ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 10, October 2015

Double Watermarking Based Media File Sharing on Mobile Media Cloud

Madhura Jagdale[1], S.H. Patil[2]

M. Tech Student, Dept. of Computer, Bharati Vidyapeeth Deemed University College of Engineering Pune, India[1]

Professor, Dept. of Computer, Bharati Vidyapeeth Deemed University College of Engineering Pune, India[2]

ABSTRACT: Cloud is a web based services hosted on Internet. It is nothing but anything as a Service (AaaS). Cloud has evolved majorly as a Data Storage Service. Due to outsourcing of the maintainability to third party, the data management cost has reduced drastically. The major challenge to the cloud service provider's face is guaranteeing the data security. Explosive volume of data is being shared via mobile or other hand held device. Due to such data demand the cloud computing has become the choice of many service providers because of its scalability and on demand self-service and other features. But security issue still persists in mobile cloud computing as well. Researchers all around the world has proposed many approaches to answer the security concerns of the users [1]. Our approach of Share based secured multimedia file sharing on Mobile cloud is one more step ahead to enhance the secured media file sharing experience of the users, where secret sharing based double watermarking technique is applied to make media file sharing more secured.

KEYWORDS: Mobile Cloud, Watermarking, Secret Sharing, Security

I. INTRODUCTION

Recent improvements in mobile devices and network technologies have change the way we use computers and access networks [1]. Cloud Computing is a new class of network based computing that takes place over the Internet. Mobile Computing is also new technology which allows transmission of data, voice and video via a computer or any other wireless enabled device without having to be connected to a fixed physical link.

In Mobile or hand held devices the cloud storage has major potential to gain popularity because of limited in device storage capacity. A mobile cloud service has following characteristics that distinguish it from traditional computing environment:

i) On-demand self-service [2]
ii) Rapid elasticity- Ability to quickly scale in/out service [6]
iii) The service is fully managed by the provider.

Since the data is stored remotely; the data owner is unaware of where the data is located and how many copies are created. The threats of illegal copying, tampering, forgery, plagiarism, falsification, and other forms of possible disruptions need to be specifically addressed so that the users trust can be gained and the user can have a fear free environment to store or share its contents.

In past many approaches has been proposed by researchers which are mainly focused on digital media modification based on watermarking etc. But none have been able to claim a fool proof mechanism to provide digital media security.

In this paper we have demonstrated how the combination of Watermarking and secret sharing can enhance the security of the Mobile media sharing on Cloud and make it almost impossible for illegitimate users to access or use the digital data shared by mobile user on cloud.

II. RELATED WORK

In [1] the author has described both secure sharing and watermarking schemes to protect user's data in the media cloud. The secure sharing scheme allows users to upload multiple data pieces to different clouds, making it impossible to derive the whole information from any one cloud. In addition, the proposed scalable watermarking algorithm can be

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 10, October 2015

used for authentications between personal mobile users and the media cloud. Also a new solution to resist multimedia transmission errors through a joint design of watermarking and Reed- Solomon codes is introduced.The paper [2] contains discussion of several challenges of media cloud. Those include Integration, Storage, Processing and Delivery. It says numerous media applications, services and devices have introduced and clients are consuming more and more media. It says Media processing requires great capacity and capability. As per the paper Cloud computing has proven a best technology for providing various services, great computing power, massive storage and bandwidth with modest cost. Integration of Media and Cloud can become very beneficial for both and hence becomes media cloud. In [3] a Visual Cryptographic Scheme for colour images where the divided shares are enveloped in other images using invisible digital watermarking is discussed. The shares are generated using Random Number. This paper says Simple visual cryptography is insecure because of the decryption process done by human visual system. The secret information can be retrieved by anyone if the person gets at least k number of shares.

III. CLOUD STORAGE RISKS AND ISSUES

There are numerous security issuesfor cloud computing as it combines manytechnologies like networks, databases, operating systems, virtualization, resource scheduling, transaction management, load balancing, concurrencycontrol and memory management, etc. Therefore,security issues for many of these systems and technologies are applicable to cloud computing.Security has been the primary concern for the cloud users mainly due to two reasons:

1. Lack of data transparency
2. Dependency on the Cloud Computing provider

These two issues can lead to a number of legal and security concerns. Some of the risk due to lack of data transparency are customer's unawareness on how, when, why and where their data is processed. This is in opposition to the data security requirement that customers knowledge of what happens with their data [2].

Mostly cloud service providers are similar to traditional service providers. Dependency on the cloud computing provider problem is also known as 'vendor lock in' problem. It is difficult to change the cloud service provider once you have registered and sometimes impossible, because you have to migrate huge data from the old provider to the new one [2].

