International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 4 Issue 03, March-2015

Robust Digital Watermarking Scheme for Jpeg Images

Sudha S
Computer Science and Engineering,
Mahendra Institute of Technology,
Namakkal-637503

Gayathri C
Computer Science and Engineering,
Mahendra Institute of Technology,
Namakkal-637503

***Abstract*--Privacy is one of the critical issue when the data storage are outsource by the data owners to a cloud, which is one of the third party computing service. In this method, we recognize a cloud computing application scenario which needs concurrently performing safe watermark detection and privacy preserving multimedia data storage. Later propose a compressive sensing based framework with the help of secure multi party computation protocols to deal with such a condition. For secure watermark detection in a CS domain to keep the privacy, the multimedia data and secret watermark pattern are offered to the cloud. During CS transformation, MPC protocols protect the privacy of CS matrix and watermark pattern with the help of semi honest security model. From the CS domain, given object image, watermark pattern of the watermark, and the CS matrix size, we obtain the estimated watermark detection presentation. The secure watermark detection in the CS domain is possible is proved by our theoretical analysis and experimental result. This can also be widespread to other shared 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 growing cloud computing technologies are more economical to shift data storage or signal processing computations to the cloud for the data holders instead of purchasing hardware and software by themselves. Preferably, the cloud will store the data storage and perform signal processing or data-mining in an encrypted domain are done in cloud, facilitate to preserve the data confidentiality. In the meantime, owing to the rapid growth of the Internet and social networks, to collect a large amount of multimedia data from different sources is very easy for a user, exclusive of knowing the patent information of those data. For storage and to work with copyright owners for watermark detection, the user may want to take advantage of the cloud, while keeping those self-collected multimedia data secret.

The watermark patterns are needed to keep private by the watermark owners through the watermark detection as well. A cloud offering storage services, may also want to contribute in watermark detection which will be initiated by the users or the watermark detection is initiated by itself. Without the contribution of the users, to check whether the uploaded multimedia data is copyright protected or not. Storing the multimedia data which is encrypted and facilitate the watermark detection in the encrypted domain is another advantage. In the cloud, those encrypted data can be reused, later for secure watermark detection either the image data holder needs to work with other watermark owners.

Usual secure watermark detection techniques are intended to prove to a verifier whether the watermark is embedded or not. An untrusted verifier cannot removes the watermark from the watermark protected copy without knowing the watermark pattern. There are two types of methods have been projected for secure watermark detection, which are asymmetric watermarking and zero-knowledge watermark detection.

However, most of the secure watermark detection mechanism presupposes that the watermarked copy is openly available and focuses on the watermark pattern's security. While watermark detection in the confidentiality of the target media is performed has expected slight awareness. It is necessary in the watermark detection process to keep the multimedia data's confidentiality in some applications. Privacy preserving storage and secure watermark detection are performing simultaneously is possible, by using the zero-knowledge proof protocols, which is the existing secure watermark detection technologies, in which the multimedia data to a public key encryption domain are transformed. The complicated algorithms, high computational and communication complexity and large storage consumption are their limitations, which may impede their practical applications in the public key encryption domain.

A compressive sensing based privacy preserving watermark detection framework is proposed in this method, which leverages secure multiparty computation and the cloud. Many signal processing algorithms are performed in the CS domain have very close concert as performed in the original domain are proved. For privacy preserving data-mining has also been proposed by using random matrix transformation, which proposed a technique for privacy preserving collaborative data-mining, which is a random projection data perturbation approach.

These works specify that signal processing or data-mining in the CS domain is possible and is computationally secure under certain conditions. In our method, the image holder only possessed the target image/multimedia data. A certificate authority (CA) server issues a compressive sensing matrix to the image holder. Before outsources it to the cloud, the DCT coefficients of the image data to a compressive sensing domain are transformed by the image holder.

The watermark is transformed to the same compressive sensing domain for secure watermark detection using a secure multiparty computation (MPC) protocol and then sent to the cloud. The data in the compressive sensing domain are available in the cloud only. Exclusive of the compressive sensing matrix, the original multimedia data and the watermark pattern cannot reveal by the cloud. Watermark detection would be performed by the cloud in the compressive sensing domain. The cloud stores the image data in the compressive sensing domain and can be reused for watermark detection from many other watermark owners.

The privacy of the system is proved under the semi-honest assumption that all parties comply with the protocol's procedure strictly, and no one of them will actively withdraw midway or incorporate false or malicious data. To attack a third one, no two parties will collude. But they may try to keep all the intermediary information during the computing process, so that they can assume others' input after the process. For the third-party service providers who are adversaries, the semi-honest model is a reasonable assumption.

