A METHOD FOR VISUAL WATERMARKING DIGITAL IMAGES

A report submitted in partial fulfilment of the requirement for the degree of

MASTER OF COMPUTER APPLICATION (MCA)

OF

TEZPUR UNIVERSITY

2024

Submitted by

SHABBIR AHMAD (CSM21010)

RAJIV KUMAR BAITHA (CSM21045)

Guided by

DR. BHOGESWAR BORAH

Professor, Tezpur University

DEPARTMENT OF COMPUTER SCIENCE & ENGNEERING

TEZPUR UNIVERSITY

TEZPUR 784028

ASSAM.

Department of Computer Science and Engineering, Tezpur University

CERTIFICATE BY THE EXAMINER

This dissertation titled "**A method for Visual Watermarking Digital Images**" submitted by **Shabbir Ahmad (CSM21010)** and **Rajiv Kumar Baitha (CSM21045**) in partial fulfilment of the requirements for the minor project of Master of Computer Applications has been examined.

Examiner

Date:

Place: Tezpur

Department of Computer Science and Engineering Tezpur University

CERTIFICATE

This is to certify that the dissertation entitled **“A method for Visual Watermarking Digital Images "** submitted by **Shabbir Ahmad** and **Rajiv Kumar Baitha** bearing roll no.: **CSM21010** and **CSM21045** respectively, was carried out by them under my supervision and guidance for partial fulfilment of the requirements and the regulations for the award of the degree of Master of Computer Application during the session 2021-2024 at Tezpur University. To the best of my knowledge: the matter embodied in the dissertation has not been submitted to any other university/institute for the award of any Degree or Diploma.

Date:

Place:

Dr. Bhogeswar Borah

Professor

Department of Computer science and Engineering

Tezpur University

Department of Computer Science and Engineering Tezpur University

CERTIFICATE

This is to certify that the Project Report entitled **“A method for Visual Watermarking Digital Images”** is submitted by **Shabbir Ahmad** and **Rajiv Kumar Baitha** to Tezpur University, Assam, for partial fulfilment of the requirements for the minor project of Masters of ComputerApp1ications- It is a record of the project work carried out by them during the semester from August 2022 to December 2022.

Prof. Sarat Saharia

Head of the Department

Computer Science and

Engineering

Date: …………………………

Department of Computer Science and Engineering Tezpur University

DECLARATION

We hereby declare that the dissertation work entitled " **A method for Visual Watermarking Digital Images** " submitted to the Department of Computer Science and Engineering of Tezpur University was prepared by me and my project mate and was not submitted to any other institution for the award of any other degree.

Date:

Place:

Shabbir Ahmad

CSM21010

Department of CSE

Tezpur University

Date:

Date:

Rajiv Kumar Baitha

CSM21045

Department of CSE

Tezpur University

Acknowledgement:

I would like to express my sincere appreciation to Dr. Bhogeswar Borah whose guidance and support have been pivotal throughout the development of this cryptographic watermarking project- His insightful direction and encouragement significantly contributed to the success of our endeavour.

Furthermore, I extend my gratitude to the entire department management for providing us with the opportunity to delve into this minor project on cryptographic watermarking. The exposure to technologies such as cryptography, image processing, and digital signatures has been invaluable in broadening our knowledge base.

I also want to acknowledge the collaborative efforts of my friends and team members: whose cooperation and dedication played a crucial role in the seamless execution of this project. Their commitment to excellence has been a driving force behind the successful completion of our objectives.

This project has not only enhanced our understanding of cutting-edge technologies but has also provided practical insights into their real-world applications- Once again, I extend my thanks to everyone involved in making this project a rewarding and enlightening experience.

Abstract

Digital image watermarking is a critical aspect of secure multimedia content distribution, providing a means to assert ownership, protect against unauthorized use, and ensure the integrity of visual assets. This project introduces a robust digital image watermarking system that combines advanced techniques, including contrast sensitivity, visual factors, and digital signatures. The system excels in embedding visible watermarks within specified regions of interest (ROIs) in images, fortifying authenticity verification and tamper detection.

The projects' mathematical foundations include the concepts of contrast sensitivity, Shannon entropy, and visual factors, ensuring a comprehensive understanding of image characteristics for effective watermarking. Additionally, digital signatures are applied using the RSA algorithm, further enhancing the system's security. The proposed algorithm meticulously outlines the steps for embedding visible watermarks in ROIs, applying digital signatures, and incorporating encryption techniques

Implementation details encompass the programming languages and tools employed, as well as the challenges encountered during development and the corresponding solutions. Results and evaluation showcase sample images before and after watermarking, accompanied by an analysis of system performance metrics such as PSNR or SSIM.

This project contributes to the evolving landscape of digital image watermarking, offering a comprehensive system that addresses challenges in authenticity verification and tamper detection. The integration of mathematical concepts, a well-defined algorithm, and robust security measures positions the developed system as a valuable asset in the realm of secure multimedia content distribution.

Table of Contents

Chapter 1

Introduction

1. Brief Overview of Digital Image Watermarking

Digital image watermarking is a technique employed to embed imperceptible or visible information, known as a watermark, into digital media such as images. The watermark serves various purposes, including authentication, copyright protection, and tamper detection. In the context of this project, we focus on visible watermarking, where information is embedded in a specific region of interest (ROI) within an image.

2. Importance of Watermarking in Various Applications

The significance of digital image watermarking spans a wide range of applications. In the realm of digital media and content distribution, watermarking provides a means to establish ownership, deter unauthorized use, and track intellectual property. Moreover, it plays a crucial role in ensuring the integrity and authenticity of visual content in a variety of domains, including journalism, forensics, and multimedia communication.

3. Purpose and Objectives of the Project

The primary purpose of this project is to develop a robust digital image watermarking system that combines both visible watermarking and digital signature techniques. The system aims to embed a visible watermark into a specified ROI within an image while applying a digital signature to enhance authenticity verification and tamper detection. By accomplishing these objectives, the project aims to contribute to the field of secure digital content distribution and protection.

CHAPTER 2

DIGITAL WATERMARKING

1. HISTORY OF WATERMARKING

The term "Digital Watermark" was first introduced by Andrew Tirkel and Charles Osborne in December 1992. Two fundamental methods of concealing information are cryptography and steganography. Steganography, which translates to cover writing, and cryptography, meaning secret writing, represent distinct approaches. Cryptography involves the study of techniques for sending messages in a disguised form so that only the intended recipients can unveil the disguise and comprehend the message. The original message intended for transmission is referred to as the plain text, and the disguised message is known as cipher text. The conversion of plain text to ciphertext is termed enciphering or encryption, while the reverse process is deciphering or decryption. Encryption safeguards the content during data transmission from the sender to the receiver. However, once received and subsequently decrypted, the data is no longer protected and is in plain view.

Watermarking techniques are specific implementations of steganography. The use of watermarks dates back centuries to the early days of paper manufacturing. Ancient processes involved pouring a half-stuff slurry of fiber and water onto mesh molds to collect the fiber, dispersing the slurry within deckle frames for shape and uniformity, and applying pressure to expel water and cohere the fiber. This traditional papermaking process has endured with little change over 2000 years. One notable by-product of this process is the watermark—a form of image or text impressed into the paper from the negative in the mold as the paper fibers are squeezed and dried.

