IJCRT.ORG ISSN : 2320-2882

INTERNATIONAL JOURNAL OF CREATIVE RESEARCH THOUGHTS (IJCRT)

An International Open Access, Peer-reviewed, Refereed Journal

Improving Cloud Data Security With Watermarking In Cloud Computing

S.K. Sahoo[1], Mohammed Arif[2], P. Das[3]
[1]Assistant Professor, Dept of CSE, GITAM, Bhubaneswar - 752054.
[2]Assistant Professor, Dept of CSE, GITAM, Bhubaneswar - 752054.
[3]Assistant Professor, Dept of CSE, GITAM, Bhubaneswar - 752054.

ABSTRACT

Cloud computing spreads data across many virtual servers. To get data from these servers, people from different places connect with cloud service providers. Users don't have to upgrade their systems or set up complicated structures to use the cloud service. This study talks about the different services in cloud computing and how watermarking techniques can help with security. It explains how using watermarking can make data stored in the cloud more secure.

Key words: Watermarking in cloud, Data security, Security using encryption.

1. INTRODUCTION

Cloud computing allows users to access services provided by service providers on a pay-per-use basis. This paradigm enables individuals and businesses to utilize remotely controlled software and hardware managed by external parties. In this study, we propose a method for enhancing security, which involves identifying unauthorized databases and verifying ownership. We utilize watermarking technology to protect databases and prevent unauthorized access and copying.

Digital watermarking is the most common and effective method for protecting owners from unauthorized use. It involves generating and recognizing invisible markings that can identify the source, integrity, and authorized use of digital data. These markings should be imperceptible and difficult to reproduce.

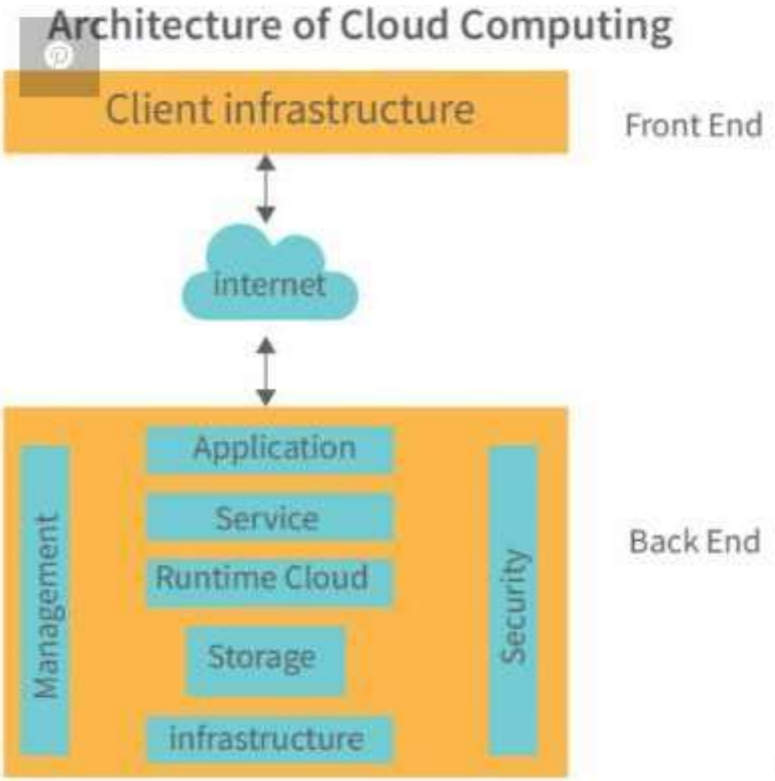
2. Cloud Computing

Cloud computing is a form of computing where resources, software, and data are provided on demand to computers and other devices from shared servers, independent of their physical location. Applications in cloud computing store and manage data and files according to user requirements. The National Institute of Standards and Technology (NIST) defines cloud computing as a model for delivering IT services that enables convenient, on-demand network access to a shared pool of configurable computing resources (such as network services, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction.

