International Journal of Information Technology & Computer Engineering

ISSN 2347–3657

Volume 13, Issue 4, 2025

Digital Data Security Through Watermarking

P Ganeh Kumar[1], Lahari Vaddireddy[2], Manya sree Godavari[3], Meghana Anugu[4]

[1]Assistant Professor, Department Of Information Technology, Bhoj Reddy Engineering College For Women, India.

[2,3,4]B. Tech Students, Department Of Information Technology, Bhoj Reddy Engineering College For Women, India.

vaddireddylahari@gmail.com, maaanyasri@gmail.com, meghanareddy1306@gmail.com

ABSTRACT

It is believed that watermarking is a technology tha t enables the protection of various media data against unlawful or improper re-use .Hawkins brought up the several watermarking methods that have been developed for copyright an intellectual property protection in the literature, but many media data use various digital water marking methods. Additionally, due to various functions and applications, different watermarking systems have distinct technological requirements. This project aims to promote digital watermarking and presents a framework for electronic business designers and developers to employ watermarking in securing their online media contents since intellectual property protections utilizing digital watermarking is still in it's infancy.

Keywords*: Digital Data Security, Watermarking, Multimedia.*

1-INTRODUCTION

Digital data security is of paramount importance in today's interconnected world. With the increasing reliance on digital media and the ease of sharing information online, protecting sensitive data from unauthorized access, copying, or tampering has become a significant concern. One approach to enhance digital data security is through the use of watermarking techniques.Watermarking is a method that allows information to be embedded into digital content, such as images, audio, video, or documents, in a way that is imperceptible to human observers. These embedded watermarks serve as a form of hidden identification or proof of ownership, enabling the detection of unauthorized use or manipulation of the content. Watermarking can be applied for various purposes, including copyright protection, authentication, tamper detection, and forensic analysis. In the 18th century watermarks appeared in America and Europe they where used in money and as trade marks .The term watermark was used to clarify the effect of water on the paper .Digital watermarks are messages embedded in a multimedia work such as an image or text or other digital objects. This can be achieved through various techniques, such as altering pixel values in images, modifying audio frequencies, or subtly manipulating document attributes.

Existing System:

Recent research trend in watermarking technique has been focusing on text data but watermarking is not limited to text documents; there are also watermarking techniques for images and video data .Watermarking for black and white text data; e.g., electronic documents and manuscripts, is so-called binary watermarks, and is similar to visual cryptography, which was a technique proposed for information hiding, another watermarking technique, such as Coxetal. Targets a wide spectrum of media data, but only the fundamental concepts of the technique are given.

Proposed System:

By In this Application we are going to implement water mark pattern for all the different types of media like images ,video and different kinds of text data

- Add image as watermark for text data.
- Add image as watermark for image data.
- Add text data as watermark for text data.
- Protects video data by providing a private key for the user.

2.RELATED WORK

To support the development of a personalized and data-driven career guidance system, a comprehensive review of existing approaches was undertaken. To develop a reliable watermarking system for digital data security, a structured review of existing watermarking techniques was conducted. This includes studying current methodologies, identifying research gaps, and exploring key areas of improvement.

3.REQUIREMENT ANALYSIS

Functional Requirements:

Functional requirement should include function performed by a specific screen outline work-flows performed by the system and other business or compliance requirement the system must meet. Functional requirements specify which output file should be produced from the given file they describe the relationship between the input and output of the system, for each functional requirement a detailed description of all data inputs and their source and the range of valid inputs must be specified.

The functional specification describes what the system must do, how the system does it is described in the design specification. If a user requirement specification was written, all requirements outlined in the user requirements specifications should be

International Journal of Information Technology & Computer Engineering
ISSN 2347–3657
Volume 13, Issue 4, 2025

addressed in the functional requirements.

