**HIDDEN WATERMARKING: A STEGANOGRAPHIC APPROACH TO COPYRIGHT PROTECTION**

|  |  |
| --- | --- |
|  |  |

**TABLE OF CONTENTS**

|  |  |  |
| --- | --- | --- |
| 1. | Abstract | 1 |
| 2. | Introduction | 5 |
| 3. | Literature Review | 7 |
| 4. | Problem Identification & Objectives | 11 |
| 5. | System Methodology | 13 |
| 6. | Overview of Technologies | 16 |
| 7. | Implementation | 18 |
| 8. | Results & Discussions | 24 |
| 9. | Conclusion & Future Scope | 36 |
| 10 | References | 37 |

**1.ABSTRACT**

In today's digital age, the rapid proliferation of multimedia content, such as images, audio, and video, has led to an unprecedented surge in copyright infringement. Protecting the intellectual property rights of creators has become a paramount concern. This project proposes a novel approach to safeguarding digital content with the help of hidden watermarks, leveraging the field of steganography.

Steganography, the art and science of concealing information within seemingly innocuous carrier files, offers an effective means to embed imperceptible watermarks into multimedia content. These hidden watermarks serve as digital fingerprints, allowing content creators and rights holders to assert ownership and trace the unauthorized distribution of their intellectual property.

This research project delves into the following key aspects:

**Steganographic Techniques:** We explore various steganographic techniques, including frequency domain, spatial domain, and transform domain methods, to determine the most suitable approach for embedding watermarks. Each technique's effectiveness in terms of imperceptibility and robustness against common attacks is assessed.

**Watermarking Algorithms:** The study evaluates watermarking algorithms to ensure the integrity and resilience of the hidden watermarks. We analyze different algorithms for their capacity to withstand compression, cropping, and other common image manipulations while remaining undetectable to the human eye.

**Detection and Authentication:** To complete the copyright protection cycle, we develop robust watermark detection and authentication methods. These methods enable rights holders to verify the presence of their watermark and confirm the authenticity of their content.

**Security Analysis:** The project conducts a comprehensive security analysis, addressing potential vulnerabilities and countermeasures to protect against attacks aimed at removing or altering the hidden watermarks.

**Real-World Applications:** We discuss practical applications of hidden watermarks in various domains, such as digital media, e-commerce, and content sharing platforms. Additionally, we examine legal and ethical considerations surrounding the use of steganography for copyright protection.

By harnessing the power of steganography to embed hidden watermarks, this project aims to provide content creators and rights holders with an effective and unobtrusive means of safeguarding their digital assets. The findings of this research contribute to the ongoing efforts to preserve intellectual property rights in the digital era, fostering a secure and sustainable digital content ecosystem.

**Algorithm used is LSB algorithm**

In the LSB (Least Significant Bit) steganographic algorithm, the primary key used is the Embedding Key. This key specifies the method and pattern for hiding data within the least significant bits of the pixel values in a digital image. It typically includes information such as:

**Bit Selection:** The embedding key defines which specific bits (usually the least significant bits) of the pixel values should be altered to encode the hidden data.

**Data Encoding:** It may specify how the hidden data should be encoded into the selected bits, whether it's a simple binary encoding or more complex methods like Huffman coding or arithmetic coding.

**Data Length:** The key can also include information about the length of the hidden data or where to find the end of the embedded message.

**Encryption (Optional):** Some LSB implementations may include encryption of the hidden data using a separate encryption key. In such cases, the encryption key is also required for both embedding and extraction.

**Embedding Algorithm Parameters:** Depending on the LSB variant and specific implementation, the embedding key may include additional parameters related to the algorithm, such as the order of pixel traversal or how to handle special cases.

The LSB (Least Significant Bit) algorithm is a steganographic technique used to hide information within digital images, audio, or other multimedia files. It works by modifying the least significant bits of the pixel values in an image or the least significant bits of audio samples to encode the hidden data. Here's a simplified overview of how the LSB algorithm works:

**Encoding (Embedding):**

**Select Bits:** In the encoding process, you choose a specific number of the least significant bits (LSBs) in the pixel values that will be used to hide the information. For example, you might choose to use the two least significant bits from each color channel (RGB) in an image.

**Convert Data:** If you are hiding text or binary data, you convert it into a binary format.

**Embed Data:** You replace the selected LSBs of the pixel values with the bits of your hidden data. This replacement is typically done sequentially or in a predetermined order.

**Adjust LSBs:** To ensure that the changes are subtle and do not visibly alter the image, you may need to make slight adjustments to the LSBs to maintain the image's overall appearance.

**Decoding (Extraction):**

**Select Bits:** During extraction, you select the same LSBs that were used for embedding.

**Extract Data:** You read the LSBs from the image or audio samples to reconstruct the hidden data.

**It is important to note that while LSB steganography is relatively straightforward to implement, it has limitations:**

**Capacity vs. Visibility:** Increasing the amount of hidden data (payload) may result in visible artifacts in the image, which can raise suspicion.

**Security:** LSB steganography is not highly secure. It is relatively easy to detect the presence of hidden data if someone is actively looking for it.

**Robustness:** LSB-encoded data may be lost or altered when the image undergoes common compression or editing processes

**Select the Bits:**

Decide how many bits per channel (per color) you want to use for hiding data. A common choice is to use the least significant bits (LSBs) because they are less visually significant.

For example, you can choose to use the two LSBs from each color channel. This means you will modify the last two bits of each pixel value in the selected channels to hide your data.

**Types of bits:**

**1-Bit LSB:** In this scenario, you replace only the least significant bit of each pixel value with the bit of your hidden data. This provides a very low data-hiding capacity and is least likely to cause noticeable changes in the cover image or audio. However, it is also the least secure and easiest to detect.

**2-Bit LSB:** Using two LSBs per pixel value allows for a slightly higher data-hiding capacity while still maintaining relatively low visibility. The changes to the image or audio are typically subtle, but it may be more robust against minor compression or editing.

**3-Bit LSB:** Steganography with three LSBs provides a higher data capacity, but it becomes more noticeable in the cover media. It may still appear visually acceptable to the human eye but can be more susceptible to detection.

**4-Bit LSB and Higher:** As you increase the number of LSBs used for data hiding, the data capacity increases, but the visibility of changes in the cover media becomes more apparent. Higher LSB values may be more susceptible to detection and may result in visible artifacts.

