International Journal of Security and Its Applications
Vol.9, No.12 (2015), pp.259-268
http://dx.doi.org/10.14257/ijsia.2015.9.12.24

A Robust Information Hiding Scheme for Protecting Digital Content in DWT-CS Domain

Huimin Zhao[1], Jun Cai[2] and Li Zhu[3]

[1,2] *School of Electronic and Information, Guangdong Polytechnic Normal University, Guangzhou 510665, China*

[3] *Industrial Training Center, Guangdong Polytechnic Normal University, Guangzhou 510665, China*

[1] *zhaohuimin@gdin.edu.cn*, [2] *caijun@gmail.com*, [3] *Zhuli@gdin.edu.cn*

Abstract

In information hiding field, the robustness is the important performance. However, due to embedding a larger amount of the watermark into host signal, transparency and robustness of the watermarked image cannot be easily obtained, simultaneously. Utilizing measurement values of original image to produce hiding information block-based Compressed Sensing (BCS) theory in DWT domain, the paper presents a robust information hiding scheme for protecting digital content. When the scheme is achieved, embedding locations of the hiding information will be selected by visual features and relation of DWT coefficients between subbands LH_3 and LH_2 of the host image. Moreover the mechanism of JND (just-noticeable distortion) was used to adjust the embedding watermark strength. Experimental results show that the scheme is more robust compared with other hiding algorithm reported, and improves effectively the recovery quality of the hidden image.

Keywords: *Robustness, watermark, compressive sensing, discrete wavelet transform*

1. Introduction

The watermarking process has been considered as an alternative solution for the copyright protection of digital materials in information hiding field, such as digital image, video and audio. During the last decade, several watermarking algorithms have been proposed in the literature. In the early approaches, watermarking was realized in the time or spatial domain [1-2], however it is difficult to get a tradeoff between imperceptibility and robustness of the watermarked image at the same time. Therefore, recently more robust watermarking algorithms have been developed in the transform domain.

Two types of watermark signals are basically used for hiding information to protect the digital content, one of them is the pseudo random sequence and another one is the two-dimensional visually recognizable image such as a logotype. In general the pseudo random sequence is generated by using a secret key, which is related to the owner or provider [3], while the second one, a two-dimensional watermark, represents directly the ownership of the provider as a logotype form [4,5]. For this reason, the second type of watermarks has a stronger impact than the first one at the ownership claiming time. However, in general, the hiding amount of the second type of watermark is much more than that of the first one [5]. Due to this fact, it is difficult to provide an invisible and robust information hiding system using second type of watermark schemes. To overcome the drawback, some adaptive watermarking algorithms based on DCT (discrete cosine transform) and DWT (discrete wavelet transform) domain were proposed [5-7]. In [6], Just Noticeable Difference (JND) was calculated using DCT coefficients to determine coefficient's position and maximum watermark insertion energy while keeping

ISSN: 1738-9976 IJSIA

imperceptibility of the watermarked image. In [7], texture information of each block of the image is used to embed watermark pattern in lower frequencies region of the DCT coefficients.

Also, many DWT-based algorithms to embed visually recognizable pattern in host image have been proposed [8-9]. In [8], Qualified Significant Wavelet Trees (QSWTs) are found in the multi-resolution wavelets coefficients and watermark data are embedded in some elements of the QSWTs, and in [9], JND information of wavelets coefficients and Chaotic Mixing method proposed by [9] were used to embed gray-scale watermark in the imperceptible manner. Both algorithms perform fairly well, however to extract watermark from the watermarked image, many additional information such as Significant Tree position and order data of the watermark, etc. These data together with original unmarked image must be stored in the secure place by the material's owner.

At present, a focus issue is how to achieve a tradeoff between the watermarked image quality and the information hiding robustness using for resisting various attacks. This is because, the additional hidden information (watermark) may often lead to host image distortion [10]. Therefore, researchers must consider the tradeoff relation from various aspects, such as watermarking information and embedding location as well as hiding capacity, etc.

