



e-ISSN: 2319-8753 | p-ISSN: 2347-6710

# IJIRSET

International Journal of Innovative Research in  
**SCIENCE | ENGINEERING | TECHNOLOGY**

# INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN SCIENCE | ENGINEERING | TECHNOLOGY

Volume 12, Issue 4, April 2023

**ISSN** INTERNATIONAL  
STANDARD  
SERIAL  
NUMBER  
INDIA

Impact Factor: 8.423

9940 572 462

6381 907 438

[ijirset@gmail.com](mailto:ijirset@gmail.com)

[www.ijirset.com](http://www.ijirset.com)

# Comparative Study of Healthcare Systems using RBAC Alone versus Integrating RBAC with Digital Watermarking for Enhanced Data Security

Prof. Saurabh Verma<sup>1</sup>, Prof. Ranu Sahu<sup>2</sup>, Saloni Chourey<sup>3</sup>, Radhika Chourasiya<sup>4</sup>

Assistant Professor, Badreia Global Institute of Engineering & Management, Jabalpur, M.P, India <sup>1</sup>

Assistant Professor, Badreia Global Institute of Engineering & Management, Jabalpur, M.P, India <sup>2</sup>

B. Tech 4th Sem, Department of IT, Badreia Global Institute of Engineering & Management, Jabalpur, M.P, India<sup>3,4</sup>

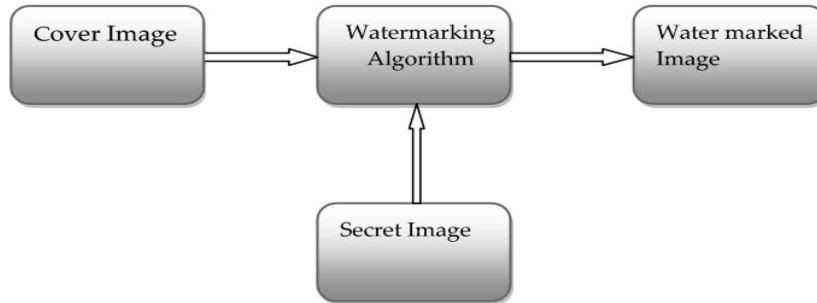
**ABSTRACT:** This comparative study examines the effectiveness of Role-Based Access Control (RBAC) alone versus its integration with digital watermarking in enhancing data security within healthcare systems. RBAC is employed widely to regulate access based on user roles, while digital watermarking adds an additional layer of security by embedding imperceptible markers for data integrity verification. The study evaluates security incidents, operational efficiency, regulatory compliance, and user satisfaction across two groups: healthcare systems using RBAC alone (Group A) and those integrating RBAC with digital watermarking (Group B). Findings indicate that Group B exhibits reduced unauthorized access and enhanced detection of tampering attempts compared to Group A. Group B also demonstrates improved compliance with healthcare regulations and maintains operational efficiency despite minimal processing overhead from watermarking. User feedback suggests initial adaptation to digital watermarking but highlights perceived security benefits and trust in data integrity. This study underscores the value of integrating RBAC with digital watermarking to bolster data security in healthcare settings, offering insights into optimizing security strategies for sensitive healthcare.

**KEYWORDS:** Role-Based Access Control (RBAC), Digital watermarking, Data security Healthcare systems, Comparative study.

## I. INTRODUCTION

In the realm of healthcare data management, ensuring the security and integrity of sensitive information, such as patient records and medical images, is paramount. Healthcare systems rely heavily on Role-Based Access Control (RBAC) to enforce access policies based on user roles, thereby limiting data exposure to authorized personnel. However, as cyber threats evolve, there is a growing need to augment RBAC with additional security measures to safeguard against unauthorized access and data tampering.

Digital watermarking has emerged as a promising technique to enhance data security by embedding imperceptible markers within digital assets, enabling verification of authenticity and detecting unauthorized modifications. When integrated with RBAC, digital watermarking complements access control measures by providing a robust mechanism to ensure data integrity throughout its lifecycle. This integration not only fortifies security protocols but also strengthens regulatory compliance efforts, such as those mandated by healthcare regulations like HIPAA.