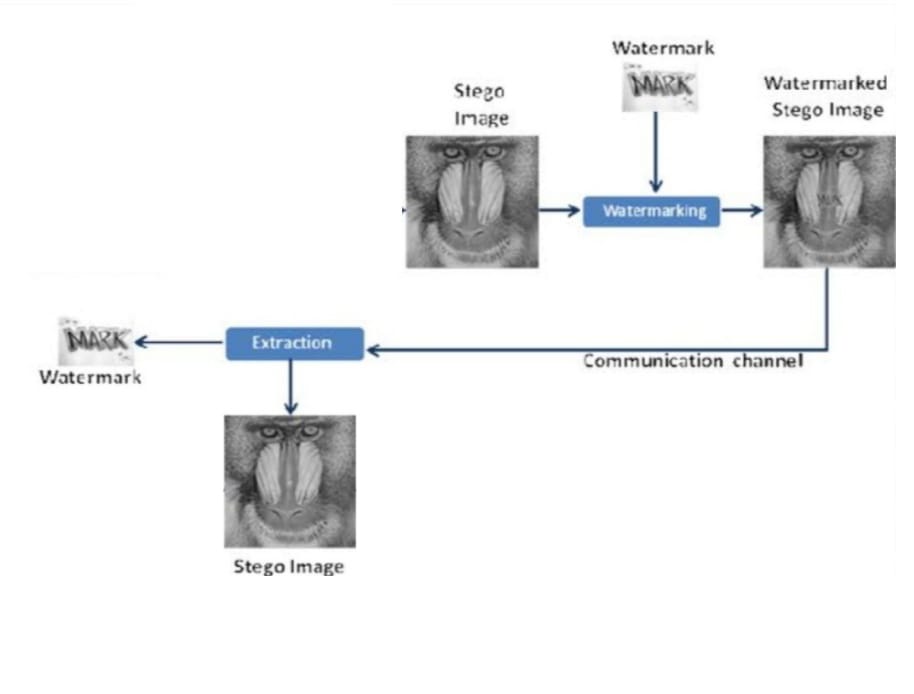


Fig1.1: Steps for steganography watermarking

The figure 1.1 represents the visualization of the project

**2. INTRODUCTION**

The aim of the project "HIDDEN WATERMARKS: A STEGANOGRAPHIC APPROACH TO COPYRIGHT PROTECTION" is to develop and implement a steganographic system that leverages hidden watermarks as a means of safeguarding digital content and protecting copyright.

**The project aims to achieve the following objectives:**

**Digital Content Protection:** Develop a robust and effective method for embedding hidden watermarks within multimedia content, such as images, audio, and video, without significantly degrading the quality or perceptibility of the content.

**Copyright Verification:** Enable content creators and rights holders to assert and verify ownership of their intellectual property through the detection and authentication of hidden watermarks.

**Security and Robustness:** Enhance the security of the watermarking technique, making it resilient against common attacks aimed at removing or altering the embedded watermarks. Ensure the watermark's persistence in the presence of compression, cropping, and other image manipulations.

**Practical Applications:** Explore practical applications of hidden watermarks in various domains, such as digital media distribution, e-commerce, and content sharing platforms, to provide a tangible solution for protecting digital content.

**Legal and Ethical Considerations:** Investigate the legal and ethical aspects of using steganography and hidden watermarks for copyright protection, ensuring compliance with relevant laws and ethical standards.

**User-Friendly Implementation:** Develop user-friendly tools or software that enable content creators and copyright owners to easily embed and verify hidden watermarks in their digital assets.

**Education and Awareness:** Raise awareness about the importance of copyright protection and educate stakeholders, including content creators, consumers, and policymakers, about the benefits and ethical considerations of using steganography for this purpose.

By achieving these objectives, the project seeks to contribute to the ongoing efforts to preserve intellectual property rights in the digital era and create a more secure and sustainable environment for the creation and distribution of digital content.

**2.1 CHALLENGES**:

Implementing a project like "Hidden Watermarks: A Steganographic Approach to Copyright Protection" involves various technical, ethical, and practical challenges.

**Here are some of the key challenges you may encounter:**

**Security:** Protecting the watermark from unauthorized removal or alteration is essential. Determining effective encryption and authentication methods to secure the watermark against malicious attacks can be challenging.

**Steganalysis:** Developing techniques to detect the presence of hidden watermarks by potential infringers is crucial. Steganalysis is an ongoing arms race, and staying ahead of detection techniques can be a challenge.

**Legal and Ethical Considerations:** Understanding and navigating the legal and ethical aspects of copyright protection through steganography can be complex. Different jurisdictions have varying laws and regulations related to copyright infringement, digital rights management, and privacy.

**Performance Overhead**: Implementing watermarking and steganographic techniques can introduce performance overhead in multimedia processing, potentially affecting the speed and efficiency of content distribution systems.

**3. LITERATURE REVIEW**

# The paper titled "A Survey on Image Steganography Techniques Using Least Significant Bit" by Bhavani et al. (2022) provides a comprehensive literature survey of image steganography methods, focusing specifically on techniques utilizing the least significant bit (LSB) approach. The authors present an in-depth analysis of various LSB-based steganography algorithms, their strengths, weaknesses, and applications. Through a systematic review, the paper explores the evolution of LSB steganography, discussing classical methods as well as recent advancements. By examining the advantages and limitations of different approaches, the survey offers insights into the effectiveness, security, and robustness of LSB-based steganographic techniques in concealing information within digital images. Additionally, the paper discusses emerging trends, challenges, and potential future directions in the field, contributing valuable insights to researchers, practitioners, and stakeholders involved in the development and deployment of image steganography systems. [1]

# The paper titled "Image feature-based watermarking" by Alexan et al. presents a comprehensive literature survey on watermarking techniques, focusing specifically on image feature-based methods. The survey explores various approaches and algorithms utilized in embedding watermarks into digital images, leveraging characteristics such as color histograms, texture features, and geometric attributes. The authors provide an overview of existing research in the field, highlighting key advancements, challenges, and emerging trends in image watermarking. Additionally, the paper delves into the theoretical foundations underlying feature-based watermarking, discussing the principles of robustness, imperceptibility, and capacity. Through an analysis of recent studies and experimental findings, the authors offer insights into the performance and effectiveness of different watermarking techniques under varying conditions and attack scenarios. This literature survey serves as a valuable resource for researchers and practitioners seeking to gain a deeper understanding of image watermarking methods and their applications in digital content protection and copyright enforcement.[2]

