A Compressive Sensing based Secure Watermark Detection and Privacy Preserving Storage Framework

Qia Wang, Wenjun Zeng, *Fellow, IEEE*, and Jun Tian, *Member, IEEE*

***Abstract*— Privacy is a critical issue when the data owners outsource data storage or processing to a third party computing service, such as the cloud. In this paper, we identify a cloud computing application scenario that requires simultaneously performing secure watermark detection and privacy preserving multimedia data storage. We then propose a compressive sensing (CS)-based framework using secure multiparty computation (MPC) protocols to address such a requirement. In our framework, the multimedia data and secret watermark pattern are presented to the cloud for secure watermark detection in a CS domain to protect the privacy. During CS transformation, the privacy of the CS matrix and the watermark pattern is protected by the MPC protocols under the semi-honest security model. We derive the expected watermark detection performance in the CS domain, given the target image, watermark pattern, and the size of the CS matrix (but without the CS matrix itself). The correctness of the derived performance has been validated by our experiments. Our theoretical analysis and experimental results show that secure watermark detection in the CS domain is feasible. Our framework can also be extended to other collaborative secure signal processing and data-mining applications in the cloud.**

***Index Terms*— Compressive sensing, secure watermark detection, secure signal processing, secure multiparty computation, privacy preserving.**

I. Introduction

THE cloud computing technologies are growing, and it is more economical for the data holders to shift data storage or signal processing computations to the cloud instead of purchasing hardware and software by themselves. Ideally, the cloud will store the data and perform signal processing or data-mining *in an encrypted domain* in order to preserve the data privacy. Meanwhile, due to the rapid growth of the Internet and social networks, it is very easy for a user to collect a large amount of multimedia data from different sources without knowing the copyright information of those data. The user may want to take advantage of the cloud for storage, and at the same time, work with copyright owners for watermark detection while keeping those self-collected multimedia data private. The watermark pattern owner wants to keep their watermark patterns private during the watermark detection as well. A legal cloud offering storage services may also desire to participate in watermark detection initiated by the users, or initiate watermark detection itself without the involvement of the users, to check if the uploaded multimedia data is copyright protected. Another benefit of storing the encrypted multimedia data and facilitating encrypted domain watermark detection in the cloud is that those encrypted data can be reused if the image data holder (or the cloud) needs to work with other watermark owners later for secure watermark detection.

Traditional secure watermark detection techniques are designed to convince a verifier whether or not a watermark is embedded without disclosing the watermark pattern so that an untrusted verifier cannot remove the watermark from the watermark protected copy [1], [2]. Two types of approaches have been proposed for secure watermark detection: asymmetric watermarking [3], [4] and zero-knowledge watermark detection [5]–[7]. However, most of the existing secure watermark detection works assume the watermarked copy are publicly available and focus on the security of the watermark pattern, while the privacy of the target media on which watermark detection is performed has received little attention. But for some applications such as the scenario given above, it is required to protect the multimedia data's privacy in the watermark detection process. Performing privacy preserving storage and secure watermark detection simultaneously is possible by using the existing secure watermark detection technologies such as zero-knowledge proof protocols [5]–[7] that transform the multimedia data to a public key encryption domain. However, their limitations, such as complicated algorithms, high computational and communication complexity [1], and large storage consumption in the public key encryption domain, may impede their practical applications.

In this paper, we propose a compressive sensing based privacy preserving watermark detection framework that leverages secure multiparty computation and the cloud. It has been shown that many signal processing algorithms performed in the CS domain have very close performance as performed in the original domain [17]–[19]. Using random matrix transformation for privacy preserving data-mining has also been proposed, e.g., by Liu *et al* [11], which proposed a random projection data perturbation approach for privacy preserving

Manuscript received May 17, 2013; revised September 27, 2013 and November 20, 2013; accepted December 9, 2013. Date of publication January 9, 2014; date of current version February 6, 2014. The associate editor coordinating the review of this manuscript and approving it for publication was Dr. Chun-Shien Lu.

Q. Wang and W. Zeng are with the Department of Computer Science, University of Missouri, Columbia, MO 65211 USA (e-mail: qwch9@mail.missouri.edu; zengw@missouri.edu).

J. Tian is with Futurewei Technologies, Bridgewater, NJ 08807 USA (e-mail: juntian@huawei.com).

Color versions of one or more of the figures in this paper are available online at http://ieeexplore.ieee.org.

Digital Object Identifier 10.1109/TIP.2014.2298980

collaborative data-mining. Lu *et al* [12], [13] have proposed a secure image retrieval system through random projection and have proven that the proposed random projection domain multimedia retrieval system is secure under the Ciphertext Only Attack model (COA) and the semi-honest model [10]. Furthermore, [20], [21] show that CS transformation can achieve computationally secure encryption. These works indicate that signal processing or data-mining in the CS domain is feasible and is computationally secure under certain conditions.

In our framework, the target image/multimedia data is possessed by the image holder only. A compressive sensing matrix is issued by a certificate authority (CA) server to the image holder. The image holder transforms the DCT coefficients of the image data to a compressive sensing domain before outsources it to the cloud. For secure watermark detection, the watermark is transformed to the same compressive sensing domain using a secure multiparty computation (MPC) protocol and then sent to the cloud. The cloud only has the data in the compressive sensing domain. Without the compressive sensing matrix, the cloud cannot reveal the original multimedia data and the watermark pattern. The cloud will perform watermark detection in the compressive sensing domain. The image data in the compressive sensing domain can be stored in the cloud and reused for detection of watermark from many other watermark owners.

Our system is secure under the semi-honest [10] assumption that all parties comply with the protocol's procedure strictly, and none of them will actively withdraw midway or incorporate false or malicious data. No two parties will collude to attack a third one. But during the computing process, they may try to keep all the intermediate information, so that they can infer others' input after the process. Semi-honest model is a reasonable assumption for adversaries such as third-party service providers [13].

The rest of this paper is organized as follows. In Section II, we show that watermark detection in the CS domain is viable theoretically, and the expected performance is derived. Section III gives the details of the proposed framework together with some analysis. Section IV presents the experimental results. The paper concludes in Section V.

II. Watermark Detection in the Compressive Sensing Domain

In this section, we first introduce the compressive sensing theory and related works on signal processing in the compressive sensing or random projection domain. We then introduce the statistical correlation based watermarking scheme proposed by Zeng and Liu [8], based on which we show that correlation based watermark detection in the compressive sensing domain is feasible. We also present a theoretical performance analysis of watermark detection in the compressive sensing domain.

A. Compressive Sensing

Restricted Isometry Property (RIP) is a required condition for the perfect reconstruction in the compressive sensing theory. Before presenting the compressive sensing theory, we first introduce the Restricted Isometry Property:

Restricted Isometry Property (RIP): A vector $x \in \mathbb{R}^n$ is k-sparse if $|\{j : |x_j| > 0\}| \leq k$. A matrix $\Phi \in \mathbb{R}^{m \times n}$ is said to have the Restricted Isometry Property of order k and level $\delta \in (0, 1)$ (equivalently, (k, δ)-RIP) if

$$(1 - \delta) \|x\|_2^2 \leq \|\Phi x\|_2^2 \leq (1 + \delta) \|x\|_2^2 \tag{1}$$

for all k-sparse $x \in \mathbb{R}^n$. The restricted isometry constant δ_k is defined as the smallest value of δ for which the above inequality holds.

The compressive sensing theory [14] asserts that when a signal can be represented by a small number of non-zero coefficients, it can be perfectly recovered after being transformed by a limited number of incoherent, non-adaptive linear measurements. Suppose a signal $s \in \mathbb{R}^n$ is a k-sparse vector (only k out of the n elements of s are nonzero) and can be transformed to $x \in \mathbb{R}^m$, $m < n$, where $x = \Phi_{m \times n} s$. If $\Phi_{m \times n}$ satisfies RIP, it can be shown [14] that solving the below optimization problem:

$$\mathbf{min} \|s\|_1 \text{ s.t. } x = \Phi_{m \times n} s \tag{2}$$

is equivalent to finding the sparsest solution s to $x = \Phi_{m \times n} s$, provided $m \geq Cklog(n/k)$, where C is a small constant. Eq. (2) presents a L1 minimization problem which can be solved by orthogonal matching pursuit (OMP) algorithms [16]. It has been shown [15] that there are many ways to construct a matrix $\Phi_{m \times n}$ that meets the RIP property, e.g., if the entries of matrix $\Phi_{m \times n}$ are generated from a Gaussian distribution with zero mean and variance $1/m$, $\Phi_{m \times n}$ is a RIP matrix with overwhelming probability. In our framework, the compressive sensing matrix is generated from such a Gaussian distribution.

