IJCSE International Journal of Computer Sciences and Engineering Open Access

Review Paper Vol.6, Special Issue.11, Dec 2018 E-ISSN: 2347-2693

Protection of Data in Cloud Computing using Image Processing - Watermarking Technique

S.Thaiyalnayaki[1*], S.Devi[2]

[1]Dept. of Computer Science, ADM College for Women, Nagapattinam, India
[2]Dept. of Computer Science, Thiru Vi. Ka. Govt. Arts College, Tiruvarur, India

Available online at: www.ijcseonline.org

Abstract— Abstract--With the dawn of easiness in manipulating and transferring digital data in today's world, insuring digital image integrity has therefore become a major issue. One solution to this problem is to embed watermark in the digital data, i.e. Digital watermarking. Usually watermarking has been used in currency notes, government documents, passport for security features and stamp papers for legal purpose. Watermarking is very beneficial for identifying the document of any authorized person. Digital watermarking emerged as a solution for copyrights detection, protection and maintenance of important data. Millions of private images are generated in various digital devices every day. Cloud computing, one of the most important computing paradigms emerged in recent years. Watermarking techniques to ensure data privacy. Consequently, this framework will increase the speed of development on ready-to-use digital humanities tools.

Keywords: Digital Watermarking, Cloud Computing, various algorithm and various Techniques**.**

I. INTRODUCTION

Digital watermarking is a technique to protect host digital data by embedding the data property like the company logo/image, copyright information into data. Digital image manipulation software is now readily available on personal computers. It is therefore very simple to alter with any image and make it available to others. Reversible watermarking inserts watermarks into digital media in such a way that visual transparency is preserved, which enables the restoration of the original media from the watermarked one without any loss of media quality. Reversible watermarking is a proven solution to this issue, where both watermark and original image can be recovered. Therefore, military, medical and quality control images must be protected against attempts to manipulate them; Fortunately, Cloud services ideally offer on-demand software and resources over the Internet to read and analyze ancient documents. In fact, once uploaded to cloud, the security and privacy of the image content can only assume upon the reliability of the cloud service providers. Lack of assuring security and privacy guarantees becomes the main barrier to further deployment of cloud based image processing systems. Recently, various solutions have been suggested to secure data processing in cloud environment. That is, data owners place the encrypted data in the cloud, and only the authorized users can decrypt the data and visit them. While watermarking method determines and maintains ownership. Image authentication techniques have recently gained great attention due to its importance for a large number of multimedia applications. Watermarking can contribute to better protect images by dissimulating into their pixels some security attributes (e.g., digital signature, user identifier).But, to take full advantage of this technology in healthcare, one key problem to address is to ensure that the image distortion induced by the watermarking process does not endanger the image diagnosis value. To overcome this issue, reversible watermarking is one solution.

II. CLOUD COMPUTING

Amazon, Google, Microsoft and few others have offered cloud based products and services to the market. Cloud computing as an internet based computing which refers to both the applications delivered as services as well as network and system softwares. The cloud looks like a big black box, content is invisible to the clients so the clients have no idea or control over what happens inside a cloud. It may result in the violation of confidentiality and integrity of the system. Fig [1] shows the structure of cloud computing used in IT organizations and is self explanatory. Among different techniques suggested, digital watermarking is considered to be very useful for data protection and authentication.

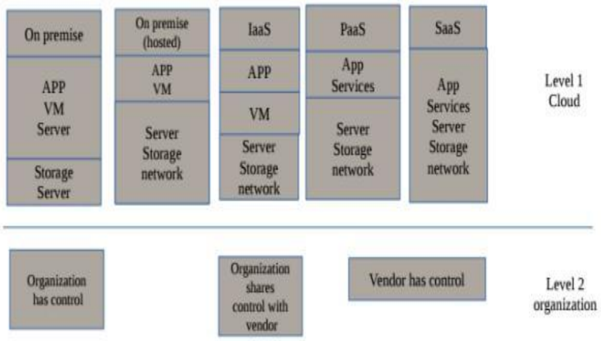

Fig.1 Impact of cloud computing on the structure of Information technologies.

III. SERVICE MODELS OF CLOUD COMPUTING

The three service models/deliverymodels available in cloud computing are

1. *SaaS (software-as-a-service*): Consumer has a capability to use the provider's applications running on a cloud infrastructure. Examples SaaS are Google Apps, Salesforce.com, etc.,
2. *PaaS (platform-as-a-service*): PaaS Provides the consumer with the capability to deploy onto the cloud infrastructure (middleware, databases), Consumer created or acquired applications, produced using programming languages and tools supported by the provider. Examples Google Application Engine, Windows Azure etc.,
3. *IaaS (infrastructure-as-a-service*):
IaaS provision the consumer with the Computational capabilities to processing, storage, networks, and other computing resources in a centralized, location transparent service and allow the consumer to deploy and run arbitrary software, which can include operating systems and applications. Amazon Web Services(AWS), Microsoft Azure, Google Compute Engine (GCE), Joyent etc.

