ENHANCED WATERMARKING TECHNIQUES USING SOFT COMPUTING

A DISSERTATION

SUBMITTED IN PARTIAL FULFILLMENT OF THE REQUIREMENTS
FOR THE AWARD OF THE DEGREE
OF

MASTER OF TECHNOLOGY
IN
COMPUTER SCIENCE AND ENGINEERING

Submitted by

AYUSH SAINI (23/CSE/26)

Under the supervision of

Dr. NIPUN BANSAL

DEPARTMENT NAME
DELHI TECHNOLOGICAL UNIVERSITY
(Formerly Delhi College of Engineering)
Bawana Road, Delhi 110042

MAY, 2025

DEPARTMENT OF COMPUTER SCIENCE AND ENGINEERING
DELHI TECHNOLOGICAL UNIVERSITY
(Formerly Delhi College of Engineering)
Bawana Road, Delhi-110042

CANDIDATE'S DECLARATION

I, **AYUSH SAINI**, Roll Number – **23/CSE/26** students of M.Tech **Computer Science and Engineering**, hereby declare that the project Dissertation titled "**Enhanced Watermarking Techniques Using Soft Computing**" which is submitted by me to the **Computer Science and Engineering**, Delhi Technological University, Delhi in partial fulfilment of the requirement for the award of degree of Master of Technology, is original and not copied from any source without proper citation. This work has not previously formed the basis for the award of any Degree, Diploma Associateship, Fellowship or other similar title or recognition.

Place: Delhi Ayush Saini

Date: 30/05/2025

DEPARTMENT OF MECHANICAL ENGINEERING
DELHI TECHNOLOGICAL UNIVERSITY
(Formerly Delhi College of Engineering)
Bawana Road, Delhi-110042

CERTIFICATE

I hereby certify that the Project Dissertation titled "**Enhanced Watermarking Techniques using Soft Computing**" which is submitted by **Ayush Saini**, Roll Number – **23/CSE/26**, **Computer Science and Engineering** , Delhi Technological University, Delhi in partial fulfilment of the requirement for the award of the degree of Master of Technology, is a record of the project work carried out by the students under my supervision. To the best of my knowledge this work has not been submitted in part or full for any Degree or Diploma to this University or elsewhere.

Place: Delhi	**Dr. Nipun Bansal**
Date: 30/05/2025	**SUPERVISOR**

DEPARTMENT OF MECHANICAL ENGINEERING
DELHI TECHNOLOGICAL UNIVERSITY
(Formerly Delhi College of Engineering)
Bawana Road, Delhi-110042

ACKNOWLEDGEMENT

I wish to express my sincerest gratitude to **Dr. Nipun Bansal** for his continuous guidance and mentorship that he provided me during the project. He 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. He was always ready to help me and clear my doubts regarding any hurdles in this project. Without his constant support and motivation, this project would not have been successful.

Place: Delhi Ayush Saini

Date: 30/05/2025

Abstract

Currently for the last ten years the research of stong digital watermarking methods is extremely important and has become popular, partly because of the large amount of data transmitted online and also the growing threats to the authenticity, confidentiality, and integrity of digital media. With the large number of malicious attacks, including noise addition, geometric-distortions, compression and many forms of tampering, digital data is more susceptible than ever. Because of this, there is a need for efficient, robust, and smart watermarking methods to get digital data secure during transmission.

To address the need to grow challenges, this study develops a new watermarking method designed to protect digital images. The suggested scheme utilizes the hybrid functions of (1)Discrete Wavelet Transform (DWT) and (2)Singular Value Decomposition (SVD) as well as an optimization tool called Artificial Bee Colony (ABC) algorithm. The reason to use the ABC algorithm is that it mimics the intelligent foraging behavior of honey bee swarms and it dynamically varies the scaling factors of (1) DWT and/or (2) SVD in embedding the watermark, thus optimizing both imperceptibility and robustness for the watermarked images. In using a hybrid DWT-SVD framework by embedding the watermark into transformed domains, the watermark is less imperceptible to the human visual system. In combination, while SVD provides the numerical stability of the watermarked images, DWT enables the resistance of image distortions.

To conclude, the watermarking system created in this research study offers robust and scaleable protection for digital image content. It has a better performance profile, which is important for us or other users of our system, and it satisfies some DRM requirements. Therefore, this system is a viable option for real-world scenarios which require secure digital content authentication, ownership protection, and copyright management capabilities(Sharma et al., 2021)[1].