In recent years, arisen compressed sensing (CS) theory provides a feasible method to solve the tradeoff relation described in [11-13]. Firstly, random measurement values of the CS can indicate perfectly all features of the image, and data amount of the measurement values is far more less than host image. Therefore, the hiding information generated by measurement values of the CS will improve the security of the information hiding system.

On the other hand, computational secrecy by the CS measurement values will satisfied for high security requirement of the information hiding system. This means that attackers will be incapable to conjecture the original hidden information while they do not have a priori knowledge about key.

Based the aim described in above, the paper proposes a novel information hiding scheme using for protecting digital content based on block compressed sensing (BCS) in DWT domain. The scheme needs only to embed smaller the information while retaining higher robustness and quality of watermarked image. In the proposed method, material's owner must only conserve unmarked original image, and visually recognizable hiding information can be any size gray-scale or binary image. The computer simulation results show the robustness of the proposed scheme when the watermarked image is suffered by intentional and no-intentional attacks.

The rest of this paper is organized as follows. Section 2 describes the proposed hiding scheme, and introduces related work for the CS theory. Section 3 shows the experimental results for hiding digital fingerprint and binary image, and demonstrates the effectiveness of the proposed the scheme. In this section, the experimental aim of using fingerprint image as the CS-watermarking signal is to protect ownership for identity authentication in e-commerce application. Finally, we give our conclusion in Section 4.

2. The Proposed Hiding Scheme

2.1. BCS Principle

In BCS, an image is divided into $B \times B$ blocks, and each block is sampled using an appropriately-sized measurement matrix. That is, suppose that x_j is a vector representing of block j of input image x. The corresponding a measurement sample y_j is then

$$y_j = \Phi \cdot x_j \tag{1}$$

Where y_j has length M_B, and Φ is an $M_B \times B^2$ measurement matrix such that the subrate for the image as a whole is $S = M_B / B^2$. It is straightforward to see that (1) applied block-by-block to an image is equivalent to a whole-image measurement matrix A in which $y = A \cdot x$ with a constrained structure. specifically, A is constrained to have a block-diagonal structure,

$$A = \begin{bmatrix} \Phi & 0 & \cdots & 0 \\ 0 & \Phi & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & \Phi \end{bmatrix} \tag{2}$$

Where A is an M×N measurement matrix, and $M << N$. Therefore, BCS was proposed wherein the sampling of an image is driven by random matrices applied on a block-by-block basis, while the reconstruction is a variant of the projected Landweber (PL) reconstruction that incorporates a smoothing operation intended to reduce blocking artifacts. Since it combines BCS with a smoothed PL (SPL) reconstruction, in [14], the overall technique was called BCS-SPL.

2.2. Watermarking Process for Hiding Information

Because measurement samples of the BCS can indicate all features of an original image, we regard the CS measurement samples as hiding information which is also called CS-watermark in the paper [15-16]. In the scheme, the original hiding image is carried out by a wavelet transform, and BCS is deployed independently within each subband of each decomposition level of the wavelet transform to provide variable sampling. Finally, we combine these sampling values to produce CS-watermark. The production principle of the CS-watermark is showed in Figure 1.

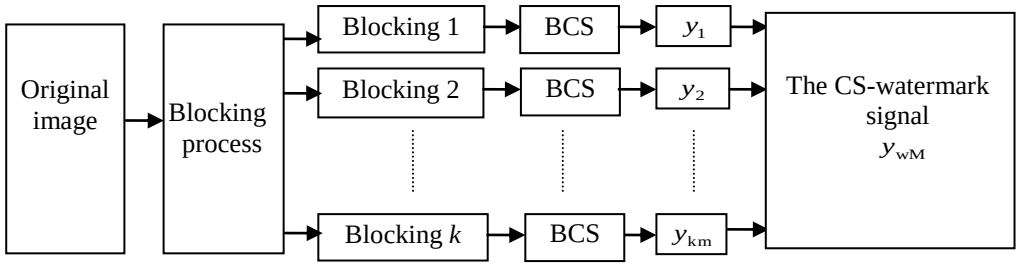


Figure 1. Process of the CS-Watermarking Signal

In Figure 1, suppose total pixels of the hiding image is $M_1 \times M_2$ and total pixels of the CS-watermark is $M \times M$, size of the measurement samples of each subblock of the image is $m = \lfloor MB_l^2 / M_1 \times M_2 \rfloor$. If measurement samples of block j of subband s at level l are $y_{l,s,j}(j = 1,2,...,B_l^2)$, then we will compose all measurement samples of each block of each subband in DWT domain to a normalized form of the CS-watermark is showed in (3):

