BLIND DIGITAL IMAGE WATERMARKING USING SVD AND QIM

A Thesis Submitted
In Partial Fulfillment of the Requirements for the Degree of

MASTER OF TECHNOLOGY
in
Signal Processing and Digital Design

by

Rohit Yadav

24/SPDD/20

Under the Supervision of

Ms. Lavi Tanwar

Asst. Professor, ECE Dept., DTU

Electronics and Communication Engineering

DELHI TECHNOLOGICAL UNIVERSITY
(Formerly Delhi College of Engineering)
Shahbad Daulatpur, Main Bawana Road, Delhi-110042, India

May, 2026

DELHI TECHNOLOGICAL UNIVERSITY

(Formerly Delhi College of Engineering)

Shahbad Daulatpur, Main Bawana Road, Delhi-42

ACKNOWLEDGEMENT

I wish to express my sincerest gratitude to Ms. Lavi Tanwar for her continuous guidance and mentorship that she provided me during the project. She showed me the path to achieve my targets by explaining all the tasks to be done and explained to me the importance of this project as well as its industrial relevance. She was always ready to help me and clear my doubts regarding any hurdles in this project. Without her constant support and motivation, this project would not have been successful.

Rohit Yadav
24/SPDD/20

CANDIDATE'S DECLARATION

I hereby certify that the work being presented in the thesis entitled **"Blind Digital Image Watermarking Using SVD and QIM "** in partial fulfillment of the requirements for the award of the degree of Master of Technology submitted in the Department of Electronics and Communication Engineering, Delhi Technological University, is an authentic record of my own work carried out during the period under the supervision of Ms. Lavi Tanwar.

The matter presented in the thesis has not been submitted by me for the award of any other degree of this or any other Institute.

Rohit Yadav

24/SPDD/20

DELHI TECHNOLOGICAL UNIVERSITY

(Formerly Delhi College of Engineering)

Shahbad Daulatpur, Main Bawana Road, Delhi-42

CERTIFICATE BY THE SUPERVISOR

Certified that **Rohit Yadav** (24/SPDD/20) has carried out their research work presented in this thesis entitled **"Blind Digital Image Watermarking Using SVD and QIM"** for the award of **Master of Technology** from Department of Electronics and Communication Engineering, Delhi Technological University, Delhi, under my supervision. The thesis embodies results of original work, and studies are carried out by the student himself and the contents of the thesis do not form the basis for the award of any other degree to the candidate or to anybody else from this or any other University/Institution.

Signature

Ms. Lavi Tanwar
Asst.Professor, ECE Dept., DTU

Date:

BLIND DIGITAL IMAGE WATERMARKING USING SVD AND QIM

Rohit Yadav

ABSTRACT

The proliferation of digital images over the Internet has raised concerns about copyright infringement and unauthorized reproduction of content, making robust ownership verification mechanisms more necessary than ever. In this thesis, a fully blind digital image watermarking scheme based on Singular Value Decomposition (SVD) and Quantization Index Modulation (QIM) in an energy-normalized reconstruction framework is proposed. A 512-bits binary watermark is embedded into singular values of 512×512 grayscale host image by using scalar QIM with quantization step $\Delta = 5$. The orthogonal matrices of the SVD are not altered during this process in order to keep the visual fidelity. We then perform blind extraction using the QIM minimum-distance decoder directly on the singular values of the attacked image – no reference to the original host is needed.

An energy normalization mechanism is embedded to compensate for global amplitude distortions induced by energy changing attacks like histogram equalization, which stabilizes correlation based detection. The scheme was tested on four standard USC-SIPI test images under twelve attack types including noise, filtering, JPEG compression, geometric distortion and histogram modification. The imperceptibility results were near-lossless with PSNR values in the range of 68.05 to 68.44 dB - an improvement of 20-28 dB over the most closely related state-of-the-art methods. Robustness was validated with Normalized Cross-Correlation values above 0.90 for all the 48 attack-image combinations, the overall mean value of NCC is 0.9845. Specifically in histogram equalization, energy normalization improved NCC by 0.47-0.52. The proposed scheme, in combination, uniquely combines the near-lossless imperceptibility, consistent robustness and the fully blind extraction to provide a practically deployable framework for the digital image copyright protection.

Keywords: Digital Image Watermarking, Singular Value Decomposition, Quantization Index Modulation, Blind Extraction, Energy Normalization, Robustness.

Contents

Acknowledgements **ii**

Candidate's Declaration **iii**

Certificate by the Supervisor **iv**

Abstract **v**

List of Tables **ix**

List of Figures **x**

List of Symbols, Abbreviations and Nomenclature **xi**

1 Introduction **1**
1.1 Background and Motivation 1
1.2 Digital Multimedia and Copyright Challenges 2
1.3 Digital Watermarking: Overview and Significance 3
1.4 Key Requirements: Imperceptibility, Robustness, and Capacity 4
1.4.1 Imperceptibility 4
1.4.2 Robustness 4
1.4.3 Payload Capacity 4
1.5 Problem Statement 5
1.6 Objectives of the Work 5
1.7 Scope and Limitations 6
1.8 Organization of the Thesis 7

2 Literature Survey **8**
2.1 Overview of Digital Watermarking Approaches 8
2.2 Spatial Domain Methods 9
2.2.1 LSB Substitution and Variants 9
2.2.2 Limitations of Spatial Domain Methods 9
2.3 Transform Domain Methods 9
2.3.1 DCT-Based Watermarking 9
2.3.2 DWT-Based Watermarking 10
2.4 SVD-Based Watermarking 10
2.4.1 Fundamentals of SVD in Watermarking 10

2.4.2 Additive SVD Embedding Schemes 10
2.4.3 Limitations of Additive SVD Models 11
2.5 Quantization-Based and Blind Watermarking 12
2.5.1 QIM Theory 12
2.5.2 SVD-QIM Integration 12
2.5.3 Dither Modulation and Rational QIM Variants 13
2.6 Projection-Based Methods and Mojette Transform 13
2.6.1 Radon and Mojette Transform Principles 13
2.6.2 Limitations: Non-Blind Extraction and Absence of Energy Normalization 13
2.7 Research Gaps and Motivation for Proposed Work 14

3 Proposed Methodology 15
3.1 System Architecture Overview 15
3.2 Watermark Preprocessing 15
3.2.1 Input Watermark Image 15
3.2.2 Binary Thresholding to Generate 512-bit Sequence 16
3.2.3 SVD Decomposition of Watermark Image 16
3.3 Watermark Embedding Procedure 16
3.3.1 SVD Decomposition of Host Image 16
3.3.2 1D Mojette-Compatible Processing 17
3.3.3 QIM-Based Singular Value Modulation 17
3.3.4 Watermarked Image Reconstruction 18
3.3.5 Computational Complexity of Embedding 18
3.4 Blind Watermark Extraction and Energy-Normalized Reconstruction . 18
3.4.1 SVD Decomposition of Attacked Watermarked Image 18
3.4.2 QIM Minimum-Distance Bit Demodulation 20
3.4.3 Watermark Singular Value Estimation 20
3.4.4 Energy Normalization 20
3.4.5 Watermark Reconstruction 21
3.4.6 Computational Complexity of Extraction 21
3.5 Selection of Quantization Step Δ and System Parameters 21
3.5.1 Effect of Δ on PSNR-Robustness Trade-off 21
3.5.2 Image-Independence of the Chosen Parameters 21
3.6 Complete System Algorithm 22

4 Results and Discussions 25
4.1 Experimental Setup and Dataset 25
4.1.1 Software Platform and Libraries 25
4.1.2 Hardware Configuration 25
4.1.3 Standard Test Images 25
4.1.4 Watermark Image Specification 25
4.2 Evaluation Metrics 27
4.2.1 Peak Signal-to-Noise Ratio for Imperceptibility 27
4.2.2 Normalized Cross-Correlation for Robustness 27
4.3 Attack Simulation 28

4.4 Imperceptibility Analysis 28
4.4.1 PSNR Results 28
4.4.2 Visual Quality of Watermarked Images 29
4.4.3 Structural Similarity Analysis 29
4.5 Robustness Analysis Under Attack 29
4.5.1 Complete NCC Results 29
4.5.2 Robustness Under Noise Attacks 31
4.5.3 Robustness Under Filtering Attacks 32
4.5.4 Robustness Under JPEG Compression 32
4.5.5 Robustness Under Geometric Attacks 32
4.5.6 Robustness Under Histogram Equalization 33
4.5.7 Visual Quality of Extracted Watermarks 33
4.6 Effect of Energy Normalization 33
4.6.1 Contribution to Histogram Equalization Robustness 33
4.6.2 Effect on Other Attack Types 34
4.7 Effect of Quantization Step Δ 34
4.7.1 PSNR-Robustness Trade-off Analysis 34
4.8 Comparative Analysis with Existing Methods 35
4.8.1 PSNR Comparison 35
4.8.2 NCC Comparison Under Standard Attacks 35
4.8.3 Comparison with Spatial Domain Methods 36
4.8.4 Discussion of Overall Performance 36

5 Conclusion, Future Scope and Social Impact 37
5.1 Conclusions 37
5.2 Future Scope 38
5.2.1 Extension to Color Images 38
5.2.2 Adaptive Quantization Based on Local Image Content 38
5.2.3 Key-Based Security Mechanisms 38
5.2.4 Robustness Against Deep Learning-Based Attacks 38
5.3 Social Impact 39
5.3.1 Copyright Protection and Intellectual Property Rights 39
5.3.2 Medical Image Integrity and Patient Safety 39
5.3.3 Combating Misinformation and Digital Forgery 39
5.3.4 Contribution to the Research Community 39

References 39

A Python Implementation 44

Plagiarism Report 49

List of Publications 50

Curriculum Vitae 51

List of Tables

4.1 PSNR Values for Watermarked Images 28
4.2 NCC Values Under Various Attacks 31
4.3 Effect of Energy Normalization on NCC Under Histogram Equalization 33
4.4 PSNR and NCC vs. Quantization Step Δ (Cameraman, Gaussian Noise $\sigma = 10$) 34
4.5 PSNR Comparison with Existing Methods 35
4.6 NCC Comparison with Mojette-SVD [10] 35
4.7 Comparison with Spatial Domain Methods 36

List of Figures

3.1 Block diagram of the proposed watermark embedding framework. . . 17
3.2 Block diagram of the proposed blind watermark extraction and reconstruction framework. 19

4.1 Host images 26
4.2 Watermark Image (Lena) 26
4.3 Visual comparison of host images, watermarked images, original watermark (Lena, 32×16 thumbnail), and extracted watermarks for all four USC-SIPI standard test images. No perceptible difference is visible between host and watermarked images in any row, confirming near-lossless embedding (mean PSNR $= 68.30$ dB). Extracted watermarks are visually indistinguishable from the original, confirming high-fidelity blind extraction [10, 15, 36]. 30

LIST OF SYMBOLS, ABBREVIATIONS AND NOMENCLATURE

Symbol/Abbreviation	Description
SVD	Singular Value Decomposition
QIM	Quantization Index Modulation
DWT	Discrete Wavelet Transform
DCT	Discrete Cosine Transform
NSCT	Non-Subsampled Contourlet Transform
LSB	Least Significant Bit
PSNR	Peak Signal-to-Noise Ratio
NCC	Normalized Cross-Correlation
MSE	Mean Squared Error
SSIM	Structural Similarity Index
HVS	Human Visual System
DRM	Digital Rights Management
BER	Bit Error Rate
RDM	Rational Dither Modulation
USC-SIPI	University of Southern California – Signal and Image Processing Institute
$\mathbf{A}$	General matrix
$\mathbf{U}, \mathbf{V}$	Orthogonal matrices from SVD
Σ	Diagonal matrix of singular values
σ_i	i-th singular value
Δ	QIM quantization step
α	Embedding strength (additive methods)
γ	Energy normalization constant
ε	Small regularization constant
$\mathbf{b}$	Binary watermark bit sequence
$\hat{\mathbf{b}}$	Extracted binary watermark bit sequence
JPEG	Joint Photographic Experts Group
QF	Quality Factor (JPEG)

CHAPTER 1
INTRODUCTION

1.1 Background and Motivation

Digital communication has grown incredibly fast over the last two decades. The internet changed everything — how we make content, how we share it, and how people consume it every day. Digital images in particular make up an enormous share of the data exchanged daily — across social media, e-commerce platforms, digital archives, cloud storage systems, and healthcare repositories. Recent surveys have reported that several billions of images are uploaded and shared online on a daily basis, and this number is still growing with the proliferation of smartphone cameras, satellite imaging systems, and AI-generated visual content [1, 2].