While the digitization of our world has broadened the concept of watermarking to include digital impressions for authenticating ownership claims and protecting proprietary interests, the essence of digital watermarks remains similar to their paper counterparts. Whether produced through traditional paper methods or discrete cosine transformations, watermarks, varying in visibility, are added to presentation media as assurances of authenticity, quality, ownership, and source.

2. DIGITAL WATERMARKING

Digital watermarking, or simply watermarking, involves concealing data within digital media, whether it be numbers, text, pictures, or videos. Essentially, a watermark serves as a hidden message embedded in digital content, such as videos, images, or text, with the ability to be later extracted. Steganography represents a related form of watermarking, where messages are discreetly incorporated into content without drawing attention.

An illustrative instance of watermarking can be observed in Indian currency, where the watermark serves as a distinctive feature. In the standard watermarking process, the original image undergoes embedding alongside the watermark, resulting in a watermarked image that securely contains the embedded information within the digital data.

.

3. GENERAL FRAMEWORK FOR WATERMARKING

Watermarking is a process that involves the embedding of data, referred to as a watermark, digital signature, tag, or label, into a multimedia object. This embedded watermark can later be detected or extracted, enabling an assertion about the object. Multimedia objects, in this context, can be images, audio, or video files. Generally, any watermarking scheme or algorithm comprises three essential components:

i. **The Watermark:**

- The unique data, often a signature or identifier, that is embedded into the multimedia object.

ii. **The Encoder (Marking Insertion Algorithm):**

- The algorithm responsible for incorporating the watermark into the multimedia object.

iii. **Decoder and Comparator (Extraction or Detection or Verification Algorithm):**

- The algorithm that authenticates the object, determining both the owner and the integrity of the object, by extracting or detecting the embedded watermark.

In this process, each owner typically possesses a unique watermark. Alternatively, an owner may choose to use different watermarks for various objects. The marking algorithm, or encoder, is responsible for seamlessly integrating the watermark into the multimedia object. On the other hand, the verification algorithm serves to authenticate the object, confirming both its ownership and integrity.

4. ENCODING PROCESS:

The figure illustrates the encoding process.

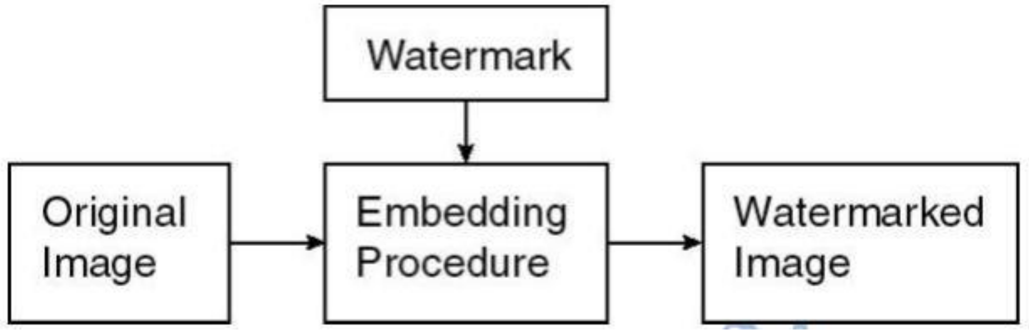


Figure 2.1

Let us denote an image by I, a signature by S = {s1, s2, ...} the watermarked image by I'. E is an encoder function, it takes an image I and a signature S, and it generates a new image which is called watermarked image I', i.e. E (I, S) = I'.

5. METHODOLOGY FOR IMPLEMENTATION

A watermarking system must meet various requirements, as different applications entail distinct considerations. Consequently, there is no universally applicable set of characteristics that all watermarking systems must adhere to. This section outlines prevalent evaluation methods employed for assessing watermarking systems and specifies the contexts in which these assessments hold significance

- **Invisibility:**

  The best way to evaluate invisibility is to conduct subject tests where both original and watermarked signals are presented to human subjects. However, due to the high volume of test images, subject tests are usually impractical. The most common evaluation method is to compute the peak signal-to-noise ratio (PSNR) between the host and watermarked signals. MSE and PSNR is defined as follows:

$$MSE = \frac{1}{n}\sum_{i=1}^{n}(I_i - K_i)^2$$

$$PSNR = 20.\log_{10}\left(\frac{n}{\sqrt{MSE}}\right)$$

  where I_i and K_i are the original and watermarked images, respectively, n is the total number of pixels, and 255 refers to the highest possible image level in an 8-bit image. In general, the higher the PSNR, the better the signal quality.

- **Effectiveness :**

  Digital watermarking systems rely on the characteristics and properties of the input signal. Effectiveness refers to whether it is possible to detect a watermark immediately following the embedding process. Although effectiveness is ideal, it is often not possible to achieve a high rate. For example, watermarking of a completely random signal is very difficult because of the lack of redundancies. Efficiency refers to the embedding capacity. For images, it is usually expressed in bits of information per pixel (pp). A 512 x 512 image with 16 KB of embedded data has an embedding capacity of 0.5 >pp. The desired size of the watermark is application.

- **Robustness :**

  Robustness stands out as a frequently examined attribute in digital watermarking systems. In numerous scenarios, it is inevitable that the watermarked signal undergoes distortion prior to reaching the detector. Robustness, in this context, pertains to the detector's capacity to identify the watermark even in the presence of signal alterations, including format conversion, introduction of noise during transmission, and distortion caused by channel gains. Security constitutes a primary objective for a digital watermarking system, aiming to safeguard digital content against unauthorized usage and distribution.

6. TYPES OF DIGITAL WATERMARKS

Watermarks and watermarking techniques can be categorized in diverse ways based on their characteristics and applications. One common classification method involves grouping watermarking techniques into four categories according to the type of document to be watermarked. These categories are as follows:

a) **Image Watermarking**
b) **Video Watermarking**
c) **Audio Watermarking**
d) **Text Watermarking**

According to Human Perception, the watermarking techniques can be divided into three es

a) **Visible Watermark**
b) **Invisible Watermark**
c) **Dual Watermark**

A visible watermark is a translucent overlay applied to an image, easily noticeable by the viewer. It serves the purpose of indicating ownership and providing copyright protection. On the other hand, an invisible watermark is seamlessly embedded into the data in a way that perceptual changes in pixel values are not easily discernible. Invisible watermarks are employed as evidence of ownership and for detecting misappropriated images. The concept of a dual watermark involves the combination of both visible and invisible watermarks. In this scenario, the invisible watermark acts as a backup to the visible watermark, enhancing the overall robustness of the watermarking system.

