Security of Multimedia Data Transmission stored on Cloud - Watermark Technique

Ujwala Pawar
Department Of Information Technology
RMD. Sinhagad School of Engineering
Pune,India
E-mail: upawar28@gmail.com

Prof. Dhara T. Kurian
Department Of Information Technology
RMD. Sinhagad School of Engineering
Pune,India
E-mail:dtkurian@sinhgad.edu

Abstract— **When we collect large amount of data and stores it on cloud then privacy of the data is the main issue. To protect privacy of the data certain cryptographic techniques are used. Watermark detection is one of the key aspects for the privacy of the data. Digital music downloads and multimedia data storage create new challenge to the aim of information protection events aimed at preventing copyright violation. Digital watermarking has been proposed as a possible brick of such protection systems. This paper mainly deals with cloud computing applications that perform secure watermark detection and privacy of the data. Multiparty computation protocol is used with semi honest assumption. In the watermark detection procedure Signal processing technique is used for efficiently acquiring and reconstruction of the signals.**

Index Terms-- Signal processing, Compressive sensing, Multiparty Computation.

I. INTRODUCTION

Now a day the cloud computing technologies are growing faster and it is more difficult for the data owner to shift the data from one cloud to another. Security for the large collected data is also a major issue. Privacy for the storage of the multimedia data such as audio video becomes a major concern. So, for the privacy of the data some encryption decryption techniques are there. watermark detection is one of the more important cryptographic method for the privacy of the normal data as well as multimedia data. The user can store the data on the cloud and side by side, work with copyright owners for watermark detection while the self-collected multimedia data keep as a private [1]. As the cloud technology growing faster many time the cloud allows the storage for the legally edited and republished data only. Digital watermark technique provides a communication channel multiplexed into the original content with which it is possible to pass on some application related information. For example in forensic lab a watermark can be used to combine a unique code such as fingerprint into every replica of the content to be distributed. When unauthorized published contents are found, the fingerprint allows tracing the user who has redistributed the content or information. when the watermark is fixed at the sharing server, a client whose watermark has been found on illegal copies can claim that he/she has been framed by a malicious vendor who inserted his/her individuality as watermark in an random object. The simple existence of this problem may question the reliability of the forensic tracing planning. A feasible solution to this problem is to build fingerprinting asymmetric schemes, where only the customer has access to the fingerprinted content(data); however, if the merchant afterward finds a copy of the data, he/she can still recognize the customer and prove to third parties that this customer bought this copy[2]. Another difficulty is the system scalability: in conventional distribution models, the watermark attaching process is carried out by a trusted server before releasing the content to the client. However, in large-scale systems, servers may become congested, since the computational load due to watermark embedding increase linearly with the number of users. Further, since the allocation of individually watermarked copies requires point-to-point communication channels, bandwidth requests can become unaffordable. Another problem is the existence of untrusted verifiers. In the watermark detection process, a data owner can be asked to confirm to another party that a watermark is present in his/her copy[2]. This process usually requires exposing secret information related to watermark embedding, such that a corrupt party could then use the knowledge of the secrets to remove the watermark from the content. These problems can be solved with the secure signal processing technique. In most of the watermarking methods the surrounded signal must be known for watermark detection, which leads to cruel security risks. Many times there is security problem when watermark is embedded to the multimedia data, to cope with this problem asymmetric scheme is proposed. In these a scheme the detector(receiver) only needs to know a public key, which does not give sufficient information to destroy the embedded watermark. Traditionally there were mainly two approaches for watermark detection Asymmetric watermarking schemes and zero knowledge watermarking technique[5].

The objective of zero-knowledge watermark detection is to permit a prover to firmly convince a verifier of the existence of a watermark in definite data without illuminating any information which the verifier can use to remove the watermark[7]. In the compressive sensing framework, the target image/multimedia data is hold by the image holder (data owner) only. A CS matrix is provided by a certificate authority (CA) server. The data

holder /data owner transforms the District Cosine Transform (DCT) coefficients of the target image data to a CS domain before transfer it to cloud. To make secure watermark detection the watermark is changed to the equal compressive sensing domain through a secure multiparty computation (MPC) protocol and the data is sent it to the cloud. Without the CS matrix, the cloud cannot disclose the original data as well as the watermark pattern. Then the cloud will execute watermark detection in the compressive sensing domain. Multimedia data in the compressive sensing domain might be stored in the cloud as well as reused further for recognition of watermark from many other watermark owners [1].