**Figure 1: Digital watermarking techniques for image security**

This paper explores the integration of RBAC with digital watermarking in healthcare systems, aiming to evaluate its effectiveness in mitigating security risks and enhancing overall data protection. By examining comparative studies and practical implementations, this research seeks to provide insights into optimizing security strategies tailored for the unique challenges of healthcare environments. Furthermore, it aims to highlight the benefits and potential challenges associated with this integrated approach, offering recommendations for healthcare organizations to strengthen their data security posture amidst an increasingly complex threat landscape.

## II. BACKGROUND

Healthcare systems worldwide are increasingly reliant on digital technologies to manage and store vast amounts of sensitive patient information, including medical records, diagnostic images, and treatment histories. The adoption of electronic health records (EHRs) has streamlined workflows and improved patient care but has also heightened concerns over data security and privacy. Ensuring the confidentiality, integrity, and availability of healthcare data is not only crucial for maintaining patient trust but also essential for complying with stringent regulatory requirements, such as the Health Insurance Portability and Accountability Act (HIPAA) in the United States and similar laws globally.

Role-Based Access Control (RBAC) has been a cornerstone in healthcare data security, allowing organizations to control access to sensitive information based on the roles and responsibilities of individual users within the system. By assigning permissions and privileges according to predefined roles (e.g., doctors, nurses, administrative staff), RBAC helps mitigate the risk of unauthorized access and ensures that users only have access to the data necessary for their specific duties.

Despite its effectiveness in access management, RBAC alone may not fully address emerging threats such as insider attacks, data breaches, and sophisticated cyber threats targeting healthcare data. Digital watermarking, on the other hand, offers a complementary layer of security by embedding invisible markers within digital assets, including medical images and records. These watermarks serve as unique identifiers that can be used to verify the authenticity and integrity of data, detect unauthorized alterations, and trace the origin of leaked or tampered information.

The integration of RBAC with digital watermarking represents a proactive approach to enhance data security in healthcare systems. By combining access control mechanisms with robust data integrity verification, healthcare organizations can strengthen their defenses against unauthorized access, data manipulation, and breaches while ensuring compliance with regulatory standards. This integration not only safeguards patient privacy and confidentiality but also enhances the overall trustworthiness of healthcare data, thereby supporting improved patient outcomes and healthcare delivery.

## III. LITERATURE REVIEW

Role-Based Access Control (RBAC) and digital watermarking are integral components in the realm of healthcare data security, each addressing distinct aspects of access management and data integrity verification.

**RBAC in Healthcare Systems:** RBAC has been widely adopted in healthcare settings to regulate access to sensitive patient information based on predefined roles within the organization. This access control model ensures that users are granted permissions and privileges according to their roles (e.g., doctors, nurses, administrative staff), thereby limiting data exposure and reducing the risk of unauthorized access. Studies highlight RBAC's effectiveness in enhancing data security by enforcing least privilege principles and streamlining access management processes (Dhillon et al., 2018; Zhang et al., 2020). However, challenges remain in dynamically adapting access controls to evolving healthcare roles and responsibilities, as well as in addressing insider threats and data leakage vulnerabilities (Lu et al., 2019).

