On the Robustness with Secure Video Watermarking Data via Compressed Sensing

L.F. Cai
Guangdong Engineering Polytechnic
Guangdong, China

H.M. Zhao, W.G. Wei
School of Electronic and Information, Guangdong
Polytechnic Normal University
Guangdong, China

Y.M. Fang
School of Information Science and Technology, Sun Yat-sen University
China

Abstract—**In video information hiding processes, the security and robustness of watermarking data are two important performances. Based on the generation of robust watermarking signal, this paper proposes a secure video information hiding solution for protecting fingerprint content. In our proposed method, construction of the fingerprint watermarking signal is obtained by the compressed sensing (CS) measurements relies on the knowledge of the measurement matrix used for sensing, in which the pseudo-random sensing matrix can offer a natural method for the secret key. Our analysis and results indicate that the proposed fingerprint hiding system can possess a better robustness, and the watermarking data has a higher security.**

Keywords-robustness; watermarking; compressed sensing; security

I. INTRODUCTION

Digital watermarking is the process for hiding some secret information in a carrier signal [1]. In video information hiding field, the hidden data should be recoverable even after the host has undergone standard transformations, such as compression, noise, and attack [2], [3]. Since a video is formed from a sequence of frames, it presents the data owner with the possibility to embed and send a large amount of watermarking data. Therefore, the video watermarking security and robustness have emerged as the domain of extensive research in recent years, especially for the e-commerce and the cloud application [4].

Compressed sensing (CS) theory has been developed recently and has provided a suitable method for identifying the best relation between the security and robustness as described in [5,6,7]. Based on the CS theory, Zhao *et al.* [8] proposed an image semi-fragile watermarking algorithm, where the measurement values of CS are registered as the zero-watermarking, and can recover the tampered image with the watermarking information. Wang *et al.* [9] has proposed a secure image retrieval system through random projection in CS domain. In our previous work [10], we investigated a generation form of the video watermarking signal, and proposed a method of tampering detection of the video content in spatial domain.

These works indicate that signal processing or watermarking data-mining in the CS domain is feasible and is computationally secure under certain conditions.

Based on the above description methods, in this paper, we investigate the security of CS with robust watermarking signal. The security of our proposed method relies on the fact that the sensing matrix is not known to an attacker who does not have the pseudo-random key used to generate the matrix. Our experiment results indicates that the CS-based watermarking signal is computationally secure against the some attacks, i.e., compression, noise, and brute tampering attacks.

The rest of this paper is organized as follows. Section 2 presents our proposed method about the CS-watermarking data. Section 3 describes the embedding and extraction of our proposed method for the CS-watermarking data. Section 4 shows the experimental results for fingerprint watermarking, and demonstrates the effectiveness of the proposed the scheme. Finally, we give our conclusion in section 5.

II. THE WATERMARKING DATA CS-BASED

In the scheme presented, we divide firstly the original fingerprint watermark image into a lot of non-overlapping blocks, in which blocking criteria of the image is jointly decided by size of the watermarking signal and positioning accuracy of the watermarking as extraction and recover purpose. Next, each block of the image is carried out by a sparse basis matrix in which we use DCT as the sparse basis Ψ, and form various DCT coefficients blocks. Simultaneously, measurement matrix Φ_B of the block compressed sensing (BCS) is deployed to sense these DCT coefficients independently within each block based on [8]. The process is simply random linear projection, and can be achieved by inner product operation of corresponding two elements between Ψ and Φ_B. Here, according to the principle of CS theory in [6,7], selection of Φ_B is incoherent with Ψ. By considering that the sparse basis Ψ is a type of DCT matrix in our method, we can solve the constraint by designing an appropriate measurement matrix Φ_B in [8]. Finally, the watermarking data is produced by combining the all sampling values of measurement matrix Φ_B. The realization principle of the watermarking data is shown in fig.1.

In fig.1, assume that an original gray watermarking image is size of $N = N_1 \times N_2$, in which N_1 and N_2 denote rows and columns (both N_1 and N_2 are multiples of 8), respectively. We segment the watermarking image into nonoverlapping 8×8 pixel blocks, and denote the pixels as $x_k(i, j)$, where $1 \le k \le N/64, 1 \le i \le 8$ and $1 \le j \le 8$.

