A Signal Processing Technique for Watermark Recognition Using MPC Protocol

Ujwala Pawar, Dhara T. Kurian
ME (IT) -RMD Sinhgad Pune,
Assistant Professor-RMD Sinhgad, Pune,
upawar28@gmail.com – 9075714221

Abstract— Privacy preserving of the data is major concern when a user or data owner outsources the data to another party on cloud. Here the main task is to find the cloud computing structure so as to make it secure for the watermark detection. To deal with such requirements in compressive sensing (CS) based layout secure multiparty computation (MPC) protocol is used. While in CS conversion the secrecy is maintained by MPC of CS matrix. Data holder, Watermark owner and the cloud for storage are major part. Homomorphism based pallier public key and secrete sharing based techniques can be used for the conversion of the data. The secrecy is maintained by the semi-honest model as all the MPC follows unique protocol. The framework provides protection for multimedia data which is stored on cloud and condensed and republished legally. RIP (Restricted Isometric Property) plays a significant role for renovation of the image. In CS, it includes the aimed image, watermark reorganization and size of CS matrix. Some methods such as Normal Distribution with District Cosine Transformation (DCT) can be used for detection of watermark. The accuracy of the extracted functionality is approved through experiments. The hypothetical analysis and the results of experiments give realistic solution by means of watermark reorganization. The outline can also be extensive to other mutual protected signal processing and data-mining applications in the cloud.

Keywords— Compressive sensing, secure watermark detection, Discrete Cosine Transform, Multipart Computation Protocol, AES algorithm

INTRODUCTION

Cloud computing is growing technology for storing the large amount of data on the cloud and also provide security for that data. When the one party wants to outsource the data to another party on the cloud then maintaining privacy of that particular data is the main issue. For achieving privacy of the data there are many algorithms are available such as anonymous ID assignment, Zero knowledge proof .In this paper we are providing the privacy for the image by using watermark technique. The image that is to be transferred is attached with watermark then with the help of Discrete Cosine Transform technique with forward DCT algorithm the image is divided and with reverse DCT the image is reconstructed. The correctness of the image is depending upon the CS matrix rate.

With the help of Multiparty Computation multiple parties at the sender side and the multiple parties at the receiver side can send the data and receive the data at the same time. The framework can be secure under different types of attack such as Bruit force attack, Password crack attack etc. In this framework the target image is contained by data holder/image holder or cloud user directly. If the image is possessed by the cloud user then image is directly encrypted and save it on cloud and if the image is possessed by the image holder then the image can be added with the desired watermark and then it is uploaded on the cloud.

The existing cryptographic techniques are based on the asymmetric as well as symmetric type in which same or different public and private keys are used at the sender side and the receiver side for the privacy preserving purpose. Here in this paper watermark technique is used for the ownership purpose.

RIP (Restricted Isometric Property is used at the time of image reconstruction).With the help of RIP the correctness of the image can be increases. There are many techniques for the secure scalar protocols such as Commodity server based, Secret sharing based, Homomorphism based. 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 scenario. In this paper we used the protocol based on Paillier public key system and its homomorphism properties.

Homomorphic Encryption:

Homomorphic encryption is a form of encryption which allows specific types of computations to be carried out on cipher text and generate an encrypted result which, when decrypted, matches the result of operations performed on the plain text.

Paillier cryptosystem:

The Paillier cryptosystem is a probabilistic asymmetric algorithm for public key cryptography. The scheme is an additive homomorphic cryptosystem; this means that, given only the public-key and the encryption of m1 and m2, one can compute the encryption of m1+m2.

EXISTING SYSTEM

Existing system is based on the security of the multimedia data on the cloud. The watermark method is used for the security purpose. In the following system the target image is enclosed with the image holder only. A CS matrix key is issued by the certificate authority to the image holder. The image holder transforms the DCT coefficient of the image data to the CS domain. The system is secure under the semi honest assumption that is two can be compute their function together without disturbing the third party.

