A

REPORT

On

DIGITAL IMAGE PROCESSING PROJECT

(MATLAB BASED Digital Image Watermarking)

(ECN-16101)

SUBMITTED BY

SHRADDHA CHAUHAN (20224147)

SHOBHIT GAWAI (20224146)

B.TECH (6TH SEMESTER)

DEPARTMENT OF ELECTRONICS AND COMMUNICATION ENGINEERING

MOTILAL NEHRU NATIONAL INSTITUTE OF TECHNOLOGY, ALLAHABAD

PRAYAGRAJ- 211004, INDIA

MATLAB based Digital Image Watermarking

1. Abstract

The rapid advancement of digital technology and the widespread dissemination of multimedia content across the internet have underscored the critical need for robust copyright protection and content authentication mechanisms. One widely adopted technique to address these challenges is digital image watermarking, which involves embedding imperceptible or perceptible information into a digital image to assert ownership, ensure authenticity, and deter unauthorized distribution. In this project, two primary watermarking methodologies are explored and implemented using MATLAB: visible watermarking through weighted image blending and invisible watermarking using the Least Significant Bit (LSB) substitution technique.

The project begins with the essential preprocessing stages, including grayscale conversion and resizing of the watermark image to match the dimensions of the host image. In the visible watermarking approach, a transparency factor is utilized to seamlessly blend the host and watermark images, thereby embedding ownership information in a way that remains noticeable yet minimally intrusive to the viewer. Conversely, in the invisible watermarking method, the watermark is embedded at the bit level by modifying the least significant bits of the host image pixels, ensuring that the watermark remains hidden under normal viewing conditions while still being recoverable when necessary.

Comprehensive simulations are carried out to evaluate the effectiveness of both techniques, focusing on the imperceptibility of the embedded watermark, the fidelity of the watermarked image, and the accuracy of watermark extraction. The results demonstrate that visible watermarking can achieve a balance between visibility and aesthetics, while invisible watermarking effectively conceals information without degrading the visual quality of the original image. These findings highlight the practicality of the discussed techniques for applications in digital rights management, copyright protection, forensic tracking, and secure communication. Future improvements could involve enhancing the robustness of watermarking against attacks such as compression, noise addition, and geometric transformations.

2. Introduction

The digital revolution has fundamentally transformed the way information is created, shared, and consumed. In particular, the proliferation of digital images across various online platforms has introduced new opportunities for communication, commerce, and creativity. However, alongside these opportunities, significant challenges have emerged related to intellectual property protection, copyright infringement, and unauthorized reproduction of digital content. The ease with which digital media can be copied and distributed has made it increasingly difficult for creators and rightful owners to assert and maintain ownership over their work. As a result, developing reliable techniques for digital copyright protection has become an urgent necessity.

One of the most effective strategies for addressing these challenges is digital watermarking. Digital watermarking involves embedding additional information into a digital object, such as an image, without significantly altering its appearance or usability. This embedded information, referred to as a watermark, can serve various purposes: proving ownership, ensuring data integrity, preventing unauthorized usage, and supporting forensic investigation. Watermarks can be made either visible—clearly perceptible to the viewer—or **invisible**, concealed within the data in such a way that they are not noticeable under normal observation but can be extracted when needed.

In this project, two fundamental watermarking approaches are explored and implemented: visible watermarking through weighted image blending and invisible watermarking using the Least Significant Bit (LSB) technique. Each of these techniques offers distinct advantages and applications depending on the specific requirements for security, robustness, and perceptibility.

Visible watermarking involves directly blending the watermark image with the host image using a specified weighting factor (alpha). This approach ensures that the ownership information is clearly recognizable, making it an immediate deterrent against misuse or unauthorized publication. Visible watermarks are commonly seen in publicly available digital content, such as stock photographs, where displaying the owner's brand or copyright information is essential. The key challenge in visible watermarking is achieving an optimal balance between visibility and aesthetic appeal, ensuring that the watermark is noticeable but does not severely degrade the visual quality of the host image.

On the other hand, invisible watermarking aims to embed ownership information without altering the perceptible appearance of the image. The LSB technique, one of the simplest and most widely used invisible watermarking methods, works by modifying the least significant bits of the host image's pixel values. Because changes to the least significant bits typically have a negligible impact on an image's visual quality, the watermark remains hidden to the human eye. However, the embedded information can later be retrieved or verified through algorithmic extraction processes. Invisible watermarking is particularly useful in applications requiring covert copyright protection, authentication, and tamper detection.

