International Journal of Application or Innovation in Engineering & Management (IJAIEM)
Web Site: www.ijaiem.org Email: editor@ijaiem.org
Volume 3, Issue 11, November 2014 **ISSN 2319 - 4847**

Privacy Enhancement of data with safe watermark extraction using signal processing

H.N.Ranotkar[1], Prof. M.S.Deshmukh[2]

[1]Department of Information Technology, PRMITR, Badnera

[2] Assistant Professor, Department of Information Technology, PRMITR, Badnera

ABSTRACT

In this era of cloud computing, protecting the data privacy is an important consideration. Also, due to the rapid growth of the Internet and social networks, a user can easily gather large amount of data from different sources without worrying about its copyright information. So it becomes essential for the data owner to add their ownership information into the data which can be done by using watermark technique. Due to this, only authenticated users can reuse and republish the data. In this paper, we propose an architecture that provides privacy protection of image data as well as the secure watermark extraction in a simultaneous manner by using sparse sampling and secure computation. This paper enhances the privacy of data by applying layer of encryption over the data using data hiding technique before it is passed to the sparse sampling transformation. This will make the proposed architecture tolerable against the semi-honest security assumption required for the simultaneous operation in sparse sampling domain. At the side of reconstructing an image, we proposed to yield with better quality and robustness than the existing system.

Keywords:- sparse sampling, privacy protection, data hiding, DWT, safe watermark extraction, secure computation

1.INTRODUCTION

In this era of cloud computing, protection of privacy of the data is an important issue. In order to protect the privacy of the data, most of the storage places hold it in an encrypted form. But, the rapid growth of the Internet and social networks made it very easy for a normal user to gather a large amount of multimedia data from different sources without having the copyright information of those data. So, data owner also wants to add ownership information in the multimedia data so that it can be reused and republished by the authenticated user only. This is done by using a watermark technique. It means that the protection of the privacy of watermark pattern, if applied, from the unauthorized user is also an important aspect. But, in many outsourced processing application it is identified that safe watermark extraction and multimedia data privacy protection is required simultaneously. To resolve this issue secure signal processing is performed over the encrypted domain. The normal user wants to take benefit of the storage place for storage, simultaneously working with the copyright owners for watermark extraction keeping the privacy of the multimedia data. The watermark pattern provider also wants to keep their watermark patterns private during the watermark extraction. The different legal storage place offering storage services may also wishes to participate in watermark extraction process to decide whether the uploaded multimedia data is copyright protected or not. Another advantage of storing data in an encrypted form and facilitating watermark extraction at storage place is that we can reuse the same encrypted data if data holder wants to work with another watermark provider who provides more safe extraction. In traditional safe watermark extraction techniques, verifier is convinced to the presence or absence of watermark in the data without revealing the watermark pattern so that an untrusted verifier cannot remove the watermark from the watermark righted copy [3], [11]. There are two approaches for safe watermark extraction: 1. Asymmetric watermarking [14] and 2. Zero-knowledge watermark detection [4], [7]. But most of the existing watermark extraction techniques deeply concentrate on the security of watermark pattern paying very less attention towards the privacy of the data on which the extraction process is carried out. But as we cannot compromise with the privacy of the data, in many applications, it is required to protect the multimedia data's privacy during the watermark extraction process. Implementing such privacy protecting storage and safe watermark extraction simultaneously is possible by using the existing safe watermark extraction technologies such as zero-knowledge proof protocols [4], [7] that transform the multimedia data to a public key encryption domain. But it too has certain limitations like complicated algorithms, high computational and communication complexity [11], which may affects its practical implementations. So to overcome these issues Q.Wang et al[19]used a compressive sensing technique with secure multiparty computation protocol to form a framework that simultaneously perform privacy protection and safe watermark extraction in the storage place. By this, they made the first attempt to provide attention to the privacy of data while extracting the watermark. But, this system is secured under semi-honest assumption only and there is no way to protect the privacy of data if the compressive sensing matrix value is leaked.. It uses DCT coefficients of the image over

which the compressive sensing transformation is performed before it is passed to the storage place. For privacy preserving storage, since the DCT coefficients are not perfectly sparse, the CS reconstruction will introduce distortion to the reconstructed image. Also it is not robust against major modification .So the quality of the reconstructed image and robustness with semi-honest assumption is an issue. Hence, to improve the quality of reconstructed image, we need to improve the SNR and have to minimize the MSE and has to find a way to make the architecture tolerable against semi-honest assumption [6].