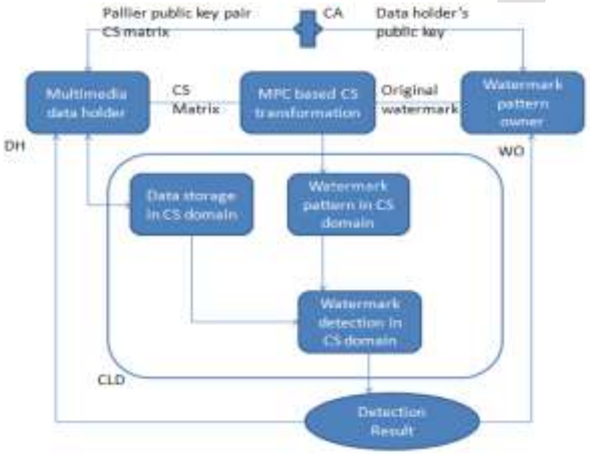


FIG.EXIST ING SYSTEM

PROPOSED SYSTEM

The proposed system involves the privacy of the image data on the cloud when the image data is transformed from one party to another party. The system involves data/image holder, watermark owner and the cloud.

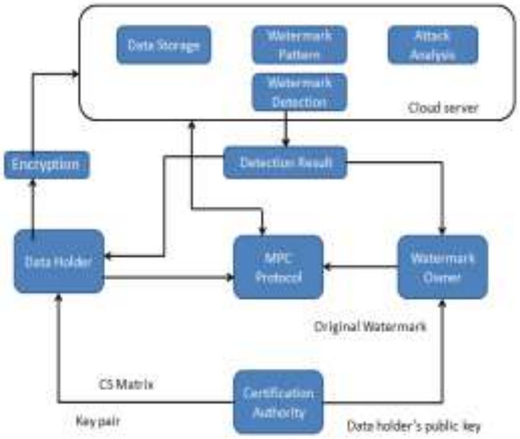


FIG.PROPOSED SYSTEM

Data Holder: Data holder/image holder can possess the image which is to be transformed. The image can be in any format such as png, jpg, jpeg etc.

Watermark Owner: Watermark owner is responsible for providing the watermark for the image which is stored on cloud. The watermark in this scenario is responsible as encryption key. Watermark is added to maintain the ownership of the particular data.

Cloud: Cloud is used for storing the images and other data such as audio. The major use of the cloud storage is that the data can be used publically of only private user can used the authenticate data. In this framework cloud user can also store the image which is stored on cloud in the encrypted form and transform. In this framework certification authority is responsible for the providing the public key to the data holder as well as watermark owner.

This framework is secure under semi honest assumption, Due to multiparty computation two and more parties can compute their data without disturbing their inputs. Because of the large length watermark (key value) the attack minimization can be done. In this paper multiparty computation can be done at the sender side as well as receiver side. When the data owner collects amount of data from different resources then the data must be unique or it can be edited data Many time not only data owner and watermark owner concern about duplication of the data, cloud also provide the storage services for the original data only. Many times cloud not offers the storage services to the copyright data.

DISCRETE COSINE TRANSFORM

The discrete cosine transform helps to divide the image into different parts with respect to visual quality of image. The DCT is similar to the Discrete Fourier Transform. It transforms different images and the signals from the spatial domain to frequency domain.

The basic steps involved in DCT are as follows:

- The input image is A by B;
- f(i, j)represents pixels in row and columns.
- F(u,v) is the DCT coefficient for row k1 and column k2 of the DCT matrix.
- For several images, a large amount of the signal energy kept at low frequencies; these come into view in the upper left corner of the DCT.
- Input for the DCT is an 8 by 8 array of integers. This array contains every pixel's gray scale level;
- 8 bit pixels have levels from 0 to 255.