# The paper by Wan et al. (2022) presents a comprehensive survey on robust image watermarking techniques, providing valuable insights into the state-of-the-art methods employed to embed and extract watermarks in digital images effectively. Through an extensive literature review, the authors explore various aspects of robust image watermarking, including algorithmic approaches, evaluation metrics, and challenges faced in achieving robustness against common attacks such as noise addition, compression, and geometric transformations. The survey encompasses both traditional and contemporary watermarking algorithms, discussing their strengths, limitations, and applicability in real-world scenarios. Furthermore, the paper delves into emerging trends and advancements in the field, such as deep learning-based watermarking techniques, which offer promising opportunities for enhancing robustness and scalability. By synthesizing existing research findings and highlighting future research directions, Wan et al. provide a valuable resource for researchers, practitioners, and stakeholders interested in advancing the field of image watermarking for applications ranging from copyright protection to content authentication.[3]

The paper by Michaylov and Sarmah (2024) explores the application of steganography and steganalysis techniques in enhancing forensic analysis of digital images. Through a comprehensive literature survey, the authors provide an overview of existing methodologies, algorithms, and tools utilized in steganography for concealing information within digital images, as well as steganalysis for detecting such hidden content. They delve into various aspects including embedding techniques, cover image selection, payload capacity, and robustness against attacks. Furthermore, the paper evaluates the effectiveness of steganographic methods in evading detection by steganalysis techniques and discusses their implications for forensic investigations. By synthesizing insights from prior research, the authors offer valuable recommendations for improving the reliability and efficiency of digital image forensic analysis in detecting concealed information. The study contributes to the advancement of cyber security technology by addressing the challenges posed by covert communication channels and facilitating the development of more sophisticated tools for digital image forensics and anti-steganalysis measures.[4]

The paper titled "Image Watermarking Using Least Significant Bit and Canny Edge Detection" by Faheem et al. presents a literature survey that explores the utilization of least significant bit (LSB) embedding technique combined with Canny edge detection for image watermarking. The authors likely delve into existing research in the field of image watermarking, focusing on methodologies and approaches employed by previous studies to embed and extract watermarks in digital images. They may discuss various techniques such as LSB embedding, which involves replacing the least significant bit of pixel values with watermark data to achieve imperceptible alterations in the image, as well as Canny edge detection, which can enhance robustness and security by embedding the watermark in edge regions. The survey likely highlights the strengths and limitations of different watermarking techniques, their applicability in different scenarios, and the challenges encountered in achieving robust and imperceptible watermarking. Additionally, it may discuss recent advancements, emerging trends, and areas for further research in the domain of image watermarking, providing valuable insights for researchers and practitioners in the field.[5]

The paper by Hameed, Abdel-Aleem, and Hassaballah (2023) presents a comprehensive literature survey focusing on a secure data hiding approach employing least-significant-bit (LSB) and nature-inspired optimization techniques. By integrating LSB with nature-inspired optimization, the study explores innovative methods for enhancing data security and confidentiality. The survey delves into existing research on data hiding, covering various aspects such as steganography, cryptography, and optimization algorithms. It reviews prior works that have utilized LSB embedding and extraction methods, highlighting their strengths and limitations in terms of robustness, imperceptibility, and resistance against attacks. Additionally, the paper examines the integration of nature-inspired optimization techniques, such as genetic algorithms, particle swarm optimization, and simulated annealing, to improve the efficiency and effectiveness of data hiding processes. Through a critical analysis of the literature, the authors identify gaps and challenges in current approaches and propose novel strategies to address them. Overall, the literature survey serves as a valuable resource for researchers and practitioners in the field of data security, providing insights into recent advancements and guiding future directions for developing more secure and robust data hiding techniques.[6]

The paper titled "On Estimating Uncertainty of Fingerprint Enhancement Models," authored by Joshi et al. (2023), presents a comprehensive literature survey on the topic within the broader context of digital image enhancement and reconstruction. The authors delve into the critical aspect of uncertainty estimation, specifically focusing on fingerprint enhancement models. Through their survey, they elucidate the various methodologies, techniques, and advancements in this field, providing valuable insights into the challenges and opportunities associated with uncertainty quantification in fingerprint enhancement. By examining a range of existing approaches, the paper offers a nuanced understanding of the complexities involved in enhancing the quality and reliability of fingerprint images. Moreover, the authors explore the implications of uncertainty estimation for practical applications, such as forensic analysis and biometric authentication systems. Overall, this literature survey serves as a pivotal resource for researchers and practitioners seeking to navigate the intricacies of fingerprint enhancement and its associated uncertainties within the realm of digital image processing. [7]

The paper titled "CONCEAL: A Robust Dual-Color Image Watermarking Scheme" by Luo et al. presents a comprehensive literature survey on the development and application of watermarking techniques, focusing specifically on dual-color image watermarking. The authors delve into the existing methodologies, advancements, and challenges in the field, offering a critical analysis of various approaches proposed by researchers. Through their survey, they highlight the importance of robustness, imperceptibility, and security in watermarking schemes, especially in the context of dual-color images. The paper provides insights into the evolution of watermarking techniques, ranging from traditional methods to more sophisticated algorithms, and discusses their effectiveness in different scenarios. Furthermore, the authors identify gaps in the current research landscape and propose their watermarking scheme, CONCEAL, as a novel solution to address these challenges. Overall, the paper serves as a valuable resource for researchers and practitioners in the field of digital watermarking, offering a comprehensive overview of the state-of-the-art techniques and paving the way for future advancements in the domain. [8]

The paper authored by Hasan et al. (2021) presents a comprehensive literature survey on encryption-based image watermarking algorithms operating in the 2DWT-DCT domains. The authors delve into the existing body of research, evaluating various methodologies, techniques, and approaches employed in the field of image watermarking. Through their survey, they elucidate the strengths, weaknesses, and advancements in encryption-based watermarking schemes within the context of the 2DWT-DCT domains. By synthesizing findings from diverse studies, the paper contributes to a deeper understanding of the state-of-the-art techniques and their applicability in ensuring robustness, security, and imperceptibility of watermarked images. The literature survey conducted by Hasan et al. serves as a valuable resource for researchers and practitioners engaged in the development and enhancement of watermarking algorithms, paving the way for further innovations in the realm of image security and copyright protection. [9]