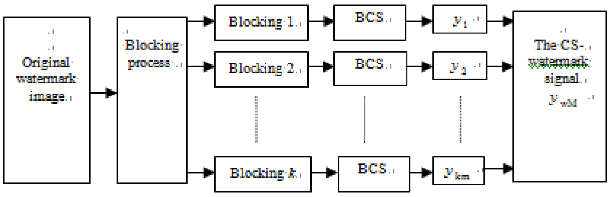


FIGURE I. GENERATING OF THE CS-WATERMARK SIGNAL

Then, perform DCT in *k*th block to yield the DCT coefficients

$$C_k(u,v) = \frac{C(u)C(v)}{4} \sum_{i=1}^{8} \sum_{j=1}^{8} x_k(i,j) \cos\frac{(2i-1)\pi u}{16} \times \cos\frac{(2j-1)\pi v}{16} \tag{1}$$

where $1 \le u \le 8, 1 \le v \le 8$, and

$$C(u) = C(v) = \begin{cases} 0.707, & for \quad u = v = 0 \\ 1, & for \quad u = v \ne 0 \end{cases} \tag{2}$$

By zig-zag scanning, the 64 coefficients of each block are rearranged as vector

$$V_k(u,v) = [C_k(1,1), C_k(1,2), C_k(2,1), \ldots, C_k(2,2), \cdots, C_k(8,8)]^T \\ k = 0,1,..,N/64 \tag{3}$$

Thus, a one-to-one mapping relationship between the *k* reference values set and *k* image blocks is then established in DCT domain. For the size 8×8 of each block-group, we quantize the reference values in a non-uniform manner.

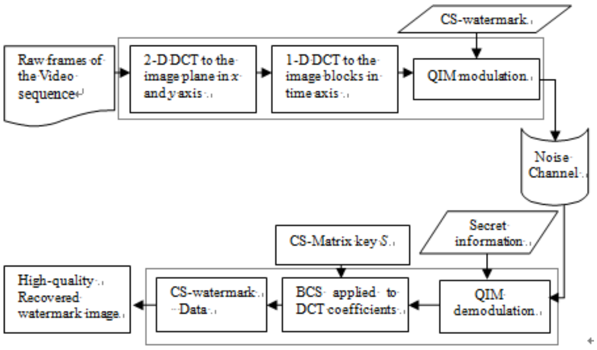
By the quantization, $V_k(u,v)$ of each block values is converted into an integer within [0, 1]. Suppose total pixels of the watermarking signal hidden are *M*, then, the sizes of the measurement samples of each block of the watermark image are $m = \lfloor M \cdot B^2 / N \rfloor$. If the measurement samples of block *l* are $y_l(i, j)(l = 1,2,\ldots,k)$, then all measurement samples of each block will be composed to a form of the watermarking signal in the CS domain, as shown in (4). Usually, the elements of Φ_B in (4) are binary, then values of the watermark

$$y_{wM} = \Phi x = \begin{bmatrix} \Phi_B & & & \\ & \Phi_B & & \\ & & \ddots & \\ & & & \Phi_B \end{bmatrix} \begin{bmatrix} C_1(u,v) \\ C_2(u,v) \\ \vdots \\ C_k(u,v) \end{bmatrix} = \begin{bmatrix} y_1 \\ y_2 \\ \vdots \\ y_{km} \end{bmatrix} \\ = [w_1, w_2, \ldots, w_M]^T \tag{4}$$

signal $w_M \in [0,1], M = km.$ As described above, if we have selected an appropriate measurement matrix Φ corresponding the sparse basis Ψ DCT-based, the measurement samples of the image can express all features of the original watermarking image in DCT-CS domain, so we can take the measurement samples as the watermark signal that is called the CS-watermarking data in this paper.

III. EMBEDDING AND EXTRACTION OF THE CS-WATERMARKING DATA IN VIDEO STREAM

In the paper, we have established a video information hiding system with CS-watermarking data as in fig.2.



CS-watermark
Raw frames of the Video sequence
2-D DCT to the image plane in x and y axis
1-D DCT to the image blocks in time axis
QIM modulation
Noise Channel
CS-Matrix key S
Secret information
High-quality Recovered watermark image
CS-watermark Data
BCS applied to DCT coefficients
QIM demodulation

FIGURE II. SKETCH OF THE CS-WATERMARKING PROCEDURE

Firstly, in fig.2, we take four consecutive frames as a group, and every frame within a group is divided some blocks. And then, according to the algorithm of H.Huang proposed in [11], the DC value of each block located in the same position of successive frames for a group is transformed into the DCT domain again. After transforming the second DCT process, we will obtain a new DC value and several AC values. Thus, we embed the CS-watermarking data into these AC values, and can extract the CS-watermarking data based on the principle of embedding and extraction in fig.2. We achieve the video hiding process with the CS-watermarking data by QIM in [12]. The detailed process of in fig.2 refers to the description combining [11] and [12].