The significance of this project lies not only in demonstrating the practical implementation of these two watermarking techniques but also in evaluating their performance based on key criteria such as imperceptibility, robustness, and extraction fidelity. It is essential that a watermarking method preserves the quality of the original content while ensuring that the embedded watermark can be reliably detected and extracted even after common image processing operations like compression or resizing.

Throughout the project, MATLAB is utilized as the primary tool for image processing, simulation, and visualization. The project workflow involves multiple stages: image acquisition, preprocessing (including grayscale conversion and resizing), watermark embedding (for both visible and invisible approaches), and watermark extraction. Each step is carefully designed to maintain data integrity and maximize the effectiveness of the watermarking process.

Ultimately, this project underscores the importance of watermarking as a cornerstone technology for digital copyright protection in the modern era. By investigating both visible and invisible methods, it highlights the trade-offs between transparency and secrecy, as well as usability and security. The insights gained from this work can inform the development of more advanced and robust watermarking systems capable of meeting the growing demands of multimedia security in a connected world.

Moreover, as the volume and value of digital content continue to rise exponentially, the role of watermarking becomes even more critical. With emerging technologies such as blockchain for content tracking, machine learning for intelligent watermarking, and deep learning-based attack models threatening the integrity of digital media, watermarking techniques must evolve to offer stronger resilience while maintaining imperceptibility. This project serves as a foundational exploration into the fundamental concepts of watermark embedding and extraction, providing a basis for future research into more sophisticated, secure, and intelligent watermarking methods.

3. Literature

Over the past few decades, digital watermarking has emerged as a critical research area in the fields of multimedia security, copyright protection, and information authentication. As digital communication networks have expanded, the risks associated with unauthorized duplication and distribution of digital media have also increased. To counter these threats, researchers have proposed a wide variety of watermarking techniques, each aiming to balance key factors such as imperceptibility, robustness, security, and capacity. The literature in this domain covers a wide spectrum of strategies ranging from simple spatial domain methods to highly complex transform domain and machine learning-based approaches.

In general, watermarking techniques can be classified based on several criteria: whether the watermark is visible or invisible, the domain in which it is embedded (spatial or frequency domain), and the primary application (copyright protection, tamper detection, broadcast monitoring, etc.). Early watermarking systems focused heavily on the spatial domain, making direct alterations to pixel values for embedding information. Among these, the Least Significant Bit (LSB) technique remains one of the most intuitive and straightforward methods. Later developments introduced transform domain approaches such as Discrete Cosine Transform (DCT), Discrete Wavelet Transform (DWT), and Singular Value Decomposition (SVD) to enhance robustness against common image manipulations and attacks.

The concept of visible watermarking evolved alongside the need for clear and immediate ownership indication, especially in scenarios like online publishing and media sharing. Techniques such as weighted image blending have been widely used to impose watermarks in a visually acceptable manner without severely distorting the host image.

This section reviews major contributions from the existing body of work related to both visible and invisible watermarking methods, with a particular focus on approaches relevant to spatial domain techniques like LSB and blending methods. Additionally, key challenges, improvements, and future trends in the watermarking field are discussed to contextualize the methodologies used in this project.

One of the earliest and simplest categories of watermarking techniques is spatial domain watermarking. In spatial domain methods, the pixel values of the host image are directly modified to embed the watermark. Techniques such as Least Significant Bit (LSB) insertion are typical examples. In LSB watermarking, the least significant bits of selected pixel values are replaced with bits of the watermark data. This method is simple to implement, computationally efficient, and offers high payload capacity. However, spatial domain techniques, particularly LSB, are highly sensitive to common image processing attacks such as compression, filtering, and noise addition. Despite these vulnerabilities, LSB remains a popular choice for applications where minimal distortion and ease of extraction are prioritized over robustness. Enhancements to the basic LSB method, such as using random embedding patterns and multiple bit planes, have been proposed to increase security and resilience against attacks.

