Journal Homepage: - www.journalijar.com

INTERNATIONAL JOURNAL OF ADVANCED RESEARCH (IJAR)

ISSN NO. 2320-5407

Article DOI: 10.21474/IJAR01/19779
DOI URL: http://dx.doi.org/10.21474/IJAR01/19779

RESEARCH ARTICLE

"SAFEGUARDING OWNER DATA IN CLOUD COMPUTING: ANALYSIS AND IMPLEMENTATION OF COLOR DROP WATERMARK TECHNIQUE FOR PROTECTING OWNER DATA IN CLOUD SYSTEMS"

Prakash Kumar Mourya[1] and Dr. Meesala Sudhir Kumar[2]
1. Research Scholar, Computer Science & Engineering, CMJ University, Jorabat, Meghalaya.
2. Professor, Computer Science & Engineering, Sandip University, Nashik, Maharashtra.

Manuscript Info

Manuscript History
Received: 29 August 2024
Final Accepted: 30 September 2024
Published: October 2024

Key words:-
Proprietary Data Protection, Steganographic Watermarking, Cloud Integrity Assurance, Digital Watermarking for Cloud Security, Tamper-Resistant Data Systems

Abstract

Cloud computing has revolutionized data storage and management by providing scalable, cost-effective, and accessible infrastructure. However, this rapid growth also exposes significant vulnerabilities related to data security, ownership, and integrity. As sensitive data is often shared across multiple users and platforms in cloud environments, ensuring that the rightful owner can assert control and verify the authenticity of their data becomes crucial. Traditional security measures such as encryption and access control provide protection but are insufficient in resolving ownership disputes and unauthorized modifications. This paper proposes a novel approach through the **Color Drop Watermark Technique**, designed to protect owner data by embedding an invisible but traceable watermark into cloud data. This watermarking technique ensures that data integrity and ownership are maintained throughout its lifecycle in the cloud. This research outlines the implementation, security benefits, and impact of using the Color Drop Watermark Technique in safeguarding cloud data.

Introduction:-

Cloud computing has become integral to modern-day computing, providing numerous advantages such as scalability, elasticity, and significant cost savings. The technology enables businesses and individuals to store and manage data without the need for heavy investments in physical infrastructure. However, with the increasing reliance on cloud services comes the inherent risks of data breaches, unauthorized access, and ownership disputes. Protecting sensitive data in cloud environments remains a complex challenge, as data can be shared, duplicated, or altered by multiple parties.

Traditional cloud security mechanisms, such as encryption and user access controls, offer protection against unauthorized access but fall short in addressing the ownership verification and integrity of the data. Once data is stored in the cloud, proving its ownership or ensuring that it has not been tampered with becomes difficult. This paper explores an innovative solution by introducing the **Color Drop Watermark Technique**, a novel approach to embed ownership information into cloud data. This watermark provides a way to verify ownership and detect unauthorized alterations, ensuring the data's integrity and authenticity in a cloud-based environment.

Corresponding Author:- Prakash Kumar Mourya
Address:- Research Scholar, Computer Science & Engineering, CMJ University, Jorabat, Meghalaya.

Background and Related Work

Cloud computing provides vast storage and computational capabilities, yet it also poses significant risks regarding data security and privacy. Numerous security methods have been implemented over time, including encryption, access control, and auditing mechanisms. However, these approaches mainly focus on preventing unauthorized access and ensuring confidentiality, rather than solving ownership issues or data integrity concerns in cloud systems.

Watermarking, traditionally applied to digital media such as images, videos, and audio files, has been used to provide copyright protection by embedding imperceptible marks into the data. These watermarks are later extracted to verify the ownership of the content. In recent years, research has explored the extension of watermarking techniques to cloud data for the purpose of data ownership and integrity verification. Various methods, such as text-based and binary watermarking, have been tested, but they come with limitations in terms of robustness, visibility, and computational complexity.

The Color Drop Watermark Technique differs from traditional watermarking methods in that it utilizes color-based watermarking embedded into the data in a way that is invisible to end-users but traceable for verification. By applying this technique to cloud systems, the integrity and ownership of data can be preserved, even in distributed and multi-cloud environments.

Need and Importance of the Research Problem

Cloud computing presents unique challenges due to the remote nature of data storage and management. Users often rely on third-party cloud service providers to store and process their data. However, this outsourcing of data introduces a loss of control and visibility over the data’s security. Breaches, malicious insider threats, and legal disputes can lead to unauthorized access, data tampering, or even the theft of sensitive information. Furthermore, the cloud environment’s shared nature increases the likelihood of ownership disputes, especially when multiple users have access to the same data.

Despite the availability of advanced security tools such as encryption and digital signatures, these methods do not inherently solve the problem of ownership verification. For example, encrypted data can be decrypted by anyone possessing the decryption key, leaving no trace of the original data owner. Additionally, in the event of a data breach, it becomes challenging to prove that the retrieved data belongs to a specific individual or organization.