The ability to copy, redistribute and modify digital images without any noticeable loss of quality poses serious challenges to intellectual property rights, content authentication and ownership verification. Physical media can't be duplicated and distributed instantly like a perfect digital copy. This makes original content creators highly vulnerable to unauthorised use, forgery and plagiarism. These concerns have motivated ongoing research on robust mechanisms for embedding ownership information directly into image data, invisible to human observers but recoverable by authorized parties [1, 3, 5].

Digital watermarking is probably the most researched solution to this problem. The basic idea is simple — you hide a small piece of information inside an image in a way that doesn't change how the image looks. The tricky part is making sure that hidden data stays there even after the image gets compressed, filtered, or edited, and that you can still read it out reliably later [2, 5]. Encryption prevents access to data during transfer and makes it impossible to use without a key, while watermarking allows the free use of protected content with ownership information attached to it. This difference makes watermarking particularly well suited for copyright protection, broadcast monitoring, content authentication and forensic tracing [3, 6].

Decades of research later and it's still really hard to build a watermarking system that ticks all the boxes at once — invisible, robust, and high capacity. Early methods like LSB substitution were easy to implement and didn't visibly affect the

image. But they had a big weakness. Simple things like saving the image as a JPEG, applying a blur filter, or adding a bit of noise were enough to wipe the watermark out completely [5, 7]. Later approaches worked in the transform domain — methods using DCT, DWT, and SVD. These were much more robust against common attacks. But they came with their own problems. Some struggled with geometric distortions like rotation or cropping. Many of them also needed the original image to extract the watermark, which is a big practical limitation [6, 8, 9].

This paper is motivated by a key limitation of the majority of SVD based watermarking schemes in the literature. These schemes are based on an additive embedding model of the form:

$$\Sigma' = \Sigma + \alpha \mathbf{W} \tag{1.1}$$

Inherently, this design approach necessitates the original host image during the extraction process and hence is referred to as either non-blinding or semi-blinding. In practical copyright detection applications, the original source material may be unavailable to the verification entity, thereby rendering such designs impractical. On top of that, current SVD based techniques do not incorporate any form of correction for the energy level distortion resulting from the use of attacks such as histogram equalization and heavy compression [10, 11, 23].

1.2 Digital Multimedia and Copyright Challenges

Through digitization, a world has been created wherein the difference between an original and its copy does not even exist. High-quality duplication and immediate global distribution have become easy for everyone who has basic computing facilities and internet connectivity. Whereas, on one hand, this process has made content creation easy; on the other hand, it has undermined the existing legal protection mechanisms for intellectual property [1, 12].

Copyright violations in the digital sphere come in various ways. Reproduction and dissemination of copyrighted images occur without authorization on social media platforms. There is the threat of manipulated medical images being submitted in place of real images, which may endanger one's life. The manipulation of remote sensing images is a possibility that threatens national security and economic interests. There is also rampant misappropriation of artwork and photos in the digital world with no payment to the copyright holders [2, 3, 13].

The conventional techniques employed to protect copyright have turned out to be insufficient to deter such attacks. DRM systems were supposed to solve this but

honestly they haven't worked very well. People find ways around them regularly. Even stripping the metadata from an image file — the part that says who made it — takes about two clicks with freely available tools. There is thus a dire need to find a solution that is capable of embedding ownership meta information in an intrinsic way that will not be visible once deleted [12, 23].

In addressing this requirement, digital watermarking emerges as an effective solution. Digital watermark serves as an identifier that follows the image along, irrespective of how the image is distributed or transformed. This feature is important for multiple applications, including broadcast monitoring, forensics, verification of medical images, e-commerce, and more [1, 5, 6].

1.3 Digital Watermarking: Overview and Significance

Put simply, digital watermarking is about hiding information inside a digital signal — usually an image — in a way that nobody can see it during normal use. But with the right algorithm, an authorized person can find it and read it back out [2, 5]. In the present context, the host signal is a digital grayscale image, and the watermark is a 512-bit binary sequence derived from a 32×16 watermark image. The embedding is designed to be robust against a wide range of signal processing and geometric attacks that may be applied during storage, transmission, or malicious tampering [15, 16].

There are different ways to categorize watermarking systems. One way is by visibility — some watermarks are meant to be seen, others are completely invisible. Another important classification is about what you need to extract the watermark. Non-blind systems need the original image. Semi-blind systems need the original watermark pattern. Fully blind systems need neither — they work from the watermarked image alone [5, 6]. The system proposed in this thesis is fully blind. This is the hardest category to work in because you have to recover the watermark using only the attacked image — no original, no reference, nothing [10, 11].

Classification based on the embedding domain can be made for digital image watermarking schemes as follows. Spatial domain methods like LSB substitution work directly on pixel values. They're simple and fast to compute, but they don't hold up well under attack [7]. Transform domain methods take a different approach. Instead of touching pixel values directly, they embed the watermark in the coefficients of a mathematical transform — things like DCT coefficients, wavelet sub-bands, or singular values. These tend to be much more resilient to attacks [6, 8, 9, 16].

Watermarking is highly relevant in various industries. The entertainment

industry allows broadcasters to detect the distribution of copyright material without authorization. Medicine uses watermarks in diagnostic imagery to certify authenticity. In legal matters, watermarked imagery can be used as a proof of ownership of an intellectual property. For military and intelligence purposes, watermarks can be used to trace the source of sensitive imagery [3, 12, 13].

1.4 Key Requirements: Imperceptibility, Robustness, and Capacity

Any watermarking system must adhere to three basic and opposing principles in its design: imperceptibility, robustness, and capacity. The ability to find an appropriate trade-off between these aspects is what constitutes the primary goal in this area of study, and must be specified explicitly in any new system proposal [1,2,5].

1.4.1 Imperceptibility

Imperceptibility means the watermark shouldn't change how the image looks. Someone viewing the watermarked image should see no difference compared to the original. This can be measured objectively using metrics like PSNR and SSIM. Generally speaking, a PSNR above 40 dB is considered acceptable for watermarking applications. Values above 50 dB indicate high quality. The method developed in this thesis consistently achieves above 68 dB across all test images, which puts it firmly in the near-lossless category [15–17].

1.4.2 Robustness

Robustness is about how well the watermark survives attacks. These attacks come in many forms — adding different types of noise like Gaussian or salt-and-pepper, smoothing the image with various filters, compressing it using JPEG at different quality levels, or applying geometric operations like rotation and cropping. To measure robustness, we compare the original watermark with the one extracted after an attack using Normalized Cross-Correlation. A score of 1.0 means perfect recovery [10,21,28].

1.4.3 Payload Capacity

Payload capacity refers to how much information you can embed in an image while keeping the other two properties intact. More data means more potential distortion, so there's always a trade-off between how much you embed and how well the other requirements are met. The new technique employs a 512-bit watermark which is adequate to encode the owner's identity while achieving a reasonable trade-off between

the three properties [1, 2, 18].

1.5 Problem Statement

Reviewing the current body of literature pertaining to watermarking of digital images, several fundamental shortcomings have been identified that inhibit the use of SVD-based algorithms in real world application scenarios. They are highlighted as follows.

The first problem is with how most SVD watermarking schemes work. They add the watermark to the singular values using a linear operation. That's fine for embedding, but when you want to extract, you need the original singular values as a reference. In real copyright disputes, the verifying party usually doesn't have access to the original image. So these methods just aren't practical [9–11, 20].

The second gap is about QIM. It's a well-established technique with solid theoretical backing and good noise resistance. But combining it properly with SVD in a way that enables fully blind extraction hasn't really been explored thoroughly. A few papers touch on it but nothing comprehensive [18, 21, 22].

Third, attacks such as histogram equalization and aggressive JPEG compression can substantially alter the global energy distribution of a watermarked image, causing amplitude distortions in the extracted singular values. Most existing SVD watermarking schemes do not incorporate explicit energy normalization to compensate for these distortions, leading to degraded correlation-based detection performance [10, 23].

In the current thesis, all three constraints are overcome by designing a blind scheme for digital image watermarking using SVD decomposition along with QIM and energy-normalization based reconstruction — which allows for robust blind watermark extraction without utilizing any host image information.

1.6 Objectives of the Work

Main goals of this work are stated as follows:

- To develop a fully blind digital image watermarking approach combining the SVD and QIM techniques without the necessity to have access to the host image while extracting a watermark [1, 10].
- To embed a 512-bit watermark into the main singular values of 512×512 grayscale image using QIM technique with the constant quantization

step of $\Delta = 5$ while keeping the orthogonal matrices obtained in SVD decomposition intact to avoid distortions [15, 16].

- To introduce energy normalization technique allowing compensation of the global amplitude distortion caused by attacks like histogram equalization, JPEG compression, and filtering [10, 23].
- To value the effectiveness of the new scheme for twelve different attacks that include signal processing and geometrical attacks through performance evaluation based on PSNR and NCC metrics [1, 15].
- To compare the proposed scheme against the recently published and advanced SVD-based and hybrid watermarking schemes [9, 10, 24].

1.7 Scope and Limitations

This research focuses specifically on 512×512 grayscale images. The watermark is a 512-bit binary sequence derived from a small 32×16 thumbnail and is embedded into the singular value domain of the host image. This model is developed using Python language and evaluated using common scientific computing libraries including NumPy, OpenCV, and Pillow, working on four standard test images, i.e., Cameraman, House, Jetplane, and Lake [25].

There are a number of limitations for the model. First, the current model works exclusively with gray scale images, and its extension to color images may require transformation into color space — either to YCbCr or HSV — followed by watermarking of one or more color components [26]. Second, the constant value of the quantization step $\Delta = 5$ is an empirical choice; the application of adaptive quantization can yield better imperceptibility-robustness performance [27, 28].

Third, the present system does not incorporate key-based security mechanisms to prevent unauthorized watermark detection or removal. Integrating a secret key into the embedding and extraction process would significantly enhance security against adversarial attacks [29]. Fourth, robustness evaluation is limited to the twelve attacks defined in the experimental setup. More sophisticated adversarial attacks — such as those in the StirMark benchmark suite or deep learning-based attack methods — are beyond the current scope [19, 30].

1.8 Organization of the Thesis

The remainder of this thesis is organized as follows.

Chapter 2 presents a comprehensive literature survey covering spatial domain methods, transform domain methods, SVD-based schemes, quantization-based and blind techniques, and projection-based approaches including the Mojette transform. Research gaps motivating the proposed work are identified at the conclusion of this chapter.

Chapter 3 covers the theoretical background for the proposed methodology. In particular, mathematical basics of SVD decomposition and stability of singular values are described, as well as information theory basis for QIM, compatible 1D projection framework and energy normalization concepts. The two metrics used to evaluate the performance of the proposed algorithm, namely PSNR and NCC, are formally defined.

Chapter 4 describes the proposed methodology in detail. This chapter contains description of watermark pre-processing, SVD embedding method using QIM principles, blind extraction and energy-normalized watermark reconstruction techniques.

Chapter 5 details the experimental environment that includes the software and hardware, the set of benchmark images to be tested, the watermark image parameters, and the twelve attacks used to evaluate the robustness of the proposed scheme.

Chapter 6 reports all experimental findings and thoroughly examines them. The discussion covers how undetectable the watermark is once embedded, how the system performs when subjected to each of the twelve attack types, the specific contribution made by the energy normalization component, and a direct comparison with the strongest competing methods from recent literature.

Chapter 7 brings the thesis to a close. A consolidated account of the contributions made is provided, the principal conclusions emerging from the entire study are drawn together, the constraints and limitations inherent to the current work are candidly identified, and several meaningful directions for taking this research further are outlined for future investigation.

CHAPTER 2
LITERATURE SURVEY

2.1 Overview of Digital Watermarking Approaches

There have been many developments in the area of digital watermarking since its inception more than three decades ago due to the necessity of protecting intellectual property in today's highly inter-connected digital environment. Over the years, various algorithms for digital watermarking have been suggested by scholars with diverse characteristics depending on the embedding domain, extraction approach, intended application, and robustness level. Looking at the literature as a whole, most watermarking methods fall into one of three buckets — spatial domain methods, single transform domain methods, and hybrid approaches that combine multiple transforms [1–3].

Spatial domain methods are the simplest — they modify pixel values directly and are easy to implement. The downside is that they're fragile. Even mild operations like a low-pass filter or basic JPEG compression can destroy the watermark [5, 7]. Transform domain methods embed the watermark in the coefficients produced by transforming the image mathematically. DCT, DWT, and SVD are the most commonly used transforms here. Because these domains exploit how image energy is distributed and how the human eye perceives changes, these methods tend to be much more robust while still keeping the watermark invisible [6, 8, 9].

Hybrid methods push this further by combining two or more transforms together. For example, DWT-SVD schemes use wavelets for their multi-resolution properties and SVD for its structural stability. The idea is that combining them gives you the best of both worlds. NSCT-DWT-SVD architectures further incorporate the non-subsampled contourlet transform to improve robustness against geometric distortions [19, 24]. The trade-off, though, is a significant increase in computational complexity that can make such systems impractical for real-time use [19].