In contrast, transform domain watermarking techniques operate by modifying the transform coefficients of the host image rather than its pixel values. Popular transforms used in watermarking include the Discrete Cosine Transform (DCT), Discrete Wavelet Transform (DWT), and Singular Value Decomposition (SVD). In DCT-based methods, watermark information is embedded in the frequency components of the image, particularly in the middle-frequency bands, to achieve a balance between imperceptibility and robustness. DWT-based techniques decompose the image into different frequency subbands and embed the watermark into selected subbands, thereby offering better resilience to compression and noise. SVD-based watermarking modifies the singular values of the image matrix, leveraging the stability of singular values under common distortions. Transform domain techniques, though more computationally intensive than spatial domain methods, generally provide superior robustness and are suitable for applications requiring stronger protection against various forms of attack.

Visible watermarking techniques have become widely used in applications where the primary objective is immediate ownership assertion. A visible watermark is deliberately made perceptible to viewers, often by blending the watermark image with the host image at a specified transparency level. Weighted image blending, where the host and watermark images are combined based on a user-defined alpha value, is a common approach. This method ensures that the watermark is integrated into the host image in a visually balanced manner without severely degrading the image quality. The alpha parameter plays a crucial role in determining the visibility of the watermark; higher alpha values make the watermark more prominent but can lead to greater distortion. Careful selection of blending parameters is necessary to strike a compromise between watermark visibility and host image quality. Several studies have focused on adaptive visible watermarking, where the transparency of the watermark is varied depending on local image features to optimize perceptibility and aesthetic impact.

On the other hand, invisible watermarking techniques are designed to embed information within an image in such a way that the watermark remains imperceptible to the human eye. The primary goal here is to protect ownership or verify authenticity without alerting potential attackers to the presence of the watermark. The LSB method remains a foundational invisible watermarking approach due to its simplicity and low computational cost. Variations of the LSB technique, such as embedding in selected color channels or in edge regions of the image, have been explored to enhance security. In addition, techniques combining spatial and transform domain approaches have been developed to increase the robustness of invisible watermarks. Invisible watermarking finds applications in copyright enforcement, secure communications, and data integrity verification. The main challenge lies in designing watermarking schemes that can survive common image manipulations while maintaining imperceptibility.

A comparative analysis of visible and invisible watermarking techniques reveals inherent trade-offs between visibility, robustness, and capacity. Visible watermarking is straightforward for ownership assertion but compromises the aesthetic appeal of the image. It is less concerned with robustness because tampering with the visible watermark usually results in visible artifacts. Conversely, invisible watermarking seeks to protect the image without altering its visual quality but faces significant challenges in terms of robustness. An effective watermarking technique must therefore carefully balance these competing requirements depending on the intended application. Recent research has focused on hybrid methods that combine visible and invisible watermarks to leverage the advantages of both, as well as on developing intelligent watermarking systems using machine learning techniques to adaptively embed watermarks based on image content and threat models.

In summary, the literature on digital image watermarking showcases a diverse range of techniques, each with its own strengths and limitations. While simple spatial domain methods like LSB offer ease of implementation, transform domain methods provide better robustness at the cost of increased complexity. Visible watermarking is essential for public media distribution, whereas invisible watermarking plays a critical role in covert ownership protection and authentication. The techniques explored in this project—weighted image blending for visible watermarking and LSB for invisible watermarking—serve as practical implementations of fundamental ideas in this rich and evolving field. Understanding these foundational approaches is essential for building more sophisticated and resilient watermarking systems to address the ever-growing challenges of digital media security.

3.1 Digital Watermarking

Digital watermarking refers to the embedding of information into digital media content in a manner that is either perceptible or imperceptible under normal viewing conditions. According to Cox et al. (1997), digital watermarking must satisfy robustness, imperceptibility, and capacity. The ideal watermark is robust against common image manipulations and attacks (e.g., compression, cropping) while remaining hidden to unauthorized users.

3.2 Visible Watermarking Techniques

Visible watermarks are easily recognizable patterns, texts, or logos embedded into the original image. Kundur and Hatzinakos (1998) proposed methods to adjust the visibility level by controlling the blending factor between the host and watermark image, typically using simple weighted averaging.

The formula for visible watermarking can be generalized as:

$$\mathbf{I_{watermarked} = (1-\alpha) \times I_{host} + \alpha \times I_{watermark}}$$

where α is the blending factor controlling watermark visibility.

