ISSN: 2321-7782 (Online)

Volume 3, Issue 1, January 2015

International Journal of Advance Research in Computer Science and Management Studies

Research Article / Survey Paper / Case Study

Available online at: www.ijarcsms.com

A Strong Security and Authentication Approach between End-Users and Mobile Media Cloud

Shifa Panhalkar[1]
Department of Computer Engineering
Anantrao Pawar College of Engineering and Research
Pune, India

Tanuja Singh[2]
Assistant Professor, Department of Computer Engineering
Anantrao Pawar College of Engineering and Research
Pune, India

Abstract: Multimedia on phones is the fast growing sector and almost every mobile user would have an apparent need for a Multimedia based Application. As mobile device have limited supply and media processing some task must be moved to the media cloud for further processing. Cloud is becoming more accepted as it's an important resource in a cost-effective way. Due to its increasing demand threat of its security is becoming a major issue. Media security and privacy protection are the two key factors of user's concerns about the cloud technology. Security in the multimedia cloud has become a most important factor for data storage and is able to control over wireless network. There are many challenges to protect user data in media cloud, for example, traditional security method which does not make sure complete security for uploading and downloading images and videos from media is larger in size than the processing media data of cell phones. Therefore security method design must be lightweight. Considering these challenges, a new approach for mobile media security has been introduced in this paper.

Keywords: MMC (Mobile Media Cloud), DFR (Digital Foundation Raptor), Watermark Technique, DWT (Discrete wavelets transform), Multimedia Application, Digital Watermark, Security.

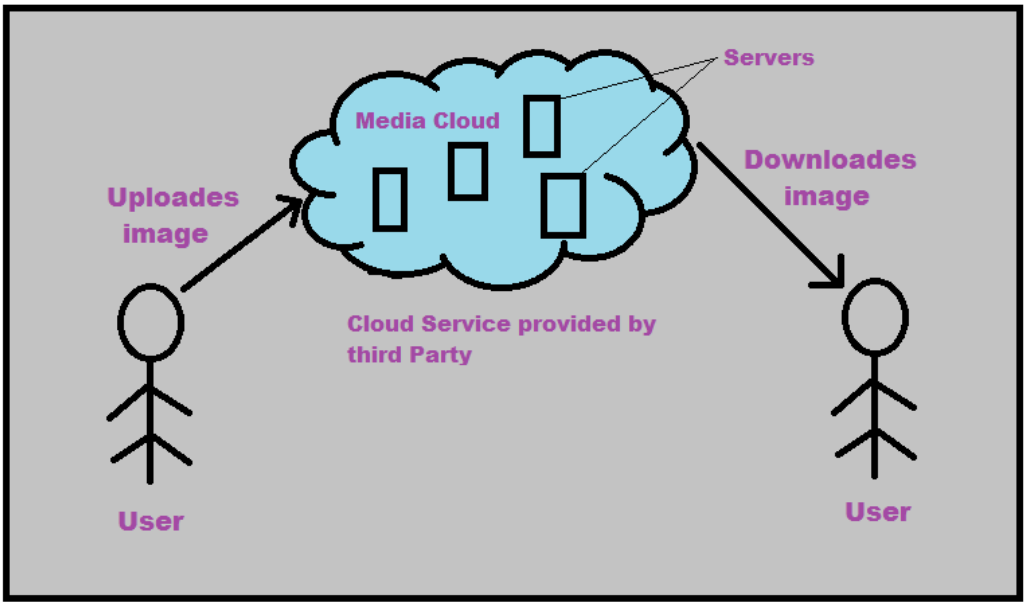
I. INTRODUCTION

Electronic devices such as Tablets, Phablets, Smartphones, PDAs, etc have essentially become part of our life as they are small enough to be handheld commonly known as Handheld Computer. Some of the leading Manufactures that produces these types of devices are as:

a) SAMSUNG
b) SONY
c) APPLE
d) HTC
e) MOTOROLA MOBILITY and many more.

All the above manufactures mostly use different operating system Android, Apple iOS, Blackberry OS, Windows OS, etc. Mobile Devices has become popular to consume Different web resources specially Web Services. The use of Tablets, Smartphones and many other mobile devices contributes of sharing Mobile Media on different Social Networking sites like Facebook Twitter, Orkut, YouTube, etc. Different Multimedia content can easily be send to the cloud system through internet. And due to the open Environment of the Internet, it introduces many Challenging Problems regarding Security and illegal distribution of privately owned image. Multimedia security has become most important and major concern for cloud data access. As data access over an wireless network has increased popularity due to fast growth of different multimedia applications.