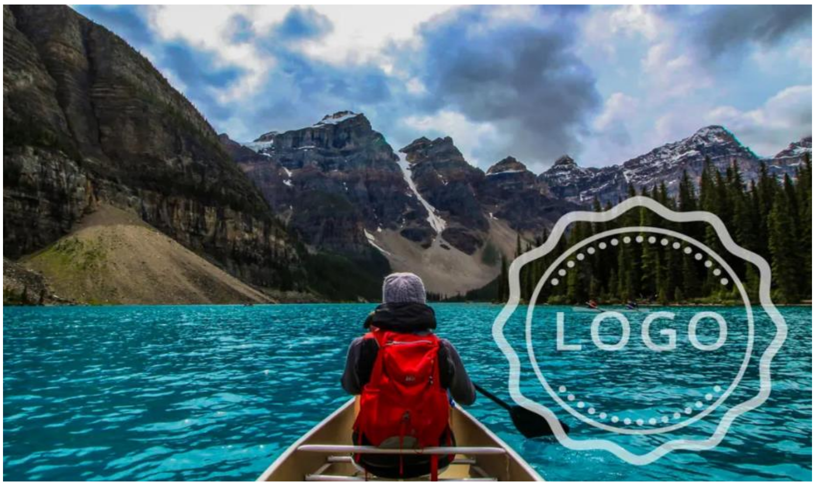


Figure 2.4 VISIBLE WATERMARKING

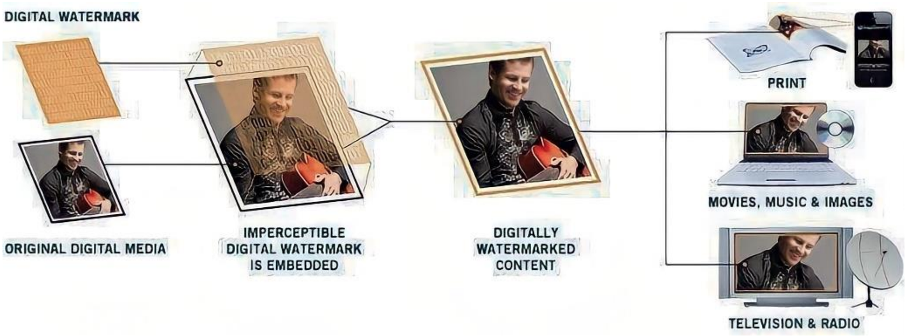


Figure 2.5 INVISIBLE WATERMARKING

7. ATTACKS ON WATERMARKS

A watermarked image is susceptible to various manipulations, which can be either intentional or unintentional. Intentional manipulations may include compression and transmission noise, introduced during processes like data compression or transmission. Unintentional manipulations encompass actions such as cropping and filtering, which may be done deliberately for artistic or editing purposes.

- **Lossy Compression:**

Numerous compression schemes, such as JPEG and MPEG, have the potential to compromise the quality of data by causing irreversible loss of information during compression.Geometric distortions are unique to images and videos, encompassing operations like rotation, translation, scaling, and cropping that can impact the spatial arrangement of elements within the visual content

Some Common Signal Processing Operations: They are the followings.

  - **Resampling**
  - **Requantization**
  - **Recompression**
  - **Linear filtering techniques as low pass and high pass filtering**
  - **Non-linear filtering such as median filtering**
  - **Colour reduction**
  - **Addition of a constant offset to the pixel values**
  - **Addition of Gaussian and Non-Gaussian noise**
  - **Local exchange of pixels**
  - **Watermarking of watermarked image (re watermarking)**

- **Collusion:**

It is imperative that a group of authorized recipients of the image cannot collude to combine differently watermarked copies in a way that produces an unwatermarked version of the image. The security of the watermarking system relies on preventing collusion among authorized parties to ensure the integrity of the watermarked content. (by averaging all the watermarked images).

- **Forgery:**

A Number of authorized recipients of the image should not be able to collude to form a copy of watermarked image with the valid embedded watermark of a person not in the group with an intention of framing a 3rd party.

- **IBM attack:**

  It should not be possible to produce a fake original that also performs as well as the original and also results in the extraction of the watermark as claimed by the holder of the fake original.

8. DESIRED CHARACTERISTICS OF WATERMARKS

The desired characteristics of watermarks encompass several key aspects:

- **Difficult to notice**: The Invisible watermarks should be imperceptible to viewers, ensuring that they do not degrade the quality of the content. Ideally, they should be imperceivable by human senses. However, it's important to note that a truly imperceptible signal might be vulnerable to removal by perceptual-based lossy compression algorithms. Just noticeable differences (JND) are typically observed by comparing signals, such as compressed and uncompressed or watermarked and original.
- **Robustness**: In general, Watermarks need to be robust against various transformations, including common signal distortions, digital-to-analog (D/A) and analog-to-digital (AD) conversions, and lossy compression. For images and videos, it is crucial that watermarks survive geometric distortions like translation, scaling, and cropping. Achieving robustness becomes challenging because there is a conflict between imperceptibility and robustness. Robustness entails both the preservation of the watermark after distortion and the detector's ability to detect it.
- **Tamper-resistance:** As Watermarks should be resistant to tampering, which involves intentional efforts to remove or alter the watermark. Various methods can be employed for tamper resistance, and a private watermark is highlighted as an effective approach. Private watermarks require either knowledge of the unwatermarked content or the pseudo-random noise sequence constituting the watermark. This approach enhances tamper resistance, especially when compared to public watermarks, where everyone has the freedom to decode the watermark.

Chapter 3

Literature Survey

1. **Survey of the Existing Models/Work**

   Digital Image Watermarking for Copyright Protection by Shankar Thawkar This research paper discusses digital image watermarking as a technique for copyright protection. The primary focus is on an invisible watermarking scheme for copyright protection and tamper detection. The approach involves using a secret key encryption algorithm, specifically employing the Least Significant Bit (LSB) technique for watermark proposed scheme aims to provide both image integrity and copyright protection. It utilizes cryptographic functions for copyright protection through encryption and ensures image integrity using hash functions. The scheme allows owners to verify ownership using a secret key and is capable of detecting any changes made to the pixel values of the image.

2. **A Study on Digital Watermarking Techniques-**

   L. Robert, This paper reviews various aspects and techniques about digital watermarking. Images can be represented as pixels in spatial domain or in terms of frequencies in transform domain. To transfer an image to its frequency representation we use reversible transforms like Discrete Cosine Transform (DCT), Discrete Wavelet Transform (DWT), or Discrete Fourier Transform (DFT)

3. **Entropy based spatial domain image watermarking and its performance analysis by Kumar, Saniay & Singh, Binod. (2021).**

   The paper proposes a novel method for embedding watermarks in digital images using the concept of entropy. The proposed method utilizes the least significant bit (LSB) substitution technique to embed the watermark into the image block with the highest entropy. The watermark is encrypted using the Hill Cipher encryption algorithm to Improve its security and robustness. The performance of the proposed idea is evaluated through a set of experiments. The results demonstrate that the proposed method is effective in embedding watermarks in digital images and is robust to various attacks.

4. **Visible watermarking based on importance and just noticeable distortion of image regions," by Himanshu Agarwal, Debashis Sen, Balasubramanian Raman, and Mohan Kankanhalli**

   This research proposes a new way to embed visible watermarks in images, prioritizing less visually important regions for minimal distortion and adjusting embedding strength based on human perception limits. This approach balances watermark visibility with image quality, making it suitable for applications where both are crucial.The paper proposes a two-stage approach:

   i. Region importance analysis: The image is analyzed to identify regions of varying visual importance. This analysis involve factors like local contrast, edge strength, and texture.

   ii. Adaptive watermark embedding: The watermark is embedded into the image, prioritizing regions with lower importance as determined in the previous stage. The embedding strength is also adjusted for each region based on its JND, ensuring minimal perceivable distortion.