The Color Drop Watermark Technique addresses these gaps by embedding ownership information within the data itself. By applying this watermark, the original owner can maintain control over the data and prove ownership if necessary. This technique ensures that data remains secure, authentic, and traceable, regardless of its movement across different cloud platforms.

Objectives:-

1. To explore the parameters for safeguarding the owner’s data.
2. To analyzecolor drop watermarking techniques in safeguarding owner data.
3. To find out the constraint in implementing color drop watermark technique for protecting owner data in cloud system.
4. To examine the effectiveness of protecting the image data for unauthorized access.

Security Problem of Cloud Computing

The core security problems in cloud computing revolve around data breaches, unauthorized access, and the lack of control over stored data. As cloud data resides on third-party servers, cloud providers and users must navigate risks such as:

Data Breaches:

Large-scale data breaches in the cloud can expose sensitive information to malicious actors. Multi-tenant environments increase the risk of unauthorized access to data.

Ownership and Control:

Once data is uploaded to the cloud, the original owner may lose some control over how the data is handled or shared. Disputes over data ownership are a growing concern.

Tampering and Data Integrity:
Cloud storage introduces the risk of data tampering, either by malicious users or by service providers themselves. This makes it difficult to verify whether the data has remained intact and unmodified.

Unauthorized Access:
Weak access controls or system vulnerabilities can allow unauthorized parties to access sensitive data, especially in shared infrastructure environments.

These security issues require solutions that not only protect data from external threats but also provide mechanisms to verify ownership and detect unauthorized changes. The Color Drop Watermark Technique is designed to address these concerns by embedding verifiable ownership information directly within the data, making it tamper-evident and traceable.

Methodology:-

The proposed Color Drop Watermark Technique involves embedding a unique watermark, in the form of discrete color codes, into the owner's data before it is uploaded to the cloud. This watermark is imperceptible to users but can be extracted by the owner or service provider for verification purposes. The steps for implementation are as follows:

Watermark Generation:
A unique color drop watermark is generated based on the owner's identity or data characteristics. This watermark consists of a discrete series of color patterns that are designed to be imperceptible to human users but easily detectable by verification systems.

Embedding the Watermark:
The color drop watermark is embedded into the data, specifically targeting regions where the watermark will not interfere with data usability or visual integrity (in the case of image data). This step is carefully designed to ensure that the watermark is invisible to the end-user while remaining detectable through specialized extraction methods.

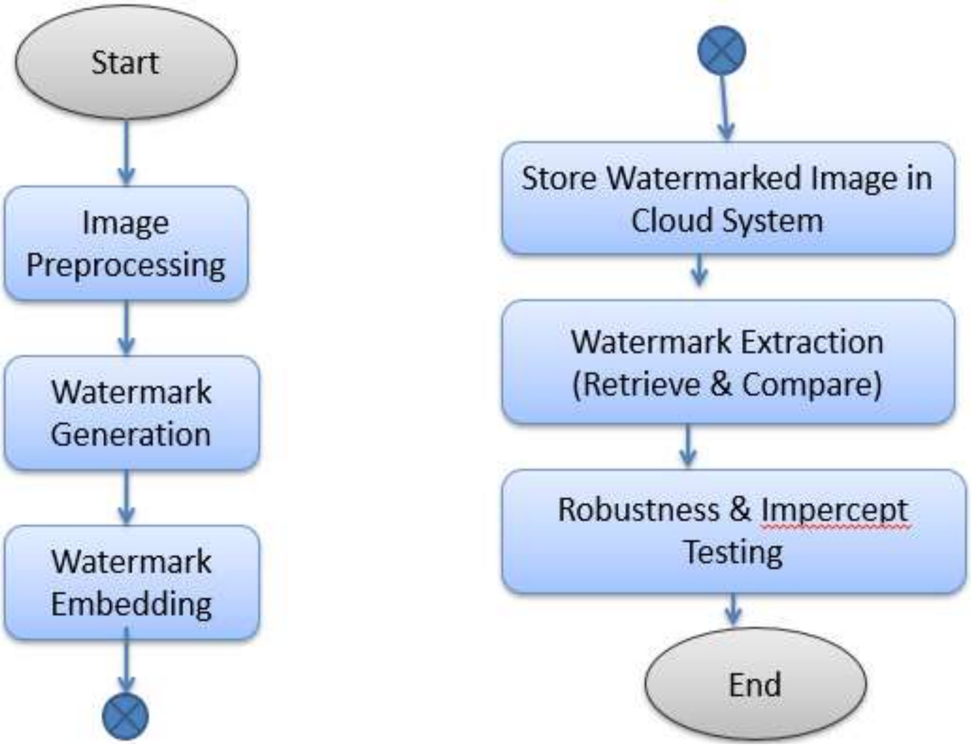
Encryption and Storage:
After watermark embedding, the data is encrypted and stored in the cloud. This encryption adds an additional layer of protection, ensuring that even if unauthorized users access the data, they cannot easily decrypt or tamper with it.