The paper titled "A DWT-SVD based robust digital watermarking for medical image security" by Zermi et al. (2021) presents a comprehensive literature survey focused on digital watermarking techniques tailored specifically for enhancing the security of medical images. The authors delve into the domain of discrete wavelet transform (DWT) and singular value decomposition (SVD) as fundamental components of their proposed watermarking scheme. Through their survey, they explore the efficacy of existing methods, analyzing their strengths and limitations in preserving the integrity and confidentiality of medical imagery. By synthesizing insights from prior research, the paper establishes a foundation for the development of a novel watermarking approach that leverages the combined power of DWT and SVD to embed imperceptible yet robust watermarks into medical images. This survey not only offers a comprehensive overview of the state-of-the-art techniques but also highlights the necessity and potential advancements in the field of medical image security, thereby contributing to the broader landscape of forensic science and healthcare data protection.[10]

**4. PROBLEM IDENTIFICATION AND OBJECTIVES**

**4.1. PROBLEM DEFINITION:**

Problem identification is a crucial step in any research project, including "Hidden Watermarks: A Steganographic Approach to Copyright Protection." It involves clearly defining the issues or challenges that your project aims to address.

Here are some problem identification points for your project:

**Digital Copyright Infringement:** The unauthorized distribution and sharing of copyrighted digital content, such as images, audio, and videos, have become rampant. This project aims to tackle the problem of copyright infringement in the digital age.

**Lack of Effective Protection:** Existing copyright protection mechanisms may not provide sufficient security and deterrence against copyright violations. This project seeks to develop a more robust and effective solution for protecting copyrighted digital content.

**Data Privacy Concerns:** In some cases, traditional copyright protection methods can compromise user privacy by collecting extensive personal data. There is a need for copyright protection techniques that respect user privacy while still deterring infringement.

**Steganographic Detection Advances:** Steganalysis techniques, which are used to detect hidden information in multimedia content, have become more sophisticated. This project must address the challenge of staying ahead of advancements in steganographic detection methods.

**4.2. OBJECTIVE:**

The main objective for the project "Hidden Watermarks: A Steganographic Approach to Copyright Protection" is to develop and implement an effective and secure steganographic solution for safeguarding digital content copyrights.

**This project aims to achieve several specific objectives:**

**User Experience:** Minimize the impact on the user experience while still providing effective copyright protection, so consumers can enjoy multimedia content without significant disruptions.

**Performance:** Optimize the performance of the watermarking process to minimize processing overhead and latency during content distribution.

**Detection Prevention:** Develop countermeasures to prevent or deter attackers from detecting and removing the hidden watermarks.

**Scalability:** Design the solution to be scalable and applicable to various types of digital media, including images, audio, and video.

**Documentation and Education:** Create documentation and educational resources to help content creators, rights holders, and users understand how to use and benefit from the watermarking system.

**5. SYSTEM METHODOLOGY**

**5.1. PROPOSED METHODOLOGY:**

**5.1.1 Project Initiation:**

Define the project's objectives and scope, including the types of multimedia content (e.g., images, audio, video) to be protected and the expected level of copyright protection.

Establish a clear understanding of the legal and ethical considerations relevant to copyright protection and steganography.

**5.1.2 Literature Review:**

Conduct a comprehensive literature review to understand the current state of steganography, watermarking, and copyright protection in digital media.

Identify existing methodologies, techniques, and best practices.

**5.1.3 Requirement Analysis:**

Define the specific requirements for your copyright protection system, including:

Data capacity requirements (how much metadata can be embedded).

Desired robustness against common image/audio processing operations.

Security requirements (e.g., encryption of embedded data).

Legal and ethical compliance.

**5.1.4 Data Pre-processing:**

Prepare the multimedia content (cover media) for watermark embedding. This may involve resizing, compression, and format conversion while ensuring minimal loss of quality

**5.1.5 Watermark Generation:**

Generate unique watermarks or identifiers that will be embedded in the multimedia content. These watermarks should be designed to be imperceptible but easily detectable when needed.

**5.1.6 Embedding Process:**

Implement the steganographic algorithm to embed the watermark into the cover media. The algorithm should adhere to the LSB or another chosen method based on the project's requirements.

Consider encryption and authentication techniques to protect the watermark's integrity.

**5.1.7 Quality Assurance:**

Conduct thorough testing and quality assurance to ensure that the embedded watermarks do not significantly degrade the visual or auditory quality of the multimedia content.

Assess the robustness of the watermarked content against common image/audio processing operations and potential attacks.

**5.1.8 Extraction and Authentication:**

Develop methods for extracting and authenticating the hidden watermarks from the protected multimedia content.

Ensure that the watermark extraction process is both accurate and secure.

**5.1.9 Security Assessment:**

Evaluate the security of the watermarking system, including the encryption and authentication mechanisms.

Test the system against potential attacks, such as steganalysis or unauthorized watermark removal.

**5.1.10 Performance Evaluation:**

Measure the system's performance in terms of data capacity, robustness, and perceptual quality.

Compare the results to the project's requirements and objectives.

**5.1.11 Documentation and Reporting:**

Document the entire methodology, including algorithms, parameters, and test cases.

Prepare a detailed report summarizing the project's findings, methodology, and outcomes.

**5.1.12 Legal Compliance:**

Ensure that the copyright protection system complies with applicable copyright laws and regulations.

**5.1.13 Future Improvements:**

Identify areas for future improvements and research in the domain of steganographic copyright protection.

**5.1.14 Deployment and Integration:**

If the system is intended for practical use, develop deployment strategies and integration plans into relevant platforms or industries.

**5.2. WORKING ARCHITECTURE:**

**5.2.1 Watermark Generation:**

In this step, a watermark is created, typically consisting of some digital data or information that uniquely identifies the owner or source of the content. It could be a text string, a logo, or some other information.

The watermark should be robust enough to withstand common signal processing operations (like compression, cropping, and resizing) and attacks (like noise addition or filtering) without being easily destroyed or altered.

**5.2.2 Embedding:**

The next step is to embed the watermark into the multimedia content. This is done by modifying the content in a way that is not easily detectable by human observers but can be recovered later using the watermark extraction process.