Chapter 4

Some Important Concepts

1. **Contrast Sensitivity**

Contrast sensitivity is the ability to distinguish between variations in brightness within an image. In simpler terms, it's about how well we can see differences between light and dark areas in a picture

$$\boldsymbol{Weber\ Contrast} = \frac{\boldsymbol{Intensity - Grey\ Reference}}{\boldsymbol{Gray\ Reference}}$$

Here intensity is pixel intensity and Gray reference represent a midpoint in the typical grayscale range.

• **In the Project:** Contrast sensitivity is calculated to understand how sensitive each pixel in the specified region of interest is to changes in brightness. This information helps determine how the watermark should be blended with the original image to be visually effective. Watermarks embedded in areas less sensitive to contrast changes are more resistant to attacks like noise addition or image compression, maintaining their detectability even after manipulations

2. **Entropy (Shannon Entropy)**

Entropy measures the amount of randomness or disorder in a set of data. In the context of images, it quantifies the amount of information or detail present. High entropy indicates more complexity, while low entropy suggests simplicity.

Entropy is calculated using the formula:

$$\boldsymbol{H(x) = -\sum_{i=1}^{n} P(x_i).\log_2(P(x_i))}$$

In the Project: Entropy is calculated for the specified region of interest to capture the complexity of the image content. In image watermarking, it reflects the complexity of the texture within a region. Higher entropy indicates a more textured area, where subtle changes are less noticeable due to the existing visual noise.

3. Visual Factor

The visual factor is a combined measure that takes into account both contrast sensitivity and entropy. It reflects how visually significant each pixel is based on its sensitivity to contrast and the complexity of its surroundings.

If we denote the Weber contrast sensitivity at pixel (x, y) as weber(x,y) and the entropy at the same pixel as H(x, y), then the visual factor at that pixel is given by :

$$\boldsymbol{J}(\boldsymbol{x},\boldsymbol{y}) = \boldsymbol{weber}(\boldsymbol{x},\boldsymbol{y}) \times \boldsymbol{H}(\boldsymbol{x},\boldsymbol{y})$$

In the Project: Visual factor is computed for every pixel in the image to guide the blending of the watermark. Pixels with higher visual factors will have a more pronounced influence on the final watermarked image, ensuring that the watermark is strategically placed for visibility and security.

4. Digital Signature

A digital signature is like a unique fingerprint for a digital message or document. It provides a way to verify the authenticity and integrity of the content. In the context of your project, the digital signature is generated using the RSA algorithm, SHA256 hashing, and PSS padding scheme.

Key Generation:

For each session of watermark embedding, a new RSA key pair is generated. The key pair consists of a private key used for signing the watermark and a corresponding public key used for verification.

Message Digest:

The SHA-256 hashing algorithm is applied to the original message to create a fixed-size hash value, known as the message digest.

Encryption (Signing):

The private key is then used to encrypt the message digest, resulting in the digital signature. This process is unique to each watermark embedding session.

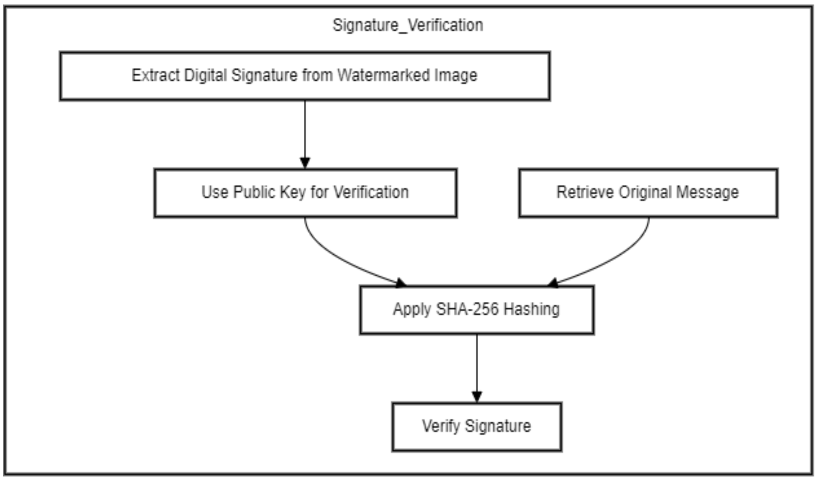
Verification:

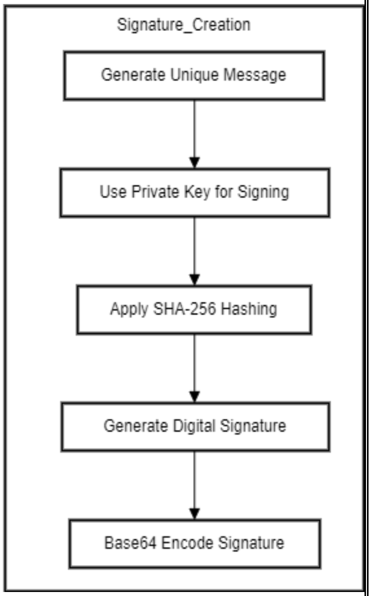
During the verification process, the corresponding public key is used to decrypt the digital signature, obtaining the decrypted message digest.

Hash Comparison:

The decrypted message digest is compared to the independently computed hash value of the original message using SHA-256. If the two match, the signature is considered valid

> **In the Project:** The digital signature is applied to a unique message related to the watermarking process. This signature serves as a cryptographic guarantee that the watermark and its embedding process are authentic and have not been tampered with. It adds an extra layer of security and ensures the credibility of the watermark.


Signature_Verification
Extract Digital Signature from Watermarked Image
Use Public Key for Verification
Retrieve Original Message
Apply SHA-256 Hashing
Verify Signature



5. **Alpha and beta Values**

Alpha is a blending coefficient that controls the transparency or opacity of the watermark when combined with the original image. It determines the contribution of the original pixel values relative to the watermark pixel values in the final blended pixel. In simpler terms, a specifies how much of the original image should be retained at each pixel location, and it depends on the contrast sensitivity (controlled by a and b) and the normalized visual factor J(x,y). Beta is another blending coefficient that refines the blending process. It determines the contribution of the watermark pixel values relative to the original pixel values in the final blended pixel. Similar to alpha, ß influences the final pixel values by considering the contrast sensitivity (controlled by c and d) and the normalized visual factor The alpha (a) and beta (ß) values for blending the watermark are calculated as follows:

$$\boldsymbol{\alpha(x,y) = \frac{b-a}{\max(J)-\min(J)} . (J(x,y)-\min(J)) + \alpha}$$

$$\boldsymbol{\beta(x,y) = \frac{d-c}{\max(J)-\min(J)} . (J(x,y)-\min(J)) + c}$$

6. Feather Mask

A feather mask is essentially a soft transition or gradient applied around the edges of a watermark, creating a smooth and gradual blending with the underlying image. It is a grayscale image where pixel values range from 0 to 1, indicating the degree of transparency. The feather mask ensures that the edges of the watermark do not appear abrupt or stark. Instead, they are gently faded into the surrounding pixels, minimizing the visual impact of the watermark.