II. WATERMARK DETECTION IN THE COMPRESSIVE SENSING DOMAIN

A. Compressive Sensing

Restricted Isometry Property (RIP) is a necessary condition for the ideal reconstruction. The secure watermark detection technique is one of the detection techniques. This technique is designed to prove to a verifier whether a watermark is embedded or not. So that the watermark from the watermark protected copy cannot be removed by an untrusted verifier. Compressive sensing based privacy preserving watermark detection is future in this framework. This framework leverages secure multiparty computation and the cloud.

A secure image retrieval system are proposed through random projection and have shown that, under the Cipher text Only Attack model (COA) and the semi-honest model, the proposed random projection domain multimedia retrieval system is secure.

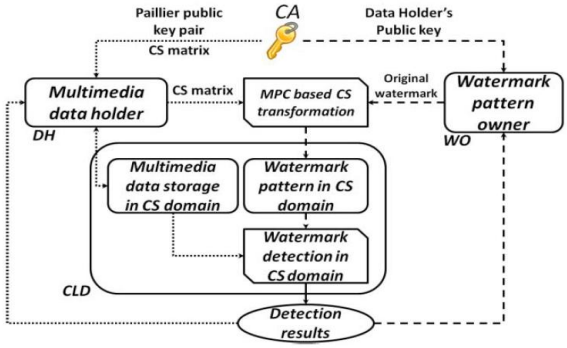

Fig. 1. Architecture of the proposed framework

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. When a large volume of multimedia data are collected from the internet for DH such as media agencies and their encrypted versions are stored in the CLD, it desires to make definite those multimedia can be reduced and republished with authorization.

Watermark owners (WOs) are also the content providers such as watermark owners(WOs), distribute their watermarked content. WOs constantly would like to know if their contents are officially used and republished. CLD, who offers storage services may also desire to initiate the watermark detection to check if the uploaded multimedia data is copyright protected. For example, to check whether the copyright protected data illegally owned or not, a CLD may choose not to provide storage services. If DH would like to use a CLD for storage or migrate the encrypted multimedia data from another cloud to this CLD, before providing the storage services that it requires the CLD to perform the detection of watermark on the encrypted multimedia data.

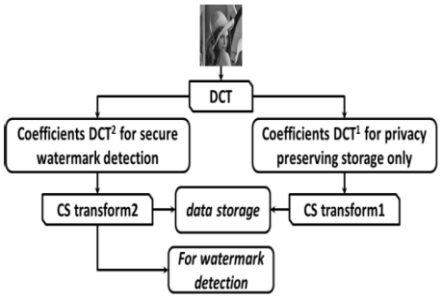

Fig.2 DCT coefficients are used for storage and watermark detection purposes

Initially, the CS matrix is issued by CA, which suites to the DH. Gaussian CS matrix is generated by using the CS matrix that suites include the seeds and the random function. Random function used to guarantee the randomness of the generated Gaussian CS matrix that is issued by CA. The CA also wants to issue a key pair, which is Paillier's public key pair to the DH and the public key of DH's to the WO. MPC based CS transformation protocol use this public key.

In common, there is different private compressive sensing matrix in DH for each image. The image's DCT coefficients are transformed by DH to the compressive sensing domain. For data storage, CLD have the CS domain. If watermark detection is required with WO, we require to let the watermark is in the same CS domain of the CLD. This is achieved under the semi-honest model through running a secure multiparty protocol by DH, WO and CLD collaboratively. If the watermark exists in the CS domain then CLD can detect and the detection results are known to both DH and WO. After the execution of Protocol 2, the secret values of the image holder are still possessed by the compressive sensing matrix, the watermark pattern and the watermark pattern owner correspondingly. In this method, DCT coefficients use each CS matrix only once to encrypt the images, which are shown to be computationally secure.

There are two issues in this 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 performance of watermark detection, in our framework, DCT coefficients that are in the zigzag order are dividing into two groups. They are DCT1 and DCT2, which includes the DCT1, potentially higher frequency AC coefficients and DCT2, the lower frequency AC coefficients.

The CS transformation of DCT2 serves for both secure watermark detection and privacy preserving storage but DCT1 serves for privacy preserving storage only. This is due to the detection of watermark performance in the CS domain, which will be penalized if the coefficients from DCT1 are integrated. DC and higher frequency AC coefficients will introduce noises for the watermark detection in the CS domain, as will be shown in our experimental results section. The DH wants to coordinate with WO about DCT2.