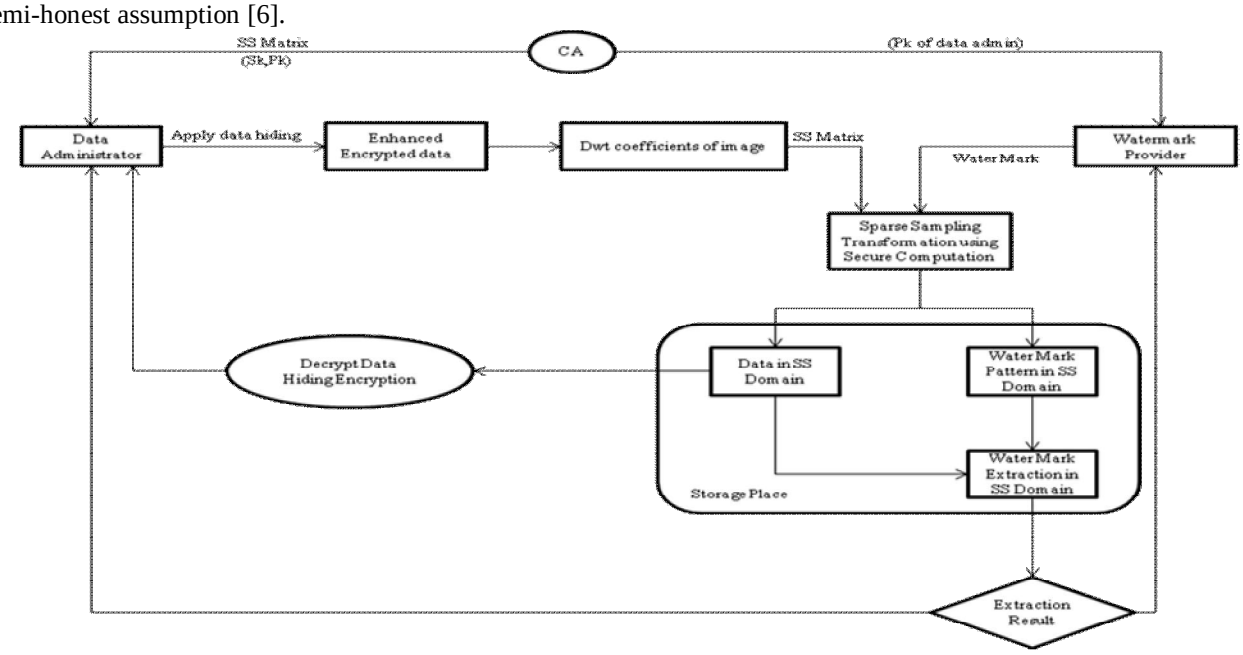

Figure1 Proposed architecture

In our proposed architecture, the target image/multimedia data is possessed by the data holder only. Firstly he will apply data hiding principle over the target image data that makes the architecture tolerable against the semi-honest security assumption required at sparse sampling transformation. . As protection of data is a primary issue, we must enhance the privacy of data before it is forwarded for SS transformation. A sparse sampling matrix is then issued by a certificate authority server to the data holder. He then obtains DWT coefficients [1], [17] of the image over which sparse sampling transformation is performed before it is outsourced to storage domain. Using secure computation protocol [5], the watermark is transformed to the same sparse sampling domain then sent to the storage place for secure watermark extraction. It means that the storage place will have the data only in the sparse sampling domain. So, it is very essential for the storage administrator to have the sparse sampling matrix used for SS transformation to reveal the original data. Also to improve the robustness and quality of an image at reconstruction side, we supposed to improve the signal to noise ratio of the image and try to minimize the MSE. For this, we prefer to deal with DWT (Discrete Wavelet Transform) coefficients of the image rather than DCT in existing system [19]. To enhance the privacy of data we apply the data hiding principle over the data to form a new secret data. To protect their privacy form the outsource user, unless he is a legally authenticated person, we need to perform the randomize encryption over the data. The randomized encryption is performed by providing the new sparse sampling matrix for every data/image. This randomized encryption makes the attacks over the data (like brute force) only probabilistic as every time new sparse sampling matrix is generated for the data. The use of secure computation protocol in our work will provide public encrypt domain watermark detection in the storage place that makes reuse of encrypted data possible if the image/data administrator wants to work with other watermark providers for the safe watermark extraction.

2.LITERATURE SURVEY

In 1999, P.Paillier [2] studied various public key cryptographic systems. In this paper, he found out a new problem called Composite Residuosity Class problem and its application in public key cryptography He then proposed a new trapdoor mechanism and obtained three new encryption schemes of which two are homomorphic probabilistic encryption scheme and one is trapdoor permutation scheme. He also proved it secure under adequate intractability assumptions. The limitation is that he had not given any proof of security against chosen ciphertext attacks. In 2000, J.Eggers et al [3] reviewed most of the watermarking schemes in which watermark detection is not possible without explicitly referring he embedded signal which is a security risk. In this paper, they extended a public watermark detection scheme of Van Schyndel et al which does not require referring an embedded signal for the detection of watermark to a linear transform. They also proved that the complexity of their work is less as to the previous scheme. The robustness against major modifications of their proposed work is also better than the previous work. But, to do so,