Most of the literature of compressive sensing has focused on improving the speed and accuracy of compressive sensing reconstruction. Davenport *et al* [17] take some initial steps towards a more general framework called compressive signal processing (CSP), which shows fundamental signal processing problems such as detection, classification, estimation, and filtering can be solved in the compressive sensing domain. Hsu *et al* [19] use compressive sensing to learn to predict compressed label vectors and then reconstruct the learned compressed label vectors. It provides mathematical proof and experimental results that show prediction of sparse vectors could be done in the compressive sensing domain. Calderbank *et al* [18] give some theoretical results and show that compressed learning, learning directly in the compressed domain, is possible. It gives the tight bounds demonstrating that the linear kernel SVM's classifier in the measurement domain, with high probability, has an accuracy close to the accuracy of the best linear threshold classifier in the original data domain. Earlier than the birth of the compressive sensing theory, random projection using the Johnson-Lindenstrauss Lemma [11] was also used for privacy preserving data-mining. The paper by Liu *et al* [11] gave the following lemma about linear correlation in the compressive sensing domain:

Lemma 1. [11]: Let $X = \{x_i\}$, $Y = \{y_i\}$ be two $n\text{-}dimensional$ vectors and $\Phi_{m \times n}$ be an $m \times n\text{-}dimensional$

random matrix. Each entry of $\Phi_{m\times n}$ is independent and identically chosen from Gaussian distribution with mean zero and variance $1/m$. Further, let $P = \Phi_{m\times n}X$; and $R = \Phi_{m\times n}Y$.

Then:

$$E[X^TY - P^TR] = 0$$
$$Var[X^TY - P^TR] = \frac{1}{m}\Big(\sum_1^n x_i^2 \sum_1^n y_i^2 + \Big(\sum_1^n x_i y_i\Big)^2\Big).$$

B. Correlation based Watermarking System

In Zeng and Liu's work [8], watermarks are embedded in the discrete cosine transform (DCT) domain. Let the feature set $\{d_i\}$ be the set of selective DCT coefficients (i.e., those with absolute values larger than certain perceptual thresholds) excluding the DCs. The embedding process is $d_i^{'} = d_i + w_i$, where $\{w_i\}$ is the inserted watermark signals which is derived from the watermark pattern $\{y_i\}$. In the detection process, the test feature set $\{x_i\}$ is correlated with the watermark pattern $\{y_i\}$. Detection of the watermarks is accomplished via the hypothesis testing:

$H_0 : x_i = d_i + n_i$, without watermark

$H_1 : x_i = d_i + w_i + n_i$, with watermark

where n_i is the noise. The normalized correlating detector outputs the test statistic q, which is compared to a threshold T to determine if the test image contains the claimed watermarks:

$$q = \frac{\sum_{i=1}^n z_i}{V_{z_i} * \sqrt{n}} = \frac{M_{z_i} * \sqrt{n}}{V_{z_i}} \tag{3}$$

where $z_i = x_i y_i$, n is the size of the feature set $\{z_i\}$. M_{z_i} and $V_{z_i}^2$ are the sample mean and sample variance of z_i, given by:

$$M_{z_i} = \frac{\sum_{i=1}^n z_i}{n}; \quad V_{z_i}^2 = \frac{\sum_{i=1}^n (z_i - M_{z_i})^2}{n-1} \tag{4}$$

Then under hypothesis H_0, for large n, q is approximately a normal distribution $q \sim N(0,1)$. Under H_1, $q \sim N(\mu, 1)$, where $\mu > 0$.

C. Watermark Detection in the Compressive Sensing Domain

Compressive sensing or random sampling domain linear correlation hypothesis test has been proven feasible and the error bound analysis has been given in works such as [17], [22]. In [17], [22], the analysis is based on the *Neyman-Pearson* detector and the statistic for detection is computed *given that the random projection matrix Φ is known*. However, in the scenarios addressed in our work, the entity who performs watermark detection does not have access to Φ, as described in Section III.A. In our work, the statistic is calculated based only on the observation in the compressive sensing domain. We not only demonstrate that the statistical correlation hypothesis test based watermark detection is feasible by using only the data in the CS domain, but also show specifically what parameters will affect the watermark detection performance.

Let vector X and Y represent the sets $\{x_i\}$ and $\{y_i\}$ in Section II.B respectively:

$$X = [x_1, x_2, \ldots, x_n]^T; \quad Y = [y_1, y_2, \ldots, y_n]^T$$

Let the compressive sensing matrix be $\Phi_{m\times n}$ whose entries $\Phi_{i,j}$ have the distribution given in Lemma 1, then after the projection we have:

$$P = [p_1, p_2, \ldots, p_m]^T = \Phi_{m\times n}X$$
$$R = [r_1, r_2, \ldots, r_m]^T = \Phi_{m\times n}Y$$

where given X and Y, $\{p_i\}$ and $\{r_i\}$ are both i.i.d. Gaussian.

Similarly, we define the statistic q^{cs} in the CS domain as:

$$q^{cs} = \frac{\sum_{i=1}^m z_i^{cs}}{V_{z_i^{cs}} * \sqrt{m}} \tag{5}$$

where $z_i^{cs} = p_i r_i$; Then under H_0, for large m, q^{cs} is approximately a normal distribution with unit variance, $q^{cs} \sim N(0,1)$. Under H_1, $q^{cs} \sim N(\mu^{cs}, 1)$, where $\mu^{cs} > 0$. To analyze the relationship between μ and μ^{cs}, let us look at the conditional expectation of q^{cs}, given X, Y:

$$\begin{aligned} E\left(q^{cs}|X,Y\right) &= E\left[\frac{\sum_{i=1}^m z_i^{cs}}{V_{z_i^{cs}} * \sqrt{m}}|X,\ Y\right] \\ &= E\left(\sum_{i=1}^m z_i^{cs}|X,Y\right) * E\left(\frac{1}{V_{z_i^{cs}} * \sqrt{m}}|X,Y\right) \\ &\quad + Cov\Big(\sum_{i=1}^m z_i^{cs}, \frac{1}{V_{z_i^{cs}} * \sqrt{m}}|X,\ Y\Big) \end{aligned} \tag{6}$$

Since $\{f(x) = \frac{1}{x},\ where\ x > 0\}$ is a convex function, according to the Jensen's inequality: $E(f(x)) \geq f(E(x))$. Then we have:

$$E\left(\frac{1}{V_{z_i^{cs}} * \sqrt{m}} \mid X, Y\right) \geq \frac{1}{E(V_{z_i^{cs}} * \sqrt{m}|X,Y)} \tag{7}$$

Since $f(x) = \sqrt{x},\ where\ x > 0$ and $f(x) > 0\}$ is a concave function, according to the Jensen's inequality: $E(f(x)) \leq f(E(x))$.:

$$\frac{1}{E(V_{z_i^{cs}} * \sqrt{m}|X,Y)} \geq \frac{1}{\sqrt{E\left(V_{z_i^{cs}}^2|X,Y\right) * m}} \tag{8}$$

Then:

$$\begin{aligned} E\left(q^{cs}|X,Y\right) \geq\ & Cov\Big(\sum_{i=1}^m z_i^{cs}, \frac{1}{V_{z_i^{cs}} * \sqrt{m}}|X,\ Y\Big) \\ & + \frac{E\left(\sum_{i=1}^m z_i^{cs} \mid X,Y\right)}{\sqrt{E\left(V_{z_i^{cs}}^2|X,Y\right) * m}}. \end{aligned} \tag{9}$$

Lemma 2. Let the compressive sensing matrix $\Phi_{m\times n}$ be an $m \times n$-*dimensional* random matrix. Each entry of $\Phi_{m\times n}$ is independently and identically chosen from a Gaussian distribution with mean zero and variance $1/m$. Then, given X, Y,

$$E\big(V_{z_i^{cs}}^2|X,Y\big) = \frac{1}{m^2}\big(\big(\sum_{a=1}^n x_a y_a\big)^2 + \sum_{a=1}^n x_a^2 \sum_{a=1}^n y_a^2\big) \tag{10}$$

Proof of Lemma 2: Please see Appendix I for the proof.

Based on Lemma 1 and Lemma 2, we have:

$$\frac{E\left(\sum_{i=1}^{m} z_i^{cs} \mid X, Y\right)}{\sqrt{E\left(V_{z_i^{cs}}^2 | X, Y\right) * m}} = \frac{\sum_{i=1}^{n} x_i y_i}{\sqrt{\frac{1}{m}\left(\left(\sum_{a=1}^{n} x_a y_a\right)^2 + \sum_{a=1}^{n} x_a^2 \sum_{a=1}^{n} y_a^2\right)}} = \frac{M_{z_i}}{\sqrt{\frac{1}{mn^2}\left(\left(\sum_{a=1}^{n} x_a y_a\right)^2 + \sum_{a=1}^{n} x_a^2 \sum_{a=1}^{n} y_a^2\right)}} = \beta.$$

Then, from Eq. (9), we have:

$$E(q^{cs}|X, Y) \geq Cov\left(\sum_{i=1}^{m} z_i^{cs}, \frac{1}{V_{z_i^{cs}*\sqrt{m}}} \middle| X, Y\right) + \beta \approx \beta \quad (11)$$

It is well known in statistics that when a random variable is i.i.d Gaussian, its sample mean and sample variance are independent [27]. $\{z_i^{cs}\}$ is not i.i.d Gaussian, however, our experimental results (see Section IV.C) validate that the covariance term in Eq. (11) is very small (close to zero). From the β above, we can see that given the original input X and Y for watermark detection, the statistic q^{cs}'s mean value μ^{cs} is affected by the CS matrix height m: if m is smaller, the μ^{cs} will be smaller. In the experimental results section, we show that β is validated to be very close to the mean of the statistic q^{cs}. *This is important since the expected watermark detection performance q^{cs} can be estimated by β (for example during the watermark embedding process) disregard the actual CS matrix used later by other parties for secure watermark detection.*

