Cognitive Computation of Compressed Sensing for Watermark Signal Measurement

Huimin Zhao and Jinchang Ren

***Abstract*—As an important tool for protecting multimedia contents, scrambling and randomizing of original messages is used in generating digital watermark for satisfying security requirements. Based on the neural perception of high-dimensional data, compressed sensing (CS) is proposed as a new technique in watermarking for improved security and reduced computational complexity. In our proposed methodology, watermark signal is extracted from the CS of the Hadamard measurement matrix. Through construction of the scramble block Hadamard matrix utilizing a cryptographic key, encrypting the watermark signal in CS domain is achieved without any additional computation required. The extensive experiments have shown that the neural inspired CS mechanism can generate watermark signal of higher security, yet it still maintains a better trade-off between in transparency and robustness.**

***Index Terms*— Cognitive computation; digital watermark; compressive sensing (CS); measurement matrix; discrete cosine transform (DCT); scrambled block Hadamard matrix (SBHM).**

I. Introduction

Digital watermark is an important secret communication technology being developed for multimedia services, where the owner, for retrieval only by those authorized, embeds significant amounts of hidden data into a host data source. The hidden data should be recoverable even after the host has undergone standard transformations, such as compression and noise [1], [2]. For satisfying the security requirements, conventional approaches need have the watermark signal scrambled and randomized before embedding them into the host data source. In [3], J. Cox *et al*. showed a basic implementation in frequency domain, in which a watermark signal consists of a spread spectrum (SS) sequence of real numbers $X = x_1, \cdots, x_n$, and each value x_i is constructed from independent, identically distributed (I.I.D.) samples drawn from a Gaussian distribution. To increase the security of the watermark signal, G.Voyatzis *et al*. [4] proposed a type of watermark signal construction method based on chaotic system and cryptography principles in the spatial domain. Let *X*, *W* and *K* be three sets, representing digital product to be protected, the watermark signal, and secret keys, respectively, the watermark algorithm *G* can be defined as follows in [4]:

$$G = T \cdot R, \qquad R : K \to W, \qquad T : W \times X \times K \to W \tag{1}$$

Here, *R* is controlled by a pseudo random generator, and *K* maps directly to a type of seed of the pseudo random generator, such as Logistic mapping. While *R* is regarded as a chaotic system, *K* is formed by certain transforms with many initial conditions. Under these conditions, the set of *K* needs to be large enough, and satisfy a uniqueness condition as requested by the watermark signal. Fig. 1 shows a general process how the image watermark signal is generated.

As seen in Fig.1, in conventional scheme, for the generation of the image watermark signal, the original watermark image must be firstly sampled by using some complete transformations, such as Fourier Transform (FT), discrete cosine transform (DCT), discrete wavelet transform (DWT), and singular value decomposition (SVD) [5]. One interesting approach introduced in [6] applies DFT on predefined disks rather than image blocks, where the disk centers are determined as the feature points using scale invariant feature transform (SIFT). However, block based transform is widely used for its easy implementation.

Afterwards, all coefficients of the transformed image need be scrambled and encrypted, using approaches such as the Arnold and Fibonacci Q method [1]. As the original watermark image needs to be sampled and scrambled by a convolution form of some matrix in a nonlinear way, a high degree of data redundancy can be identified in the transformed watermark signal [7]. On one hand, this increases the capacity of the embedded watermark signal. On the other hand, the additional hidden information (watermark) to be embedded may become difficult or even impossible to be extracted due to the distortion of the transform domain coefficients [8].

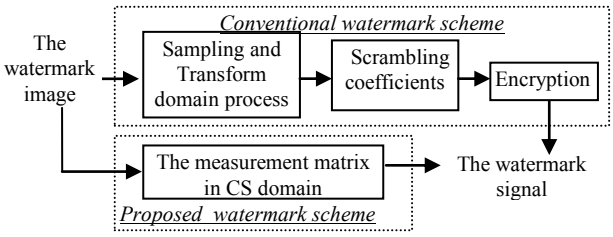


Fig.1. Comparison of conventional watermark scheme and our proposed one in the CS-domain.

When the dimensionality of the data increases, the task to model and identify statistical relationships between the data patterns becomes significantly difficult, and this phenomenon is called the curse of dimensionality [9]. To address this challenge, compressed sensing theory (CS) is proposed recently as it helps to achieve centripetal sensing and compression of sparse signals. Due to a simple linear measurement step used, it is found that CS is particularly useful in simulating the neural perception mechanism of our human brains in effectively dealing with multidimensional data [11-12]. As shown in Fig. 2, the vision system of our brain actually contains a multi-stage compressed sensing mechanism. The first stage is from object to optic nerve, where the data rate has been reduced from 10^9 to 10^7 bits per second (bps) [13-14]. In the next stage of compressed sensing, the date rate has been further reduced to 10^2 bps when it reaches the visual cortex yet still maintains the essential information. This has demonstrated the efficacy of sparse coding networks in CS in maximizing the coding efficiency [11, 15, 16].

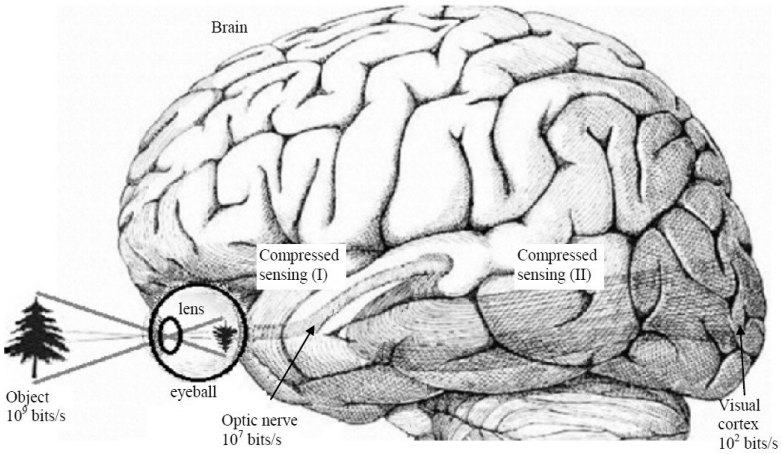


Fig. 2. How compressed sensing (CS) has been embedded in our brain when vision perception is achieved.

By applying CS to watermark, it has provided the best trade-off between the security and robustness of watermark signal [17-19]. Orsdemir *et al* [17] found that CS measurement matrix had pseudo-random entries, and could be achieved by using a cryptographic key shared between the sender and receiver. In [19], Lu *et al* proposed a secure image retrieval system through random projection in CS domain. As shown in [20] and [21], many signal processing algorithms performed in the CS domain had very close performance as those in the original domain. Based on the measurement matrix of CS, Zhao *et al.* [22] proposed an image semi-fragile watermarking algorithm, in which the measurement values of the CS were registered as the zero-watermark signal and used to recover the tampered image with the watermark signal. In [23], Zhang *et al* proposed a novel watermarking scheme, using a CS technique to retrieve the coefficients by exploiting the sparseness in the DCT domain. In [24], Wang and Zeng *et al*. proposed a scheme of integrated secure watermark detection and privacy preserving storage in the CS domain, in which multimedia data and the watermark signal were presented to the cloud for secure watermark detection in a CS domain to protect the privacy. In our previous work [25], based on the CS theory, a spatial domain approach with a deterministic measurement matrix was presented for watermarking generation and intraframe tampering detection. However, in this paper we have introduced CS domain Hadamard measurement matrix to cope with the sparsity level of the input signals.

The emerging theory of CS indicates that CS-based watermark models can be used to simplify the acquisition of high-dimensional signals that might otherwise be difficult to collect or encode. Rather than collecting an entire ensemble of signal samples, CS requires only a small number of random linear measurements, with the number of measurements proportional to the sparsity level of the signal. As a result, signal processing or watermarking data-mining in the CS domain is feasible and computationally secure under certain conditions.

