MINISTRY OF EDUCATION
AND TRAINING

VIETNAM ACADEMY OF
SIENCE AND TECHNOLOGY

GRADUATE UNIVERSITY OF SIENCE AND TECHNOLOGY

PHẠM QUANG HUY

RESEARCH ON THE DEVELOPMENT OF SEVERAL WATERMARKING TECHNIQUES BASED ON TYPICAL CHARACTERISTIC REGIONS OF DIGITAL IMAGES

SUMMARY OF DISSERTATION ON INFORMATION SYSTEM
Code: 9 48 01 04

Ha noi - 2024

The dissertation is completed at: Graduate University of Science and Technology, Vietnam Academy of Science and Technology

Supervisors:

Supervisor 1: Assoc. Prof. Dr. Ta Minh Thanh

Supervisor 2: Dr. Dao Nam Anh

Referee 1: …

Referee 2: …

Referee 3: ….

The dissertation will be examined by Examination Board of Graduate University of Science and Technology, Vietnam Academy of Science and Technology at……………………….. (time, date, year…)

This dissertation can be found at:

1) Graduate University of Science and Technology Library
2) National Library of Vietnam

1. Problem Statement

In the current digital age, protecting the copyright of digital images has become extremely important and complex due to the widespread availability of the Internet and mobile devices, posing significant challenges in protecting intellectual property rights. Images are not only used in arts and entertainment but also in advertising, communication, education, and scientific research. Unauthorized copying and distribution of images without the permission of the rightful owner is easy, causing financial harm to authors and publishers, affecting creativity and innovation. The unauthorized use of images also leads to legal issues and disputes over rights.

2. Objectives of the dissertation

The objective of the dissertation is to develop and improve digital watermarking techniques based on the salient features of digital images to protect copyrights and manage digital assets. Specifically, the main objectives include:

i. Developing watermarking techniques based on non-salient regions to embed information into images without degrading visual quality.

ii. Applying machine learning and models for detecting saliency to select watermarking regions with greater accuracy.

iii. Improving methods of embedding data into JPEG images by using quantization tables to increase information capacity.

iv. Developing reversible watermarking techniques that ensure the original image can be fully restored after watermark extraction.

v. Evaluating the effectiveness of the proposed watermarking techniques under real-world conditions, focusing on both robustness and the integrity of the watermark.

These objectives aim to enhance the efficiency and applicability of watermarking methods in digital environments.

3. New contributions of the dissertation

The dissertation has two main contributions as follows:

i. Developing watermarking techniques based on the salient features of digital images to utilize visual features for embedding information into less noticeable regions of the image, making the watermark information difficult to detect by the naked eye without degrading the visual quality of the image; improving the ability to resist common attacks such as cropping, rotation, and compression, ensuring the robustness of the watermark information under various processing conditions.

ii. Developing reversible watermarking techniques that ensure the integrity of the original image, guaranteeing no changes in the original image quality; allowing the embedding of large amounts of data without significantly reducing the visual quality of the image, expanding the applicability in fields requiring high security.

4. Structure of the dissertation

The dissertation is divided into three main chapters:

- Chapter 1: Literature review and some fundamental knowledge
- Chapter 2: Analysis of the impact of image saliency in digital watermarking
- Chapter 3: Development of watermarking techniques ensuring the integrity of the original image

CHAPTER 1. LITERATURE REVIEW AND SOME FUNDAMENTAL KNOWLEDGE

1.1. Introduction

1.1.1. The origin and concept of digital watermarking

Digital watermarking is a technique of embedding information into digital data such as images, audio, or video for the purposes of copyright protection, origin authentication, or control of data copying. The term "watermark" originates from the mark on paper that becomes visible when the paper is soaked in water, but in the digital context, it refers to the subtle and hard-to-detect embedding of information into digital data. Digital watermarking began to be extensively researched and developed in the 1990s, playing a crucial role in copyright protection and combating copyright infringement in digital media.