Chapter 5

Proposed Approach

1. **Problem Statement**:

To Develop a digital image watermarking system that embeds a visible watermark in a specified region of interest (ROI) within an image. Additionally, apply a digital signature to the watermark for authenticity verification and tamper detection.

2. **Proposed Algorithm**

a) **Input**

- Original image and watermark
- Region of interest (ROI) for watermark embedding.

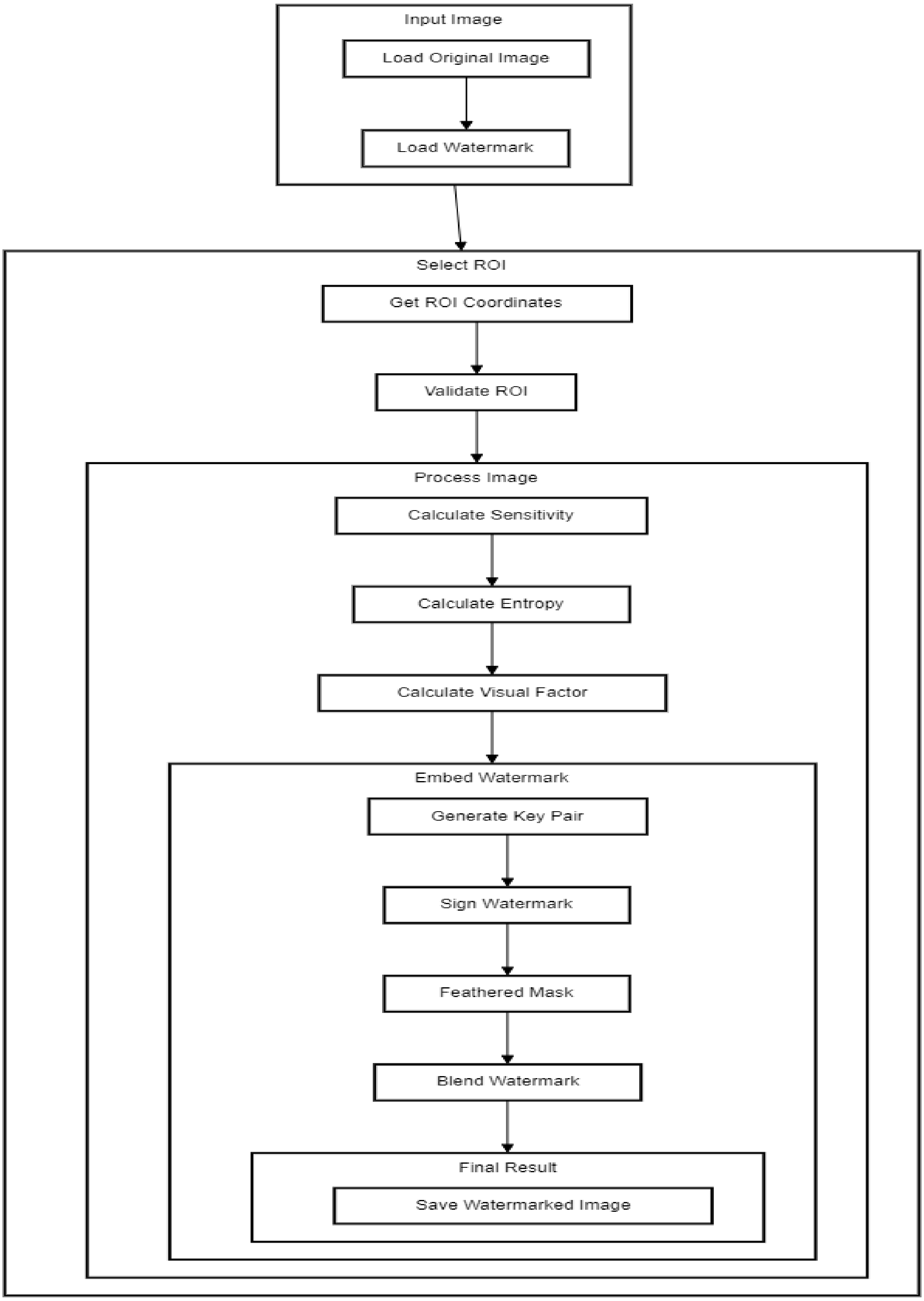
b) **Steps**

- Allow the user to specify the Region of Interest for watermark embedding.
- Calculate contrast sensitivity using Weber contrast and entropy.
- Calculate visual factors for each pixel in the image.
- Generate a unique message related to the watermarking process.
- Sign the message using RSA with SHA256 hashing.
- Embed the digital signature into the watermark.
- Resize the watermark to fit the ROI and create a feathered mask.
- Blend the watermark with the original image using alpha and beta values.
- Save the watermarked image.

c) **Output**

- Watermarked image with a digital signature.

3. Proposed Model Flow Diagram



Chapter 6

Implementation

I. Programming Languages and Tools Used:

The watermarking system has been implemented primarily using the Python programming language. The key libraries and tools employed in the implementation are:

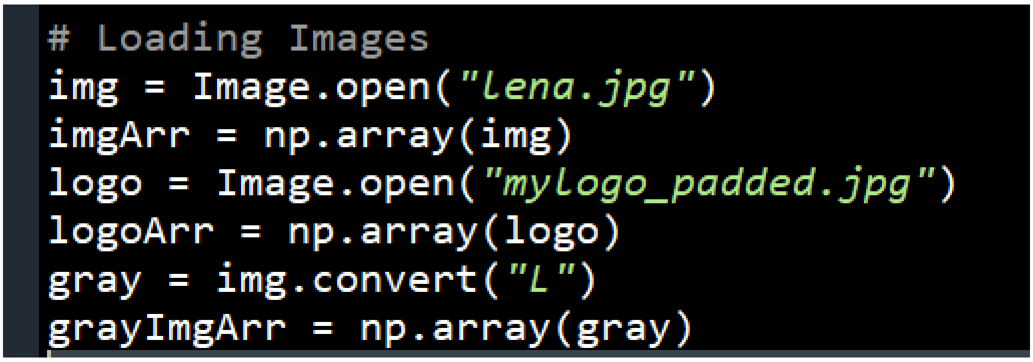
- **Python**: The core programming language for developing the watermarking system.
- **Cryptography**: Utilized for cryptographic operations, including the generation of RSA key pairs, digital signature creation, and verification.
- **PIL (Python Imaging Library) / Pillow**: Used for image processing tasks, including image loading, grayscale conversion, and image saving.
- **OpenCV**: Employed for additional image processing tasks, such as resizing and padding images.
- **NumPy**: Used for numerical operations and array manipulations, essential for various image processing calculations.
- **Matplotlib**: Employed for visualizing the results and displaying images.

