# Apply watermarking Technique for Cloud Computing: An Overview

*Atul Kumar Dwivedi, #Rajbhan Singh

*,#Ph.D. Research Scholar

Madhyanchal Professional University, Bhopal

**Abstract - In this research paper, we are discussing about watermarking technique for cloud computing in purpose of data security. Because the work of uploading data to the server is being done at a very fast speed through cloud computing. Therefore, there is bound to be data irregularity between them, whose only technique is watermark technology. Through this paper, which techniques are used to apply watermark technology in the server of cloud computing and which are the most powerful techniques and algorithms available to be used in the current context. A detailed description of the applications that are required to implement the watermark technology algorithm is presented here. It has also been tried to tell here that there are some essential properties for applying algorithms in the applied field, which is a necessary and essential process to take care of. It's a basic element that is involved in completing the process of watermarking in any digital content, whose details are also presented.**

**Keywords: cloud computing, watermark, server, algorithms etc.**

## I. INTRODUCTION

Today's era is completely the era of technology, in this era human beings are interconnected with each other with the help of wired or wireless through computer and internet network. Various types of digital content related to entertainment have been invented to create abundance in the human community. The creation, manipulation and entertainment of data are done by the devices available for the creation of these digital materials such as cameras, camcorders, MP3 players, PDAs etc. Today the development of internet has converted the whole world into a village. Creation of various electronic files through this internet, electronic publication of these files, e-advertisement, e-newspaper, e-magazine, e-library, online video, online audio, online product ordering, online transaction, real time information delivery etc. are being done. All these functions have made it very easy to store, transmit and distribute data on the server. However, many multimedia productions are afraid to broadcast and distribute these valuable videos due to copyright protection issues. The basic reason for this is that the data uploaded to the server can be easily copied, modified, and looks exactly like the original file. This leads to malicious intent called piracy. There is an effective way to prevent this problem, through which multimedia data is protected against illegal retransmission and recording. The signal used to provide ownership of the data is called a digital signature or copyright label or watermark. This technique is known as digital watermarking, which is a state-of-the-art technology that places a secret message behind a covered medium in such a way that it is not visible to the eyes of the common man. He considers it to be a normal cover page. Invisible message on the back of a generic cover page may contain the manufacturer's name, company logo/name or any other mark that can only be removed if some specific algorithm is applied to remove the country, which provides proof of ownership.

Mostly it has been observed that storing and accessing data in cloud computing increases the risk of data insecurity. We all know that in the world of the Internet, no type of data can be considered completely secure. Especially when data is being used globally with the help of Internet servers and various types of computer devices, then the need for a technology is felt, which can protect the data uploaded to the server and protect the copyright of the original author. In this situation, the watermark technique seems to be the most efficient and appropriate method. In the field of cloud computing, many scientists have developed various types of algorithms and they have also been applied in computers. This algorithm is also fully capable of providing mediocre results to an extent. Therefore, under this research paper, various methods have been discussed in detail and various dimensions have been presented.

## II. RESEARCH METHODOLOGY

Qualitative method has been used in present research paper. After studying various other researches work related literature like: research paper, books etc. and then details have been presented using qualitative research methodology.

## III. APPLICATION OF WATERMARKING

At present, watermarking technology can be used in various applications; the details of the main applications are presented below:

i. **Authentication:**
Digital watermarks are used to authenticate any type of digital content. Watermarks are used to detect changes or modifications to any digital content. To identify the watermark, the watermark needs to be delicate so that any modification marks in the image can be destroyed. It is also ensured through digital watermark that any type of digital content has not been modified or any change has been made after the original creation of the content. Often this is very fine, even if the content has been changed to a very small extent; the watermark may have a large change, which may be perceptible or imperceptible. This is achieved through the use of fragile or semi-fragile watermarks, reducing the scope for modification of the material.

ii. **Copyright Protection:**
Its purpose is to mark any type of digital content as permanent and irrevocable by a special mark so that the original content does not conflict with any kind. If the original owner of the data content wishes to check for illegal copies of his content, he can claim his ownership by using a watermark. Information about the creator or owner of digital content is marked. This method is usually very robust, understandable and imperceptible. With the help of watermark technology, the ownership of the original documents is provided with great ease.