The statistic q of the original domain is defined as $M_{z_i}/\sqrt{V_{z_i}^2/n}$. In order to find the relationship between β and q, we need to compare the relationship between $V_{z_i}^2/n$ and $\frac{1}{mn^2}\left(\left(\sum_{a=1}^{n} x_a y_a\right)^2 + \sum_{a=1}^{n} x_a^2 \sum_{a=1}^{n} y_a^2\right)$ as:

$$\begin{aligned}
\lambda &= \frac{1}{mn^2}\left(\left(\sum_{a=1}^{n} x_a y_a\right)^2 + \sum_{a=1}^{n} x_a^2 \sum_{a=1}^{n} y_a^2\right) - \frac{\sum_{a=1}^{n}(x_a y_a)^2 - nM_{z_i}^2}{(n-1)n} \\
&\geq \frac{1}{nn^2}\left(\sum_{1}^{n} x_a^2 \sum_{1}^{n} y_a^2 + n^2 M_{z_i}^2\right) - \frac{\sum_{i=1}^{n}(x_a y_a)^2 - nM_{z_i}^2}{(n-1)n} \quad \text{(Since } m \leq n\text{)} \\
&= \frac{1}{nn^2}\left(n^2\overline{(x_a y_b)^2} + n^2 M_{z_i}^2\right) - \frac{\overline{(x_a y_a)^2} - M_{z_i}^2}{n-1} \\
&\approx \frac{1}{n}\left(\overline{(x_a y_b)^2} + M_{z_i}^2\right) - \frac{\overline{(x_a y_a)^2} - M_{z_i}^2}{n} \quad \text{(Since } n \approx n-1\text{)} \\
&= \frac{1}{n}\left(\overline{(x_a y_b)^2} - \overline{(x_a y_a)^2} + 2M_{z_i}^2\right) \quad (12)
\end{aligned}$$

where $\overline{(x_a y_b)^2}$ is the average of all possible $(x_a y_b)^2$, (where $1 \leq a, b \leq n$); $\overline{(x_a y_a)^2}$ is the average of all possible $(x_a y_a)^2$, (where $1 \leq a \leq n$).

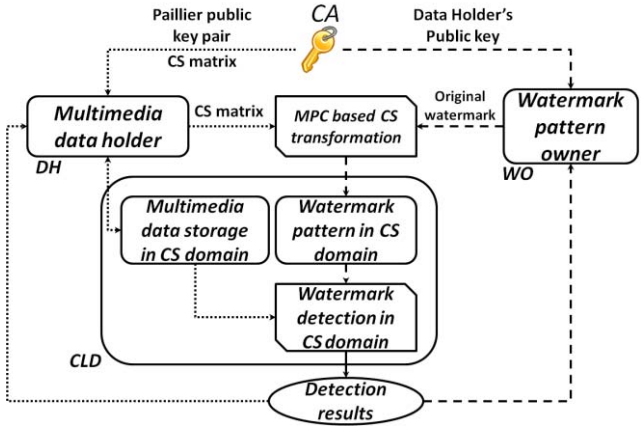

Fig. 1. Architecture of the proposed framework.

Note that it is expected that the difference between $\frac{1}{n}\overline{(x_a y_b)^2}$ and $\frac{1}{n}\overline{(x_a y_a)^2}$ is very small, as $(x_a y_b)^2$ and $(x_a y_a)^2$ are statistically similar. Our experiment shows that $\frac{1}{n}\overline{(x_a y_b)^2}$and $\frac{1}{n}\overline{(x_a y_a)^2}$ are very close, and $\lambda > 0$, which means that the watermark detection in the CS domain will be inferior to that in the original domain.

Furthermore, based on Eq. (12), we have:

$$\gamma = \frac{q}{\beta} = \sqrt{1 + \frac{\lambda}{V_{z_i}^2/n}} \geq \sqrt{1 + \frac{\left(\overline{(x_a y_b)^2} - \overline{(x_a y_a)^2} + 2M_{z_i}^2\right)}{V_{z_i}^2}} \quad (13)$$

A larger γ means larger watermark detection distortion caused by the CS transformation.

III. The Proposed Framework

We first provide an overview of the proposed framework in Section III.A. The framework relies on a secure CS transformation protocol which is introduced in Section III.B. The complexity and security analysis of the framework is given in Section III.C.

A. The Framework

There are three parties in the proposed framework, the data holders (DH) of the potentially watermarked images, the watermark owners (WO) and the cloud (CLD) as illustrated in Fig. 1. The framework also requires a certificate authority (CA) to issue the public keys and CS matrix keys to certain parties of the framework. For DH (e.g., media agencies), when it collects a large volume of multimedia data from the Internet and stores their encrypted versions in the CLD, it wants to make sure those multimedia can be edited and republished legally. Watermark owners (WOs) are also the content providers who distribute their watermarked content (the watermark embedding is performed by WO before the contents are published). WOs always want to know if their contents are legally used and republished.

In some scenarios, not only DH and WO care about the copyright of the multimedia data, certain CLD who offers storage services may also desire to initiate the watermark

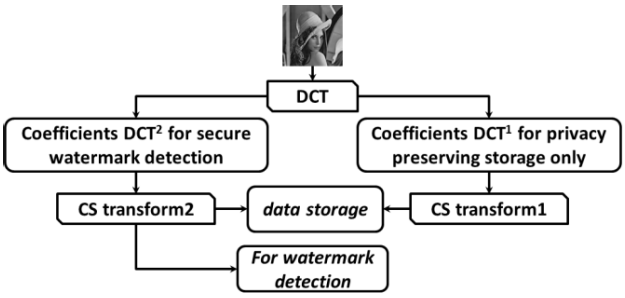

Fig. 2. Some DCT coefficients (DCT^1) are only used for storage; The other coefficients (DCT^2) serve for both the storage and watermark detection purposes.

DC	1	5	6	14	15	27	28
2	4	7	13	16	26	29	42
3	8	12	17	25	30	41	43
9	11	18	24	31	40	44	53
10	19	23	32	39	45	52	54
20	22	33	38	46	51	55	60
21	34	37	47	50	56	59	61
35	36	48	49	57	58	62	63

(a)

DC	1	5	6	14	15	27	28
2	4	7	13	16	26	29	42
3	8	12	17	25	30	41	43
9	11	18	24	31	40	44	53
10	19	23	32	39	45	52	54
20	22	33	38	46	51	55	60
21	34	37	47	50	56	59	61
35	36	48	49	57	58	62	63

(b)

Fig. 3. 8×8 DCT block zig-zag scan order: (a) an example of selective DCT coefficients for watermark embedding: the bold underlined numbers indicate that the corresponding DCT channels are embedded with watermark signals. (b) top 20 AC coefficients (white areas) are selected for watermark detection in the CS domain (i.e., DCT2 in Fig. 2).

detection to check if the uploaded multimedia data is copyright protected. For example, a CLD may choose not to provide storage services to copyright protected data illegally owned. If DH would like to use a CLD for storage or migrate the encrypted multimedia data from another cloud to this CLD, it will require the CLD to perform watermark detection on the encrypted multimedia data before providing the storage services.

In our framework, initially, the CA needs to issue CS matrix suites to the DH. The CS matrix suites include the seeds and the random function used to generate the Gaussian CS matrix. We use the CA to issue the random function to guarantee the randomness of the generated Gaussian CS matrix. The CA also needs to issue a Paillier public key pair to the DH and the DH's public key to the WO. The public key is used for the MPC based CS transformation protocol as discussed in Section III.B.

In general, the DH *also has a different private compressive sensing matrix (derived from the seed) for each image.* DH transforms the image's DCT coefficients to the compressive sensing domain and let CLD have the CS domain data for storage. If watermark detection with WO is required, we need to let CLD have the watermark in the same CS domain, which is achieved through running a secure multiparty protocol (Protocol 2: Secure CS transformation protocol to be introduced in Section III.B) by DH, WO and CLD collaboratively under the semi-honest model [10]. Then CLD can detect if the watermark exists in the CS domain and let both DH and WO know the detection results. After Protocol 2 is executed, the compressive sensing matrix and the watermark pattern are still the secret values of the image holder and the watermark pattern owner respectively. In the framework, each CS matrix is used **only once** to encrypt the images' DCT coefficients, which is proven to be computationally secure in [21]. Note, however, that *a CS encrypted image will be stored and reused for secure detection of multiple watermarks on the same image.*

In Zeng and Liu's work [8], the best watermark detection performance is achieved by using selective DCT coefficients for detection [i.e., select the potentially watermark embedded DCT channels for watermark detection as shown in Fig. 3(a)]. However, the DH in our framework may not have the information about the criteria for the selection process. Even if we assume that the DH has such information, the DH needs to let the WO know which DCT channels are used for watermark detection. This will cause two issues for the framework. Firstly, the privacy issue: the image information of the DH might be leaked to the WO. Secondly, DH needs to send WO a large amount of data describing the selected DCT channels. To ensure the watermark detection performance, in our framework, DCT coefficients in the zig-zag order are split into two groups DCT^1 and DCT^2, as shown in Fig. 2. DCT^1 [e.g., grey areas in Fig. 3(b)] includes the DC coefficients and potentially higher frequency AC coefficients, and DCT^2 [e.g., white areas in Fig. 3(b)] includes the lower frequency AC coefficients. The CS transformation of DCT^2 serves for both secure watermark detection and privacy preserving storage while DCT^1 serves for privacy preserving storage only. This is because the watermark detection performance in the CS domain will be penalized if the coefficients from DCT^1 are included. Note that in Zeng and Liu's work [8], most watermarks are embedded in the low- and mid- frequency AC coefficients, while DC coefficients and most of the higher frequency AC coefficients are not even selected for watermark embedding [as demonstrated in Fig. 3(a)]. Including DC and higher frequency AC coefficients (none-watermark-carriers) will introduce noises for the watermark detection in the CS domain, as will be shown in our experimental results section. The DH needs to synchronize with WO about DCT^2 (e.g., Top 20 AC coefficients in the zig-zag order).

