

AquaGuard

Project Synopsis Submitted

to

MANIPAL ACADEMY OF HIGHER EDUCATION

For Partial Fulfilment of the Requirement for the

Award of the Degree

Of

Bachelor of Technology

in

Computer and Communication Engineering

by

Sinjini Kar, Disha Gomes, Ryan Gupta

Reg. No. 230953136, Reg. No. 230953010, Reg. No. 230953288

Under the guidance of

Dr. Divya Rao
Associate Professor
School of Computer Engineering
Manipal Institute of Technology
MAHE, Manipal, Karnataka, India

Dr. Yogesh Ganapati Chandavakar
Lab Co Faculty
School of Computer Engineering
Manipal Institute of Technology
MAHE, Manipal, Karnataka, India



MANIPAL INSTITUTE OF TECHNOLOGY

MANIPAL

A Constituent Unit of MAHE, Manipal

August 2025

Objective:

To design and implement a comprehensive digital watermarking and copyright protection system that ensures intellectual property security through invisible watermark embedding and robust verification mechanisms. The project utilizes LSB Steganography combined with AES encryption for secure watermark insertion and SHA-3 hashing for content integrity verification, providing creators with a reliable tool to protect their digital assets.

Scope:

This project delivers a web-based platform that enables content creators, photographers, artists, and organizations to protect their digital intellectual property. The system supports multiple file formats (images: JPEG, PNG, BMP; documents: PDF) and implements advanced cryptographic techniques including Least Significant Bit (LSB) steganography, Advanced Encryption Standard (AES) encryption, and SHA-3 hashing. The scope encompasses both watermark embedding capabilities and comprehensive verification tools to detect tampering or unauthorized usage.

Need for the Application:

In today's digital era, intellectual property theft is a growing concern, and visible watermarks are easily removed. **AquaGuard** provides **invisible watermarking** that preserves content quality, ensures **cryptographic security**, and survives common image processing. It enables creators and businesses to **prove ownership**, detect tampering, maintain integrity, and perform **easy verification** through a secure, user-friendly platform.

Project Description:

AquaGuard is a web-based digital watermarking system that provides secure copyright protection through a structured workflow.

1. User Registration & Authentication: AquaGuard begins with secure user registration, including email verification for account authenticity. Passwords are protected with **SHA-3 hashing** to prevent brute-force and rainbow table attacks. Users can manage profiles to track watermark ownership, ensuring proper attribution and accountability.

2. Watermark Embedding Process: Users can upload images (JPEG, PNG, BMP) or PDF documents. The system generates a unique watermark containing user ID, timestamp, copyright information, and a digital signature. The watermark is encrypted using **AES-256** and embedded using **LSB steganography** for images or metadata embedding for PDFs. A **SHA-3 hash** is generated for integrity, and both the watermark metadata and hash are stored securely in the database.

3.Verification & Detection: Uploaded files suspected of containing watermarks undergo **LSB extraction**. The watermark is decrypted with stored keys, and its integrity is verified using **SHA-3 hash comparison**. Ownership details are cross-checked with database records, and a detailed verification report is generated showing authenticity and any detected tampering.

4.Security Features: Watermarks remain **invisible**, ensuring content quality is unaffected. Any modification triggers **integrity violations**. **AES-256 encryption** protects watermark data from extraction, and timestamped records provide **legal proof of ownership**.

Functionalities implemented:

- Multi-format support: JPEG, PNG, BMP, PDF
- Invisible watermarking with LSB steganography
- AES-256 encryption and SHA-3 hashing for security and integrity
- Web interface for upload and verification
- Batch processing and RESTful verification API
- Detailed verification reports and user dashboard for tracking protected files

Hardware Requirements:

- **Processor:** Intel i5 or AMD Ryzen 5 (minimum)
- **RAM:** 8 GB or above (16 GB recommended)
- **Storage:** 1 TB HDD/SSD for file storage

Software Requirements:

- **Operating System:** Linux Ubuntu 20.04+ or Windows Server
- **Programming Language:** Python 3.9+
- **Database:** PostgreSQL or MongoDB
- **Languages:** HTML5, CSS3, JavaScript
- **Framework:** React.js or Vue.js
- **UI Library:** Bootstrap or Material-UI

Submitted by

Name	Registration number	Roll Number	Semester & Branch	Section
Sinjini Kar	230953136	15	V (CCE)	D
Disha Gomes	230953010	4	V (CCE)	D
Ryan Gupta	230953288	30	V (CCE)	D