Admin :

- login
- view user and owner list
- Add watermark
- Logout

Owner:

- Registration
- Login
- Upload watermark
- Upload files
- Delete Files
- Logout

Non-Functional Requirements:

Describe user-visible aspects of the system that are not directly related with the functional behavior of the system. Non-Functional requirements include quantitative constraints, such as response time (i.e., how fast the system reacts to user commands.) or accuracy (e. how precise are the systems numerical answer)

4. DESIGN

System Architecture:

It describes the structure and behavior of technology infrastructure of an enterprise, solution or system. In other words, System architecture can be described as the flow of application which is represented below in the pictorial form. He purpose of system architecture activities is to define a comprehensive solution based on principles, concepts, and properties logically related to and consistent with each other. The solution architecture has features, properties, and characteristics which satisfy, as far as possible, the problem or opportunity expressed by a set of system requirements (traceable to mission/business and stake holders requirements).

System architecture is abstract, conceptualization-oriented, global, and focused to achieve the mission and life cycle concepts of the system. It also focuses on high-level structure in systems and system elements. It addresses the architectural principles, concepts, properties, and characteristics of the system-of-interest. It may also applied to more than one system, in some cases forming the common structure, pattern, and set of requirements for classes or families of similar or related systems.

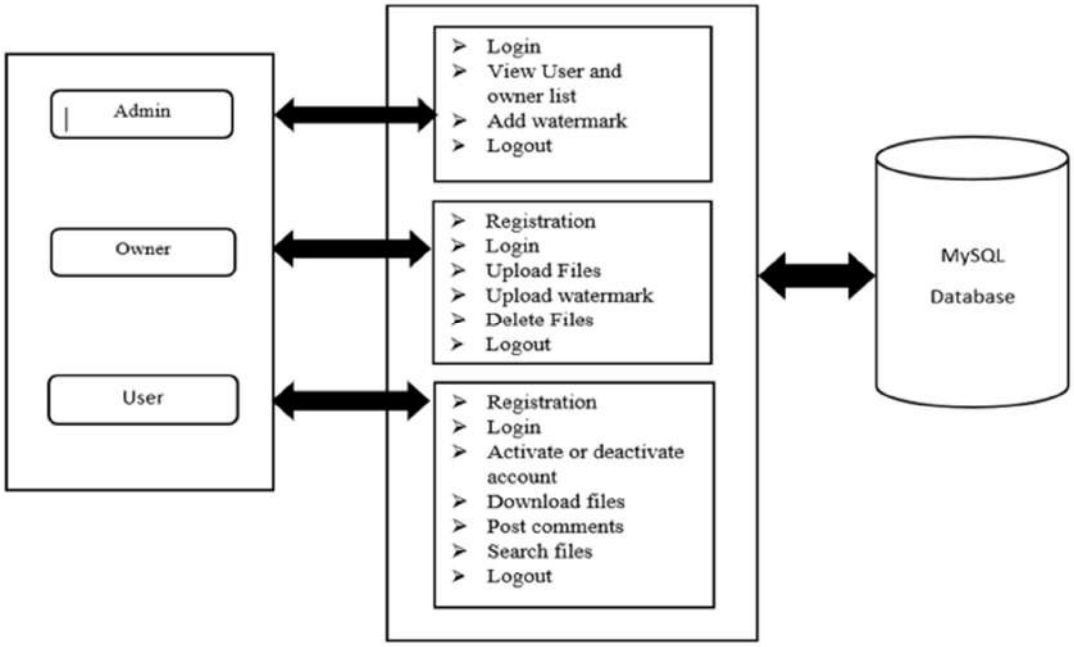


Fig. 1 System Architecture

Technical Architecture:

Technical Architecture refers to the structural process of designing and building system's architecture with focus on the users and sponsors view of the environment. Technology architecture associates application components from application architecture with technology components representing software and hardware components. Its components are generally acquired in the market place and can be assembled and configured to constitute the enterprise's technological infrastructure. A technical architecture diagram provides a bird's eye view of the infrastructure of our project. The diagram illustrates how components in a system interact with one another in the large scale of things. Technical Architecture (TA) is a form of IT architecture that is used to design computer systems. It involves the

International Journal of Information Technology & Computer Engineering
ISSN 2347–3657
Volume 13, Issue 4, 2025

development of a technical blueprint with regard to the arrangement, interaction, and interdependence of all elements so that system-relevant requirements are met.