Contents

Candidate's Declaration **i**

Certificate **ii**

Acknowledgement **iii**

Abstract **iv**

Content **vi**

List of Tables **vii**

List of Figures **viii**

List of Symbols, Abbreviations **ix**

1 INTRODUCTION **1**
1.1 Overview 1
1.2 Problem Statement 3

2 Literature Review **5**
2.1 Overview of Digital Watermarking 5
2.2 Watermarking Techniques and Approaches 5
2.3 Hybrid Domain Watermarking 6
2.4 Role of Optimization in Watermarking 6
2.5 Artificial Bee Colony Algorithm in Watermarking 7
2.6 Research Gaps 8
2.7 Summary 8

3 Proposed Methodology **9**
3.1 Overview of the Proposed Scheme 9
3.2 Watermark Embedding Process 9
3.3 Watermark Extraction Process 11
3.4 Artificial Bee Colony Algorithm for Optimization 12
3.5 Summary 14

4 RESULTS and DISCUSSION **15**
4.1 Results 15
4.1.1 SSF and MSF's Effect on Visual Quality 15
4.1.2 Effects of SSF and MSF on the Watermarking Scheme's Robustness 18
4.2 Robustness Analysis 22

4.3 Input and Output Images 24
4.3.1 Input Images 24
4.3.2 Output Images 24
4.4 Result Analysis 25
4.4.1 Imperceptibility Analysis 25
4.4.2 Robustness Analysis 25
4.4.3 Comparative Analysis 26

5 Conclusion **27**

A **29**
A.1 Parameter Tuning Strategy for ABC Algorithms 29
A.2 Images Used 29
A.3 Watermark Details 29

List of Tables

4.1 *The suggested approach and current methods are compared in terms of the PSNR and NC values of signed images.* 16

4.2 *Compilation of PSNR and NC values for four additional signed images* . 17

4.3 Comparison of SSF and MSF Under Various Attacks for Different Images 20

4.4 *Comparison of SSF and MSF Under Various Attacks for Different Images* . 21

List of Figures

3.1 *Watermark Embedding Flow Diagram* 11
3.2 *Watermark Extraction Flow Diagram* 12

4.1 *Better image quality preservation is indicated by ABC(MSF)'s consistent higher PSNR compared to ABC(SSF) and other techniques.* 17
4.2 *The bar graph demonstrates that ABC(MSF) performs better in PSNR than ABC(SSF), suggesting improved image quality retention.* 18
4.3 *Test images used in the experiment.* 24
4.4 *Watermarked images as an output.* 24

List of Symbols

r	Radius, m
α	Angle of thesis in degrees
β	Flight path in degrees

Chapter 1

INTRODUCTION

1.1 Overview

In today's technological ecosystems that are changing rapidly, the speed and volume of data that is exchanged and transferred across global networks have increased considerably more than in the past. The emergence of rapid data exchange has raised vital and significant privacy, integrity, and ownership challenges. As digital content moves across media, the risks associated with unauthorized access, manipulation, and redistribution are ever increasing, not least in social media and cloud services environments. There are increasing examples of these issues through studies and reporting such as the reports from the European Union Agency for Cybersecurity (ENISA.2023)[2] and the unconditional peer-reviewed work published in the Journal of Cybersecurity (Smith et al., 2021)[3] referencing the vulnerabilities inherent in data exchange at large scales in digital ecosystems. digital watermarking is one of the most successful and studied approaches to mitigate risks to ownership, piracy, and copyright infringement. digital watermarking is a form of embedding data, most usually related to ownership or copyright information, within digital media. The data can be extracted from the digital media and verified for authenticity and ownership even after extensive processing or transmitting of the media.

Digital watermarking can be classified in a number of ways, but one broad distinction can be made according to the watermark's visibility. Visible watermarking encodes the information in a manner that is easy to notice, such as by using a logo or text overlay with some degree of transparency. An invisible watermark encodes the watermark in the content itself so that it doesn't visually impact the image or video after the watermark is applied. This form of watermarking is quite useful for copyright enforcement and protecting intellectual property rights because it allows copyright holders to retain the appearance of the content in its original state while still embedding actual evidence of ownership (Cox et al., 1997)[4].