B. Secure CS Transformation Protocol

Our secure CS transformation protocol is a secure multiparty computation (MPC) protocol, the general goal of which is to enable parties to jointly compute a function over their inputs, while keeping these inputs private. Since the CS transformation essentially is a scalar product between vectors, our secure CS transformation protocol is constructed from secure scalar product protocol.

1) Secure Scalar Product Protocol: There are many existing secure scalar protocols such as homomorphism based, commodity server based, secret sharing based techniques as summarized in [24]. Homomorphism based techniques only require two parties to be involved in the computation process and let the third party have the final results, which is the best fit for our scenario. In this paper, we adopt the protocol proposed by Goethals *et al* [25] based on the Paillier public key system and its homomorphism properties. The definition

of homomorphism and the Paillier public key system are presented below:

Homomorphism:

Given two algebra systems A and B, $\bullet$ and $\circ$ are the operations in A, B, respectively. If $\forall$ x, y $\in$ A, we have $f(x \circ y) = f(x) \bullet f(y)$, then the mapping f: A $\rightarrow$ B is called A to B's homomorphism.

Paillier Cryptosystem [23]:

Let $N = ps$, where p and s are two large primes. Choose $g \in \mathbb{Z}^*_{N^2}$ (integers less than N^2 but bigger than zero) such that the order of g is divisible by N. Any such g is the form of $g \equiv (1+N)^a b^N mod\ N^2$ for a pair (a, b), where $g \in \mathbb{Z}_N$ and $g \in \mathbb{Z}^*_N$. Let $\lambda = lcm(p-1, s-1)$ (lcm means least common multiple). Then the public key is (g, N) and the private key is λ. Let $E_{pk}(m, r)$ be the encryption function using the public key, where m is the plaintext message and $r \in \mathbb{Z}_N$ is the blinding factor. Let $D_{sk}(c)$ be the decryption function using private key, where c is the ciphertext. The Paillier public key system has the following homomorphic properties:

$$D_{sk}(E_{pk}(m_1, r_1) \cdot E_{pk}(m_2, r_2)\ mod\ N^2) = m_1 + m_2\ mod\ N \quad \text{(a)}$$

$$D_{sk}(E_{pk}(m_1, r_1)^{m_2}\ mod\ N^2) = m_1 * m_2\ mod\ N \quad \text{(b)}$$

Goethals's original protocol contains two parties who will share the final scalar product. It is straightforward to extend it to a three party protocol, in which the added party will have the final scalar product result, as shown in Protocol 1.

Protocol 1. Private secure scalar protocol

Input: DH owns private vector $\vec{x} \in \mathbb{Z}^M$ and WO owns private vector $\vec{y} \in \mathbb{Z}^M$.

Output: Only CLD gets product $\vec{x} \cdot \vec{y}$.

1. Setup phase. DH does:
   Generate a Paillier key pair (sk, pk). Send pk to WO
2. DH does for $i \in \{1, \dots, M\}$:
   Generate a random new number r_i. Send $c_i = E_{pk}(\vec{x}_i, r_i)$ to WO.
3. WO does: Set $w \leftarrow \prod_{i=1}^{M} c_i^{\vec{y}_i}$.
   Generate a random plaintext $s_B \in \mathbb{Z}$ and a random number $r' \in \mathbb{Z}$.
   Send $w' = w \cdot E_{pk}(-s_B, r')$ to DH. Send s_B to CLD.
4. DH does: Computes $s_A = D_{sk}(w') = \vec{x} \cdot \vec{y} - s_B$ and sends $s_A \in \mathbb{Z}$ to CLD.
5. CLD has $\vec{x} \cdot \vec{y} = s_A + s_B$.

2) Secure CS Transformation Protocol: Based on Protocol 1, it is straightforward to give the secure CS transformation protocol (Protocol 2).

Protocol 2. Secure CS transformation

Input: DH has CS matrix $\Phi_{m \times n}$, WO has $\vec{v}$, an $n \times 1$ vector.

Output: CLD has $\vec{k} = \Phi_{m \times n} * \vec{v}$.

Between DH and WO, for all $\vec{\theta}_j$, where $1 \le j \le m$, a row of $\Phi_{m \times n}$, apply Protocol 1, let CLD have $\vec{\theta}_j^T \cdot \vec{v}$. Finally, CLD will have $\vec{k}_{m \times 1} = \Phi_{m \times n} * \vec{v}$.

3) Handling Real Values Through Scaling: The Pailler public key system only takes positive integers as input, while our framework involves real-number values. We scale the floating point values into integer values with certain scaling factor. Negative integers are represented by the upper half of the range $[0, N-1]$ (N is the modulo) in a modulo field, e.g., -1 is represented as $N-1$, as suggested in [26]. We show how to handle negative values in the Paillier homomorphic properties (a) and (b). Given two messages m_1 and m_2 to encrypt, and without loss of generality, assume m_1 is a positive number and m_2 is negative, where $|m_1|, |m_2| \in \mathbb{Z}_{N/2}$. Let $N + m_2$ represent m_2, we have:

$D_{sk}(E_{pk}(m_1, r_1) \cdot E_{pk}(N + m_2, r_2)\ mod\ N^2) = N + m_1 + m_2\ mod\ N = \tau$, then:

$$m_1 + m_2 = \begin{cases} \tau - N, & \tau > N/2 \\ m_1 + m_2, & \tau \le N/2 \end{cases}$$

$D_{sk}(E_{pk}(m_1, r_1)^{N+m_2}\ mod\ N^2) = m_1 * (N + m_2) mod\ N = \tau$, then:

$$m_1 * m_2 = \begin{cases} \tau - N, & \tau > N/2 \\ m_1 * m_2, & \tau \le N/2. \end{cases}$$

C. Analysis

1) Complexity Analysis: When the CLD has the image and the watermark pattern in the CS domain, watermark detection in the CS domain only involves linear correlation, hence only introducing negligible computational overhead. The computational and the communication complexity of Protocol 2 is based on Protocol 1. When the watermark size is n and the CS matrix size is m*n, WO performs m*n exponentiations and m encryptions in the public key domain, and DH performs m*m encryptions and m decryptions in the public key domain. For communication complexity, DH sends WO m*n public key encrypted values and WO sends DH m public key encrypted values.

Note that the DH might be a computationally weak party such as a mobile device. In our framework, the complexity of DH is reduced when there are multiple watermark owners who are interested in performing watermark detection. When there are multiple watermark owners who are involved in performing watermark detection on an image, the data holder can send the public key encrypted CS matrix to the cloud (i.e., Step 1&2 of Protocol 1 only needs to be done once for all watermark owners). The watermark owners can get the public key encrypted CS matrix from the cloud to continue the secure CS transformation protocol. Then DH only needs to receive m public key encrypted values and decrypt them (Step 4) for every run of Protocol 2.

In a practical system, some trade-offs between complexity and security could be considered. When a user has many images, the same CS matrix could be used multiple times for multiple images so that a CS encrypted watermark pattern could be stored and reused for secure watermark detection on multiple images. However, the security level of the CS transformation encryption might be sacrificed due to multi-time use of the same CS matrix on different images, as discussed in Section III.C.(2).

2) Security Analysis: It has been proven in the original paper [25] that Goethals's secure scalar protocol is secure under the semi-honest model. It is straightforward to see that the MPC protocols (Protocol 1&2) are also secure under the semi-honest assumption that all the parties follow the protocol strictly and no two parties will collude to attack a third party. After running the secure CS transformation protocol, DH and WO do not leak their private values to other parties. Only the CLD has the image data and watermark pattern in the CS domain.

The security of using compressive sensing transformation as an encryption has been explored in [20] and [21] and it was concluded that it is computationally secure under the brute force and structured attacks when each CS matrix is used only one time. So if the data holder encrypts different images with different CS matrix keys, the CS domain data are secure in the cloud.

When watermark detection with multiple watermark patterns is required for a certain image, multiple watermark patterns in the same CS domain are presented to the CLD. Such a scenario is similar to the system proposed by Lu *et al* [12], [13] for secure image retrieval. As discussed in the security analysis given in [12] and [13], when multiple data in the same random projection domain (ciphertext only) are obtained by a third party, it gains no additional information other than the correlations between different data. The leakage of correlation between the image and watermark patterns is inevitable since we desire the CLD to provide such watermark detection services. Since the watermark patterns we use are i.i.d Gaussian, their corresponding CS domain versions are uncorrelated (but dependent on the same CS matrix). So the CLD cannot infer anything about the watermarks.