IV. PROPOSED SYSTEM

In the discussed system we have demonstrated a secret sharing based double watermarking technique to enhance the privacy preserved and secured mobile media cloud storage and sharing.

Our approach consists of three steps for secured media file sharing on cloud:

1. User Authentication Code watermarking
2. Share Generation
3. Watermarking of the shares

As shown in System Architecture (Figure 1), a mobile based application where the user A has to provide an authentication code. This authentication code is blind watermarked using LSB in Spatial Domain Image Watermarking algorithm in the Image media file I to be shared. Then using the Shamir's secret sharing algorithm the Media file I is divided into multiple shares n as (S1, S2…. Sn) [8].These individual shares are then further being blind watermarked into the Carrier Images (C1, C2…Cn). These Carrier images are then stored in the distributed Mobile Cloud storage environment.While retrieving the image the user fetches only the t Carrier Images (C_1, C2…C_t) from the Mobile Cloud storage and using De watermarking the t shares (S_1, S_2, S_t) are retrieved. The by applying the reverse Shamir's secret sharing algorithm the Original Image I is reconstructed [8]. De watermarking technique is then used to retrieve the hidden authentication code and matched with the downloader provided authentication code. When match found then only the image is displayed.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 10, October 2015

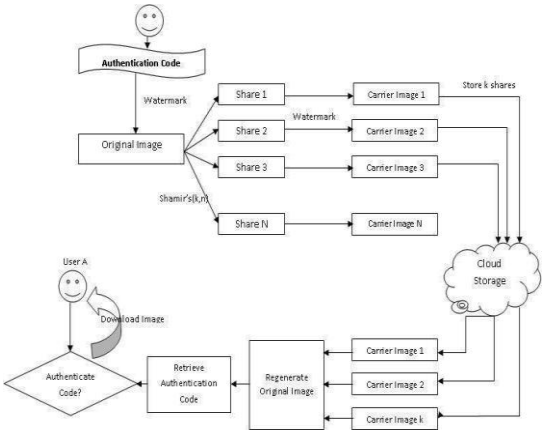


Figure 1: System Architecture

V. METHODOLOGY

The system of Secured Mobile media cloud storage will allow user to upload image file to cloud storage and then download the image from cloud storage. For the purpose the approach used is double watermarking based image file sharing.

The upload process comprises of below steps:

1. Browse Image: User Input
2. Input Authentication Code: User Input
3. Text to Image Invisible watermark
4. Secret Share Generation from the Watermarked image
5. Share Image watermark on carrier images
6. Upload Carrier Images to Cloud Storage

The download process comprise of below steps:

1. Download Carrier Images from the Cloud storage
2. Extract the shares from Carrier Images
3. Regenerate the Image from the shares
4. Remove the invisible watermarked text
5. Input the Authentication Code: User Input
6. Compare the User authentication Code and Image Authentication Code
7. On Code match success, display the Image

VI. ALGORITHM

A. *Modified LSB in Spatial Domain Image Watermarking:*

Modified LSB in Spatial Domain Image Watermarking is presented as example invisible image watermarking technique [10]. As modification, the experimentation is done to hide embed data in blue component with bit position 1 to bit position 5 separately. We can hide binary data in bit position 1 of blue component of pixel as follows:

Let binary values of an image pixel are:

10100111 11101001 11001000 10100111

11001000 11101001 11001000 00100111

We will hide a binary value say 10010011 by changing only the LSB of the above mentioned image pixel value. The result will be as following:

10100111 11101000 11001000 10100111

11001000 11101000 11001001 00100111

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 10, October 2015

LSB Invisible Watermark

Input: Cover Image, binary: Input String
Output: Watermarked image

1: Read Cover_Image
2: Grab pixels of Cover_Image into grabber.
3: Formulate Input String using 4 to 7
4:StringBuilder binary = new StringBuilder();
5: for x = 10 to 40
6: StringBuilder b = binary.append(Integer.toBinaryString(x));
7: end for
8: Display 'binary' as string to be embedded.
9: intpixels [] =new int[width*height]
where w and h are width and height of Cover_Image
10: Cover_pixel = (int[]) grabber.getPixels();
11: for i=0 to Cover_pixel.length
12: int c= Cover_pixel[i];
13: int r= (c&0xff0000)>>16;
14: int g= (c&0x00ff00)>>8;
15: int b= (c&0x0000ff);
16: if (i <watermark_string_length)
17: if (binary.charAt (i) == '0')
18: b = b & 254;
19: Else
20: b = b | 1;
21: pixels[i] = ((255<<24) || ((r&0xff) <<16) || ((g&0xff) <<8) || (b&0xff));
22: end if
23: Else
24: pixels[i] = ((255<<24) || ((r&0xff) <<16) || ((g&0xff) <<8) || (b&0xff));
25: end for
26: Create Watermarked_image using pixel

