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 $\Psi$, and form various DCT coefficients blocks. Simultaneously, measurement matrix $\Phi_B$ 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 $\Psi$ and $\Phi_B$. Here, according to the principle of CS theory in [6,7], selection of $\Phi_B$ is incoherent with $\Psi$. By considering that the sparse basis $\Psi$ is a type of DCT matrix in our method, we can...
solve the constraint by designing an appropriate measurement matrix $\Phi_{\Psi}$ in [8]. Finally, the watermarking data is produced by combining the all sampling values of measurement matrix $\Phi_{\Psi}$. 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 $8 \times 8$ pixel blocks, and denote the pixels as $x(i, j)$, where $1 \leq k \leq N / 64,1 \leq i \leq 8$ and $1 \leq j \leq 8$.

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

$$C(u, v) = C(v) = \begin{cases} 0.707, & \text{for } u = v = 0 \\ 1, & \text{for } u = v \neq 0 \end{cases}$$

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

$$V_k(u, v) = [C_1(u, v), C_2(u, v), C_3(u, v), \ldots, C_{64}(8, 8)]$$

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 $8 \times 8$ of each block-group, we quantize the reference values in a non-uniform manner. Suppose total pixels of the watermarking signal hidden are $M$, then, 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].

**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.

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 $160 \times 160$. 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 \(8\times8\) 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 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.

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

(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.

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.

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, in which 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