As discussed in Section III.C.(1), if a practical system chooses to use the same CS matrix for multiple images to reduce the secure watermark detection complexity, multiple image data in the same CS domain will be presented to the CLD simultaneously, in which case their dependencies on the same CS matrix may reveal the correlations and Euclidean distances ([11] shows the distance preserving property of the CS transformation) between the images, and may be used to reduce the attacking complexity. In addition, statistical information of the multimedia data is common sense knowledge [21], which may also be used to reduce the attacking complexity. The RIP property in Section II.A suggests that the CS transformation can preserve the energy of the original data, which means the overall energy of the image's DCT coefficients is leaked to the CLD. But this problem can be addressed, since the data holder can normalize all the original data vectors before outsourcing the CS encrypted data to the CLD, and the normalization will not affect the performance of the watermark detection. More analysis considering the above security concerns will be studied in our future work.

3) Comparison to Previous Works and Complexity Evaluation: When compared to previous works, our framework has the following advantages:

1) Our framework utilizes the computing and storage resource of the cloud simultaneously and provides better efficiency and flexibility as the encrypted image data (and the encrypted watermark pattern under some circumstances, if so chosen) can be reused for multiple watermark detections in the cloud.
2) Most of the existing secure watermark detection works paid little attention to the privacy of the multimedia data, while our framework protects the privacy of the self-collected data.

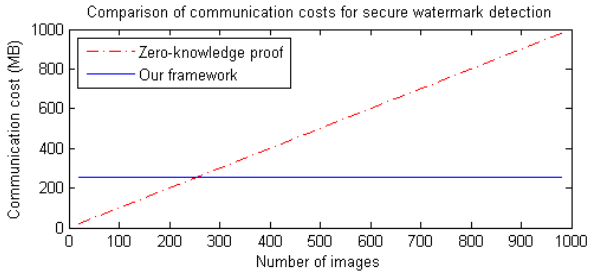

Fig. 4. Comparison of the communication costs between our framework and the Zero-knowledge proof protocol [6] when the total number of target images increases.

We compare the communication cost of our framework to other secure watermarking systems such as [6] under the following setting (chosen for the sake of complexity evaluation and comparison): the Paillier public key domain value takes 2048 bits; the image size is 1000×1; the secure CS transformation protocol is executed with a CS matrix size of 1000×1000 and a watermark size of 1000×1. We focus our evaluation on the communication cost of the data in the public key encryption domain, since it is the dominant factor over other communication cost. The watermark pattern is transformed to the CS domain in the initial step: DH needs to send WO around 256 MB of data (i.e., public key encrypted CS matrix) and WO needs to send 0.256 MB of data (i.e., public key encrypted watermark pattern) to DH. As analyzed above, when multiple images can be transformed to the same CS domain and the CS encrypted watermark pattern exists in the CLD, there is no communication cost between DH and WO for secure watermark detection. Note that for the previous secure watermarking systems such as [6], each time when secure watermark detection is performed on a new image, DH (corresponding to the verifier in [6]) has to work with WO (corresponding to the prover in [6]), which introduces computational and communication overhead for both DH and WO. As given in [6], the communication overhead to execute the zero-knowledge watermark detection protocol once is in the order of 1MB when the length of the watermark signal reaches 1000. In Fig. 4, we show that as the number of target images for secure watermark detection increases, our framework (when all the target images are transformed to the same CS domain) outperforms previous secure watermark detection systems such as [6] in terms of communication cost. Our framework has much better scalability and higher efficiency when performing secure watermark detection on a large number (e.g., thousands) of images, even though our framework has the semi-honest assumption that [6] is not constrained to.

TABLE I

MEAN SQUARE ERROR W.R.T SCALING FACTOR

Scaling factor	1.E3	1.E4	1.E5	1.E6	1.E7	1.E8
MSE	2.24 E-5	3.48 E-7	3.12 E-9	3.05 E-11	3.31 E-13	3.52 E-15

It is also very important to note that previous secure watermark detection methods [3]–[7] assume the multimedia data is available to all the parties and do not consider the privacy of the multimedia data. It might be possible to adapt those methods to protect the privacy of the multimedia data by encrypting it into a public key encryption domain. Then the computational and communication overhead will be increased significantly.

IV. EXPERIMENTAL RESULT

A. Experimental Settings and Notations

We tested the proposed system using some standard 512×512 images. For the watermark detection, there are several detection methods proposed in [8]. We choose the one in which the watermark pattern used for watermark detection is directly generated from a Normal distribution $N(0, 1)$. Given a CS matrix $\Phi_{m\times n}$, m/n will be referred to as the compressive sensing rate (*CS rate*). Since the CS matrix size will be extremely large if we convert the 512×512 image to a vector for CS transformation. Instead, we cut the image into pieces and each piece contains 64 8×8 DCT blocks. Selective DCT coefficients of each piece will form a vector and be transformed to a CS domain with the same CS rate but using different CS matrixes. The data in the CS domain from all pieces is treated as $\{p_i\}$. Similarly, we get $\{r_i\}$ from the 512×512 original watermark pattern. We test the watermark detection performance when different numbers of DCT components are transformed to the CS domain as DCT^2 in Fig. 2. In the rest of this section, "Top AC 20" means top 20 AC coefficients in the zigzag order are selected as DCT^2.

B. Scaling Floating Point to Integer Error Analysis

Since the MPC protocol is based on the Paillier public key system which requires integers as input, we scale the floating point values to integers with certain scaling factors. We test the error introduced by the conversion by comparing the result from secure CS transformation protocol to CS transformation with the original CS matrix and the watermark pattern. As shown in Table I, the MSE decreases significantly as the scaling factor increases. In the following experiments, the scaling factor is set to 1.0e8.

C. Secure Watermark Detection in the Compressive Sensing Domain

1) Assertions Validation: Table II summarizes the mean and variance of the sample covariance term in Equation (11) with different CS rates, under H_1 and H_0. The test result is based on several images including 512×512 'Lenna', 'Baboon', 'Barbara', 'Goldhill', 'Peppers' and etc. We can see that the covariance is very small and close to zero. However, it is interesting to see that under H_1, the covariance term is concentrated around a very small *negative* value. This may suggest that the expected watermark detection output q^{cs} might be slightly lower than the β in Eq.(11). Table III summarizes some values for λ in Eq. (12) and γ in Eq.(13) using 'Lenna', when different DCT components are selected. It shows that the assertion $\lambda > 0$ is true. Furthermore, if "Top AC 10" is chosen as DCT^2, γ is close to one, meaning that the CS transformation of such DCT channel coefficients will introduce nearly no distortion to the watermark detection. This is because almost all of the top 10 AC coefficients are selected for watermark embedding for the 'Lenna' image, while the distortions are mainly introduced by none-watermark-carriers that are mixed with watermark-carriers in the CS domain.

2) Watermark Detection in the CS Domain: Fig. 5 shows the watermark detection performance in the CS domain with different CS rates when different DCT components are selected. We give the watermark detection results (q under H_1) in the

TABLE II

TEST RESULTS OF THE COVARIANCE TERM IN EQUATION (11)

CS rate	1.0	0.7	0.4	0.1
H_1(mean/ variance)	-3.3E-03/ 1.98E-06	-3.36E-03/ 2.5E-06	-3.71E-03/ 3.64E-06	-5.51E-03/ 7.4E-06
H_0(mean/ variance)	1.69E-04/ 2.39E-06	8.59E-04/ 2.99E-06	-3.78E-03/ 5.09E-06	-1.63E-03/ 9.79E-06

TABLE III

VALIDATION FOR THE ASSERTION: $\lambda > 0$ (WHEN $m = n$).

(FOR THE 512 × 512 'LENNA' IMAGE)

Coefficients	$\frac{1}{n}\overline{(x_a y_a)^2}$	$\frac{1}{n}\overline{(x_a y_b)^2}$	λ	γ
Top AC 63	0.0179	0.0879	0.0704	2.24
Top AC 40	0.0301	0.089	0.0602	1.75
Top AC 30	0.0367	0.0926	0.0577	1.62
Top AC 20	0.0486	0.0707	0.0243	1.21
Top AC 10	0.1582	0.1627	0.0092	1.02

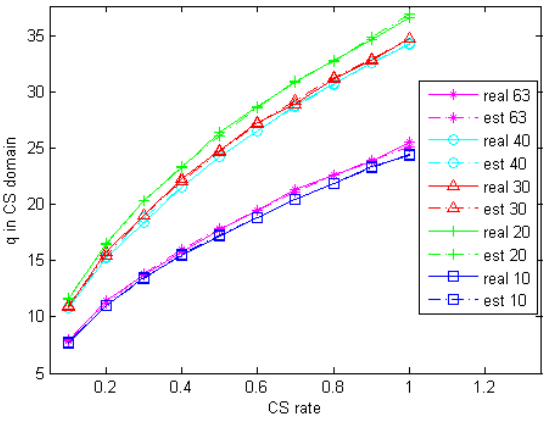

Fig. 5. Watermark detection in the CS domain under different CS rates when different DCT components are selected. For the legend of the figure, "real" means the mean of q^{cs} calculated from $\{z_i\}$, while "est" means the estimated mean of q^{cs} based on Equation (11). The number "xx" means "Top AC xx". (for the 512 × 512 'Lenna' image).

