ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 8, August 2015

Reduction Secure Watermarking Detection Signal Sensing by CS Protocol

Balasubramanyam, Bullarao Domathoti, Nageswara Rao Putta

Pursuing M. Tech, Dept. of CSE., SITS, JNT University Aanthapur, Tirupati, AP, India.

Assistant Professor, Dept. of CSE., SITS, JNT University Aanthapur, Tirupati, AP, India.

Associate Professor, Dept. of CSE., SITS, JNT University Aanthapur, Tirupati, AP, India.

ABSTRACT: Privacy could be a vital issue once knowledge, the information house owners source data storage or process to a 3rd party computing service, like the cloud. during this paper, we tend to determine a cloud computing application state of affairs that needs at the same time playacting secure watermark detection and privacy conserving multimedia system information storage. we tend to then propose a compressive sensing (CS)-based framework mistreatment secure multiparty computation (MPC) protocols to handle such a demand. In our framework, the multimedia system information and secret watermark pattern are conferred to the cloud for secure watermark detection in a very cesium domain to shield the privacy. throughout cesium transformation, the privacy of the cesium matrix and also the watermark pattern is protected by the MPC protocols beneath the semi-honest security model. we tend to derive the expected watermark detection performance within the caesium domain, given the target image, watermark pattern, and also the size of the caesium matrix (but while not the caesium matrix itself). The correctness of the derived performance has been valid by our experiments. Our theoretical analysis and experimental results show that secure watermark detection within the caesium domain is possible. Our framework may be extended to alternative cooperative secure signal process and data-mining applications within the cloud.

KEYWORDS: Compressive sensing; secure watermark detection; secure signal processing; secure multiparty computation; privacy preserving;

I. INTRODUCTION

The cloud computing technologies are growing, and it's a lot of economical for knowledge|the info|the information} holders to shift data storage or signal process computations to the cloud rather than getting hardware and code by themselves. Ideally, the cloud can store the info associated perform signal process or data-mining in an encrypted domain so as to preserve the info privacy. Meanwhile, attributable to the rising of the net and social networks, it's terribly straightforward for a user to gather a large quantity of multimedia system information from completely different sources while not knowing the copyright data of these information.

The user might want to require advantage of the cloud for storage, at identical time, work with copyright house owners for watermark detection whereas keeping those collected multimedia system information personal. The watermark pattern owner desires to stay their watermark patterns personal throughout the watermark detection additionally. A legal cloud giving storage services may additionally need to participate in watermark detection initiated by the users, or initiate watermark detection itself while not the involvement of the users, to envision if the uploaded multimedia system information is copyright protected. Another advantage of storing the encrypted multimedia system information associated facilitating encrypted domain watermark detection within the cloud is that those encrypted information may be reused if the image information holder (or the cloud) must work with alternative watermark house owners later for secure watermark detection ancient secure watermark detection techniques area {unit|square measure} designed to convert a booster whether or not or not a watermark is embedded while not revealing the watermark pattern so an un trustworthy booster cannot take away the watermark from the watermark protected copy . 2 sorts of approaches are planned for secure watermark detection: uneven watermarking and zero-knowledge watermark detection. However, most of the prevailing secure watermark Detection works assume the watermarked copy ar

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 8, August 2015

publically accessible and specialize in the safety of the watermark pattern, whereas the privacy of the target media on that watermark detection is performed has received very little attention. except for some applications like the state of affairs given higher than, it's needed to shield the multimedia system data's privacy within the watermark detection method.

playacting privacy conserving storage and secure watermark detection at the same time is feasible by mistreatment the prevailing secure watermark detection technologies like zero-knowledge proof protocols that remodel the multimedia system information to a public key cryptography domain. However, their limitations, like sophisticated algorithms, high procedure and communication quality and huge storage consumption within the public key cryptography domain, could impede their p In our framework, the target image/multimedia information is possessed by the image holder solely. 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 information to a compressive sensing domain before outsources it to the cloud. For secure watermark detection, the watermark is reworked to identical compressive sensing domain employing a secure multiparty computation (MPC) protocol so sent to the cloud. The cloud solely has the info in the=compressive sensing domain. while not the compressive sensing matrix, the cloud cannot reveal the first multimedia system information and also the watermark pattern. The cloud can perform watermark detection within the compressive sensing domain. The image information within the compressive sensing domain may be hold on within the cloud and reused for detection of watermark from several alternative watermark house owners.ctical applications.