Inspired by the theory of CS, a new watermark scheme is introduced in this paper. It is our aim to establish a novel secure information hiding system by utilizing the watermark signal measured from the CS Hadamard matrix which can express all features of the original watermark signal and possess itself an encryption property from random elements of the Hadamard matrix that encryption occurs implicitly in the sensing process-*without requiring additional computation*. With the proposed CS-domain watermark scheme, as compared in Fig. 1, our scheme has several advantages: Firstly, most of the existing watermarking scheme paid little attention to security of the watermark signal, while our scheme improves the security. Second, watermarking data-mining in the CS domain is feasible with measurement values and posses computationally better transparency under certain statistical conditions. Third, with watermarking data measured in received side, original watermark signal can be constructed high probability.

The remaining paper is organized as follows: Section II gives some related works for CS. The proposed CS-watermark scheme is presented in detail in Section III. Section III discusses dataset description and experimental settings. Comprehensive results and discussions are reported in Section IV. Finally Section V concludes the paper.

II. Related Work for the CS Theory

When a signal can be represented by a small number of non-zero coefficients, the CS asserts that it can be perfectly recovered after being transformed by a limited number of incoherent, non-adaptive linear measurements [26-28]. Let a signal $f \in R^N$ be a K-sparse vector, i.e. only K out of the N elements of f are nonzero. If f can be transformed to $x \in R^M$ with $x = \Theta f$ and $M < N$, Θ is namely the sparse matrix. For image data Θ is usually chosen as the DCT and DWT. If Θ satisfies Restricted Isometry Property (RIP) [26-27], the sparse matrix can be obtained by solving the following optimization problem:

$$\min \| f \|_1 \qquad s.t. \qquad x = \Theta f \tag{2}$$

Actually, this process equals to finding the sparsest solutions to $x = \Theta f$, subject to $M \geq C_K \log(N/K)$, where $C_K = K/N \in (0,1)$ is a small constant which denotes the sparsity level of the input signal. The CS theory states that the sparse signal x can be reconstructed by using only M linear projection in a non-adaptive measurement as follows:

$$y = \Phi x = \Phi \Theta f \tag{3}$$

where y is an $M \times 1$ sampled vector, and Φ is an $M \times N$ measurement matrix that is incoherent with Θ, i.e., the maximum magnitude of the element in $\Phi\Theta$ is small.

In fact, Eq. (2) presents an $l1$ minimization problem, which can be solved by using the orthogonal matching pursuit algorithm [28]. For Eq. (3), if the entries of the matrix Φ are generated from a Gaussian distribution (zero mean and variance σ), Φ is a RIP matrix with overwhelming probability in [26-27]. The Gaussian CS matrix suits include the seeds and a random function.

It has been shown that it is feasible for many signal-processing algorithms to be performed in the CS domain [20-25]. In practical applications, an image sized of $N = N_1 \times N_2$ is divided generally into $B \times B$ blocks. For each block, ideally the size of the measurement matrix in CS domain needs be appropriately selected by considering the associated sparsity C_K. That is, assume that x_i is a sparse vector representing block i of the input image $x \in R^M, M < N$. The corresponding measurement sample y_i can be decided by

$$y_i = \Phi_B \cdot x_i \tag{4}$$

where the length of the signal y_i is m, and Φ_B is a $m \times B^2$ measurement matrix. For each image block, the numbers of measurement samples can be determined as $m = \lfloor M \cdot B^2 / N \rfloor$, where M is size of samples needed by the CS measurement for the whole image. In this way, Φ has a block-diagonal structure as given in (5). Therefore, the overall technique above was called block CS (BCS) [29].

$$\Phi = diag[\Phi_B] \tag{5}$$

III. The Proposed CS Watermark Scheme

In this section, detailed algorithm description is given to discuss how the proposed CS domain watermark scheme works in terms of signal measurement, measurement matrix construction and security analysis.

A. The measurement of the watermark signal

In the proposed watermark scheme, the original watermark image is firstly divided into same-sized non-overlapping blocks, in which blocking criteria of the watermark image is jointly decided by the size and positioning accuracy of the watermark signal as requested for extraction and recovery. Next, each block of the watermark image is transformed by a sparse basis matrix in which we use DCT as the sparse basis Ψ, and forms various DCT coefficients blocks. Meanwhile, measurement matrix Φ_B is deployed to sense these DCT coefficients independently within each block. This process is simply a 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 the CS theory [26-27], selection of Φ_B is incoherent with Ψ. As the sparse basis Ψ is a type of DCT matrix, we can solve the constraint by an appropriate measurement matrix Φ_B. We will discuss the designing of Φ_B in a later subsection. Finally, the watermark signal

y_{wM} is generated by combining the sampling values from the measurement matrix Φ_B of each image block.

Assume the total numbers of pixels of the original gray watermark image is $N = N_1 \times N_2$, in which both N_1 and N_2 are multiples of *B*, denoting the number of rows and columns, respectively. We segment the watermark image into K_0 non-overlapped $B \times B$ pixel blocks, and denote the pixels as $x_k(i, j)$, where $1 \le k \le K_0 = N / B^2$ and $0 \le i, j \le B-1$.

For the *k*th image block x_k, $k \in [1, K_0]$, its DCT results with $B = 8$ is denoted as ω_k, whose 64 coefficients are rearranged as a vector V_k by using a zigzag scanning, i.e.

$$V_k = [\omega_k(0,0), \omega_k(0,1), \cdots, \omega_k(7,7)]^T \tag{6}$$

For the re-organized 64 DCT coefficients in V_k, they are quantized in a non-uniform manner below to map them into integers within [-64, 63].

$$Q_k(t) = \begin{cases} 63, & if \quad V_k(t) \ge f_{63} \\ t, & if \quad f_t \le V_k(t) < f_{t+1} \\ -t-1, & if \quad -f_{t+1} \le V_k(t) < -f_t \\ -64, & if \quad V_k(t) < -f_{63} \end{cases} \tag{7}$$

where $f_t = \dfrac{t}{6} + \dfrac{t^2}{300}$ with $t \in [0,63]$.

Let *M* represent the total size of samples of the watermark signal measured in CS domain, the size of the measurement samples for each image block of the original watermark image is $m = \lfloor M / K_0 \rfloor$ or $\lfloor M / K_0 \rfloor$. If the measurement samples of block *l* are $y_l(i, j)(l = 1,2,...,K_0)$, measurement samples of each block are then put together to form the watermark signal in the DCT–CS domain, as given by

$$\begin{aligned} \mathbf{Y}_{wM} = \mathbf{\Phi X} &= \begin{bmatrix} \Phi_B & & & \\ & \Phi_B & & \\ & & \ddots & \\ & & & \Phi_B \end{bmatrix} \begin{bmatrix} Q_1(u,v) \\ Q_2(u,v) \\ \vdots \\ Q_k(u,v) \end{bmatrix} = \begin{bmatrix} y_1 \\ y_2 \\ \vdots \\ y_{K_0} \end{bmatrix} \\ &= [w_1, w_2, ..., w_M]^T \end{aligned} \tag{8}$$

Usually, the elements of $\mathbf{Y}_{\mathrm{wM}}$ in (8) need be normalized to have $w_M \in [0,1]$ where $M = K_0 m$. If an appropriate measurement matrix Φ is selected corresponding to the DCT-based sparse basis Ψ, the measurement samples of the original image can represent all features in DCT-CS domain. As a result, we can take the measurement samples as the watermark signal, namely the CS-watermark signal in this paper. In other words, the CS-watermark signal shows inherent characteristics of the watermarking image by measurement samples, and the size of watermark signal *M* is far less than *N*, the length of the original watermark image. Consequently, the basis Ψ provides a *M* sparse representation of signal *x* (*M*<<*N*).