Cloud computing offers a new type of computing architecture that provides services on demand and at a lower cost. The three well-known and widely used service models in cloud computing are SaaS (Software as a Service), PaaS (Platform as a Service), and IaaS (Infrastructure as a Service). SaaS delivers applications to users over a network, allowing access from any device with internet connectivity. PaaS provides a platform and environment for developers to build applications and services, which are hosted online in the cloud. IaaS offers internet users access to computing resources in a virtualized environment known as "the cloud."

Cloud computing can be categorized into three types: public cloud, private cloud, and hybrid cloud, based on access scope. Public cloud services are owned and operated by a service provider and are available for use by anyone. Private clouds are owned and operated by specific organizations, limiting access to authorized users. Hybrid clouds combine elements of both public and private clouds, allowing data and applications to be shared between them.

2.1 Characteristics of Cloud Computing



Following are the five essential characteristics:

- **On-demand self-service:** The cloud offers users all necessary computer resources based on their needs.
- **Wide Network Access:** Users can use a desktop computer, a laptop, a mobile phone, etc. to access cloud services online.
- **Resource Pooling:** The cloud provider allocates resources to users in accordance with their needs.
- **Quick Elasticity:** Depending on the situation, cloud computing can swiftly allocate and de-allocate services.
- **Measured Service:** Resource utilisation is controlled by the cloud provider.

2.2 Benefits of cloud Computing

Following is list of key benefits on enterprise can expect to achieve when adopting cloud infrastructure.

- **Cost reduction:** One can save a lot of money by using cloud infrastructure instead of buying and manufacturing expensive equipment. Also, it lowers downtime-related expenditures.
- **Data Security:** The cloud provides cutting-edge security measures to ensure that data is handled and kept safely.
- **Scalability:** Cloud-based solutions are perfect for companies with expanding or varying bandwidth requirements. Without having to invest in physical infrastructure, you can quickly increase your cloud capacity as your business demands grow.
- **Mobility:** Cloud computing enables access to company data on the go via a smartphone and other mobile devices.

- **Disaster Recovery:** Cloud-based services offer speedy data recovery in a variety of emergency situations, including power outages and natural catastrophes.
- **Control:** The cloud gives you total visibility and management of your data. You can easily choose which people have access to what data at what degree.

3Using a watermark

A watermark is a message—typically a logo or stamp used as a signature—that is highly transparently overlaid over an image. The use of watermarking to obscure multimedia data is relatively recent. There are two categories for the watermarking technique: visible watermarking and invisible watermarking. The fundamental benefit of both visible and invisible watermarking is that it can be viewed without being extracted, but their drawback is that watermarking would ruin the presentation of the material, making it inappropriate for use in today's modern digital applications. In contrast, invisible watermarking is removed using a specific technique, however it may keep the cover image's original appearance.