$$Y_{wM} = \begin{bmatrix} y_{1,1,1} & y_{2,1,1} & \cdots & y_{L,1,1} \\ \vdots & \vdots & \cdots & \vdots \\ y_{1,2,1} & y_{2,2,1} & \cdots & y_{L,2,1} \\ \vdots & \vdots & \ddots & \vdots \\ y_{1,4,B_1^2} & y_{2,4,B_2^2} & \cdots & y_{L,4,B_L^2} \end{bmatrix}, \quad \{W(l,s,j), W(l,s,j) \in (0,1)\} \tag{3}$$

Here, seeds generated for CS measurement matrix Φ_B and size of blocking are saved as a key of the CS-watermark, respectively. Due to the adoption of CS theory here, so the CS-watermark is only a random process of the simple linear projection. Time complexity of the CS-watermark depends on size of the measurement matrix. According to some parameters described above, time complexity of feature extraction within each block of the original watermark image is $O(mB_i^2)$. Because of total block of the whole image is $S = N^2 / B^2 (B = \sum_{i=1}^{L} B_i)$, therefore the total time complexity is $O(mM_1 \times M_2)$.

2.3. Watermark Embedding Process

The watermark embedding process is shown by the Figure 2. The steps of the watermark embedding process are as follows:

Step 1: DWT decomposition.

The original host image is realized three level decomposition using 2D-DWT to get 10 subbands (LL_3,LH_3,HL_3,HH_3,LH_2,HL_2,HH_2,LH_1,HL_2,HH_1). We use two subbands (LH_3, LH_2) or (HL_3,HL_2) for embedding location because some modification in these subbands causes fewer perceptible degradation and wavelets coefficients in these subbands survive common attacks.

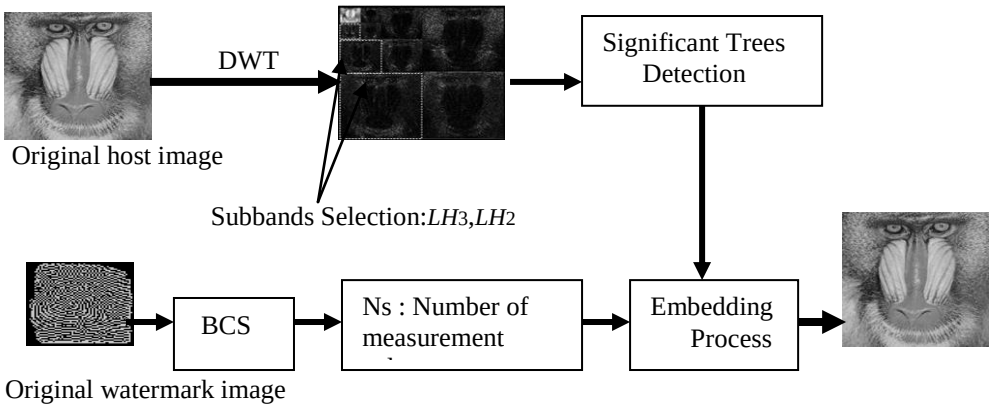


Figure 2. The CS-Watermark Embedding Process

Step 2: Significant Trees detection.