B. Construction of measurement matrix

Construction of the measurement matrix Φ in (5) and (11) is the most important factor in generating the CS-watermark signal. Cands *et al*. [28] have proved that Gaussian random matrix satisfied the RIP requirement under statistical condition. However, storage and transmission of this kind of matrix needs huge memory requirement and high computational complexity. For other options of deterministic measurement matrix, we have come over polynomial matrix [25], discrete Chirp matrix and Reed-muller codes matrix [30]. Unfortunately, the operators of these matrixes are not universal as they are only incoherent with the identity matrix.

Considering the security requirement of the information hiding with the robust CS-watermark signal, in this paper, we have proposed a new sampling operator called scrambled block Hadamard matrix (SBHM). In SBHM, Φ employs the partial block Hadamard transform and randomly permute its columns, hence we have a form of Φ as follows

$$\mathbf{\Phi} = U_M \Phi_{M \times N} V_N \tag{9}$$

where the matrix $\Phi_{M\times N}$ is a block diagonal matrix as in (4). Actually, $\Phi_{M\times N}$ represents the set of the block Hadamard matrix (BHM) Φ_B, where U_M is an operator which picks up *M* rows of $\Phi_{M\times N}$ at random, and V_N denotes a scrambling operator which randomly records the *N* columns of $\Phi_{M\times N}$. For satisfying the incoherent of Φ and Ψ, we compile a wish-list to show the construction criteria of Φ.

- Near optimal performance: The number of measurements for perfect reconstruction is close to the theoretic bound.
- Universality: Φ can be paired with a variety of sparse basis matrix Ψ for natural watermark images.
- Security: each element of $\Phi\Psi$ has scrambling and random coefficient, and is asymptotically normally distributed with zero mean and variance of N^{-1}.

Based on the criteria above, we map the elements of the BHM $\Phi_{M\times N}$ in Sylvester's form using the group homomorphism $\{1,-1,\times\}\mapsto\{0,1,\oplus\}$ as follows. Consider a rank *n* matrix H_n sized of $n\times 2^n$, whose columns consist of all *n*-bit numbers ascendingly arranged. Sylvester's Hadamard matrix H_n can then be recursively defined by

$$H_1=[0,1]$$
$$H_n=\begin{bmatrix}0_{1\times 2^{n-1}} & 1_{1\times 2^{n-1}}\\ H_{n-1} & H_{n-1}\end{bmatrix} \tag{10}$$

It can be inducted that the image of the Hadamard matrix above satisfies

$$H_{2^n}=H_n^T H_n \tag{11}$$

When $B=2^n$, we can obtain a form of BHM $\Phi_{M\times N}$ as

$$\Phi_{M\times N}=diag[\Phi_B]=diag[H_{2^n}] \tag{12}$$

This construction process shows that the rows of the BHM $\Phi_{M\times N}$ can be viewed as a linear error-correcting code of rank *n* (with a length 2^n), and the minimum distance 2^{n-1} with the generating matrix H_n. In addition, it is obvious that small *B* is advantageous for computational and storage efficiency. The bound of *B* can be further improved, as *B* can be actually very small ($B=2^4=4\times 4=16$) for image watermarking.

Besides, the block diagonal structure of $\Phi_{M\times N}$ enables its fast and parallel measurement at a complexity $O(N\log B)$ along with small memory requirement [29]. In addition, based on the combinatorial central limit theorem, we can even prove that, for the Φ given in (9) and a sparse basis Ψ based-DCT, let $\Phi_f=\Phi\Psi$, each element $\Phi_f(i,j)$ is asymptotically normally distributed with zero mean and variance of N^{-1}.

After determining $\Phi_{M\times N}$, for data security purpose, each element of the matrix needs to be scrambled. The sparse input signal sampled from the original image V_k is pseudo-randomly permuted in a chaotic way so that Φ is incoherent with Ψ based-DCT. However, in practice, for limited computational complexity, V_N cannot be selected as a pure random operator. Here, we will consider the method of linear congruential permutation (LCP) [18], which is a simple pixel level scrambler.

For an input vector $V_k(u,v)$, it outputs are determined as follows, where again $k\in[1,K_0]$ denotes the number of blocks:

$$V_n(u,v)=V_{V_k(u,v)},\ 0\le u,v\le 7 \tag{13}$$

$$V_k(u,v)=[A(u,v)\bmod 64],\quad A<64 \tag{14}$$

where *A* is a positive integer relative prime with *N*. Therefore, V_N ($N\in[0,K_0]$) can be restructured by

$$V_N=[V_1(u,v),V_2(u,v),...,V_n(u,v)]^T \tag{15}$$

where n denotes the total number of re-ordered coefficients obtained from all image blocks.

Because there is only one parameter *A* in (14), an LCP can be easily implemented for pixel-by-pixel scrambling. In addition, as U_M is an operator from *M* rows of $\Phi_{M\times N}V_N$ uniform at random in (9), we can save H_n, U_M and V_N as secret keys *S* with small memory requirement. This set of secret keys will further be applied to extract the CS-watermark signal at the receiver side.

Based on the analysis above, with the support of CS theory, the CS-watermark signal is generated. The time complexity of the CS-watermark signal depends on the size of the measurement matrix Φ. For each DCT block of the original watermark image, the time complexity for feature extraction is $O(mB^2)$ and thus the total time complexity for the whole image is $O(mN)$.

C. Security analysis of the CS-watermark signal

In the proposed scheme, measurement of CS technique itself is an encryption that occurs implicitly in the sensing process. This can provide an effective security of compression and encryption for the watermark signal, where the encryption does not need any extra computational cost. In the encryption process, measurements matrix of CS may be regarded as a realization form of secure and reliable keys. In [31], Y. Rachlin *et al*. proved that if an attack did not have a priori knowledge of the measurement matrix, it could only try all possible keys by using some exhaustive algorithms. This is a NP-hard problem, which is almost impossible to be solved. Therefore, security of the CS-watermark signal can be decided by the encryption property of the CS measurement matrix, in which random elements of the measurement matrix decide the measurement values property with random noise.

In addition, we can also show the security of the CS-watermarking from the signal detection point of view as detailed below. For (3), if data *x* is attacked by operation Δx in CS domain, we have $\vec{x} = x + \Delta x$. Thus, the measurement values of matrix Φ will be changed correspondingly as

$$\vec{y} = \Phi\vec{x} = \Phi x + \Phi\Delta x = y + \Delta y \tag{16}$$

It is obvious from (3) and (16), we obtain

$$\Delta y = \Phi\Delta x \tag{17}$$

As can be seen, after the original data are changed by the attack operation, the measurement difference values of CS are the projection Δy of Δx on the matrix Φ. For simplicity, assume the original data *x* is only changed in a pixel, that is only a nonzero elements in Δx

$$\Delta x = [0,0,...,\Delta x_f,...,0] \tag{18}$$

Then, Δy modified by the measurement values of a block matrix Φ_B becomes

$$\Delta y = \begin{bmatrix} h_{11} & h_{12} & \cdots & h_{1B} \\ h_{21} & h_{22} & \cdots & h_{2B} \\ \vdots & \vdots & \ddots & \vdots \\ h_{B1} & h_{B2} & \cdots & h_{B\times B} \end{bmatrix} \begin{bmatrix} 0 \\ \vdots \\ \Delta x \\ \vdots \\ 0 \end{bmatrix} = \Delta x_f \begin{bmatrix} h_{1x} \\ \vdots \\ h_{Bx} \end{bmatrix} = \begin{bmatrix} \Delta y_1 \\ \vdots \\ \Delta y_m \end{bmatrix} \tag{19}$$

where $h_{11}, h_{12},...,h_{B\times B}$ denote each element of the Hadamard matrix. Then, the *i*th element in Δy_i can be represented as

$$\Delta y_i = \Delta x_f \cdot h_{ix} \tag{20}$$

From (19) and (20), it can be clearly observed that, local modification from the original signal would cause the global modification by measurements matrix of CS. We use a squared Euclidean distance *D* as the security standard between the original data and the attacked one below

$$D = \sum_{i=1}^{M} (\vec{y_i} - y_i)^2 = \sum_{i=1}^{M} \Delta y_i^2 = \sum_{i=1}^{M} (\Delta x_f \cdot h_{ix})^2 = \Delta x_f^2 \sum_{i=1}^{M} h_{ix}^2 \tag{21}$$