Many watermarking schemes are evaluated by two primary performance metrics: robustness and imperceptibility. Imperceptibility refers to the visual quality of the watermarked media; that is, the watermark is intended to cause no noticeable distortion, or distortion such that the watermark is undetectable. Robustness is the measure of the watermark, and how resilient it is against attacks or manipulations, e.g., noise addition, cropping, rotation, compression, filtering. These metrics are typically in conflict, as increasing robustness often comes at the expense of imperceptibility, and vice versa.This trade-off makes watermarking a fundamental optimization question, which often requires complex methods to balance two opposing goals. Foundational publications like Cox et al. (2002)[5] and Barni and Bartolini (2004)[6] have provided grand descriptions of these trade-offs with many proposals to tackle the problem.

Watermarking methodologies are classified into three categories in their initial taxonomy: Fragile, Robust and Semi-fragile. Robust methods are specifically designed to protect the watermark and ensure that the watermark will not get removed with extensive image processing and deliberate attacks. Robust methods are typically used in copyright protection. In contrast implementations, fragile watermarking is extremely sensitive to changes and is used to determine the integrity of the content—any change, however slight, will destroy the watermark, effectively notifying unauthorized intrusion. Semi-fragile watermarking is an intermediate approach, where it can tolerate some benign changes (such as compression), but can also distinguish between authorized and unauthorized changes, which is where it competes most closely with acceptable implementations of fragile watermarking for content authentication.

The spatial domain and the transform domain are the two main areas in which digital watermarking techniques function. In order to embed the watermark, spatial domain techniques directly modify the host image's pixels. These techniques tend to be less resilient to common image processing operations, despite being simpler and more computationally efficient overall. Conversely, transform domain techniques use mathematical transforms like Discrete Fourier Transform (DFT), Discrete Cosine Transform (DCT), and Discrete Wavelet Transform (DWT) to embed watermark data in the host image's frequency coefficients. Because of their frequency-domain embedding, which is less vulnerable to simple manipulations, these techniques typically provide increased robustness (Hernandez et al., 2000)[7]. Among these, DWT has become a popular method because of its ability to analyze data at multiple resolutions, which enables watermark embedding to be effectively localized in both the spatial and frequency domains (Dawei et al., 2004)[8].

In addition to DWT, Singular Value Decomposition (SVD) has shown to be another useful mathematical tool for image watermarking. SVD allows the separation of an image matrix into singular values that can be selectively modified without significantly impacting perceptual quality. When DWT and SVD are used in conjunction, they enhance watermark embedding performance by leveraging the spatial-frequency localization of DWT and the numerical stability of SVD. This hybrid method has been shown to improve both robustness and imperceptibility, as demonstrated in several studies including Liu and Tan (2002)[9] and Loukhaoukha et al. (2014)[10].

Watermarking is continuing to grow and entails new methods designed to approach the optimization problems involved in the watermark embedding process, using nature-inspired optimization algorithms to provide indirect solutions. Various watermarking schemes have been augmented using intelligent algorithms such as Genetic Algorithms (GA), Ant Colony Optimization (ACO), Cuckoo Search Algorithm, and the Artificial Bee Colony (ABC). These algorithms mimic various biological or natural behaviors in the search for the optimal embedding parameters (e.g., scaling factors) from high-dimensional problem solution spaces (Agarwal et al., 2014[11]; Mishra et al., 2016[12]).

Among these algorithms, the Artificial Bee Colony (ABC) algorithm is notable for its ease of use, adaptability, and efficiency in solving numerical optimization problems. ABC simulates food source exploration and exploitation over a solution space. For watermarking, ABC is used to increase the embedding strength as indicated by a scaling factor that minimizes the error between the original and watermarked image while maintaining image quality and robustness against various attacks. ABC modifies the watermark embedding operations to achieve imperceptibility and robustness against attacks by responding to the structural and statistical properties of the host image (Mishra et al., 2014[13]).

In this thesis, I present a new hybrid digital image watermarking method which contains DWT, SVD, and the ABC optimization algorithm. The proposed scheme has a watermark embedding phase that can use either **single-scaling-factors (SSF) or multiple-scaling-factors (MSF)**. After embedding into color or grayscale images, the watermark is verified via some standard image processing attacks. The performance is quantified by objective function, which incorporates **Peak-Signal-to-Noise-Ratio (PSNR)** for image quality and **Normalized Corre- lation (NC)** for watermark validity after attack. The experimental results prove the proposed method has a solid watermarking solution, which carefully balances high imperceptibility and strong resilience to distortion.