B. Secure CS Transformation Protocol

Our secure CS transformation protocol is one of the secure multiparty computation (MPC) protocols. The common goal is to enable parties to jointly compute a function over their inputs, by keeping these inputs private. Since the CS transformation is a scalar product between vectors. The secure scalar product protocols construct a secure CS transformation protocol.

Secure Scalar Product Protocol

Homomorphism based, commodity server based and secret sharing based techniques are the most existing secure scalar protocols. In homomorphism based techniques, only two parties involved in the computation process. But the third party has the final results, which is the best fit for our circumstances.

Goethals's protocol which is original contains two parties. They will share the final scalar product. It is uncomplicated to extends it to a three party protocol, in which the added party will have the final scalar product result is available with the added party, as 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 $\vec{x} \cdot \vec{y} = s_A + s_B$.

Secure CS Transformation Protocol

Based on Protocol 1, the secure CS transformation protocol (Protocol 2) is straightforward.

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 $\vec{k}_{m \times 1} = \Phi_{m \times n} * \vec{v}$.

C. Handling Real Values through Scaling

The Paillier's public key system takes the input as only positive integers. But our structure involves real-number values. We extent the floating point values into integer values by using certain scaling factor.

III. ANALYSIS

1) Complexity Analysis

When the image and the watermark pattern in the CS domain are presented in the CLD, watermark detection of watermark in the CS domain involve only in linear correlation. The Protocol 2 complexities of the computational and the communication are based on Protocol 1.

In our framework, the DH complexity is reduced when the owners of watermark are multiple, who are interested in performing the detection of watermark. When they are performing watermark detection on an image, the public key encrypted CS matrix can be send by the data holder to the cloud. The watermark owners can get it from the cloud to carry on the secure CS transformation protocol. Then DH only needs to receive public key encrypted values are need to received by the DH and decrypt them.

2) Security Analysis

Goethals's protocol is one of the secure scalar protocols. This is secure under the semi-honest model. MPC protocols (Protocol 1&2) are also secure under the semi-honest assumption. These parties follow the protocol strictly and no two parties will join together to attack a third party. DH and WO do not disclose their private values to other parties, after running the secure CS transformation protocol. The image data and watermark pattern in the CS domain are in the cloud.

Encryption is used as the security for compressive sensing transformation. It has been proved that when each CS matrix is used only one time, it is computationally secure under the brute force and structured attacks. So the CS domain data are secure in the cloud, if the data holder encrypts various images with dissimilar CS matrix keys.

When the detection of watermark with several watermark patterns is essential for a certain image, multiple watermark patterns in the unchanged CS domain are offered to the CLD. When many data are presented in the same random projection domain (ciphertext only) are obtained by a third party, it gains the information about the correlations between different data and no additional information other than that. The correlation between the image and watermark patterns is inevitable if there is leakage, since we need to make available such watermark detection services by the cloud. Since we use the Gaussian watermark patterns, their related CS domain versions are uncorrelated. So the CLD cannot assume about the watermarks.

3) Comparison to Previous Works and Complexity Evaluation

Our framework has the following advantages when compared to preceding works:

1) It utilizes the cloud computing and storage resource concurrently and provides better effectiveness and elasticity due to the encrypted image data (encrypted watermark pattern under some circumstances, if so chosen) can be reused in the cloud for several watermark detection.

2) It protects the privacy of the self collected data but however, most of the existing secure watermark detection paid slight attention to the security of the multimedia data.

IV. CONCLUSION

A compressive sensing based secure signal processing framework is proposed, which enables secure watermark detection and privacy preserving storage simultaneously. To protect the private of the data, this framework is secure under the semi-honest adversary model. It will fail to protect the secret values without the semi-honest assumption. For example, there cause the leakage of DH's CS matrix when the collusion between WO and CLD exists. Our framework offers better efficiency and flexibility, when compared to previous secure watermark detection protocols, and protects the privacy of the multimedia data. Secure watermark detection in the CS domain is feasible has been demonstrated hypothetically and practically. Analysis of the covariance term will be conducted in the upcoming work more theoretically. Our framework can also be extended for other secure signal processing algorithms in addition to the detection of watermark. Advance estimation of the robustness of the watermark detection in the CS domain under some other attacks also includes in the future work. Developing MPC protocols for secure CS reconstruction besides secure CS transformation is part of the future work also.

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.