1.1.2. Classification of digital watermarking

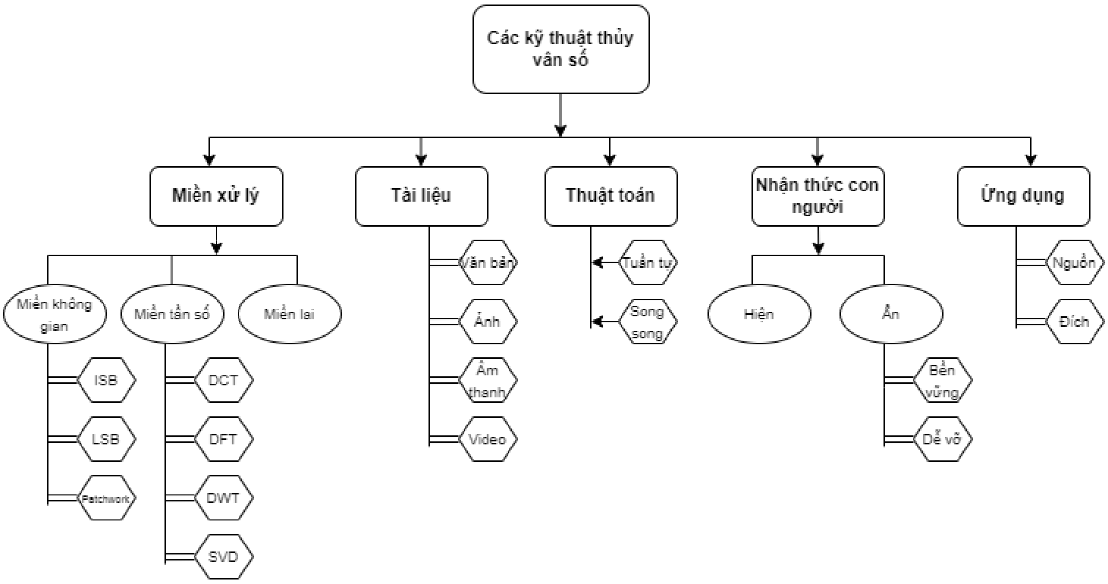


Figure 1.1: *Classification of digital watermarking*

The diagram based on Kumar [15] in Figure 1.1 provides an overview of recent advancements in the field of digital watermarking, including classifications based on the domain of implementation, the host environment, and human perception.

1.1.3. The process of building a digital watermarking model

Digital watermarks are created from images or text, typically encoded or transformed before being embedded into host data such as images, audio, or video. The embedding process uses a watermark key and embedding tools to generate data that is robust against noise and attacks. The extraction process uses an extractor and the key from the embedding process to produce a watermark that may be identical to or different from the original. There are two types of extraction: blind (does not require the original image) and non-blind (requires the original image).

1.1.4. Characteristics of digital watermarking

The characteristics of digital watermarking include key factors such as robustness, imperceptibility, and fragility. Robustness refers to the watermark's ability to withstand transformations such as compression, cropping, or filtering during image processing. Imperceptibility is the watermark's ability to avoid affecting the visual quality of the image, meaning that users cannot detect the presence of the watermark with the naked eye. Fragility is required in certain specific applications, where the watermark must be destroyed if any unauthorized alteration occurs to the data. These characteristics play a crucial role in ensuring the safety, security, and integrity of information in applications related to copyright protection and digital data security.

1.1.5. Evaluation criteria for digital watermarking

When evaluating the quality of digital image watermarking algorithms, the following important criteria should be considered:

1. **Confidentiality**: Assessing the level of "invisibility" of the watermark on the image, ensuring the protection of the watermark's confidentiality. However, in some cases, such as product authentication, revealing the watermark may be necessary.

2. **Integrity**: The ability to resist watermark tampering, a crucial factor in protecting copyright and legal recognition of the product.
3. **Robustness**: The watermark should withstand both intentional and unintentional attacks, including compression, resampling, filtering, and other transformations.
4. **Capacity**: Evaluating the storage and management capacity of the watermark, which is important for the use and security of digital watermark data.

Balancing quality (confidentiality, integrity, and robustness) and capacity is essential to creating effective watermarking solutions.

1.1.6. Applications of digital watermarking

Digital watermarking is an important tool in protecting intellectual property rights and managing copyright for digital images [7]. It not only ensures authorship and prevents unauthorized distribution, but also plays a crucial role in information verification and distortion detection [75]. Digital watermarking is also applied in user authentication [43] and supports access control in information management systems [69].

1.1.7. Common digital watermarking attack scenarios

In the modern context, digital watermarking is becoming an important information security tool. However, digital watermarking systems also face challenges from increasingly complex attack scenarios [70]. Common attacks include:

1. **Simple attacks**: Damaging the watermark by randomly altering pixels without needing to identify the specific watermark. The goal is to corrupt the watermark without retrieving information from it.
2. **Detection attacks**: Aiming to break the relationship between the data and the watermark by applying complex transformations such as scaling, rotating, cropping, deleting, or inserting additional pixels.
3. **Confusion attacks**: Creating fake data or fake watermarks to cause confusion, thereby undermining the certainty and reliability of the original watermark.

4. **Removal attacks**: Attempting to separate the embedded watermark data from the original data and watermark to access critical information.

1.2. Overview of related research and some existing limitations

1.2.1. Image saliency

Image saliency is an important concept in the field of digital image processing, relating to the identification of regions in an image that are easily recognized and noticed by humans. Saliency models are developed to replicate this human ability, serving various applications such as object recognition, image information retrieval, and especially in digital watermarking techniques to embed information into less noticeable regions, helping to protect the integrity and security of the information.