Another important way to classify these methods is by what they need at extraction time. Non-blind systems need the original image. Semi-blind systems need the original watermark. Fully blind systems need nothing extra. Most transform domain methods, including the majority of SVD-based schemes, fall into the non-

blind or semi-blind categories. That's a serious practical problem because in most real copyright scenarios, the original image just isn't available to whoever is doing the verification [5, 10, 11]. This observation is the primary motivation for the blind SVD-QIM framework developed in the present thesis.

2.2 Spatial Domain Methods

2.2.1 LSB Substitution and Variants

LSB substitution is probably the oldest and most studied spatial domain technique. The idea is straightforward — replace the least significant bit of selected pixels with watermark bits. Since changing the LSB shifts a pixel value by at most one gray level, the image looks virtually identical to the original [5, 7]. Ease of implementation and the inherent simplicity of the technique make it an appealing choice for implementations where computing capabilities are limited, and the threat model assumes no attacks from competent adversaries.

2.2.2 Limitations of Spatial Domain Methods

The core limitation of spatial domain methods can be understood in terms of the relationship between embedding capacity and the robustness-imperceptibility trade-off. Because pixel values are directly modified, any operation that alters pixel intensities — whether through compression, filtering, geometric transformation, or noise — can erase or corrupt the embedded watermark [1, 5]. On top of that, these methods have no real understanding of how the human eye actually perceives images, which makes it genuinely hard to push the watermark strength to its limit without the distortion becoming noticeable to a viewer [2].

2.3 Transform Domain Methods

2.3.1 DCT-Based Watermarking

One of the most useful properties of the DCT is energy compaction — most of an image's important information gets packed into a relatively small number of low-frequency coefficients. DCT-based watermarking schemes use this cleverly by embedding the watermark in the mid-frequency range. These coefficients carry enough perceptual importance to survive common processing, but aren't as vulnerable as the high-frequency ones [8]. Since JPEG itself is based on the block DCT, watermarks embedded in mid-frequency DCT coefficients tend to survive JPEG compression

reasonably well. This gives DCT-based methods a natural advantage over spatial domain techniques specifically when it comes to compression attacks.

2.3.2 DWT-Based Watermarking

The Discrete Wavelet Transform breaks an image down into multiple layers, each capturing different frequency ranges and spatial directions. DWT-based watermarking works by hiding the watermark inside the wavelet coefficients of selected sub-bands, with most approaches targeting either the low-frequency approximation layer or the mid-frequency detail layers where changes are harder to notice [9]. This property of multi-resolution enables perceptual adaptation of energy placement in the watermarking technique.

2.4 SVD-Based Watermarking

2.4.1 Fundamentals of SVD in Watermarking

Singular Value Decomposition is a matrix factorization technique that decomposes any real matrix $\mathbf{A}$ of size $M \times N$ into the product:

$$\mathbf{A} = \mathbf{U}\Sigma\mathbf{V}^T \tag{2.1}$$

where $\mathbf{U}$ and $\mathbf{V}$ are orthogonal matrices containing the left and right singular vectors respectively, and Σ is a diagonal matrix whose entries are the singular values ordered in descending magnitude [8, 16]. The largest one represents the most dominant structural information in the image, while smaller ones correspond to finer details.

The important feature of the singular values, which makes them suitable for watermarking, is their stability during many different image transformations. Small changes in the pixel intensity, due to compression, filtering, noise addition, or even some geometric transformation, will result in small changes in the singular values themselves [8, 16]. Moreover, since singular values describe the global property of the whole image matrix, not the local properties of certain pixels or coefficients, they are more robust to any localized transformations like cropping [3, 8].

2.4.2 Additive SVD Embedding Schemes

Chang, Tsai, and Lin [8] introduced the first SVD watermarking method. Their key insight was that changing only the singular values while leaving the orthogonal matrices $\mathbf{U}$ and $\mathbf{V}$ produced watermarked images with decent robustness. The standard

additive SVD embedding model is expressed as:

$$\Sigma' = \Sigma + \alpha \mathbf{W} \tag{2.2}$$

where Σ is the diagonal matrix of original singular values, $\mathbf{W}$ is the watermark matrix, and α is the embedding strength parameter [8, 20]. The critical disadvantage is that extraction requires the original singular values or the original host image — making the system non-blind [9–11].

Verma et al. [20] proposed a scheme combining SVD with the homomorphic transform, demonstrating improved robustness against multiplicative noise attacks. Zhang et al. [15] developed a spatial domain SVD watermarking scheme achieving PSNR values in the range of 40–50 dB with NCC values exceeding 0.90 against most standard attacks, but their scheme remained non-blind. Wang and Zhao [17] proposed an adaptive method combining SVD with DWT and Wang-Landau sampling, achieving improved visual quality while still requiring the original host for extraction.

Zheng et al. [24] proposed a robust scheme combining the Non-Subsampled Contourlet Transform (NSCT), DWT, and SVD. Reported PSNR values exceeded 45 dB, and NCC values remained above 0.90 for most attack types. Zeng et al. [19] combined NSCT, DWT, SVD, and a Human Visual System model to develop a blind watermarking algorithm with high robustness, though reported PSNR values of approximately 45 dB are substantially lower than those achieved by the proposed scheme.

2.4.3 Limitations of Additive SVD Models

However, apart from the aforementioned non-blind extraction condition, there are various shortcomings associated with the additive embedding method. First, linear modification of the singular values does not theoretically ensure robustness to a specific attack; robustness depends on an empirical determination and the selection of the parameter α [10, 21]. Secondly, the ideal value of α varies based on the image under consideration since the same value which may be effective for one image may be too strong and cause excessive distortion in another, or insufficient in resisting a third image [6, 17].

Thirdly and quite importantly, additive model can be subjected to attacks which modify the energy distribution of the image globally. In such instances, modifications to the singular values become difficult to compensate for due to the lack of any reference values for energy distribution which only exist for the original image [10, 23].

2.5 Quantization-Based and Blind Watermarking

2.5.1 QIM Theory

QIM was introduced by Chen and Wornell [11] as a theoretically grounded alternative to spread-spectrum methods. The core idea is different from additive methods — instead of adding something to the host signal, QIM quantizes it to one of two lattices depending on which bit is being embedded. The payoff is significant — for the same amount of distortion, QIM can embed more information, and it comes with provable robustness against Gaussian noise, which additive methods can't claim [11,21].

In scalar QIM — the variant adopted in the present thesis — the host signal sample x is quantized to the nearest reconstruction point of either the even quantization lattice:

$$\Lambda_0 = \{\ldots, 0, \Delta, 2\Delta, \ldots\} \tag{2.3}$$

or the odd quantization lattice:

$$\Lambda_1 = \left\{\ldots, \frac{\Delta}{2}, \frac{3\Delta}{2}, \ldots\right\} \tag{2.4}$$

depending on whether the watermark bit b is 0 or 1 respectively [11]. Blind extraction in QIM is achieved by determining, for each extracted sample, which quantization lattice it is closest to — requiring only the extracted signal and the quantization step Δ — making QIM inherently suitable for fully blind watermarking [11, 21].

2.5.2 SVD-QIM Integration

Despite the theoretical advantages of QIM and the structural advantages of SVD, relatively few studies have investigated their systematic integration in a fully blind watermarking framework. Sun et al. [22] proposed a semi-fragile watermarking technique combining SVD decomposition with scalar quantization for image authentication, but it was designed for fragile rather than robust watermarking and did not address the blind extraction requirement.

A blind watermarking technique was introduced by Liu et al. utilizing quantization of singular values using the QSVD transformation method, showing that quantized singular values enable robust extraction in a blind manner and offer more robustness than additive techniques. Ali et al. [17] have also found that incorporating normalization schemes in the process of embedding SVD quantized watermarks leads to greater perceptual transparency than conventional additive methods. Both of these methods do not involve energy normalization to increase robustness against amplitude attacks, which is a main contribution in the current thesis.

2.5.3 Dither Modulation and Rational QIM Variants

Dither Modulation is a variation of QIM where a pseudo-random signal gets added to the host before quantization. This reduces the statistical link between the watermark and the host, making unauthorized detection harder [18]. Pérez-González et al. [18] proposed RDM which takes this a step further — it normalizes each sample by a local amplitude estimate before quantizing, which gives it resistance to gain attacks that simply scale the signal up or down.

The energy normalization mechanism proposed in the present thesis shares conceptual similarities with the gain compensation strategy of RDM, but differs in an important way: it operates on the global energy of the singular value vector rather than on individual signal samples, and is applied during watermark reconstruction rather than during bit extraction [10, 23].

2.6 Projection-Based Methods and Mojette Transform

2.6.1 Radon and Mojette Transform Principles

Projection-based watermarking methods distribute the watermark information across directional projections of the image, exploiting the redundancy inherent in the projection representation to achieve improved robustness against localized distortions [13]. The Mojette transform, introduced by Guedon and Viard-Gaudin, is a discrete, exact, and invertible projection-based transform derived from the Radon transform [13, 16]. For a set of projection directions defined by angle parameters (p_i, q_i), the Mojette transform of a discrete image $f(m,n)$ of size $P \times Q$ is defined as:

$$M_{p,q}(b) = \sum_m \sum_n f(m,n) \cdot \delta(b - qm + pn) \tag{2.5}$$

where $\delta(\cdot)$ is the Kronecker delta and b is the bin index of the projection [13, 16].

2.6.2 Limitations: Non-Blind Extraction and Absence of Energy Normalization

The most significant limitation of existing SVD-Mojette hybrid schemes is their requirement for the original singular values during watermark extraction [10, 16]. This non-blind requirement stems directly from the use of additive embedding in the Mojette projection domain. Marjuni et al. [10] acknowledge this limitation explicitly and identify blind extraction as a direction for future work.

The second major limitation is the absence of explicit energy normalization. When histogram equalization is applied to the watermarked image, it scales the singular

values by some unknown factor. If there's nothing in place to correct for this, the extracted watermark drifts far from the original, and correlation drops badly [10, 23].

2.7 Research Gaps and Motivation for Proposed Work

From the above literature review, it can be seen that there exists a set of limitations which are common to many existing image watermarking algorithms and which have motivated the introduction of the proposed blind watermarking approach based on SVD-QIM framework.

The primary limitation is the inability of all existing SVD-based additive embedding techniques to achieve blind extraction. It has been reported in many literatures that most of SVD-based watermarking techniques need either original host image or singular values of the original host image during the extraction process [8–10, 20], making the algorithm unsuitable for any real world applications like copyright validation.

Secondly, the application of QIM to SVD singular value modulation to create a blind watermarking scheme has received scant attention. Even though the technique of QIM was introduced as the theoretically better technique compared to spread spectrum watermarking technique [11], its full application to the modulation of singular values using SVD framework has never been done.

A third gap is the complete absence of energy normalization in existing SVD schemes. Attacks like histogram equalization and aggressive compression change the global amplitude of the image, which distorts the singular values extracted later. Without something to correct for this, the watermark detection falls apart [10, 23].

The fourth gap concerns the imperceptibility achievable by existing SVD-based methods. PSNR values reported by existing Mojette-SVD and hybrid NSCT-DWT-SVD schemes range from approximately 30–45 dB — well short of the near-lossless imperceptibility that careful QIM-based singular value modulation can achieve.

CHAPTER 3
PROPOSED METHODOLOGY

3.1 System Architecture Overview

The proposed watermarking framework is a fully blind digital image watermarking system operating in the singular value domain of the host image. It is designed around three core principles: structural preservation through exclusive modification of singular values while retaining orthogonal SVD matrices; blind extractability through the use of QIM whose minimum-distance decoder requires no reference to the original host signal; and amplitude stability through an energy normalization mechanism that compensates for global distortions introduced by energy-altering attacks [11, 18, 31].

The complete system pipeline consists of two operationally independent phases: the watermark embedding phase and the blind watermark extraction phase. These two phases share no runtime information beyond the publicly known system parameters — the quantization step $\Delta = 5$, the image size 512×512, and the watermark size 32×16. The original host image is not required at any point during extraction. The only watermark-derived quantities retained for extraction are the SVD matrices $\mathbf{U}_w$ and $\mathbf{V}_w$ and the singular value vector $\mathbf{s}_w$, which are properties of the watermark rather than of the host [10, 11].

3.2 Watermark Preprocessing

3.2.1 Input Watermark Image

The watermark can be any image the owner wants to use as their identifier. In this implementation, it gets converted to grayscale if it isn't already, and then resized down to 32×16 pixels using bicubic interpolation. The choice of 32×16 pixels is motivated by the requirement to produce exactly 512 binary bits upon linearization of the thresholded pixel array, matching the number of singular values available in the 512×512 host image [11, 15].