IV. EXPERIMENT PROCESS AND RESULTS

A. *Experiment Objects*

In our experiment, the watermark image is denoted by a gray level fingerprint with the size 160×160. Before experiment, we captured the fingerprint image from sensor FPS110 of Verdicom Inc., and preprocessed the image by binaryzation method.

For video signal, experiment used Basketball and Scene videos stream for demonstration, respectively. The size of each video is 720×480, and every video consists of 80 frames. We take four successive frames as a group and each frame is divided into numbers of 8×8 blocks, which is the same method with process of the fingerprint image by using (6). Meanwhile, in order to find the obvious comparison result, the watermarking data of the fingerprint image are also generated by DCT method of H.Huang *et al.* [11] and SVD method of W.Kong *et.al* [13], respectively.

B. *Performance Measurement*

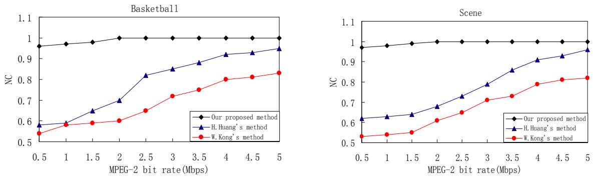
In our experiment, a measure of the normalized correlation (*NC*) used for calculating the difference between the extracted the CS-watermarking $\hat{W}(i, j)$ in receiver side and the original CS-watermarking $W(i, j)$ in sender side. *NC* is defined in equation (5). In (5), *N* denotes the size of the watermark image, and N_1 and N_2 are the height and width of one image.

$$NC = \frac{\sum_{i=1}^{N_1}\sum_{j=1}^{N_2} W(i,j)\hat{W}(i,j)}{\sum_{i=1}^{N_1}\sum_{j=1}^{N_2} [W(i,j)]^2} \tag{5}$$

C. *Experiment Results*

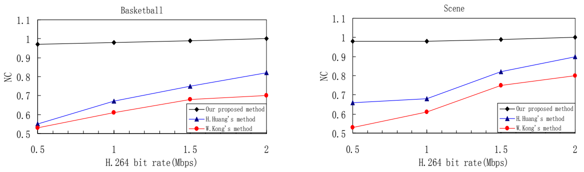
Robustness of the proposed method has been tested through simulation of the following under various conditions.

1)Compress process: We use MPEG-2 and H.264 compression to evaluate the robustness of the information hiding system. Figures 3-4 show the results after those of compressions under the different bit rates compared with our method, Huang *et al.*'s method, and Kong *et.al*'s method. Obviously,after embedded watermark, the hiding data can almost be extracted even though the bit rate is as low as 0.5Mbps.



(a) (b)

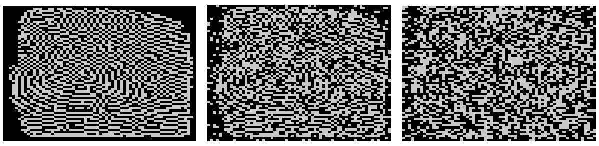
FIGURE III. COMPARISON RESULTS UNDER THE DIFFERENT MPEG-2 BIT RATES. WATERMARKED BASKETBALL; (B) WATERMARKED SCENE



(a) (b)

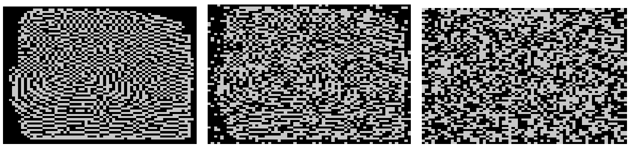
FIGURE IV. Comparison results under the different H.264 bit rates. (a) Watermarked Basketball; (b) Watermarked Scene.

2) Recovered fingerprint image after filtering and noise attacks: In order to study deeply the robustness of the information hiding system, we consider also various intentional or unintentional attacks, such as Gaussian noise (mean zero and variance 0.05) and "pepper & salt" (density 0.1) attacks. Figures 5-6 present the experimental results of the watermark image recovered from Basketball video stream by three methods after various attacks. From these results, we can understand no matter what the attacks are, the NC values of the fingerprint image recovered from our proposed hiding system can still exceed 0.998, and the image can reconstruct with higher quality than the methods of Huang and Kong *et al*.