LSB Watermark Extraction

Input: Watermarked_image
Output: sb: Output Extracted String

1: Read Watermarked_image formed in embedding
2: Grab pixels of Watermarked_image in grabber1
3:intpixels1 [] =new int[width*height];
Where w and h are width and heights of Watermarked_image
4: for i=0 to watermark_string_length-1
5: int c= watermarkedArray[i];
6: int r1= (c&0xff0000)>>16;
7: int g1= (c&0x00ff00)>>8;
8: int b1= (c&0x0000ff);
9: String binString =Integer.toBinaryString(b1);
10: Char s=binString.charAt((binString.length()-1));
11:sb.append(s);
12: end for
13:Display 'sb' as Output Extracted String

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 10, October 2015

B. *Secret Share Generation:*

Secret Share Generation

Input: In this process consider secret 'I' as an image, and 'n' number of participants such as threshold t ⩽ n.
Output: The output is 'n' shares in the form of an integer for the n participants.

1. In this step the Image is read and converted in to bytes. These bytes are the converted into array of Integers
2. In this step consider a random prime number 'p', which is larger than 'c'.
3. Choose t-1 integer values m1, m2... mt-1 between 0 to p-1
4. Choose n distinct real values y1, y2 … yn
5. By using the following (t-1) degree polynomial equation we can compute n function values *f(yj)*, known as partial shares, for j=1, 2.....n

f(yi)=(c+m1y1i+m2y2i+….+mt-1 yt-1t-1) mod p

6. Then transfer the two tuple *(yj,f(yj))* as a share to the jth participant where j=1, 2, 3.....n.

Therefore there is t number of coefficients denoted by c and m1through mt−1. Finally to form t equation to recover secret c, collect t shares from the n participants.

Secret Recovery of Shares

Input: Share Holding Carrier Image
Output: Original Image

1. Shares are extracted from the Carrier Images
2. Shares in byte form are converted into Integers
3. In this step the t shares are used as

(y1, f (y1))(y2, f (y2))….. (yt, f(yt) to set up*f(yi)=(c+m1y1i+m2y2i+….+mt-1 yt-1t-1) mod p*

4. By using Lagrange's interpolation equation solve the above equations.
   C= (-1)$^{k-1}$

$$\left[f(y1)\frac{y2y3y4.....yk}{((y1-y2)(y1-y3).....(y1-yk))}\right] + \left[f(y1)\frac{y2y3y4.....yk}{((y1-y2)(y1-y3).....(y1-yk))}\right] +.....+$$

$$\left[f(yk)\frac{(y1y2y3.....yk)}{((yk-y1)(yk-y2).....(yk-yk-1))}\right] mod\ p$$

5. Then following equality and comparing the result with equation in step 5 of Secret Share Generation find out the m1through mt-1while regarding variable y in the equality below to be yj in

$$f(y) = \left[f(y1)\frac{(y-y2)(y-y3)..(y-yt)}{(y1-y2)(y1-y3)...(y1-yt)}\right] + \left[f(y2)\frac{(y-y1)(y-y3)....(y-yt)}{(y2-y1)(y2-y3)...(y2-yt)}\right] +...+$$

$$\left[f(y)\frac{(y-y1)(y-y3)...(y-yt-1)}{(yt-y1)(yt-y3)...(yt-yt-1)}\right] mod\ p$$

VII. EXPERIMENTAL RESULT

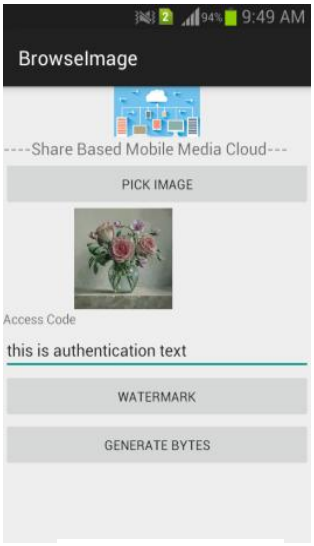
The first screen **(Screen 1)** displays the original image and user input authentication code. The second screen **(Screen 2)** shows the water marked image. Though our algorithm is capable of invisible watermarking, to demonstrate the watermarking we have kept the visibility to 10%.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