The embedding algorithm determines how the watermark data is integrated into the multimedia content. The key is to find a balance between robustness and imperceptibility.

**5.2.3 Steganography Techniques:**

Steganography methods are often used in the embedding process to hide the watermark efficiently. Common techniques include Least Significant Bit (LSB) substitution, spread spectrum, or frequency domain methods.

These techniques ensure that the watermark becomes a part of the host content in a way that is difficult for unauthorized users to detect.

**5.2.4 Storage or Distribution:**

The watermarked content can be stored, distributed, or transmitted as usual. It appears to viewers or listeners as the original content with no apparent alterations.

**5.2.5 Detection and Extraction:**

To verify the presence of the watermark and extract it, one needs access to the watermarked content and knowledge of the watermarking algorithm and key (if used).

The detection process involves analysing the content to identify the watermark's presence and possibly its location and strength.

The extraction process retrieves the watermark data from the content, which can then be used for various purposes, such as copyright infringement detection or content authentication.

**5.2.6 Robustness and Security:**

The watermarking system should be designed to be robust against common signal processing operations and attacks, while also maintaining security to prevent unauthorized removal or tampering with the watermark.

Encryption and authentication mechanisms may be used to protect the watermark or the information it carries.

**5.2.7 Usage:**

The extracted watermark information can be used for various purposes, such as proving ownership, tracking unauthorized copies, or monitoring the distribution of copyrighted content.

**6. OVERVIEW OF TECHNOLOGIES**

**6.1. HARDWARE REQUIREMENTS:**

**Computer System:**

A computer system capable of running the required software for steganography and watermarking.

Sufficient processing power to handle image and video processing tasks efficiently.

Adequate RAM for working with large multimedia files.

Sufficient storage space for storing datasets, multimedia files, and project-related data.

**Display Monitor:**

A high-resolution display monitor for viewing and analyzing images and multimedia content.

**Input Devices:**

Standard input devices such as a keyboard, mouse, and/or graphics tablet for interacting with software tools.

**Storage Devices:**

External storage devices (e.g., external hard drives, SSDs) for backup and archiving of multimedia files and project data.

**Network Connection:**

An internet connection may be necessary for accessing online resources, downloading datasets, or collaborating.

**6.2. SOFTWARE REQUIREMENTS:**

Libraries and Modules used are:

**6.2.1 numpy is imported as np:** NumPy is a fundamental package for scientific computing with Python, enabling operations on large, multi-dimensional arrays and matrices.

**6.2.2 matplotlib.pyplot is imported as plt:** Matplotlib is a plotting library for Python, and pyplot provides a MATLAB-like interface for creating plots and visualizations.

**6.2.3 tkinter.filedialog**: tkinter.filedialog is imported, and specifically, the askopenfilename function is imported from it: Tkinter is the standard GUI toolkit for Python, and filedialog module provides dialogs for file selection. askopenfilename is used to prompt the user to select a file using a dialog box.

**6.2.4 cv2:** OpenCV (OpenSource Computer Vision Library) is a library of programming functions mainly aimed at real-time computer vision. Here, cv2 module is imported for computer vision operations.

**6.2.5 matplotlib.image is imported as mpimg:** This module provides functions to read and write image files. mpimg is used for reading and displaying images.

**6.2.6 warnings:** Python's built-in warnings module provides functions for issuing warning messages to alert the user about potential issues or non-critical problems in the code.

**6.2.7 from matplotlib import pyplot as plt:** Matplotlib is a Python library for creating static, interactive, and animated visualizations. "plt" is a commonly used alias for the pyplot module, providing a simple interface for creating plots and visualizations.

**6.2.8 from skimage import img\_as\_float:**img\_as\_float is a function from the scikit-image (skimage) library in Python used to convert an image to a floating-point representation, typically ranging from 0.0 to 1.0, which is often useful for image processing tasks.

**6.2.9 from PIL import Image:**"from PIL import Image" is a Python statement that imports the Image module from the Python Imaging Library (PIL), which is a library used for opening, manipulating, and saving many different image file formats.

# 7. IMPLEMENTATION

# 7.1 Software Implementation:

INPUT IMAGE

INPUT IMAGE

# 

Image Resizing

# 

Gray Scale Conversion

Image preprocessing

Bilinear Interpolation

Image Enhancement

Contrast Stretching

# 

Histogram Equalization

# 

# 

# 

# Fig 7.1.1: Flowchart for software implementation

**7.1.1 Image Processing:**

Image processing plays a crucial role in embedding and extracting digital watermarks within multimedia content. This process involves manipulating the pixel values of images to conceal copyright information in a manner that is imperceptible to human perception but detectable through specialized algorithms. Here's how image processing is typically utilized in such a project:

**Embedding Watermarks:** Image processing techniques are employed to embed copyright watermarks into digital images. This involves altering specific pixel values in the image to incorporate hidden information. Techniques like least significant bit (LSB) substitution, discrete cosine transform (DCT), and spread spectrum are commonly used for this purpose. These techniques ensure that the watermark is integrated seamlessly into the image while maintaining its visual quality.

**Detecting and Extracting Watermarks:** Image processing algorithms are utilized to detect and extract the embedded watermarks from watermarked images. These algorithms analyze the image to identify the presence of hidden information and retrieve it accurately. Techniques such as correlation analysis, statistical analysis, and frequency domain analysis are employed to locate and extract the watermark without causing any noticeable degradation to the image quality.

**Enhancing Robustness and Security:** Advanced image processing methods are employed to enhance the robustness and security of the embedded watermarks. Techniques such as error correction coding, cryptographic hashing, and digital signatures may be integrated into the watermarking process to protect against unauthorized tampering or removal of the watermark. These methods ensure the integrity and authenticity of the copyright information embedded within the digital content.

**Evaluation and Quality Assessment:** Image processing techniques are utilized for evaluating the effectiveness and quality of the watermarking process. Objective metrics such as peak signal-to-noise ratio (PSNR), structural similarity index (SSIM), and bit error rate (BER) are often used to assess the perceptual quality and robustness of watermarked images. Additionally, subjective evaluations involving human observers may be conducted to gauge the visual impact of the embedded watermarks on image quality.

**7.1.2 Gray Scale conversion:**

Gray scale conversion is pivotal in augmenting the effectiveness and imperceptibility of the watermarking process. It entails converting a color image into a gray scale format, where the intensity of each pixel is denoted by a single value spanning from 0 (representing black) to 255 (indicating white).

