:

Forward transform:

$$F = CfC^T \tag{1}$$

Inverse transform:

$$f = CFC^T \tag{2}$$

where, C is the DCT matrix; C^T is the transpose matrix of C. The transform matrix C can be expressed as:

$$C = \sqrt{\frac{2}{N}}\begin{bmatrix} \sqrt{\frac{1}{2}} & \sqrt{\frac{1}{2}} & \cdots & \sqrt{\frac{1}{2}} \\ cos\frac{\pi}{2N} & cos\frac{3\pi}{2N} & \cdots & cos\frac{(2N-1)\pi}{2N} \\ \vdots & \vdots & \vdots & \vdots \\ cos\frac{(N-1)\pi}{2N} & cos\frac{3(N-1)\pi}{2N} & \cdots & cos\frac{(2N-1)(2N-1)\pi}{2N} \end{bmatrix} \tag{3}$$

If N=2, the transform matrix C can be established as:

$$C = \begin{bmatrix} \sqrt{\frac{1}{2}} & \sqrt{\frac{1}{2}} \\ cos\frac{\pi}{4} & cos\frac{3\pi}{4} \end{bmatrix} \tag{4}$$

The information of an image can be reflected by wavelet coefficients. Global information like image contour depends on the low-frequency wavelet coefficients. Meanwhile, edge information and high-frequency information of the image are determined by high-frequency wavelet coefficients. Although the wavelet coefficients of the image are partially affected by JPEG compression, some of the image features can be preserved.

Wavelet coefficients can be used for digital watermarking of compressed images. The wavelet coefficients of an image are affected by JPEG compression. The relationship of wavelet sub-bands before and after compression can be defined as:

$$w_l = [p_i, \cdots, p_{i+m}] \tag{5}$$

$$w_t = \begin{bmatrix} p_i \\ \vdots \\ p_{i+m} \end{bmatrix} \tag{6}$$

where, w_t and w_l are the sliding windows in the vertical and horizontal directions, respectively.

Table 1 shows the relationship between high-frequency wavelet sub-band coefficients before and after JPEG compression.

Table 1. Relationship between high frequency wavelet sub-band coefficients before and after JPEG compression

Degree of JPEG	First-Order Neighborhood	Second-Order Neighborhood	Third-Order Neighborhood
10	0.943	0.887	0.789
8	0.912	0.835	0.713
6	0.876	0.806	0.709

As shown in Table 1, the relationship between any two wavelet sub-band coefficients within a sliding window is immune to JPEG compression, as long as the following two conditions are satisfied:

(1) The size of adjacent coefficients is stable;

(2) The sliding window length is limited within a certain range.

3.2 Anti-compression image watermark encryption based on wavelet sub-band coefficient

According to the above analysis, the difference between the two coefficients in the sliding window can be binarized into a relationship matrix H:

$$H = \begin{bmatrix} p_i - p_{i+1} & \cdots & p_{i+m} - p_{i+m+1} \\ p_i - p_{i+2} & \cdots & p_{i+m} - p_{i+m+2} \\ \vdots & \vdots & \vdots \\ p_i - p_{i+n} & \cdots & p_{i+m} - p_{i+m+n} \end{bmatrix} \tag{7}$$

If the difference between any two coefficients p_i and p_{i+m} is positive, it is quantized to 0; otherwise, it is quantized to 1.

The quantized relation matrix can be expressed as:

$$H = \begin{bmatrix} b_{1,i} & \cdots & b_{1,i+m} \\ b_{2,i} & \cdots & b_{2,i+m} \\ \vdots & \vdots & \vdots \\ b_{n,i} & \cdots & b_{n,i+m} \end{bmatrix} \quad (8)$$

Considering the features of JPEG image compression, the authors adopted a watermark embedding method related to the size relationship between coefficient pairs. Specifically, the information embedded according to the relationship between coefficients pair in the first-order neighborhood is very stable, but it might damage the original image if the coefficients differ greatly. If the watermark information is embedded by the coefficient pair relationship in the high-order neighborhood, its stability to JPEG compression is slightly poor. To reduce the damage to the original image, it is suitable to choose the coefficient pair with a small coefficient difference for modification. Therefore, error correction coding should be performed on the watermark to enhance its robustness, so as to balance anti-compression ability with peak-signal-to-noise ratio (PSNR).

