ISSN 2395-1621

Multi-owner Data Sharing using Visual Cryptography

[#1]ShaharukhPathan, [#2]Saood khan, [#3]Pramodmahale

[1]pramod.mahale6@gmail.com
[3]pathanshaharukh786@gmail.com

[#123]Student of Computer Engineering
AAEMF'S COE & MS,BhimaKoregaonPune,India

ABSTRACT

In this paper, we are going to propose sharing of the data among many (multi) owners in the cloud system . As we know that cloud is a threatful area which we are going to use as a platform and provide security to our image data for transporting it form one place to another. And also many new techniques are being used for as a security shield in our proposedsystem.

Keywords: Visual Cryptography, RSA technique, Alpha ChannelWatermarking

ARTICLE INFO

Article History

Received:19th December 2015

Received in revised form :

22st December 2015

Accepted:23rdDecember, 2015

Published online :

24th December 2015

I. INTRODUCTION

In the fast technological world, many traditional security techniques are provided to secure data exchange between various devices. But the existing system does not provide much of the security to the media. In the existing system, lightweight security is used, secondly digital rights management is most important. There are multiple owners who are having equal rights for a single data; there is a need to give an equal authority to all the data owners. There is no single administrator who has all the rights to that confidential data. The confidential data should be secured in such a way that no single administrator from all the data owners will be able to get the data as a whole. The need for implementing adequate security services is increasing so that the confidential data cannot be accessed by unauthorized people. To address the above challenges, we proposed the system to use both secure sharing and watermarking schemes to protect user's data. The secure sharing scheme gives the security to the data and watermarking scheme will authenticate the particular data to the individual owners.

Thus our proposed approach achieves good security performance.

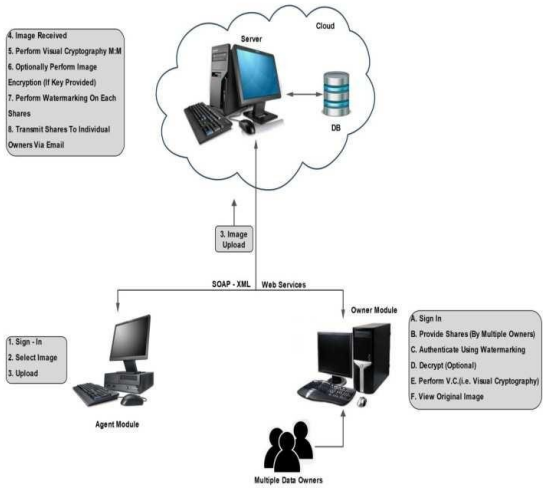
II. EXISTINGSYSTEM

The system that were used initially were containing some basic approaches . For example, some used to provide the data security by just using encryption method. This process used to upload the data and after that apply the process of encryption . Also they used to generate a KEY which will then use for the decryption of the data. Also some used to give the access time for the data. This was also another kind of security .The complexities of user participation and revocation in these schemes are linearly increasing with the number of data owners and the number of revoked users

III. PROPOSEDSYSTEM:

In this system we are going to provide a multi level of security to the data .this security will be provided to the image on the cloud .In this project, visual cryptography is used to provide equal digital right to all the owners. To provide more security during transmission of the shares, encryption can be applied on each share. Watermarking is applied on the shares to authenticate each share with itsowner.

IV. SYSTEM ARCHITECTURE



V. MODULES

A. RegistrationPhase

In the registration phase, along with the personal information, password, watermark details and number of owners of the image must be provided by Up loader. All the information is stored in database. Up loader and data owners must register to the cloud. No further processing can be done withoutregistration.

B. ProcessingPhase

up loader uploads image to the cloud. Cloud splits the received image into N number of shares defined by up loader. If Uploader wants to provide more security to the shares then these shares can be encrypted. For authentication of each share and its owner, watermark is applied on these shares. These shares are transmitted to its particular owner via E-mail. processing. These watermarked shares are checked for authentication of the owner. Valid shares are then decrypted using the key provided by the owner if encryption is applied on the shares. Once all the shares are decrypted, these shares are superimposed to obtain the original secret image. Shares less than N cannot reveal the secret; all the shares are required to obtain the original secretimage.

C. Reverse ProcessingPhase

To retrieve the original image, the data owners must provide their shares to the cloud for further

VI. WORKING

As we have discussed about the working scheme of our system , the registration phase include the signing in of the user . He will first sign in and will select the select the image that we want to send. The image will then be uploaded on the cloud .the main process starts from here, the image will first undergo visual – cryptography. In this process the image will be broken down into different shares. The no of shares wll be decided by the user who wants to send the image to other place .

Then particular share of the image will undergo image encryption. This is the second step of providing security totheimage share. As the encryotion is done the key is generated , this key is then send to the owner who are at the receiving end.

Then after that the share of image will go under water marking process. The water marking is basically used for authentication .this is the third level for providing the security to theimage.