II. RELATED WORK

However, most of the prevailing secure watermark detection works assume the watermarked copy ar publically accessible and specialize in the safety of the watermark pattern, whereas the privacy of the target media on that watermark detection is performed has received very little attention. except for some applications it's needed to shield the multimedia system data's privacy within the watermark detection method. playacting privacy conserving storage and secure watermark detection at the same time is feasible by mistreatment the prevailing secure watermark detection technologies like zero-knowledge proof protocols that remodel the multimedia system information to a public key cryptography domain. However, their limitations, like sophisticated algorithms, high procedure and communication quality and huge storage consumption within the public key cryptography domain, could impede their sensible applications Most of the prevailing secure watermark detection works paid very little attention to the privacy of the multimedia system information, whereas our framework protects the privacy of the self collected information.

III. PROPOSED ALGORITHM

ancient secure watermark detection techniques area {unit|square measure} designed to convert a booster whether or not or not a watermark is embedded while not revealing the watermark pattern so associate un trustworthy booster cannot take away the watermark from the watermark protected copy during this paper, we tend to propose a compressive sensing based mostly privacy conserving watermark detection framework that leverages secure multiparty computation and also the cloud. it's been shown that several signal process algorithms performed within the caesium domain have terribly shut performance as performed within the original domain .Using random matrix transformation for privacy conserving data-mining has conjointly been planned, that planned a random projection information perturbation approach for privacy conserving cooperative data-mining. The planned a secure image retrieval system through random projection and have proved that the planned random projection domain multimedia system retrieval system is secure beneath the Cipher text solely Attack model (COA) and also the semi-honest model . what is more that caesium transformation are able to do computationally secure cryptography. These works indicate that signal process or data-mining within the caesium domain is possible and is computationally secure beneath sure conditions. In our framework, the target image/multimedia information is possessed by the image holder solely. 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 information to a compressive sensing domain before outsources it to the cloud. For secure watermark detection, the watermark is reworked to identical compressive sensing domain employing a secure multiparty computation (MPC) protocol so sent to the cloud. The cloud solely has the info within the compressive sensing domain. while not the compressive sensing matrix, the cloud cannot reveal the first multimedia system information and also the watermark pattern. The cloud can perform watermark detection within the compressive

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 8, August 2015

sensing domain. The image information within the compressive sensing domain may be hold on within the cloud and reused for detection of watermark from several alternative watermark house owners.

A. Data Admin(Holder):

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.

B. *Watermark Owner* :

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.

C. *Compressive Sensing*:

The compressive sensing theory asserts that when a signal can be represented by a small number of nonzero coefficients, it can be perfectly recovered after being transformed by a limited number of incoherent, non-adaptive linear measurements. Most of the literature of compressive sensing has focused on improving the speed and accuracy of compressive sensing reconstruction 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.

D. *Correlation in Watermarking*:

In this module correlation module Watermark--an invisible signature embedded inside an image to show authenticity or proof of ownership Discourage unauthorized copying and distribution of images over the internet. Ensure a digital picture has not been altered. This can be used to search for a specific watermark

E. *Secure CS Transformation Protocol*:

Our secure CS transformation protocol is a secure multi- party 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 trans- formation 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 exist- ing secure scalar protocols such as homomorphism based, commodity server based, secret sharing based techniques as summarized in [4]. 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 [2] 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, • and ◦ are the operations in A, B, respectively. If ∀ x, y ∈ A, we have f (x ◦ y) = f (x) • f (y), then the mapping f: A → B is called A to B's homomorphism. Paillier Cryptosystem [23]: Let N = ps, wherep and s are two large primes. Chooseg ∈ Z∗ N2 (integers less than N2 but bigger than zero) such that the order of g is divisible by N. Any suchg is the form of g ≡(1+ N)abNmod N2 for a pair (a, b), whereg ∈ ZN and g ∈ Z∗ N. Letλ=lcm(p−1,s−1) (lcm means least common multiple). Then the public key is (g, N) and the private key is λ. LetEpk(m,r) be the encryption function using the public key, where m is the plaintext message and r ∈ ZN is the blinding factor. Let Dsk(c) be the decryption function using private key, where c is the ciphertext. The Paillier public key system has the following homomorphic properties: Dsk(Epk(m1,r1)· Epk(m2,r2)mod N2)=m1+m2 mod N (a) Dsk(Epk(m1,r1)m2 mod N2)=m1 ∗m2 mod N (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.

