Watermark Detection for Security of Multimedia Data through MPC Privacy of multimedia Data on the Cloud

Ujwala Pawar[1], **Dhara Kurian**[2]

[1, 2]Department of Information Technology, RMD School of Engineering, Pune, India

Abstract: ***Privacy preserving is major concern when a user or data owner outsources the data through third party on cloud. The main task here is finding the structure of cloud computing so as to make it secure with the use of watermark detection. For dealing with such requirements, compressive sensing (CS) based layout along with using secure multi-party computation (MPC) protocols can be utilized. While in the CS conversion the secrecy is maintained by MPC of CS matrix and watermark reorganization. The data holder, the watermark owner and the cloud for storage of data are main major parts in this system. 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 unique protocol is followed by all MPC models. 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 image. In CS, it includes the aimed image, watermark reorganization and size of CS matrix. Some of the methods used such as Normal Distribution with District Cosine Transformation (DCT) can be used for watermark detection. The accuracy of the extracted functionality is approved through experiments. The analysis and the results of experiments give realistic solution by means of watermark reorganization.***

Keywords: digital, watermark, multimedia, encryption, compressive sensing, signal, processing, privacy, secure, multiparty computation

1. Introduction

Cloud Computing is one of the fastest growing technologies in the world. It helps the data holders by saving them the hassle of buying hardware and software and instead transfers all their data storage or computations of signal processing to the ever growing cloud. In order to preserve the privacy of data, the data storage and signal processing or data mining in the cloud will be done in an encrypted domain to preserve the privacy of data. As there is huge growth of social networks, public file sharing and Internet, a user may collect huge amount of multimedia data from various sources without the knowledge of the copyright information of that data. Many times the situation may arise so that, the user would want to make use of advantages of storage in cloud and simultaneously also work together with the owners of copyright for detection of watermarks while the multimedia data collected by self are kept private. Also, the owner of the watermark pattern would want to keep their watermark patterns private during watermark detection. Many cloud storage services may also wish to participate in detection of watermarks with or without the involvement of users of its service, so that it can check if the multimedia data that is being uploaded is copyright protected. There are many more benefits of storing the multimedia data that are encrypted and providing or using encrypted domain watermark detection in the cloud is that the encrypted data can also be reused if the original owner or the cloud would need to work together with other owners of watermark later for the purpose of secure watermark detection. The two types of approaches that have been proposed earlier for secure watermark detection are Asymmetric Watermarking and Zero Knowledge Watermark Detection. However, many of the existing watermark detection techniques presume that the watermarked document is available publicly and look mainly for the watermark pattern security but the security and privacy of the target media on which the watermark detection technique is performed has been ignored. In some applications, it is necessary that the multimedia data's privacy is protected in the watermark detection process. There are limitations in implementing privacy preserving storage and secure watermark detection at the same time by using the watermark detection techniques already existing like Zero Knowledge Proof protocols to transform user's multimedia data into a public key encryption domain, like complicated algorithms and communication, high computation and huge storage consumption in the public key encryption domain, which prevents their practical applications.

In this paper, we discuss about a privacy preserving watermark detection technique based on compressive sensing that uses secure MPC (Multi Party Computation) and the Cloud. It has been shown that many signal processing algorithms performed in the domain of CS (Compressive Sensing) have a very close performance as performed in the original domain.

2. Zero Knowledge Protocol and Asymmetric protocol

This system allows owner of the statement, to prove assured statement or clause to a different party, called verifier of the statement, without illuminating any understanding to the verifier apart from the fact that the assertion is valid.

For example: Where the owner claims to have a way of factorizing large numbers. The owner will send the verifier a large number and verifier will send back the factors. Successful factorization of several large integers will decrease verifier’s doubt in the truth of the owner’s claim. By the side of, the verifier will learn nothing about the actual factorization method.

In case of asymmetric protocol, where the consumer first commit to a secret that only consumer knows , then both consumer and retailer follow a procedure ,after which only the consumer receives a copy of the watermarked work. However, if the copy is unlawfully distributed, the retailer can recognize the consumer from whom the copy originate, and confirm it to a moderator by using a proper quarrel resolution protocol. A primary goal of asymmetric fingerprinting is a functionality that allows the retailer and consumer to mutually perform watermark embedding in such a way that the original content **xyz** is a secret input of the retailer, whereas the fingerprint data **bcd** is a private input of the consumer.

Privacy preserving storage of the data and safe watermark recognition concurrently is possible by using the existing secure watermark recognition technologies such as zero-knowledge proof protocols that transform the multimedia data to a public key encryption domain.

3. Secure CS Transformation Protocol

Secure multi party computation is similar to secure CS transformation protocol. The main goal of the secure multi party computation is to allow the participants to mutually perform the functions with their inputs, while keep their inputs private. Secure CS renovation protocol is constructed from secure scalar product protocol.

There are many secure scaling protocols called as homomorphism based, commodity based protocols and many more. In the homomorphism based protocol it requires two parties to jointly compute their functions without affecting the third party. In the technique of secrete sharing based protocol the secret information is distributed among the multiple participants involved in the computations the output will be generated only when all the secrets or many of them are combined together at the receiver side.

Pallier public key is used for this protocol for the cryptographic purpose. The Pallier public key takes only integer number or real number as input, but this framework also includes floating point numbers as well as characters. Therefore scaling of floating numbers into integer values is required.