The integration of gray scale conversion into the watermarking process offers several advantages:

**Simplified Complexity:** Gray scale images possess a singular channel, simplifying the watermark embedding and extraction procedures in contrast to the complexities associated with multi-channel color images.

**Enhanced Robustness:** Gray scale images exhibit resilience against color variations and distortions, thereby fortifying the watermark against prevalent image processing operations like compression, resizing, and filtering.

**Augmented Imperceptibility:** Watermarks imprinted within gray scale images tend to evade detection by human observers more effectively, seamlessly blending into the overall intensity variations of the image.

**Enhanced Compatibility:** Gray scale images enjoy widespread support across diverse platforms and devices, ensuring seamless integration into prevailing systems and applications.

**7.1.3 Image Interpolation:**

Bilinear interpolation is pivotal in bolstering the quality and durability of embedded watermarks within digital content. Through the utilization of bilinear interpolation techniques, the project endeavors to refine the visual integrity and perceptual excellence of watermarked images or videos, thus ensuring minimal distortion to the original content while embedding imperceptible watermarks. Bilinear interpolation entails the estimation of new pixel values by averaging the values of adjacent pixels, facilitating smoother transitions and more authentic alterations. By integrating bilinear interpolation into the watermarking process, the project enables a more seamless embedding and extraction of watermarks, fortifying the resilience of copyrighted materials against illicit tampering or dissemination. Furthermore, by fine-tuning interpolation parameters such as kernel size and method, the project can achieve a delicate equilibrium between watermark invisibility and robustness, thereby strengthening the efficacy of steganographic techniques in shielding digital assets from infringement.

Bilinear interpolation is used in this project

**7.1.3.1 Bilinear Interpolation:**

Bilinear interpolation serves as a valuable tool within the realm of hidden watermarking, primarily aimed at bolstering the visual quality of watermarked images. In the embedding phase, where a watermark is integrated into an image, pixel alterations may inadvertently introduce visual artifacts or degrade image quality. By employing bilinear interpolation during this process, the transitions between adjacent pixels can be smoothed, yielding a more seamless integration of the watermark while minimizing perceptible changes to the overall image. This enhancement not only preserves the integrity of the original content but also enhances the visual appeal of the watermarked image.

Furthermore, bilinear interpolation finds utility in the extraction phase of hidden watermarking, facilitating the accurate recovery of embedded watermarks from watermarked images. Through interpolation of pixel values within the watermarked image, the distinction between the original content and the embedded watermark is clarified, fortifying the robustness and reliability of the extraction process. Ultimately, the integration of bilinear interpolation into hidden watermarking methodologies contributes to elevating the visual quality and fidelity of watermarked images, thus amplifying the efficacy of copyright protection mechanisms in safeguarding digital content.

**7.1.4 Image Enhancement:**

Image enhancement is integral to bolstering the quality and resilience of the hidden watermarking process. Employing various techniques, it refines the visual presentation of both the original content and the embedded watermark, maintaining imperceptibility to human observers while fortifying integrity against potential threats. Preprocessing enhances the original content's visual fidelity, mitigating imperfections and augmenting details to optimize the subsequent watermark embedding. During this embedding phase, sophisticated methods such as frequency domain manipulation and spread spectrum embedding are leveraged to conceal the watermark effectively, ensuring resilience against compression, cropping, and noise addition. Furthermore, post-processing techniques are instrumental during watermark extraction, refining the quality and accuracy of the extracted watermark through noise filtering and correlation-based detection, thereby bolstering its visibility and readability in the extracted content. Overall, image enhancement serves as a linchpin in fortifying the hidden watermarking approach, fortifying its effectiveness in safeguarding digital content copyrights.

**7.1.5 Contrast Stretching:**

Contrast stretching emerges as a pivotal tool within the domain of hidden watermarking for augmenting both the resilience and subtlety of embedded watermarks. This technique, primarily utilized to enhance image visual quality by broadening the spectrum of pixel intensity values, finds application in concealing watermarks within digital content while preserving their integrity amidst diverse transformations and potential attacks. By expanding the dynamic range of pixel intensities, contrast stretching amplifies the perceptibility of subtle alterations introduced during the watermarking process, facilitating more effective embedding without compromising the original content's visual fidelity.

**7.1.6 Histogram Equalization:**

Histogram equalization is a key technique employed in the project "Hidden Watermarking: A Steganographic Approach to Copyright Protection." By leveraging histogram equalization, the project aims to enhance the robustness and imperceptibility of hidden watermarks embedded within digital content. This process involves redistributing the intensity levels of pixels in an image, thereby improving its contrast and enhancing the visibility of subtle features. Through this method, the project endeavors to embed copyright information or ownership data in a manner that is concealed from casual observers yet resistant to various forms of tampering or unauthorized duplication. By incorporating histogram equalization into the watermarking process, the project seeks to bolster the integrity and security of digital assets, thereby safeguarding intellectual property rights in an increasingly digitized world.

# 7.2 Project Implementation

# 7.2.1 Input Process

Select an input image

# 

# 

# 

Image Preprocessing techniques, Bilinear interpolation, Image enhancement, Contrast stretching, Histogram equalization

Write the text to be hidden in the image (watermark)

Enter how image should be stored

Embedded Image

# 

# Fig 7.2.1.1: Input Process

# The Figure 7.2.1.1 represents the input format for the project. The input steps include selection of input image in which the watermark should be hidden. After selection of input image, preprocessing steps will be taken and also the steps like bilinear interpolation, image enhancement, contrast stretching and histogram equalization will be taken in order to main the image quality after image preprocessing. Then the text that is watermark which should be hidden in the image should be entered. After entering, the image format need to be entered in order to save the hidden watermarked image.

# 7.2.2 Output Process:

Select the image to be decoded

Select the pixels (length and width) in an image in order to show the watermark on the image

Watermark completed

Output image with watermark

Given text (Watermark)

# 

# Fig 7.2.2.1: Output Process

# The Figure 7.2.2.1 represents the output process that is decoding the image. In order to decode the image, first select the image which is to be decoded, the select the pixels in order to show the watermark on the image. After selecting the pixels the watermarking for the image will be completed. Then the final output that is the watermarked image and the entered text that is watermark will be visible.