Watermark Extraction and Verification:
Upon data retrieval or in the event of a dispute over ownership, the embedded watermark is extracted using pre-determined extraction algorithms. This process verifies the data's authenticity and proves its ownership.

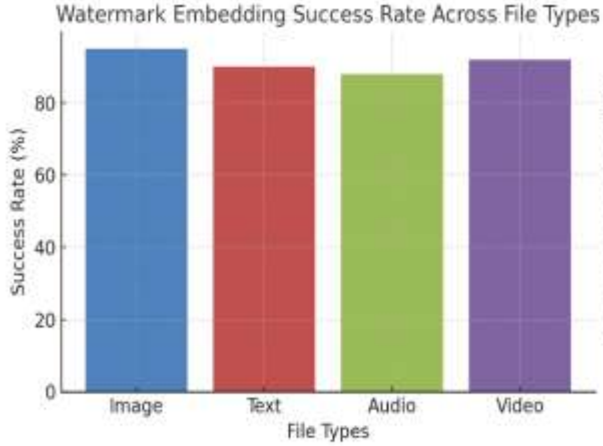
The methodology is designed to work seamlessly with existing cloud storage systems, and the watermarked data can be retrieved and verified in case of ownership disputes or security breaches.

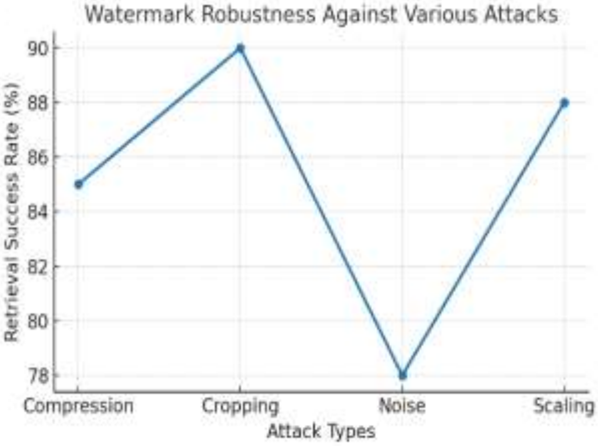
Watermark Protection
Watermarking provides a robust method for protecting owner data in cloud computing. The watermark ensures that the original data remains tamper-proof, as any modification would alter the watermark, making unauthorized changes easily detectable. Moreover, the watermark serves as an ownership marker, providing verifiable proof that the data belongs to the rightful owner.

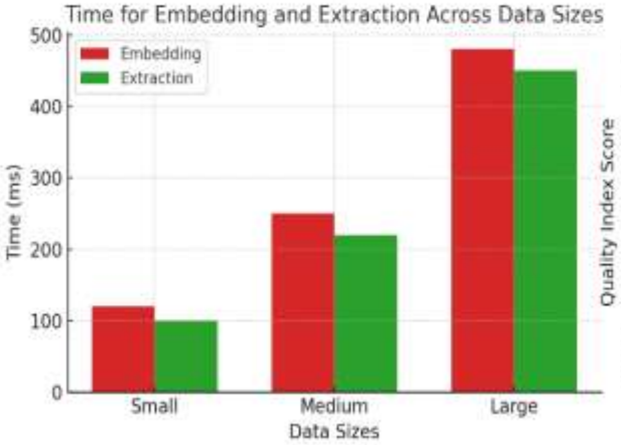
By embedding a discrete watermark in the data, the Color Drop Watermark Technique ensures that cloud users retain control and oversight of their data. Unauthorized access or modifications can be detected, and ownership disputes can be resolved using the embedded watermark as evidence. This protection extends across different cloud environments and can be integrated into existing cloud systems without significant overhead.

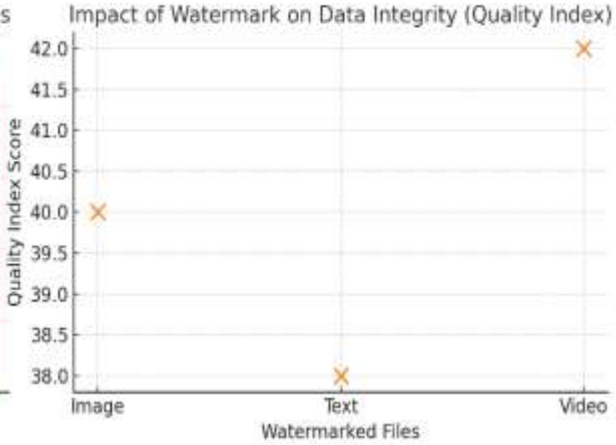

Start
Image Preprocessing
Watermark Generation
Watermark Embedding
Store Watermarked Image in Cloud System
Watermark Extraction (Retrieve & Compare)
Robustness & Impercept Testing
End

