ISSN: 2321-7782 (Online)

Volume 2, Issue 12, December 2014

International Journal of Advance Research in Computer Science and Management Studies

Research Article / Survey Paper / Case Study

Available online at: www.ijarcsms.com

Cloud Data Security for Mobile Users

Sujit Laxman Thorat[1]
Department of Computer Engineering
G. S. Moze College of Engineering
Savitribai Phule Pune University
Pune – India

Pradnya Velhal[2]
Department of Computer Engineering
G. S. Moze College of Engineering
Savitribai Phule Pune University
Pune – India

Abstract: Digital watermarking is a technology being developed to ensure and facilitate data authentication, security and copyright protection of digital media. We have studied about watermarking technique for authentication of cloud users. We propose to use both secure sharing and watermarking schemes to protect users' 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 used for authentications between personal mobile users and the media cloud. This paper provides the literature survey about what is done regarding Watermark authentication, Secret sharing of data in multiple clouds, Reed Solomon Code for transmission errors in digital watermark.

Keywords: Watermarking, Wavelet, Threshold, Cryptography, Media.

I. INTRODUCTION

This survey paper describes about security techniques for data in cloud. Firstly, we study about Digital Watermarking authentication which acts as main security for data access. Secondly, we study about Secret Data Sharing using shamir's (r,n) threshold scheme. Thirdly, we study about Reed Solomon code for correcting transmission errors in watermark. We have also given future scope and work of securities of data in cloud.

It is reasonable that a cloud system can provide security access control. However, the cloud itself may not be trusted since it is managed by third parties such as cloud service providers. The security can only be guaranteed by contracts between users and cloud service providers. There are some potential risks, such as security attacks or misconduct of the cloud manager. Strictly speaking, users should only trust themselves rather than cloud security services. A further question is, can users have other approaches to protect their media data from the media cloud? In this article, we propose to utilize secret sharing and watermarking to address the challenges. Our design is user-oriented, and allows users to protect their data's security and privacy. First, we focus our studies on media authentication. It is well known that some steaming level authentication methods such as media authentication code (MAC) or content level approaches such as watermarking can be used to authenticate media data over wireless networks.

However, MAC approaches generate high overhead due to adding hash values to each media packet. Content-level authentication approaches such as watermarking consider the characteristics of media data and thus can be used to authenticate media with lower overheads. However, both traditional streamingbased authentication and content level approaches fail to deal with the authentication of scaled multimedia over wireless networks. As shown in Fig. 1, user A uploads a large high-resolution image at home using WiFi to the media cloud for storage. When the user moves to a bus stop, he/she might want to download the image at lower resolution due to limited bandwidth and battery resource. In the scenario, it is worth noting that the user needs to guarantee the media integrity by themselves. If we use traditional watermarking algorithms, the watermark may not be detectable due to the image's compression and scaling to a smaller size. Therefore, a key issue is how to verify that the downloaded multimedia is not modified in the cloud. Traditional packet level authentication approaches are not feasible to deal with this problem. In this article, we propose a scalable authentication approach using watermarking, which could be scalable and adapted to the size of a scaled image from the media cloud. Another research challenge in the article is the reduction of wireless transmission errors, which could corrupt the embedded watermark and fail the process of watermark detections.

II. Watermarking Technology

Digital watermarking hides the copyright information into the digital data through certain algorithm. The secret information to be embedded can be some text, author‘s serial number, company logo, images with some special importance. This secret information is embedded to the digital data (images, audio, and video) to ensure the security, data authentication, identification of owner and copyright protection. The watermark can be hidden in the digital data either visibly or invisibly. For a strong watermark embedding, a good watermarking technique is needed to be applied. Watermark can be embedded either in spatial or frequency domain. Both the domains are different and have their own pros and cons and are used in different scenario.

A. Requirement of Watermark Technology

There are a number of important characteristics that a watermark can exhibit, Jalil and Mirza (2010), Bandyopadhyay and Paul (2010). The most important properties of digital watermarking techniques are transparency, robustness, security, capacity, invert ability (reversibility) and complexity and possibility of verification. Transparency relates to the properties of the human sensory. A transparent watermark causes no artifacts or quality loss.

1) *Robustness:* Robustness means Resistance to blind□, non-targeted modifications, or common media operations. For example the Stirmark or Mosaik tools attack the robustness of watermarking algorithms with geometrical distortions. For manipulation recognition the watermark has to be fragile to detect altered media. There are two major problems when trying to guaranty robustness; the watermark must be still present in the media after the transformation or it must be still possible for the watermark detector to detect it.

2) *Security:* Security describes whether the embedded watermarking information cannot be removed beyond reliable detection by targeted attacks based on a full knowledge of the embedding algorithm and the detector, except the key, and the knowledge of at least one watermarked data. Watermarking security implies that the watermark should be difficult to remove or alter without damaging the host signal. As all watermarking systems seek to protect watermark information, without loss of generality, watermarking security can be regarded as the ability to assure secrecy and integrity of the watermark information, and resist malicious attacks.