1.2 Problem Statement

The unprecedented rise in digital communication technologies has also given rise to rapid growth in multimedia—especially digital images—being shared over open, insecure networks. While this new technology has increased the ease and availability for sharing information, it has also introduced new critical issues regarding the security of content, ownership verification and copyright protection. As we become more dependent on online platforms for the distribution of valuable digital content, we are becoming more exposed to unauthorized access, illegal redistribution, and tampering with multimedia data. These challenges present a need for effective methods that not only provide protection for digital content but also provide reliable and scalable characterizations of established and protected intellectual property rights.

Digital watermarking is one of many security mechanisms. However, it is an efficient and viable way to hide ownership information within digital content. In this form of digital right management, the original image will embed information that will identify copyright ownership, which can be extracted or detected at a later time. There are two opposing requirements that must be satisfied in watermarking scenarios, namely the watermarking scheme must be imperceptible to avoid distortion of the image; and the watermark must also be robust, which guarantees that the watermark remains recoverable after common attacks such as compression, resizing, cropping, noise, or filtering in an image.

However, balancing these two opposing objectives is inherently difficult, and poses a **multi-objective optimization problem**. Existing watermarking approaches often make trade-offs between imperceptibility and robustness. In spatial domain watermarking, where pixel values are directly modified, the schemes are computationally simple but highly vulnerable to common image processing attacks. Transform domain techniques—such as DCT, DFT, and DWT —provide better robustness, since the frequency domain contains the watermark, making it less susceptible to direct tampering. Among these, DWT stands out for its ability to perform multi-resolution analysis, which allows selective embedding of watermark data in perceptually less significant regions of the image.

Besides DWT, **Singular Value Decomposition (SVD)** has also gained popularity in the watermarking area as it is able to decompose an image into components exhibiting various energy characteristics. Watermarking the singular values of an image will allow a greater resistance to distortions compared to DWT and also will remain visually similar to the original image. However, even using a method like DWT with SVD creates limitation if the rules that control the selection of embedding parameters, specifically in the use of **scaling factors**, are poor. Poor embedding parameterization, either by making choices through trial and error or using arbitrary fixed values, may yield undesirable results, either making the watermark too difficult to detect or creating permanent artifacts in the host image.

In an attempt to address these limitations, recent studies have determined the potential of natural-**inspired optimization algorithms** for optimizing the watermark embedding process. Certain methods such as Genetic Algorithms (GA), Particle-Swarm-Optimization (PSO), and Artificial Bee Colony (ABC) algorithms have been proposed that would automatically find appropriate embedding parameters for usage. Of the three methods, the **ABC algorithm** has a potential advantage over the others, as it has a balanced exploration and exploitation operation structure, and as well is modeled after the foraging process of bee colonies. By way of applying the ABC in order to optimize the scaling factors, the watermark's embedding strength can also dynamically modified based on the image properties, thus minimally contribute to imperceptibility and enhancing robustness without human parameters being established. Nevertheless, there still exists on the issuing side, a void that is currently not filled with a comprehensive watermarking framework, one that effectively will provide synergy utilizing **DWT, and SVD**, as well as the **ABC optimization**, while allowing flexibility by using **single and multiple scaling factors** in the embedding process. Furthermore, many of the studies conducted do not operate toward a sufficient evaluation against various image processing and geometric attacks, in conjunction to insufficiently benchmarking processes due to using different evaluation methods that are inconsistent with one another across the black-and-white and color images datasets.

Therefore, the central challenge being investigated in this work is the **absence of a rigorous, flexible, and thoroughly optimized watermarking system** that provides a workable trade-off between distortion of the carrying image and resiliency of a watermark. From this, we derive the following research question:

"How can we develop a hybrid watermarking system that integrates Discrete Wavelet Transform (DWT), SVD, and ABC optimization to achieve high imperceptibility and resiliency for both grayscale and color images using scalable embedding methods, while sustaining performance across a wide range of image processing attacks?"

In order to answer this question, the project proposes the development of an optimized watermarking system where the ABC algorithm is used to optimize the embedding parameters within the DWT-SVD system. By means of embedding parameters optimization via ABC, we look to mitigate the challenges described above by achieving:

* Minimal perceptible distortion of watermarked images (high PSNR and SSIM),

* A high level of resilience against commonly observed attacks (high NC values post attack),

* Scalability to grayscale and color formats,

* Flexibility through support for both Single-Scaling-Factor (SSF) and Multiple-Scaling-Factor (MSF) methods

By tackling these objectives, this research aims to contribute a novel and effective solution for the secure and reliable embedding of ownership information in digital images—one that meets current demands for media authentication, copyright enforcement, and content integrity in the digital age.