In this paper, a semi-fragile watermarking algorithm robust is proposed to remain robust in common compression operations. During the authentication of electronic bills, the only sensitive information includes easily tampered contents like amount, and date, while the other common information needs not be treated as sensitive information. The proposed semi-fragile watermarking algorithm can distinguish accidental attacks from malicious tampering, and effectively improve the operation efficiency and robustness of the original image to compression operations.

According to the stability of high-frequency sub-band coefficients of wavelet transform before and after JPEG compression, the watermark image can be embedded into coefficients with a constant relative size. When modifying the sub-band coefficients, the target coefficients of the embedded watermark image were selected according to two conditions: First, the difference between the original image coefficient pairs in the sliding window is greater than a certain threshold; Second, the difference between the coefficients is below an upper limit. The damage to the original image can be minimized by embedding bit information of digital watermark, using the coefficients with small difference.

For LH_1 sub-band coefficients, the size relationship is relatively stable in the horizontal direction. Hence, the watermark information was embedded into the quantized horizontal difference relationship matrix H. For LH_1 sub-band coefficients, the size relationship is relatively stable in the vertical direction. Thus, the watermark information was embedded into its relationship matrix H^T in the vertical direction. For the ease and efficiency of information embedding, the watermark image was binarized before embedding watermark information.

To further enhance the security of electronic bills and the privacy of watermarks, chaotic mapping was applied to the watermarking algorithm of JPEG images, thereby improving the ability to preserve privacy and detect tampering in key areas of financial bills. Owing to the high sensitivity of chaotic systems to initial values, our method is very good at locating tampering risks.

The chaotic encryption of watermark image consists of three steps:

(1) Binarize the watermark image into a two-dimensional matrix with only zeros and ones, and then reducing the dimension of the matrix to a binary sequence.

(2) Select the initial value x of the chaotic map as a key to obtain a chaotic sequence with the same length as the watermark, and binarize the chaotic sequence.

(3) Perform exclusive or exclusive disjunction (XOR) on the generated binary chaotic sequence, and the watermark sequence for encryption.

The initial value of chaotic system was treated as the key for encryption and decryption, providing a good guarantee of security. Meanwhile, chaotic sequences conform to the statistical features of white noise and effectively withstand steganalysis, which facilitates image scrambling. The embedding method of semi-fragile watermark can be defined as follows:

Algorithm 1: Embedding method of semi-fragile watermark

Input: An N×N watermark image matrix, initial key at iteration $x[0]$
Output: Watermarked image
y = ENCR (Arr[]; $x_{[0]}$)
H = GENMATRIX(Image)
result = y + H
function ENCR (Arr[]; $x_{[0]}$)
s=FLATTEN(Arr[])
b=BINARY(s)
for $i = 1 \rightarrow$ N ×N do
$x_{[i]} \leftarrow u \times \min\{x_{[i-1]}, 1 - x_{[i-1]}\}$
$y_{[i]} \leftarrow b_{[i]} \oplus x_{[i]}$
end for
return y
end function
function GENMATRIX(Image)
for $i = 1 \rightarrow$ N - m do
$w_t \leftarrow [p_i, \ldots, p_{i+m}]^T$

$$H = \begin{bmatrix} p_i - p_{i+1} & \cdots & p_{i+m} - p_{i+m+1} \\ p_i - p_{i+2} & \cdots & p_{i+m} - p_{i+m+2} \\ \vdots & \vdots & \vdots \\ p_i - p_{i+n} & \cdots & p_{i+m} - p_{i+m+n} \end{bmatrix}$$

for each $p \in$ H do
if $p > 0$ then
$p \leftarrow 1$
else
$p \leftarrow 0$
end if
end for
end for
return H
end function

4. MULTIPLE WATERMARK ENCRYPTION BASED ON KEY INFORMATION AREA DETECTION

This section focuses on the location and encryption of the key areas in financial bills. Every electronic bill image contains many patterns, such as background, amount, drawer, issuing bank, and date. Among them, amount, date, drawer and issuing bank call for high-level protection against tampering. However, many existing watermark encryption algorithms cannot identify or distinguish the image contents, not to mention protecting the key sensitive contents. In view of the features of financial bills, this paper proposes a machine learning mechanism to extract image features, locate the areas of key contents, and encrypt these areas with multiple digital

watermarks. The location of key areas of bill image is explained in Figure 2. The original electronic image of the financial bill is shown in Figure 3.