# 8. RESULTS AND DISCUSSION:

# 8.1 Output:

# The following the are results and outcomes:

# 

# Fig8.1.1 Input image

# The figure 8.1.1 displays the input image that is the image where the steganography watermarking will be used.

# 

# Fig 8.1.2a Preprocessing of an image Fig 8.1.2b Gray Scale image The second step which is preprocessing of an image include resizing of an image and grayscale image conversion. The figure 8.1.2a represents the resized image of an original image provided and the figure 8.1.2b represents the gray scale conversion of resized image.

# Fig 8.1.3: Bilinear Interpolation

# Figure 8.1.3 indicates the step 3 in code execution that is image interpolation. The bilinear image interpolation is used in the project so the figure 8.3 show the bilinear interpolation of an input image.

# 

# Fig 8.1.4: Low Contrast Image

# The figure 8.1.4 shows the low contrast image of the provided input image.

# 

# Fig 8.1.5: Contrast Stretching

# The figure 8.1.5 shows the contrast stretching of image after bilinear interpolation.

# 

# Fig 8.1.6: Histogram Equalization

# The Figure 8.1.6 shows the result of histogram equalization which is used to regain the clarity of an image after resizing the image.

# 

# Fig 8.1.7: Input image and text

# The Figure 8.1.7 shows the input image format that is out.png is the input image, and “Team5” is the text, that is the watermarking which will be hidden in the input image.

# 

# Fig 8.1.7: Embedded image

# The figure 8.1.7 shows the image where the watermark is hidden in the image that is the text we’ve given in the previous step.

# 

# Fig: 8.1.8: Decryption

# The figure 8.1.8 represents the decryption details.

# 

# Fig 8.1.9: Position details

# The figure 8.1.9 shows the details of the word which is to be decrypted and the details of the height and width of the pixel where the watermark should be stored.