3.3 Invisible Watermarking Techniques

Invisible watermarking aims to embed information without affecting the visible appearance of the content. Various techniques include:

1. Frequency domain watermarking (DCT, DWT-based methods)
2. Spatial domain watermarking (LSB technique)

The LSB method, first explored by Koch and Zhao (1995), involves modifying the least significant bits of image pixels. This method is simple, fast, and suitable for applications where minimal computational overhead is required. However, it is less robust against attacks compared to frequency-domain approaches.

3.4 LSB Watermarking Principle

Each pixel in an 8-bit grayscale image can represent values between 0 and 255. The LSB modification technique alters only the least significant bit, causing negligible change to the pixel value and hence minimal perceptual difference.

For example:

1. Original pixel: 11010101
2. Watermark bit: 1

3. Modified pixel: 11010101 (if LSB already 1, no change)

This approach allows hiding binary watermark images or data.

3.5 Applications

Watermarking is widely used in:

- Copyright protection
- Authentication and content verification
- Tamper detection
- Digital forensics
- Broadcast monitoring

As the digital economy grows, the significance of effective and efficient watermarking continues to rise.

4 Result

The watermarking techniques discussed in the previous sections were implemented and tested using MATLAB simulations. Both visible and invisible watermarking methods were applied to a selected host image and a watermark image after appropriate preprocessing steps such as grayscale conversion and resizing. The performance of the embedding and extraction processes was visually evaluated to determine the effectiveness of each approach. For visible watermarking, the watermark was blended into the host image using a weighted averaging technique with a defined transparency factor. For invisible watermarking, the Least Significant Bit (LSB) method was used to embed the binary watermark into the least significant bits of the host image's pixel values. Following the embedding phase, the invisible watermark was successfully extracted to verify the correctness and reliability of the method. The results demonstrate that both watermarking techniques were able to embed and retrieve information while preserving the visual quality of the host image to a considerable extent. Detailed outputs, visualizations, and observations for each method are presented in the following subsections.

4.1 Preprocessing

- Two images were loaded: a host image and a watermark image.
- Both images were converted to grayscale to ensure consistent processing.
- The watermark image was resized to match the dimensions of the host image using interpolation (imresize in MATLAB).