iii. **Copy Prevention:**
Watermarks are also used for copy prevention and control. If the copyright owner of the original document wishes to control the terms of use of his work, he can find out by whom the original work was completed by means of a signal marked in the digital data. For example: DVD video, audio etc. If DVD video is used by someone else, recording may be stopped via a signal marked by a watermark. Copying or viewing any type of multimedia content requires special hardware. The watermark can be modified by the hardware, as a result of which after some time the hardware will no longer allow another copy of the data. In this way the original form of the digital content can be protected without alteration.

iv. **Fingerprinting:**
Watermark is used as a fingerprint to identify the source of an illegal copy. Just as partial fingerprint recovery is an important method of forensic science in the general crime world, watermarks serve to deter crime of digital content. Different types of digital content available in the market are watermarked differently by the owner in the copies of the data supplied to different customers. For example: DiVX. This is a modified version of the DVD. Through this it traces the source of illegal copies.

v. **Broadcast Monitoring:**
Watermark technology monitors when and where the advertisement is broadcast. Such as TV, Radio, Newspaper, Internet etc. In advertising applications, by removing the watermark to be broadcast with host media, advertisers can monitor whether advertisements that have been paid for are broadcast by broadcasters in accordance with the agreements.

vi. **Temper Detection:**
Any tampering with digital content can be detected by tamper detection. If any watermark has been tampered with for the purpose of destroying or damage to the identity of the watermark, it should be assumed that the digital content cannot be relied upon or that the digital content has been altered. This original document or material cannot be produced as evidence for the purpose of original content. Tamper detection can also be used as evidence in a court of law to prove that the original material has been tampered with.

vii. **Covert Communication:**
Covert communication is a powerful means with the help of which tampering of digital content can be prevented. The main problem in the transmission of data content is that apart from the sender and receiver of the data, there is also a person who has the ability to make changes in the data. In this situation the communication is kept covert while encoding and decoding the data to retain the original data. E.g.: Text Modification, Audio Modification, Video Modification etc.

## IV. PROPERTIES OF WATERMARKING

There are some properties are available for the purpose of implemented watermark technique, which are following:

i. **Imperceptibility:**
Invisibility refers to the conceptual similarity between the original digital content and the data marked with a watermark. The owner of the original data does its best to avoid any loss of most of its original digital content. Therefore, watermarked digital content with watermarks should be conceptually invisible. Embedded watermarks in any kind of original content should not reduce the quality in any way. Original content must be completely lossless. Lossless watermark planning is a good solution to maintain the quality of the original content.

ii. **Robustness:**
Here robustness means being able to protect a watermark that is embedded in any digital content from various other attacks. Watermarks are

DOI : 10.35291/2454-9150.2022.0438

commonly attacked in the crime world by various digital signals and several methods are used, such as: blurring, JPEG compression, noise addition, sharpening, scaling, rotation, cropping and printing-recovering after photocopying-scanning, must be eligible. In other words, understand the way the watermark must be strong enough to protect against attacks so that digital content can retain its original ownership.

iii. **Capacity:**

Watermarking capability refers to being able to verify and differentiate different watermarks with less chance of error, as the number of versions increases after watermarks are applied to digital content. The capability of a watermarking system can also be understood in the way that the watermark is to be embedded in the digital content without affecting the quality of the digital content. The watermarking capability depends on the size of the original host signal, i.e. if the size of the original host signal is large then watermarking does not have much effect, but if the size is small then the original content is affected to a large extent. A high-quality watermark can be said to be one that has the ability to display bits of information firmly against various types of digital attacks. As the robustness of the watermark increases, so does the capacity while the imperceptibility decreases. Keeping all the above requirements in mind, it is advisable to propose a watermarking method.

iv. **Security:**

The security of the crypto system should not depend only on keeping the crypto algorithm secret, but the security of the watermarking should be limited to the key only. When the watermark is not removable, the watermarking algorithm should be publicly displayed. One thing should always be remembered that the user also knows the exact algorithm to deactivate and detect the watermark. So the only way to preserve the watermark is to select the key. Algorithms to be applied by the user are matched with the help of keys. The user will be able to remove the watermark with the help of algorithm but it will be impossible for him to match the key, which is of great importance for the security and strength of the watermark.

