Advanced Science and Technology Letters
Vol.48 (CIA 2014), pp.103-107
http://dx.doi.org/10.14257/astl.2014.48.18

Watermark-based Provable Data Possession for Multimedia File in Cloud Storage

Yongjun Ren[1,2], Jiang Xu[1,2], Jin Wang[1,2], Liming Fang[3], Jeong-Uk Kim[4]

[1]Jiangsu Engineering Center of Network Monitoring，Nanjing University of Information Science & Technology, Nanjing 210044, China

[2]Computer and Software School, Nanjing University of Information Science & Technology, Nanjing 210044, China

[3]Computer and Software School, Nanjing University of Aeronautics and Astronautics, Nanjing 210044, China

[4] Department of Energy Grid, Sangmyung University, Seoul 110-743, Korea

Abstract. In cloud computing, data owners host their data on cloud servers and data consumers can access the data from cloud servers. Due to the data outsourcing, however, this new paradigm of data hosting service also introduces new security challenges, which requires an independent auditing service to check the data integrity in the cloud. However, the existing solutions are not specific to the multimedia data. Moreover copyright protection is not provided. In this paper, we define specially a provable data possession model for multimedia file, and present a framework based on digital watermarking for multimedia data storage audit service, in which we define the security features of audit service for multimedia data outsourcing and the corresponding properties of digital watermarking.

Keywords: Cloud computing, Data storage auditing, Provable data possession

1 Introduction

Cloud Computing has been envisioned as the next-generation architecture of IT enterprise. Storing the data in cloud environment becomes natural and also essential. Cloud is a large shared resource pool and the users move towards them with respect to their needs. It offers amenities for data storage, data access and other computational capabilities in a reliable manner. But, security becomes the major concern for all entities in cloud services. In order to solve the problem of data auditing service, many schemes are proposed under different systems and security models [1-13].

Existing solutions are not specific to multimedia data. Besides, copyright protection is not provided. In this paper, we present an efficient watermarking-based audit service for image outsourced storages. Our audit system uses self-embedding watermarking to provide image content audit and support authenticity and integrity for image content in cloud computing. In addition we also provide the ability of copyright protection for image by using self-embedded technology.

ISSN: 2287-1233 ASTL

2 Related Work

The message authentication code (MAC) is a kind of hash function which has been used for checking the data integrity for a long time. Some solutions using MAC for storage auditing service have been proposed. Based on the pre-computed MACs stored on the verifier, the protocols proposed by Lillibridge et al.[2] and Naor et al. [3]can detect any data loss or corruption with high probability. Shacham et al. [4] proposed a MAC-based batch verification for multiple data blocks. In 2007 Ateniese, et al [5] proposed a PDP model to solve the storage problems of files. They divided the file into blocks, and computed a homomorphic tag [6] for each block, completed the proof of the data integrity by sampling and verifying the correspondence of the tags and blocks randomly. A.Juels, et al [7] proposed a provable data recovery (POR) model. Instead of tagging file blocks, they inserted some sentinel blocks, and verified the integrity of the file by checking the correctness of sentinel blocks. For the sentinel blocks are one-time labels, the number of times that the file can do integrity verification is limited, related to the number of sentinel blocks. Havav Shacham and Brent Waters [4] proposed an improved POR model under the security model defined in [7], and had a very complete proof. They used tags similar to [5], and applied to public authentication. Kevin D. Bowers et al [8] and Yevgeniy Dodis et al [9] made some theory and application extensions based on [4][7]. Zheng and Xu also present a dynamic POR model in [10].PDP model proposed in [5] only applied to private authentication. It meant that only the person who has the private key can verify the integrity of the file. Ateniese improved PDP model to apply to public authentication in [11]. They replaced the homomorphic tags in [5] with homomorphic tags supported public authentication [12].

3 Self-Embedding Watermark-Based PDP

3.1 Watermark generation and embedding

Let the original image (Q) is $N \times N$. In cloud image owners make the following calculation to generate watermark for image auditing.

①.The original Q is divided into $n \times n$ sub-block without overlap. Each sub-block is recorded as OB_k, k is the serial number the sub-block, and $k = 1,2,\ldots,(N/n)^2$.

②.The least significant m bits of each pixel of OB_k are set into zero. And the new sub-block is recorded as OB_k'. The process can be marked as the equality.

$OB_k' = BitSet(OB_k, j, 0)$, $j = 1,2,\ldots,m$, $BitSet(.)$ is setting function.

③. Computing singular value decomposition (SVD) of OB_k' .The generated singular value is recorded as δ_k^i , i is the serial number of singular value, and $i = 1,2,\ldots,n$.

④. According to the following formula to compute the norm of singular value for OB_k', i.e. $Norm_k$.

$$Norm_k = \sqrt{\sum_{i=1}^{n} (\delta_k^i)^2} \quad (1)$$

⑤.Extraction the parity of the highest order for $Norm_k$ and produce original robust watermark W. If the parity of the highest order for $Norm_k$ is even, $W_k = 0$;otherwise $W_k = 1$,W_k is the k-th bit of W.

⑥.Embedding W_k to the least significant m bits of every pixel for OB_k' and getting sub-block OB_k'' with watermarking. OB_k'' is restructured and produce an image (Q') including watermark. The self-embedding process can be expressed as:

$$OB_k'' = BitGet\ (OB_k', j, W_k) \quad (2)$$

From the above mentioned we know that the length of W is $(N/n)^2$ bits, W_k is embedded to n^2 pixels and every pixel is embedded by m bits. So the total bit number of self-embedded W_k is mn^2 and the embedding capacity of the watermarking is mN^2 .Because W_k is embedded into the least significant m bits of every pixel for OB_k', which lead to mall change, the invisibility of watermark algorithm is very good. Moreover the watermarking W is generated by the characteristics of the original image and has the robustness against the attack, which is called *robust watermarking*.