That is, the smaller Δx_f is, the less *D* is, and the higher the security of the signal extracted becomes. Correspondingly, when Δx_f increases, *D* will become larger, and the security will be rapidly reduced. In our proposed method, as the CS-watermark signal executes some general signal process operations (i.e., DCT, DWT, SVD, and Hadamard transform), modification of Δx_f is usually small. Therefore, modification of *D* remains insignificant. If the CS-watermark signal is attacked by some unauthorized operations, the value Δx_f of the CS-watermarked signal will be rapidly increased, the *D* will be exponentially changed. Accordingly, the value *D* will also cause global distortion of measurement values in CS domain. Therefore, meaningful hidden messages are unable to be recovered by the attackers at the receiver side. As an information hiding result, the CS-watermark signal will be still secured in our proposed scheme.

IV. Datasets and Experimental Settings

To test the security and robustness of the proposed CS-watermark scheme, we have applied the scheme for information hiding in videos with the experiment system shown in Fig. 3. Firstly, we take four consecutive frames as a group, and each frame within a group is divided into blocks. Then, according to the Huang's algorithm [32], the DC value of each block located in the same position of successive frames within a group is transformed into the DCT domain. As there are four frames in a group, the second DCT actually contains four elements, one DC and three AC coefficients. Afterwards, we embed the CS-watermark signal into these AC values by using QIM (Quantization Index Modulation) [33]. Finally, after the watermarked video streams are transmitted in noise channel, we can extract the watermark signal by a cryptographic key of the measurement matrix shared between the sender and receiver.

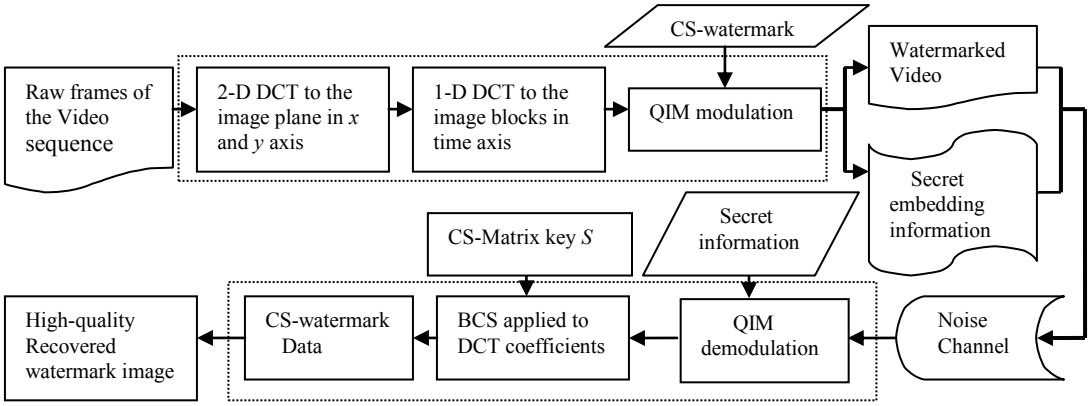


Fig. 3. A video information hiding experiment system with the CS-watermark signal.

The description of the datasets and the experimental settings are discussed in detail as follows.

A. Datasets used

In our experiments, the original watermark image, is obtained from a real gray level fingerprint from the FVC2004 database (DB3) with a size 160×160 [34]. The fingerprint image is then processed by a sparse basis Ψ based DCT. Finally, we obtain the CS-watermark signal of the fingerprint image by block Hadamard matrix Φ combining (11) and (15). The original fingerprint image and the measurement samples with various sizes are illustrated in Fig. 4, where the measurement samples from CS have clearly shown some random properties.

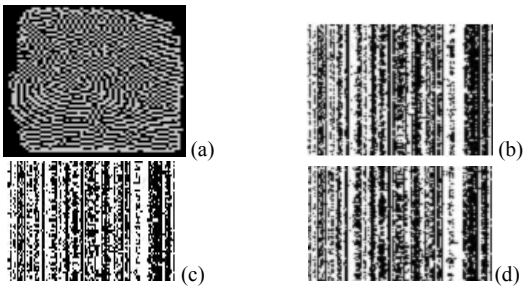


Fig. 4. Original fingerprint image (160×160) (a) and three measurement samples sized of 100×100 (b), 80×80 (c), and 80×100 (d), respectively.

Three well-known video sequences, *Basketball*, *Scene* and *Mobile*, are used in our experiments for CS-watermark signal embedding. The frame size of these videos is 720×480, and each sequence contains 80 frames. For each video, one representative frame is shown in Fig. 5 for information.

Fig.5. Three test videos: Basketball (left), Scene (middle) and Mobile (right).

As we take four successive frames as a group, there are 20 groups from 80 frames. For the 6400 bits within the watermark signal, we embed 640 bits in each image group. As a result, 10 groups of images are needed for the watermark signal, and the watermark signal is embedded twice in the 20 groups of frames. In addition, we divide each frame into 8×8 blocks, and embed 640bits watermark data into the 160 AC coefficients of middle-frequency selected by using Huang's algorithm [32].

B. *Evaluation criteria*

In information hiding systems, the transparency and the robustness are usually used for performance assessment [22], and [25]. For transparency, we use the peak signal-to-noise ratio (*PSNR*) as a criterion to estimate the invisibility of the embedded watermark signal. The *PSNR* can judge the received image quality by comparing the degree of diversity between the received image and the original one. The *PSNR*, derived from the mean square error (*MSE*), is defined as follows.

$$PSNR = 20\log\frac{H_{\max}}{\sqrt{MSE}}$$
$$MSE = (I_h I_w)^{-1}\sum_{i=1}^{I_h}\sum_{j=1}^{I_w}|H_1(i,j)-H_2(i,j)|^2 \tag{22}$$

where $H_{\max}$ is 255 for a gray-level image; $H_1(i,j)$ and $H_2(i,j)$ denote the received image and the original image corresponding to i and j coordinates in 2D space. I_h and I_w denote the height and width of the image, respectively.

Robustness is also one important metrics for performances measurement in watermarking. In our experiment, the normalized correlation (*NC*) is used for calculating the difference between the extracted watermark signal $\bar{W}(i,j)$ at the receiver side and the original watermark signal $W(i,j)$ at the sender side as defined below

$$NC = \frac{\sum_{i=1}^{N_1}\sum_{j=1}^{N_2}W(i,j)\bar{W}(i,j)}{\sum_{i=1}^{N_1}\sum_{j=1}^{N_2}[W(i,j)]^2} \tag{23}$$

where N_1 and N_2 denote the height and width of the original watermark image (fingerprint), respectively.

According to the measurement samples in Fig. 4, extracted fingerprint images using the BCS-SPL algorithm [29] are given in Fig. 6. As can be seen, the original fingerprint image can be successfully recovered in high quality, though larger sampled image produces slightly higher quality image indicated by the obtained PSNR values. To test the robustness of our proposed watermark scheme, the size of the watermark signal in our experiment is chosen as M=80×80 or 6400 bits.

