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. 4, Issue 2, February 2016

A CS based Secure Watermark Detection and Privacy Preserving Storage Framework

Dipali P. Nimase, Snehal S. Londhe, Sonali U. Phatangare, Prof. Jagruti R. Mahajan

Student, Dept. of IT, G.H. Raisoni College of Engineering Ahmednagar, Maharashtr, India

Student, Dept. of IT, G.H. Raisoni College of Engineering Ahmednagar, Maharashtr, India

Student, Dept. of IT, G.H. Raisoni College of Engineering Ahmednagar, Maharashtr, India

Assistant Professor, Dept. of IT, G.H. Raisoni College of Engineering Ahmednagar, Maharashtra, India

ABSTRACT: When data owner outsource data storage then privacy is main concern of these data or when processing on third party computing service like Cloud. In these studies we define cloud application scenarios it has required perform watermarking detection and privacy preserving multimedia data storage simultaneously. We proposed as using secure multiparty computation described the compressive sensing CS based framework protocol to address such a requirement. For the secure watermark detection in CS domain to maintaining the privacy in our studies we are presented watermarking pattern and multimedia data are presented. CS matrix and the watermark pattern is protected by the MPC protocols under the semi-honest security model during the CS transformation. We specify the watermark detection performance as given target image size of CS Matrix. Watermarking detection performance can be validate by the experiments. As per our analysis and experimental result in CS domain secure watermarking detection is feasible.

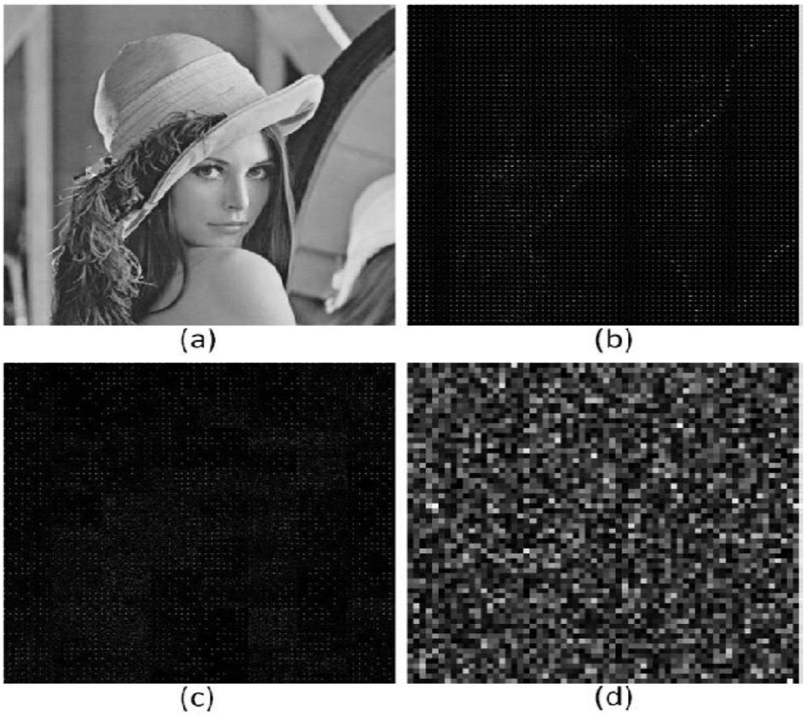
KEYWORDS: Compressive sensing, secure watermark detection, secure signal processing, secure multiparty computation, privacy preserving.