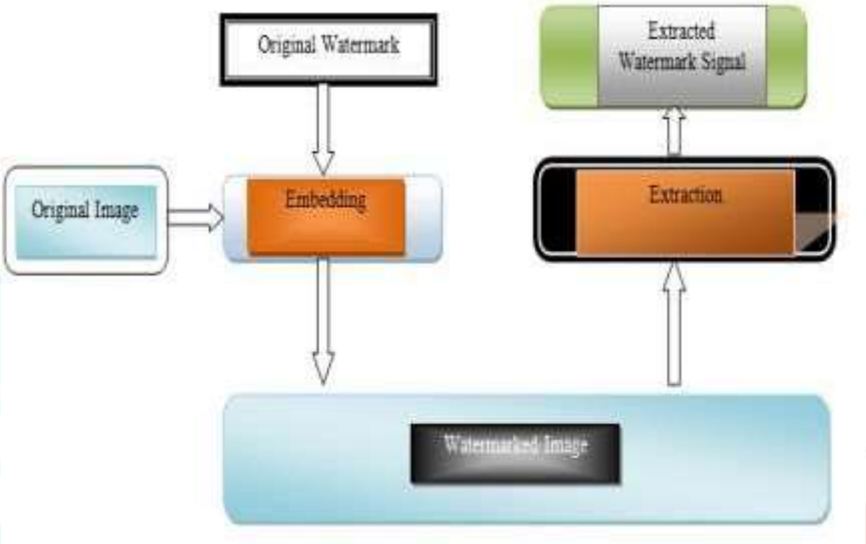


Fig.1: Block diagram of Watermarking

Electronic Watermarking

Data is inserted into digital multimedia content using the digital watermarking technique. This is used to confirm the legitimacy of the content or identify the owner of digital information. Watermarking on digital images is used to insert secret information. Upon embedding, a watermarking image is created that is more resistant to attacks. Water marking can be broken down into three stages:

Embedding stage: -

Watermarking is initially inserted into the original image during the embedding stage using an embedding technique and a secret key. Afterwards an image with a watermark is created. Hence, the watermarked image is sent over the internet.

Attack / Distortion Stage: At this phase, our watermarked data is either altered or destroyed as it is transported across a network, depending on whether noise is introduced to the watermarked image or an attack is launched against it.

Stage of detection and retrieval: In this stage, the watermark is recognised or retrieved from the watermarked image by the specialised detector utilising a detection algorithm and a secret key. Noise has also been identified in addition to this.

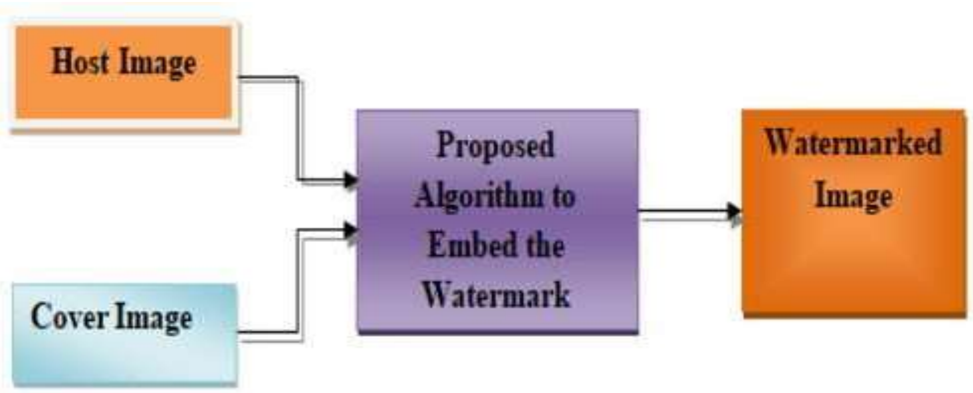


Fig.1: Basic Watermarking Principle

Type of Digital Watermarking

Watermarks and watermarking techniques can be categorised in a number of different ways. According to the type of document that needs to be watermarked, watermarking techniques can be categorised into the following four groups:

1. Text watermarking
2. Image watermarking
3. Audio watermarking
4. Video watermarking

Many techniques provide watermarking in the spatial domain for photography. Frequency domain watermarking is an alternative to spatial watermarking.

Category of Watermarking:

Depending on a variety of factors, digital watermarking techniques can be categorised in a number of ways. The following is a list of different types of watermarking techniques.

1. **Strong & Weak watermarking:**
   While using robust watermarking, any changes to the watermarked content have no bearing on the watermarking. Contrarily, fragile water marking is a method in which water marking is lost when the contents being water marked are altered or interfered with.
2. **Watermarking that is both visible and transparent:**
   Visible watermarks are those that are incorporated into visual content in a way that makes them visible when the content is viewed. When examining digital content, transparent watermarking cannot be seen and cannot be identified.
3. **Public vs. Private Watermarking:**
   Users of the content are permitted to identify watermarks in cases of public watermarking, but not in cases of private watermarking.
4. **Symmetric and Asymmetric Water Marking:**
   Symmetric Watermarking uses the same key to embed and detect the water mark, whereas Asymmetric Watermarking uses distinct keys.
5. **Steganographic and Non-Steganographic Water Marking:**
   Steganographic Water Marking is a method in which readers of the content are not aware that Water Marking is present.