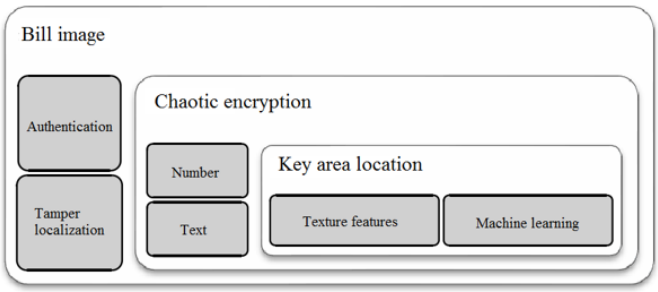

Figure 2. The location of key areas of bill image

Figure 3. The original electronic image of the financial bill

As shown in Figure 3, the original image contains many patterns. Some patterns are sensitive, and some are not sensitive. Before locating the sensitive patterns (i.e., the key areas), it is important to preprocess the original electronic images, and obtain the key information of pixel gradient change through compilation and extraction. The connected areas were further distinguished through contour extraction. Each contour topology was represented by a color edge. The center point of each contour was marked by a white circle, reflecting the distribution area of key information in this bill image. These key areas were subjected to location checks, with the focus on protecting the numerical information and preventing tampering.

Owing to the features of financial bills, digital information is prone to be tampered with. Therefore, the primary problem of the encryption and authentication system of electronic bills is to detect and locate digital images.

In the field of area detection and location, computer vision and artificial intelligence algorithms are important instruments. Such an algorithm generally involves two steps: feature extraction and training modeling.

Image features reflect much of bill information and play a key role in the extraction and construction of two-dimensional image features and the identification of image content. The training of key area detection algorithm can be defined as follows:

Algorithm 2: Training of key area detection algorithm

Input: Train images, including positive samples and negative samples.
Step 1: Prepare training data. Take images containing key information areas as positive samples and those containing background areas as negative samples.
Step 2: Normalize the size of the images.
Step 3: Extract the inverted invariant scale-invariant feature transform (SIFT) feature of the image to obtain a fixed-length feature vector.
Step 4: Train the model through machine learning, e.g., support vector machine (SVM) and artificial neural network (ANN).

The detection of key areas can be carried out by classifying background images and target images. The detection process can be defined as follows:

Algorithm 3: Key area detection algorithm

Input: Train images, including positive samples and negative samples.
Step 1: Traverse the target image with sliding windows of different sizes.
Step 2: Enter the sliding window into the machine learning model.
Step 3: Wait for the machine learning model to output a result about whether it is a key area.
Step 4: Merge the rectangular windows whose distance is close to a certain threshold to obtain the final result.

The image features can be detected and analyzed using the SIFT [14], and the template can be recognized by three algorithms: template matching (TM) [15], SVM, and ANN. The TM can be expressed as:

$$S_T = \sum_{x,y} T(x,y)F(x,y) \tag{9}$$

where, T is the template and F is the target area. Changes in the gray value and size of the target area always affect the results of related operations. After normalizing the parameters, the following expression can be obtained:

$$S_T = \frac{\sum_{x,y}[T(x,y)-E(T)][F(x,y)-E(F)]}{\sqrt{\sum_{x,y}[T(x,y)-E(T)]^2 \sum_{x,y}[F(x,y)-E(F)]^2}} \tag{10}$$

where, E is the expectation of the gray value of the image.

Then, the image areas of the financial bill can undergo TM through a sliding window. The TM-based image area detection can be defined as follows:

Algorithm 4: TM-based image area detection

Input: An N ×N image template
Output: Area detection results x, y, w, and h (abscissa, ordinate position, width and height)
Extract features of template image, SIFT (Matrix T×T)
for $x, y = 0$, $0 \rightarrow$ X, Y do
Extract features of image area, SIFT (Matrix $w \times h$)
Calculate TM score = S (T, F, E)
$x = x + \delta x$
$y = y + \delta y$
end for
Return the position of the detection result, x, y, w, h

Through the above analysis, this paper proposes a multiple watermark encryption method using both visible and invisible watermarks, with the aim to identify the source information of financial bills and detect tampering behaviors. The algorithm improves the security of the electronic image of financial bill, even if the image is intercepted by an attacker. The source, copyright, and other information of the original bill cannot be

hidden by malicious tampering with key information, due to the visible copyright effect of the watermarks. While protecting sensitive information, our algorithm realizes authentication of tampering location and bill anti-counterfeiting through invisible watermark.