TABLE IV

WATERMARK DETECTION (q UNDER H_1) IN ORIGINAL DOMAIN WITH DIFFERENT DCT COEFFICIENTS. (FOR THE 512 × 512 'LENNA' IMAGE)

Top AC 63	Top AC 40	Top AC 30	Top AC 20	Top AC 10
5.6E+01	6.1E+01	5.6E+01	4.5E+01	2.5E+01

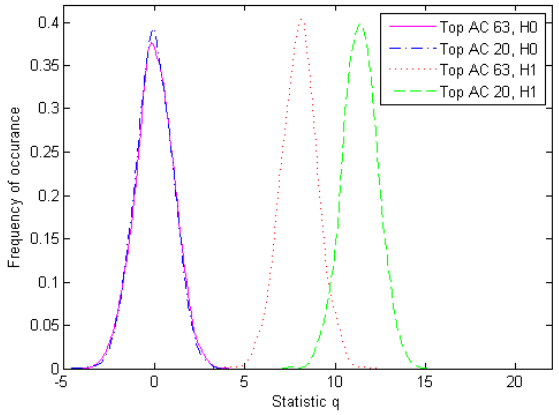

Fig. 6. q^{cs}'s distribution under H_0 and H_1 with CS rate 0.1 using the top 20 AC coefficients as DCT^2 and the top 63 AC coefficients as DCT^2 (for the 512 × 512 'Lenna' image).

original domain in Table IV. Table IV and Fig. 5 show that watermark detection in the CS domain has lower performance than in the original domain. The distortion is introduced by the CS transformation. Fig. 5 also presents the estimated q^{cs} based on Eq.(11). We can see that the estimated q^{cs} and the tested real q^{cs} agree with each other very well. The estimated q^{cs} is calculated based only on the original signals and the CS rate, but not on the CS matrix used. It can be used as a reference to set a certain CS rate and achieve desired watermark detection performance in that CS domain. From Fig. 5, we can see that when top 20 AC's are selected, the watermark detection performance is the best for the 512×512 'Lenna' image. This is because most of the watermarks are embedded in the top 20 AC coefficients and γ is relatively smaller as seen from Table III. The one with all the 63 AC coefficients selected has lower q^{cs} value because the higher frequency DCT coefficients without watermark embedded will introduce noise to the watermark detection.

Fig. 6 shows the distribution of the statistic q^{cs} with CS rate 0.1 by using the top 20 and 63 AC coefficients as DCT^2 for watermark detection for the 512×512 'Lenna' image. The figure shows that even with high dimension reduction, the watermark can still be detected.

We evaluate the watermark detection performance in the CS domain when both the watermark signals and certain noises are transformed to the CS domain simultaneously. Fig. 7 shows the watermark detection performance in the CS domain when Gaussian noise (generated by the Gaussian random value generator in Matlab) is inserted into the test image. The figure shows that the watermark detection performance decreases only slightly even when the zero-mean Gaussian noise has a standard deviation of 40. The CS reconstruction will introduce

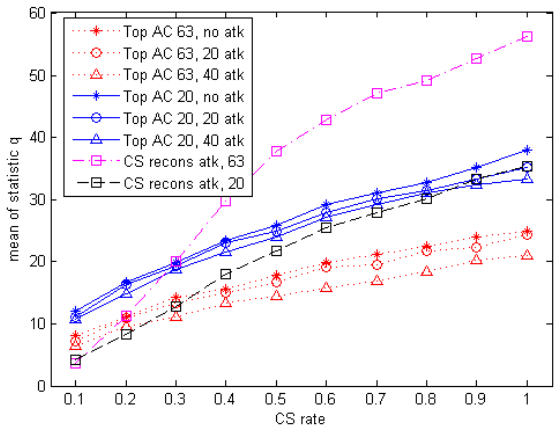

Fig. 7. The mean of q^{cs} at different CS rates under zero-mean Gaussian noise attack (i.e. "20 atk" means Gaussian noise with zero mean and standard deviation 20); The mean of q in the original domain after CS reconstruction (i.e. if top 63 AC coefficients are selected for CS transformation, denoted as "CS recons atk, 63"). (for the 512 × 512 'Lenna' image).

TABLE V

AVERAGE q^{cs} AND β FOR DIFFERENT IMAGES WHEN DIFFERENT TOP AC COEFFICIENTS ARE CHOSEN (CS RATE = 0.1)

Image/q^{orig}		TopAC 63	TopAC 20	TopAC 10
'Baboon'/ 1.16E+02	q^{cs}	3.26E+01	1.70E+01	9.93E+00
	β	3.29E+01	1.70E+01	9.97E+00
'Barbara'/ 6.01E+01	q^{cs}	1.45E+01	1.24E+01	8.48E+00
	β	1.45E+01	1.25E+01	8.52E+00
'Goldhill'/ 7.68E+01	q^{cs}	1.43E+01	1.56E+01	9.54E+00
	β	1.42E+01	1.56E+01	9.54E+00
'Peppers'/ 5.57E+01	q^{cs}	8.49E+00	1.04E+01	6.68E+00
	β	8.41E+00	1.04E+01	6.64E+00

distortion to the test image, which is referred to as CS reconstruction attack (e.g., labeled as "CS recons atk, 63" in Fig. 7) for the watermark detection. We transform the top 63 (and 20) AC coefficients to a CS domain and perform watermark detection in the original domain after CS reconstruction. Fig. 7 shows that when the CS rate is very low, the performance could be inferior to CS domain watermark detection, due to significant loss of information in the CS reconstruction process. Compared with "CS recons atk, 63", "CS recons atk, 20" of Fig. 7 shows that the watermark detection in the original domain after CS reconstruction is even lower than the CS domain across most CS rates. This is because most of the top 20 AC DCT channels are selected for watermark embedding and the CS reconstruction distortion to any of those channels will affect the watermark detection performance. However, the CS reconstruction distortion for "CS recons atk, 63" goes to the higher frequency DCT coefficients, most of which are not selected for watermark embedding.

Table V and Fig. 8 present the test results with 512 × 512 'Baboon' image, 'Peppers' image and etc. Table V gives the watermark detection results q^{cs} in the CS domain and the estimated watermark detection performance β, when different images and different AC coefficients are selected with CS rate being 0.1. The first column also gives the watermark detection q in the original domain. The table shows that even with a

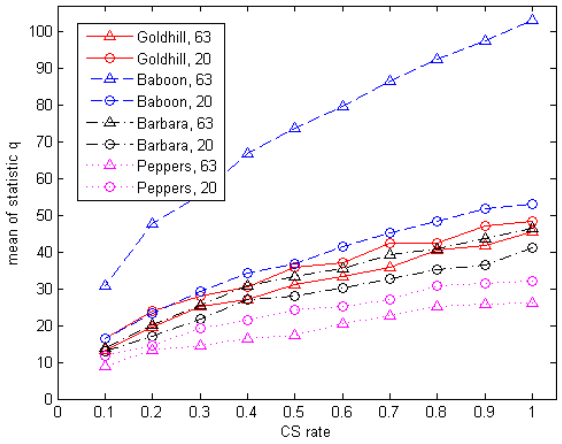

Fig. 8. Watermark detection performance in the CS domain for other images (i.e. "Goldhill, 63" means Goldhill image with top 63 AC coefficients selected).

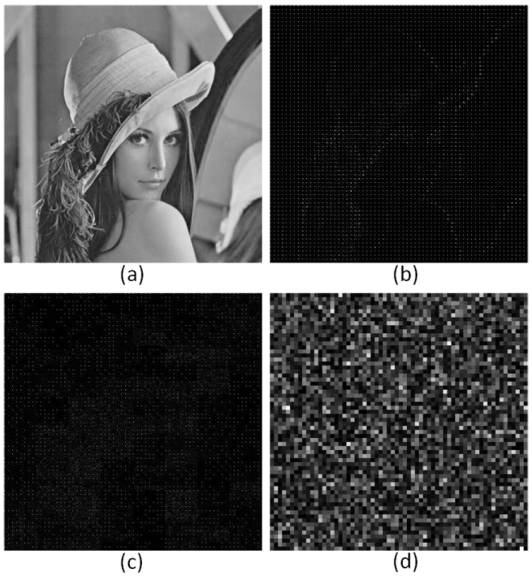

Fig. 9. (a) Original image; (b) Image in 8×8 DCT domain; (c) DCT coefficients after CS transformation; (d) Image reconstruction with the wrong CS matrix. (CS rate 1.0 is chosen here, similar effects are observed under other CS rates).

CS rate of 0.1, the watermark can still be successfully detected for all the images when different AC coefficients are selected. Furthermore, the table also confirms our analysis in Section II.C that β in Eq.(11) can be used for accurately estimating the expected watermark detection performance in the CS domain. Fig. 8 summarizes the watermark detection performance under different CS rates. The watermark detection performance in the CS domain for the 'Baboon' image is very good when top 63 AC coefficients are selected. This is because 'Baboon' is a highly textured image and many of its higher frequency DCT coefficients are also selected for watermark embedding.

D. Compressive Sensing Encryption

Fig. 9 shows the encryption results using the CS matrix as the encryption key. Fig. 9(d) shows that if a different CS matrix

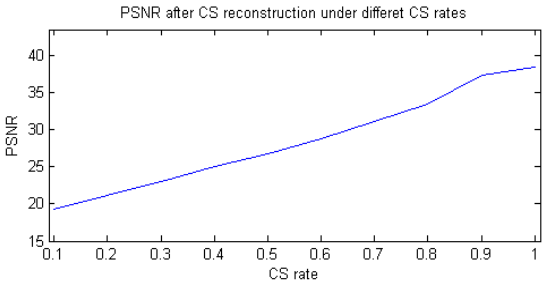

Fig. 10. CS reconstruction distortion when top 63 AC coefficients are transformed to the CS domain.

is used for the CS reconstruction, the reconstructed image is totally random. The block effect is due to the inverse-DCT operation on the 8×8 DCT block. If watch closely, it can be observed that Fig. 9(c) still preserves the spatial contour of Fig. 9(b) roughly. The reason is that the CS transformation in our experiment is performed piece-wisely as mentioned in Section IV.A instead of treating the whole image as a single vector. As the RIP property given in Section II.A suggests, the CS transformation can preserve the energy of the original data. Such spatial contour similarity between DCT coefficients in the original domain and the CS domain can be removed by permuting the order of the pieces or by treating the whole image as a single vector.

