SECURE DATA SHARING USING VISUAL CRYPTOGRAPHY AND WATERMARKING METHOD IN FOG COMPUTING

Suraj Gajul, Anirudhha Gite, Vikas Kedari, Prashant Kumbhar

Suraj Gajul, Computer Science Department, SKNSITS, Collage Lonavala, Maharashtra, India
Aniruddha Gite, Computer Science Department, SKNSITS Collage Lonavala, Maharashtra, India
Prof: Madhuri Mali, Computer Engineering, SKNSITS College Lonavala, Maharashtra, India

---***---

Abstract - *Now a days, fog computing is the popular for the storage of the data. Fog computing is further version of cloud computing. Fog computing secure about data, compute, storage, and application services to end-users.We know many security issue are generated like as attack on network. In previous systems they are used encryption and decryption technique with watermarking technique for the security purpose. Encryption technique refer as the to provides the security key in the form of cipher text to the data while decryption mean to convert the encoded data to the decoded data that means to get the back text in the form of computer read. In propose systems we are using a visual cryptographic technique with watermarking for security purpose. Visual cryptographic is defined as the technique which allows the information in the form of visual for the encrypted and decrypted data. Watermarking provides the authentication to client and server for the security purpose. In previous systems they were used a simple watermarking technique.Here,we used the digital watermarking technique by using the discrete wavelength transformer(DWT).By using the visual cryptography and watermarking we share the data on fog computing.*

***Key Words*: Fog computing, Encryption, Decryption, Visual cryptography, Watermarking etc.**

1. INTRODUCTION

In today's worlds the small as well as big organizations are using cloud computing technology to protect their data and to use the cloud resources as and when they need. Now a these day, the digital word provides such as electronic contains, computer fields such as information technology is popular for the share the data which is demand of the people. It is benefits for the people. Security issue also generated for the transmission of the data from sender to receiver like as mobile users and media cloud .Cisco introducing fog computing for the overcome problems of the share of the data secure purpose. Fog computing support to store of the data, compute, and geographical users for the users. Visual cryptography refers for the shares the image secretly between to users. Here, we applied encryption for the transmission purpose. Watermarking provides authenticate for the owner's data.

2. LITERATURE SURVEY

2.1 VISUAL CRYPTOGRAPHY

Cryptographic confidential about security purpose of the data which is belongs from the encrypted scheme. This technique uses binary images which is consist from SH1 and SH2 encoded blocks and black white color[1].These systems is implemented by the Naor and Shamir.After that, [2]Wu and Chen experiments told to us encoded two binary images shares, suppose fiest and second. First can be revealed by stacking both shares and second share can be revealed by rotating one of them by some angle in both direction. Borchert mentioned about segment based visual cryptography used for the encryption of messages containing alphanumeric symbols [3]. Indrakanti S. P. and Avadhani P are worked on segment based visual cryptography for Key distribution [4]. S. S. Hegde, Bhaskar Rao, introduced secret sharing scheme in which secret shares are hidden in meaningful cover images[5].The expriments of Sian Jheng Lin and Wei-Ho Chung provides about a probabilistic model of visual cryptography scheme with dynamic group which means the divide the an image into n shares.[6]

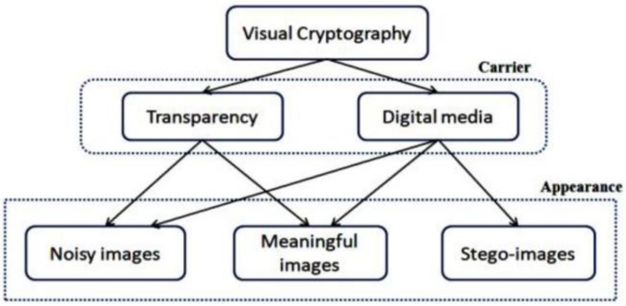

Fig 1: Classification of visual cryptography

2.2 WATERMARKING AND VISUAL CRYPTOGRAPHY

This day's internet is a popular medium for the transmission purpose the digital information from source to destionation.That means time of the transfer, illegal copies of the original data can be made to make interchange the information. The watermarking schemes provide watermark to directly image to be protected, in order to prevent abuses and illegitimate distribution of the image. Watermarking algorithm used for the give the input to the embedding phase and another algorithm for the stored and protected. The modulus of the watermarking are owner of the image and trusted authority for no one stolen them image.

2.3 WATERMARKING WITH (2,2)VC SCHEME

We know VC scenario is the combination of watermarking and visual cryptography. Naor, M., Shamir thought that private key cryptosystem, the phase of the encoded are first share the cipher test and another is role of secret key [7]. Wherever the cipher text decoded by different transfur.Hencefourth, input image to the VC scheme I as the watermark.