v. **Computational Complexity:**

Another feature of watermarking algorithms is the computational complexity, as embedding the watermark into the digital content and extracting the information from the watermark is a necessary process. If the watermark algorithm is robust then encoding or decoding in digital content is a very sensitive process. If the watermark algorithm is not robustly encoding or decoding, then its usefulness in real life will be reduced. It is very important in various applications that the process of embedding is as simple and fast as possible, thereby avoiding any tampering with the digital content. When designing a strong watermark algorithm, it becomes essential to minimize the computational complexity.

vi. **Multiple watermarking:**

A method of multiple watermarks is proposed to provide additional security to any digital content. Watermarking is done by adding some secret messages to it. Copyright information can be protected by authentication using multiple watermarking techniques. It is a very important and useful technique to trace the distribution of digital content. However, when multiple watermark techniques are used in the same digital content, the second watermark should not be used by crossing the front watermark. A good watermark algorithm will need to overcome this weakness.

vii. **Unambiguity:**

The ownership of any digital content must be accurately and clearly verified by watermarking technology. Tampering with digital content may confuse ownership by adding or tampering with the watermark by adding other illegal watermarks. Therefore, it is very important for any type of watermark to be unambiguous. Such as, various types of problems related to ownership.

## V. Conclusion

Therefore, in conclusion, it can be said that watermark technology is an effective and important process to retain the original and to provide ownership of the data stored in the cloud server. Through this research paper, a detailed description has been presented on the various applications and features of watermark technology. It is widely accepted that watermark algorithms are the only way through which tampering and irregularities of data can be reduced or saved. The application area of watermarks is very wide and vast. Today digital content is being used in abundance and through many mediums. There is no hesitation in self-declaring even after having sufficiently tampered with the digital content. Controlling which is an urgent and necessary work has been done. The details of some of the required applied areas have been presented in the above for performing watermark algorithms in any digital content. So that it can be understood in detail that after the development of the watermark algorithm, in which applications it can be used and data security can be provided. Some essential elements are included while applying watermark technology under watermark properties, their brief description has been presented. Finally, as a conclusion, we

DOI : 10.35291/2454-9150.2022.0438

get whether the necessary condition in building a good algorithm is being fulfilled and whether the data is getting complete security or not.

## REFERENCES

[1] Bhasha, Syed Jeelan. Saxena, Sachin. A literature review on DWT-SVD Based Watermarking Technique. International Journal of Advanced Technology and Innovative Research. ISSN 2348-2370, Vol. 10, Issue. 04, April-2018, Pages: 0374-0379.

[2] Sunesh. Malik, Vinita. Sangwan, Neeti. Sangwan, Sukhdip. Digital Watermarking using DWT-SVD Algorithm. Advanced in Computational Sciences and Technology. ISSN 0973-6107 Volume-10, Number 7 (2017) pp. 2161-2171 @ Research India Publications.

[3] Kandoi,Varsha. Singhawat, Brijraj. A Literature Review on Digital Video Watermarking. International Journals of Innovative Science and Research Technology, Vol-1, Issues 3, June-2016.

[4] Guru, Jaishri. Damecha, Hemant. A review of Watermarking Algorithms for Digital Image. International Journal of Innovative Research in Computer and Communication Engineering. (An ISO 3297: 2007 Certified Organization) Vol. 2 Issue 9, September 2014.

[5] Sinha, Manoranjan Kr. Rai, Rajesh. Kumar, G. Literature survey on Digital Watermarking. International Journal of computer and information technology, vol-5, 2014, ISSN: 0975-9646.

[6] S, Maheshwari. Novel DWT based watermarking techniques for two dimensional and spectral images for copyright protection and authentication, unpublished Ph.D. Thesis, Anna University Chennai. 2013.

[7] Shah, prassana. Et al. A DWT based digital watermarking technique for copyright protection. International conference on Electrical, electronics, communication and optimization, 2015.

[8] S, Maheswari: "Novel DWT based watermarking techniques for two dimensional and spectral images for copyright protection and authentication". Ph.D. thesis, Anna University, Chennai 600025, November 2013.

[9] Rashid, Aaqib: "Digital watermarking Applications and techniques: a brief review", International Journal of Computer Applications Technology and research, Volume 5-Issue3, 147-150, 2016, ISSN: 2319-8656.

[10] sondhi, preeti. Gull, Soufia: "survey on digital video watermarking techniques, attacks and applications". International Journal of trends in scientific research and development, Volume 5 Issue 5, July-August 2021, pages 60-65.

DOI : 10.35291/2454-9150.2022.0438