1.2.2. Reversible watermarking

Reversible watermarking is a technique that allows information to be embedded into a digital image such that after the information is extracted, the original image can be fully restored without any alterations. This technique is commonly used in applications that require the preservation of data integrity, and it is particularly important in fields such as medicine and law, where the quality and reliability of images are crucial factors.

CHAPTER 2. ANALYSIS OF THE IMPACT OF IMAGE SALIENCY IN DIGITAL WATERMARKING

2.1. Introduction

In Chapter 2, the dissertation focuses on the use of image saliency models to enhance the security of digital watermarking. The main proposed method is to embed watermark information into non-salient regions of the image. This approach increases the difficulty of detection and enhances the security of the embedded information.

2.2. Watermarking based on non-salient features of digital images

2.2.1. Method based on non-salient region learning

This section of the dissertation introduces a new digital watermarking method, which relies on saliency detection and the selection of specific subregions within a color image to embed a message. The process involves evaluating the saliency map of the image and identifying the appropriate sub-region to embed the message without affecting the quality of the original image. The information and parameters related to the embedding process are treated as a secret key, exchanged through a secure channel between the sender and the receiver. The watermarked image is then sent through a public channel. The receiver uses a similar saliency detection model to analyze and extract the message m from the image. The goal is to accurately recover the message without losing the original image information.

2.2.1.1. Salient features

This section introduces a digital watermarking method based on image saliency, using non-salient sub-regions to hide messages without easy detection.

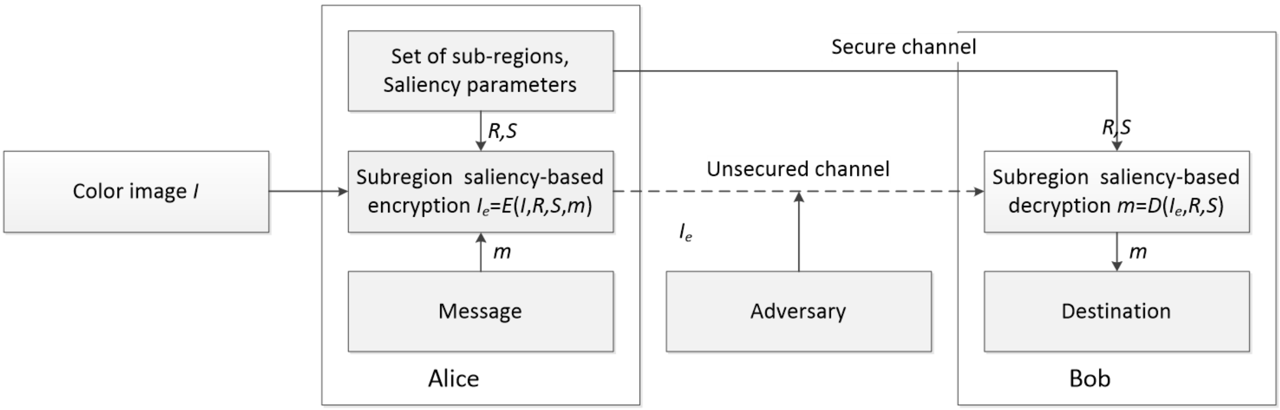

Set of sub-regions, Saliency parameters
R,S
Color image I
Subregion saliency-based encryption I_e=E(I,R,S,m)
m
Message
Alice
Secure channel
Unsecured channel
I_e
Adversary
R,S
Subregion saliency-based decryption m=D(I_e,R,S)
m
Destination
Bob

Figure 2.2: *The watermarking method for image I during communication between the sender (Alice) and the receiver (Bob) using salient features with a secure channel to exchange private keys R, S*