Users are aware of the presence of the watermark in njon-steganographic watermarking. While non-steganographic watermarking techniques can be used to detect privacy,steganographic watermarking is used in fingerprinting applications.

Characteristics of Digital Water Marking

1. **Invisibility:** An embedded water marking is not visible.
2. **Robustness:** Piracy attack or image processing should not affect the embedded water marking.
3. **Readability:** A watermarking should convey as much information as possible. A watermarking should be statistically undetectable. Moreover, retrieval of the digital Water Marking can be used to identify the ownership & copyright ambiguously.

4. **Security:** A watermarking should be secret & must be undetectable by an unauthorized user in general. A Water Marking should only be accessible by authorized parties.

WATERMARKING TECHNIQUES: There are primarily two types of digital picture watermarking schemes:

1. Techniques using the spatial and frequency domains.

A. Methods for the spatial domain: Some of the spatial domain techniques of watermarking are following. LSB, or Least Significant Bit: That is the simplest method for putting a watermark. The LSB of the pixel has a watermark thanks to this method. Provided that an image has pixels and that each pixel is represented by an 8-bit sequence, the watermarking is encoded in a few chosen pixels' last (least important) bit. Although this technology is simple to use and does not significantly distort the image, it is not highly resistant to attacks.Attacks may, for instance, just randomise all LSBS, which would obliterate the secret data. Method Based on SSM Modulation: Spread-spectrum modulation techniques purposefully spread or appropriate energy created at various discrete frequencies in time for the development of secure communications, to increase resistance to interference from the environment and jamming, and to avoid detection.By fusing the cover picture with a little amount of pseudo-noise signal modulated by the additional watermark, the SSM watermarking technique embeds information in the content of the image watermarking. A. Using the frequency domain method This method aims to include the watermarks into the image's spectral coefficients. The properties of the human virtual system (HVS) are better captured by the spectral coefficients than by the most often employed transforms, the discrete cosine transform (DCT) and discrete Fourier transform in the frequency domain. More information concealing capacity and excellent robustness against various geometrical attacks are provided by these strategies. The DWT approaches were used in this paper.

2. DWT in image Processing:

(DWT) Distinct A mathematical method for hierarchical breakdown of an image is the wavelet transform. The transformation is based on breaking down a signal into wavelets, which are brief waves with different frequencies. An original signal is divided up into wavelet transform coefficients by the wavelet characteristics, and these coefficients carry positional data. When these coefficients are subjected to an inverse wavelet transformation, the original signal can be fully recreated.

An image is divided up into three details and one approximation using DWT. LL, LH, HL, and HH are the bands. Low frequencies are present in LL in both the horizontal and vertical directions. High frequencies are present in HH in both the horizontal and vertical directions. High frequencies are present in the horizontal direction of HL. low frequencies moving vertically LH consists of low frequencies oriented horizontally and high frequencies oriented vertically. The signal's coarse information is contained in the low frequency portion, but the high frequency portion contains data on the direction of the signal's edge components.

The most important band is the LL band, which approximates the image and includes the majority of the image energy. The high frequency detail bands (LH, HL, and HH) can accommodate water marking since human eyesight is less sensitive in these areas. Without degrading the image's clarity further, embedding into these bands makes the water marking more resistant. The DWT is carried out in two steps at each level of decomposition: first in the vertical direction, then in the horizontal. Four subbands are produced by the first level of decomposition: LL1, LH1, HL1, and HH1. Every each level of the decomposition starts with the input from the LL sub band of the previous level. This LL subband is further decomposed into four multi resolution Sub- bands to acquire next coarser wavelet coefficients.

The number of times the process is repeated depends on the application.