IV. CLOUD COMPUTING SECURITY

The concern is for security in cloud computing environment when passing on any organizations critical information to geographically dispersed cloud platforms and that too is not in control of that particular organization whose data is to be stored on a cloud platform. Security issues related to the security of cloud computing are

- Privileged access
- Separation of the data from its actual location
- Data availability
- Regulatory compliance
- Long term viability

Security concerns based on delivery and deployment models are data integrity, data locality, data confidentiality, and data access.

V. OVERVIEW OF DIGITAL WATERMARKING

Digital watermarking is a communication method in which the information is embedded directly and ephermally into digital data e.g., image, video, or audio signals, also called original data or host data to form watermarked data. Watermarking can be defined as a group of bits inserted into a digital data(audio or video or image) file that identifies the file's copyright information(author, rights).

From the above Fig. there are 2 phases in watermarking technique: In phase 1 user adds dataset (D) along with a private key (K). Watermark is calculated and available as watermark data (WD). In phase 2 the embedded watermark is extracted by giving Watermark dataset and his private key. So the original data (D) will be extracted with proof of ownership.

VI. DIGITAL WATERMARKING VARIOUS TECHNIQUES

The watermarking technique had provided extra security to cloud data. For the last few years, reversible watermarking techniques are gaining popularity because of increasing some applications in sensitive and important areas, i.e., important military communication, medical department, and some law-enforcement.

Digital watermarking techniques are classified according to documents types such as:

1. *Text Watermarking*: It is an approach for text document copyright protection. Digital watermarking for text documents are primarily classified into 3 types.

- *Line shift coding*: This vertically shifts location of text lines to encode the document.
- *Word shift coding*: This horizontally shifts location of words to encode the document.
- *Feature coding*: This will choose certain features and alerts those selected features.

2. *Image Watermarking*: In this method a watermark is added to image copied. The watermark is a part of the image and cannot be easily removed from a picture.

3. *Video Watermarking*: This involves embedding cryptographic information derived from frames of digital video into the video itself.

4. *Audio Watermarking*: In this method an electronic identifier is embedded in an audio signal. Some authors proposed the use of text or images to be embedded in the audio file such that any of such audio file could be analyzed for a possible recovery.

First technique is to embed the *visible watermark* which can be seen by everybody who is seeing the data object. Second technique is to insert the *hidden watermark* which provides backup facility in case when visible watermark fails to prove trustworthiness of data. Both *visible and hidden watermarks* are embedded in the data objects when these data packets are created or added for the first time in the cloud. Some of the audio watermarking techniques available are spread spectrum, amplitude modification, replica method, dither watermarking and self marking methods. Numerous watermarking techniques have been proposed by the researchers for ensuring the security of shared data.

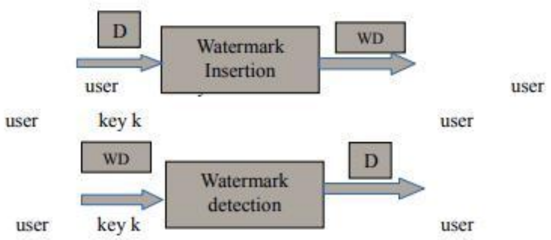

Fig.2. Watermarking Technique

These techniques are categorized on the basis of types of watermark like digital watermark, visible watermark, invisible watermark, etc., These techniques can also be characterized by data provenance, data lineage, usability, and robustness. Likewise, medical research requires severe product quality data checks because errors can harm people's health.

VII. DIFFERENT WATERMARKING METHODOLOGY USED TO SECURE DATA IN CLOUD

It is thus important to ensure the invisibility of reversible watermark in order to ensure a permanent image protection. The main focus is how watermarking technique can be used to maintain original rights about data in cloud computing.

- One of the watermarking techniques for data provenance is practically examined using a free and opensource cloud software known as ownCloud. ownCloud is a file sharing server that permits its users to store data objects in a centralized location, much like Dropbox. These data objects can be any type of images or text documents.
- To implemented technique of watermarking SVD-DCT-DWT techniques has been implemented on cloud architecture. To check robustness of the watermarked data, sharpened attack, contrast attack and salt-pepper attack has been triggered and performance is analyzed with PSNR and MSE value.