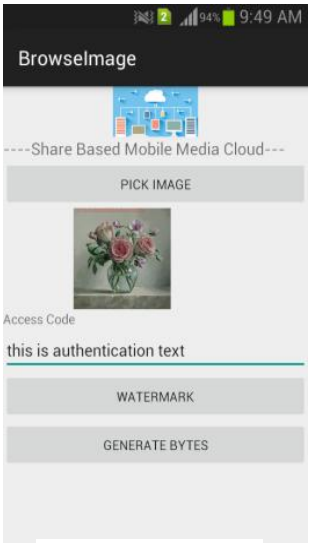
International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 10, October 2015

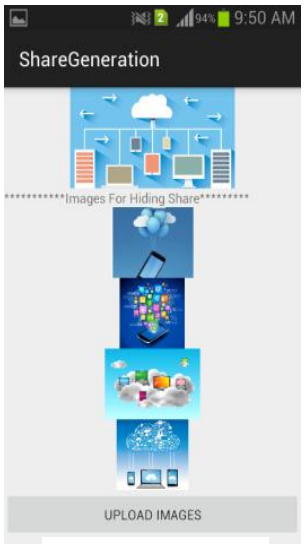


Screen 1

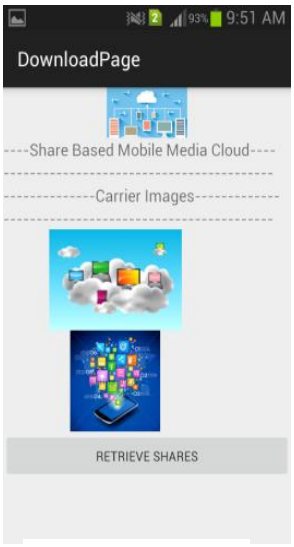


Screen 2

Once the image has been watermarked then On Click of the Generate Bytes Button on **Screen 2** the Shamir's Secret Sharing Algorithm comes into picture and shares are generated and hidden into carrier images, for demonstration purpose we have kept N=4 and K=2, i.e. 4 shares will begenerated and out of them 2 will be required for original image retrieval.



Screen 3



Screen 4

The **Screen 3** displays the carrier images which has stored the image shares created by the Shamir's K algorithm and on click of the Upload Images button the carrier images will be stored on the Cloud Storage Space, which in our case in Google Drive**. Screen 4** shows the download process where two carrier images got downloaded and original image is retrieved for them.But the original image retrieval does not happen until the authentication code entered by user downloading image does not match the authentication code watermarked in original image.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 10, October 2015

VIII. CONCLUSION

To demonstrate our approach we have used the Google Drive as the Cloud Storage Service provider. The security aspect for the image shared is evident from the fact that we have restrained ourselves from storing the original image itself on Cloud storage in any form, instead we are storing the carrier images on Cloud and that also the original image is converted into multiple shares hidden into multiple carrier images. The Shamir's secret shares further makes the retrieval of the image impossible and the authentication code is with the user only thus it makes the media file security breach nearly impossible

REFERENCES

1. Honggang Wang, Min Chen Wang, Wei Wang , " Security protection between users and the mobile media cloud"- Communications Magazine, IEEE (Volume:52 , Issue: 3) , Pages 73-79, 2014
2. Ms. LajjaVyas, Ms. ShrutiRaval, Ms. RichaSinha, "A Survey on Challenges to the Media Cloud"-Computer Engineering and Intelligent Systems ISSN 2222-1719 (Paper) ISSN 2222-2863 (Online) Vol.5, No.5, pages 9-12, 2014
3. ShyamalenduKandar, ArnabMaiti, Bibhas Chandra Dhara, "Visual Cryptography Scheme for Color Image Using Random Number with Enveloping by Digital Watermarking"-IJCSI International Journal of Computer Science Issues, Vol. 8, Pages 534-549, 2011
4. "Cloud computing implementation, management & Security" by John W. Rittinghouse& James F. Ransome,
5. Fernandes, D. A., Soares, L. F., Gomes, J. V., Freire, M. M., &Inácio, P. R. Security issues in cloud environments: a survey. International Journal of Information Security, 13(2), 113-170, 2014.
6. Nikolas Roman Herbst, Samuel Kounev, Ralf Reussner ,"Elasticity in Cloud Computing: What It Is, and What It Is Not"
7. Frank Hartung, Martin Kutter, "Multimedia Watermarking Techniques", Proceeding of the IEEE, VOL. 87, No. 7, July 1999
8. MoniNaor, Adi Shamir "Visual Cryptography" Springer-Verlag, 1998

BIOGRAPHY

MadhuraSampatraoJagdale is an MTech Student in the Computer Department, Bharati Vidyapeeth University College of Engineering Pune, India. She received Bachelor of Engineering (BE) degree in 2012 from ADCET, Ashta, India. Her research interests are Could Computing Security.