The significance of visible watermark mainly lies in its certification of the source of financial bills. Because it is visible, anyone can view the information embedded in visible watermarked bills. This feature can effectively prevent financial fraud.

Drawing on the features of the visual system, the block stretching coefficient was simplified, and the edge information in the spatial domain was used to improve the watermark embedding effect. The watermarks can be superimposed by:

$$c_{ij} = \alpha_n c_{ij}(n) + \beta_n w_{ij}(n), n = 1,2,\cdots \tag{11}$$

where, $c_{ij}(n)$ and $w_{ij}(n)$ are the DCT coefficients of image and watermark, respectively; α_n and β_n are the stretching coefficients of block n:

$$\alpha_n = \sigma_n' exp\ (-(\mu_n' - \mu')^2) \tag{12}$$

$$\beta_n = (\frac{1}{\sigma_n'})(1 - exp\ (-(\mu_n' - \mu')^2)) \tag{13}$$

where μ_n and μ_n' are the mean gray levels of block and the whole image, respectively; σ_n' is the coefficient variance; α_n and β_n are the factor controlling image distortion, whose values should minimize the change to the image edge. Due to the sudden change of the stretching coefficient, this watermark embedding method may produce a block effect at the edge in the experiment, which reduces the image quality.

The steps of the watermark embedding algorithm can be summarized as follows:

Algorithm 5: Visible watermark embedding algorithm

Input: An N ×N watermark image matrix, initial key at iteration *x*[0]
Output: Watermark embedding image
y = Watermark (Matrix)
Perform DCT transform to obtain texture information
Calculate embedding coefficients α and β
H = GENMATRIX (Image)
DCT image blocking matrix $N_i \times N_i$
Embed DCT coefficients
Result = *y* + H

5. EXPERIMENTS AND RESULTS ANALYSIS

5.1 Experiment on anti-compression image watermark encryption method

The first experiment aims to verify the robustness of the proposed anti-compression image watermark encryption method, using the electronic bill in Figure 3. The effect of the method was measured by the PSNR [16], which reflects the distortion degree of digital images and the damage degree of JPEG to image compression. The PSNR is a common way to measure the reconstruction quality of regional signals such as image compression, and its mathematical definition is mean squared error (MSE).

Let A and B be monochromatic images of the size $m \times n$. If A and B are approximate noises to each other, the MSE between A and B can be expressed as:

$$MSE = \frac{1}{mn}\sum_{i=0}^{m-1}\sum_{j=0}^{n-1}\|A(i,j) - B(i,j)\|^2 \tag{14}$$

By modifying the wavelet sub-band coefficients in JPEG compression process, the relative coefficients are adjusted to realize bit embedding. Therefore, the extent to which the coefficients are modified determines the degree of damage to the original image. The PSNR can be defined as:

$$PSNR = 10 \times log\frac{MAX_I^2}{MSE} \tag{15}$$

where, MAX_I is the maximum value representing the color of the image pixel. The higher the PSNR, the more similar the two images, and the less their distortions.

In experiment, the variances of wavelet sub-band coefficients are measured in horizontal and vertical directions, and the change of PSNR before and after electronic bill encryption was monitored closely. The experimental results are shown in Figure 4.

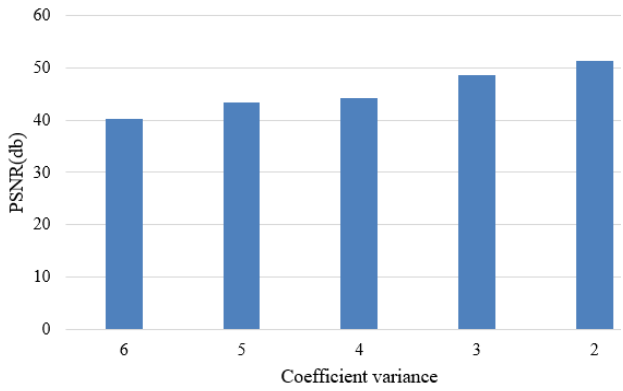

Figure 4. Change of PSNR before and after electronic bill encryption

As shown in Figure 4, the original image was not greatly damaged, when the variance of sub-band coefficients was small. In practical application, however, the variance of wavelet coefficients cannot be reduced blindly. Watermarks should be embedded at places with a certain coefficient value difference, in order to resist the influence of JPEG compression. The threshold is generally set to 2. The position of watermark embedding can be selected if the coefficient difference is greater than 2.