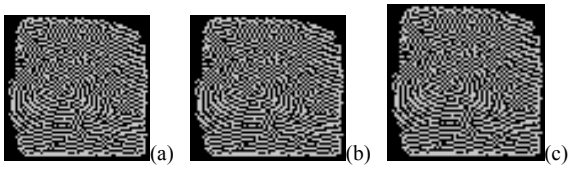

(a) (b) (c)

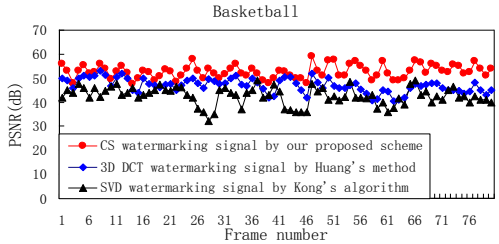
Fig. 6. Recovered fingerprint images with CS watermark signal by BCS-SPL. (a) PSNR=66.32dB (measurement samples of size 80×80), (b) PSNR=69.93dB (80×100), (c) PSNR=70.18dB (100×100).

V. Results and Discussions

Under the aforementioned experimental settings, the abovementioned three video sequences are used for performance measurement and evaluation. The results from our proposed approach have been compared with the methods from Huang [32] and Kong [35]. These approaches are selected as they represent two groups of typical algorithms performed in the spatial domain and SVD domain, respectively. Various attacks including MPEG and H.264 compression, noise contamination and filtering are used for performance assessment. Comprehensive results are reported and discussed as detailed below.

A. *Transparency measurement*

After embedding the fingerprint-based watermark signal into every 40 frames of the video sequence, the PSNR of the resulted sequences are calculated to measure the transparency of the proposed CS watermark signal scheme. For each sequence, the PSNR values over 80 frames are illustrated in Fig. 7, in benchmarking with Huang [32] and Kong [35].



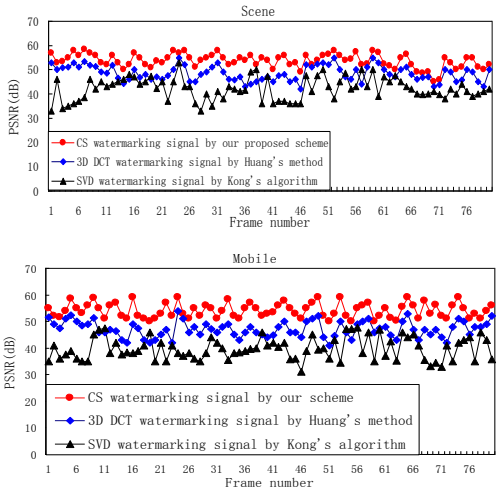


Fig. 7. Comparison of transparency of our watermark scheme and those in [32] and [35] using PSNR of the watermarked videos from the three sequences.

As can be seen, our approach has generated the highest PSNR values, 50-60dB, among the three. Kong's approach [35], on average, produces the worse results in this group of experiments. This has indicated that our method causes very slight distortion to the video signal and simultaneously provides high visual quality of the watermarked videos. Thanks to the proposed CS-watermark scheme, we only need 25% of samples for embedding as requested in [32] and [35]. This has explained the high transparency of our CS-watermark methodology.

B. Robustness measurement

The robustness of the proposed CS-watermark scheme has been tested with different attacks, including compression, filtering, noise and collusion. Relevant results are reported in detail below.

i) *Compression attack:* To evaluate the robustness of the watermark scheme under different compression attacks, MPEG-1, MPEG-2 and H.264 codecs are employed. For MPEG-1 and MPEG-2, the bit rate used is within 0.5-5Mbps in 10 levels. For H.264, due to it is designed for low bit rate applications, we can only manage have the bit rate changed within 0.5-2Mbps. For the video sequences compressed using the three approaches above, the acquired NC values under different bit rates are plotted in Figs. 8-11, respectively.

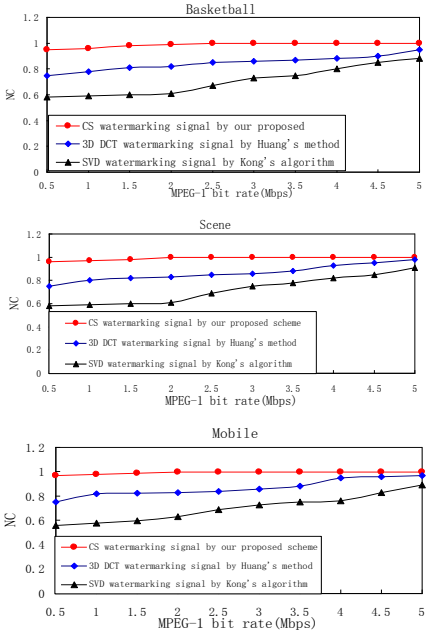


Fig. 8. NC-based robustness comparison under different MPEG-1 bit rates.

As can be seen, our approach significantly outperforms the other two in these three figures in terms of high NC values achieved and consistency of NC when the bit rate varies. The larger the NC value is, the better the robustness of the information hiding system is. This has indicated that the proposed approach is extremely robust to the three commonly used compression attacks. On the

contrary, the two benchmarking approaches have produced much lower NC values, which are inevitably affected by the changing of bit rate.

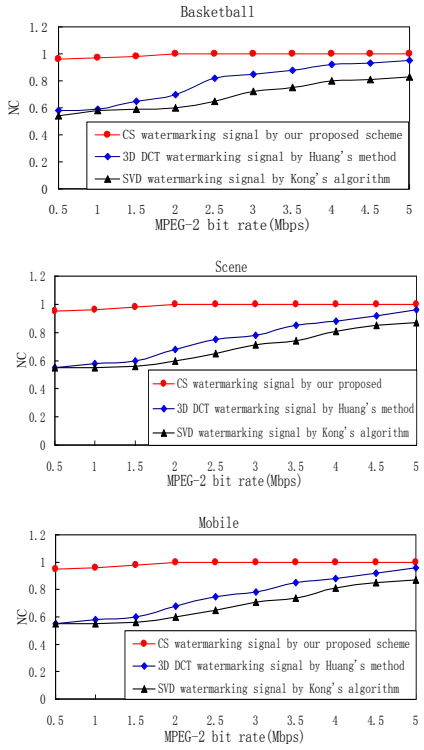


Fig.9. NC-based robustness comparison under different MPEG-2 bit rates.

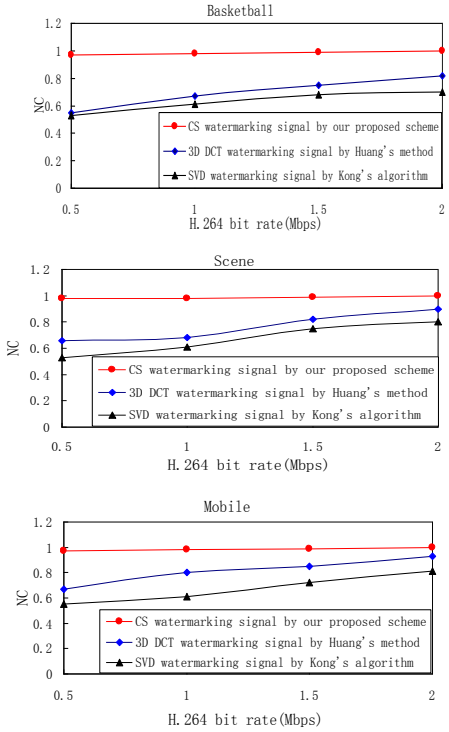


Fig.10. NC-based robustness comparison under different H.264 bit rates.

ii) *Filtering attacks:* To further assess the robustness of the proposed CS-watermark scheme, we consider also various intentional or unintentional attacks, such as 2-D 3×3 Wiener and median filtering. The results are compared in Figs. 11-12 below.

When Wiener and median filtering are respectively applied to the watermarked video frames, the detected watermark signal is affected by the degraded images. As such, the NC values for the two benchmarking approaches have declined to 0.5-0.7. However,

our proposed approach can always maintain a high NC value over 0.997. This again has validated the robustness of the proposed CS-watermark scheme.