The excellent spatio-frequency localization capability of DWT has been extensively used to pinpoint the regions of a picture where a disturbance can be simply concealed.Moreover, this method does not need the original image to detect watermarks. As a result, it is employed in numerous signal processing-related applications, such as noise removal and audio and video compression

Conclusions:

This paper focuses on improving security for cloud databases for all cloud users. We'll use a combination of watermarking techniques to enhance security and ensure the authentication of cloud users.

References:

1. U. Yadav, J.P. Sharma, D. Sharma and P.K. Sharma, “Different Watermarking Techniques and its Applications: A Review”, International Journal ofScintilla and Engineering Research, Vol. 5, no.4, (2014) April.
2. Chih-Chin Laiand Cheng-ChihTsai, “Digital Image Watermarking Using Discrete Wavelet Transform and Singular Value Decomposition”, IEEE TRANSACTIONS ON INSTRU- MENTATION AND MEASUREMENT, VOL.59, NO.11, NOVEMBER 2010.
3. C.-c. Lai and c.-c. Tsai, “Digital Image Watermarking Using Discrete Wavelet Trans- form and Singular Value Decomposition”, IEEE Transactions on Instrumentation and Measurement, vol. 59, no.11, (2010) November.
4. M. Narang and S. Vashisth, “Digital Watermarking using Discrete Wavelet Transform” International Journal of Computer Applications (1975-88887) vol.74, no.20, (2013) July.
5. Salama, A., Atta, R. , Rizk, R. Wanes, F., “A robust digital image watermarking technique based on wavelet transform”. In: IEEE Int. Conf. on Sys. Eng. and Tech., pp. 100-104 (2011).
6. Ahmed S. Salama, Mohammed A. AI- Qodah, Abdullah M. Tliyasu, Awad Kh. AI-Asmari and Fei Yan: A Hybrid Fusion Technique for watermarking Digital Images: Advances in Intelligent Systems and Computing Volume 240, pp 207-217, (2014).
7. lliyasu, A., Le, P., Dong, F., Hirota, K.: Watermarking and authentication of quantum images based on restricted geometric transformations. Information Sciences 186(1), 126-149 (2012). 562.
8. AI-Asmari, A., Salama, A., T1liyasu, A., AI-Qodah, M.: A DWT ordering scheme for hiding data in images using pixel value difference. In: IEEE Eighth Int. Conf. on Computational Intelligence and Security (CIS), pp. 553-557 (2012).
9. Abid Khan, Ayyaz Yaqoob, Kinza Sarwar, Mouzna Tahir, Mansoor Ahmed, “Secure Logging as a Service Using Reversible Watermarking”, The 12th International Conference on Future Networks and Communications, (FNC- 2017)
10. Rita Choudhary, Girish Parmar, “A Robust image Watermarking Technique using 2-level Discrete Wavelet Transform (DWT) “, IEEE 2nd International Conference on Communication, Control and IntelligentSystems (CCIS)
11. Mr. Y. Gangadhar, Dr. V.S. Giridhar Akula, Dr. P. Chenna Reddy, “ A Survey on Geo metric Invariant Watermarking Techniques” , 2016 IEEE
12. Ahmed S. Salama, Mohamed Amr Mokhtar, “Combined Technique for Improving Digital Image Watermarking”, 2016 2nd IEEE International Conference on Computer and Communications
13. Mr. R. D. Shelke, Dr. Milind U. Nemade, “Audio Watermarking Technique Protection : A Review”, 2016 International Conference on Global Trends in Signal Processing, Information Computing and Communication
14. Chengxiang Yin, Jin Hu, Xuejun Zhang, Xiang Xie, “Advertising system based on cloud computing and audio watermarking”, 2015 International Conference on Intelligent Information Hiding and Multimedia Signal Processing
15. Muhammad Imran and Bruce A. Harvey, Adnan Ali Memon, “A Novel Blind Color Image Watermarking Technique Based on Singular Value Decomposition and Principal Component Analysis”, 2016, The Sixth International Conference on Innovative Computing Technology.