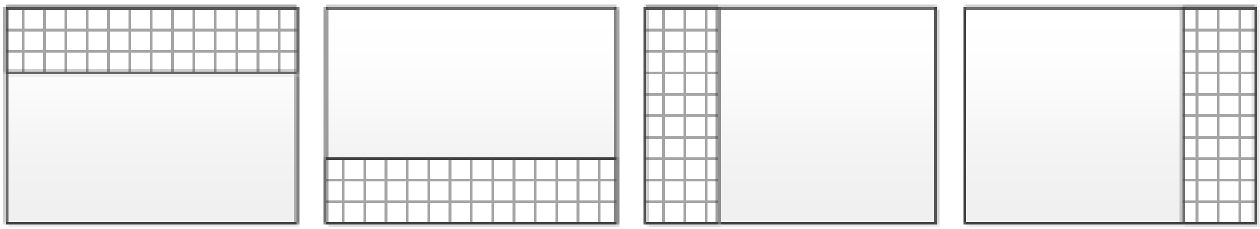
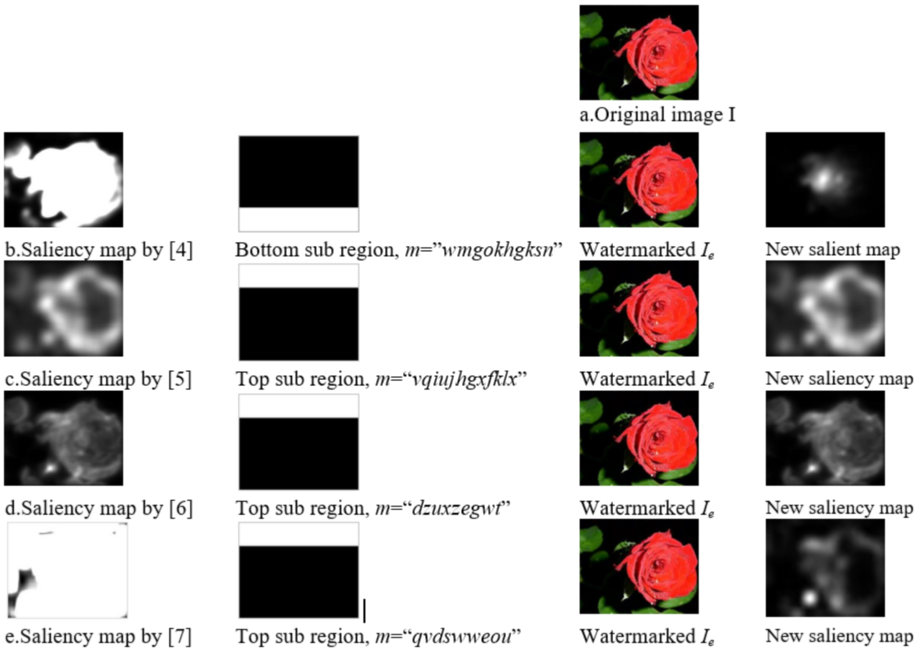


Figure 2.4: *Sub-region transformation positions within the image, covering $\frac{1}{4}$ of the image area*

By comparing the saliency of pixels with a certain threshold, a saliency map is created to identify the appropriate sub-region for embedding the message. The message is encoded into the image at the selected region, and the receiver uses a similar process to decode the message from the watermarked image. This method emphasizes the use of non-salient regions, enhancing security and accuracy in the embedding and extraction of the watermark message.

2.2.1.2. Digital watermark authentication

This section of the dissertation focuses on digital watermark authentication, using the Bayesian method [5] to evaluate the selection of sub-regions based on salient features. The process involves comparing the sub-regions r and u, with the goal being $r = u$ to ensure that the embedded message can be correctly detected and decoded. Equations (2.12) and (2.13) are used to describe the relationships between the variables. The dissertation also discusses the use of support vector machines (SVM) to estimate probabilities and optimize the saliency model through the likelihood function. Finally, the accuracy of deter-



a.Original image I

b.Saliency map by [4] Bottom sub region, *m*=”*wmgokhgksn*” Watermarked I_e New salient map

c.Saliency map by [5] Top sub region, *m*=“*vqiujhgxfklx*” Watermarked I_e New saliency map

d.Saliency map by [6] Top sub region, *m*=“*dzuxzegwt*” Watermarked I_e New saliency map

e.Saliency map by [7] Top sub region, *m*=“*qvdswweou*” Watermarked I_e New saliency map

Figure 2.6: *Example of watermark embedding using different saliency models*

mining the appropriate sub-region for message decoding is examined, showing the relationship between the saliency features s and e after watermark embedding.

$$p(r, e, u, s) = p(r|e)p(e|u)p(u|s)p(s) \tag{2.1}$$

$$p(r = u|s) \quad \sum_{r\in\{0,1,2,3\},e\in[0,1],u\in\{0,1,2,3\}} \quad p(r = u|e, u, s) \tag{2.2}$$

2.2.2. Experimental results

The dissertation explores the use of non-salient features in images to improve the effectiveness of digital watermarking. By employing models such as saliency using region covariance by [23], sparse saliency by [29], rare saliency by [67], and spectral residual saliency by [30], the SVM training process was carried out to determine the watermark embedding regions. The difference between the original image and the watermarked image was evaluated using metrics such as precision, recall, F-measure [11], MSE [63], SAD [100], SSIM, and PSNR [72]. The results demonstrated the efficiency and stability of digital watermarking, with the Highlighting and Rare models achieving the best scores.

Table 2.1: *Imperceptibility of watermarking based on non-salient features (Bold scores are the best, italicized scores are the second best)*

Saliency model	Precision	Recall	F-measure	rMSE
Covariance [70]	0.8895	0.9947	0.9391	0.9638
Highlighting [71]	**0.9266**	*0.9959*	**0.9573**	*0.9652*
Spectral [72]	0.9154	0.9944	0.9505	**0.9655**
Rare [73]	*0.9189*	**0.9965**	*0.9510*	0.9651

2.3. Watermarking based on image saliency features

This dissertation explores the use of image saliency features for embedding watermarks, an effective copyright protection technique that preserves the original information. The method selects non-salient sub-regions of the image to hide the message, minimizing the likelihood of detection. By evaluating the saliency map and identifying the appropriate sub-regions, the message is securely encoded. The selected areas are based on saliency levels relative to a fixed threshold, and the embedding process requires the exchange of secret keys between the sender and the receiver. This work also applies machine learning to optimize the selection of non-salient regions, enhancing the security and effectiveness of the watermarking. Experimental results show that this method achieves high robustness and good recoverability, paving the way for new applications of digital watermarking in copyright protection and anti-counterfeiting.