their scheme requires long signal and so performance time was an issue. In 2001, A.Adelsbach et al [4] gives the precise definition of zero-knowledge watermark detection scheme. The objective of zero-knowledge watermark detection is to allow a prover to convince the verifier regarding the presence of watermark in certain data. But, doing so he should not expose any information that the verifier can use to remove the watermark. In this paper, efficient and provably secure zero-knowledge protocols are proposed for the different blind and non-blind versions of different watermarking schemes. These protocols provide improvable security to all the applications where a user has to prove the presence of watermark to any untrusted third party. They also proposed the protocols for proof of ownership which does not require the presence of trusted third party in the activity of proof of ownership. This in turn provides improvement in scalability and practicality of proof of ownership. The limitations of their work were complicated algorithms in implementation, high computation and communication complexity had affected their practical applications. In 2004, B.Goethals et al [5] had worked out on need of private scalar product protocol for privacy preserving in many data mining applications. When we integrate data from multiple sources privacy of data is an important issue. In this paper they made it clear that in several different contexts, the security of the full privacy-preserving data mining protocol depends on the security of the private scalar product protocol it uses. In their work, they compare different private scalar product protocol and showed how they are insecure. They proposed a private scalar product protocol based on standard cryptographic assumptions and showed that it is secured. This protocol is based on homomorphism technique and yields an improvement in its efficiency. In this protocol there are two parties that will share the final scalar product. In 2006,M.Malkin et al[7] had proposed a cryptographic method for safe watermark detection. They described a semi-public key implementation of quantization index modulation watermarking called Secure QIM .For a given signal, a watermark detector was supposed to learn the presence of a SQIM watermark without focusing on anything else from the detection process. In this paper, the watermark detector transformed the signal with secret transform and then quantizes the transformed coefficients value with secret quantizer. However, both the secret values are unknown to the watermark detector. For doing so, they used homomorphic cryptosystems. At the end trusted, secure module is used that reveals whether the signal was watermarked or not. This method is also based on the zero-knowledge watermark detection. The limitations of the work was complicated algorithm, high computational complexity, large storage consumption in public key encryption domain In 2006,K.Liu et al[11] studied random projection-based multiplicative perturbation techniques for the problems like computation of inner product matrix ,Euclidean distance, correlation matrix for distributed data owned by different parties which may play vital role in many data mining techniques as clustering,classification,principal component analysis.Later,they introduced random orthogonal transformation-based data perturbation approach. This had preserved the length and distance between the original data vectors. Then for breaching privacy they brought up Independent Component Analysis as a tool. Finally, they proposed a random projection-based technique to perform transformation over the data while preserving its certain characteristics in an effective manner. In 2006, D.Donoho [14] proposed compressed data acquisition protocol. This protocol collects only the important information form the input signal rather than acquiring the entire signal. This proposed protocol does not require the knowledge of input signal in advance. So, they were non-adaptive and parallelizable. Since, the measurements made in this compressed sensing protocols are holographic they must be processed in nonlinear fashion. In his work he had provided the rules for reconstructing the object and proved that good reconstruction of the compressible object was possible though we were under sampling the input signal. In 2006, M.Rudelson et al [15] precisely describes the sparse reconstruction problem and its convex relation. They then proved the best known guarantees for the perfect reconstruction of the sparse signal form the random Fourier and Gaussian measurements. These proofs were based on Geometric Functional Analysis methods. In 