II. LITERATURE SURVEY

A. Watermark Model

A watermark model for a digital watermarking system is given in Figure 1. The inputs of the system are a vector a=[a1,a2,…] representing either the unique host signal samples or, a set of features of the host signal computed by a suitable transform such as discrete Fourier transform (DFT) and the discrete cosine transform (DCT)), and some application dependent information, here represented as a binary vector b=[b1,b2…], with the values in between {0,1}. The encoder insert the watermark code b into the host signal to produce a watermarked signal a**x**, by making the use of a secret key {sk} to control the embedding process and allow the watermark recovery only to authorized users. Sometime decoders may also use the original content **a** to recover the concealed information, in which case they are referred to as non-blind detector/decoder. Many combination of keyword or it may be some phrase or well-formed natural language. Once a user query is input to the search engine the list of documents is presented to the user with a document title. Then it generate a histogram on the basis of threshold values. Query classification before retrieval is applied in . Before gathering the documents information query classification is performed. It is nothing but the pre-retrieval of the query. Author proposes three different mechanisms to classify the obtained results[2] .

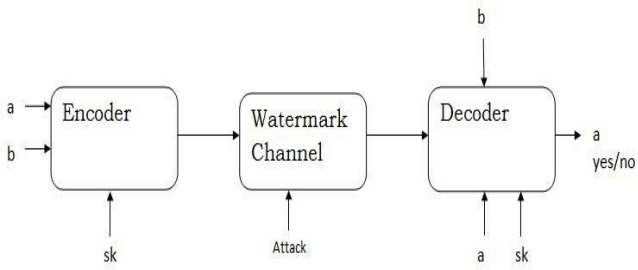


Fig1. A Watermark System

B. Server-Side Watermark Embedding

Homomorphism technique is used for secure server side watermark method. Consider that the server can have the pair of public/private key of a homomorphism cryptography technique. So with the help of watermarking model client and server can perform the encryption of the watermark signal and the watermark embedding can be performed at the server side. In this case the server knows the plaintext value and can perform the encryption with the help of client public key. The alternative approach for the this is use integer value for the encryption which can be obtained by integer transformation[2].

C. Client-side Watermark Embedding

Client-side watermark embedding technique broadcast the same encrypted description of the original data to all the clients in the structure, but a particular client-specific decryption key allows decrypting the data or the contents and at the same time completely embedding a watermark. When the client uses his/her key (secrete key) to decrypt the content, he/she obtains a exclusively watermarked version of the content. Client side approach uses a stream-cipher method that allows the use of numerous decryption keys, which decrypt the identical cipher text to slightly different plain texts[2].

D. Commitment Schemes

There are mainly two types of protocols for the commitment scheme that are protocol com and protocol open for the M message space and C commitment space[7].

E. Ownership proof Model and Scheme

The main three parties involved in the proof of ownership are data holder, registration centre and the third party. Here it is assume that the registration centre is trusted by the all the parties[7].

III. PROPOSED SYSTEM

Conventional secure watermark recognition techniques are designed to prove to a verifier whether a watermark is attached without revealing the watermark pattern to the an untrusted verifier or outsider cannot take out the watermark from the watermark confined copy. In this paper, we suggest a compressive sensing based privacy protected watermark recognition structure that allows secure multiparty computation on the cloud. Numerous signal processing algorithms execute in the CS domain has similar performance as in the original domain .Using the technique for random matrix transformation for the privacy preserving data-mining is achieved, which estimated a random projection data perturbation perspective for privacy of the collaborative data-mining. It has confirmed that the proposed random projection based multimedia retrieval system is protected under the model named Cipher text Only Attack model (COA) and the other is semi-honest model. However the CS transformation can be reached computationally secure

encryption. And this technique specifies the signal processing or the data-mining which is in the CS domain is possible and is computationally secure under definite conditions. In this framework, the objective image/multimedia data is hold by the image owner r/data holder only. A compressive sensing matrix is executed by a certification authority (CA).The image owner transforms the DCT coefficients regarding image data for the compressive sensing domain while transmitting the data to the cloud. To make secure watermark detection, it is also transformed to the same compressive sensing area used as a secure multiparty computation (MPC) protocol and then also sent to the cloud. Then the data on cloud is stored in the compressive sensing domain. With the help of compressive sensing matrix only, the cloud can disclose the genuine multimedia data and the watermark pattern. Then the cloud performs watermark recognition in the compressive sensing domain. Data image in the compressive sensing domain might be stored on the cloud and further reused for uncovering of watermark from many other watermark owners.