Significant Trees have same concept of the QSWTs proposed by [8] and inverse concept of Zero Trees used for image compression EZW by [9]. We consider the wavelets coefficients of the coarser subband and its correspond finer subband create a Significant Tree, if $\left|x_{i,j}^{LH_3}\right| \geq T_1$ and $|x_{k,l}^{LH_2}| \geq T_2$, $\forall k = 2^* i, 2^* i - 1; l = 2^* l, 2^* j - 1$, where $x_{i,j}^{LH_3}$ and $x_{k,l}^{LH_2}$ are (*i*,*j*)-th coefficient in LH_3 and *(k,l)-th* coefficient in LH_2, respectively, and T_1,T_2 are threshold determined by equation (4).

$$T_1 = \frac{Median(|x_1|,|x_2|,|x_3|,.....,|x_N|)}{N}, \quad x_i \in LH_3$$
$$T_2 = \frac{Median(|x_1|,|x_2|,|x_3|,.....,|x_M|)}{M}, \quad x_i \in LH_2 \tag{4}$$

where N and M are number of coefficients in the subband LH_3 and LH_2, respectively.

Each Significant Tree contains five elements, which are one parent (coefficient in LH_3) and four children (four coefficients in LH_2). After all Significant Trees are detected, total number of the Significant Trees is saved in Ns. Naturally, total number of Significant Trees is depend on the original image.

Step 3: BCS application to the CS-Watermark.

Watermark (gray-scale or binary) image is transformed to the frequency domain by 2D-BCS and Ns measurement values are arranged in zig-zag manner from $W(1,1)$ to $W(i,j)$ as shown by Figure 3. First Ns coefficients are selected to embed.

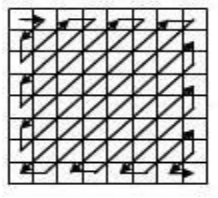


Figure 3. CS-Watermarks Embedding Order

Step 4: Sorting Significant Trees.

All Significant Trees are sorted in descending order by sum of absolute value of parent coefficient and maximum absolute value of four children, as given by Equation (5).

$$\left|x_{i,j}^{LH_3}\right| + \max_{k,l}\left(\left|x_{k,l}^{LH_2}\right|\right), k = 2*i, 2*i-1, l = 2*j, 2*j-1 \tag{5}$$

Step 5: Information embedding process

Ns measurement values of the hiding information (watermark) embed to the sorted Significant Trees, this process is given by Equation (6) and (7).

$$wx_q^{LH_3} = x_q^{LH_3} + \alpha w_q, \quad q = 1...Ns \tag{6}$$

$$wx_q^{LH_2} = \bar{x}_q^{LH_2} + \alpha w_q, \quad q = 1...Ns \tag{7}$$

where $x_q^{LH_3}$ is parent of the q-th sorted Significant Tree and $\bar{x}_q^{LH_2}$ is one child of the q-th Significant Tree, whose absolute value is maximum between four children. w_q is CS-watermark data of the q-th Significant Tree. The embedding factor α is inversely proportional to CS component of the watermark image to conserve same imperceptibility without regard to size of the hiding information (watermark). It is given by (8)

$$\alpha = \frac{\| w_q \|}{\| Y_{wM} \|} \tag{8}$$

Where $\|w_q\|$ is CS component's value and $\|Y_{wM}\|$ is the embedding energy of the watermark signal.

Step 6: Inverse DWT.

Finally, DWT coefficients are transformed by inverse DWT to get watermarked image.

2.4. Information Extraction Process

Watermark extraction process is shown by Figure 4. In this process not only watermarked image but also original image are required. Both images are decomposed ten subbands by applying 2D-DWT. Significant Trees are detected from subbands (LH3 and LH2) of original image. After Significant Trees are sorted, we can extract CS measurement values of the watermarked image using eqs. (8) and (9).

$$\begin{aligned} W_q^{LH_3} &= \bar{Y}_q^{LH_3} - Y_q^{LH_3} \\ W_q^{LH_2} &= \bar{Y}_q^{LH_2} - Y_q^{LH_2} \qquad q = 1..Ns \end{aligned} \tag{9}$$

$$W_q = \frac{\left(W_q^{LH_3} + W_q^{LH_2}\right)}{2\alpha}, \qquad q = 1...Ns \tag{10}$$

where α is watermark energy used in the embedding process.

The q-th CS values of the watermark image is the average of extracted measurement from parent element and extracted CS values from maximum child element of the q-th sorted Significant Trees.