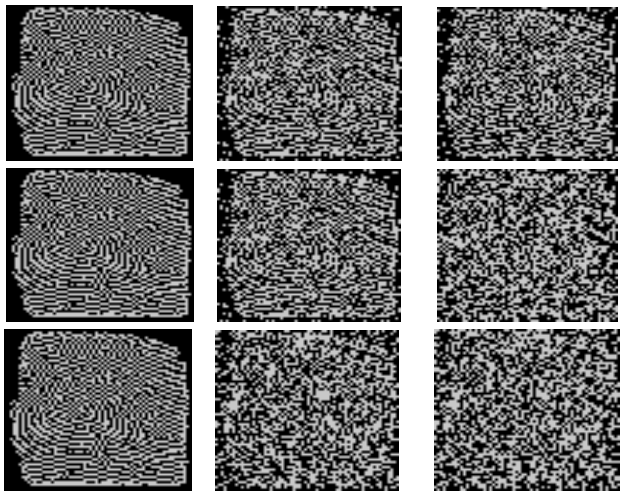


Fig.11. Wiener filtering attack results for the Basketball (top), Scene (middle) and Mobile (bottom) videos. In each row, the three images (left-right) are from our approach, Huang [32] and Kong [35] with NC values of (1.0, 0.682, 0.573), (0.998, 0.661, 0.552), and (0.997, 0.626, 0.508), respectively.

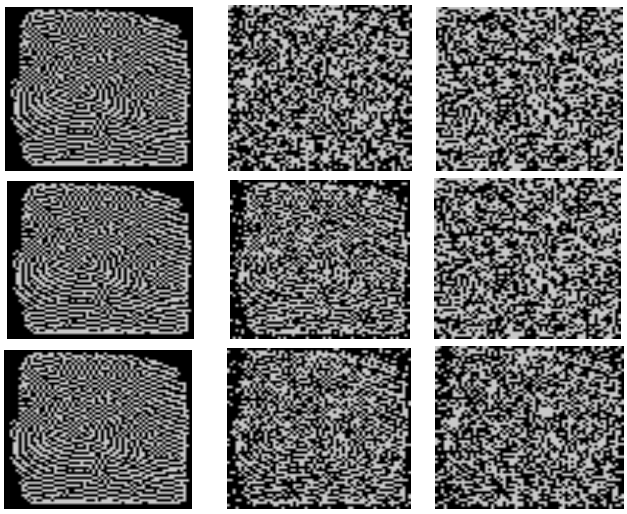


Fig.12. Median filtering attack results for the Basketball (top), Scene (middle) and Mobile (bottom) videos. In each row, the three images (left-right) are from our approach, Huang [32] and Kong [35] with NC values of (0.998, 0.623, 0.503), (0.999, 0.718, 0.559), and (0.997, 0.709, 0.602), respectively.

iii) N*oise attacks:* To further validate the robustness of the proposed approach, Gaussian (zero-mean with a variance of 0.05) and "pepper & salt" noise (with a density of 0.1) are used to attack the watermarked videos. The attached images are shown in Fig. 13 to indicate the severity of the noise introduced. The associated results are compared in Figs. 14-15 below.

When Gaussian and Pepper & Salt noise are respectively applied to the watermarked video frames, the detected watermark signal is also affected by the degraded images (see in Fig. 13). As such, the NC values for the two benchmarking approaches have declined to 0.6-0.9. However, our proposed approach can always maintain a high NC value no less than 0.999. This again has validated the robustness of the proposed CS-watermark scheme.

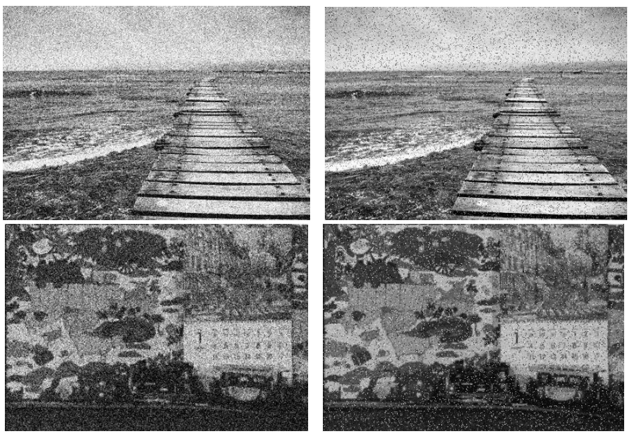


Fig. 13. Noise attached Basketball (top), Scene (middle) and Mobile (bottom) sequences using Gaussian (left) and Pepper & salt (right) noise, respectively.

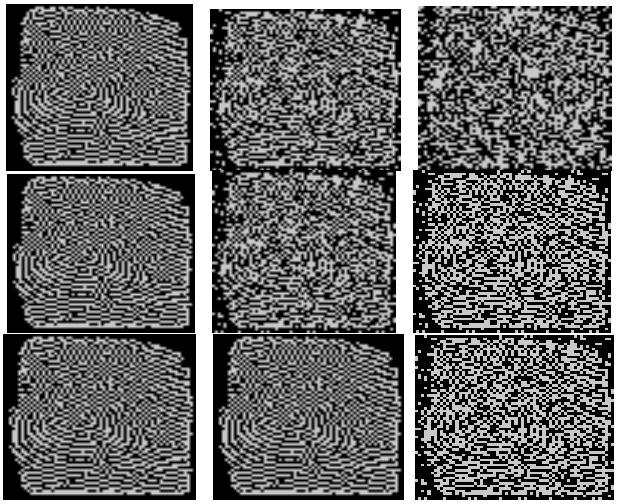
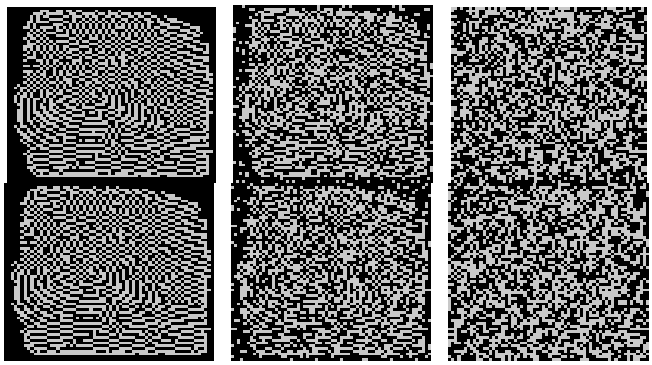


Fig.14. Result against Gaussian noise attacked videos for Basketball (top), Scene (middle) and mobile (bottom). In each row, the three images (left-right) are from our approach, Huang [32] and Kong [35] with NC values of (1.0, 0.732, 0.611), (1.0, 0.750, 0.682), and (1.0, 0.896, 0.702), respectively.

iii) *Collusion attack:* Collusion is one of the most common attacks in video information hiding [2], where the hidden watermark signal can be removed after it has been successfully identified by the attacker. Here, the robustness of the proposed method against this type of attack is assessed.

First, we embedded only one watermark image into 80 frames in video streams, and an attempt was made to obtain an estimate of the watermark by averaging the 80 frames directly. Fig. 16 shows the relevant results, which has indicated that the proposed CS-watermark signal cannot be easily estimated than those from Huang [32] and Kong [35]. For the two benchmarking approaches, the watermark signal has been removed when the colluded frames reaches 45-68. While for our approach, the watermark signal can still survive, with an NC value over 80%, even if all the 80 frames have been colluded.