(a) (b) (c)

FIGURE V. COMPARISON RESULT AGAINST GAUSSIAN NOISE ATTACK FOR BASKETBALL VIDEO. (A) OUR PROPOSED METHOD, NC=1; (B) H.HUANG'S METHOD, NC=0.862; (C) W.KONG'S METHOD, NC=0.766



(a) (b) (c)

FIGURE VI. COMPARISON RESULT AGAINST PEPPER&SALT NOISE ATTACK FOR BASKETBALL VIDEO. (A) OUR PROPOSED METHOD, NC=0.998; H.HUANG'S METHOD, NC=0.761; (C) W.KONG'S METHOD, NC=0.595

D. *Security Analysis of the CS-watermarking Data*

Signal processing of CS technique is itself an encryption process, and the process can provide an effective security of compression and encryption for the signal, in which the encryption does not need any extra computational cost caused from other encryption protocol [2]. In the process of the encryption, measurements matrix of CS can be regarded as a realization form of secure and reliable key. Therefore, security of the information hiding system based CS-watermarking data can be decided by the encryption property of measurement values of CS, in which random elements of measurements matrix decide the measurement values property with random noise.

V. CONCLUSIONS

In this paper, we have proposed a secure and robust video information hiding system based on the CS-watermarking data for protecting fingerprint image. The CS-watermarking data is generated by measurement values of CS block-based which can express all features of the original fingerprint image, and the measurement values itself possess an encryption property from random elements of sensing matrix. Therefore, the CS-watermarking data has higher security than traditional methods achieved by scrambling and random process. In further, we will research deeply information forensics by CS theory.

ACKNOWLEDGMENTS

This work was supported by the National Natural Science Foundation of China (61272381), Natural Science Foundation of Guangdong of China (S2012010008639), Science and Technology Project of Education Department of Guangdong Province (2013KJCX0118), Science and Technology Project of Guangzhou (2014J4100078).

REFERENCES

[1] Feng Ji, Dongyu Huang, Cheng Deng, Yifan Zhang, and Wen Miao, Robust curvelet-domain image watermarking based on feature matching, International Journal of Computer Mathematics, 88(18),pp.3931-3941, 2011.

[2] Orsdemir, A., Altun, H., Sharma,O. G., and Bocko,M.F., On the security and robustness of encryption via compressed sensing,*IEEE Military Communications Conference*, pp.1040- 1046, 2008.

[3] Zhang, X., Qian, Z., Ren,Y., and Feng, G.,Watermarking with flexible self-recovery quality based on compressive sensing and compositive reconstruction. *IEEE Transaction on Information Forensics and Security,* 6(4), pp.1223-1232, 2011.

[4] Wang, Q., Zeng, W., and Tian, J.,Integrated secure watermark detection and privacy preserving storage in the compressive sensing domain. *IEEE International Workshop on Information Forensics and Security*, Guangzhou, China, pp. 67-72, 2013.

[5] Abdulfetah, A., Sun, X., and Yang, H., Robust Adaptive Video Watermarking Scheme using Visual models in DWT domain. Information Technology Journal, 9(7),pp. 1409-1414,2010.

[6] Candes, E., Romberg, J., Terence Tao., Robust uncertainty principles: Exact signal reconstruction from highly incomplete frequency information. *IEEE Trans. On Information Theory*, 52(2),pp.489-509, 2006.

[7] Donoho, D.L., Tsaig, Y.,Extensions of compressed sensing . *Signal Processing,* 86(3), pp.533-548, 2006.

[8] Zhao, C.H., LIU W., Block Compressive Sensing Based Image Semi-fragile Zero-watermarking Algorithm. Acta Automatica Sinica , 38(4), pp.609-617, 2012.

[9] Tao Wan, Zengchang Qin. An application of compressive sensing for image fusion, International Journal of Computer Mathematics, 88(18), pp.3915-3930, 2011.

[10] Zhao, H.M., Lai, J.H., Cai, Jun., Chen, X.L., A Video Watermarking Algorithm for Intraframe Tampering Detection Based Compressed Sensing. Acta Electronica Sinica, 41(6), pp.1153-1158, 2013.

[11] Huang, H.Y., Yang, C.H., Hsu, W.H., A Video Watermarking Technique Based on Pseudo-3-D DCT and Quantization Index Modulation, *IEEE Transactions On Information Forensics and Security*, 5(4), pp.625-627,2010.

[12] Seo, Y.S., Kim, W.G., Huh, Y.H., Oh, W.G., and Hwang, C.J., QIM watermarking for image with tow adaptive quantization step-sizes. *In Proc. 9th Int. Conf. Advanced Communication Technology*, pp.997-800, 2007.

[13] Kong, W., Yang, B., Wu, D., and Niu, X., SVD based blind video watermarking algorithm. I*n Proc. First Int. Conf.* Innovative Computing, Information and Control, pp. 265-268, 2006.