F. DCT(Discrete Cosine Transformation in Cs Matrix)Using Image Processing:

- Divides image into parts based on the visual quality of the image
- Input image
- intensity of pixel in row i and column j
- DCT coefficient in DCT matrix

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

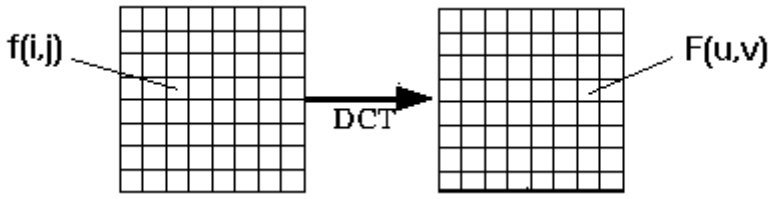
International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 8, August 2015

- Larger amplitudes closer.

Compression possible because higher order coefficients are *generally* negligible



***Restricted Isometry Property (RIP)*:** A vector x ∈ Rn is k-sparse if |{j:| xj| > 0}|≤ k. A matrix Φ ∈ Rm×n is said to have the Restricted Isometry Property of order k and level δ ∈(0,1) (equivalently, (k,δ)-RIP) if

$$(1-\delta)\, x\Phi\, x \leq (1+\delta)x\ 22 \quad (1)$$

for all k-sparse x ∈ Rn.

The restricted isometry constant δk is defined as the smallest value of δ for which the above inequality holds. The compressive sensing theory [4] 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 ∈ Rn is a k-sparse vector (only k out of the n elements of s are nonzero) and can be transformed to x ∈ Rm, m < n, wherex = Φm×ns. If Φm×n satisfies RIP, it can be shown [4] that solving the below optimization problem:

Mins1 s.t. x =Φm×ns (2) is equivalent to finding the sparsest solution s to x =Φm×ns, provided m ≥ Cklog(n/k), whereC is a small constant. Eq. (2) presents a L1 minimization problem which can be solved by orthogonalmatching pursuit (OMP) algorithms [6]. It has been shown [5] that there are many ways to construct a matrixΦm×n that meets the RIP property, e.g., if the entries of matrix Φm×n are generated from a Gaussian distribution with zero mean and variance 1/m, Φm×n is a RIP matrix with overwhelming probability. In our framework, the com- pressive 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 [7] 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 [9] 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 vec- tors could be done in the compressive sensing domain. Calderbank et al [8] 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 [1] was also used for privacy preserving data-mining. The paper by Liu et al [1] gave the following lemma about linear correlation in the compressive sensing domain: Lemma

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 8, August 2015

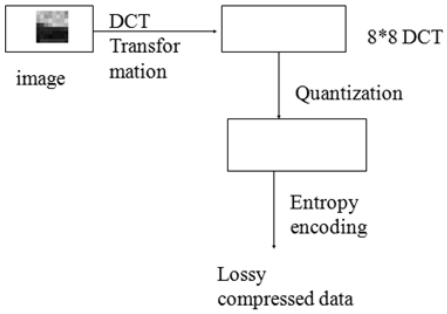


Fig:DTC coding system

IV. EXPERMENTAL RESULTS

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 Φm×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 {pi}. Similarly, we get {ri} 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 DCT2 in Fig. 2. In the rest of this section, "Top AC 20" means top 20 AC coefficients in the zigzag order are selected as DCT2.

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.

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 H1 and H0. The test result is based on several images including 512×512 'Lenna', 'Baboon', 'Barbara', 'Goldhill', 'Peppers' and etc. We can see that

TABLE II Test Results Of The Covarianceterm In Equation

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:λ>0 (whenm =n). (for the512×512 '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

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 8, August 2015

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 qcs calculated from {zi}, while "est" means the estimated mean of qcs based on Equation . The number "xx" means "Top AC xx". (for the 512×512 'Lenna' image).The covariance is very small and close to zero. However, it is interesting to see that under H1, the covariance term is concentrated around a very small negative value. This may suggest that the expected watermark detection output qcs 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 λ>0 is true. Furthermore, if "Top AC 10" is chosen as DCT2, 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 showsthe watermark detection performance in the CS domain with dif- ferent CS rates when different DCT components are selected. We give the watermark detection results (q under H1) in the WANG et al.: Compressive Sensing Based Secure Watermark Detection 1325