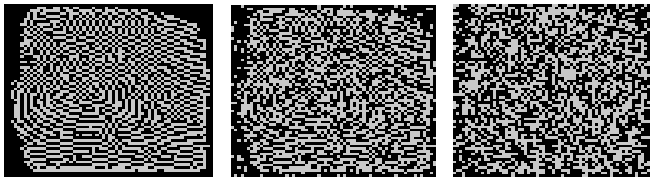


Fig.15. Result against Pepper & salt noise attacked videos for Basketball (top), Scene (middle) and mobile (bottom). In each row, the three images (left-right) are from our approach, Huang [30] and Kong [31] with NC values of (1.0, 0.761, 0.655), (1.0, 0.763, 0.631), and (0.999, 0.783, 0.642), respectively.

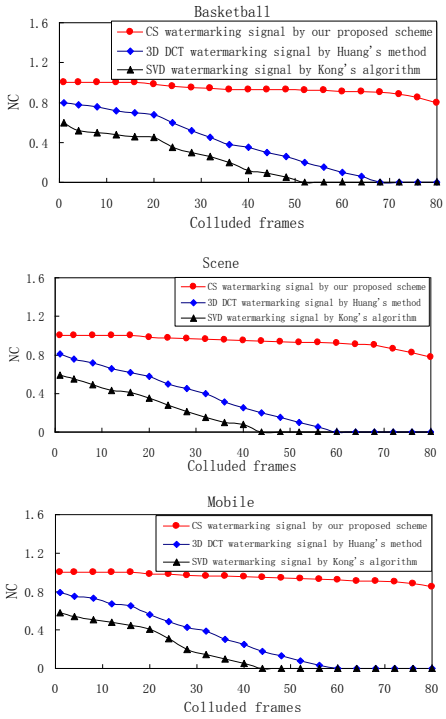


Fig. 16. Comparison results after collusion attack.

The proposed CS-watermark scheme benefits from two key factors, i.e. much less measurement samples required, and asymptotically normally distributed samples (ANDS). Usually, attackers may take advantage of the motionless regions in successive frames to remove the watermark signal. Although the identical watermark image is used within all frames, ANDS has prevented attackers from removing the watermark signal by averaging the frames. In the other words, attackers cannot estimate the CS-watermark signal by statistical averaging and remove it from our proposed CS-watermarked video. As a result, the resistance to collusion attacks has been significantly enhanced.

C. The influence of key parameters

In this part, how the key parameters of the proposed CS-watermark scheme may affect the quality of the resulted images is discussed. Under different parameters in terms of payloads, CS watermark sizes and the proportion of changed pixels, the image quality is measured using PSNR with results shown in Table I and Table II for comparison. These are results for the three test videos, Basketball, Scene and Mobile.

TABLE I
AVERAGE PSNR (dB) FOR THREE TEST VIDEOS WITH VARYING CS-WATERMARK SIZES w_M AND PAYLOADS (EMBED 1 w_M /FRAMES)

Payloads	Ratios of w_M					
	0.25	1	4	9	16	25
Results for the Basketball Sequence						
20	58.82	55.61	50.06	49.54	47.86	38.95
40	61.42	56.95	53.58	51.91	49.18	48.92
60	63.18	58.34	55.09	53.95	52.11	50.08
80	65.98	63.26	60.62	58.97	56.86	55.81
Results for the Scene Sequence						
20	57.69	55.12	49.96	49.85	49.72	40.58
40	61.01	57.86	55.56	51.81	50.82	49.62
60	62.98	58.42	54.89	53.91	52.97	51.42

80	67.75	63.18	60.22	58.16	56.13	55.89
Results for the Mobile Sequence						
20	58.62	55.42	49.66	48.94	45.69	39.45
40	62.40	56.44	53.28	51.11	47.19	46.82
60	64.06	58.02	55.04	53.81	51.97	50.01
80	66.75	63.15	60.12	58.75	56.11	54.93

TABLE II
AVERAGE PSNR (DB) FOR THREE TEST VIDEOS WITH VARYING CS-WATERMARK SIZES w_M AND PIXEL RATIOS

Ratio of black or changed pixels %	Ratios of w_M					
	0.25	1	4	9	16	25
Results for the Basketball Sequence						
0.01	56.29	52.02	50.61	46.28	43.09	38.35
0.25	61.01	55.12	53.18	50.12	45.17	40.96
0.5	63.14	56.92	54.81	52.19	49.92	42.76
0.75	65.25	62.11	58.23	52.66	54.19	44.13
1.0	67.82	67.72	61.07	52.18	52.59	45.93
Results for the Scene Sequence						
0.01	55.32	52.82	51.39	47.72	44.13	39.37
0.25	60.98	55.87	53.91	50.86	46.14	44.93
0.5	63.94	56.82	54.95	52.87	50.86	50.71
0.75	65.16	62.91	60.29	57.67	55.49	52.03
1.0	66.65	65.29	62.87	59.11	56.57	55.82
Results for the Mobile Sequence						
0.01	58.24	53.92	52.41	46.88	45.44	39.85
0.25	61.81	55.96	53.98	49.72	44.16	43.86
0.5	63.85	57.12	54.72	50.28	45.98	44.86
0.75	65.19	61.92	59.13	53.46	54.13	42.73
1.0	68.50	66.71	65.04	54.88	53.58	50.96

With the increasing of watermark size, the image quality decreases accordingly as indicated by the achieved PSNR values in Tables I-II. For a given CS watermark size, increasing payloads or ratio of changed pixels can generally help to produce higher PSNR values, i.e. improved image quality. However, there are exceptional cases for the Mobile sequence in Table II, where increased pixel ratios sometimes cannot yield improved PSNR values, especially when the watermark size is larger, say 16 and 25. The inconsistency is mainly due to the complicity of the scene.

VI. Conclusions

In this paper, based on the neural perception mechanism of our human brains in dealing with multidimensional data, a novel cognitive computation based CS-watermark approach is proposed for information hiding inside videos. As the CS-watermark signal is generated by measurement values of the scramble block Hadamard matrix, all features of the original watermark image can be represented. Accordingly, this naturally possesses an encryption property from random elements of measurement matrix where encryption occurs implicitly in the sensing process-***without requiring additional computation***. As a result, the CS-watermark signal is computationally simple, and has higher security than traditional methods achieved by extra scrambling and random processing in information hiding field. In addition, as only a small amount of the watermark data needs be embedded into the video, the proposed data hiding approach can effectively resist compressions, noise and filtering attacks and still maintain a better performance in terms of transparency and robustness. This has shown the great potential of applying CS-based cognitive computation in this emerging topic. Future works include combining machine-learning based data hiding analysis approaches such as extreme learning machine [38] and sparse representation based measurement matrix reconstruction [39] to further improve the security and robustness of data hiding.

Acknowledgements

The authors would like to thank the editors and the anonymous reviewers for their constructive comments to further improve the quality of this paper.

References

[1] M. L. Miller, G. J. Doerr, I. J. Cox, "Applying informed coding and embedding to design a robust high-capacity watermark," *IEEE Trans Image Process*, vol.13, no.6, pp. 792-807, Jun. 2004.

[2] S. Biswas, R. Das, and M. Petriu, "An adaptive compressed MPEG-2 video watermarking scheme", *IEEE Transactions on Instrumentation and Measurement*, vol. 54, no. 5, pp. 1853-1861, Oct. 2005.