Next, experiments were carried out on 200 financial bill images. From the statistical results in Figure 5, PSNR and coefficient variance are indeed correlated on a large statistical scale. When the coefficient variance changed from 6 to 2, the PSNR increased from 40.3 to 51.5. The relationship between the sub-band coefficient and the damage degree of the image remained valid, that is, the smaller the variance of the sub-band coefficient, the smaller the damage to the original image.

Then, the robustness of the proposed watermark algorithm was tested under different JPEG compression levels. Under the JPEG compression levels of 6, 8, and 10, the watermark was embedded and extracted, and PSNR values under different conditions were calculated, thereby acquiring the distortion degree of images under different compression levels.

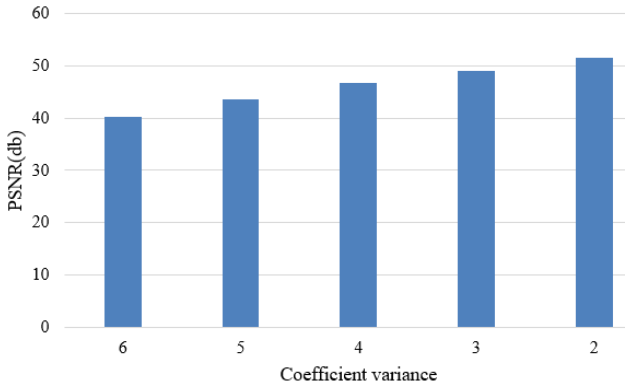

Figure 5. Statistical results between PSNR and coefficient variance

The results in Figure 6 show that our watermark algorithm is robust to JPEG compression. Despite the growing compression rate, the watermark image always maintained a good quality.

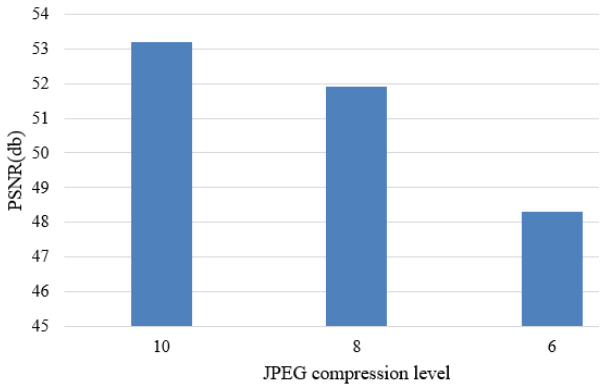

Figure 6. Statistical results between PSNR and coefficient variance

5.2 Experiments on multiple watermark encryption

(a) Visible reversible watermark

(b) Remove the reversible watermark

Figure 7. Effect of multiple watermark encryption

The generation algorithm of reversible visible watermark can improve the security of electronic bills. Typical reversible watermarks insert watermark information by additive spread spectrum technology or by embedding information bits.

As shown in Figure 7, after the removal of visible watermarks, the bill information covered and protected were effectively restored.

6. CONCLUSIONS

This paper probes into the principle of digital image watermarking and its application in anti-counterfeiting of electronic bills. Firstly, the authors summarized the attack methods of digital watermarking and the JPEG image compression standard, and proposed a method to resist the JPEG compression attack according to the relationship between wavelet sub-band coefficients. Application results show that the embedded watermark pattern was little impacted at different image compression rates, suggesting that the proposed method effectively prevents the attacks on electronic bills in transmission. To further overcome the security risks in the application of financial bills, the authors further designed a detection and location method for key areas on electronic bills. Compared with the existing location algorithms of image contents, the chaotic encryption algorithm was used to protect sensitive information. With the aim to prevent financial fraud, multiple visible and invisible watermarks were adopted to authenticate and protect electronic bills. The experimental results verify that our method can identify and encrypt the key area of each bill, as well as detect and curb tampering and forgery, providing a guarantee to the security of financial bills.

