WWW.IJRPR.COM

International Journal of Research Publication and Reviews

Journal homepage: www.ijrpr.com ISSN 2582-7421

DIGITAL WATERMARKING USING STEGANOGRAPHY

Ms. Anushki Talekar[1], Mr. Jai Thakar[2], Mr. Dipesh Pendkalkar[3], Mr. Dhiraj Patil[4]

[1] Student Information Technology Pravin Patil College of Diploma Engineering & Technology Bhayandar, Thane-401107 Anushkitalekar1@gmail.com
[2] Student Information Technology Pravin Patil College of Diploma Engineering & Technology Bhayandar, Thane-401107 jaithakar03@gmail.com
[3] Student Information Technology Pravin Patil College of Diploma Engineering & Technology Bhayandar, Thane-401107 dipeshpendkalkar@gmail.com
[4] Sr. Lecturer Information Technology Pravin Patil College of Diploma Engineering & Technology Bhayandar, Thane-401107 Prpdhirajif21@gmail.com

ABSTRACT :

In today's digital landscape, a vast amount of multimedia data is generated frequently in various formats, including text, images, and audio. Ensuring the security of this multimedia data has become a crucial concern due to the risk of unauthorized modifications by intruders. Techniques such as watermarking and steganography play vital roles in protecting this data from unauthorized access. Watermarking involves embedding data within a carrier signal, while steganography entails hiding digital information within other digital files. This paper explores different applications of watermarking, its characteristics, and the fundamental concepts of image processing. Furthermore, it thoroughly reviews existing literature on digital image watermarking and discusses various optimization techniques employed in the field.

Key Words:- LSB, Digital Watermarking, Discrete Wavelet Transform, Genetic Algorithm, privacy, security.

INTRODUCTION :

The notion of watermarking dates back to ancient times, when messages were concealed within human bodies and later in paper, altering its thickness to embed a watermark. This technique is particularly effective when the paper is damp, hence the term "watermark." In the contemporary digital era, the swift advancement of the internet and technology has greatly facilitated the generation and alteration of information in digital formats. Unauthorized access and modifications of digital data pose significant threats to intellectual property rights. Watermarking serves as a means of copyright protection.
digital images, thus safeguarding intellectual property. Watermarks are inserted into carrier data and may be extracted later. The term steganography combines two Greek words: 'steganus' (meaning covered or concealed) and 'graphic' (meaning writing), indicating that it primarily conceals the existence of embedded data, unlike watermarking.
which integrates identifying data into host data. Watermarking can be accomplished through two primary methods: in the spatial domain and the frequency domain. This paper is structured as follows: Section 2 discusses watermarking concepts, including types, characteristics, and performance parameters. Section 3 reviews relevant literature. Section 4 explores various optimisation techniques. Section 5 outlines the proposed work, and Section 6 concludes the paper. Digital watermarking and steganography are two closely related techniques used to protect, authenticate, or hide information within digital media. Both approaches are used for security purposes, but while they share some similarities, they differ in their underlying goals and methodologies. Digital watermarking focuses on embedding a recognizable signal in a way that can later be extracted for verification or proof of ownership, while steganography is more concerned with concealing information, making it imperceptible to unauthorized observers.
Digital watermarking can be classified into several types based on various criteria, such as visibility, robustness, and the type of media. Here are the types of watermarks:

1) Visible Watermark, 2) Invisible Watermark

- **Visible Watermark**

A **visible watermark** is a type of watermark that is intentionally placed on a digital medium (such as an image, video, or document) in a way that makes it noticeable to viewers. The purpose of visible watermarks is typically to indicate ownership, protect intellectual property, or prevent unauthorized use of the content. They are designed to be visible and easily identifiable, usually taking the form of a logo, text, or graphic. In contrast to invisible watermarks, which are embedded in the content in a way that isn't easily perceived.

- **Invisible Watermark**

An **invisible watermark** is a digital marker embedded within a file that's imperceptible to the human senses. It's designed to carry hidden information (such as a copyright statement, serial number, or identification code) while ensuring that the watermark doesn't distort or alter the original content. This is achieved by encoding the watermark in a way that does not affect the visual quality of images, the audio quality of sound files, or the viewing experience of videos. Invisible watermarks are primarily used for purposes like **copyright protection**, **authentication**, and **tamper detection**. Since

these watermarks are not visible or audible, they are useful when the content creator wants to keep the visual appeal of the media intact while still protecting it.