After all CS measurement values of the watermark image are extracted, these are rearranged in zig-zag manner to get a matrix with size of $d_1 \times d_2 = N_s$. Finally the matrix is applied by BCS-SPL algorithm to get watermark image extracted in [14].

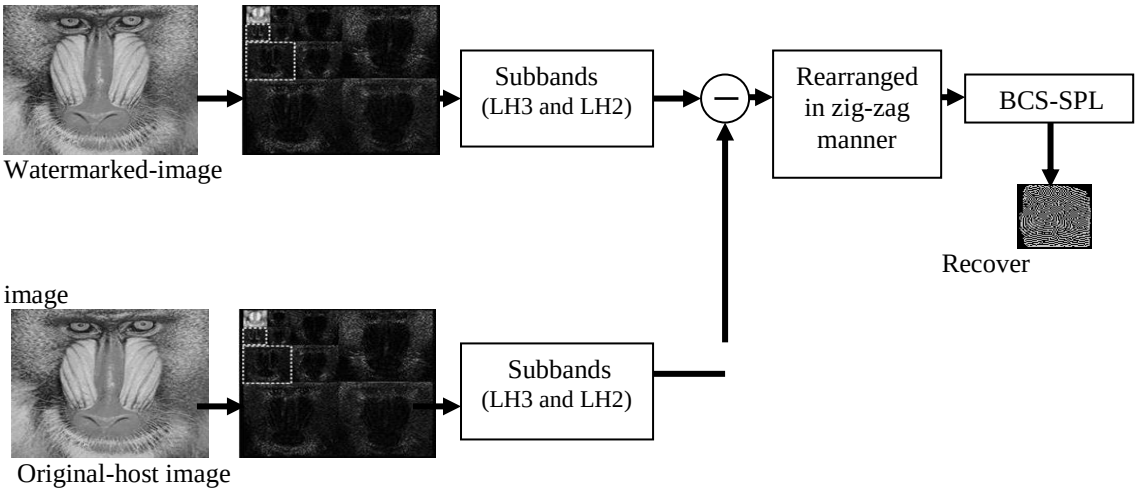


Figure 4. Detection Process of Hidden Information

3. Computer Simulation Results

The Figures 5 and 6 show watermarked image (512 x 512) with different size of hidden information and extracted image. Here, information extracted is fingerprint image, and it can be recovered by BCS-SPL algorithm in [14]. In the Figure 5, hiding information (watermarks) are 8-bits gray-scale images with different size (64x64, 96x96 and 128x128), and in the Figure 6, hiding information are binary pattern. Total number of Significant Trees detected in subbands LH_3 and LH_2 of the original image is 3602, which means the embedding capacity without truncate amount of data of the CS-watermark is 60 x 60. The PSNRs of the watermarked images are approximately 41 dB (41.2, 40.8 and 40.7 respectively, for gray-scale watermark and 41.5, 40.9 and 40.8 for binary watermark). The Figure 7 shows the

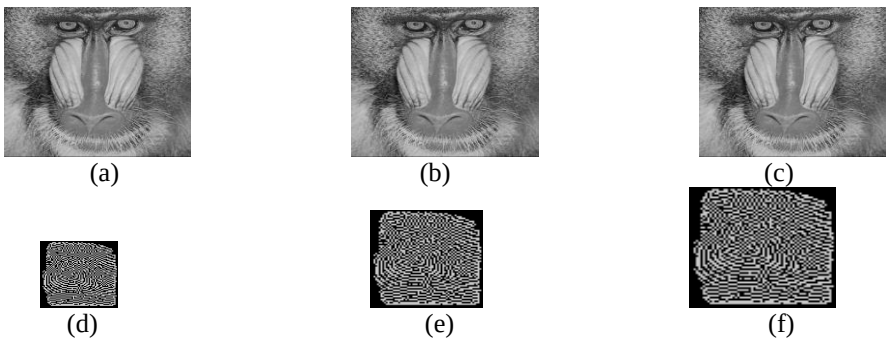


Figure 5. (a),(b),(c) are Watermarked Image with Different Size of Gray-Scale Fingerprint Information. (d) is Extracted Information (64x64) from (a), (e) is

Extracted Information (96x96) from (b), and (f) is Extracted Information (128x128) from (c).

relations between degradation of the watermarked image respect to the original one and watermark pattern size when median filters are applied to the watermarked image, and compares with DWT and DCT watermarking algorithm when amount of embedded information are of equal values in [8-9], respectively. From the figures, we can observe that watermarked images suffered minimum distortion in spite of the large size of the watermark.

