Volume 5, Issue 1, January 2015 ISSN: 2277 128X
International Journal of Advanced Research in Computer Science and Software Engineering
Research Paper
Available online at: www.ijarcsse.com

Robust Image and Video Data Hiding Using Secure Watermark Detection

Pinal Chhajed, Sejal Bhatewara, Nikita Andhrutkar, Komal Ghuge
Department of Computer Engineering, Pune University,
Pune, Maharashtra, India

Abstract— We propose a framework where 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 in the form of key. The image holder transforms the images into DCT Coefficient matrix embeds the watermark image and then sends it to the server for watermark detection. The server detect the watermark and authenticates the owner of the multimedia data. On successful authentication the server uploads the watermarked image to the cloud. Our system is secure under the semi-honest 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.

Keywords— Data Holder, DCT Algorithm, Watermarking, Compressive Sensing, Cloud

I. INTRODUCTION

Cloud computing has promoted the hosting and delivery of services over the Internet and the movement of computation and data from terminal devices and local servers to core data centre due to advantages in flexibility, scalability, and economics of savings. Most services have been supported by massive-scale distant data centres located at sites. However, some services will require low latency (e.g. alarms in smart grids, safety applications in transportation, monitoring in remote health, fire or emergency alarms in smart cities), the processing of large volumes of local information (e.g. video capturing in lecture rooms), or high security provided by intelligent converged network and computing at the edge of the network, for example in the premises of traditional telecom service providers. While the benefits of cloud computing is clear, security is a severe concern in these infrastructures. Kandukari et al. considers five cloud security issues that should be included in a Service Level Agreement. There are the following: privileged user access, data location, data segregation, data disposal and investigation and protective monitoring. Privileged user access ensures only authorized users have access to an organization data and resources. Protection of digital works against misuse and illegal distribution has become a challenging task in the information society and there has been intensive research in this area in the last years. As the total prevention of misuse does not seem to be achievable at reasonable cost, most technical copyright protection schemes aim to deter illegal usage or redistribution of digital content by making misuse detectable. 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. Two types of approaches have been proposed for secure watermark detection: asymmetric watermarking and zero-knowledge watermark detection. 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 that transform the multimedia data to a public key encryption domain. However, their limitations, such as complicated algorithms, high computational and communication complexity, and large storage consumption in the public key encryption domain, may impede their practical applications.

II. SYSTEM ARCHITECTURE

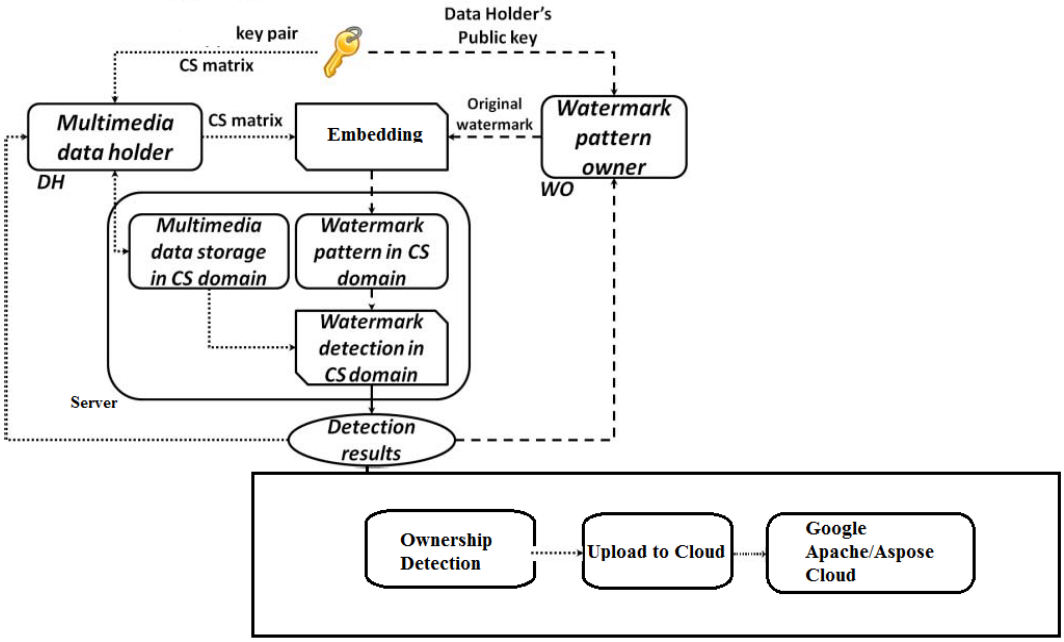

Fig 1.1 System Architecture

The Proposed architecture ensures security in user data and privacy in the watermark pattern used for embedding. The User of the system is provided with a application through which he interacts with the system. The user register and login. The users maintain his/her multimedia data on the cloud storage. The user embeds data in to the multimedia image using DCT watermark technique. While embedding the user is provided with a key or a matrix by the intermediate server. This matrix will encrypt the user data before it is embedded. The server maintains a session and tracks the keys for further decryption. The User then embeds the data and the new watermarked image is further given to the server. The server finds out for any watermark data. If the server finds the watermark data then the server authenticates the watermark owner. On successful ownership the server allows the image to be uploaded to the cloud server.