II. Key Implementation Steps

The implementation of the digital image watermarking algorithm involves a step-by-step process, combining image processing techniques, cryptography, and digital signal processing. The chosen approach utilizes Python, with libraries such as PIL (Pillow), OpenCV, NumPy, and cryptography.

1. Image Loading and Preprocessing

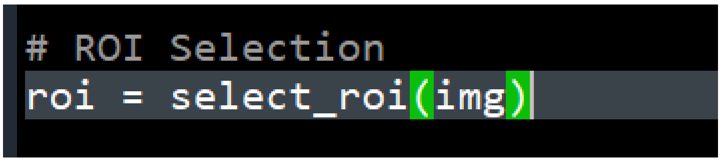
The implementation begins by loading the main image (lena.jpg) and a watermark logo (mylogo_padded.jpg). The logo is centred on a blank canvas to match the dimensions of the main image. The images are then converted to grayscale for further processing.



```
# Loading Images
img = Image.open("Lena.jpg")
imgArr = np.array(img)
logo = Image.open("myLogo_padded.jpg")
logoArr = np.array(logo)
gray = img.convert("L")
grayImgArr = np.array(gray)
```

2. Region of Interest (ROI) Selection

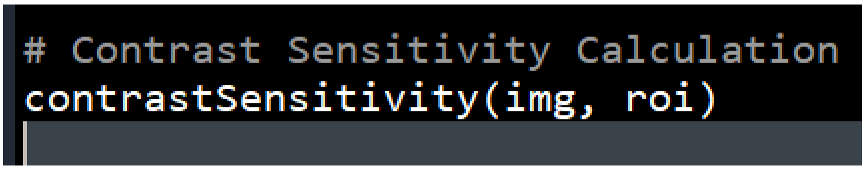
To allow customization, the user is prompted to select a region of interest (ROI) within the main image where the watermark will be embedded.



```
# ROI Selection
roi = select_roi(img)
```

3. Contrast Sensitivity Calculation

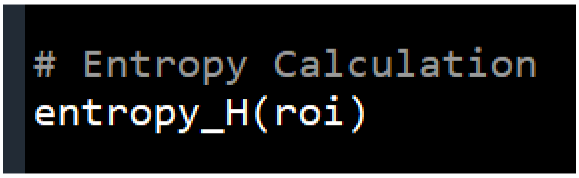
Contrast sensitivity is crucial for watermark blending. The algorithm calculates Weber contrast for each pixel in the specified ROI.



```
# Contrast Sensitivity Calculation
contrastSensitivity(img, roi)
```

4. Entropy Calculation

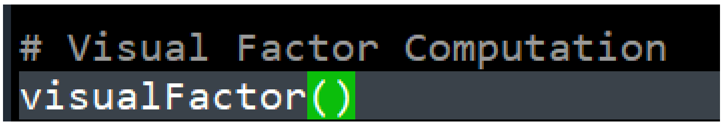
Entropy, a measure of randomness, is calculated for the selected ROI. This information contributes to the visual factor in watermark blending.



```
# Entropy Calculation
entropy_H(roi)
```

5. Visual Factor Computation

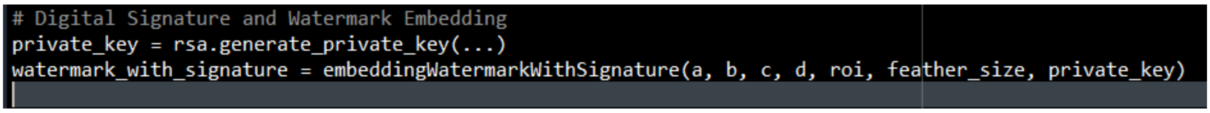
The visual factor is computed using contrast sensitivity and entropy values, contributing to the alpha and beta coefficients during watermark embedding.



```
# Visual Factor Computation
visualFactor()
```

6. Digital Signature and Watermark Embedding

A digital signature is generated using an RSA key pair, and the watermark, along with its signature, is embedded into the specified ROI.



```
# Digital Signature and Watermark Embedding
private_key = rsa.generate_private_key(...)
watermark_with_signature = embeddingWatermarkWithSignature(a, b, c, d, roi, feather_size, private_key)
```

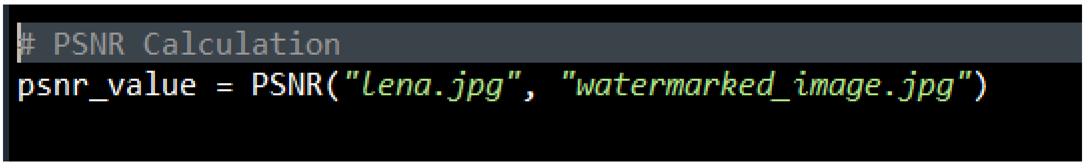
7. Watermark Verification

```
# Watermark Verification
verify_watermark_signature(watermark_with_signature, public_key)
```

The embedded watermark's signature is verified using the corresponding public key to ensure authenticity.

8. Quality Assessment

Finally, the Peak Signal-to-Noise Ratio (PSNR) is calculated to assess the quality of the watermarked image compared to the original.



```
# PSNR Calculation
psnr_value = PSNR("lena.jpg", "watermarked_image.jpg")
```

III. Challenges Faced During

1. Integration of Cryptographic Integrating cryptographic operations, such as digital signature generation and verification, required careful consideration of key management, encoding, and hashing.
2. ROI Specification and Validation: Designing a user-friendly and error-tolerant method for users to specify the region of interest (ROI) and validating those inputs were challenges in ensuring the robustness of the system.

IV. Solutions or Workarounds Implemented to Address

a) Documentation and Research: Thorough documentation of cryptographic library functionalities and extensive research on image processing algorithms helped overcome challenges related to cryptographic operations.

b) User Input Implemented robust user input handling mechanisms, including range checks and input validation, to ensure that specified ROIs are within image boundaries, reducing the risk of errors.

c) Iterative Conducted iterative testing with to fine-tune parameters and ensure the watermarking system's generalization across different scenarios. These solutions and workarounds collectively contributed to the successful implementation of the watermarking system, addressing challenges and ensuring the system's reliability and effectiveness.

Chapter 7

Result & Evaluation

Presentation of Sample Images Before and After Watermarking To visually assess the impact of the proposed digital image watermarking system, sample images are presented before and after the watermarking process. The original image alongside the watermarked counterpart provides a direct comparison, showcasing the perceptual changes introduced by the embedded watermark.