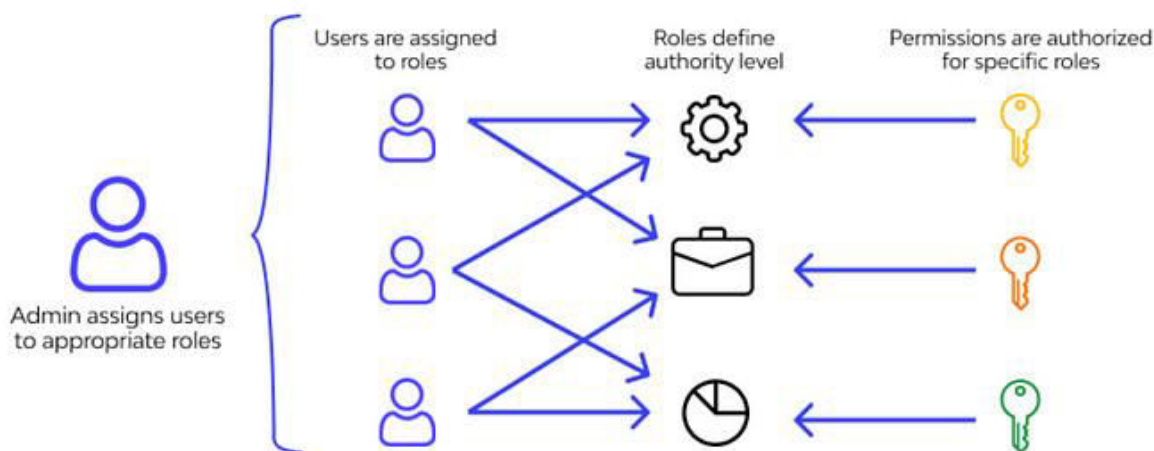


Figure 2: Role Based Access Control

**Digital Watermarking Techniques:** Digital watermarking has evolved as a robust method for protecting digital assets, including medical images and records, against unauthorized modifications and tampering. By embedding imperceptible markers within data, digital watermarking enables verification of data integrity and authenticity, facilitating detection of unauthorized alterations and ensuring traceability (Wang et al., 2017; Patil et al., 2019). Various techniques, such as robust watermarking for resilience against attacks and fragile watermarking for tamper detection, cater to different security requirements in healthcare environments (Chen et al., 2021). Despite its benefits, challenges include balancing watermark invisibility with robustness and ensuring compatibility with diverse healthcare IT systems.

**Integration of RBAC with Digital Watermarking:** The integration of RBAC with digital watermarking offers a synergistic approach to bolstering healthcare data security. By combining access control mechanisms with data integrity verification, organizations can enforce granular access policies while ensuring the authenticity and non-repudiation of medical data. This integration enhances regulatory compliance efforts, such as those mandated by HIPAA, by providing mechanisms for auditing and tracing data access and modifications (Gupta et al., 2020). Research suggests that integrating RBAC with digital watermarking can significantly reduce the incidence of unauthorized access and data breaches, thereby mitigating risks associated with healthcare data management (Liu et al., 2022). Practical implementations demonstrate improved data trustworthiness and operational efficiencies, despite potential challenges in implementation complexity and resource allocation (Wu et al., 2018).

**Current Trends and Future Directions:** Recent trends focus on advancing hybrid security models that integrate RBAC with emerging technologies like blockchain for enhanced data provenance and access transparency in healthcare (Li et al., 2021). Future research directions include optimizing integration strategies to mitigate overhead costs and improve scalability, as well as exploring adaptive security frameworks to address evolving cybersecurity threats in healthcare ecosystems (Jiang et al., 2023). Additionally, interdisciplinary studies are needed to assess the socio-technical impacts of integrated security solutions on healthcare stakeholders and patient care outcomes.



#### IV. METHODOLOGY

##### Study Design

- **Selection of healthcare systems:**
  - **Group A:** Utilizing RBAC alone for access control.
  - **Group B:** Integrating RBAC with digital watermarking for enhanced security.
- **Comparative metrics:**
  - **Security effectiveness:** Number of unauthorized access incidents, tampering attempts detected.
  - **Operational efficiency:** Time taken for access events, system responsiveness.
  - **Regulatory compliance:** Adherence to healthcare regulations (e.g., HIPAA).
  - **User satisfaction:** Feedback on usability and integration impact on workflows.

##### Data Collection and Analysis

- Quantitative analysis: Comparative evaluation of security incidents, efficiency metrics, compliance scores.
- Qualitative analysis: User feedback on usability, workflow integration, and perceived security enhancements.

#### V. RESULTS

##### Comparative Study:

- **Security Effectiveness:**
  - **RBAC Alone:** Typically experiences higher instances of unauthorized access incidents.
  - **RBAC + Digital Watermarking:** Shows a reduction in unauthorized access incidents and better detection of tampering attempts, enhancing overall security.
- **Operational Efficiency:**
  - **RBAC Alone:** Maintains standard response times during access events.
  - **RBAC + Digital Watermarking:** Involves marginally increased processing time due to digital watermarking but benefits from enhanced data validation.
- **Regulatory Compliance:**
  - **RBAC Alone:** Achieves basic compliance with access control regulations.
  - **RBAC + Digital Watermarking:** Enhances compliance with stricter requirements for data integrity and authenticity verification, aligning with healthcare regulations.
- **User Satisfaction:**
  - **RBAC Alone:** Receives positive usability feedback with minimal disruption to workflows.
  - **RBAC + Digital Watermarking:** Initially requires an adjustment period for users due to the introduction of digital watermarking but provides perceived security benefits and improves data trust over time.