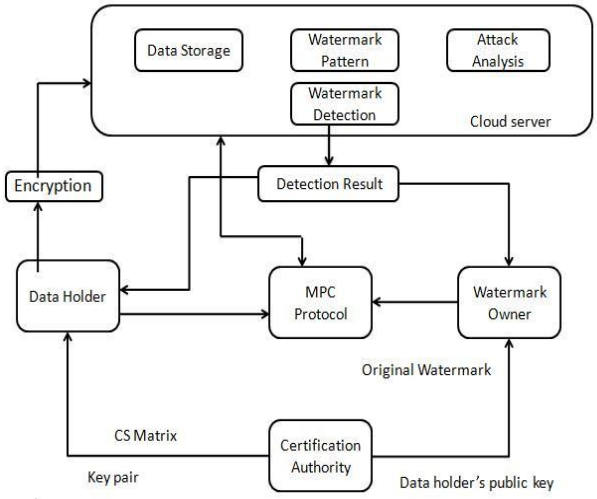


Fig 2. System Architecture

Data Holder/Image Owner :

Data Holder collects a large amount of multimedia data from the different resources like internet and stores their encrypted version in the cloud, it wants to make sure that the multimedia data can be edited and republished legally.

Watermark Owner :

Watermark owner also called as content provider, that is WO provide watermark to the data(with the help of public key). WOs at all times want to identify if their context are legally used and again published.

Compressive Sensing :

The compressive sensing is a signal processing technique for efficiently acquiring and reconstruction of the signal. Most of the compressive sensing techniques has focused on improving the rate and correctness of compressive sensing reconstruction. It takes some preliminary steps towards a more common framework called compressive signal processing (CSP), it shows primary signal processing problems such as recognition, arrangement, estimate, and filtering might be solved in the compressive sensing domain.

Correlation in Watermarking:

This part is a association module that is Watermark {an undetectable signature fixed inside an image to show validity or proof of ownership. It minimizes the unauthorized replication and distribution of images over the internet. It can be used for searching a specific watermark

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

- Splits image into different parts based on the illustration excellence of the image
- Input image/Input Data
- strength of pixel in the row i and the column j respectively
- DCT coefficient in DCT matrix [1].

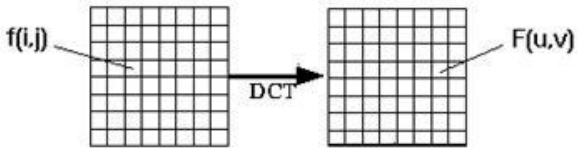


Fig : District Cosine Transform

.

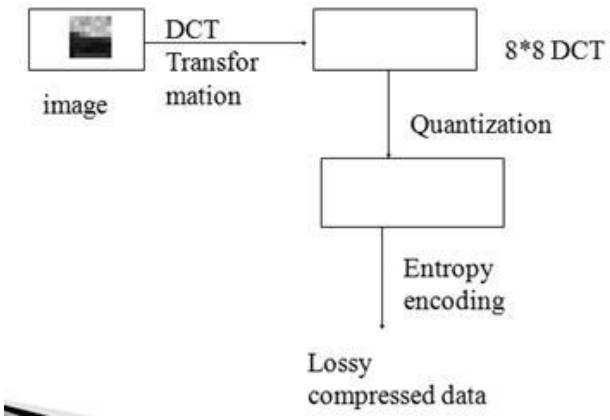


Fig 3. DCT Coding System

IV. CRYPTOGRAPHIC PREFACE

Secure Multi-Party and Two-Party Computation are the two main concepts for the cryptographic technique. For the assurance of the protocol to be secure under many applications as possible, it is necessary to use the secure multi-party and two-party techniques. A two-party protocol between party A and Party B is secure when privacy and accuracy are definite for both party A and party B.

A protocol protects privacy, when the information that is leaked by the distributed computation is partial to the information that can be learned from the elected output of the computation.

Here the semi honest model can be consider for the security of the protocol. semi-honest model, assumed that both party A and party B follow the protocol or the guidelines, but they are also have to store all exchanged data and try to assume information from it. In the malicious model, no guess is made about the behavior of the two different parties that is party A and party B, and it is necessary that the privacy of one party is preserved even if an arbitrary behavior of the second party.

V. SECURITY OF THE PRIVACY PRESERVING OF DATA

To provide better security and privacy protection ahead of traditional access control techniques, privacy preserving multimedia recovery techniques have been proposed for the content-based multimedia recovery directly over encrypted databases and accomplish accurate recovery equivalent to conventional retrieval schemes.

The security analysis presented here is in the ciphertext Only Attack model (COA), these model assume that the adversary has access only to the ciphertext, i.e. the encrypted images and indexes. Furthermore, it assume that the adversary is semi-honest, i.e., the adversary will follow the execution condition of the protocol but may utilize what they notice throughout the execution to compute more than what they need to identify. Semi-honest model is a logical assumption for adversaries such as third-party service providers. For protected online multimedia organization, the encrypted images and their encrypted features or indexes are stored on the remote(main) server and thus accessible by system administrators and the other members. In the COA model, a secure recovery scheme should be able to protect the following items from the adversary **:**

(1) plaintext data of the encrypted database images and the query image;
(2) the secret key S*k* used in the encryption; and
(3) any function of the images which can be plaintext features of the images.