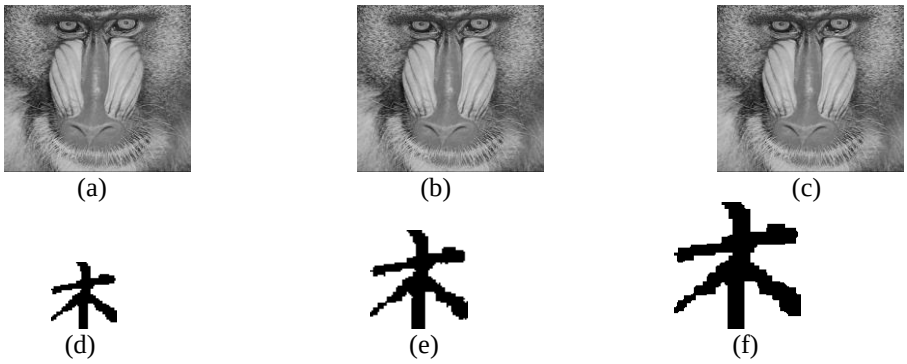


Figure 6. (a),(b),(c) are Watermarked Image with Different Size of Binary Watermarks. (d) is Extracted Watermark (64x64) from (a), (e) is Extracted Watermark (96x96) from (b), and (f) is Extracted Watermark (128x128) from (c).

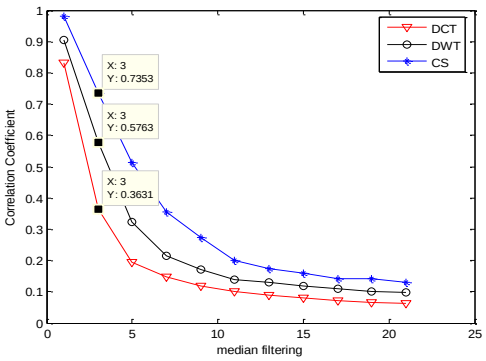


Figure 7. Relation between PSNR of the Watermarked Image and Watermark Pattern size when Median Filters are Applied to the Watermarked Image.

The Figures 8 and 9 show robustness of the proposed algorithm, when JPEG compression is applied to the watermarked image. In the Figure 8, hiding information is 8-bits gray-scale fingerprint image, and in the Figure 9, hiding information is binary image. In both cases, size of hiding information is 64 x 64. Figure 10 shows the normalized correlation (NC) of original fingerprint and extracted one, when JPEG compression ratio is changed.

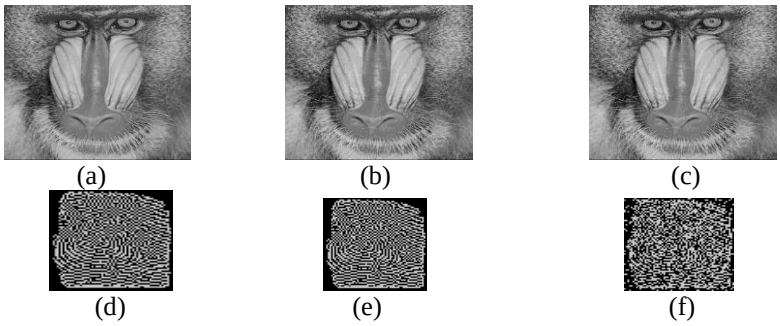


Figure 8. Robustness Against JPEG Compression, (a), (b) and (c) are Watermarked Compressed Images by JPEG Compression with Quality factor 80, 40, 20, Respectively, and (d), (e) and (f) are Extracted Information from (a), (b) and (c), Respectively.