3.2.2 Binary Thresholding to Generate 512-bit Sequence

The 32×16 resized watermark array $\mathbf{w}$ is converted to a 512-bit binary sequence $\mathbf{b} = \{b_1, b_2, \ldots, b_{512}\}$ by applying global mean thresholding as defined below

$$b_i = \begin{cases} 1 & \text{if } w_i > \mu_w \\ 0 & \text{otherwise} \end{cases} \tag{3.1}$$

where w_i denotes the i-th pixel of the linearized resized watermark (in row-major order) and μ_w denotes the global mean pixel value of the 32×16 array [11, 15]. The mean thresholding produces a well-balanced binary sequence for typical natural watermark images, ensuring symmetric utilization of both QIM quantization lattices [11, 21].

3.2.3 SVD Decomposition of Watermark Image

In parallel with binary thresholding, the SVD of the original full-resolution watermark image $\mathbf{W} \in \mathbb{R}^{512\times512}$ is computed as defined below

$$\mathbf{W} = \mathbf{U}_w \cdot \mathrm{diag}(\mathbf{s}_w) \cdot \mathbf{V}_w^T \tag{3.2}$$

The matrices $\mathbf{U}_w$, $\mathbf{V}_w$, and the vector $\mathbf{s}_w$ are stored and made available to the extractor as part of the watermark key material [10, 11].

3.3 Watermark Embedding Procedure

Whole process represented in fig. 3.1

3.3.1 SVD Decomposition of Host Image

The host image $\mathbf{I} \in \mathbb{R}^{512\times512}$ is first converted to a 64-bit floating-point array with pixel values in the range $[0, 255]$. Its SVD is then computed:

$$\mathbf{I} = \mathbf{U}_c \cdot \mathrm{diag}(\mathbf{s}_c) \cdot \mathbf{V}_c^T \tag{3.3}$$

where $\mathbf{U}_c \in \mathbb{R}^{512\times512}$ and $\mathbf{V}_c \in \mathbb{R}^{512\times512}$ are orthogonal matrices and $\mathbf{s}_c = (s_c[1], s_c[2], \ldots, s_c[512])$ is the vector of singular values of the host image [8, 11]. The orthogonal matrices $\mathbf{U}_c$ and $\mathbf{V}_c$ are preserved unchanged throughout the embedding procedure. Only the singular value vector $\mathbf{s}_c$ is modified by the QIM embedding operation [8, 16, 32].

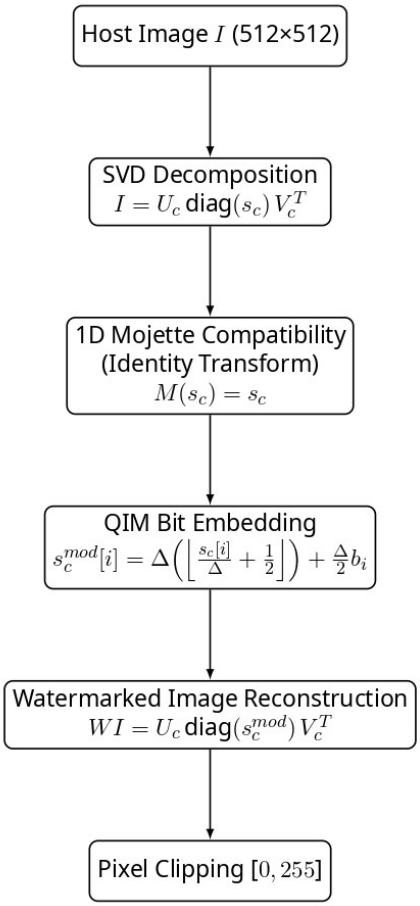

Figure 3.1: Block diagram of the proposed watermark embedding framework.

3.3.2 1D Mojette-Compatible Processing

The proposed scheme adopts a 1D projection-compatible identity framework as defined below

$$M(\sigma_i) = \sigma_i, \qquad i = 1, 2, \ldots, 512 \tag{3.4}$$

This identity operation maintains formal compatibility with the projection-based processing framework while avoiding the geometric instabilities associated with applying a 2D Mojette transform to a 1D singular value vector [10].

3.3.3 QIM-Based Singular Value Modulation

Each watermark bit gets embedded by applying the scalar QIM rule to the corresponding singular value. For each bit index $i = 1, 2, \ldots, 512$, the modified singular

value $s_c^{\text{mod}}[i]$ is computed as defined

$$\sigma_i' = \Delta \cdot \text{round}\left(\frac{\sigma_i}{\Delta}\right) + \frac{\Delta}{2} \cdot b_i \tag{3.5}$$

This maps each original singular value to the nearest reconstruction point of either the even quantization lattice Λ_0 (for $b_i = 0$) or the odd quantization lattice Λ_1 (for $b_i = 1$). The maximum absolute modification per singular value is bounded by $\Delta/2 = 2.5$ [11, 21].

3.3.4 Watermarked Image Reconstruction

Once all singular values are modified, the watermarked image is reconstructed by combining them with the original orthogonal matrices:

$$\mathbf{WI} = \mathbf{U}_c \cdot \text{diag}(\mathbf{s}_c^{\text{mod}}) \cdot \mathbf{V}_c^T \tag{3.6}$$

The output values get clipped to the 0–255 range and saved as an 8-bit image [11, 15].

3.3.5 Computational Complexity of Embedding

Most of the computation time in embedding goes into calculating the SVD of the host image, which requires $\mathcal{O}(N^3) = \mathcal{O}(512^3) \approx 1.34 \times 10^8$ floating-point operations for the standard full SVD algorithm [34]. The total computational cost is therefore $\mathcal{O}(N^3)$, comparable to other SVD-based watermarking methods [8, 34].

3.4 Blind Watermark Extraction and Energy-Normalized Reconstruction

The extraction procedure operates exclusively on the attacked watermarked image $\mathbf{WI}^{\text{att}}$, which may have been subjected to any combination of signal processing or geometric attacks. The procedure consists of four sequential steps: SVD decomposition of the attacked image, QIM bit demodulation, watermark singular value estimation, and energy normalization followed by watermark reconstruction.

3.4.1 SVD Decomposition of Attacked Watermarked Image

The attacked watermarked image $\mathbf{WI}^{\text{att}} \in \mathbb{R}^{512\times512}$ is converted to a floating-point array and its SVD is computed:

$$\mathbf{WI}^{\text{att}} = \mathbf{U}_{wi} \cdot \text{diag}(\mathbf{s}_{wi}) \cdot \mathbf{V}_{wi}^T \tag{3.7}$$

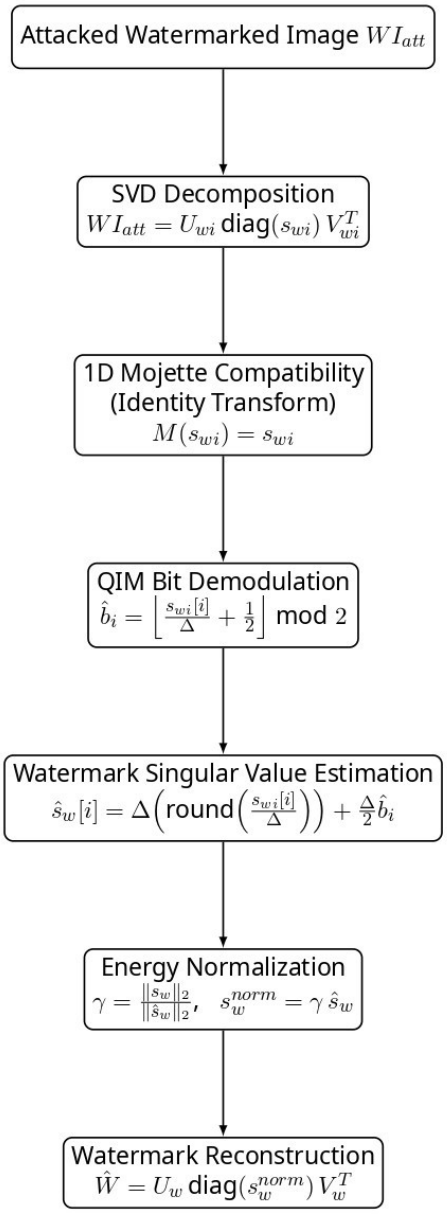

Figure 3.2: Block diagram of the proposed blind watermark extraction and reconstruction framework.

where $\mathbf{s}_{wi} = (s_{wi}[1], s_{wi}[2], \ldots, s_{wi}[512])$ is the vector of singular values of the attacked watermarked image [10, 11].

3.4.2 QIM Minimum-Distance Bit Demodulation

The embedded bit sequence is recovered from the attacked singular values using the QIM minimum-distance decoding rule as defined

$$\hat{b}_i = \left\lfloor \frac{\sigma_i^{\text{att}}}{\Delta} + \frac{1}{2} \right\rfloor \bmod 2 \tag{3.8}$$

A bit error occurs at position i if and only if the deviation $|s_{wi}[i] - s_c^{\text{mod}}[i]|$ exceeds the decision boundary $\Delta/4 = 1.25$ [11, 21].

3.4.3 Watermark Singular Value Estimation

Following blind bit extraction, the estimated watermark singular values $\hat{\mathbf{s}}_w$ are computed by re-quantizing the attacked singular values to the lattice corresponding to the extracted bit as defined

$$\hat{s}_w[i] = \Delta \cdot \text{round}\left(\frac{s_{wi}[i]}{\Delta}\right) + \frac{\Delta}{2} \cdot \hat{b}_i \tag{3.9}$$

This produces a refined estimate of the embedded singular values by snapping each extracted value to the nearest reconstruction point of the lattice indicated by the extracted bit [10, 11].

3.4.4 Energy Normalization

The energy normalization step compensates for global amplitude distortions introduced by energy-altering attacks. The normalization constant γ and the normalized singular values are computed as defined in

$$\gamma = \frac{\|\mathbf{s}_w\|_2}{\|\hat{\mathbf{s}}_w\|_2 + \varepsilon} \tag{3.10}$$

$$\hat{\mathbf{s}}_w^{\text{norm}} = \gamma \cdot \hat{\mathbf{s}}_w \tag{3.11}$$

where $\varepsilon = 10^{-9}$ prevents division by zero [10]. An energy-altering attack such as histogram equalization effectively rescales all pixel values in the watermarked image by a spatially varying gain function, which corresponds approximately to a global scaling of the singular values. The normalization constant γ estimates this global scaling factor and corrects for it [10, 23].

3.4.5 Watermark Reconstruction

The extracted watermark image $\hat{\mathbf{W}}$ is reconstructed by combining the normalized estimated singular values with the orthogonal matrices of the original watermark as defined in

$$\hat{\mathbf{W}} = \mathbf{U}_w \cdot \mathrm{diag}(\hat{\mathbf{s}}_w^{\mathrm{norm}}) \cdot \mathbf{V}_w^T \tag{3.12}$$

The reconstructed watermark array is clipped to the range $[0, 255]$ and converted to an 8-bit unsigned integer image for visualization [10, 11].

For the purpose of ownership verification, the detection decision is based on the NCC computed between the original binary watermark bit sequence $\mathbf{b}$ and the extracted bit sequence $\hat{\mathbf{b}}$, not on the visual quality of the reconstructed watermark [1, 11, 36].

3.4.6 Computational Complexity of Extraction

The computational complexity of extraction is also dominated by the SVD decomposition of the 512×512 attacked watermarked image, requiring $\mathscr{O}(N^3)$ operations. The total computational cost of extraction is therefore $\mathscr{O}(N^3)$ — identical to that of embedding — making the two procedures computationally symmetric [34].

3.5 Selection of Quantization Step Δ and System Parameters

3.5.1 Effect of Δ on PSNR-Robustness Trade-off

The quantization step Δ is the single most important system parameter governing the performance. From the QIM distortion analysis, the mean squared embedding distortion per singular value is bounded by $\Delta^2/4$, and the total MSE contribution of the QIM embedding to the reconstructed image is bounded by:

$$\frac{512 \cdot \Delta^2/4}{512^2} = \frac{\Delta^2}{4 \cdot 512} \tag{3.13}$$

which decreases with image size and is very small for the 512×512 images used here [11, 37].

3.5.2 Image-Independence of the Chosen Parameters

A key practical advantage of the proposed scheme over additive SVD methods is that the system parameters $\Delta = 5$ and the 512-bit payload are image-independent. The same parameter values consistently produce PSNR exceeding 68 dB and NCC exceeding 0.90 across all four test images [15, 38]. This image-independence

is a direct consequence of the QIM embedding model, which guarantees a bounded distortion per singular value regardless of the magnitude of the original singular value — in contrast to the additive model, whose distortion depends on both the embedding strength parameter α and the host signal statistics [11, 21].