2.3.1. Saliency-based anti-counterfeiting method

This dissertation introduces a new image watermarking method, Saliency Guided Watermarking (SGW), which emphasizes the use of saliency features for embedding information to counteract forgery. This method employs mathematical techniques to determine the watermark embedding regions in the image, using saliency to generate a secret key that is then used in the encoding and decoding process. This involves selecting non-salient sub-regions of the image for watermark embedding, with the goal of keeping the watermark undetectable.

The encoding and decoding processes are illustrated through mathematical formulas, allowing for the accurate embedding and extraction of the watermark information. Specifically, the dissertation explores the use of saliency features from various models to optimize the embedding and decoding processes. Saliency measurements are used to identify the most suitable sub-region for watermark embedding, with the assistance of support vector machines (SVM) in identifying regions with minimal saliency change after watermark embedding.

The original and encoded images are analyzed to ensure that the watermark information can be accurately decoded, even if the image is attacked or altered. The ultimate goal is to achieve a robust watermarking solution that effectively counters forgery, while ensuring high security and the ability to recover the original information.

2.3.2. Experimental results

This section of the dissertation introduces and tests a new method for image watermarking based on saliency features, aimed at anti-counterfeiting. The method, applied to the MSRA10K dataset, focuses on using non-salient regions of the image to embed information. Experiments compare the performance of four different saliency models and utilize support vector machines (SVM) to generate kernels, while also assessing the stability of the watermark against various types of attacks such as rotation, noise, histogram equalization, median filtering, and cropping.

The experimental results demonstrate that this watermarking method achieves high imperceptibility and maintains stability after attacks, thanks to the careful selection of sub-regions based on saliency features. The saliency models and the message embedding process are described in detail through mathematical formulas, providing a multi-sub-region approach to optimize the embedding process. The kernels formed through SVM training help identify the most suitable sub-region for watermark embedding without altering the salient characteristics of the original image.

The dissertation also addresses the computational complexity of the method, indicating that it has linear complexity with respect to the size of the image and the selected sub-regions. This demonstrates the method's practical applicability for real-world watermark embedding and extraction tasks, while maintaining high security and recoverability after attacks.

2.4. Conclusion

This dissertation develops a new digital watermarking method focused on identifying and utilizing non-salient areas in images for information embedding, thereby enhancing the imperceptibility of the watermark. The integration of machine learning with SVM allows for precise selection of non-salient sub-regions for the encoding and decoding process, while the robustness of the learning method ensures effective handling of changes in the saliency map caused by watermark embedding. The study tested this method with four different saliency models, with sparse and rare models demonstrating robustness in message embedding.

The saliency-based watermarking method has proven to be imperceptible and stable through experiments, with low computational complexity and broad applicability in areas such as authentication and anti-counterfeiting. This approach opens up new research directions in designing specific sub-region structures for each watermarking case, while providing a comprehensive and effective solution for information protection.

CHAPTER 3. DEVELOPMENT OF WATERMARKING TECHNIQUES ENSURING THE INTEGRITY OF THE ORIGINAL IMAGE

3.1. Introduction

This document analyzes Reversible Data Hiding (RDH) techniques, which are used to embed secret information into multimedia content without distorting either the original content or the secret information upon extraction. RDH has important applications in fields such as medical imaging, military, and forensic analysis [12, 25].

RDH algorithms for JPEG images are proposed to protect image integrity, image authentication, and image privacy, but they face challenges related to limited hidden information capacity, reduced image quality, and increased image size after embedding.

The document also analyzes the advantages and disadvantages of three popular data hiding algorithms: the distributed coding algorithm [33], RDH algorithms [46, 104], and the DCT transformation algorithm [103] for JPEG images, providing insights into the capability of each algorithm to protect information in digital content. This reflects the trade-offs between the benefits and limitations of each method in data hiding.

3.2. Method using structuring elements

3.2.1. Structuring elements

The dissertation introduces a new approach to embedding information into images using a structuring element h, allowing information to be embedded without degrading the quality of the original image. The information is encoded into the image by adjusting the gray values of pixels based on the watermark. The pixels selected for embedding information are based on the 2D binary matrix of the structuring element h, with the aim of making the changes in the image's gray values difficult to detect.

The watermark embedding and extraction process uses gray values c_1, c_2, and c_3 to adjust the gray values of the pixels, enabling the original image and the embedded information to be restored without leaving any traces. This ensures the imperceptibility and high security of the hidden information while maintaining the image quality.