[3] I. J. Cox, I. Kiliam, F. T. Leighton, and T. Shamoon, "Secure spread spectrum watermarking for multimedia", *IEEE Transaction on Image Processing,* vol.6, no.12, pp.1673-1687, 1997.
[4] G. Voyat zis and I. Pit as, "Chaotic watermarks f or embedding in the spatial domain," *in Proc. ICIP'98,* Chicago, IL, Oct . 1997, pp. 432- 436.
[5] H.Y. Huang, C.H. Yang, W.H. Hsu, "A Video Watermarking Technique Based on Pseudo-3-D DCT and Quantization Index Modulation," IEEE Transactions On Information Forensics and Security, vol.5, no.4, pp.625-627, Dec.2010.
[6] X. Gao, C. Deng, X. Li and D. Tao, Local Feature Based Geometric-Resistant Image Information Hiding, Cognitive Computation, 2(2): 68-77, June 2010
[7] F. Cayre, C. Fontaine, T. Furon, "Watermarking security: theory and practice," *IEEE Transaction on Signal Processing,* vol.53, no.10, pp. 3976 -3987, Nov. 2005.
[8] M. Fallahpour, S. Shirmohammadi, M. Semsarzadeh, J. Zhao, "Tampering detection in compressed digital video using watermarking," *IEEE Transaction on Instrumentation and Measurement*, vol.63,no.5, pp. 1057-1072, May 2014.
[9] S. Ganguli and H. Sompolinsky, "Compressed sensing, sparsity and dimensionality in neuronal information processing and data analysis," Annual Review of Neuroscience, vol. 35, pp. 485-508, 2012
[10] B. A. Olshausen and D. J. Field, "Emergence of simple-cell receptive field properties by learning a sparse code for natural images," Nature, vol. 381, pp. 607–608, 1996.
[11] M. Aghagolzadeh and K. Oweiss, "Compressed and distributed sensing of neuronal activity for real time spike train decoding," IEEE Trans. Neural System Rehability Engineering, vol. 17, no. 2, pp. 116-128, 2009.
[12] S. Eldawlatly, R. Jin and K. G. Oweiss, "Identifying functional connectivity in large-scale neural ensemble recordings: a multiscale data mining approach," Neural Computation, vol. 21, no. 2, pp. 450-477, 2009
[13] S. Kim, S. Kwon, I. S. Kweon, "A perceptual visual feature extraction method achieved by imitating V1 and V4 of the human visual system", Cognitive Computation, vol. 5, no. 4, pp. 610-628, Dec. 2013
[14] Z. Li, "Theoretical understanding of the early visual processes by data compression and data selection, " Network: Computation in Neural Systems, vol. 17, no. 4, pp. 301-334, Dec. 2006
[15] J. Hunt, P. Dayan and G. Goodhill, "Sparse coding can predict primary visual cortex receptive field changes induced by abnormal visual input," PLoS Computational Biology, vol. 9, no. 5, Article number: e1003005, 2013.
[16] O. Schwartz, A. Hsu and P. Dayan, "Space and time in visual context," Nature Reviews Neuroscience, vol. 8, pp. 522-535, July 2007
[17] A. Orsdemir, H.O. Altun, G. Sharma and M.F. Bocko, "On the security and robustness of encryption via compressed sensing", *IEEE Military Comm. Conference*, 2008, pp.1040- 1046.
[18] M. Davenport, P. Boufounos, M. Wakin, and R. Baraniuk, "Signal processing with compressive measurements," *IEEE Journal of Selected Topics in Signal Processing*, vol. 4, no.2, pp. 445-460, 2010.
[19] W. Lu, A. L. Varna and M. Wu, "Security analysis for privacy preserving search for multimedia," in *Proceedings of IEEE 17th Inter. Conf. on Image Processing*, 2010.
[20] R. Calderbank, S. Jafarpour and R. Schapire, "Compressed learning: universal sparse dimensionality deduction and learning in the measurement domain", *http://dsp.rice.edu/sites/dsp.rice.edu/files/cs/* , 2009.
[21] D. Hsu, S. M. Kakade, J. Langford and T. Zhang. "Multi-label prediction via compressed sensing", In *Neural Information Processing Systems* (NIPS), 2009.
[22] C. H. Zhao, W. Liu, "Block Compressive Sensing Based Image Semi-fragile Zero-watermarking Algorithm", *Acta Automatica Sinica*, vol. 38, no. 4, pp.609-617, May. 2012,
[23] X. Zhang, Z. Qian, Y. Ren, and G. Feng, "Watermarking with flexible self-recovery quality based on compressive sensing and compositive reconstruction," *IEEE Transaction on Information Forensics and Security,* vol.6, no.4, pp. 1223-1232, Dec. 2011.
[24] Q. Wang, W. Zeng, and J. Tian, "Integrated secure watermark detection and privacy preserving storage in the compressive sensing domain," *IEEE International Workshop on Information Forensics and Security*, November 2013, Guangzhou, China, pp. 67-72.
[25] H.M. Zhao, J.H. Lai, J. Cai, X.L. Chen, "A Video Watermarking Algorithm for Intraframe Tampering Detection Based Compressed Sensing," *Acta Electronica Sinica*, vol.41, no.6,pp.1153-1158, Jun. 2013.
[26] D. Donoho, "Compressed sensing," *IEEE Transaction on Information Theory*, vol. 52, No. 4, pp.1289-1306, 2006.
[27] D.L. Donoho,Y. Tsaig, "Extensions of compressed sensing ," *Signal Processing,* vol.86, no.3,pp.533-548, 2006.
[28] E. Candes and M. Wakin, "An introduction to compressive sampling," *IEEE Signal Processing Magazine*, vol.25, no. 2, pp.21-30, Mar.2008.
[29] J.E. Fowler, S.W. Mun, and E. W. Tramel, "Multiscale Block Compressed Sensing with Smoothed Projected Landweber Reconstruction", 19th European Signal Processing Conference (EUSIPCO 2011), Barcelona, Aug 29-Sep 2, 2011, pp. 564-568.
[30] K. Ni, S. Datta, P. Mahanti, S. Roudenko, and D. Cochran, "Efficient Deterministic Compressed Sensing for Images with Chirps and Reed-Muller Codes," *SIAM Journal on Imaging Sciences*, vol.4, no.3,pp.931-953, 2011.
[31] Y. Rachlin, D. Baron, "The secrecy of compressed sensing measurements," *In: Proc. the 46th Annual Allerton Conf. n Communication, Control and Computing,* Illinois, USA, 2008, pp. 813-817.
[32] H.Y. Huang, C.H. Yang, W.H. Hsu, "A Video Watermarking Technique Based on Pseudo-3-D DCT and Quantization Index Modulation," IEEE Transactions On Information Forensics and Security, 2010, vol.5, no.4, pp:625-627.
[33] Y.S. Seo, W.G. Kim, Y.H. Huh, W.G. Oh, and C.J. Hwang, "QIM watermarking for image with tow adaptive quantization step-sizes," in Proc. 9th Int. Conf. Advanced Communication Technology, 2007, pp:997-800
[34] Fingerprint verification competition, http://bias.csr.unibo.it/fvc2004/.
[35] W. Kong, B. Yang, D. Wu, and X. Niu, "SVD based blind video watermarking algorithm," *in Proc. First Int. Conf.* Innovative Computing, Information and Control, 2006, pp: 265-268.
[36] V. Sachnev, S. Ramasamy, S. Sundaram, et al, "A cognitive ensemble of extreme learning machine for steganalysis based on risk-sensitive hinge loss function," Cognitive Computation, vol. 7, no. 1, pp. 103-110, 2015
[37] J. Xu, G. Yang, Y. Yin, H. Man and H. He, "Sparse-representation-based classification with structure-preserving dimension reduction," Cognitive Computation, vol. 6, no. 3, pp. 608-621, 2014

HuiMin Zhao, was born in Shaanxi, China, in 1966. He received the B.Sc. and the M.Sc. degrees 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.

Jinchang Ren received his B. E. degree in computer software, MEng in image processing, DEng in computer vision, all from Northwestern Polytechnical University, Xi'an, China. He was also awarded a PhD in Electronic Imaging and Media Communication from Bradford University, U.K.

Currently he is with University of Strathclyde, Glasgow, U.K. His research interests focus mainly on visual computing and multimedia signal processing, especially on semantic content extraction for video analysis and understanding and more recently hyperspectral imaging. He has published over 130 peer reviewed journal and conferences papers, and acts as an Associate Editor for two international journals including Multidimensional Systems and Signal Processing (Springer) and Int. J. of Pattern Recognition and Artificial Intelligence.