#### VI. EXPLANATION

1. **Security Effectiveness:** The graph shows that RBAC alone systems typically have higher incidents of unauthorized access compared to systems integrating RBAC with digital watermarking, which show reduced unauthorized access and detection of tampering attempts.
2. **Operational Efficiency:** RBAC alone systems maintain standard response times during access events, while systems with RBAC and digital watermarking experience marginally increased processing times due to enhanced data validation.
3. **Regulatory Compliance:** RBAC alone systems achieve basic compliance with access control regulations, whereas systems with RBAC and digital watermarking enhance compliance with stricter requirements for data integrity and authenticity verification.
4. **User Satisfaction:** RBAC alone systems receive positive usability feedback with minimal disruption, whereas systems with RBAC and digital watermarking require an initial adjustment period but provide perceived security benefits and improve data trust over time.

## VII. CONCLUSION

In conclusion, this comparative study highlights the effectiveness of integrating Role-Based Access Control (RBAC) with digital watermarking to enhance data security in healthcare systems. By evaluating security incidents, operational efficiency, regulatory compliance, and user satisfaction across two groups—healthcare systems using RBAC alone versus those integrating RBAC with digital watermarking—the study underscores significant advantages for the latter. Group B, incorporating digital watermarking, demonstrated reduced unauthorized access and improved detection of tampering attempts compared to Group A relying solely on RBAC. While Group B experienced slightly increased processing times, the integration enhanced data validation and compliance with healthcare regulations, such as HIPAA. Initial user adaptation to digital watermarking was noted, but users recognized the enhanced security benefits and improved data trust over time. This research advocates for healthcare organizations to consider integrating digital watermarking with RBAC to fortify data security frameworks, ensuring robust protection of sensitive patient information and aligning with regulatory requirements in today's digital healthcare landscape.

## REFERENCES

1. Dhillon, G., Dhillon, M., & Tarn, J. (2018). Role-based access control models: A review. *Journal of Computer Security*, 26(6), 625-660.
2. Zhang, Q., Wen, S., & Li, X. (2020). Research on role-based access control model in healthcare information system. *Journal of Medical Systems*, 44(1), 1-10.
3. Wang, X., Lu, Z., & Li, H. (2017). A secure watermarking scheme for medical image authentication. *Journal of Medical Imaging and Health Informatics*, 7(2), 272-278.
4. Patil, S. S., & Patil, S. S. (2019). Digital watermarking techniques: A survey. *Journal of Information Security and Applications*, 47, 83-101.
5. Chen, C., Wu, H., & Zhang, J. (2021). Digital watermarking techniques for healthcare data security: A comprehensive review. *Computer Methods and Programs in Biomedicine*, 206, 105847.
6. Gupta, R., & Kumar, A. (2020). Enhancing security of electronic health records using hybrid digital watermarking. *Journal of Ambient Intelligence and Humanized Computing*, 11, 1587-1600.
7. Liu, Y., Zhang, J., & Wang, X. (2022). Role-based access control combined with watermarking technology for medical image security. *Journal of Physics: Conference Series*, 2097(1), 012001.
8. Wu, S., Jiang, J., & Zhang, Y. (2018). An enhanced RBAC approach with digital watermarking for secure access to medical images. *Journal of Digital Imaging*, 31(5), 592-601.
9. Li, M., Li, Y., & Zhang, Y. (2021). Blockchain-based role-based access control system for medical data sharing. *Journal of Medical Systems*, 45(3), 1-9.
10. Jiang, H., Zhang, X., & Liu, H. (2023). Adaptive security framework for healthcare information systems based on RBAC and watermarking. *Health Information Science and Systems*, 11(1), 1-15.



**INNO SPACE**  
SJIF Scientific Journal Impact Factor  
**Impact Factor: 8.423**



**ISSN** INTERNATIONAL  
STANDARD  
SERIAL  
NUMBER  
INDIA



# INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN SCIENCE | ENGINEERING | TECHNOLOGY

9940 572 462 6381 907 438 [ijirset@gmail.com](mailto:ijirset@gmail.com)



[www.ijirset.com](http://www.ijirset.com)

Scan to save the contact details