4. The Proposed Framework

The framework mainly includes data owner, watermark owner and the cloud. Here following fig shows the actual working:

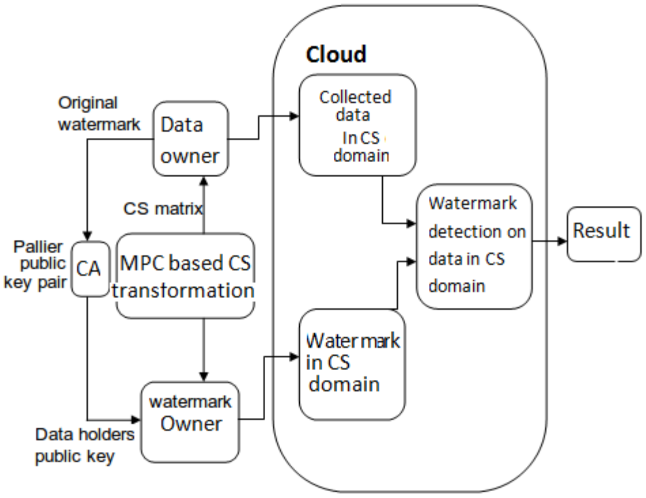

Figure: The Proposed Framework

There are mainly three parties in the projected structure, the data owner also called as data holder(DH) which can collect large amount of multimedia data, watermark owners (WO) which provide watermark for particular data to be transfer or for the image and the cloud (CLD)which is used for storage purpose as stated in Fig. The structure also requires a certificate authority (CA) for issuing the public keys (it may b Pallier public key or secrete sharing based key) and compressive sensing (CS) matrix keys to convinced participants including in the framework. When DH, collects a large amount of multimedia data from the Internet and stores their encrypted version in the cloud, those multimedia data can be edited and republished legally. Watermark owners (WOs) are the information providers who distribute their watermarked information. WOs always want to know if their information is officially used and republished. In some cases, not only DH and WO care about the duplication of the multimedia data, certain cloud who offers storage services may also want to start the watermark.

5. Analysis

1. Security Analysis

Secure scalar protocol is secure under the semi-honest model, multiparty computation protocol is also secure under semi honest model, that is two or more parties can jointly perform their function without affecting to the third party. Following running the secure CS transformation protocol, Data Owner and Watermark Owner do not disclose their personal values to other parties. Only the CLD has the image information and watermark outline in the CS domain.

Information theoretic privacy relies on the statistical properties of a system, and provides protection even in the face of a computationally unbounded adversary. An encryption scheme achieves perfect secrecy if the probability of a message conditioned on the cryptogram is equal to the a priori probability of the message, $P(X = x |Y = y) = P(X = x)$. Alternatively, this condition can also be stated as $I(X; Y) = 0$.

2. Complexity Analysis

When the image is stored on cloud and the watermark pattern for the image in the Compressive Sensing domain, watermark detection in the CS domain involves linear correlation, so it can shows slight computational overhead. Consider the watermark size is x and the CS matrix size is x*y, Watermark Owner performs x*y exponentiations and x encryptions in the public key domain, and Data Holder performs x*x encryptions and x decryption in the public key domain. For communication complexity, DH sends WO m*n public key encrypted values and WO sends DH m public key encrypted values. Sometimes the Data owner might be a computationally weak party such as mobile device. In this framework, the complexity of Data owner is reduced when there are multiple watermark owners who are interested in performing watermark detection. When there are multiple watermark owners who are involved in performing watermark detection on an image, the data owner can send the public key encrypted CS matrix to the cloud.

6. Experimental Results

For the testing purpose of the proposed system 512*512 image is considered. For watermark detection there are several methods. We choose the one in which the watermark pattern used for watermark detection is directly generated from a Normal distribution *N* (0, 1).

Consider a CS matrix *Φm×n*; *m/n* will be referred to as the compressive sensing rate (*CS rate*). Since the CS matrix size will be extremely large if we convert the 512×512 image to a vector for CS transformation. Instead, we cut the image into pieces and each piece contains 64 8×8 DCT blocks.

Selective DCT coefficients of each piece will form a vector and be transformed to a CS domain with the same CS rate but using different CS matrices. The data in the CS domain from all pieces is treated as {pi*}*. Similarly, we get {*ri*} from the 512×512 original watermark pattern.

Scalability is required for converting the floating point values into integer values as Pallier public key is used. Reconstructed image is totally random and not that much clear. Restricted Isometric Property (RIP) is used for the reconstruction of the image as original image contour is preserved during transformation.

7. Conclusion

This paper proposes a Secure Signal Processing Framework based on Compressive Sensing that would enable simultaneous secure watermark detection and privacy preserving storage. To protect private data, this framework is secured under the semi-honest adversary model. This framework would fail to protect the secret values without the semi-honest adversary assumption. Collision between WO and CLD will cause the leakage of DH's CS matrix. This framework is more efficient and flexible and also protects privacy when compared to previous secure watermark detection protocols. This framework can be also extended for other secure signal processing algorithms in addition to watermark detection.

References

[1] E. Candes, J. Romberg, and T. Tao, “Robust uncertainty principles: Exact signal reconstruction from highly incomplete frequency information,” IEEE Transactions on Information Theory, vol. 52(2), pp. 489–509, 2006.

[2] E. Candes and T. Tao, “Near optimal signal recovery from random projections: Universal encoding strategies?” IEEE Transactions on Information Theory, vol. 52(12), pp. 5406–5425, 2006.

[3] D. Donoho, “Compressed sensing,” IEEE Transactions on Information Theory, vol. 52(4), pp. 1289–1306, 2006.

[4] T. M. Cover and J. A. Thomas, Elements of Information Theory. Wiley-Interscience, 2006.

[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.