2007, Z.Erkin et al [2] studied the different cryptographic primitives used in applications that directly manipulates encrypted signals and identified the need of security requirements in these applications. They described the secure signal processing into two domains as content retrieval and content protection. They studied out the various approaches for performing secure signal processing and find out the challenges of content protection. In 20007, J.Tropp et al [16] proposed an comparable alternative for Basis Pursuit. In this paper, they described the greedy algorithm called Orthogonal Matching Pursuit and proved it had the ability to correctly recover the signal from given random linear measurements of that signal. The proposed algorithm provides improved result than the previous work done over the Orthogonal Matching Pursuit. In 2008, A.Orsdemir et al [21] gives the precise description of compressive sensing. In this paper, they studied security and robustness of compressive sensing based encryption methods. For the security issues they considered various structured attacks and brute force attack and showed that the compressive sensing based encryption is secured against these attacks. They also found that compressive sensing based encryption was tolerant to the additive noise in the compressive sensing based measurement that made it a robust encryption. In 2009, D.Hsu et al [19] , showed how to apply algorithms for compressed sensing to the output coding approach. In their work, they focused on accuracy of reconstruction based on prediction that showed how to reconstruct an uncompressed label from the compressed predicted labels using reconstruction algorithm. In this paper, they considered prediction problems with output sparsity and applications of compressive sensing to it. They developed an efficient output-coding scheme that made the number of prediction only be logarithmic to the total number of labels. They also guaranteed the robustness of this method in the form of regret transform bounds. In 2010, W. Lu et al [13]

identified the problems of content-based multimedia retrieval over the encrypted databases. In this paper, they proposed two types of secured privacy preserving content retrieval schemes. In the first technique one would encrypt features of multimedia data and perform similarity comparison of the features in their encrypted forms. The other type of scheme was to encrypt the state-of-art search indexes and did not affect their search capability. When discussed about the performance, they had shown that performance comparable to the plaintext retrieval was achieved. They had proved that these schemes are secured against the ciphertext only attack model. In 2010, M. Davenport et al [17] had identified that many signal processing problems did not require the recovery of entire signal. In this paper, they had taken first step towards the use of compressive sensing for solving the inference problems as detection, classification, estimation and filtering problems. They had provided the experimental results that demonstrate efficiency and accuracy of extracting information from signals compressive measurement directly in many applications rather than reconstructing the signal and then extracting the information. In 2013, T. Bianchi et al [1] had discussed various benefits and issues of secure watermarking schemes an let the signal processing community to have the recent results of secure watermarking. In this paper, they discussed three schemes of secure watermarking: secure server-side embedding, secure client-side embedding and secure watermark detection. They asked to explore the various challenges in secure watermarking for secure signal processing communities. In 2014, Q.Wang et al [19] proposed a compressive sensing based secure watermark detection and privacy preserving storage framework. By this work, they put the first step towards providing a framework that simultaneously allows secure watermark extraction and privacy protection .In their work, while performing the watermark extraction over the data its privacy protection is considered which had never done before. The limitation of the work is that it is secured under the semi-honest assumption and if the privacy of compressive sensing matrix is leaked then there is no way to protect the privacy of data .The proposed framework makes use of the DCT coefficients of the image. So, at the time of reconstruction, the image may be the distorted one, especially when the compressive sensing rate is low. As a result, the quality of an reconstructed image is an issue. Besides this, the robustness against modification is also an issue.