Cloud computing and different web services run on a network Structure so they r open to network type attack. Consider an example if a user upload an media from his mobile device to MMC (i.e Mobile Media Cloud) then after that the same user wants to download the uploaded image from the mobile media cloud, can that user trust on cloud service whether the downloaded image is same as that of the uploaded image and the media is not been edited. As the cloud services are been provided by the third parties the user cannot trust on the cloud services (As shown in the figure).



II. Related Work

There many traditional approaches introduced for the media security in the MMC (Mobile Media Cloud) such as Secure Sharing, Different Watermark Technique, Crossbreed Algorithm, RSA Algorithm. In this paper we are going to use Watermark Algorithm. There are many traditional Watermark algorithms, which may not detect the watermark because of the images scaling and compression to a smaller scale. As the Traditional Watermark is not detectable the challenge to how to verify whether the downloaded image is edited or it is the original image. Here we use the scalable Authentication approach using Watermark Technique introduced in [1] with the DF RAPTOR code. And when the user wants to download the image the Watermark of the image should be invisible and limited information should be visible the User.

The Security Protection Between Users and the MMC(Mobile Media Cloud) proposed by Hongganv Wang Shaoen Wu, Wei Wang and Min chen, paper they used watermark algorithm and Reed-Solomon(RS) codes Together for verifying the media's watermark bits whether they are original media or edited media in MMC(Mobile Media Cloud). But there are many disadvantages of Reed-Solomon error correction code. Therefore DF Raptor error correction code is used in the place of Reed-Solomon code.

III. DWT based Watermark Technology

Discrete wavelets transform (DWT) is the process of transforming the image into its transform domain. It decomposes the input image into mainly four different components; they are HL, LL, HH, LH. The first letter of the components is used for applying either a low pass frequency operation or high pass frequency operation and the second letter refers to the filter applied to the columns, as shown in the figure2.

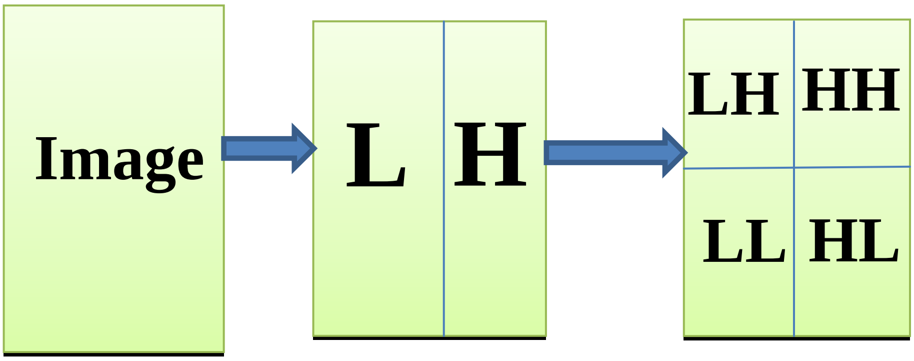


Figure 2: DWT

LL lowest resolution level consist of a part of the original image and the remaining three levels consist of the detail parts and the give the vertical high (LH), horizontal high(HH), and high (HH) frequencies.

IV. Advantage of DF Raptor error correction code over the Reed-Solomon error correction code

1) Reed-Solomon code is Block-Based error correcting code whereas DF Raptor are Block and Pixel based error correcting code.

2) Reed-Solomon Code takes a block of data and adds extra redundant bits whereas no redundant bits are added in DF Raptor code.

3) Disadvantage of Reed-Solomon code is that it is inefficient and there are limitations in Packet-level erasure code whereas DF Raptor codes are more efficient, and use Non-Block base coding.

4) DF Raptor code has multiple decoding paths whereas Reed-Solomon code does not have multiple decoding path.

5) When more then one Reed-Solomon code is used and interleaved the performance can deteriorate because of randomly distributed nature of packet loss as this doesn't happens in DF Raptor code.

6) Interleaving overhead is a key reason why RS codes reveal inferior performance in many applications.

7) Raptor codes provide flexibility, while Reed Solomon codes are subjected to constraints that limit their utility and diminish their relative performance.

8) Raptor codes require less processing power than Reed Solomon codes.