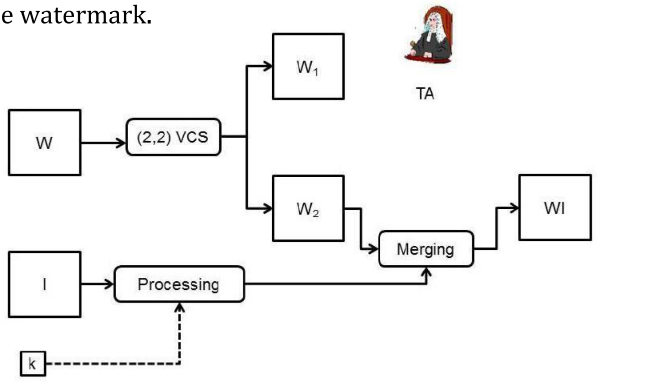

Fig - 2: Embedding phase for watermarking com-bined with a (2, 2) VC scheme

3. ARCHITETURE

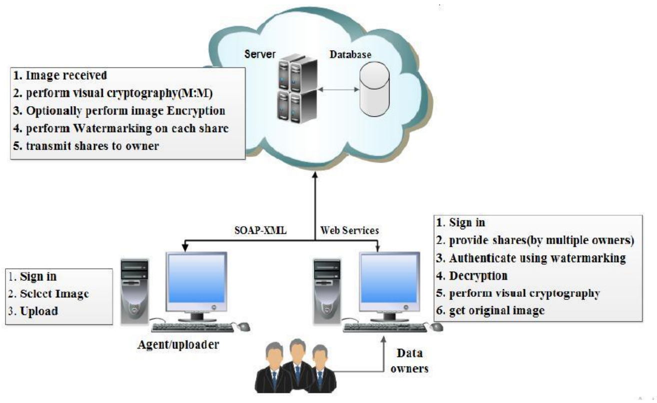
Server
Database
1. Image received
2. perform visual cryptography(M:M)
3. Optionally perform image Encryption
4. perform Watermarking on each share
5. transmit shares to owner
SOAP-XML
Web Services
1. Sign in
2. Select Image
3. Upload
Agent/uploader
1. Sign in
2. provide shares(by multiple owners)
3. Authenticate using watermarking
4. Decryption
5. perform visual cryptography
6. get original image
Data owners

Fig- 3: System Architecture

System architecture consisting of three parts described as follows:

3.1 REGISTRATION PHASE

In the registration phase, provides the information of a person about password, watermark details and number of owners of the image must be provided by User. All the information is stored inperticular database. Uploader and data owners must register to the fog. No further processing can be done without registration

3.2 PROCEESING PHASE

Uploader uploads image to the fog. fog splits the received image into N number of shares of uploader. If Uploader wants to provide more security to the shares then these shares will be encrypted. For authentication of each share and its owner, watermark is answer of the applied on these shares. These shares are transmitted to its particular owner's E-mail.

3.3 REVERSE PROCESSING PHASE

For the retrieve the original image, the data owners provide their shares to the fog for further processing. These watermarked shares are checked for authentication of the users. Valid shares are then decrypted provided by the owner if encryption is applied on the shares. The original image obtained the when all the key decrypted. Second thing is n shouldn't retrieve.

4. CONCLUSIONS

In this paper, we proposed security for the particular image whoever having multiple owners. The main objective of this paper is to provide equal digital rights to the owners of the image. Visual cryptography technique refers for which generates N shares according to the number of owners and the watermarking gives to authenticate each share with its owner. The security of data is maintained using both visual cryptography and watermarking. Thus the proposed systems is the requirement of security and digital rights management by using the fog computing.

REFERENCES

[1] Moni Naor and Adi Shamir, "Visual cryptog-raphy". In Proceedings of the advances in cryptology- Eurocrypt, 1-12,1995.

[2] C.C. Wu and L.H. Chen, \A Study On Visual Cryptography", Master Thesis, Institute of Com- puter

and Isnformation Science, National Chiao Tung University, Taiwan, R.O.C., 1998.

[3] B. Borchert, \Segment Based Visual Cryptogra-phy", WSI Press, Germany, 2007

[4] Indrakanti S. P. and Avadhani P. S. \Segment based Visual Cryptography for Key Distribu-tion". IJCSES Vol. 3, No. 1, Feb 2012.

[5] S. S. Hegde, Bhaskar Rao, \Cloud Security Using Visual Cryptography", International Journal of Distributed and Parallel Systems (IJDPS) Vol.3, No.1, January 2012,pp.9-13.

[6] Sian-Jheng Lin and Wei-Ho Chung, \A Prob-abilistic Model of (t,n) Visual Cryptography Scheme With Dynamic Group", IEEE Transac-tions on Information Forensics and Security, vol. 7, No. 1, February 2012, pp.197-207.

[7] Naor, M., Shamir, A.: Visual cryptography. In: De Santis, A. (ed.) EUROCRYPT 1994. LNCS, vol. 950, pp. 1{12. Springer, Heidelberg (1995)