With the goal of minimizing changes to the image after watermark embedding, the dissertation proposes a method that can effectively hide information without affecting the visual perception of the image. This method opens up potential applications in various fields where information security in images is required, along with the need to fully recover the information and the original image.

3.2.2. Algorithm

This dissertation develops a new digital watermarking method using structuring elements to reversibly embed and extract information from the original image. The structuring elements are designed through the createElements function, based on the analysis of the grayscale histogram of the original image to identify optimal positions for information embedding. This approach focuses on selecting gray values c_1, c_2, and c_3 based on their low distribution in the grayscale histogram, which optimizes the imperceptibility of the watermark.

During the embedding process, the structuring element h and the code values c_1=8, c_2=3, and c_3=5 are used to modify the gray values of the corresponding pixels in the original image, creating the watermarked image v. This process ensures that the embedded information does not significantly affect the quality of the original image, maintaining the subtlety required for information hiding.

The extraction and restoration process of the original image from the watermarked image uses the same structuring element h and code values to determine the hidden space D'_m, from which the watermark and the original image can be recovered without any loss of information. This approach enables the storage of secret information in the image without degrading the image quality, while also ensuring the security of the embedded information through reversibility.

In summary, the dissertation proposes an effective digital watermarking solution that leverages structuring elements to embed and extract information imperceptibly and reversibly, while maintaining the original image quality and ensuring the security of the embedded information.

3.2.3. Performance evaluation metrics

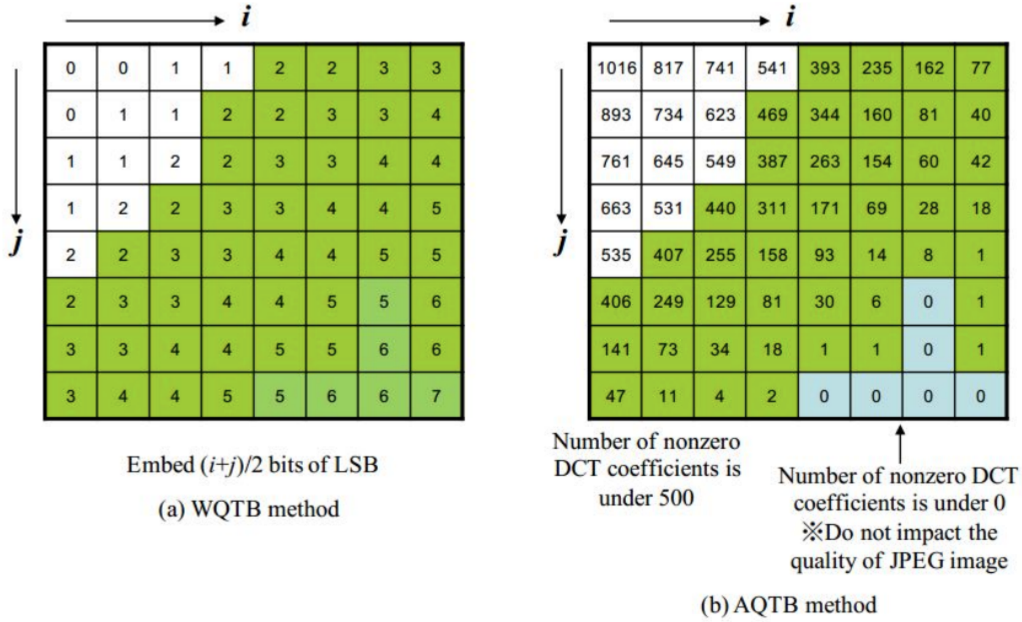
The dissertation evaluates the effectiveness of the digital watermarking method by using PSNR and MSE to assess the imperceptibility and stability of the watermark. PSNR provides the degree of difference between the original and watermarked images, while MSE calculates the mean squared error between them. These metrics help verify the ability to hide information without affecting the original image quality and ensure reversibility, allowing the original image to be restored after watermark extraction.

3.2.4. Experimental results

The dissertation investigates digital watermarking, focusing on embedding information into images without significantly altering the quality of the original image. By using structuring elements and gray values for embedding and extracting information, the dissertation proposes a new method that ensures high imperceptibility and reversibility of the watermark. A key feature of this method is its ability to fully recover the original image and the hidden information after extraction, with high computational complexity ensuring information security. Experiments demonstrate that this method is effective across various types of images, particularly the Lena image, yielding results that allow the embedding of large amounts of information while maintaining image quality. This opens up broad applications in data security and integrity verification for digital content.