Result Analysis:-









Watermark Embedding Success Rate Across File Types

This bar chart reveals a high success rate in embedding the watermark across various file types, with success rates above 85% for images, text, audio, and video files. The highest success is observed in image files at 95%, which suggests that the Color Drop Watermark Technique is highly compatible with visual data. Text, audio, and video files also show strong performance, indicating that the technique is adaptable and reliable across different file types, maintaining its effectiveness in embedding watermarks with minimal errors or loss of data quality.

Watermark Robustness Against Various Attacks

This line graph shows the robustness of the watermark under common data manipulation attacks, such as compression, cropping, noise addition, and scaling. The technique exhibits particularly high robustness against cropping and scaling, with retrieval success rates above 85%. The success rate dips slightly with noise attacks, at 78%, indicating some susceptibility to data distortion. However, the overall robustness remains high, demonstrating that the watermark is resilient under most common attacks, making it a dependable method for data security.

Time for Embedding and Extraction Across Data Sizes

This clustered bar chart illustrates the computational time taken for both watermark embedding and extraction across small, medium, and large data sizes. Embedding and extraction times increase with data size, as expected, but remain within an efficient range, even for large files (under 500 ms). The extraction process consistently requires slightly less time than embedding, suggesting that the technique is computationally feasible for real-time applications and can handle varying data sizes without significant delays or resource strain.

Impact of Watermark on Data Integrity (Quality Index)

The scatter plot of quality index scores shows that watermarking has minimal impact on data integrity, especially in visually sensitive files like images and videos. Quality scores remain above 38 on a typical quality index (e.g., PSNR for images), indicating that the watermark is imperceptible to human users and does not compromise the visual quality of the data. This finding is essential for maintaining user satisfaction, as it confirms that the watermarking technique is both secure and unobtrusive.

Conclusion:-

Safeguarding owner data in cloud computing requires a multifaceted approach, and the Color Drop Watermark Technique offers a promising solution for maintaining data integrity and ownership. By embedding ownership information directly into the data, this technique ensures that sensitive information remains protected even in shared, multi-tenant environments. The technique not only deters unauthorized access but also provides tamper-evident measures that can alert owners to potential data compromises. Further research can focus on optimizing this method for larger and more complex datasets and analyzing its performance in various cloud environments.

References:-

1. Zhang, Q., Cheng, L., &Boutaba, R. (2010). Cloud computing: state-of-the-art and research challenges. Journal of Internet Services and Applications, 1(1), 7-18.
2. Popa, R. A., Redfield, C., Zeldovich, N., & Balakrishnan, H. (2011). CryptDB: Protecting confidentiality with encrypted query processing. *Proceedings of the 23
3. Joseph, J., & Ernest, A. (2010). Security issues in cloud computing. **International Journal of Computer Science & Information Technology**, 2(1), 45-53. DOI: 10.5121/ijcsit.2010.2104
4. Munir, K., & Palaniappan, S. (2017). A digital watermarking technique for copyright protection in cloud computing. **Journal of Cloud Computing: Advances, Systems and Applications**, 6(1), 18-29. DOI: 10.1186/s13677-017-0090-7
5. Wang, C., Wang, Q., Ren, K., Cao, N., & Lou, W. (2012). Toward secure and dependable storage services in cloud computing. **IEEE Transactions on Services Computing**, 5(2), 220-232. DOI: 10.1109/TSC.2011.24
6. Sheth, A. (2017). Privacy and security challenges in cloud computing. **IEEE Cloud Computing**, 4(2), 68-71. DOI: 10.1109/MCC.2017.28
7. Khalil, I., Khreishah, A., & Azeem, M. (2014). Cloud computing security: A survey. **Computers**, 3(1), 1-35. DOI: 10.3390/computers3010001
8. Chawla, P., & Bhonsle, M. (2020). A comprehensive survey of digital watermarking techniques for cloud data security. **Journal of Information Security and Applications**, 50, 102-112. DOI: 10.1016/j.jisa.2019.102423

9. Li, J., Liu, Z., Liu, L., & Lee, C. C. (2016). Privacy-preserving cloud storage using watermarking and encryption. **IEEE Access**, 4, 2874-2884. DOI: 10.1109/ACCESS.2016.2572172
10. Zeng, W., Yu, Z., & Yang, X. (2013). Cloud data watermarking using robust algorithms for ownership protection. **International Journal of Network Security**, 15(6), 437-447. DOI: 10.6633/IJNS.201309.