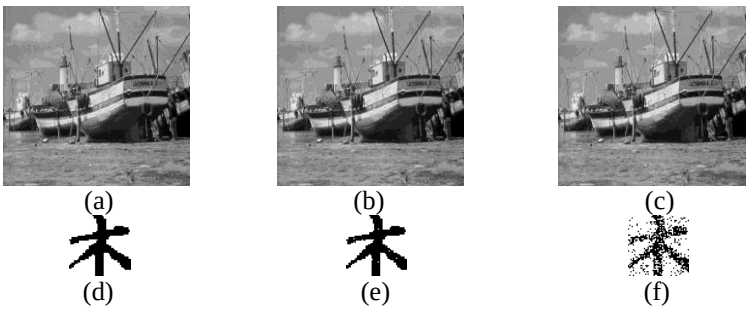


Figure 9. Robustness against JPEG Compression, (a), (b) and (c) are Watermarked Compressed Images by JPEG Compression with Quality Factor 80, 40, 10, Respectively, and (d), (e) and (f) are Extracted Watermark from (a), (b) and (c).

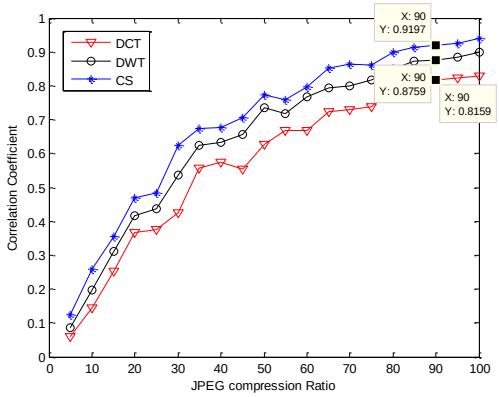


Figure 10. Relation between Compression Rate and Normalized Correlation (NC) of Extracted Fingerprint and Original One

The Figures show that embedded information survived after high ratio JEPG compression, the gray-scale information survived after compression with compression ratio 15.4 (it is equivalent to quality factor 20), and binary information survived after compression with it's ratio 22.1 (it is equivalent to quality factor 10) .

The Figure 11 shows cropped watermarked image and extracted binary information. We can observe the proposed algorithm is also robust to cropping operation.

(a) (b) (c)

Figure 11. (a) Original Image, (b) Watermarked and Cropped Image and (c) Extracted Binary Image.

4. Conclusion

In this paper we proposed an information hiding scheme BCS-based in DWT domain, in which hiding information is perceptual significant gray-scale fingerprint image or binary image. In the proposed scheme, size of the hiding information (watermark) is not limited, due to the application of BCS. Imperceptibility of the watermarked image can be controlled by the CS measurement values of the image. The proposed scheme is robust for some common attacks, such as JPEG compression, corruption by noise, *etc*.

In the information extraction process, the original unmarked image is required, but information about the watermark such as sorting order, *etc*. is not necessary.

Acknowledgments

This work was supported by the National Natural Science Foundation of China (61272381), Major Project of Education Department of Guangdong Province (2014KZDXM060), Science and Technology Project of Education Department of Guangdong Province (2013KJCX0118), Science and Technology Project of Guangzhou (2014J4100078).