After the above operation, MDO will be able to upload the image Q' with watermarking to CSP for cloud storage service.

3.2 Copyright protection of cloud image service from robust watermarking

Image auditor MDA download image Q' from cloud service provider. And then it extracts the robust watermarking to identify copyright of the image.

①. Image Q' is divided into $n \times n$ sub-block without overlap. Each sub-block is recorded as AB_k , k is the serial number the sub-block, and $k = 1,2,\ldots,(N/n)^2$.

②.The least significant *m* bits of each pixel in AB_k are set into zero. And the new sub-block is recorded as AB_k'. The process can be marked as the equality:

$AB_k' = BitSet(AB_k, j, 0)$, $j = 1, 2, \ldots, m$, $BitSet(.)$ is a setting function.

③.Computing singular value decomposition of AB_k'.The generated singular value is recorded as $\delta_k^{i\prime}$, *i* is the serial number of singular value, and $i = 1, 2, \ldots, n$.

④.Computing the norm of singular value for AB_k',i.e. $Norm_k'$.

$$Norm_k' = \sqrt{\sum_{i=1}^{n} (\delta_k^{i\prime})^2} \quad (3)$$

⑤.Extraction the parity of the highest order for $Norm_k'$ and produce robust watermark W'. If the parity of the highest order for $Norm_k'$ is even, $W' = 0$; otherwise $W' = 1$. W' is the *k*-th bit of W'.

⑥.Calculating and analyzing the NC identify copyright of W' and W

$$NC = \left(\sum_{k=1}^{(N/n)^2} (W_k \times W_k')\right) / \left(\sqrt{\sum_{k=1}^{(N/n)^2} W_k^2} \times \sqrt{\sum_{k=1}^{(N/n)^2} W_k'^2}\right) \quad (4)$$

3.3 Integrity and authenticity verification of image content

Image auditor download image Q' from cloud service provider and implement the following operation to verify the image content.

①. Image Q' is divided into $n \times n$ sub-block without overlap. Each sub-block is recorded as AB_k, *k* is the serial number the sub-block, and $k = 1, 2, \ldots, (N/n)^2$.

② .The least significant *m* bits of each pixel in AB_k are extracted, i.e. $L_k^j(r) = BitGet(AB_k, j)$;where $BitGet(.)$ is extraction potential function. $L_k^j(r)$ is the bit sequence of the minimum *j* bits for each pixel in the *k*-th sub-block. $j = 1, 2, \cdots, m$, and $r = 1, 2, \cdots, n^2$.

③. Contrasting the extracted robust watermark W' and $L_k^j(r)$. Image auditors verify the consistence between them. If any one bit for every *j* and *r* is not consistent, the sub-block content has been altered; otherwise the image Q' is intact.

4 Conclusions

In this paper, we present an efficient watermarking-based audit service for image outsourced storages. We integrate image content audit service and copyright protection through a double function self-embedded watermarking scheme, which greatly reduced the consumption of resources and is very suitable for multimedia data in cloud environment.

Acknowledgments. This work was supported by the Industrial Strategic Technology Development Program (10041740) funded by the Ministry of Trade, Industry and Energy (MOTIE) Korea. It was also supported by the Natural Science Foundation of Jiangsu Province (No. BK2012461). Prof. Jeong-Uk Kim is the corresponding author.

References

1. Yang, K., Jia, X.: Data storage auditing service in cloud computing: challenges, methods and opportunities. The journal of World Wide Web. July 2012, Volume 15, pp 409-428.
2. Lillibridge, M., Elnikety, S., Birrell, A., Burrows, M., Isard, M.: A cooperative internet backup
3. Naor, M., Rothblum, G.N.: The complexity of online memory checking. In: Proceedings of the 46th Annual IEEE Symposium on Foundations of Computer Science, FOCS ’05, pp. 573–584.
4. IEEE Computer Society, Washington, DC, USA (2005) H. Shacham and B. Waters. Compact proofs of retrievability. In ASIACRYPT '08, pp. 90-107, 2008.
5. G. Ateniese, R. Burns, R. Curtmola, J. Herring, L. Kissner, Z. Peterson, and D. Song. Provable data possession at untrusted stores. In CCS '07, pp.598-609, 2007.
6. R. Johnson, D.Molnar, D. Song, and D. Wagner.: Homomorphic signature schemes. In Proc. of CT-RSA, volume 2271 of LNCS, pp. 244-262, 2002.
7. A. Juels and B. Kaliski. PORs: Proofs of retrievability for large files. In CCS '07, pp.584-597, 2007.
8. Bowers, K., Juels, A. and Oprea, A.: Proofs of retrievability: Theory and implementation. Technical Report 2008/175, Cryptology ePrint Archive, 2008.
9. Y. Dodis, S. Vadhan, and D. Wichs. Proofs of retrievability via hardness application. In TCC, vol.5444 of LNCS, pp. 109-127, 2009
10. Zheng, Q. and Xu, S.: Fair and Dynamic Proofs of Retrievability. CODASPY’11, February 21–23, 2011, San Antonio, Texas, USA.
11. G. Ateniese, S. Kamara, and J. Katz. Proofs of storage from homomorphic identification protocols. ASIACRYPT’09, LNCC, 2009.
12. D Boneh, B Lynn, H Shacham. Short signatures from the weil pairing. ASIACCRYPT 2001. LNCS, vol. 2248, pp. 514-532, 2001.