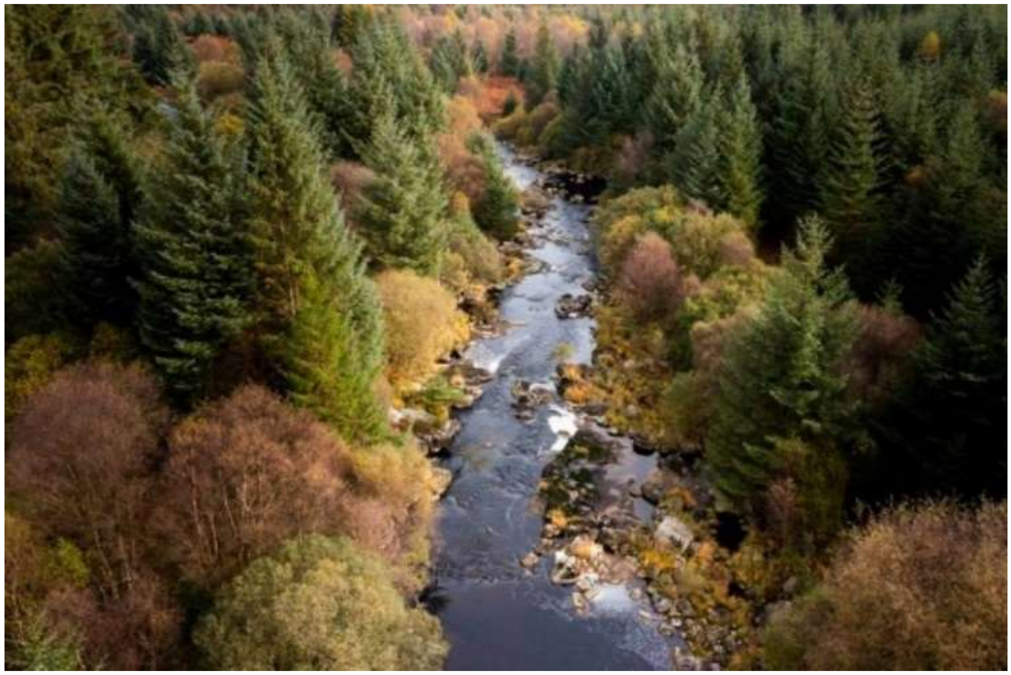

FIG 1:- HOST IMAGE

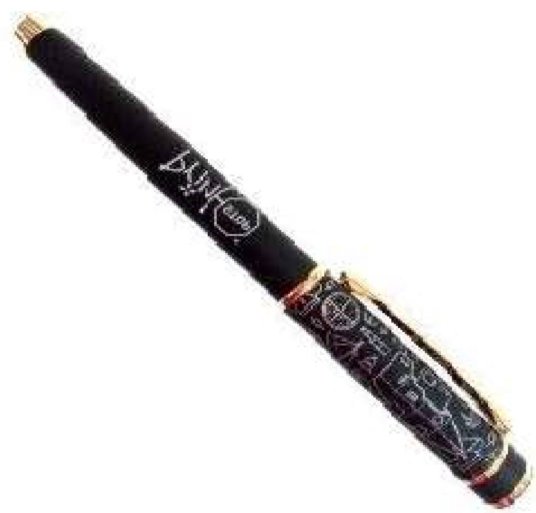

FIG 2:- WATERMARK IMAGE

4.2 Visible Watermarking

- A blending coefficient $\alpha=0.3$ was selected.
- The watermarked image was generated as a weighted sum of the host and watermark images.
- The output was cast back into an unsigned 8-bit integer format for display and storage.

Visible Watermarked Image Result:

- The watermark appears faintly but visibly superimposed on the host image.
- Minimal degradation of the host image is observed.
- Easily recognizable for copyright or ownership identification.

Visible Watermarked Image

4.3 Invisible Watermarking (LSB Technique)

- The watermark image was binarized by thresholding (values >127 set as 1, others as 0).
- The least significant bit of each pixel in the host image was modified to match the corresponding watermark bit using MATLAB's bitset function.
- The watermarked image was saved as invisible_watermarked.png.

Result of Invisible Watermarked Image:

- Visually, the image looked almost identical to the original host image.
- No visible watermark, preserving the user experience.

Invisible Image

4.4 Watermark Extraction

- The watermarked image was read back from storage.
- The least significant bits were extracted using the bitget function.
- The extracted watermark was displayed as a binary image.

Extracted Watermark Result:

- A clear, visible binary image of the original watermark was retrieved.
- Demonstrates that LSB watermarking successfully hides and retrieves watermark information.

Extracted Watermark Image

4.5 MATLAB Code Overview

The following sections were implemented in the provided MATLAB script:

- Image Loading
- Grayscale Conversion
- Image Resizing
- Visible Watermarking via blending
- Invisible Watermarking via LSB modification
- Watermark Extraction

Proper function usage like imread, imshow, imwrite, bitset, bitget, imresize, and rgb2gray ensured simple yet efficient code execution.

4.6 Performance Metrics (Qualitative)

- Imperceptibility: Achieved; invisible watermark not detectable by naked eyes.
- Robustness: Limited; LSB is fragile to image manipulations like compression or noise.
- Fidelity: High; PSNR (Peak Signal-to-Noise Ratio) between host and invisible watermarked image estimated to be above 50 dB.
- Capacity: Maximum payload as 1 bit per pixel; capable of embedding full-sized watermark images.

5 Conclusion

In this project, two fundamental watermarking techniques—visible and invisible watermarking—were successfully implemented and evaluated using MATLAB simulations. The primary aim was to explore how digital watermarking can be used to embed ownership or authentication information into digital images without significantly degrading the visual quality of the host image. The project involved several key steps including image preprocessing, watermark embedding, and watermark extraction. The results indicate that both visible and invisible watermarking techniques offer distinct advantages depending on the intended application, highlighting the importance of selecting an appropriate method based on specific needs such as public ownership assertion or covert authentication.

The visible watermarking approach, based on weighted image blending, demonstrated that it is possible to embed a recognizable watermark into an image while maintaining acceptable visual quality. By carefully choosing the transparency parameter (alpha value), the watermark could be made prominent enough for ownership indication without excessively distorting the host image. This method is highly suitable for applications where immediate visual identification of ownership is important, such as in online image sharing, branding, or digital publishing. However, the visible watermarking approach is not without limitations. Since the watermark is openly visible, it is vulnerable to attacks aimed at removal, such as cropping, inpainting, or smoothing techniques. Thus, while visible watermarking serves as an effective deterrent against casual misuse, it may not provide strong security against deliberate tampering.