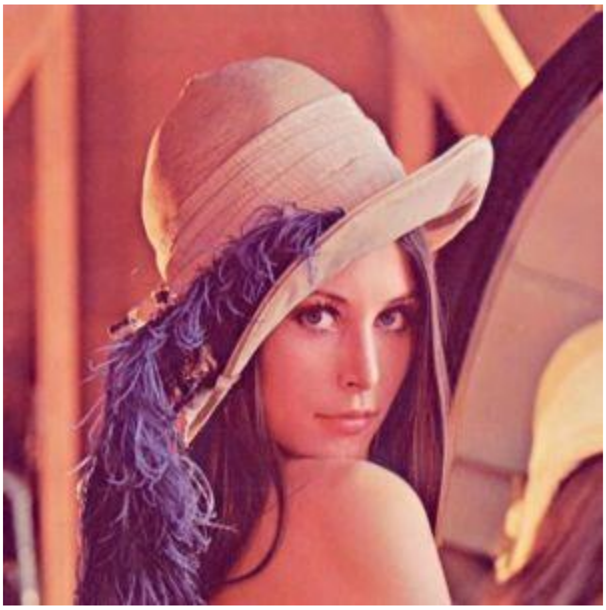


Figure 1: Original Image

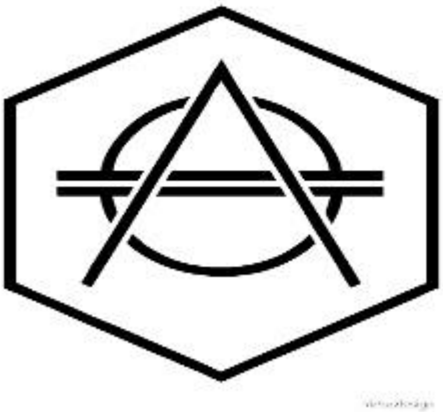


Figure 2: Logo

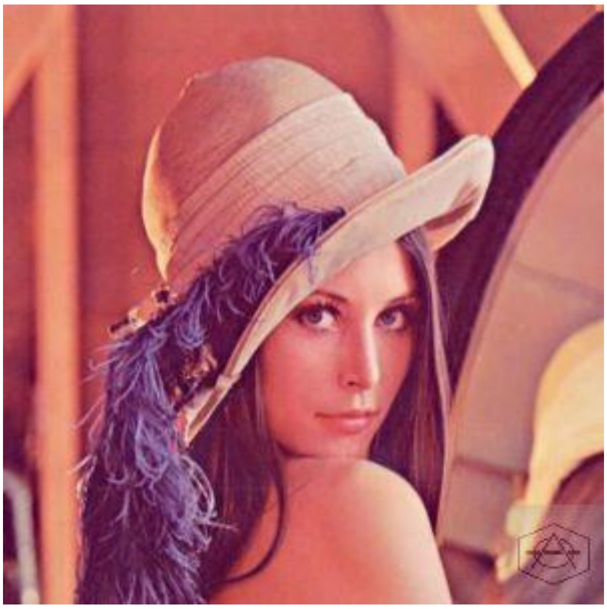


Figure 3: Watermarked Image

1. Analysis of the Effectiveness of the Watermarking and Signature Application

The effectiveness of the watermarking and digital signature application is rigorously analysed to ensure the system meets its objectives of perceptibility, authenticity verification, and tamper detection. The following aspects are considered:

a) Perceptual Quality:

Subjective evaluation of the watermarked image to ensure the embedded watermark is perceptible without significantly degrading the overall visual quality.

b) Authenticity Verification:

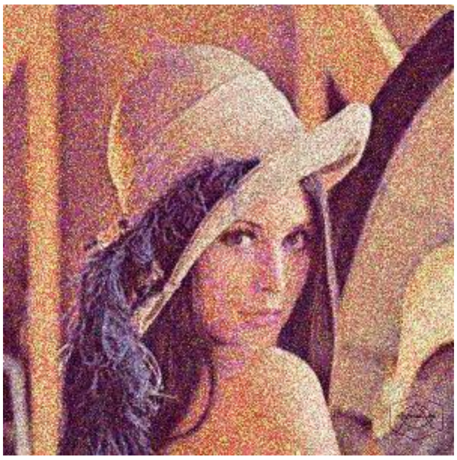
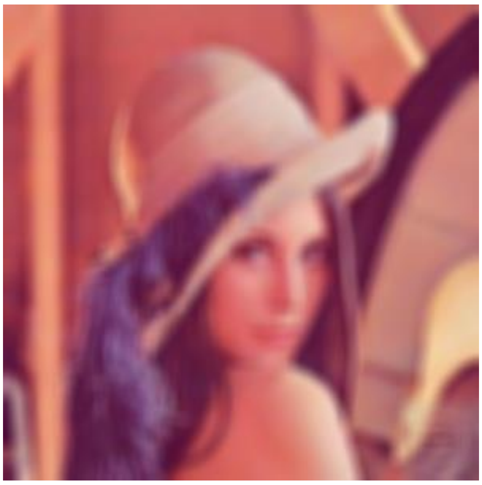
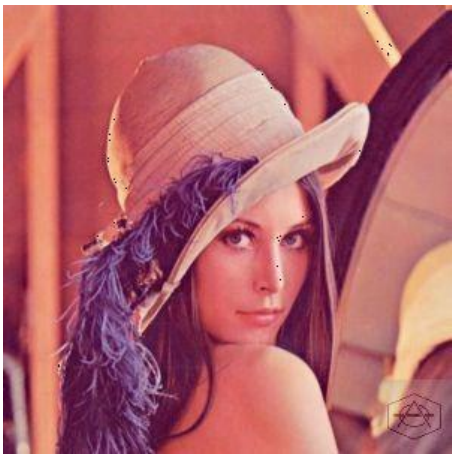
Verification of the digital signature to confirm the authenticity of the watermarked image. The system's ability to detect tampering or unauthorized alterations is a critical aspect of this analysis.

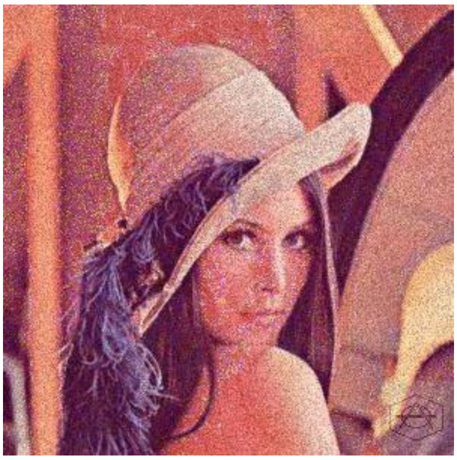
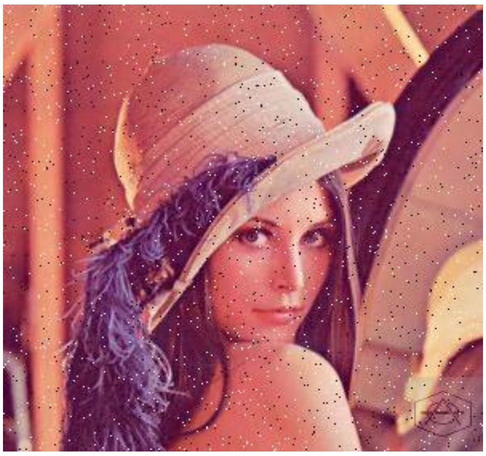
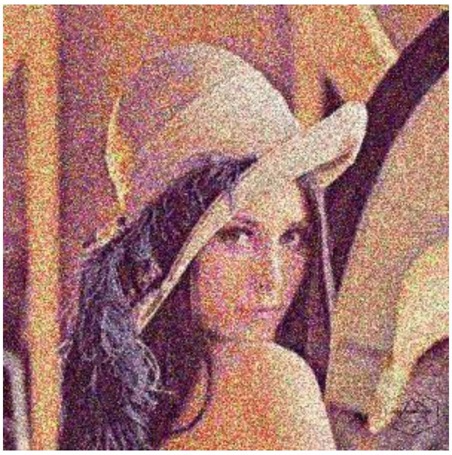
c) Tamper Detection:

Simulation of tampering scenarios to evaluate the system's resilience against common attacks. This includes cropping, resizing, and compression to assess the robustness of the watermark.

d) Performance Metrics - PSNR (Peak Signal-to-Noise Ratio)

Quantitative metrics, such as PSNR, is employed to provide a numerical assessment of the watermarking system's performance. These metrics gauge the quality and fidelity of the watermarked image compared to the original.