# 

# Fig 8.1.10: Watermarked image

# The figure 8.1.10 shows the final watermarked image and the text which the user gives as watermark.

# 8.2 Sample Code:

# import numpy as np

# import matplotlib.pyplot as plt

# from tkinter.filedialog import askopenfilename

# import cv2

# import matplotlib.image as mpimg

# import warnings

# warnings.filterwarnings('ignore')

# #========================== STEP 1 =========================

# print("-------------------------------------------")

# print("Step 1 ------> Input Image ")

# print("-------------------------------------------")

# print()

# filename = askopenfilename()

# image = mpimg.imread(filename)

# plt.imshow(image)

# plt.title('Original Image')

# plt.axis ('off')

# plt.show()

# #============================ 2.IMAGE PREPROCESSING ====================

# from matplotlib import pyplot as plt

# #==== RESIZE IMAGE =====#

# print("-------------------------------------------")

# print("Step 2 ------> Preprocessing ")

# print("-------------------------------------------")

# print()

# resized\_image = cv2.resize(image,(300,300))

# img\_resize\_orig = cv2.resize(image,((50, 50)))

# plt.imshow(resized\_image)

# plt.title('Resized Image')

# plt.axis ('off')

# plt.show()

# print()

# print("-------------------------------------------------------------------")

# print()

# #==== GRAYSCALE IMAGE ======#

# try:

# gray1 = cv2.cvtColor(img\_resize\_orig, cv2.COLOR\_BGR2GRAY)

# except:

# gray1 = img\_resize\_orig

# plt.imshow(gray1)

# plt.title('Gray Scale Image')

# plt.axis ('off')

# plt.show()

# print("-------------------------------------------")

# print("Step 3 ------> Image Interpolation ")

# print("-------------------------------------------")

# print()

# bilinear\_img = cv2.resize(image,None, fx = 10, fy = 10, interpolation = cv2.INTER\_LINEAR)

# plt.imshow(bilinear\_img)

# plt.title('Bilinear Interpolation')

# plt.axis ('off')

# plt.show()

# print("-------------------------------------------------------------")

# print('Original Image Shape :', image.shape)

# print('Bilinear Interpolation Image Shape :', bilinear\_img.shape)

# print("-------------------------------------------------------------")

# #======================= IMAGE ENHANCEMENT ==================

# import numpy as np

# import matplotlib

# from skimage import img\_as\_float

# from skimage import exposure

# matplotlib.rcParams['font.size'] = 8

# def plot\_img\_and\_hist(image, axes, bins=256):

# image = img\_as\_float(image)

# ax\_img, ax\_hist = axes

# ax\_cdf = ax\_hist.twinx()

# # Display image

# ax\_img.imshow(image, cmap=plt.cm.gray)

# ax\_img.set\_axis\_off()

# # Display histogram

# ax\_hist.hist(image.ravel(), bins=bins, histtype='step', color='black')

# ax\_hist.ticklabel\_format(axis='y', style='scientific', scilimits=(0, 0))

# ax\_hist.set\_xlabel('Pixel intensity')

# ax\_hist.set\_xlim(0, 1)

# ax\_hist.set\_yticks([])

# # Display cumulative distribution

# img\_cdf, bins = exposure.cumulative\_distribution(image, bins)

# ax\_cdf.plot(bins, img\_cdf, 'r')

# ax\_cdf.set\_yticks([])

# return ax\_img, ax\_hist, ax\_cdf

# # Contrast stretching

# p2, p98 = np.percentile(image, (2, 98))

# img\_con = exposure.rescale\_intensity(image, in\_range=(p2, p98))

# # Equalization

# img\_eq = exposure.equalize\_hist(image)

# # Adaptive Equalization

# img\_adapteq = exposure.equalize\_adapthist(image, clip\_limit=0.03)

# plt.imshow(image)

# plt.title('Low contrast image')

# plt.axis ('off')

# plt.show()

# plt.imshow(img\_con)

# plt.title('Contrast stretching')

# plt.axis ('off')

# plt.show()

# plt.imshow(img\_eq)

# plt.title('Histogram equalization')

# plt.axis ('off')

# plt.show()

# plt.imshow(img\_eq)

# plt.title('Histogram equalization')

# plt.axis ('off')

# plt.show()

# from PIL import Image, ImageDraw, ImageFont

# def watermark\_image(original\_image\_path, output\_image\_path, text\_watermark):

# # Open the original image

# original\_image = Image.open(original\_image\_path)

# # Create a drawing object

# draw = ImageDraw.Draw(original\_image)

# # Choose a font and size for the watermark

# font\_size = 30

# font = ImageFont.load\_default()

# # Get the size of the original image

# image\_width, image\_height = original\_image.size

# # Get the size of the watermark text

# text\_width, text\_height = draw.textsize(text\_watermark, font)

# # Calculate the position to center the text watermark

# x\_position = (image\_width - text\_width) // 2

# y\_position = (image\_height - text\_height) // 2

# # Define the color of the text (white in this example)

# text\_color = (255, 255, 255)

# # Add the text watermark to the image

# draw.text((x\_position, y\_position), text\_watermark, font=font, fill=text\_color)

# # Save the watermarked image

# original\_image.save(output\_image\_path)

# print("Watermarking complete.")

# # Example usage

# original\_image\_path = filename

# output\_image\_path = "watermarked\_image.jpg"

# hidden\_text = input("Enter the hidden message")

# # Watermark the image with text

# watermark\_image(original\_image\_path, output\_image\_path, hidden\_text)

# image = mpimg.imread("watermarked\_image.jpg")

# plt.imshow(image)

# plt.title('Watermarked Image')

# plt.axis ('off')

# plt.show()

# # ===== EXTRACT THE MESSAGE

# print("-------------------------------")

# pritn(" The Extracted Text")

# print("-------------------------------")

# print()

# print(hidden\_text)

# 9.CONCLUSION AND FUTURE SCOPE

# 9.1 Conclusion:

In this project, we explored hidden watermarking as a steganographic approach to copyright protection. Steganography, the art of concealing information within other data, offers a subtle yet effective means of embedding ownership information or copyright marks into digital content without altering its perceptual quality. This technique is particularly valuable in safeguarding intellectual property rights, especially in the digital age where content can be easily copied, distributed, and manipulated.

Our project focused on implementing a steganographic watermarking technique using Python, leveraging libraries such as PIL and matplotlib. Through our implementation, we demonstrated how to embed a watermark image into a host image discreetly, ensuring that the watermark remains hidden yet recoverable by authorized parties. This approach allows content creators to assert their ownership rights without compromising the visual integrity of their work.

Furthermore, we addressed the importance of choosing appropriate watermarking techniques and parameters to balance between robustness, imperceptibility, and security. By considering factors such as watermark strength, embedding capacity, and resistance to attacks, we aimed to develop a robust watermarking solution capable of withstanding various forms of manipulation and distortion.

Overall, hidden watermarking serves as a valuable tool in the arsenal of copyright protection measures, enabling content creators to assert their ownership rights in an increasingly digital and interconnected world. However, it is essential to continuously refine and adapt watermarking techniques to keep pace with emerging threats and advancements in digital media technology. Through ongoing research and innovation, we can further enhance the effectiveness and resilience of hidden watermarking solutions, safeguarding the rights and interests of content creators worldwide.

**9.2 Future Scope:**

The future scope of the project "Hidden Watermarking: A Steganographic Approach to Copyright Protection" lies in its potential for further advancements in steganography techniques and their application in safeguarding digital assets. As technology evolves and digital content becomes increasingly susceptible to unauthorized use and distribution, innovative methods like hidden watermarking offer promising avenues for enhancing copyright protection. Future developments could focus on refining algorithms to embed watermarks more robustly, ensuring imperceptibility to maintain the integrity of the original content, and exploring adaptive approaches to counter emerging threats in digital piracy. Moreover, integrating machine learning and artificial intelligence could enhance detection capabilities, enabling automated tracking and enforcement of copyright infringements across vast digital landscapes. Collaboration with stakeholders across industries, including technology, entertainment, and legal sectors, could foster the adoption of standardized practices and regulatory frameworks to bolster the effectiveness of hidden watermarking as a vital tool in preserving intellectual property rights in the digital age.

**10. REFERENCES**

[1] Bhavani, Y., Kamakshi, P., Kavya Sri, E. and Sindhu Sai, Y., 2022. A survey on image steganography techniques using least significant bit. In *Intelligent Data Communication Technologies and Internet of Things: Proceedings of ICICI 2021* (pp. 281-290). Singapore: Springer Nature Singapore.

[2] Alexan, W., Mamdouh, E., ElBeltagy, M., Hassan, F. and Edward, P., 2022, July. Image feature-based watermarking. In *2022 International Telecommunications Conference (ITC-Egypt)* (pp. 1-6). IEEE.

[3] Wan, W., Wang, J., Zhang, Y., Li, J., Yu, H. and Sun, J., 2022. A comprehensive survey on robust image watermarking. *Neurocomputing*, *488*, pp.226-247.

[4] Michaylov, K.D. and Sarmah, D.K., 2024. Steganography and steganalysis for digital image enhanced Forensic analysis and recommendations. *Journal of Cyber Security Technology*, pp.1-27.

[5] Faheem, Z.B., Ishaq, A., Rustam, F., de la Torre Díez, I., Gavilanes, D., Vergara, M.M. and Ashraf, I., 2023. Image watermarking using least significant bit and canny edge detection. *Sensors*, *23*(3), p.1210.

[6] Hameed, M.A., Abdel-Aleem, O.A. and Hassaballah, M., 2023. A secure data hiding approach based on least-significant-bit and nature-inspired optimization techniques. *Journal of Ambient Intelligence and Humanized Computing*, *14*(5), pp.4639-4657.

[7] Joshi, I., Utkarsh, A., Kothari, R., Kurmi, V.K., Dantcheva, A., Roy, S.D. and Kalra, P.K., 2023. On estimating uncertainty of fingerprint enhancement models. In *Digital Image Enhancement and Reconstruction* (pp. 29-70). Academic Press.

[8] Luo, Y., Wang, F., Xu, S., Zhang, S., Li, L., Su, M. and Liu, J., 2022. CONCEAL: A robust dual-color image watermarking scheme. *Expert Systems with Applications*, *208*, p.118133.

[9] Hasan, N., Islam, M.S., Chen, W., Kabir, M.A. and Al-Ahmadi, S., 2021. Encryption based image watermarking algorithm in 2DWT-DCT domains. *Sensors*, *21*(16), p.5540.

[10] Zermi, N., Khaldi, A., Kafi, R., Kahlessenane, F. and Euschi, S., 2021. A DWT-SVD based robust digital watermarking for medical image security. *Forensic science international*, *320*, p.110691.

|  |
| --- |
|  |