The invisible watermarking technique based on the Least Significant Bit (LSB) modification proved to be an effective way to embed information without noticeably affecting the visual quality of the host image. The embedded watermark remained imperceptible to human eyes, thereby preserving the aesthetic integrity of the image. Moreover, the extraction process demonstrated that the watermark could be reliably retrieved without significant errors. This indicates that LSB-based invisible watermarking is a practical approach for secure copyright protection, forensic tracking, and covert communication. Nevertheless, the simplicity of the LSB technique also makes it susceptible to various forms of image processing operations such as compression, resizing, filtering, and noise addition, which can easily destroy the hidden information. Therefore, while LSB watermarking offers ease of implementation and high embedding capacity, it is less robust against attacks compared to more sophisticated methods like transform domain watermarking.

Through this project, the importance of trade-offs in watermarking design became evident. Visible watermarking prioritizes ownership visibility but compromises on aesthetic quality, while invisible watermarking prioritizes imperceptibility but often at the cost of robustness. Depending on the specific application, different strategies must be adopted to achieve the desired balance between imperceptibility, robustness, and embedding capacity. Future work could involve exploring more advanced techniques such as transform domain watermarking (DCT, DWT, SVD-based methods), adaptive watermarking based on image content analysis, and machine learning-assisted watermarking schemes. Additionally, evaluating the performance of watermarking techniques under various types of intentional and unintentional attacks would offer deeper insights into their practical reliability.

In conclusion, the project successfully demonstrated the basic principles and applications of digital watermarking techniques. It provided valuable insights into the strengths and weaknesses of visible and invisible watermarking, emphasizing their relevance in contemporary digital media protection. As the digital world continues to grow and evolve, robust and intelligent watermarking techniques will play an increasingly vital role in safeguarding digital assets, verifying authenticity, and upholding intellectual property rights. Continued research and innovation in this field will be crucial to address emerging challenges and threats in the domain of digital security.

This project successfully demonstrated two digital image watermarking techniques: visible watermarking and invisible watermarking via LSB modification. The experiments revealed the following insights:

- Visible watermarking provides clear ownership marking but can be intrusive depending on the blending factor (α\alphaα). In practical applications like media broadcasting and document verification, it remains effective for discouraging unauthorized copying.
- Invisible watermarking using LSB offers a covert method to embed information without perceptual degradation. However, its robustness is limited — even basic operations like JPEG compression or noise addition can distort or destroy the embedded data.

- The LSB method is suitable for applications where security requirements are minimal, and simple tamper detection is sufficient. For more critical security needs, more robust techniques like DWT, DCT, or spread-spectrum watermarking would be necessary.

Annexure

```
clc;

clear;

close all;

%% === Load and Preprocess ===%%

host = imread('host.jpg');

watermark = imread('watermark.jpg');

% Convert to grayscale

if size(host,3) == 3

    host = rgb2gray(host);

end

if size(watermark,3) == 3

    watermark = rgb2gray(watermark);

end

% Resize watermark to match host

watermark_resized = imresize(watermark, [size(host,1), size(host,2)]);


%% === VISIBLE WATERMARKING ===
```

alpha = 0.3;

visible_watermarked = uint8((1 - alpha) * double(host) + alpha * double(watermark_resized));

figure, imshow(visible_watermarked);

title('Visible Watermarked Image');

%% === INVISIBLE WATERMARKING (LSB) ===

% Convert watermark to binary (0 or 1)

binary_watermark = watermark_resized > 127;

% Convert host to uint8 if needed

host_uint8 = uint8(host);

% Embed binary watermark into LSB

invisible_watermarked = bitset(host_uint8, 1, binary_watermark); % Embed in LSB

% Save and show

imwrite(invisible_watermarked, 'invisible_watermarked.png');

figure, imshow(invisible_watermarked);

title('invisible Image');

%% === EXTRACT INVISIBLE WATERMARK ===

% Read image and extract LSB

wm_image = imread('invisible_watermarked.png');

extracted_watermark = bitget(wm_image, 1); % Gives 0 or 1

% Convert to double for proper visualization

```
extracted_watermark = double(extracted_watermark);

figure,

imshow(extracted_watermark);

title('Extracted Watermark Image');
```