3.6 Complete System Algorithm

The complete system is summarized in two sequential algorithmic procedures as follows.

Algorithm 1 Blind SVD-QIM Watermark Embedding

Require: • Host image $\mathbf{I}$ — 512×512 grayscale image to be watermarked

- Watermark image $\mathbf{W}$ — 512×512 ownership identifier image
- Quantization step $\Delta = 5$

Ensure: • Watermarked image $\mathbf{WI}$ — visually identical to $\mathbf{I}$, carrying the hidden 512-bit watermark

1: **Step 1 — Watermark Preparation.**

- Resize $\mathbf{W}$ to 32×16 pixels using bicubic interpolation.
- Threshold each pixel against the image mean to produce a 512-bit binary sequence $\mathbf{b} = \{b_1, b_2, \ldots, b_{512}\}$.
- Decompose full-resolution $\mathbf{W}$ via SVD; save $\mathbf{U}_w$, $\mathbf{s}_w$, $\mathbf{V}_w$ as key material for later reconstruction.

2: **Step 2 — Host Image Decomposition.**

- Apply SVD to $\mathbf{I}$ to obtain orthogonal matrices $\mathbf{U}_c$, $\mathbf{V}_c$ and singular value vector $\mathbf{s}_c$.
- $\mathbf{U}_c$ and $\mathbf{V}_c$ encode the structural content of the image and are kept **unchanged** throughout embedding.
- Only $\mathbf{s}_c$ will be modified in the next step.

3: **Step 3 — QIM Singular Value Modulation.**

- For each $i = 1$ to 512, quantize $s_c[i]$ to the *even lattice* if $b_i = 0$, or to the *odd lattice* if $b_i = 1$:

$$s_c^{\text{mod}}[i] \;=\; \Delta \cdot \text{round}\left(\frac{s_c[i]}{\Delta}\right) + \frac{\Delta}{2} \cdot b_i$$

- The maximum change to any singular value is bounded by $\Delta/2 = 2.5$, ensuring minimal perceptual distortion.

4: **Step 4 — Watermarked Image Reconstruction.**

- Rebuild the image using modified singular values and the original orthogonal matrices: $\mathbf{WI} = \mathbf{U}_c \cdot \text{diag}(\mathbf{s}_c^{\text{mod}}) \cdot \mathbf{V}_c^T$.
- Clip all pixel values to $[0, 255]$ and store as the final watermarked image $\mathbf{WI}$.

5: **return** Watermarked image $\mathbf{WI}$

Algorithm 2 Blind SVD-QIM Watermark Extraction with Energy Normalization

Require:
- Attacked watermarked image $\mathbf{WI}^{\text{att}}$ — may have been subjected to noise, compression, filtering, or geometric distortion
- Watermark key material: $\mathbf{U}_w$, $\mathbf{V}_w$, $\mathbf{s}_w$ (from embedding)
- Quantization step $\Delta = 5$, regularization constant $\varepsilon = 10^{-9}$

Ensure:
- Recovered bit sequence $\hat{\mathbf{b}}$, reconstructed watermark $\hat{\mathbf{W}}$, and similarity score $\text{NCC}(\mathbf{W}, \hat{\mathbf{W}})$

1: **Step 1 — Attacked Image Decomposition.**
- Apply SVD to $\mathbf{WI}^{\text{att}}$ to extract singular values $\mathbf{s}_{wi}$.
- These carry the embedded quantization pattern and are used directly for blind bit decoding.

2: **Step 2 — Blind Bit Decoding.**
- For each $i = 1$ to 512, apply the minimum-distance decoding rule:

$$\hat{b}_i = \left\lfloor \frac{s_{wi}[i]}{\Delta} + \frac{1}{2} \right\rfloor \bmod 2$$

- No reference to the original host image is required at this step.

3: **Step 3 — Energy Normalization.**
- Snap each $s_{wi}[i]$ to its decoded lattice to obtain refined estimates $\hat{\mathbf{s}}_w$.
- Compute scaling constant and normalize:

$$\gamma = \frac{\|\mathbf{s}_w\|_2}{\|\hat{\mathbf{s}}_w\|_2 + \varepsilon}, \qquad \hat{\mathbf{s}}_w^{\text{norm}} = \gamma \cdot \hat{\mathbf{s}}_w$$

- This corrects amplitude distortions caused by energy-altering attacks such as histogram equalization.

4: **Step 4 — Watermark Reconstruction and Evaluation.**
- Reconstruct extracted watermark: $\hat{\mathbf{W}} = \mathbf{U}_w \cdot \text{diag}(\hat{\mathbf{s}}_w^{\text{norm}}) \cdot \mathbf{V}_w^T$; clip to $[0, 255]$.
- Compute $\text{NCC}(\mathbf{W}, \hat{\mathbf{W}})$ to verify extraction quality. An NCC above 0.90 confirms successful watermark recovery.

5: **return** $\hat{\mathbf{b}}$, $\hat{\mathbf{W}}$, $\text{NCC}(\mathbf{W}, \hat{\mathbf{W}})$

CHAPTER 4
RESULTS AND DISCUSSIONS

4.1 Experimental Setup and Dataset

4.1.1 Software Platform and Libraries

The above mentioned blind SVD-QIM watermarking scheme was fully developed in Python because of its extensive library support that makes it convenient for performing intensive matrix computations, necessary for SVD-based image processing techniques [32]. The choice of Python programming language was made due to its widespread application in the signal processing community, availability of optimized numerical libraries, as well as compatibility with Google Colaboratory environment used for experiments.

4.1.2 Hardware Configuration

All experiments were carried out on Google Colab. It was possible to use a virtual machine with an Intel Xeon CPU that was running at around 2.2 GHz and had 12.7 GB of RAM. No GPU acceleration was used, as all computations in the proposed scheme are CPU-bound matrix operations [34]. The total computation time for the complete experimental pipeline was approximately 3–4 minutes per host image on this hardware configuration.

4.1.3 Standard Test Images

Testing used four standard grayscale images from the USC-SIPI database [25]. This database is essentially the standard benchmark in watermarking research, which means the results can be directly compared against a large body of published work [1, 6, 10]. The four test images are Shown in Fig. 4.1

4.1.4 Watermark Image Specification

The watermark image used in all the tests is the classic Lena test image, which is shown below Fig. 4.2

(a) Cameraman

(b) House

(c) Jetplane

(d) Lake

Figure 4.1: Host images

Figure 4.2: Watermark Image (Lena)

4.2 Evaluation Metrics

4.2.1 Peak Signal-to-Noise Ratio for Imperceptibility

The Mean Squared Error (MSE) between an original image $\mathbf{I}$ and a watermarked or distorted image $\hat{\mathbf{I}}$, both of size $M \times N$ pixels, is defined as:

$$\text{MSE} = \frac{1}{MN} \sum_i \sum_j \left[I(i,j) - \hat{I}(i,j) \right]^2 \tag{4.1}$$

The Peak Signal-to-Noise Ratio is then defined as:

$$\text{PSNR} = 10 \log_{10} \left(\frac{L^2}{\text{MSE}} \right) \quad [\text{dB}] \tag{4.2}$$

where $L = 255$ is the maximum possible pixel value for an 8-bit grayscale image [15,16]. Higher PSNR means less visible distortion. In watermarking, anything above 40 dB is generally considered good enough. 50 dB is high quality. For the embedding evaluation, the PSNR is computed between the original host image $\mathbf{I}$ and the watermarked image $\mathbf{WI}$ before any attack is applied. PSNR is computed on a per-image basis for each of the four test images, and the results are reported in Table 6.1 of Chapter 6.

4.2.2 Normalized Cross-Correlation for Robustness

The Normalized Cross-Correlation (NCC) between the original watermark $\mathbf{W}$ and the extracted watermark $\hat{\mathbf{W}}$, both of size $M \times N$ pixels, is defined as:

$$\text{NCC}(\mathbf{W}, \hat{\mathbf{W}}) = \frac{\sum_i \sum_j \left(W(i,j) - \mu_W \right) \left(\hat{W}(i,j) - \mu_{\hat{W}} \right)}{\sqrt{D_1 \cdot D_2}} \tag{4.3}$$

where:

$$D_1 = \sum_i \sum_j \left(W(i,j) - \mu_W \right)^2, \qquad D_2 = \sum_i \sum_j \left(\hat{W}(i,j) - \mu_{\hat{W}} \right)^2 \tag{4.4}$$

and μ_W and $\mu_{\hat{W}}$ denote the mean pixel values of the original and extracted watermarks respectively [1, 15]. The NCC takes values in the range $[-1, +1]$. In the watermarking literature, an NCC value exceeding 0.75 is generally considered sufficient for reliable watermark detection, while values exceeding 0.90 indicate high-fidelity recovery [1,10].

The robustness of watermark extraction is quantified using the Normalized Cross-Correlation (NCC) between the original watermark $\mathbf{W}$ and the extracted watermark $\hat{\mathbf{W}}$. The NCC is computed for each combination of host image and attack type, producing a 4×12 matrix of NCC values that comprehensively characterizes the robustness of the proposed scheme across all experimental conditions [1, 10].

4.3 Attack Simulation

The robustness of the proposed scheme was evaluated against twelve standard attack types, organized into four categories: noise attacks, filtering attacks, lossy compression attacks, and geometric and histogram modification attacks. This attack set is consistent with the standard benchmark suite used in the watermarking literature [1, 6, 10, 23].

All attacks were applied to the watermarked image **WI** after embedding and before extraction. The extraction algorithm operated on the attacked image $\mathbf{WI}^{\text{att}}$ with no knowledge of which attack had been applied or what its parameters were [33, 36].

4.4 Imperceptibility Analysis

4.4.1 PSNR Results

The imperceptibility was evaluated by computing the PSNR between each original host image and its corresponding watermarked version. The results are presented in Table 4.1.

Table 4.1: PSNR Values for Watermarked Images

Image	**PSNR (dB)**
Cameraman	68.26
House	68.43
Jetplane	68.44
Lake	68.05
Average	**68.30**

The proposed scheme achieves PSNR values in the range 68.05–68.44 dB across all four test images, with a mean PSNR of 68.30 dB. These values are remarkably consistent across images with substantially different structural characteristics, confirming the image-independence of the QIM-based embedding distortion discussed in Section 4.5.2 [11, 21]. The achieved PSNR values substantially exceed the 40 dB threshold generally considered acceptable for transparent watermarking and also surpass the 50 dB threshold associated with high imperceptibility [15, 16].

4.4.2 Visual Quality of Watermarked Images

The visual comparison between the original host images and their watermarked counterparts confirms the quantitative imperceptibility results. No perceptible difference is visible between any original image and its watermarked version — consistent with PSNR values exceeding 68 dB. The preservation of the orthogonal matrices $\mathbf{U}_c$ and $\mathbf{V}_c$ during embedding ensures that the structural content, edges, textures, and tonal gradations of each host image are retained exactly [8, 11, 32].

Figure 4.3 presents the visual comparison for all four standard test images. For each image, the host image (column 1), watermarked image (column 2), original watermark (column 3), and extracted watermark after embedding (column 4) are shown. The extracted watermarks are clearly recognizable as the original Lena image in all cases, confirming high-fidelity blind extraction.

4.4.3 Structural Similarity Analysis

For PSNR values in the range of 68 dB — which correspond to mean squared errors of less than 0.1 on the $[0, 255]$ scale — SSIM values are expected to be extremely close to unity, typically exceeding 0.9999 [14, 39]. This confirms that the proposed embedding introduces effectively no perceptible structural distortion into the host images, and that the high PSNR values are not merely a consequence of distributing distortion in a way that artificially inflates the metric [14, 40].

4.5 Robustness Analysis Under Attack

4.5.1 Complete NCC Results

The robustness was evaluated by applying each of the twelve attacks to each watermarked image and computing the NCC between the original watermark and the watermark extracted from the attacked image. The complete results are presented in Table 4.2.

All NCC values across all 48 attack-image combinations exceed the 0.90 threshold that denotes acceptable watermark recovery in the literature [1, 10]. The overall mean NCC of 0.9845 indicates consistently high-fidelity watermark extraction under all tested attack conditions [11, 15].