3.ACKNOWLEDGEMENT

I owe my deep gratitude to my respected guide Prof. Ms. M.S.Deshmukh who gives me the valuable guidelines with a touch of inspiration and motivation to progress my way through quite substantial barrier between early problem statement and something that resembled a fine work.

4.CONCLUSION

In this paper, we proposed the architecture that protects and enhances the privacy of the data and simultaneously allows the secure watermark attraction. The architecture enhances the privacy of data by forming the new encrypted data using data hiding principle that makes it tolerable against the semi-honest security assumption. It also supposed to improve the robustness, scalability and quality of an image data as it operates on DWT coefficients of image data. It is proposed to provide better SNR ration than the existing system.

REFERENCES

[1] Rafael C. Gonzalez, Richard E. Woods.(1992), Digital Image Processing(2nd edition), NJ:Prentice Hall
[2] P. Paillier, “Public-key cryptosystems based on composite degree residuosity classes,” in Proc. Adv. \ Cryptology-Eurocrypt, 1999, pp. 223–238.
[3] J. Eggers, J. Su, and B. Girod, “Public key watermarking by eigenvectors of linear transforms,” in Proc. Euro. Signal Process. Conf., 2000.
[4] 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.
[5] B. Goethals, S. Laur, H. Lipmaa, and T. Mielikainen, “On private scalar product computation for privacy-preserving data-mining,” in Proc. 7th Int. Conf. Inf. Security Cryptology, 2004, pp. 104– 120.
[6] O. Goldreich, The Foundations of Cryptography. Cambridge, U.K.:Cambridge Univ. Press, 2004.
[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] 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.
[9] D. Donoho, “Compressed sensing,” IEEE Trans. Inf. Theory, vol. 52,no. 4, pp. 1289–1306, Apr.2006.
[10] 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.
[11] 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

[12] J. Tropp and A. Gilbert, "Signal recovery from random measurements via orthogonal matching pursuit," IEEE Trans. Inf. Theory, vol. 5, no. 12, pp.4655-4666. Dec. 2007
[13] 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
[14] D. Hsu, S. M. Kakade, J. Langford, and T. Zhang, "Multi-label prediction via compressed sensing," in Proc. NIPS, 2009, pp. 772–780
[15] 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.
[16] M. Davenport, P. Boufounos, M. Wakin, and R. Baraniuk, "Signal processing with compressive measurements," IEEE J. Sel. Topics SignalProcess., vol. 4, no. 2, pp. 445–460, Apr. 2010.
[17] Anilkumar Katharotiya ,Swati Patel, Mahesh Goyani, "Comparative Analysis between DCT & DWT Techniques of Image compression" in Journal of Information Engineering and Applications Vol 1, No.2, 2011
[18] 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.
[19] Qia Wang, Wenjun Zeng, Fellow, IEEE, and Jun Tian,Member, "A compressive sensing based secure watermark detection and privacy preserving storage framework", IEEE issues in IEEE Transactions on image processing, vol. 23, no. 3,march 2014