The security of privacy-preserving recovery schemes under the COA model has been experimentally carried out. The research is carried out over a subset of Corel database which contains 1000 images equally divided into 10 subparts. Query indexes encrypted using both right and incorrect keys are used to search the database. The accuracy value around 0.1 for the incorrect key recovery verifies that query indexes encryption done using a incorrect key are evenly probable to be closest to any encrypted index in the database and such retrieval is equivalent to alternative images arbitrarily from the database. It should be renowned that none of the schemes can be protected under the more rigorous Chosen-Plaintext Attack model, because then the adversary can prefer any plaintext image as query to study the content of the whole image database[3].

VI. RECONSTRUCTION OF THE IMAGE AT RECEIVER SIDE

In the case of privacy preserving storage, as the District Cosine Transform (DCT) coefficients are not completely sparse, the CS modernization will introduce distortion to the reconstructed image, especially when Compressive Sensing rate is low .Here the CS reconstruction experimental results when all AC components are changed to a compressive sensing domain. For thre good quality image after the CS reconstruction, the compressive sensing rate wants to be high.

The experiments demonstrate that the PSNR (Peak Signal-to-Noise Ratio) is around 35 after the CS transformation/reconstruction process when the CS rate is 0.8. Even when the CS rate is set to 1.0, the CS reconstruction algorithm still introduces distortion as 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. Restricted Isometric Property is proposed for the reconstruction of the Image.RIP property 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[1].

VII. EXPERIMENTAL RESULT (EXPECTED RESULT)

The 512 X 512 image is used for the testing purpose. There are different methods are available for watermark detection eg.Canny edge detection. Here we can use the method of normal distribution in which watermark pattern itself can be used for the watermark detection. The target image is cut into different pieces and each piece contains 8 X 8 DCT blocks.DCT coefficients for each piece form vector and transform into CS domain with same CS rate with different CS matrix [1].

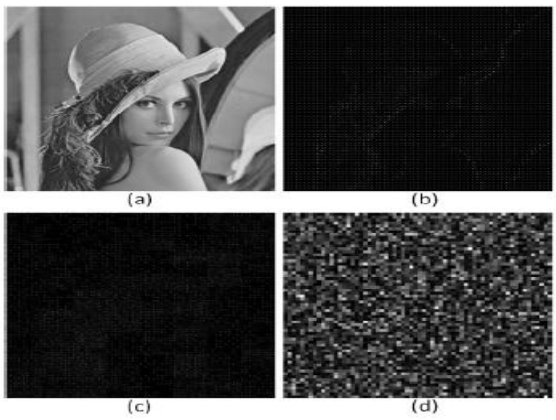
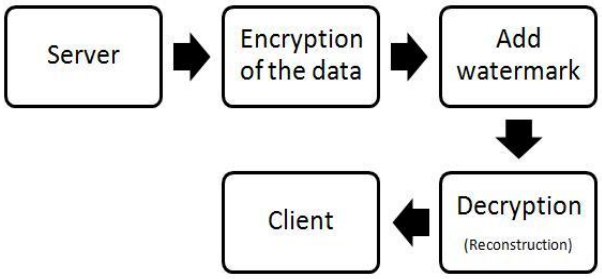


Fig 4 .(a)Original image (b)Image in 8X8 DCT domain (C) DCT coefficient after CS transformation (d) Reconstructed image

Overall functioning:



CONCLUSION

A compressive sensing based secure signal processing framework that performs concurrent protected watermark recognition and privacy preserving storage. Digital watermarking used for the multimedia content protection but in case of realistic scenario some issue can be occur to solve these issue secure watermarking system can be established. Here also conclude that a private scalar product protocol based on standard cryptographic techniques is secure. The security classification is proposed for the ciphertext only attack model .This paper also includes the embedding of the watermark the content at server side as well as client side.

ACKNOWLEDGMENT

I would like to take this opportunity to express our profound gratitude and deep regard to my guide Prof. Dhara T. Kurian for her exemplary guidance, valuable feedback and constant encouragement throughout the duration of the project. Her valuable suggestions were of immense help throughout my project work. Her perceptive criticism kept me working to make this project in a much better way. Working under her was an extremely knowledgeable experience for me.

REFERENCES

[1] Qia Wang, Wenjun Zeng, Fellow, IEEE, and Jun Tian, Member, IEEE,A Compressive Sensing based Secure Watermark Detection and Privacy Preserving Storage Framework, IEEE Transactions on Image Processing, VOL. 23, NO. 3, MARCH 2014

[2] 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.

[3] 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.

[4] 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.

[5] 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.

[6] 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.

[7] A. Adelsbach and A. Sadeghi, Zero-knowledge watermark detection and proof of ownership,
in Proc. 4th Int. Workshop Inf. Hiding, vol. 2137. 2001, pp. 273288.