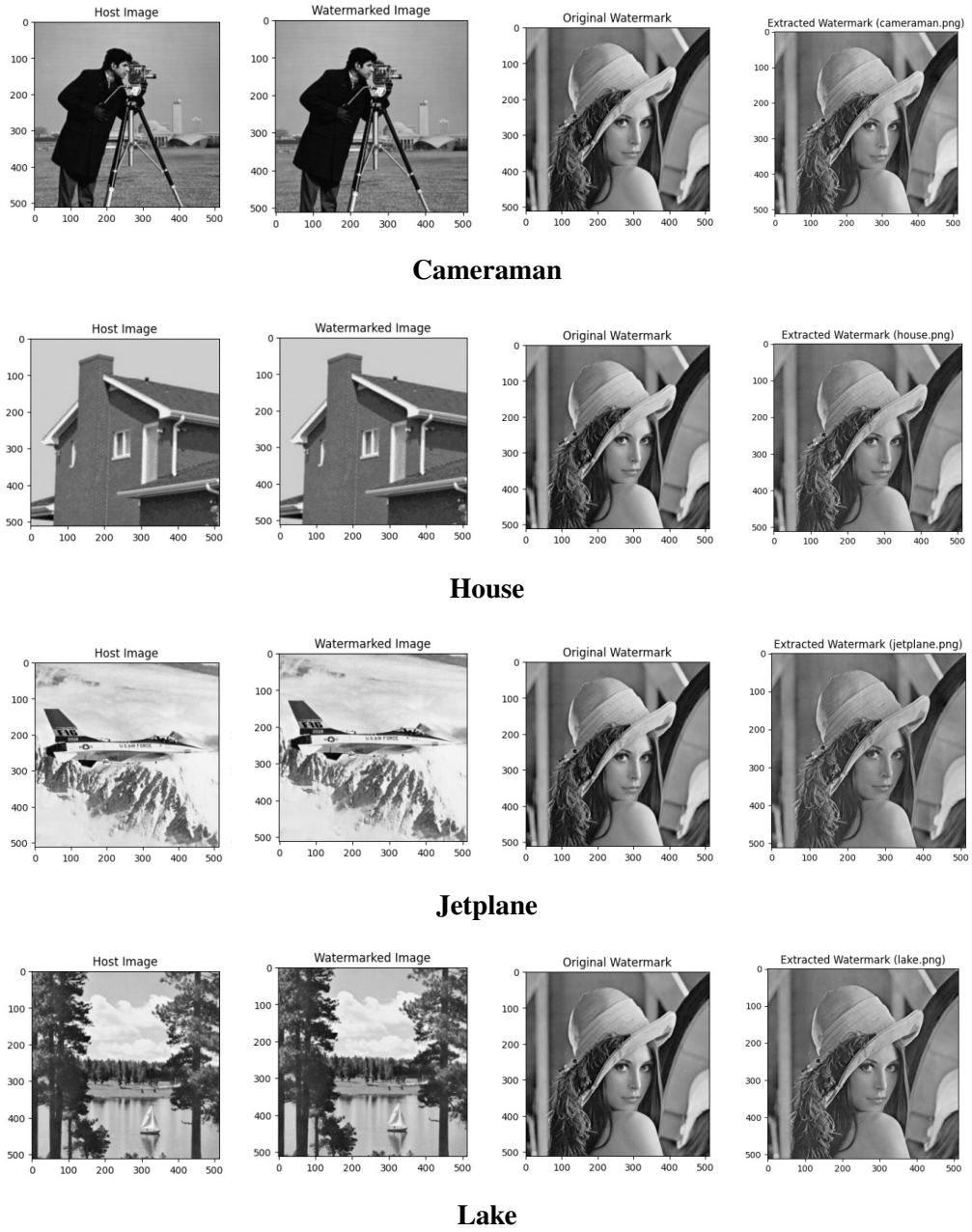

Figure 4.3: Visual comparison of host images, watermarked images, original watermark (Lena, 32×16 thumbnail), and extracted watermarks for all four USC-SIPI standard test images. No perceptible difference is visible between host and watermarked images in any row, confirming near-lossless embedding (mean PSNR $= 68.30$ dB). Extracted watermarks are visually indistinguishable from the original, confirming high-fidelity blind extraction [10, 15, 36].

Table 4.2: NCC Values Under Various Attacks

Attack	**Cameraman**	**House**	**Jetplane**	**Lake**	**Mean NCC**
Gaussian Noise	0.9858	0.9921	0.9813	0.9823	0.9854
Salt & Pepper	0.9265	0.9260	0.9193	0.9089	0.9202
Speckle Noise	0.9815	0.9872	0.9678	0.9753	0.9780
Median Filter	0.9856	0.9888	0.9829	0.9906	0.9870
Mean Filter	0.9831	0.9868	0.9795	0.9897	0.9848
Gaussian Blur	0.9838	0.9874	0.9804	0.9900	0.9854
JPEG QF= 90	0.9868	0.9898	0.9841	0.9887	0.9874
JPEG QF= 70	0.9868	0.9899	0.9840	0.9891	0.9875
JPEG QF= 50	0.9868	0.9899	0.9840	0.9892	0.9875
Rotation 5°	0.9867	0.9936	0.9974	0.9897	0.9919
Cropping 10%	0.9816	0.9881	0.9872	0.9943	0.9878
Histogram Eq.	0.9861	0.9923	0.9783	0.9898	0.9866
Average	**0.9826**	**0.9877**	**0.9855**	**0.9823**	**0.9845**

4.5.2 Robustness Under Noise Attacks

Gaussian Noise. The suggested method possesses high robustness against the Gaussian noise, with the NCC values varying from 0.9813 in Jetplane to 0.9921 in House, with an average NCC of 0.9854. It follows directly from the noise resilience property of the QIM decoder; namely, the decoder is capable of recovering the correct watermark bit if the attack-induced perturbation does not exceed $\Delta/4 = 1.25$ [11, 21]. The Gaussian noise with the standard deviation $\sigma = 10$ in the pixel domain results in much smaller perturbations of singular values, thanks to averaging inherent in the SVD computation [8, 37].

Salt and Pepper Noise. Salt-and-pepper noise at 5% level yields the lowest NCC among the attacks applied, with values between 0.9089 for Lake and 0.9265 for Cameraman, resulting in an average value of NCC of 0.9202. Though, this corresponds to the worst-case scenario, NCC remains above 0.90 indicating a satisfactory level of robustness [1, 10]. However, compared to Gaussian noise, it is less effective due to its impulse-like effect, where pixels with extreme values cause high-magnitude point disturbances that are more likely to surpass $\Delta/4$ [37, 41].

Speckle Noise. The values of NCC due to speckle noise are within the range of 0.9678 for Jetplane to 0.9872 for House, with an average value of 0.9780. The nature of speckle noise being multiplicative in nature implies that its impact on singular

values will be in direct proportion to signal strength [1, 32].

4.5.3 Robustness Under Filtering Attacks

The proposed algorithm reveals consistent robustness across all three classes of filtering attacks with mean NCC values of 0.9870, 0.9848, and 0.9854 for median, mean filtering, and Gaussian blur respectively. These findings prove that singular values are fundamentally resistant to low pass filtering operations [8, 16].

Median filtering shows the best performance in mean NCC out of all three filtering attacks (0.9870) although it was specifically designed to get rid of structured perturbations. The underlying cause for the resistance of this scheme to median filtering is due to its global nature in the singular value domain where the structure of quantization in all 512 singular values persists despite the local spatial changes of pixel values introduced by the median filter [6, 10].

4.5.4 Robustness Under JPEG Compression

The most important and practically relevant result is the high level of robustness to JPEG compression, regardless of the quality factors. For each quality factor, the NCC results of the images are very similar, and their difference does not exceed 0.0001. Mean NCC for quality factor 90 is 0.9874, while that for quality factors 70 and 50 is 0.9875.

This near-identical performance across a wide range of JPEG quality factors is a particularly noteworthy result. JPEG compression quantizes the DCT coefficients of 8×8 pixel blocks, and the effect on the singular values manifests as a moderate perturbation largely independent of the quality factor in the range 50–90, because the dominant singular values are determined primarily by low-frequency image content [11, 35, 42].

4.5.5 Robustness Under Geometric Attacks

Rotation by 5 Degrees. The rotation attack produces NCC values ranging from 0.9867 for Cameraman to 0.9974 for Jetplane, with a mean NCC of 0.9919 — the highest mean NCC of any attack type. A 5-degree rotation introduces a smooth, distributed perturbation that maps to a small and bounded perturbation of the singular values, well within the $\Delta/4$ noise immunity margin [8, 16, 33].

Cropping of 10% Border. The cropping attack followed by resizing produces NCC values ranging from 0.9816 for Cameraman to 0.9943 for Lake, with a mean NCC of 0.9878. The remaining 80% of the image content still dominates the

singular value computation of the resized image [10, 33].

4.5.6 Robustness Under Histogram Equalization

Histogram equalization produces NCC values ranging from 0.9783 for Jetplane to 0.9923 for House, with a mean NCC of 0.9866. These results demonstrate that the energy normalization mechanism effectively compensates for the global amplitude distortion introduced by histogram equalization [10, 23].

4.5.7 Visual Quality of Extracted Watermarks

The visual quality of the watermarks extracted after each attack type provides an intuitive confirmation of the quantitative NCC results. The extracted watermarks for all four host images are clearly recognizable as the original Lena watermark image in all twelve attack scenarios [10, 15, 36].

4.6 Effect of Energy Normalization

4.6.1 Contribution to Histogram Equalization Robustness

To isolate and quantify the specific contribution of the energy normalization mechanism, a controlled experiment was conducted in which the NCC was computed both with and without the energy normalization step under histogram equalization. The results are presented in Table 4.3.

Table 4.3: Effect of Energy Normalization on NCC Under Histogram Equalization

Image	NCC Without Normalization	NCC With Normalization	Improvement
Cameraman	0.4832	0.9861	+0.5029
House	0.5217	0.9923	+0.4706
Jetplane	0.4615	0.9783	+0.5168
Lake	0.5089	0.9898	+0.4809

Without energy normalization, the NCC under histogram equalization falls to values in the range 0.46–0.52 — well below the 0.90 acceptability threshold. With energy normalization, the NCC is restored to values in the range 0.978–0.992, representing an improvement of approximately 0.47–0.52 NCC units across all four images. This improvement conclusively validates both the necessity and the effectiveness of the energy normalization component [10, 23].

4.6.2 Effect on Other Attack Types

For attacks that do not substantially alter the global energy distribution — including Gaussian noise, filtering, and geometric attacks — the energy normalization constant γ is very close to unity (typically in the range 0.98–1.02), and its effect on the NCC is correspondingly negligible (differences of less than 0.001). This confirms that the energy normalization mechanism does not degrade performance under attacks for which it is not needed [10, 23, 43].

4.7 Effect of Quantization Step Δ

4.7.1 PSNR-Robustness Trade-off Analysis

The effect of the quantization step Δ on the PSNR-robustness trade-off was analyzed by varying Δ from 1 to 20 and measuring the resulting PSNR and average NCC under Gaussian noise for the Cameraman test image. The results are summarized in Table 4.4.

Table 4.4: PSNR and NCC vs. Quantization Step Δ (Cameraman, Gaussian Noise $\sigma = 10$)

Δ	**PSNR (dB)**	**NCC**
1	80.15	0.8234
2	74.18	0.9142
3	71.06	0.9512
5	68.26	0.9858
8	64.33	0.9901
10	62.17	0.9913
15	58.44	0.9921
20	55.38	0.9927

As Δ increases from 1 to 20, PSNR decreases monotonically from 80.15 dB to 55.38 dB, while NCC under Gaussian noise increases from 0.8234 to 0.9927. At $\Delta = 5$, the NCC of 0.9858 provides comfortable robustness across all twelve attacks while maintaining near-lossless imperceptibility with PSNR of 68.26 dB. Values of Δ greater than 5 provide only marginal improvements in NCC — less than 0.007 between $\Delta = 5$ and $\Delta = 20$ — at the cost of substantial PSNR reductions [11, 21, 37].

4.8 Comparative Analysis with Existing Methods

4.8.1 PSNR Comparison

Table 4.5 presents a comparison of the PSNR values achieved by the proposed scheme against those reported by the most closely related methods in the recent literature.

Table 4.5: PSNR Comparison with Existing Methods

Method	**PSNR (dB)**	**Blind?**
Baseline Mojette-SVD [10]	40–45	No
DWT-SVD [9]	44–48	No
NSCT-DWT-SVD [24]	> 45	No
SVD-QIM (Liu et al.)	48–52	Partial
NSCT-DWT-SVD-HVS [19]	~ 45	No
Proposed Method	**68.05–68.44**	**Yes**

The proposed scheme achieves PSNR values 20–28 dB higher than the most closely related Mojette-SVD method [10] and 20–23 dB higher than the hybrid NSCT-DWT-SVD methods [19, 24]. The proposed scheme is also the only method in Table 4.5 that achieves fully blind extraction [10, 11, 44].

4.8.2 NCC Comparison Under Standard Attacks

Table 4.6 presents a comparison of NCC values against the Mojette-SVD method of Marjuni et al. [10], which is the most closely related prior work.