PROBLEM STATEMENT :

Existing systems that use digital watermarking or steganography face a number of challenges. One major issue is their susceptibility to common attacks, like compression, cropping, and noise addition, which can weaken or completely erase the watermark. This directly impacts the security of the content. Another challenge is balancing invisibility with robustness—watermarks need to be undetectable to the human eye, but they also have to be strong enough to withstand distortion. Striking this balance is tough for current systems. Furthermore, steganography often struggles with embedding large or complex watermarks without making them noticeable, limiting the amount of data it can carry. Combining both techniques for better security is also tricky and adds to the complexity. Moreover, implementing both watermarking and steganography together to enhance security can lead to additional technical hurdles, such as increased processing time and the need for more sophisticated algorithms. These added complexities make it harder to create a seamless and efficient system, further complicating efforts to improve content protection. As a result, finding the right balance between security, efficiency, and ease of implementation remains a significant challenge in this field.

LITERATURE SURVEY :

Digital watermarking and steganography are two widely studied methods for protecting digital media, each offering its own strengths and challenges. In digital watermarking, there are various techniques, like spatial-domain methods, which embed information directly into pixel values, and frequency-domain methods such as Discrete Cosine Transform (DCT) and Discrete Wavelet Transform (DWT), which work by altering the frequency components of the media. On the other hand, steganography focuses on hiding information within a cover medium, with techniques like Least Significant Bit (LSB) substitution, which hides data in the least noticeable bits of pixels, as well as more advanced methods like spread spectrum and encryption-based approaches (Bender et al., 1996). While these methods are good at keeping the hidden information out of sight, they often struggle with limited capacity and can be vulnerable to detection through statistical analysis. To overcome the drawbacks of these individual techniques, researchers have been exploring hybrid systems that combine both watermarking and steganography. One approach integrates robust watermarking algorithms with steganographic methods to hide the watermark in layers that are harder to detect while still ensuring resistance to common attacks. Some studies also focus on embedding watermarks in parts of the media that are less noticeable to the human eye, such as low- frequency components, and use steganographic techniques to further conceal the information. This combination aims to improve both the security and stealth of the protected content.

METHODOLOGY :

The methodology for this project involves a systematic approach that integrates digital watermarking and steganography to create a robust hybrid solution. First, an extensive literature review is conducted to understand existing techniques in both fields and identify the most suitable algorithms for the project. For watermarking, techniques like Discrete Cosine Transform (DCT) and Discrete Wavelet Transform (DWT) are chosen for their resilience to common attacks, while steganography methods such as Least Significant Bit (LSB) or Spread Spectrum are selected
for their ability to hide data effectively. The next step is to design a hybrid system where the watermark is embedded into the cover medium using steganographic methods. This ensures that the watermark remains imperceptible while maintaining its robustness.
The system is developed using programming languages like Python with optimization techniques to minimize computational load and ensure smooth performance, especially when handling large media files. After development, the system undergoes thorough testing against common attacks, such as compression, cropping, and noise addition. Its invisibility is assessed through both objective and subjective measures. The hybrid system is then compared to existing watermarking and steganography methods, focusing on robustness, invisibility, and data capacity, using performance metrics like Peak Signal-to-Noise Ratio (PSNR) and Structural Similarity Index (SSIM). Based on the evaluation results, the system is refined to achieve the optimal balance between invisibility, data capacity, and resilience. This process ensures that the final solution is both secure and efficient, making it well- suited for real-world applications like digital rights management and secure communication.

OBJECTIVE FUNCTIONS :

In the context of **digital watermarking** using **steganography**, **objective functions** are mathematical formulations that guide the optimization process of embedding the watermark in a way that achieves specific goals, such as
minimizing distortion, maximizing robustness, or optimizing other relevant characteristics of the watermark. These objective functions are particularly important for evaluating how well the watermark is hidden within the digital content while ensuring that it meets specific criteria like imperceptibility (invisible or inaudible to the human eye or ear), robustness (resistance to attacks and modifications), and capacity (amount of information that can be embedded).

Key Objectives in Digital Watermarking Using Steganography

- Imperceptibility
- Robustness
- Capacity
- Security

PROPOSED SOLUTION :

The proposed solution focuses on combining digital watermarking and steganography into a hybrid system to create a more secure, reliable, and efficient way to protect and authenticate digital content. By integrating both techniques, the solution aims to address the weaknesses of each individual method, ensuring the content remains protected while maintaining invisibility, robustness, and enough capacity for embedding data.