I. INTRODUCTION

Now a days Cloud computing technology using highly, and it is more economical to the data owner for the data storage transformation or signal processing computations to the cloud instead of purchasing hardware and software by themselves. Ideally, the cloud will be stored and processing the data or data mining to keep privacy of data. 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. User may use the cloud for the data storage, and at the same time, work with data owner for watermarking detection when keep the privacy of self-collected multimedia data. The data owner wants to keep their watermark patterns private during the watermark detection as well. A legal cloud provided the storage service which may desire to participate in watermarking detection initiated by user or provide watermark detection itself without the involvement of the users, to check if the uploaded multimedia data is copyright protected. The other benefit is stored encrypted multimedia data and provided facility of encrypted watermarking detection in the cloud and these 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 water mark detection techniques used for the analyse watermarking embedded correctly or not and it will be embedded without using pattern, so unconfidently content cannot remove watermark from the watermarked protected copy. There are two type of secure watermark detection: asymmetric watermarking [3], [4] and zero-knowledge watermark detection [5]–[7]. Thus the existing system can work on assumption of watermark copy publically available and focus on secure watermark detection to keep maintain privacy of watermark pattern, we focus on privacy of target copy in watermark detection but some application required the privacy for the multimedia data in the watermark detection process, as in given above scenarios. By using some existing techniques like Zero knowledge protocol that transform multimedia data to public key domain and possible to performed privacy preserving storage and secure watermark detection. Hence there is some limitations like communication complexity, complicated algorithms, highly

DOI: 10.15680/IJIRCCE.2016. 0402118

computation and high amount consumption in 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 [8]–[9]. In data mining privacy preserving using random matrix algorithms, e.g. in [11], author proposed a random projection data perturbation approach for privacy preserving collaborative data-mining. In [9], [10] author proposed through the random projection described the secure image retrieval system and the retrieval system is secure under the Cipher text Only Attack model (COA) and the semi-honest model [10]. Furthermore, show that CS transformation can achieve computationally secure encryption. The proposed system define that data mining in the compressive sensing domain is feasible and secure on the basis of certain condition. In our proposed system data owner can only controlled on image or multimedia data and the by certificate authority server has given CS matrix to the data owner. Data owner can be transfer the DCT multiplier of image to CS domain before the outsources data on 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. In the CS domain only cloud has the data. Cloud cannot retrieve the original data and watermark pattern without CS matrix. In CS domain cloud can perform the watermark detection process. CS domain stored image data in the cloud and reused for the watermark detection for others data owners



(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

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].

II. LITERATURE SURVEY

In recent days, there has been an attempt to assist the farmer by telephony service but, this service is not 24X7 Hour’s service. Sometimes, the farmers are not able to connect with experts due to communication failures. Another important problem is that in a critical situation, if the farmers are not able to explain or if the disease is a new one, then farmers would not be able to identify the diseases of the crops. Image of crop get better solution as the agree scientist can see the image and verify the exact issue for the remotely diagnosis disease. On the same way patient can send skin image or face images to expert doctor through the developed application to get health advice. Now a day's image information system become important with high powered workstation and advanced broadband network etc. On the web page large collection of images are available or videos also available on web page. Multimedia required high amount of storage memory effective index needed their and retrieve visual information from image database. In recent years, image classification has become an interesting researched in application. In this section we discussed some of the famous existing water marking techniques. Mobasseri proposed spatial domain watermarking on compressed videos. In [13] Authors can showing watermarking in raw video and also the possible way to retrieving by the decoder by exploiting the inherent processing gain of DSSS (Direct Sequence Spread Spectrum). It ensures security in user data and privacy in the watermark pattern used for embedding. The User of the system is provided with an application through which he interacts with the system. The user register and login. The data owner can maintain his image or multimedia data on the cloud. By using DCT watermark technique the data owner will be embedded data to multimedia image. While embedding the data owner will be provided key matrix by the intermediate server. This matrix will encrypt the user data before it is embedded. These server can maintain the data and the key for decryption, data owner then watermark image provide to server. Server find out watermark data in CS domain and authenticate watermark image owner. Valid owner can uploaded data on cloud.

In our studies Data Holder and the Watermark Owner are supposed to work on the Server and user side. Data holder having different multimedia and image data. As using DCT watermark owner having one particular pattern. Image, watermark pattern and key protocol create a bridge of keys for embedded process. The server keeps tracks of these keys and the embedding process. On basis on these keys data storage and watermark pattern server provide watermark detection system to find out multimedia image watermark or no. Before uploaded data on cloud server will be check owner of watermark pattern and data holder. As the keys for decryption is managed by the server it protects the user Private data and also preserves the watermark pattern.