V. Proposed Work Joint Design of DF Raptor Error Correction code and Watermark Technique

There are many error correction methods used, DF Raptor is a powerful error

Correction code which provides flexibility and requires less processing power than any other error correction code. DF Raptor uses Block based or pixel based error correction code. Therefore it can be combined with Watermark algorithm. In this Random selection and combination of data is done. Error correction and erasure capacity is depend on selection probability distribution. It is based on random distribution and probability decoding. It is a systematic or non-systematic approach. And as it is pixel based, error correction can be done easily. The motive behind this approach is to detect the watermark data. DF Raptor plays a very important role in extracting the watermark bits from the image as that of its ability of correcting errors.

In this joint design of DF Raptor error correction code and Watermark Technique, Firstly, the image which is watermarked will be given as an input to the DF Raptor error correction encoder. Secondly, the LH3 band is given as a input to the DF Raptor encoder.

As the process of detecting and correcting errors, then we will replace LH3 band obtained from the DF Raptor code in the original image and then we will apply the DWT to reconstruct the image. In this joint design of the watermark technique and DF Raptor code if noise is caused then the packets are discarded as they cannot be corrected due to the bit error.

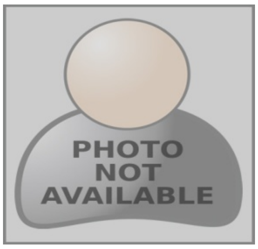
VI. Conclusion

A Strong security and authentication approach between end-users and MMC (Mobile Media Cloud) is an important and critical topic for the different multimedia applications. In this paper a joint design of DF Raptor and Watermark Technique has been introduced for multimedia protection in MMC (Mobile Media cloud). As DF Raptor code are pixel based and more flexible than any other error correction code, it guaranties for securing the data. The study of the joint design that is been proposed in this paper can effectively improve the security of the media in MMC (Mobile Media Cloud).

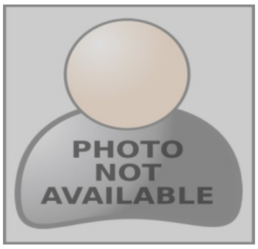
References

1. H. Wang et al.,"Security Protection between users and the mobile media Cloud," IEEE Trans. March 2014.
2. C. F. Wu and W. S. Hsieh, "Image Refining Technique Using Digital Watermarking," IEEE Trans. Consumer Electronics, vol. 46, no. 1, Feb. 2000, pp. 1–5.
3. K. Lu, Y. Qian, and H.-H. Chen, "A Secure and Service-Oriented Network Control Framework for WiMAX Networks,"IEEE Commun.Mag., vol. 45, no. 5, May 2007,pp. 124–30.
4. Priyanka Gupta and Amandeep kaur brar, "An Enhanced security Technique for storage of multimedia content over cloud server,", International Journal of Engineering Research and Applications (IJERA) ISSN: 2248-9622, www.ijera.com Vol. 3, Issue 4, Jul-Aug 2013, pp.2273-2277.
5. Ashish Sharma, Vikas Gupta, "Crossbreed Algorithm to Enhance Security for Multimedia Content: An Overview" International Journal of Computer Science and Communication Engineering Volume 2 Issue 2 (May 2013 Issue).
6. R.MYTHILI et al., "RAPTOR CODE BASED SECURE STORAGE IN CLOUD COMPUTING", International Journal of Internet Computing ISSN No: 2231 – 6965, VOL- 1, ISS- 4 2012.
7. Ming-Shing Hsieh, Din-Chang Tseng, and Yong-Huai Huang, "Hiding Digital Watermarks Using Multiresolution Wavelet Transform", IEEE TRANSACTIONS ON INDUSTRIAL ELECTRONICS, VOL. 48, NO. 5, OCTOBER 2001
8. Sonal Guleria, Dr. Sonia Vatta, "TO ENHANCE MULTIMEDIA SECURITY IN CLOUD COMPUTING ENVIRONMENT USING CROSSBREED ALGORITHM", Web Site: www.ijaiem.org Volume 2, Issue 6, June 2013.
9. D. Sahu,et al, "Cloud Computing in Mobile Applications" , International Journal of Scientific and Research Publications, Volume 2, Issue 8, August 2012
10. Deyan Chen1 and Hong Zhao," Data Security and Privacy Protection Issues in Cloud Computing", 2012 International Conference on Computer Science and Electronics Engineering

Author(s) Profile



Shifa Panhalkar, studying the B.E degree in Computer from Anantrao Pawar college of engineering pune india, respectively.



Tanuja Singh, Assistant Professor, Department of Computer Engineering Anantrao Pawar College of Engineering and Research, Pune, India.