ACKNOWLEDGEMENTS

The authors acknowledge funding from the General project of Chongqing natural science foundation (cstc2019jcyj-msxmX0731), Science and Technology Project of Chongqing Municipal Education Commission (KJQN202000905).

REFERENCES

[1] Komatsu, N., Tominaga, H. (1990). A proposal on digital watermark in document image communication and its application to realizing a signature. Electronics and Communications in Japan (Part I: Communications), 73(5): 22-33. https://doi.org/10.1002/ecja.4410730503

[2] Verma, V.S., Jha, R.K., Ojha, A. (2015). Digital watermark extraction using support vector machine with principal component analysis based feature reduction. Journal of Visual Communication and Image Representation, 31: 75-85. https://doi.org/10.1016/j.jvcir.2015.06.001

[3] Särkkä, A., Renshaw, E. (2006). The analysis of marked point patterns evolving through space and time. Computational Statistics & Data Analysis, 51(3): 1698-1718. https://doi.org/10.1016/j.csda.2006.07.008

[4] Karthigaikumar, P., Baskaran, K. (2011). FPGA and ASIC implementation of robust invisible binary image watermarking algorithm using connectivity preserving criteria. Microelectronics Journal, 42(1): 82-88. https://doi.org/10.1016/j.mejo.2010.08.023

[5] Qin, C., Chang, C.C., Chen, P.Y. (2012). Self-embedding fragile watermarking with restoration capability based on adaptive bit allocation mechanism. Signal Processing, 92(4): 1137-1150.

https://doi.org/10.1016/j.sigpro.2011.11.013
[6] Pathak, K., Bansal, M. (2017). A FPGA based Steganographic System Implementing a Modern Steganalysis Resistant LSB Algorithm. Defence Science Journal, 67(5): 551-558. https://doi.org/10.14429/dsj.67.10177
[7] Azmi, K.Z.M., Ghani, A.S.A., Yusof, Z.M., Ibrahim, Z. (2019). Natural-based underwater image color enhancement through fusion of swarm-intelligence algorithm. Applied Soft Computing, 85: 105810. https://doi.org/10.1016/j.asoc.2019.105810
[8] Bin, S., Sun, G. (2020). Optimal energy resources allocation method of wireless sensor networks for intelligent railway systems. Sensors, 20(2): 482. https://doi.org/10.3390/s20020482
[9] Li, Q., Ma, J., Erlebacher, G. (2012). A new reweighted algorithm with support detection for compressed sensing. IEEE Signal Processing Letters, 19(7): 419-422. https://doi.org/10.1109/LSP.2012.2198641
[10] Ganic, E., Eskicioglu, A.M. (2005). Robust embedding of visual watermarks using discrete wavelet transform and singular value decomposition. Journal of Electronic Imaging, 14(4), 043004. https://doi.org/10.1117/1.2137650
[11] Li, Y., Wang, J. (2019). Robust content fingerprinting algorithm based on invariant and hierarchical generative model. Digital Signal Processing, 85: 41-53. https://doi.org/10.1016/j.dsp.2018.11.009
[12] Chen, D., Wan, S., Xiang, J., Bao, F.S. (2017). A high-performance seizure detection algorithm based on Discrete Wavelet Transform (DWT) and EEG. PloS One, 12(3): e0173138. https://doi.org/10.1371/journal.pone.0173138
[13] Cao, L., Men, C., Ji, R. (2013). Nonlinear scrambling-based reversible watermarking for 2D-vector maps. The Visual Computer, 29(3): 231-237. https://doi.org/10.1007/s00371-012-0732-x
[14] Bin, S., Sun, G., Cao, N., Qiu, J., Zheng Z., Yang, G., Zhao, H., Jiang, M., Xu, L. (2019). Collaborative filtering recommendation algorithm based on multi-relationship social network. CMC-Computers, Materials & Continua, 60(2): 659-674. https://doi.org/10.32604/cmc.2019.05858
[15] Tian, G., Zhou, S., Sun, G., Chen, C.C. (2020). A novel intelligent recommendation algorithm based on mass diffusion. Discrete Dynamics in Nature and Society. https://doi.org/10.1155/2020/4568171
[16] Sun, G., Bin, S. (2018). A new opinion leaders detecting algorithm in multi-relationship online social networks. Multimedia Tools and Applications, 77(4): 4295-4307. https://doi.org/10.1007/s11042-017-4766-y