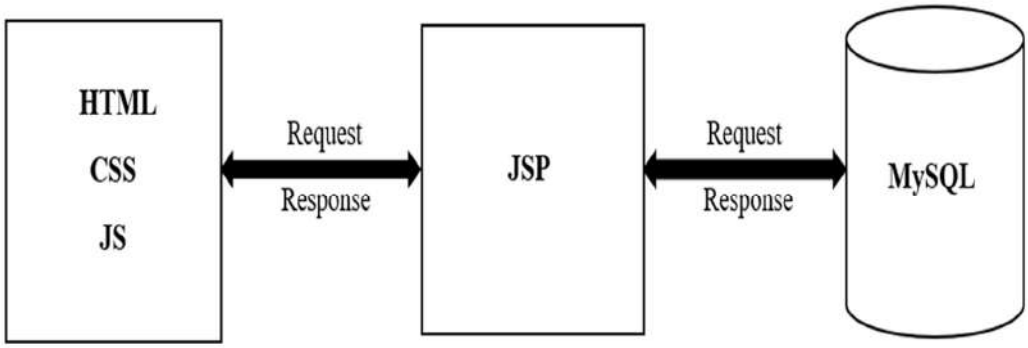


Fig. 2 Technical Architecture

Methodology:
The proposed methodology implements watermark design patterns to protect digital content in e-commerce applications. It focuses on embedding visible and invisible watermarks into various media types—text, images, and video—to prevent unauthorized use, duplication, or distribution. The system consists of three core modules: Admin, Data Owner, and Gut User. The Admin manages users and system settings. Data Owners upload content and apply appropriate watermarking methods, while Guest Users access publicly available watermarked content.
Digital watermarking begins by generating a unique key that combines copyright data, product details, and user profiles. This key is transformed into a digital watermark using a hashing function or random generator, producing a sequence of watermark bits. The watermark is then embedded into the host media using signal processing techniques. For images and videos, visible watermarks (e.g., logos) are placed using overlay methods, while invisible watermarks are embedded within the content to enable traceability. Video protection also includes a private key mechanism for secure access.
The system is developed using Python, Django, OpenCV, and SQLite. It follows the Spiral Model of software development for iterative refinement and risk management. Watermarking techniques are optimized for robustness and transparency, ensuring that they are difficult to remove without damaging the media quality.
Comprehensive testing—including unit, integration, and system testing—is performed to ensure the system's reliability and performance. Perceptual watermarking principles are applied to adapt watermark strength based on content characteristics and human sensory perception. The overall design ensures content protection, copyright assertion, and deterrence against piracy. The architecture is scalable and suitable for real-world applications where intellectual property protection is critical.

5.IMPLEMENTATION

Libraries

- ***Datetime***
  The datetime library in Python is used to work with dates and times. It allows capturing the current date and time, formatting date strings, and performing date/time arithmetic. In applications like watermarking, it's used to timestamp posts or comments, helping track when actions occurred for record-keeping or display.
- ***Random***
  The random library in Python is used to generate random numbers and perform random operations. It provides functions like randint(), choice(), and shuffle() for tasks such as creating OTPs, selecting random items, or shuffling data. It's useful in applications requiring unpredictability, like security features or simulations.
- ***Smtplib***
  The smtplib library in Python is used for sending emails using the Simple Mail Transfer Protocol (SMTP). It allows applications to connect to email servers, authenticate, and send messages. Commonly used for sending OTPs or notifications, it supports secure connections via TLS or SSL for safe email communication.
- **Django. shortcuts. render**
  The django. shortcuts. render function is a convenient method in Django to combine a template with a context dictionary and return an HTTP response. It simplifies rendering HTML pages by automatically loading the template, filling it with dynamic content, and returning it to the client. This function enhances code readability and efficiency