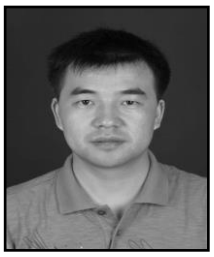
References

[1] N. Nikolaidis and I. Pitas, “Copyright protection of images using robust digital signatures”, Proc. IEEE ICASSP’96, (1996), pp. 2168-2171.
[2] M. Swanson, B. Zhu and A. Tewfik, “Robust Data Hiding for Images”, Proc. IEEE Digital Signal Processing Workshop, (1996), pp. 37-40.
[3] Z. Dazhi, W .Boying, Jiebao , H. Heyan, “A New Robust Watermarking Algorithm Based on DWT”, 2nd International Congress on Image and Signal Processing, (2009) Oct., pp.1-6.
[4] Tianyu Ye, “A Robust Watermarking Algorithm Based on Parity Resistant to Common Signal Processing and Desynchronization Attacks”, 2010 International Conference on Broadcast Technology and Multimedia Communication , IEEE Press, (2010), pp.422-425.
[5] C.Wang, J. Ni, J. Huang, “An Informed Watermarking Scheme Using Hidden Markov Model in the Wavelet Domain”, IEEE Transactions on Information Forensics and Security, Vol. 7, No. 3, (2012) June, pp.853-867.
[6] B. Corona, M. Nakano, H. Pérez, “Adaptive Watermarking Algorithm for binary Image Watermarks”, Lecture Notes in Computer Science, Springer, (2004), pp. 207-215.
[7] S. D. Lin, C.F. Chen, ”A Robust DCT-Based Watermarking for Copyright Protection”, IEEE Trans on Consumer Electronics, Vol.46, No.3,(2001), pp.415-421.
[8] Ali Al-Haj, “Combined DWT-DCT Digital Image Watermarking”, Journal of Computer Science , Vol.3, No.9, (2007), pp. 740-746.
[9] Z . Dazhi, W. Boying, S. Jiebao, H. Heyan, “ A New Robust Watermarking Algorithm Based on DWT,” 2nd International Congress on Image and Signal Processing, (2009) Oct.,pp:1-6.
[10] Z. Yigang, and L. Jia, “Blind Watermarking Algorithm Based on DCT for Color Images”, 2nd International Congress on Image and Signal Processing, (2009) Oct., pp.1-3.
[11] E.Candes, J.Romberg, Terence Tao, “Robust uncertainty principles: Exact signal reconstruction from highly incomplete frequency information”, IEEE Trans. On Information Theory,vol.52, no.2, (2006), pp:489-509.
[12] D.L.Donoho, Y.Tsaig, “Extensions of compressed sensing”, Signal Processing. vol.86, no.3, (2006), pp.533-548.
[13] C. Zhao, W. Liu, “Block Compressive Sensing Based Image Semi-fragile Zero-watermarking Algorithm”, Acta Automatic Sinica, Vol. 38, No. 4, (2012) April, pp.609-617.

[14] S. Mun and J. E. Fowler, "Block compressed sensing of images using directional transforms", in Proceedings of the International Conference on Image Processing, Cairo, Egypt, (2009) November, pp. 3021–3024.
[15] L. Gan, "Block compressed sensing of natural images", in Proceedings of the International Conference on Digital Signal Processing, Cardiff, UK, (2007) July, pp. 403–406.
[16] T. T. Do, T. D. Tran, and L. Gan, "Fast compressive sampling with structurally random matrices", in Proceedings of the International Conference on Acoustics, Speech, and Signal Processing, Las Vegas, NV, (2008) March, pp. 3369–3372.

Authors

HuiMin Zhao, he was born in Shanxi, china, in 1966. He received the B.S. and the M.Sc. degree in signal processing in 1992 and 1997 from Northwestern Polytechnical University, Xian, China, respectively. He received the Ph.D. degree in electrical engineering from the Sun Yat-sen University in 2001. At present, he is a professor of the Guangdong Polytechnic Normal University. His research interests include image, video and information security technology. E-mail: zhaohuimin@gdin.edu.cn



Jun Cai, he received the B.S degree from Hunan normal university, Changsha, China, the M.S degree from Jinan University, Guangzhou, China, and the Ph.D. degree from Sun Yat-Sen University, China in 2003, 2006 and 2012, respectively. He is currently an instructor with the School of Electronic and Information, GuangDong Polytechnic Normal University, Guangzhou, China. Complex network, traffic modeling and anomaly detection have been of particular interest over recent years. E-mail: gzhcaijun@gmail.com

Li Zhu, she was born in Guangxi, china, in 1969. She received the B.S. degree in pressure processing from Northwestern Polytechnical University, China, in 1991, and the M.S. degree in Engineering Computer Technology, Guangdong University of Technology, China, 2007. At present, she is a senior engineer of the Guangdong Polytechnic Normal University. Her research interests include multimedia processing, computer vision and information security technology. E-mail: zhuli@gdin.edu.cn