TABLE IV watermarkdetection(q under h1) in originaldomainwith differentdctcoefficients.(for the512×512 '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

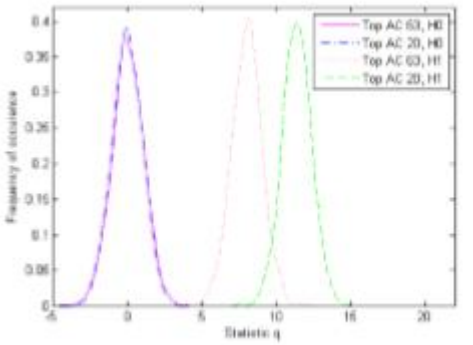


Fig. 6. qcs's distribution under H0 and H1 with CS rate 0.1 using the top 20 AC coefficients as DCT2 and the top 63 AC coefficients as DCT2 (for the 512×512 'Lenna' image).

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 qcs based on Eq.(11). We can see that the estimated qcs and the tested real qcs agree with each other very well. The estimated qcs 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 qcs 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 qcs with CS rate 0.1 by using the top 20 and 63 AC coefficients as DCT2 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 (generatedby the Gaussian randomvalue 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

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 8, August 2015

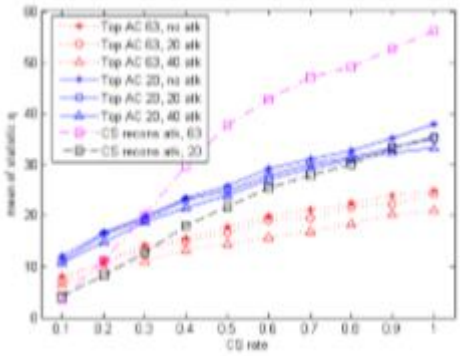


Fig. 7. The mean of qcs at different CS rates under zero-mean Gaussian noise attack (i.e. "20 atk" means Gaussian noise with zero mean and standard deviation 20); The mean of q in the original domain after CS reconstruction (i.e. if top 63 AC coefficients are selected for CS transformation, denoted as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

TABLE V Average Qcs And B For Differentimages When Differenttop Ac Coefficientsare 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 recon- struction 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 watermarkdetectionin 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.

V. CONCLUSION AND FUTURE WORK

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 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.

REFERENCES

1. D. Donoho, "Compressed sensing," IEEE Trans. Inf. Theory, vol. 52, no. 4, pp. 1289–1306, Apr. 2006.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 8, August 2015

2. 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.
3. 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.
4. 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.
5. 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
6. D. Hsu, S. M. Kakade, J. Langford, and T. Zhang, "Multi-label predic- tion via compressed sensing," in Proc. NIPS, 2009, pp. 772–780.
7. Y. Rachlin and D. Baron, "The secrecy of compressed sensing measure- ment," in Proc. 46th Annu. Allerton Conf. Commun., Control, Comput., 2008, pp. 813–817.
8. 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.
9. S. Voloshynovskiy, O. Koval, F. Beekhof, and T. Pun, "Random pro- jection based item authentication," Proc. SPIE Photon. West, Elec- tron. Imag./Media Forensics Sec. XI, San Jose, CA, USA, Feb. 2009, pp. 725413-1–725413-1

BIOGRAPHY

Balasubramanyam is a pursuing MTech in the Computer Science & Engineering Department, College of Swetha institute of Technology & Science, Tirupati, Affiliated to JNT University She received Bachlor of technology of Computer Science &Engineering degree in 2013 from JNTUA, ANANTHAPURAM, India. His research interests are Computer Networks (wireless Networks), HCI, Algorithms, web 2.0 etc.

Bullarao Domathoti is working as assistant professor in in the Computer Science & Engineering epartment, College of Swetha institute of Technology & Science, Tirupati, Affiliated to JNT University. He received Master of technology of Information Technology degree in 2012 from JNTUK. Kakinada, India, His research interests are Computer Networks (wireless Networks), HCI, Algorithms, Information security, web 2.0 etc.