International Journal of Information Technology & Computer Engineering

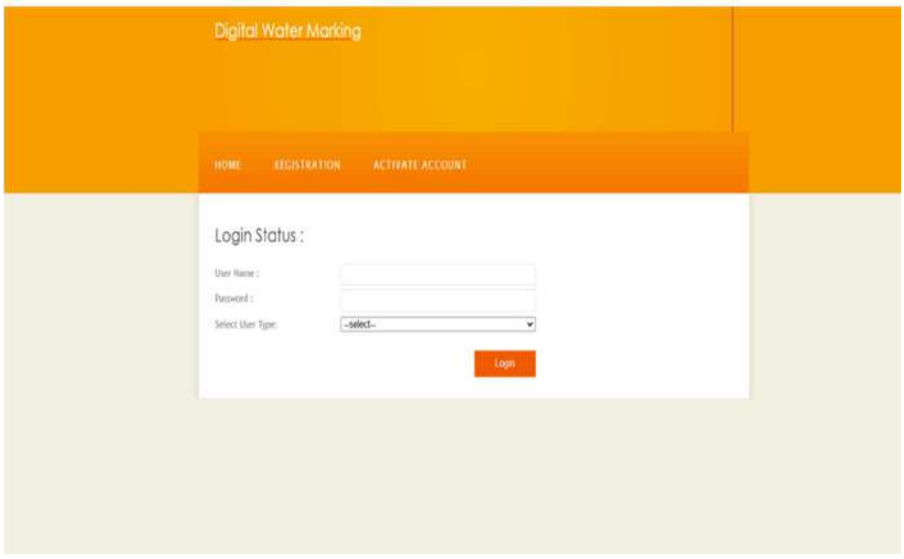
ISSN 2347–3657

Volume 13, Issue 4, 2025

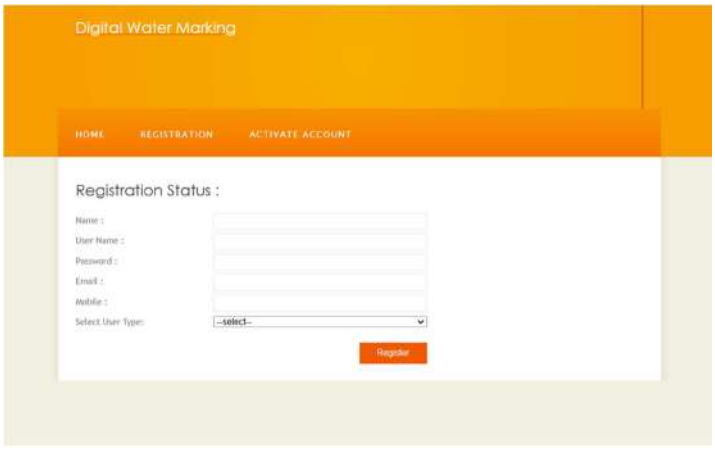
by reducing the need to manually load templates and create HttpResponse objects. It's commonly used in views to display webpages.

- **Request. POST / request. GET:** request. POST and request. GET are Django objects used to access data submitted by users through forms. request. POST retrieves data sent via HTTP POST method, typically from form submissions involving sensitive actions like login or registration. request. GET fetches data from the URL query string, often used in search or filtering. Both return dictionary-like objects that allow you to extract input values by field names. They are essential for handling user inputs and building interactive, data-driven web applications in Django.