3) *Capacity:* The watermark should not be noticeable to the viewer nor should the watermark degrade the quality of the content. The term ―imperceptible□ is widely used in this case. However, if a signal is truly imperceptible, then perceptually based lossy compression algorithms either introduce further modifications that jointly exceed the visibility threshold or remove such a signal, Gonzalez and Woods (2008). It is then important to develop techniques that can be used to add imperceptible or unnoticeable watermark signals in perceptually significant regions to counter the effects of signal processing.

B. DWT Watermarking Technique

Wavelet Transform is a modern technique frequently used in digital image processing, compression, watermarking etc. The transforms are based on small waves, called wavelet, of varying frequency and limited duration. The wavelet transform decomposes the image into three spatial directions, i.e. horizontal, vertical and diagonal. Hence wavelets reflect the anisotropic properties of HVS more precisely. Magnitude of DWT coefficients is larger in the lowest bands (LL) at each level of decomposition and is smaller for other bands (HH, LH, and HL). The Discrete Wavelet Transform (DWT) is currently used in a wide variety of signal processing applications, such as in audio and video compression, removal of noise in audio, and the simulation of wireless antenna distribution. Wavelets have their energy concentrated in time and are well suited for the analysis of transient, time-varying signals. Since most of the real life signals encountered are time varying in nature, the Wavelet Transform suits many applications very well. One of the main challenges of the watermarking problem is to achieve a better tradeoff between robustness and perceptivity. Robustness can be achieved by increasing the strength of the embedded watermark, but the visible distortion would be increased as well. However, DWT is much preferred because it provides both a simultaneous spatial localization and a frequency spread of the watermark within the host image. The basic idea of discrete wavelet transform in image process is to multi-differentiated decompose the image into sub-image of different spatial domain and independent frequencies.

III. Secret Data Sharing

We use a low-complexity DCT-JPEG-based compression algorithm for mobile media cloud so that the transmission load can be effectively reduced. In the JPEG standard, each tile (i.e., every 8 × 8 pixel block) is converted to frequency space using a two-dimensional forward discrete cosine transform. Our secret sharing method is inspired by the (r, n) threshold scheme proposed by Shamir et *al.* Specifically, we divide secret data D into n shadows (D1,…, D*on*), and the goal is that secret data D cannot be revealed without any r shadows. To split D into *n.* In a secret image sharing scenario based on Shamir's (r, n) threshold scheme, a_0 is taken as the gray value of the first pixel, and then the corresponding output $f(1) – f(n)$ is obtained. After that, a_0 is replaced by the gray value of the second pixel, and the process repeats until all pixels of the secret image are processed. However, in our proposed scheme, the size of each shadow image is 1/r of the secret image.

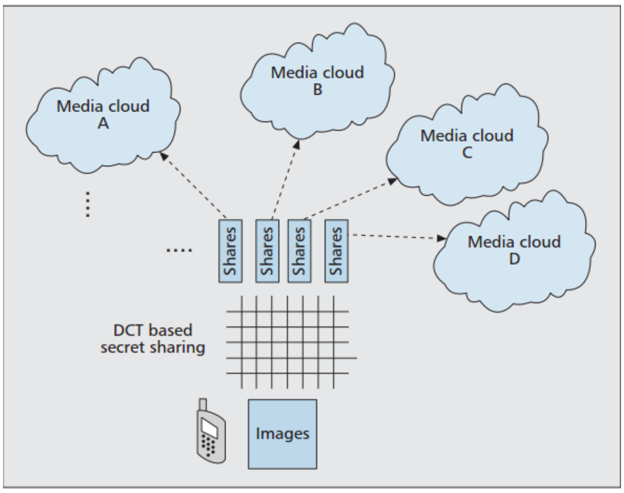

Fig. 1 Secret Sharing of Data

The essential idea is to use a polynomial function of order (r – 1) to construct n image shares from a DCT-based transformation matrix with $l \times l$ pixels of the secret image being transformed; $S\_dct(i, j)$ denotes the coefficient value at the (i, j) position after the original secret image is transformed by DCT function. $f_{x\_dct}(i, j)$ denotes the coefficient value of shadow image shares. This method reduces the size of image shares to become 1/r of the size of the secret image. Note that any r image shares can be used to reconstruct every pixel value in the secret image. As shown in Fig. 4, the image is separated into multiple shares, which are uploaded to different media clouds. Thus, any one of the clouds cannot disclose the whole information. The user only downloads a certain number of shares from multiple clouds and can recover all of the information.