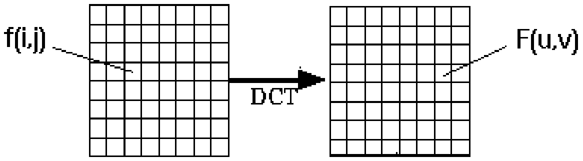


FIG. DCT TRAN SFORMATION

Encryption is the process of converting individual form of data into another form called as plaintext to cipher text conversion that is cannot be understood by anyone except authorized parties.

The main purpose of encryption is to protect the confidentiality of the digital data stored on the computer system or to protect the confidentiality of the data that is transmitted over the network. There are some key elements of the security:

a. Authentication: The origin of the message can be verified.
b. Integrity: The message that is send from the sender should be as it is received by receiver. The originality of the message should not be change.
c. Non-repudiation: The sender of a message cannot reject sending the message.

PROPOSED ALGORITHM

Steps involved:

- Attach watermark to the desired image
- Divide the image into 9*9 parts that is shuffled the image.
- Apply signal processing.
- Encrypt the image with the help of encryption technique.
- Stored the image on the cloud.
- At the side of reconstruction first decrypt the image,
- Reshuffled the image with the help of particular cryptographic key.
- Reconstructed image as a output.

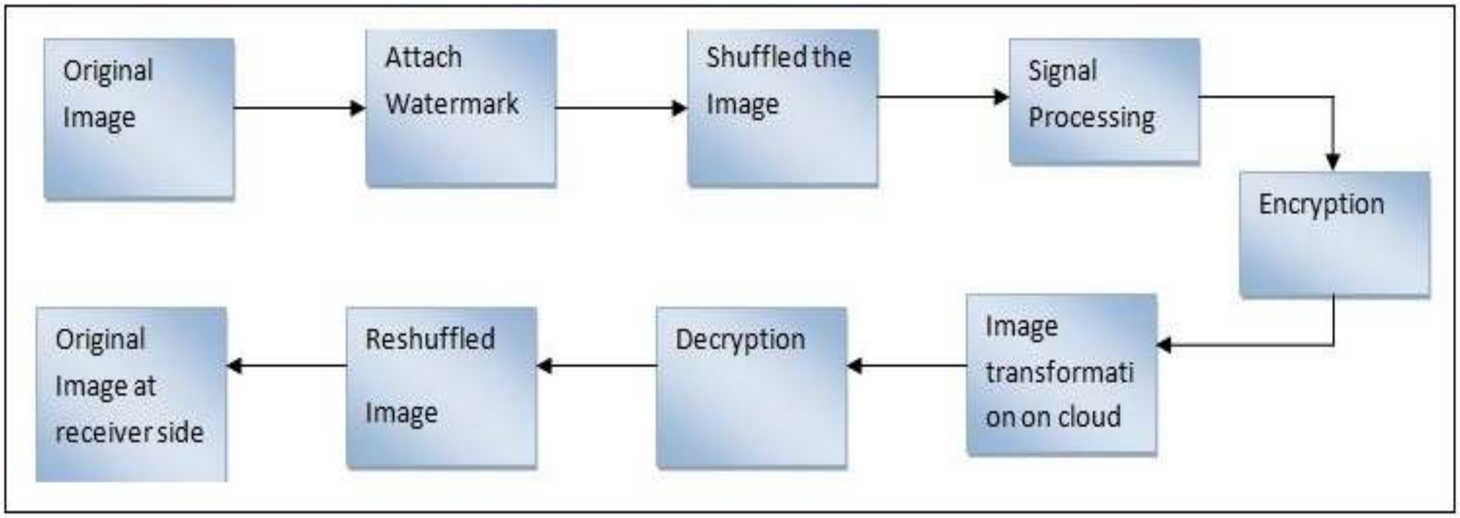


FIG. FLOW OF PROPOSED SYSTEM

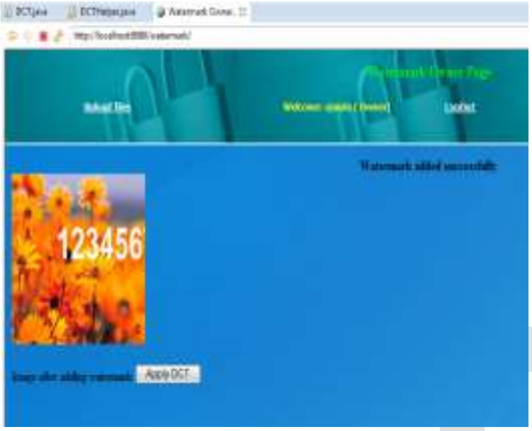
AES Algorithm:

Advance encryption standard can be used for encrypt and decrypt text, images. We can take 128,192 or 256 bit long key size for encryption and decryption.AES algorithm compare three block ciphers,AES-128,AES-192 and AES-256,Each cipher encrypt and decrypt data in blocks of 128 bit using above cryptographic keys. Symmetric or secrete key ciphers uses the same key for encryption and decryption, so both sender and receiver uses the same secret key. All key length are sufficient to protect classified information up to secrete level.

RESULT ANALYSIS

The system is tested with the standard image of size 512*512.For the watermark detection there are several methods are available but we can use the method in which watermark pattern is used for the watermark detection is directly generated from normal distribution. There will be registered user who can login into system then choose the image for the transformation attach required watermark to image and then by using Discrete cosine transformation algorithm divide that image into 8*8 block and with the help of CS matrix key encrypt that image and then reconstruct at the receiver side. The login user can be data holder/data owner. If the new user wants to send the data then he/she can register into system and then accordingly login into system.DCT does not provide the proper reconstructed image with wrong CS matrix key rate. Each new user provided with the facility of usage of different encryption key that is watermark or with the same key.

DCT Result Analysis:



Watermark added successfully

Image after adding watermark

Fig. Watermark attachment

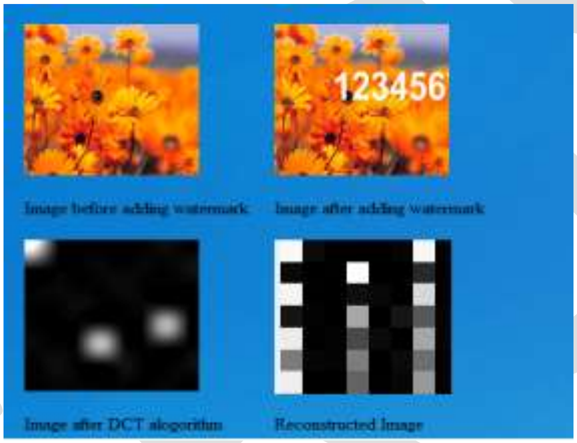
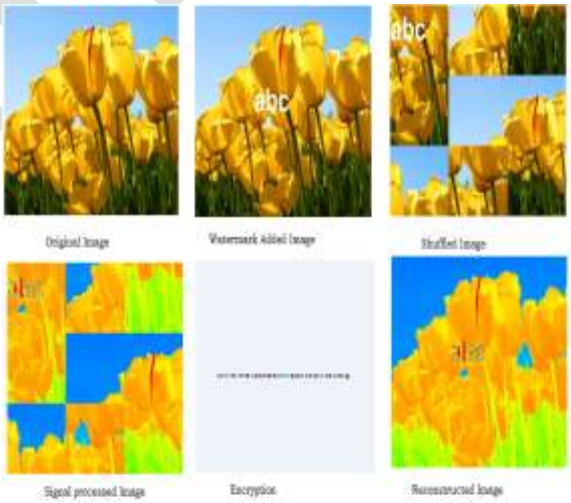
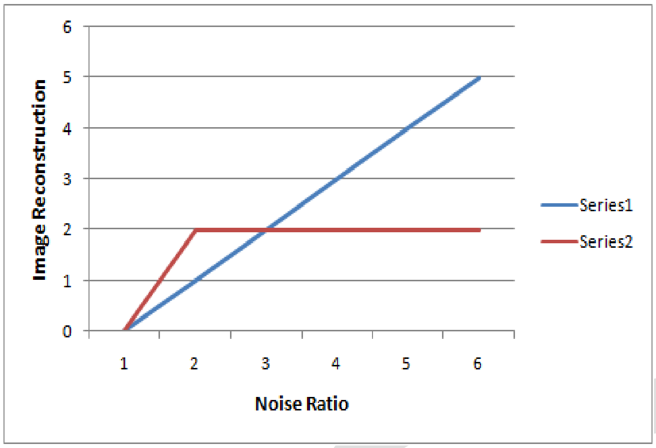