A. Encryption/Decryption

Data encryption/decryption is done using AES (Advanced Encryption Standard) which specifies a cryptographic algorithm that can be used to protect electronic data. The AES algorithm is a symmetric block cipher that can encrypt (encipher) and decrypt (decipher) information. Encryption can convert data to the cipher text, decrypted data convert in to the cipher text its called plain text.

B. Compression/Decompression

The algorithm is designed to be fast to implement but is not usually optimal because it performs only limited analysis of the data.

C. Data Hiding

For the data transformation usually DCT, FFT and wavelet methods has used. The feature of the transform domain technique they can take important properties of other domain for the overcome limitation of pixel-based methods or to Support additional features. For instance, designing a watermarking scheme in the DCT domain leads to better implementation compatibility with popular video coding algorithms such as MPEG. Generally, the main drawback of transform domain methods is their higher computational requirement.

III. Proposed System

For In our proposed system we focus on to provide software that usually works by watermarking a text message or by sending an image behind a video which makes unable for a human eye or ear to detect. On review, of a digitized video before and after a message was inserted, will show video files that appeared to have no substantial differences. The software is designed for copyright protection by storing information in the DCT domain of a digitized video file.

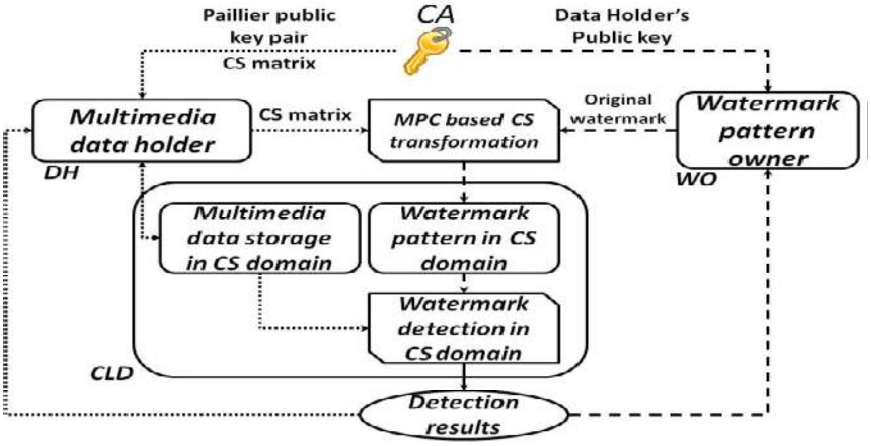


Figure 2. Architecture of the proposed framework

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 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), it was collect large amount of data from the beg pages and stored on cloud in encrypted form, it wants to make sure those multimedia can be edited and republished legally. The watermark embedded done by watermark owner before the publish content and watermark owner also content provider who can distribute their watermark content. WOs always want to know if their contents are legally used and republished. In our framework, initially, the certificate authority importance of issue compressive sensing matrix to valid data holder. 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 Parlier public key pair to the DH and the DH's public key to the WO.

IV. Conclusion and Future Work

The Watermarking transmits secrets through apparently innocuous covers in an effort to conceal the existence of a secret. Video Watermarking and its derivatives are growing in use and application. In areas where cryptography and strong encryption are being outlawed, citizens are looking at Watermarking circumvent such policies and pass messages covertly. Commercial application of |are in the form of digital watermarks and Digital fingerprinting are currently being used to track the copyright and ownership of electronic media. In view of the great number of different embodiments to which the principles of our invention can be put, it should be recognized that the detailed embodiments are illustrative only and should not be taken as limiting the scope of our invention. Rather, we claim as our invention all such embodiments as may come within the scope and spirit of the following claims, and equivalents thereto.

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.