a)Kalman filtering
b)Gabor Filtering
c)Salt and Pepper Filtering

- A new Cloud-User protocol as a solution for plain text outsourcing problem. We only allow users and CSPs to embed the ciphertext watermark, which is generated and embedded by Trusted Third Party (TTP), into the ciphertext data for transferring. Then, the receiver decrypts it and obtains the watermarked data in plain text. To the best of our knowledge, watermarking is used in copy deterrence and tracing down the distribution of illegal copies. This fact indicates watermark can be used to protect RTBF by proving the crimes of CSP(Cloud Service Provider).
- Digital watermark (W) is a signal embedded into data to identify some attributions of the data (i.e., ownership). According to the domain embedded, digital watermark embedding algorithms are divided into time-spatial embedding, which is fast and relatively easy to operate but is easy to be erased by geometrical attack, and transform domain embedding Moreover, according to the preknowledge related to data before embedding, we classify the embedding method into preknowledge dependent embedding and preknowledge independent embedding.
- In fact, the Thodi algorithm is a reversible watermarking algorithm, which is usually designed to survive normal image processing operations. This method seeks to ensure authentication. Cloud platform is typically based on a distributed system. Furthermore, different techniques are used to guarantee the availability of digital tools and technology, including load balancing, virtualization and cluster technology.
- Watermarking is to introduce small images or patterns into the data to be watermarked without aff ecting the data subject to normal use. If an illegal copy occurs, the owner of the data can therefore get watermarks from the illegal data to verify his ownership of the data. The maintenance team of cloud environment may provide copyright protection but there is a chance of stealing/hacking our own confidential information by them. Robust reversible watermarking and RSA digital signature can solve this problem. These two techniques were used after the encryption algorithm and is used to protect the data in mobile cloud environment. It offers better security performance, increase the original information quality and confidentiality. Data security is enhanced using a combination of RSA digital signature algorithm with robust reversible watermarking technique. Reversible watermarking allows full extraction of the watermark along with the complete return of the work.
- If medical research person will be analyzing patients records, they may need accurate data for the patients. Traditionally, data leakage detection is handled by watermarking technique. Watermarks can be very useful in real-time environment, but again, it involves some modification of the original data.

VIII. CONCLUSION

In this work, watermarking technique has been implemented to provide data security. We also change the combination of encryption algorithms with different watermarking algorithms to improve the output message without any loss. In fact, security and privacy need more improvements to protect clients' data. To this end, various implementations are proposed to promote digital image processing using cloud services. Still, these frameworks have certain limitations in terms of security and performance. In this study, we propose a solution based on different watermarking techniques and methods to enhance privacy and security.

REFERENCES

[1]. A survey on watermarking methods for security of cloud data, Mrs. Anitha P1 , Dr. Malini M Patil2 1.2Department of Information Science and Engineering, JSSATE (India), (ICRISEM-16), 26TH February 2016, www.conferenceworld.in.

[2]. Data Provenance for Cloud Computing using Watermark, (IJACSA) International Journal of Advanced Computer Science and Applications, Vol. 8, No. 6, 2017

[3]. To Propose A Novel Technique for Watermarking In Cloud Computing, © 2015 IJEDR | Volume 3, Issue 2 | ISSN: 2321-9939

[4]. An Efficient Approach for Security of Cloud Using Watermarking Technique, International Journal of Advanced Research in Computer and Communication Engineering Vol. 2, Issue 7, July 2013

[5]. A Survey on Security in Cloud Computing, Varsha Yadav et al, International Journal of Computer Science and Mobile Computing, Vol.3 Issue.4, April- 2014, pg. 509-513

[6]. Data Leakage Detection and Security Using Cloud Computing, S.Geetha et. Al. Int. Journal of Engineering Research and Applications, ISSN: 2248-9622, Vol. 6, Issue 3, (Part - 2) March 2016, pp.01-04

[7]. The Amalgamation of Digital Watermarking & Cloud Watermarking for Security Enhancement in Cloud Computing, IJCSMC, Vol. 2, Issue. 4, April 2013, pg.333 – 339, ISSN 2320–088X.

[8]. A Cloud-User Protocol Based on Ciphertext Watermarking Technology, Security and Communication Networks, Volume 2017, Article ID 4376282,14 pages, https://doi.org/10.1155/2017/4376282

[9]. A method for trust management in cloud computing: Data coloring by cloud watermarking,International Journal of Automation and Computing 8(3):280-285 · August 2011

[10]. An Efficient Approach for Data Security in Cloud Environment using Watermarking Technique and RSA Digital Signatures, International Research Journal of Engineering and Technology (IRJET), Volume: 04 Issue: 02 | FEB -2017.

[11]. A Secured Data Processing Technique for Effective Utilization of Cloud Computing, HAL Id: hal-01466986 https://hal.archives-ouvertes.fr/hal-01466986v2 Submitted on 21 Nov 2017.

[12]. A Survey about Cloud Computing and an Improved Method of Data Security using Watermarking Technique with RSA Algorithm in Cloud Environment, Asian Journal of Research in Social Sciences and Humanities Vol. 7, No. 5, May 2017, pp. 325-336

[13]. Secure Medical Images Sharing over Cloud Computing environment, (IJACSA) International Journal of Advanced Computer Science and Applications, Vol. 4, No. 5, 2013.

[14]. A Survey on Watermarking Methods for Security of Cloud Data, Mrs. Anitha P1 , Dr. Malini M Patil2 1.2Department of Information Science and Engineering, JSSATE (India), (ICRISEM-16), 26TH February 2016, www.conferenceworld.in.

[15]. Amandeep verma ,sakshi kaul ,"Cloud computing Issues & challenges :A survey ", Springer verlag Berlin Heidelberg, part IV,ccis 193,2011,pp.445-454.