3.3. Method using the DCT domain

The dissertation proposes a new approach to enhancing Reversible Data Hiding (RDH) methods in JPEG images by leveraging the characteristics of the quantization tables Q_y, Q_{cb}, Q_{cr}. This method examines how quantization tables affect DCT coefficients in JPEG images, especially for the luminance coefficients. The objective is to embed secret information into quantization coefficients that



0	0	1	1	2	2	3	3
0	1	1	2	2	3	3	4
1	1	2	2	3	3	4	4
1	2	2	3	3	4	4	5
2	2	3	3	4	4	5	5
2	3	3	4	4	5	5	6
3	3	4	4	5	5	6	6
3	4	4	5	5	6	6	7

Embed (*i*+*j*)/2 bits of LSB

(a) WQTB method

1016	817	741	541	393	235	162	77
893	734	623	469	344	160	81	40
761	645	549	387	263	154	60	42
663	531	440	311	171	69	28	18
535	407	255	158	93	14	8	1
406	249	129	81	30	6	0	1
141	73	34	18	1	1	0	1
47	11	4	2	0	0	0	0

Number of nonzero DCT coefficients is under 500

Number of nonzero DCT coefficients is under 0 ※Do not impact the quality of JPEG image

(b) AQTB method

Fig 3.9: *Number of nonzero DCT coefficients of Girl image*

have minimal impact on image quality, thereby increasing storage capacity while maintaining high image quality.

Through the analysis of the "Girl" image, the dissertation identifies that quantization coefficients, which do not significantly affect non-zero DCT coefficients, can be used as targets for embedding secret information. The results show that embedding information into these coefficients can increase the storage capacity of secret information without significantly degrading image quality.

In summary, the dissertation proposes a new RDH method in JPEG images by exploiting information from quantization tables, aiming to improve the storage capacity for secret information while maintaining the original image quality.

3.3.1. Embedding method using weights for quantization tables

In the proposed RDH method, the embedding domain focuses on the DCT coefficients from the low and mid-frequency domains, as shown in Figure 4.2(a). This method employs Weights for Quantization Table (WQTB) to target these frequency domains for conventional embedding according to Tian's method [], while also extending the quantization table's domain to increase storage capacity.

Since the DCT coefficients from the high-frequency domain of JPEG images are nearly zero, the proposed method embeds $(i+j)/2$ bits into the corresponding quantization coefficients. This is expected not to significantly degrade the quality of the JPEG image, thereby improving both the storage capacity and the quality of the image after embedding.

3.3.2. Embedding method using the frequency of non-zero DCT coefficients

To protect the quality of JPEG images when embedding secret information, the proposed method focuses on identifying and utilizing factors that do not affect image quality. This approach is illustrated in Figure 4.2(b), where the number of zero DCT coefficients from each position (i, j) of the quantization tables (All zero DCT coefficients from each position of quantization tables - AQTB) is calculated, denoted as $N_z(i, j)$. Based on the value of $N_z(i, j)$, the information embedding process is carried out as follows:

- If $N_z(i, j) = 0$, replace $Q_t(i, j)$ with 8 bits of secret information from W.
- If $N_z(i, j) < T_q$, embed the information bit b into the LSB of $Q_t(i, j)$.
- If $N_z(i, j) \leq T_q$, do not embed anything.

The details of this embedding method can be found in the paper [7]. The improved method also incorporates techniques from Sections 4.2.1 and 4.2.2, making this approach distinct and unique. The proposed method ensures that both the storage capacity and the quality of the JPEG image after embedding can be effectively enhanced.

3.3.3. Experimental results

The new RDH method was evaluated by embedding information into eight JPEG images (QF=75) such as "airplane", "barbara", "boat", "fruits", "goldhill", "lena", "peppers", and "zelda", using the quantization tables (AQTB) and weighted tables (WQTB). The threshold T_q was set to 500. The results (Table 4.2) show that this method improves the capacity for embedding secret information without degrading image quality compared to the method [81] and other methods.

Table 3.5: *Comparison of embedding capacity (bits)*

JPEG Image (QF = 75)	[81]	AQTB	WQTB
airplane	5969	6483	6385
barbara	5654	6266	6070
boat	5684	6296	6100
fruits	6384	6797	6800
goldhill	5744	6258	6160
lena	6424	7026	6840
peppers	5625	6194	6041
zelda	5918	6619	6334

CONCLUSION AND FUTURE RESEARCH DIRECTIONS

1. Conclusion

This dissertation has made the following key contributions to the field of digital watermarking:

Development of watermarking techniques based on image saliency features:

- Enhanced confidentiality: The saliency-based watermarking method leverages visual features to embed information into less noticeable regions of the image, making the watermark difficult to detect by the naked eye without degrading the visual quality of the image.

- Resistance to attacks: This method improves the ability to resist common attacks such as cropping, rotation, and compression, ensuring the robustness of the watermark information under various processing conditions.

Development of reversible watermarking techniques ensuring the integrity of the original image:

- Recovery of the original image: The reversible watermarking technique allows information to be embedded into the image such that, after extraction, the original image can be fully restored without any degradation in the original image quality.