6. SCREENSHOTS

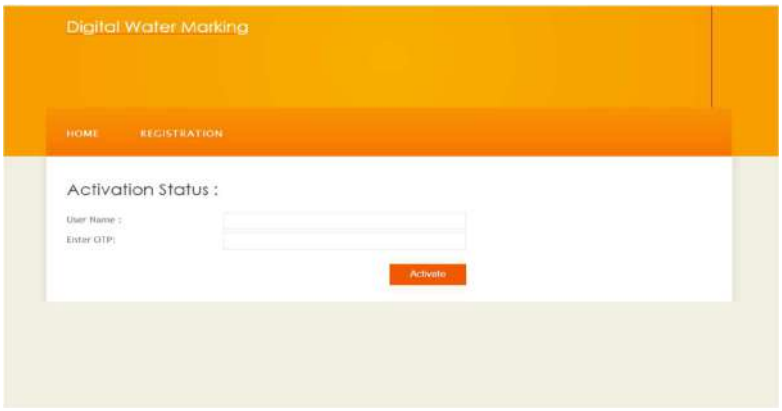


Screenshot 1: Home Page

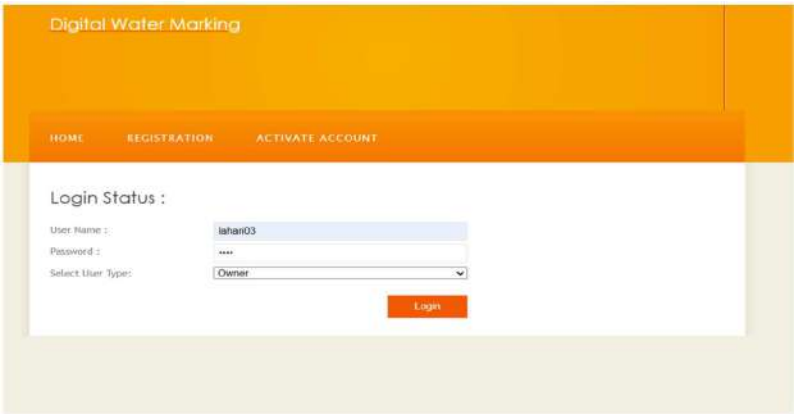


Screenshot 2: Registration Page

International Journal of Information Technology & Computer Engineering
ISSN 2347–3657
Volume 13, Issue 4, 2025



Screenshot 3: Activation status



Screenshot 4: Login Status

8. CONCLUSION

In conclusion, watermarking is a vital technology that plays a significant role in various domains, including digital media, copyright protection, security, and content authentication. It provides a means to embed and extract information within digital content, such as images, videos, and audio, without compromising the content's quality or functionality. Watermarking offers several key benefits:

1.Copyright Protection: Watermarks are essential for protecting the intellectual property of content creators by providing a clear indicator of ownership and authorship. They serve as a deterrent to unauthorized copying and distribution.

Content Authentication: Watermarks enable the verification of the authenticity and integrity of digital content. They help in establishing the source and history of content, which is crucial in legal and forensic contexts.

Content Tracking: Watermarking is instrumental in monitoring the distribution and usage of digital media, allowing for tracking and reporting of unauthorized or infringing use. This is especially important in the age of the internet and social media.

Deterrence and Prevention: Watermarks act as a deterrent to potential infringers. Knowing that their actions can be traced back to the source, individuals and entities may be less inclined to engage in unauthorized use of copyrighted content.

10. REFERENCES

1. Cox, I. J., Kilian, J., Leighton, T., & Shamoon, T. (1997). Secure spread spectrum watermarking for multimedia. IEEE Transactions on Image Processing

2. Swanson, M. D., Zhu, B., & Tewfik, A. H. (1998). Transparent robust image watermarking. In Proceedings of the International Conference on Image Processing (ICIP) (Vol. 3, pp. 211-215). IEEE.

3. Kutter, M., & Jordan, M. (2002). Watermarking resistance classes: Attacks and counterattacks. IEEE Transactions on Image Processing

4. Podilchuk, C. I., & Zeng, W. (2001). A perceptual watermark for digital images. IEEE Transactions on Image Processing

5. Fridrich, J., Goljan, M., & Du, R. (2001). Lossless data embedding—new paradigm in digital watermarking. EURASIP Journal on Applied Signal Processing