In the architecture the DH and the WO are supposed to work on the server and user side. The DH may have different types of multimedia images. The WO is limited to only one type of watermark pattern using DCT. For both the image and the pattern and key management protocol is executed which creates a pool of keys for every embedding process. The server keeps tracks of these keys and the embedding process. Based on these key i.e. data storage and watermark pattern the server applies watermark detection to determine the multimedia images has watermark data or not. On having the server checks the owner of the pattern and the data holder and authenticates before the watermark image is uploaded to the server. As the keys for decryption is managed by the server it protects the user private data and also preserves the watermark pattern.

III. SYSTEM MODULES

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 Module:

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. *CS*

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. 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 matrixLarger amplitudes closer.

IV. PROPOSED FRAMEWAORK

The DCT is a very popular transform function used in signal processing. It transforms a signal from spatial domain to frequency domain. Due to good performance, it has been used in JPEG standard for image compression. DCT has been applied in many fields such as data compression, pattern recognition, and image processing, and so on. The DCT transform and its inverse manner can be expressed as follows:

$$F(u,v) = \frac{4C(u)C(v)}{n^2} \sum_{j=0}^{n-1}\sum_{k=0}^{n-1} f(j,k)\ \cos\left[\frac{(2j+1)u\pi}{2n}\right] \cos\left[\frac{(2k+1)v\pi}{2n}\right] \quad (1)$$

$$f(j,k) = \sum_{u=0}^{n-1}\sum_{v=0}^{n-1} C(u)C(v)F(u,v)\ \cos\left[\frac{(2j+1)u\pi}{2n}\right]\cos\left[\frac{(2k+1)v\pi}{2n}\right] \quad (2)$$

Where

C(w) = $1/\sqrt{2}$ when w=0

C(w) = 1 when w=1,2,3,….n-1

As an image transformed by the DCT, it is usually divided into non-overlapped *m ´ m* block. In general, a block always consists of 8´8 components. The block coefficients are shown in figure 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

(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)

The left-top coefficient is the DC value while the others stand for AC components. The zigzag scanning permutation is implied the energy distribution from high to low as well as from low frequency to high frequency with the same manner. The human eyes are more sensitive to noise in lower-frequency band than higher frequency. The energy of natural image is concentrated in the lower frequency range. The watermark hidden in the higher frequency band might be discarded after a lossy compression. Therefore, the watermark is always embedded in the lower-band range of the host image that transformed by DCT is perfect selection.The lower-band coefficients of DCT block are described as in Figure b.

A. DCT Algorithm

1. Take DCT of Image.
2. Take DCT of Hidden message.
3. Set T, the significant threshold value, below which transform coefficients will be deemed insignificant.
4. Find these T values and replace these by a function of the hidden message.
5. Take the inverse DCT of this new image.
6. Output= Stego Image

The scope of the paper which is based on securing watermarked images using DCT watermark, computing predicate over encrypted data .

1. Ability to authenticate without disclosing unencrypted data. This is achieved by using predicate over encrypted data.
2. Ability to use identity data on untrusted hosts. This is achieved through the use of the active bundle scheme. An active bundle has a self-integrity check mechanism, which triggers apoptosis (a complete self-destruction) or evaporation (a partial self-destruction) when the check fails.
3. User Registration and login.
4. Watermark using DCT
5. Watermark Detection using DCT
6. Upload and download functionality with Cloud
7. Design Protocol based authentication scheme for multimedia image ownership.

V. CONCLUSIONS

A compressive sensing based secure signal processing framework that enables simultaneous secure watermark detection and privacy preserving storage. Framework is secure under the semi-honest adversary model to protect the private data.In addition to watermark detection, 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.

ACKNOWLEDGEMENT

We could never have completed our project without the support and assistance of many people. First and foremost, we would like to express deepest gratitude to our project guide Prof M.T.Jagtap for his excellent guidance, valuable suggestions and kind of encouragement in academics. We are also thankful to Our Co-guide Prof.N.R.Shinde.We are grateful for his help. We are thankful to our HOD Prof. M. T. Jagtap and Principle Prof. Dr. N. S. Walimbe for providing us this infrastructure and labs. Last but not the least we owe a debt to our parents who are the silent guides in our life. We are also thankful to all our friends for their encouragement and support.

REFERENCES

[1] T. Ristenpart, E. Tromer, H. Shacham, S. Savage, "Hey, You, Get Off My Cloud: Exploring Information Leakage in Third- Party Compute Clouds," *Proc. 6th ACM conference on Computer and Communications Security*, Chicago, IL, Nov. 2009, pp. 199-212.

[2] Rohit Bhadauria, Rituparna Chaki, Nabendu Chaki, Sugata Sanyal, "A Survey on Security Issues in Cloud Computing",2011.,pp.1-15

[3] R. Gellman, "Privacy in the Clouds: Risks to Privacy and Confidentiality from Cloud Computing, "World Privacy Forum, Feb. 2009.

[4] A Compressive Sensing based Secure Watermark Detection and Privacy Preserving Storage Framework IEEE TRANSACTIONS ON IMAGE PROCESSING, VOL. 23, NO. 3, MARCH 2014

[5] Secure Watermarking for Multimedia Content Protection: A Review of its Benefits and Open Issues Published in: Signal Processing Magazine, IEEE (Volume:30 , Issue: 2) Date of Publication: March 2013

[6] Zero-Knowledge Watermark Detection and Proof of Ownership Andre Adelsbach and Ahmad-Reza Sadeghi