E. Compressive Sensing Reconstruction

For privacy preserving storage, since the DCT coefficients are not perfectly sparse, the CS reconstruction will introduce distortion to the reconstructed image, especially when CS rate is low. The CS reconstruction error has been studied in many other works. Here we present our CS reconstruction experimental results when all AC components are transformed to a CS domain. In order to have a good quality image after the CS reconstruction, the CS rate needs to be high. Our experiments show that the PSNR (Peak Signal-to-Noise Ratio) is around 35 after the CS transformation/reconstruction process when the CS rate is 0.8, as shown in Fig. 10. Even when the CS rate is set to 1.0, the CS reconstruction algorithm (Orthogonal Matching Pursuit) still introduces distortion as we can see the PSNR is around 38. However, it should be noted that when the CS rate equals 1.0, the original DCT coefficients can be recovered perfectly given the inverse of the CS matrix, in which case CS reconstruction is not necessary.

V. Conclusion

This paper proposes a compressive sensing based secure signal processing framework that enables simultaneous secure watermark detection and privacy preserving storage. Our framework is secure under the semi-honest adversary model to protect the private data. Note that without the semi-honest assumption, our framework will fail to protect the secret values. For example, collusion between WO and CLD will cause the leakage of DH's CS matrix. When compared to previous secure watermark detection protocols, our framework offers better efficiency and flexibility, and protects the privacy

of the multimedia data that has not yet been considered in the previous works. We have demonstrated that secure watermark detection in the CS domain is feasible theoretically and experimentally. More theoretical analysis of the covariance term in Eq.(11) will be conducted in the future work. In addition to watermark detection, our framework can also be extended for other secure signal processing algorithms. Future work also includes further evaluation of the robustness of the watermark detection in the CS domain under some other attacks. In addition to secure CS transformation, developing MPC protocols for secure CS reconstruction is part of our future work too.

APPENDIX I

Proof of Lemma 2:

An equivalent way to interpret the second formula from Lemma 1 [11] is:

$$Var\left[P^T R|X,Y\right] = \frac{1}{m}\left(\sum_1^n x_i^2 \sum_1^n y_i^2 + \left(\sum_1^n x_i y_i\right)^2\right)$$

Since given X and Y, $\{p_i\}$ and $\{r_i\}$ are both i.i.d. Gaussian, then $z_i^{cs} = p_i r_i$ are i.i.d., therefore:

$$\begin{aligned} Var\left(z_i^{cs} \mid X,Y\right) &= \frac{1}{m} Var\left[P^T R|X,Y\right] \\ &= \frac{1}{m^2}\left(\left(\sum_{i=1}^n x_i y_i\right)^2 + \sum_{i=1}^n x_i^2 \sum_{i=1}^n y_i^2\right) \end{aligned}$$

■

The proof above is based on Lemma 1. However, the link of the proof for Lemma 1's second equation is invalid in [11]. We give our proof of Lemma 2 here, in case the reader is interested.

$$\begin{aligned} E\left(V_{z_i^{cs}}^2|X,Y\right) &= Var\left(z_i^{cs} \mid X,Y\right) \\ &= Var\left[\left(\sum_{j=1}^n \Phi_{i,j} x_j\right) * \left(\sum_{j=1}^n \Phi_{i,j} y_j\right)\right] \\ &= \sum_{a=1}^n \sum_{b=1}^n \sum_{c=1}^n \sum_{d=1}^n \\ &\quad Cov[\Phi_{i,a}\Phi_{i,b}x_a y_b, \Phi_{i,c}\Phi_{i,d}x_c y_d] \\ &= \sum_{a=1}^n \sum_{b=1}^n \sum_{c=1}^n \sum_{d=1}^n x_a y_b x_c y_d \\ &\quad \times Cov\left[\Phi_{i,a}\Phi_{i,b}, \Phi_{i,c}\Phi_{i,d}\right]. \end{aligned}$$

There are three different values for $Cov\left[\Phi_{i,a}\Phi_{i,b}, \Phi_{i,c}\Phi_{i,d}\right]$:

1. When $a = b = c = d$:

Based on the moment-generating function of a Gaussian distribution, it is easy to derive the second and fourth moments of $\Phi_{i,a} \sim N(0, \frac{1}{m})$ as:

$$E\left(\Phi_{i,a}^2\right) = \frac{1}{m}, \quad E\left(\Phi_{i,a}^4\right) = \frac{3}{m^2}$$

Then:

$$\begin{aligned} Cov\left[\Phi_{i,a}\Phi_{i,a}, \Phi_{i,a}\Phi_{i,a}\right] &= Var\left(\Phi_{i,a}^2\right) \\ &= E\left(\Phi_{i,a}^4\right) - E^2\left(\Phi_{i,a}^2\right) = \frac{2}{m^2} \end{aligned}$$

2. When $(a = c, b = d,\ a \neq b)$ or $(a = d, b = c,\ a \neq b)$:

$$\begin{aligned} Cov\left[\Phi_{i,a}\Phi_{i,b}, \Phi_{i,a}\Phi_{i,b}\right] &= Var\left(\Phi_{i,a}\Phi_{i,b}\right) \\ &= Var\left(\Phi_{i,a}\right) * Var\left(\Phi_{i,b}\right) = \frac{1}{m^2} \end{aligned}$$

3. Without loss of generality, when a is not equal with any of bcd:

$$\begin{aligned} &Cov\left(\Phi_{i,a}\Phi_{i,b}, \Phi_{i,c}\Phi_{i,d}\right) \\ &\quad = E\left(\Phi_{i,a}\Phi_{i,b}\Phi_{i,c}\Phi_{i,d}\right) - E\left(\Phi_{i,a}\Phi_{i,b}\right) E\left(\Phi_{i,c}\Phi_{i,d}\right) \\ &\quad = E\left(\Phi_{i,a}\right) E\left(\Phi_{i,b}\Phi_{i,c}\Phi_{i,d}\right) \\ &\quad -E\left(\Phi_{i,a}\right) E\left(\Phi_{i,b}\right) E\left(\Phi_{i,c}\Phi_{i,d}\right) = 0 \end{aligned}$$

Then we have:

$$\begin{aligned} &x_a y_b x_c y_d Cov\left[\Phi_{i,a}\Phi_{i,b}, \Phi_{i,c}\Phi_{i,d}\right] \\ &= \begin{cases} \frac{2*x_a^2 y_a^2}{m^2}, & \text{if } a = b = c = d \\ \frac{x_a y_b x_a y_b}{m^2}, & \text{if } (a = c, b = d,\ a \neq b) \\ \frac{x_a y_b x_b y_a}{m^2}, & \text{if } (a = d, b = c,\ a \neq b) \\ 0, & \text{otherwise} \end{cases} \end{aligned}$$

Then:

$$\begin{aligned} &\sum_{a=1}^n \sum_{b=1}^n \sum_{c=1}^n \sum_{d=1}^n x_a y_b x_c y_d \\ &\quad \times Cov\left[\Phi_{i,a}\Phi_{i,b}, \Phi_{i,c}\Phi_{i,d}\right] \\ &= \frac{1}{m^2}(2\sum_{a=1}^n (x_a y_a)^2 + \sum_{b=1,b\neq a}^n \\ &\quad \sum_{a=1}^n x_a y_b x_a y_b + \sum_{b=1,b\neq a}^n \sum_{a=1}^n x_a y_a x_b y_b) \\ &= \frac{1}{m^2}(\left(\sum_{a=1}^n (x_a y_a)^2 + \sum_{b=1,b\neq a}^n \sum_{a=1}^n x_a y_a x_b y_b\right) \\ &\quad + \left(\sum_{a=1}^n (x_a y_a)^2 + \sum_{b=1,b\neq a}^n \sum_{a=1}^n x_a y_b x_a y_b\right)) \\ &= \frac{1}{m^2}\left(\sum_{b=1}^n \sum_{a=1}^n x_a y_a x_b y_b + \sum_{b=1}^n \sum_{a=1}^n x_a y_b x_a y_b\right) \\ &= \frac{1}{m^2}\left(\sum_{a=1}^n x_a y_a \sum_{a=1}^n x_a y_a + \sum_{a=1}^n x_a x_a \sum_{a=1}^n y_a y_a\right) \end{aligned}$$

Therefore:

$$E(V_{z_i^{cs}}^2|X,Y) = \frac{1}{m^2}\left(\left(\sum_{i=1}^n x_i y_i\right)^2 + \sum_{i=1}^n x_i^2 \sum_{i=1}^n y_i^2\right).$$

■

REFERENCES

[1] T. Bianchi and A. Piva, "Secure watermarking for multimedia content protection: A review of its benefits and open issues," *IEEE Signal Process. Mag.*, vol. 30, no. 2, pp. 87–96, Mar. 2013.