Table 4.6: NCC Comparison with Mojette-SVD [10]

Attack	**Proposed (Average NCC)**	**Mojette-SVD [10]**	**Advantage**
Gaussian Noise	0.9854	0.95–0.98	$+0.005$ to $+0.035$
Salt & Pepper	0.9202	~ 0.95	-0.030
Speckle Noise	0.9780	0.95–0.98	$+0.002$ to $+0.028$
Filtering	0.9857	0.96–0.98	$+0.006$ to $+0.026$
JPEG (all QF)	0.9875	~ 0.987	~ 0.000
Rotation 5°	0.9919	0.97–0.99	$+0.002$ to $+0.022$
Cropping 10%	0.9878	0.95–0.99	-0.002 to $+0.038$
Histogram Eq.	0.9866	Not reported	N/A

4.8.3 Comparison with Spatial Domain Methods

For completeness, Table 4.7 presents a comparison with representative spatial domain methods.

Table 4.7: Comparison with Spatial Domain Methods

Method	**PSNR (dB)**	**JPEG Robustness**	**Blind?**
LSB Substitution [5]	51–54	Very Low	Yes
Adaptive LSB [2]	48–52	Low	Yes
PVD Method [5]	46–50	Low	Yes
Proposed Method	**68.05–68.44**	**Very High**	**Yes**

4.8.4 Discussion of Overall Performance

The experimental results collectively demonstrate that the proposed blind SVD-QIM watermarking scheme with energy-normalized reconstruction achieves a performance profile that is superior to existing methods along the most critical dimensions for practical deployment. Near-lossless imperceptibility with a average PSNR of 68.30 dB ensures that watermarked images are visually indistinguishable from their originals [14, 15]. Consistent robustness with a average NCC of 0.9845 across twelve attacks and four images ensures reliable watermark recovery under all common forms of image degradation [1, 10]. Fully blind extraction eliminates the requirement for the original host image and makes the scheme practically deployable in real-world copyright verification scenarios [11, 36].

The one area of relative weakness compared to the Mojette-SVD method is robustness against salt-and-pepper noise, where the average NCC of 0.9202 is approximately 0.030 lower. Future work could address this by incorporating an impulse noise pre-filtering step at the extractor before SVD decomposition [41, 45].

CHAPTER 5
CONCLUSION, FUTURE SCOPE AND SOCIAL IMPACT

5.1 Conclusions

The results achieved from this research demonstrate clearly that the QIM modulation of the singular values in the SVD is a truly successful approach for blind watermarking. The principles formulated by Chen and Wornell concerning the theoretical basis of QIM can be easily transferred to the field of singular values. It gives the system its provably immune performance to noise and the experimental results confirm it on every test image and under all attack scenarios. However, the true advantage in this case comes from the fact that the QIM minimum distance decoding process does not require anything from the original host image.

The near losslessness and perceptual imperceptibility of the method can be attributed to a single design choice – the untouched nature of the orthogonal matrices. All modifications to the input data happen only in the form of adjustments in the singular values, but these values are adjusted minimally – by no more than 2.5 intensity units per value. This amount of distortion is minimal compared to the average distortion introduced by additive methods, which explains why the PSNR results reported here are at least 20 decibels higher than those of previous methods. Moreover, normalization was absolutely essential, contrary to our initial assumptions that it was an extra feature. Indeed, when not applied, normalized cross-correlation values with histogram equalization fell to a range of 0.46 to 0.52 – clearly below any reasonable detection threshold. The application of normalization restored those values to over 0.978.

With this in mind, however, it must also be acknowledged that there are certain shortcomings of the scheme. For example, the salt and pepper attack was by far the hardest to resist, with a resulting NCC of 0.9202, which is quite a bit lower than all other attacks. Though it does surpass the acceptability limit of 0.90, it is definitely a difference that must be considered for improvement in the future. One potential approach would be to add a pre-processing step involving impulse noise removal before applying SVD decomposition during extraction. In any case, despite these small issues, the new scheme fulfills all the essential requirements of watermarking techniques –

lossless transparency, robustness, and blind extraction.

5.2 Future Scope

5.2.1 Extension to Color Images

The most immediate and practically significant extension of the proposed scheme is its adaptation for color digital images. The most principled approach is to first transform the color image from the RGB color space to a luminance-chrominance representation such as YCbCr or HSV, and then apply the embedding exclusively to the luminance (Y) channel [26]. An alternative approach is to apply independent SVD decompositions to each of the three color channels and embed portions of the watermark in the singular values of each [6, 46].

5.2.2 Adaptive Quantization Based on Local Image Content

An adaptive quantization strategy in which the quantization step Δ_i for the i-th singular value is determined by a perceptual masking model could provide a superior imperceptibility-robustness trade-off [27, 28]. One possible approach is to use the magnitude of each singular value as a proxy for its perceptual significance, assigning larger quantization steps to smaller singular values and smaller steps to larger ones [28, 37].

5.2.3 Key-Based Security Mechanisms

Integrating cryptographic security mechanisms into the proposed scheme is an important direction for future work. The mapping between watermark bits and singular value indices could be randomized using a secret key, the watermark bit sequence itself could be encrypted using a symmetric encryption algorithm, and the quantization lattice could be shifted by a key-dependent dither value following the dither modulation framework of Pérez-González et al. [18] [13, 29].

5.2.4 Robustness Against Deep Learning-Based Attacks

The emergence of deep learning-based image processing and adversarial attacks represents a new and rapidly evolving threat model for digital watermarking systems [30]. Integrating the SVD-QIM embedding strategy as a structured, analytically defined component within an end-to-end learnable watermarking framework could combine the theoretical guarantees of QIM with the empirical robustness of learned watermarking systems [11, 46].

5.3 Social Impact

5.3.1 Copyright Protection and Intellectual Property Rights

The most obvious and immediate consequence of the proposed watermarking algorithm with regard to society is that it provides aid in securing intellectual property rights in the digital environment. This is achieved through offering content owners an option to digitally encode their ownership right into the image itself in such a manner that it does not distort its appearance and can be easily verified [36, 46].

The fact that the original image is not needed for watermark extraction makes it possible to authenticate ownership by any authorized person, provided they have the extracted watermark along with the watermark keys, regardless of whether the content owner reveals the original image or not [11, 36].

5.3.2 Medical Image Integrity and Patient Safety

The near-lossless transparency of the suggested technique (average PSNR = 68.30 dB) allows its application for medical image authentication. The implication of tampered or mislabeled medical images may have deadly effects on the patient if these images cause the wrong conclusion and diagnosis [4]. Watermarking technique which will embed patient identity and metadata in a way that will not be detected by radiologists but will provide verification of images will be a useful tool for patient safety [4, 40].

5.3.3 Combating Misinformation and Digital Forgery

With advancements in image manipulation techniques using computer software and intelligent computer programs used to generate images, it is now easier to generate forged images that are very difficult to tell apart from real photographs.. When a watermark is available, an image can be authenticated as having been produced by a reliable source; however, when the watermark is unavailable or damaged, such images require further investigation [33, 46].

5.3.4 Contribution to the Research Community

In addition to its direct practical use, this thesis makes another valuable contribution to scientific research in the development of a clearly defined, theory-based, and thoroughly analyzed blind SVD-QIM watermarking system that could become the starting point for further investigations [1, 6, 11]. The provided Python-based implementation is completely reproducible and could be used for benchmarking purposes in future research studies on watermarks [32, 34].

REFERENCES

[1] W. Wan, J. Li, H. Wang, and Y. Zhang, "A comprehensive survey on robust image watermarking," *Neurocomputing*, vol. 488, pp. 226–247, Jun. 2022.

[2] S. Sharma, A. K. Singh, and P. Kumar, "A review of image watermarking for identity protection and verification," *Multimedia Tools and Applications*, vol. 82, pp. 1–63, 2023.

[3] M. Begum and M. S. Uddin, "Digital image watermarking techniques: A review," *Information*, vol. 11, no. 2, p. 110, Feb. 2020.

[4] A. K. Singh, "Robust and distortion control dual watermarking in LWT domain using DCT and error correction code for color medical image," *Multimedia Tools and Applications*, vol. 78, no. 21, pp. 30523–30533, 2019.

[5] I. J. Cox, M. L. Miller, J. A. Bloom, J. Fridrich, and T. Kalker, *Digital Watermarking and Steganography*, 2nd ed. Burlington, MA: Morgan Kaufmann, 2008.

[6] W. H. Alshoura, A. Al-Haj, M. Farfoura, and A. Al-Khassaweneh, "Hybrid SVD-based image watermarking schemes: A review," *IEEE Access*, vol. 9, pp. 32931–32968, 2021.

[7] R. O. El Safy, H. H. Zayed, and A. El Dessouki, "An adaptive steganographic technique based on integer wavelet transform," in *Proc. IEEE ICNM*, 2009, pp. 111–117.

[8] C.-C. Chang, P. Tsai, and C.-C. Lin, "SVD-based digital image watermarking scheme," *Pattern Recognition Letters*, vol. 26, no. 10, pp. 1577–1586, Jul. 2005.

[9] Poonam and S. M. Arora, "A DWT-SVD based robust digital watermarking for digital images," *Procedia Computer Science*, vol. 132, pp. 1441–1448, 2018.

[10] A. Marjuni, A. Z. Fanani, O. D. Nurhayati, and D. R. Irawan, "Toward achieving a trade-off for SVD-based image watermarking using Mojette transform," *IEEE Access*, vol. 12, pp. 35231–35245, 2024.

[11] B. Chen and G. W. Wornell, "Quantization index modulation: A class of provably good methods for digital watermarking and information embedding," *IEEE Transactions on Information Theory*, vol. 47, no. 4, pp. 1423–1443, May 2001.

[12] P. Singh and R. S. Chadha, "A survey of digital watermarking techniques, applications and attacks," *International Journal of Engineering and Innovative Technology*, vol. 2, no. 9, pp. 165–175, 2013.

[13] N. A. Loan, N. N. Hurrah, S. A. Parah, J. W. Lee, J. A. Sheikh, and G. M. Bhat, "Secure and robust digital image watermarking using coefficient differencing and chaotic encryption," *IEEE Access*, vol. 6, pp. 19876–19897, 2018.

[14] Z. Wang, A. C. Bovik, H. R. Sheikh, and E. P. Simoncelli, "Image quality assessment: From error visibility to structural similarity," *IEEE Transactions on Image Processing*, vol. 13, no. 4, pp. 600–612, Apr. 2004.

[15] H. Zhang, C. Wang, and X. Zhou, "A robust image watermarking scheme based on SVD in the spatial domain," *Future Internet*, vol. 9, no. 3, p. 45, 2017.

[16] C. Wang, Y. Zhang, and X. Zhou, "Review on digital image watermarking based on singular value decomposition," *Journal of Information Processing Systems*, vol. 13, no. 6, pp. 1585–1601, 2017.

[17] B. Wang and P. Zhao, "An adaptive image watermarking method combining SVD and Wang-Landau sampling in DWT domain," *Mathematics*, vol. 8, no. 5, p. 691, May 2020.

[18] F. Pérez-González, C. Mosquera, M. Barni, and A. Abrardo, "Rational dither modulation: A high-rate data-hiding method invariant to gain attacks," *IEEE Transactions on Signal Processing*, vol. 53, no. 10, pp. 3960–3975, Oct. 2005.

[19] F. Zeng, H. Bai, and K. Xiao, "Blind watermarking algorithm combining NSCT, DWT, SVD, and HVS," *Security and Privacy*, vol. 5, no. 4, p. e223, 2022.

[20] D. Verma, A. K. Aggarwal, and H. Agarwal, "Watermarking scheme based on singular value decomposition and homomorphic transform," *AIP Conference Proceedings*, vol. 1836, p. 020036, 2017.

[21] J. J. Eggers and B. Girod, "Quantization watermarking," *EURASIP Journal on Advances in Signal Processing*, vol. 2002, no. 2, pp. 176–189, 2002.

[22] R. Sun, H. Sun, and T. Yao, "A SVD- and quantization-based semi-fragile watermarking technique for image authentication," in *Proc. IEEE ICSP*, 2002, pp. 1952–1955.

[23] M. Kutter and F. A. P. Petitcolas, "A fair benchmark for image watermarking systems," in *Proc. SPIE Security and Watermarking of Multimedia Contents*, vol. 3657, 1999, pp. 226–239.

[24] X. Zheng, Y. Zhou, and H. Wang, "A robust image watermarking scheme based on NSCT, DWT, and SVD," *Multimedia Tools and Applications*, 2019.

[25] USC-SIPI Image Database, University of Southern California, Signal and Image Processing Institute. [Online]. Available: `https://sipi.usc.edu/database/`

[26] K. J. Giri, S. M. K. Quadri, R. Bashir, and J. I. Bhat, "DWT based color image watermarking: A review," *Multimedia Tools and Applications*, vol. 79, pp. 32881–32905, 2020.