123456
Image before adding watermark
Image after adding watermark
Image after DCT alogorithm
Reconstructed Image

Fig.DCT algorithm applied

Proposed Algorithm Result Analysis:



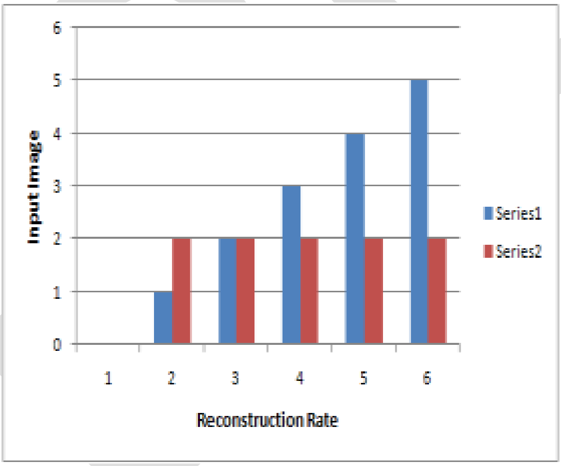
Graphical Comparison for the noise ratio and the reconstruction rate for both algorithms :



Series 1: DCT Algorithm

Series 2: Proposed Algorithm

Fig. Image noise comparison



Series 1: DCT Algorithm

Series 2: Proposed Algorithm

Fig. Image reconstruction rate

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.

CONCLUSION

Secure watermark detection is mainly used for privacy of the data on the cloud and security of the data, when the data is transferred between two different parties. Multi party computation protocol is used in this framework. Due to multiparty communication protocol two parties can be perform operation at the same time without disrupting each other and provide output. Restricted Isometric Property is used for the clearer image at the output side. Signal processing technique is used for analyzing the signals. Data holder, Watermark owner and cloud are the main concern. Certification Authority is used for providing the public key and CS matrix key. These frameworks perform better efficiency and flexibility for the storage of multimedia data. The project development part include the security of the system under different type of attack such as Brute force attack, Password cracking attack etc.

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. 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.
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. 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.
5. D. Hsu, S. M. Kakade, J. Langford, and T. Zhang, “Multi-label prediction via compressed sensing,” in Proc. NIPS, 2009, pp. 772–780.
6. 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.
7. 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.
8. 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.
9. K. Liu, H. Kargupta, and J. Ryan, “Random projection-based multiplicativedata perturbation for privacy preserving distributed data
mining,”IEEE Trans. Knowl. Data Eng., vol. 18, no. 1, pp. 92–106, Jan. 2006.
10. D. Donoho, “Compressed sensing,” IEEE Trans. Inf. Theory, vol. 52,no. 4, pp. 1289–1306, Apr. 2006.
11. J. R. Troncoso-Pastoriza and F. Perez-Gonzales, “Zero-knowledge watermark detector robust to sensitivity attacks,” in Proc. AC MultimediaSecurity Workshop, 2006, pp. 97–107.
12. 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, pp. 725413-1–725413-1.IEEE Trans. Knowl. Data Eng., vol. 18, no. 1, pp. 92–106, Jan. 2006.
13. 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