- **Hybrid Integration of Watermarking and Steganography**: At the heart of the solution is the combination of strong watermarking algorithms with advanced steganography. This approach hides the watermark in less noticeable parts of the media, making it almost invisible to the human eye while also making it resistant to attacks like compression, cropping, or noise addition. The watermark is embedded in less sensitive regions, such as low-frequency components, using frequency-domain methods (like DCT or DWT) alongside steganographic techniques such as Least Significant Bit (LSB) substitution.
- **Optimizing for Real-time Performance**: To ensure the system works efficiently with large media files, the solution is optimized for real-time performance. Using programming languages like Python or MATLAB, the algorithms are fine-tuned to reduce computational overhead without sacrificing security or quality. We also explore ways to speed up processing, such as parallel computing or using hardware acceleration, ensuring the system remains effective and fast.

LIMITATIONS :

In digital watermarking, especially when using steganography to hide watermarks, there are several **limitations** to consider. These limitations affect how effectively and securely the watermark can be embedded and detected and how it interacts with the host content. Below are some of the key limitations:

1. **Capacity Limitations**

- **Capacity** refers to how much information can be hidden within the watermark. In steganography, you might want to hide a large amount of data.
- **Limitations**: The more data you hide, the more noticeable the watermark might become, which can affect the **imperceptibility**. There's also a limit to how much data can be hidden in a file without significantly impacting its quality or size. Large amounts of hidden data could cause distortion or trigger detection.

2. **File Size and Format Constraints**

- Some watermarking techniques may slightly increase the file size, especially if a large watermark or more data is embedded. This increase in file size might not be acceptable for applications where bandwidth or storage space is limited.
- **Limitations**: The watermarking method must ensure that the file size remains within acceptable limits for practical use. Also, some file formats may not be suitable for watermark embedding due to their structure or compression methods.
- hidden information in documents or media without the knowledge or consent of the owner.
- watermarking techniques and a method that works well for one type of media might not work effectively for another.
- long-term effectiveness as media formats and digital tools evolve.
- **The trade-off between imperceptibility and robustness**: Making the watermark harder to detect may reduce its strength.

APPLICATIONS :

Several real-world applications of our system can really make a difference in a variety of industries. Here are some key examples:

1. **Authentication and Identity Verification**: In banking and finance, watermarking through steganography can secretly embed hidden information into important documents like invoices or receipts, which helps prevent fraud. Similarly, government-issued documents, such as passports or IDs, can carry hidden watermarks, ensuring their authenticity and making them much harder to counterfeit.

2. **Secure Communication**: For secure messaging, sensitive data can be discreetly embedded within digital media like images, audio, or videos. This technique is especially useful for military and intelligence operations where confidential information needs to be communicated over networks without drawing attention.

CONCLUSION :

In this paper, we get to know that digital watermarking combined with steganography is a powerful and flexible method for securing and authenticating digital content. It offers key benefits such as invisible protection, safeguarding intellectual property, ensuring data integrity, and maintaining privacy, making it crucial in industries like entertainment, healthcare, finance, and communications. Despite challenges like vulnerability to advanced attacks and limitations in embedding capacity, ongoing research and technological progress are working to overcome these obstacles, improving the robustness, scalability, and overall effectiveness of watermarking systems. The integration of emerging technologies like AI, blockchain, and quantum computing is set to further enhance the strength of steganographic watermarking, ensuring the security and traceability of digital media

REFERENCES :

1. **Cox, I. J., Kilian, J., Leighton, F. T., & Shamoon , T.** (1997). Secure Spread Spectrum Watermarking for Multimedia. IEEE Transactions on Image Processing, 6(12), 1673-1687.
2. **Anderson, R., & Petitcolas, F. A. P.** (1998). On the Limits of Steganography. IEEE Journal on Selected Areas in Communications, 16(4), 474-48.
3. **Karnan, M., & Kumaravel, N.** (2012). A Survey on Digital Watermarking Algorithms. International Journal of Computer Applications, 51(9), 20-29.
4. **Piva, A., & Barni, M.** (2000). Additive Watermarking of Digital Images with Improved Robustness. Proceedings of the International Conference on Image Processing, 1, 298-301.
5. **Chandramohan, R., & Kumaravel, N.** (2014). Steganography and Watermarking Techniques for Digital Media Protection. Journal of Computer Science and Technology.