At the other end ,the owner that were selected for receiving the image will download the image. After downloading the image the key that was sent via e-mail is applied and the decryption is done .after that the image share will then be combined by de- visual cryptography and the original image is obtained

Algorithms algorithm 1:Encryption.

RSA Algorithm includes three steps: Key generation, Encryption and Decryption described as follows: Key Generation: The keys for algorithm are generated using followingsteps:

1. Select two different large prime numbers A and B. The numbers can be selected randomly and they should be of equal bitlength.
2. Calculate n=A*B; n is used as modulus for both keys that is public and privatekey.
3. Calculate the Euler's totient function Φ as Φ(n)=(A- 1)(B-1).
4. Select a number e such that 1<e<Φ(n) and GCD(Φ(n),e)=1; e and Φ(n) must be co-prime numbers.
5. Calculate d=e-1(mod Φ(n)), where, d is the multiplicative inverse of e modΦ(n).

Encryption:

1. Select a message M, such thatM<n
2. Calculate cipher text C, C=Me(modn).

Decryption: Select the cipher text C, and recover the message M, M=Cd (modn).

Algorithm 2: Watermark Embedding.

Input: Host color image I, color watermark W, and a key K. Output: Watermarked image I'.Steps:

1)Transform the host image I into a PNG image by adding the alpha channel plane A, and assign the values of pixels in A to0.

2)Select a region R, where watermark W is to be embedded, in the host image I and replace the pixel's color values in R with the values in W, and for every replaced pixel get the RGB value of 24 bits to form data stringS.

3)Assign the values of the pixels in A to 255 underlying the watermark inR.

4)To randomize the order of the bit sequence to get S' of the bit sequence in S use a keyK.

5)Take 3 bits at a time from S' and an alpha pixel from A, as s and p, respectively , and follow the steps:

a. Convert s into a decimal numbers'.
b. If p is not equal to 255, replace p with s'; otherwise, take the next alpha pixel fromA.

6)If there are bits in S' to be embedded, then go to Step 5; otherwise,continue.

7)Add 247 to all pixels in alpha excepting those having value 255 in A; getting the new values which are in the range of 247 to 254 and denote the resulting A, containing the alpha values from 247 to 254 and those having value 255 set in Step 3, to beA'.

8)Obtain the resulting Image with the embedded W together with the A' as the desired watermarked image I'.

9)The data required for the removing the watermark from the watermarked image will be obtained from the alpha channel plane. After the removal of the watermark, the alpha channel is eliminated in order to obtain the original color host image in the reverse process.

VII. CONCLUSION

In this system we thus provided the security to our image data type .the cloud system is thus secured by using our security system. Thus cloud computing can be easily be secured to the storing of the image data type. In future we are aiming to provide the security to the data rather than images.

REFRENCES

[1] Mr. Parjanya C.A Mr. Prasanna Kumar M Advance Secure Multi-Owner Data Sharing for Dynamic Groups in the Cloud in Volume 4, Issue 3, March2014

.

[2] Xuefeng Liu, Yuqing Zhang, Boyang Wang, and Jingbo Yan, "Mona: Secure Multi-Owner Data Sharing for Dynamic Groups in the Cloud", IEEE TRANSACTIONS ON PARALLEL AND DISTRIBUTED SYSTEMS, VOL. 24, NO. 6, JUNE 2013.

[3] D. Naor, M. Naor, and J.B. Lotspiech, "Revocation and Tracing Schemes for Stateless Receivers," Proc. Ann. Int'l Cryptology Conf. Advances in Cryptology (CRYPTO), pp. 41-62,2001

[4] S. S. Hegde, BhaskarRao, "Cloud Security Using Visual Cryptography", International Journal of Distributed and Parallel Systems (IJDPS) Vol.3, No.1, January2012,pp.9-13.

[5] MoniNaor and Adi Shamir, "Visual cryptography". In Proceedings of the advances in cryptology-Eurocrypt,1-12,1995

[6] D. Boneh, B. Lynn, and H. Shacham, "Short Signature from the Weil Pairing," Proc. Int'l Conf. Theory and Application of Cryptology and Information Security: Advances in Cryptology, pp. 514-532,2001.

[7] Kai-Hui Lee and Pei-Ling Chiu, "Digital Image Sharing by Diverse Image Media", IEEE Transactions on Information Forensics and Security, vol. 9, No. 1, February2014.

[8] GhoutiL, BouridaneA and Ibrahim MK, "Digital image watermarking using balanced multiwavelets" , IEEE Transactions on Signal Processing, 54(4), pp. 1519-1536,2006

[9] Rodrigo N. Calheiros, Rajiv Ranjan, César A. F. De Rose &RajkumarBuyya, ―CloudSim: A Novel Framework for Modeling and Simulation of Cloud Computing Infrastructures andServices‖.

[10] A. Boldyreva, V. Goyal& V. Kumar, (2008)―Identity-Based Encryption with Efficient Revocation‖, Proc. 15th ACM Conf. Computer and Comm. Security(CCS).