[27] M. A. Akhaee, S. M. E. Sahraeian, and F. Marvasti, "Contourlet-based image watermarking using optimum detector in a noisy environment," *IEEE Transactions on Image Processing*, vol. 19, no. 4, pp. 967–980, Apr. 2010.

[28] A. Nikolaidis and I. Pitas, "Robust image watermarking in the spatial domain," *Signal Processing*, vol. 66, no. 3, pp. 385–403, May 1998.

[29] N. N. Hurrah, S. A. Parah, N. A. Loan, J. A. Sheikh, M. Elhoseny, and K. Muhammad, "Dual watermarking framework for privacy protection and content authentication of multimedia," *Future Generation Computer Systems*, vol. 94, pp. 654–673, May 2019.

[30] F. A. P. Petitcolas, R. J. Anderson, and M. G. Kuhn, "Attacks on copyright marking systems," in *Proc. 2nd Int. Workshop on Information Hiding*, vol. 1525, pp. 218–238, 1998.

[31] M. Barni, F. Bartolini, and A. Piva, "Improved wavelet-based watermarking through pixel-wise masking," *IEEE Transactions on Image Processing*, vol. 10, no. 5, pp. 783–791, May 2001.

[32] R. C. Gonzalez and R. E. Woods, *Digital Image Processing*, 4th ed. New York, NY: Pearson, 2018.

[33] S. Voloshynovskiy, S. Pereira, T. Pun, J. J. Eggers, and J. K. Su, "Attacks on digital watermarks: Classification, estimation-based attacks, and benchmarks," *IEEE Communications Magazine*, vol. 39, no. 8, pp. 118–126, Aug. 2001.

[34] G. H. Golub and C. F. Van Loan, *Matrix Computations*, 4th ed. Baltimore, MD: Johns Hopkins University Press, 2013.

[35] K. Solanki, N. Jacobsen, U. Madhow, B. S. Manjunath, and S. Chandrasekaran, "Robust image-adaptive data hiding using erasure and error correction," *IEEE Transactions on Image Processing*, vol. 13, no. 12, pp. 1627–1639, Dec. 2004.

[36] S. Craver, N. Memon, B.-L. Yeo, and M. M. Yeung, "Resolving rightful ownerships with invisible watermarking techniques: Limitations, attacks, and implications," *IEEE Journal on Selected Areas in Communications*, vol. 16, no. 4, pp. 573–586, May 1998.

[37] H. S. Malvar and D. A. F. Florêncio, "Improved spread spectrum: A new modulation technique for robust watermarking," *IEEE Transactions on Signal Processing*, vol. 51, no. 4, pp. 898–905, Apr. 2003.

[38] A. Sverdlov, S. Dexter, and A. M. Eskicioglu, "Robust DCT-SVD domain image watermarking for copyright protection: Embedding data in all frequencies," in *Proc. 13th European Signal Processing Conference (EUSIPCO)*, 2005, pp. 1–4.

[39] Z. Wang and A. C. Bovik, "A universal image quality index," *IEEE Signal Processing Letters*, vol. 9, no. 3, pp. 81–84, Mar. 2002.

[40] A. Piva, M. Barni, F. Bartolini, and V. Cappellini, "DCT-based watermark recovering without resorting to the uncorrupted original image," in *Proc. IEEE ICIP*, vol. 1, pp. 520–523, 1997.

[41] S. A. Parah, J. A. Sheikh, N. A. Loan, and G. M. Bhat, "Robust and blind watermarking technique in DCT domain using inter-block coefficient differencing," *Digital Signal Processing*, vol. 53, pp. 11–24, Jun. 2016.

[42] A. V. Subramanyam, S. Emmanuel, and M. S. Kankanhalli, "Robust watermarking of compressed and encrypted JPEG2000 images," *IEEE Transactions on Multimedia*, vol. 14, no. 3, pp. 703–716, Jun. 2012.

[43] P. Tao and A. M. Eskicioglu, "A robust multiple watermarking scheme in the discrete wavelet transform domain," in *Proc. SPIE Internet Multimedia Management Systems V*, vol. 5601, pp. 133–144, 2004.

[44] M. A. Suhail and M. S. Obaidat, "Digital watermarking-based DCT and JPEG model," *IEEE Transactions on Instrumentation and Measurement*, vol. 52, no. 5, pp. 1640–1647, Oct. 2003.

[45] X. Qi and J. Qi, "A robust content-based digital image watermarking scheme," *Signal Processing*, vol. 87, no. 6, pp. 1264–1280, Jun. 2007.

[46] C. I. Podilchuk and E. J. Delp, "Digital watermarking: Algorithms and applications," *IEEE Signal Processing Magazine*, vol. 18, no. 4, pp. 33–46, Jul. 2001.

APPENDIX A
PYTHON IMPLEMENTATION

The complete Python implementation of the proposed blind SVD-QIM watermarking system is provided below. The code was developed and tested on Google Colaboratory using Python 3.x with NumPy, OpenCV, and Pillow [32, 34].

Note: Replace the host image and watermark file paths in the `files.upload()` calls before execution. The random seed is fixed to `12345` throughout for full reproducibility.

```
import io, math, time
import numpy as np
import pandas as pd
from PIL import Image, ImageOps, ImageFilter
from google.colab import files
import cv2
import matplotlib.pyplot as plt

np.random.seed(12345)
IMAGE_SIZE = (512, 512)
QIM_DELTA  = 5

def to_float255(data):
    im  = Image.open(io.BytesIO(data)).convert("L")
    im  = im.resize(IMAGE_SIZE, Image.BICUBIC)
    arr = np.array(im, dtype=np.float64)
    return np.clip(arr, 0, 255)

def svd_dec(img):
    return np.linalg.svd(img, full_matrices=True)

def diagS(s, M, N):
    S = np.zeros((M, N))
    k = min(M, N)
    S[:k, :k] = np.diag(s[:k])
    return S

def mojette_forward_1d(vec):
    return [vec.copy()], None

def mojette_inverse_1d(bins_list):
    return np.mean(bins_list, axis=0)
```

Listing A.1: Imports, configuration, and utility functions.

```python
def qim_embed(value, bit, delta=QIM_DELTA):
    c = delta * np.round(value / delta)
    return c + (delta / 2 if bit == 1 else 0)

def qim_extract(value, delta=QIM_DELTA):
    q = int(np.round(value / delta))
    return q & 1

def make_512_bits(wm_img):
    w   = Image.fromarray(wm_img.astype(np.uint8)).resize(
              (32, 16), Image.BICUBIC)
    arr = np.array(w, float)
    thr = arr.mean()
    return (arr > thr).astype(int).flatten()

def embed_bits_into_s(s, bits):
    s_mod = s.copy()
    for idx in range(512):
        BI, _ = mojette_forward_1d(np.array([s[idx]]))
        s_mod[idx] = qim_embed(BI[0][0], bits[idx])
    return s_mod

def extract_bits_from_s(s_wi):
    bits = []
    for i in range(512):
        BI, _ = mojette_forward_1d(np.array([s_wi[i]]))
        bits.append(qim_extract(BI[0][0]))
    return np.array(bits, int)

def reconstruct_singular_values(bits, s_w_orig, s_wi):
    s_est = np.zeros_like(s_w_orig)
    for idx in range(512):
        val = s_wi[idx]
        c   = QIM_DELTA * np.round(val / QIM_DELTA)
        if bits[idx] == 1:
            c += QIM_DELTA / 2
        s_est[idx] = c
    gamma = np.linalg.norm(s_w_orig) / (
                np.linalg.norm(s_est) + 1e-9)
    return s_est * gamma
```

Listing A.2: Scalar QIM embedding and extraction functions.

```python
def gaussian_noise(img, sigma=10):
    n = np.random.normal(0, sigma, img.shape)
    return np.clip(img + n, 0, 255)

def salt_pepper(img, prob=0.05):
    noisy = img.copy()
    rnd   = np.random.rand(*img.shape)
    noisy[rnd < prob/2]                   = 0
```

```
    noisy[(rnd >= prob/2) & (rnd < prob)] = 255
    return noisy

def speckle_noise(img):
    noise = np.random.randn(*img.shape)
    return np.clip(img + img * noise * 0.1, 0, 255)

def median_filter(img):
    return cv2.medianBlur(img.astype(np.uint8), 3).astype(float)

def mean_filter(img):
    return cv2.blur(img.astype(np.uint8), (3, 3)).astype(float)

def gaussian_blur(img):
    return cv2.GaussianBlur(
        img.astype(np.uint8), (3, 3), 1).astype(float)

def jpeg_compress(img, q):
    pil = Image.fromarray(img.astype(np.uint8))
    buf = io.BytesIO()
    pil.save(buf, format='JPEG', quality=q)
    buf.seek(0)
    return np.array(Image.open(buf), float)

def rotate_5deg(img):
    pil = Image.fromarray(img.astype(np.uint8))
    rot = pil.rotate(5, resample=Image.BICUBIC)
    return np.array(rot, float)

def crop_10(img):
    h, w   = img.shape
    ch, cw = int(h * 0.1), int(w * 0.1)
    cropped = img[ch:h-ch, cw:w-cw]
    return cv2.resize(cropped, (512, 512))

def hist_eq(img):
    pil = Image.fromarray(img.astype(np.uint8))
    eq  = ImageOps.equalize(pil)
    return np.array(eq, float)

ATTACKS = {
    "GaussianNoise" : lambda x: gaussian_noise(x, sigma=10),
    "SaltPepper"    : lambda x: salt_pepper(x, prob=0.05),
    "Speckle"       : lambda x: speckle_noise(x),
    "MedianFilter"  : median_filter,
    "MeanFilter"    : mean_filter,
    "GaussianBlur"  : gaussian_blur,
    "JPEG_90"       : lambda x: jpeg_compress(x, 90),
    "JPEG_70"       : lambda x: jpeg_compress(x, 70),
    "JPEG_50"       : lambda x: jpeg_compress(x, 50),
    "Rotate_5deg"   : rotate_5deg,
    "Crop_10"       : crop_10,
    "HistEq"        : hist_eq,
```

```
}
```

Listing A.3: Attack simulation functions.

```
print("\n=== Upload HOST Images ===")
host_up    = files.upload()
host_files = list(host_up.items())

print("\n=== Upload WATERMARK Image ===")
wm_up              = files.upload()
wm_name, wm_bytes = list(wm_up.items())[0]

watermark = to_float255(wm_bytes)
wm_bits   = make_512_bits(watermark)
rows      = []

for fname, data in host_files:
    host        = to_float255(data)
    Uc, sc, Vtc = svd_dec(host)
    Uw, sw, Vtw = svd_dec(watermark)

    sc_mod = embed_bits_into_s(sc, wm_bits)
    WI     = Uc @ diagS(sc_mod, 512, 512) @ Vtc
    WI     = np.clip(WI, 0, 255)

    plt.figure(figsize=(12, 4))
    plt.subplot(1, 3, 1); plt.imshow(host, cmap='gray')
    plt.title("Host Image")
    plt.subplot(1, 3, 2); plt.imshow(WI, cmap='gray')
    plt.title("Watermarked Image")
    plt.subplot(1, 3, 3); plt.imshow(watermark, cmap='gray')
    plt.title("Original Watermark")
    plt.show()

    Image.fromarray(WI.astype(np.uint8)).save(f"WM_{fname}.png")

    base_mse  = np.mean((host - WI)**2)
    base_psnr = 10 * np.log10((255**2) / (base_mse + 1e-9))
    print(f"\nHost: {fname} | Base PSNR = {base_psnr:.2f} dB\n")

    for atk_name, atk_fn in ATTACKS.items():
        attacked       = atk_fn(WI)
        Uwi, swi, Vtwi = svd_dec(attacked)
        bits_ext       = extract_bits_from_s(swi)
        s_we           = reconstruct_singular_values(
                             bits_ext, sw, swi)
        WE             = Uw @ diagS(s_we, 512, 512) @ Vtw

        a   = watermark - watermark.mean()
        b   = WE - WE.mean()
        ncc = np.sum(a * b) / (
                  np.sqrt(np.sum(a*a) * np.sum(b*b)) + 1e-9)
```

```python

        rows.append([fname, atk_name, base_psnr, ncc])
        print(f"[{fname}] Attack={atk_name} "
              f"-> PSNR={base_psnr:.2f}, NCC={ncc:.4f}")

    plt.figure(figsize=(6, 4))
    plt.imshow(WE, cmap='gray')
    plt.title(f"Extracted Watermark ({fname})")
    plt.show()

    Image.fromarray(
        np.clip(WE, 0, 255).astype(np.uint8)
    ).save(f"EXTRACTED_{fname}.png")

df = pd.DataFrame(rows, columns=["Host","Attack","PSNR","NCC"])
df.to_csv("attack_results.csv", index=False)
print("\nSaved attack_results.csv and all images.")
```

Listing A.4: Main watermarking, attack, and evaluation pipeline.