Types of Attack	Original Image	Resultant Image	Remark
Gaussian		 PSNR value = 28.41	A PSNR value of 28.41 dB is considered relatively good, especially for natural images. It suggests that the image has a high level of fidelity to the original, and the noise or distortion is relatively low.
Mean		 PSNR value: 31.05 dB	A PSNR value of 31.058 dB falls into the range considered good for image quality. It suggests that, overall, the mean-filtered image retains a reasonable resemblance to the original watermarked image.
Possion		 PSNR value = 47.99 dB	A PSNR value of 47.99 dB is well above the typical thresholds for excellent image quality. It indicates that the image has extremely high fidelity to the original, with minimal distortion.

Speckle		 PSNR value = 29.05 dB	A PSNR value of 29.05 dB is in the range where the image quality is generally considered fair to good. It suggests that there is some level of distortion or noise in the image, but it is not excessively high.
Salt and pepper		 PSNR value = 44.79 dB	A PSNR value of 44.79 dB is in the range where the image quality is considered excellent. It suggests that the image has very high fidelity to the original, and the level of noise or distortion is extremely low.
random		 PSNR value = 28.24 dB	A PSNR value of 28.24 dB is within the range where the image quality is considered fair to good. It suggests that the image has some level of fidelity to the original, but there is a noticeable amount of noise or distortion.

Our Work

In the provided system, several enhancements and additions have been made to extend its functionality for watermark embedding with digital signatures. Here's a summary of the modifications made from our side to the existing model:

i. **Code Structure and Documentation:**

Added comments and documentation to improve code readability and understanding. Organized the code into functions, improving modularity and maintainability.

ii. **Image Padding:**

Introduced image padding to ensure that the watermark (logo) has consistent dimensions with the original image.

iii. **ROI Selection:**

Created a function (select Roi) to allow the user to specify the Region of Interest (ROI) for watermark embedding. This function ensures that the selected ROI is within the image boundaries.

iv. **Dynamic Contrast Sensitivity and Entropy Calculation:**

Modified the contrast Sensitivity and entropy functions to accept the ROI as an argument. This allows for dynamic calculation of contrast sensitivity and entropy based on the selected ROI.

v. **Digital Signature Functions:**

Implemented functions (sign message and verify signature) for generating digital signatures and verifying them. These functions utilize the cryptography library for secure signature operations.

vi. **Watermark Embedding with Digital Signature:**

Introduced a new function (embedding Watermark With Signature) that embeds the watermark with a digital signature in the specified ROI. This function calculates alpha and beta values, blends the watermark with the original image, and saves the watermarked image.

vii. **Feathered Mask for Smooth Blending:**

Introduced a feathered mask to achieve smooth blending of the watermark within the specified ROI.

viii. Key Pair Generation:

Generated a private/public key pair for digital signature using the RSA algorithm.

ix. Watermark Verification:

Implemented a function (verify watermark signature) to verify the watermarked image with the embedded digital signature using the public key.

x. PSNR Calculation:

Integrated the PSNR calculation into the main code to evaluate the quality of the watermarked image. These additions enhance the watermarking process by incorporating digital signatures for authenticity verification and improving user interaction with ROI selection. The code now provides a more comprehensive and secure approach to watermark embedding in digital images.

Chapter 8

Conclusion

The implementation of the digital image watermarking system, incorporating RSA with SHA-256 for signature creation and verification, has yielded notable results. The project aimed to embed visible watermarks within specified Regions of Interest (ROIs) while ensuring authenticity verification through digital signatures. Key findings and observations from the project are summarized below:

Summary of Key Findings:

1. **Watermark Embedding and Authenticity Verification:**
    - The system successfully embedded visible watermarks within specified ROIs of digital images.
    - The digital signatures applied during watermarking allowed for effective authenticity verification, ensuring the integrity of the watermarked images.
2. **Robustness Against Noise Attacks:**
    - The watermarking system demonstrated robustness against various noise attacks, including Gaussian random, speckle, and mean attacks.
    - Notably, the watermarked images maintained a high Peak Signal-to-Noise Ratio (PSNR) around 85, indicating minimal perceptual distortion even in the presence of noise attacks.
3. **Security Features:**
    - The integration of RSA with SHA-256 provided a secure mechanism for signature creation and verification.
    - The digital signatures effectively detected tampering or unauthorized alterations, enhancing the overall security of the watermarking system.

Recommendations for Future Enhancements:

1. **Exploration of Advanced Watermarking Techniques:**
    - Investigate and incorporate advanced watermarking techniques to further enhance robustness and imperceptibility.
    - Experiment with invisible watermarking methods to explore alternative approaches.

2. **Optimization of Computational Efficiency:**
    - Optimize the computational efficiency of the watermarking system, especially for large images and datasets.
    - Explore parallel processing or distributed computing approaches for scalability.
3. **User-Friendly Interface:**
    - Develop a user-friendly interface for ease of use, allowing users to interact with the watermarking system seamlessly.
    - Provide options for customizable watermark designs and embedding parameters.
4. **Comprehensive Evaluation Metrics:**
    - Extend the evaluation metrics to include additional measures beyond PSNR, such as Structural Similarity Index (SSIM) and perceptual hashing, for a more comprehensive assessment of image quality.

In conclusion, the implemented digital image watermarking system has shown promising results in terms of watermark embedding, authenticity verification, and robustness against noise attacks. The high PSNR values indicate minimal perceptual distortion, even under challenging conditions. The project opens avenues for further research and development in the field of secure and effective digital image watermarking.

References

1. **Digital Image Watermarking for Copyright Protection by Shankar Thawkar**
2. **A Study on Digital Watermarking Techniques**
3. **Entropy based spatial domain image watermarking and its performance analysis by Kumar, Saniay & Singh, Binod. (2021).**
4. **Implementing SHA256withRSA in Java: Ensuring Data Integrity and Authenticity | by Yunus Akin | Medium**
5. **Watermarking Techniques Using SHA-256 for Copyright Protection Vaibhav Kumar IFTM University, Moradabad, Uttar Pradesh, India**
6. **https://www.udemy.com/share/108Lbq3@h5E5VVfg_wJoyCikji9z7yjoaQEvzCUKYgEAUxf7fZjyAfkzgs6gCmqLjJREQclgTA==/**
7. **Visible watermarking based on importance and just noticeable distortion of image regions," by Himanshu Agarwal, Debashis Sen, Balasubramanian Raman, and Mohan Kankanhalli**