[2] Z. Erkin, A. Piva, S. Katzenbeisser, R. Lagendijk, J. Shokrollhi, G. Neven, *et al.*, "Protection and retrieval of encrypted multimedia content: When cryptography meets signal processing," *EURASIP J. Inf. Security*, vol. 7, no. 2, pp. 1–20, 2007.

[3] J. Eggers, J. Su, and B. Girod, "Public key watermarking by eigenvectors of linear transforms," in *Proc. Euro. Signal Process. Conf.*, 2000.

[4] S. Craver and S. Katzenbeisser, "Security analysis of public-key watermarking schemes," in *Proc. Math. Data/Image Coding, Compress., Encryption IV, Appl.*, vol. 4475. 2001, pp. 172–182.

[5] A. Adelsbach and A. Sadeghi, "Zero-knowledge watermark detection and proof of ownership," in *Proc. 4th Int. Workshop Inf. Hiding*, vol. 2137. 2001, pp. 273–288.

[6] J. R. Troncoso-Pastoriza and F. Perez-Gonzales, "Zero-knowledge watermark detector robust to sensitivity attacks," in *Proc. ACM Multimedia Security Workshop*, 2006, pp. 97–107.

[7] M. Malkin and T. Kalker, "A cryptographic method for secure watermark detection," in *Proc. 8th Int. Workshop Inf. Hiding*, 2006, pp. 26–41.

[8] W. Zeng and B. Liu, "A statistical watermark detection technique without using original images for resolving rightful ownerships of digital images," *IEEE Trans. Image Process.*, vol. 8, no. 11, pp. 1534–1548, Nov. 1999.

[9] N. A. Weiss, *A Course in Probability*. Reading, MA, USA: Addison-Wesley, 2005, pp. 385–386.

[10] O. Goldreich, *The Foundations of Cryptography*. Cambridge, U.K.: Cambridge Univ. Press, 2004.

[11] K. Liu, H. Kargupta, and J. Ryan, "Random projection-based multiplicative data perturbation for privacy preserving distributed data mining," *IEEE Trans. Knowl. Data Eng.*, vol. 18, no. 1, pp. 92–106, Jan. 2006.
[12] W. Lu, A. L. Varna, A. Swaminathan, and M. Wu, "Secure image retrieval through feature protection," in *Proc. IEEE Conf. Acoust., Speech Signal Process.*, Apr. 2009, pp. 1533–1536.
[13] W. Lu, A. L. Varna, and M. Wu, "Security analysis for privacy preserving search for multimedia," in *Proc. IEEE 17th Int. Conf. Image Process.*, Sep. 2010, pp. 2093–2096.
[14] D. Donoho, "Compressed sensing," *IEEE Trans. Inf. Theory*, vol. 52, no. 4, pp. 1289–1306, Apr. 2006.
[15] M. Rudelson and R. Vershynin, "Sparse reconstructions by convex relaxation: Fourier and Gaussian measurements," in *Proc. Conf. Inf. Sci. Syst.*, Mar. 2006, pp. 207–212.
[16] J. Tropp and A. Gilbert, "Signal recovery from random measurements via orthogonal matching pursuit," *IEEE Trans. Inf. Theory*, vol. 53, no. 12, pp. 4655–4666, Dec. 2007.
[17] M. Davenport, P. Boufounos, M. Wakin, and R. Baraniuk, "Signal processing with compressive measurements," *IEEE J. Sel. Topics Signal Process.*, vol. 4, no. 2, pp. 445–460, Apr. 2010.
[18] R. Calderbank, S. Jafarpour, and R. Schapire. (2009). Compressed learning: Universal sparse dimensionality deduction and learning in the measurement domain [Online]. Available: http://dsp.rice.edu/cs
[19] D. Hsu, S. M. Kakade, J. Langford, and T. Zhang, "Multi-label prediction via compressed sensing," in *Proc. NIPS*, 2009, pp. 772–780.
[20] Y. Rachlin and D. Baron, "The secrecy of compressed sensing measurement," in *Proc. 46th Annu. Allerton Conf. Commun., Control, Comput.*, 2008, pp. 813–817.
[21] A. Orsdemir, H. O. Altun, G. Sharma, and M. F. Bocko, "On the security and robustness of encryption via compressed sensing," in *Proc. IEEE Military Commun. Conf.*, Nov. 2008, pp. 1040–1046.
[22] S. Voloshynovskiy, O. Koval, F. Beekhof, and T. Pun, "Random projection based item authentication," *Proc. SPIE Photon. West, Electron. Imag./Media Forensics Sec. XI*, San Jose, CA, USA, Feb. 2009, pp. 725413-1–725413-1.
[23] P. Paillier, "Public-key cryptosystems based on composite degree residuosity classes," in *Proc. Adv. Cryptology-Eurocrypt*, 1999, pp. 223–238.
[24] I.-C. Wang, C. Shen, J. Zhan, T. Hsu, C. Liau, and D. Wang, "Toward empirical aspects of secure scalar product," *IEEE Trans. Syst., Man, Cybern.*, vol. 39, no. 4, pp. 440–447, Jul. 2009.
[25] B. Goethals, S. Laur, H. Lipmaa, and T. Mielikainen, "On private scalar product computation for privacy-preserving data-mining," in *Proc. 7th Int. Conf. Inf. Security Cryptology*, 2004, pp. 104–120.
[26] F. Kerschbaum, D. Biswas, and S. Hoogh, "Peformance comparison of secure comparison protocols," in *Proc. 20th Int. Workshop Database Expert Syst. Appl.*, 2009, pp. 133–136.
[27] L. Zhang, "Sample mean and sample variance: Their covariance and their (in) dependence," *Amer. Statist.*, vol. 61, no. 2, pp. 159–160, 2007.

Qia Wang was born in Shenyang, China, in 1985. He received the B.E. degree in computer science from Tongji University, Shanghai, China, in 2007, and the Ph.D. degree in computer science from the University of Missouri, Columbia, MO, USA, in 2013. His research interests include compressive sensing, encrypted domain signal processing, mobile computing, mobile multimedia, and computer vision. He was a Research Intern with the Media Networking Laboratory, Huawei Technologies, NJ, USA, in 2010 and 2013, respectively. He is currently with Samsung Telecommunications America, Seattle, WA, USA.

Wenjun Zeng (M'97–SM'03–F'12) is a Professor with the Computer Science Department, University of Missouri, Columbia, MO, USA. He received the B.E. degree from Tsinghua University, the M.S. degree from the University of Notre Dame, and the Ph.D. degree from Princeton University all in electrical engineering. His current research interests include mobile computing, social-semantic media analysis, distributed video coding, 3D analysis and coding, multimedia networking, and content/network security.

Prior to joining University of Missouri in 2003, he was with PacketVideo Corporation, Sharp Laboratories of America, Bell Laboratories, and Panasonic Technology. From 1998 to 2002, he was an active contributor to the JPEG 2000 and MPEG4 IPMP standard. He is an Associate Editor of the IEEE TRANSACTIONS ON CIRCUITS AND SYSTEMS FOR VIDEO TECHNOLOGY, and the IEEE MULTIMEDIA, was an Associate Editor of the IEEE TRANSACTIONS ON INFORMATION FORENSICS AND SECURITY, and the IEEE TRANSACTIONS ON MULTIMEDIA (TMM), and was on the Steering Committee of the IEEE TMM from 2009 to 2012. He served as the TPC Co-Chair of the 2013 IEEE International Workshop on Information Forensics and Security, and a Guest Editor of the ACM Transactions on Multimedia Computing, Communications, and Applications Special Issue on ACM Multimedia 2012 Best Papers. He served as the Steering Committee Chair of the IEEE International Conference on Multimedia and Expo (ICME) in 2010 and 2011, and has served as the TPC Vice Chair of ICME 2009, the TPC Chair of the IEEE Consumer Communications and Networking Conference in 2007, the TPC Co-Chair of the Multimedia Communications and Home Networking Symposium of the IEEE International Conference on Communications in 2005. He was a Guest Editor (GE) of the Special Issue on Recent Advances in Distributed Multimedia Communications of Proceedings of the IEEE in 2008 and the Lead GE of the Special Issue on Streaming Media of the IEEE TMM in 2004. He is a Fellow of the IEEE.

Jun Tian was born in Wuhan, China, in 1971. He received the Ph.D. degree in mathematics from Rice University in 1996. From 1988 to 1991, he was with Beijing University. He is with Huawei Technologies, serving on the patent review board of media technologies. He was a Senior Member of Technical Staff with Thomson Corporate Research; Principal Research Engineer with Brain Media; Visiting Professor of mathematics with Jacobs University; Senior Research Engineer with Digimarc; and Research Scientist/Project Manager with Rice University. His research interests are in the areas of audio/image/video processing, geometric analysis, media security, multimedia communication, and wavelet analysis. He was the Conference Chair of the 2001 SPIE Conference on Image Compression and Encryption Technologies. He received the Extraordinary Achievement Award from Thomson in 2007 for his contribution to the Digital Cinema Project. His article entitled Reversible data embedding using a difference expansion in the IEEE TRANSACTIONS ON CIRCUITS AND SYSTEMS FOR VIDEO TECHNOLOGY, has been selected as a featured fast moving front paper in 2009 issue of Science Watch. He holds 26 granted U.S. patents.