IV. Reed Solomon Code

We have surveyed approach on different types of images. We define the noise density at different levels, which indicates the percentage of noise that has been added into the images. We tested our watermarking solutions and compare the peak signal-to-noise ratio (PSNR) of the extracted watermark and its normalized correlation. Our studies show that with the increased noise level, the PSNR of the extracted watermark is gradually decreased. However, with RS code, the extracted watermark quality and correlation are tolerable. Figure 5 represents the normalized correlation (NC) values of the watermark. In our studies, the

NC values are obtained when LH3 is an input to RS code. From our studies, it can be concluded that the computation time when LH3 band as input to RS code is less compared to the computation time when the full image is given as input to RS code. By using LH3 band in the extraction process, the scheme reduces computation time and also decreases transmission overheads. We compare the approaches with and without RS. The results indicate that with RS code, the extracted watermark has better correlation with the original watermark. We conclude that the joint design of watermark and RS code can achieve better authentication performance. Due to page limits, we only show some of the studies on our tests of both watermarking and secret sharing schemes.

V. Future Work

Security protections mentioned above are not sufficient for data security in cloud. As Watermark can be attacked by many attacks such as Interference attack, Removal attack, Image degradation attack, collusion attack etc. Image shares are not protected in cloud by above protection mechanisms. Also, more security mechanisms are needed for data security in cloud. So, we can use Visual Cryptography technique for images so that images can be encrypted in such a way that decryption becomes a mechanical opearation that does not require a computer. There is a simple algorithm for binary (black and white) visual cryptography that creates 2 encrypted images from an original unencrypted image. The algorithm is as follows: First create an image of random pixels the same size and shape as the original image. Next, create a second image the same size and shape as the first, but where a pixel of the original image is the same as the corresponding pixel in the first encrypted image, set the same pixel of the second encrypted image to the opposite color. Also, we can calculate Digital Signatures for each image share and they can be stored on central cloud server. These digital signatures can be used for verification of owners of image shares and it can be strong security mechanism. We can use encryption technique for each image share which can be optional for more security.

VI. Conclusion

Security protection between users and the mobile media cloud is critical for future multimedia applications. In this article, we present a joint design of watermarking technique based on the significant difference of wavelet quantization with the Reed-Solomon error correcting code. The watermarking technique authenticates multimedia data from the media cloud, and the Reed-Solomon code guarantees that data transmission is reliable for multimedia data between mobile users and the media cloud. In addition, we propose the use of secret sharing schemes to maintain users' data security and privacy. Our studies show that the proposed approach can effectively improve the security performance level between users and the media cloud. Our research opens a new vista in user-oriented security research for the media cloud.

Acknowledgement

With immense pleasure, I am presenting this seminar report on the "Cloud Data Security for Mobile Users" as a part of the curriculum of M.E. of Computer Engineering at G.S.Moze College of Engineering. It gives me proud privilege to be complete this survey work under the valuable guidance of Prof. Pradnya Velhal and I would like to extend my thanks to Prof. Ratnaraj Kumar sir (H.O.D of Computer Engineering). I am also be extremely grateful to the Principal for providing all facilities and help for smooth progress of the Journal work. I would also like to thank all the Staff Members of Computer Engineering Dept. Management, friends and my family members who have directly or indirectly guided and who helped me for the preparation of this Journal and gave me an unending support right from the stage the idea was conceived.

References

1. S. Dey, "Cloud Mobile Media: Opportunities, Challenges, and Directions," Proc. Int'l. Conf. Computing, Networking and Commun., 2012, pp. 929–33.
2. F. Sardis et al., "On the Investigation of Cloud-Based Mobile Media Environments with Service-Populating and QoS-Aware Mechanisms," IEEE Trans. Multimedia, vol. 15, no. 4, June 2013, pp. 769–77.
3. Y. Xu and S. Mao, "A Survey of Mobile Cloud Computing for Rich Media Applications," IEEE Wireless Commun., vol. 20, no. 3, June 2013.

4. S. Wang and S. Dey, “Adaptive Mobile Cloud Computing to Enable Rich Mobile Multimedia Applications,” IEEE Trans. Multimedia, vol. 15, no. 4, June 2013, pp. 870–83.

5. www.enggjournals.com/ijcse/doc/IJCSE10-02-02-11.pdf.

AUTHOR(S) PROFILE

Sujit Laxman Thorat, received the B.E degree in Computer Engineering from Pravara Rural Engineering College, Loni in Pune University.

In 2012, he completed Certified PG Diploma DAC Course from IACSD under CDAC ACTS and got certificate in Java, Oracle. .Net. Now, he is pursuing M.E. in Computer Engineering from G. S. Moze College of Engineering, Balewadi in Savitribai Phule Pune University.

Ms. Pradnya Velhal received B.E in Computer from Government College of Engineering, Karad in 2005. After graduation, Ms. Pradnya has completed M.Tech in IT Engineering from Government college. Now, she is associated with G.S.Moze college of Engineering as assistant professor in Computer Engineering Department with 9 Years of experience.