- High embedding performance: New algorithms allow a large amount of data to be embedded without significantly reducing the visual quality of the image, expanding its applicability in fields requiring high security, such as legal documents and medical imaging.

Practical applications and scalability:

- Diverse applications: The proposed watermarking methods can be applied in various fields requiring high security, such as copyright protection for legal documents, medical imaging, and other digital products.

- Integration of advanced technologies: Exploring the potential integration of watermarking solutions with advanced image recognition and analysis technologies to enhance the effectiveness of intellectual property protection in

Bảng 3.1: *Comparison of techniques in Chapters 2 and 3*

Criteria	**Saliency-based watermarking**	**Reversible watermarking**
Confidentiality	High	Medium
Resistance to attacks	High	High
Recovery of the original image	None	Full
Embedding performance	Medium	High
Practical applications	High visual quality digital images	Digital images requiring full preservation of the original image
Computational complexity	Medium	High

complex digital environments.

From Table 3.1, the dissertation identifies the following suitable applications for each technique:

- Saliency-based watermarking techniques are suitable for cases where intellectual property protection is required without compromising the visual quality of the image. This method is ideal for applications such as artistic images, advertisements, and other digital content that requires high visual accuracy.

- Reversible watermarking techniques are appropriate for cases where the complete preservation of the original image is crucial, such as in the fields of medicine, law, and other important documents. This technique ensures that after the information is extracted, the original image can be fully restored without any loss of information.

2. Future Research Directions

The completion of this dissertation opens up numerous opportunities for the development and enhancement of digital watermarking methods, with the aim of improving security, flexibility, and application effectiveness in real-world scenarios. Some potential research directions include:

1. Algorithm optimization: Improving and optimizing the current saliency-based and reversible watermarking algorithms to reduce processing time and increase embedding capacity without compromising image quality. Specifically, applying deep learning and machine learning technologies to identify optimal regions for watermark embedding could yield significant efficiency gains.

2. Expanding applications: Investigating the application of digital watermarking in new domains such as digital video, audio, and other multimedia documents. This includes developing specialized watermarking methods for different types of data, each with distinct security and quality requirements.

3. Enhancing security: Developing new techniques to enhance the security of digital watermarking, including resistance to tampering and forgery attacks. Integrating advanced encryption methods into the watermarking process could be an important area for exploration.

4. Advanced saliency analysis: Continuing to research and develop advanced saliency models, leveraging the power of AI and deep learning for more accurate prediction and analysis of viewer attention. This will help optimize the placement and size of the watermark while maintaining the aesthetics of the original image.

5. Adapting to format changes: Exploring the capability of digital watermarking to adapt and preserve information through format changes such as image compression or resizing is another crucial area. Developing watermarking methods that can maintain integrity through image processing procedures is a worthwhile goal.

These research directions not only pave the way for advancements in digital watermarking techniques but also support the development of security applications in the digital age, meeting the growing demand for information protection and intellectual property rights.

LIST OF THE PUBLICATIONS RELATED TO THE DISSERTATION

1. Pham Quang Huy and Ta Minh Thanh, “Cross-frequency domain for jpeg inversible watermarking using multiple quantization tables,” Journal of Science and Technique-Section on Information and Communication Technology, vol. 12, no. 01, 2023, doi: $10.56651/lqdtu.jst.v12.n1.660.ict$.

2. Pham Quang Huy and Dao Nam Anh, “A new approach to Anti-Forgery using Saliency Guided Image Watermarking”, Journal of Computer Science and Cybernetics, 2024 (accepted).

3. Pham Quang Huy, Ta Minh Thanh, Le Danh Tai, Pham Van Toan, “Cross-domain using composing of selected dct coefficients strategy with quantization tables for reversible data hiding in jpeg image,” in Research in Intelligent and Computing in Engineering: Select Proceedings of RICE 2020. Springer, 2021, pp. 681–693, doi: $10.1007/978 - 981 - 15 - 7527 - 3\_64$.

4. Dao Nam Anh, Pham Quang Huy, Doan Thi Huong Giang, “Steerable features for resilient image watermark”, in 2019 International Conference on Multimedia Analysis and Pattern Recognition (MAPR). IEEE, 2019, pp. 1–6, doi: $10.1109/MAPR.2019.8743544$.

5. Dao Nam Anh, Pham Quang Huy, Luong Chi Mai, “Watermark by learning non-saliency”, in Frontiers in Intelligent Computing: Theory and Applications: Proceedings of the 7th International Conference on FICTA (2018), Volume 1. Springer, 2020, pp. 61–72, doi: $10.1007/978 - 981 - 32 - 9186 - 7\_7$.

6. Dao Nam Anh, Pham Quang Huy, “Structuring Element for Secure Reversible Watermarking”, in: 2020 International Conference on Multimedia Analysis and Pattern Recognition (MAPR), IEEE, 2020, pp. 1–6, doi: 10.1109/MAPR49794.2020.9237780.