Chapter 2

Literature Review

2.1 Overview of Digital Watermarking

Watermarking approaches can be subdivided into two categories; spatial or transform domain approaches. Spatial domain methods modify the pixel values themselves of the image (for example, Least Significant Bit (LSB) embedding). Spatial domain approaches are easy to implement and computationally simple, but are weak against any sort of attacks or transformations to the images such as filtering, noise addition, and compression. For example, Koch and Zhao (1995)[14], performed watermarking by modifying the LSB of the pixels, but because it was attacked the applications of LSB in a secure watermarking scenario are limited.

In the last several decades, watermarking techniques have been developed, each trying to obtain a balance between three key parameters: imperceptibility, robustness, and capacity. Imperceptibility means that the watermark cannot affect the perceived quality of the host media. Robustness is the extent to which the watermark can withstand various forms of image processing (common or otherwise) as well as possible attacks. Capacity means the amount of information that can be reliably embedded without destroying or affecting imperceptibility and robustness. A variety of methods have been tested using very simple spatial domain methods to more complex and less simple transform domain methods as well as hybrid methods to achieve the aim of watermarking.

2.2 Watermarking Techniques and Approaches

Watermarking methods can be grouped into two broad classes: spatial and transform domain. Spatial domain methods such as Least Significant Bit (LSB) embedding, usually modify pixel values directly. These methods may be simple to implement computationally, but they are very sensitive to numerous attacks as well as transformations such as lossy compression, filtering, and noise addition. For example, an early work by Koch and Zhao (1995) [14] employed the LSB method for watermark embedding, though the lack of robustness led to limited use of the method for secure watermarking.

On the other hand, transform domain methods possess higher robustness and imperceptibility. This method is done by transforming the original image to another domain, embedding the watermark, and then using the inverse transform to obtain the watermarked image. DCT, DFT, and DWT can all be used as transforms. Each transform has its advantages. DCT is effective against JPEG compression because it can compact energy. DFT is robust against geometric distortions (rotation, scaling, etc. . .), but it is more computationally costly. DWT has taken a front role because it can perform multi-resolution analysis, which is ideal for embedding imperceptible but robust watermarks.

SVD has been applied widely in watermarking partly because of its numerical stability and invariance to changes. SVD separates an image into singular vectors and singular values, which can then be modified to insert the watermark. SVD, alone or with other transforms, has been shown to be robust against a wide variety of signal processing attacks.

2.3 Hybrid Domain Watermarking

In recent years, hybrid domain watermarking has received a lot of interest because it is able to share the strengths of different transforms, and in doing so improves robustness and enhanced perceptibility. One such approach that has been successful is a combination of DWT and SVD, which has gained traction in the field of digital image watermarking. DWT compresses the image, provides multi-resolution analysis and affords the watermarking by inserting it into specific frequencies or coarser resolution; this generally provides better resistance to common signal processing attacks such as compression and noise (Barni et al., 2001)[15]. SVD takes the image matrix and determines the singular values and singular vectors. SVD gives us stability against geometric and filtering attacks because small changes made to the image generally give small changes in the singular values (Liu & Tan, 2002)[16].

Hybrid DWT-SVD watermarking takes advantage of both the spatial-frequency localization of wavelets and the numerical robustness of singular values in order to achieve a compromise that ensures the watermark is imperceptible (to the human eye) and is resistant to attacks (Mishra et al., 2014)[13]. Other researchers have studied hybridizing DWT with other transforms such as Discrete Cosine Transform (DCT) and Discrete Fourier Transform (DFT), in order to capture the advantages of the frequency domain in addition to the wavelet domain properties (Dawei et al., 2004)[8]. In general, hybrid approaches provide improved performance as determined by Peak Signal-to-Noise Ratio (PSNR) and Normalized Correlation (NC) over single domain methods (Cox et al., 2002)[5].

Although hybrid watermarking systems have their advantages, there are challenges associated with the design of these systems. The process of choosing which sub-bands to embed, computational complexity, and the trade-off between robustness and imperceptibility is important. Additionally, hybrid techniques are often strongly related to the optimized process of embedding and extracting, which results in the significance of the optimization algorithm in this area (Agarwal et al., 2014)[11].

2.4 Role of Optimization in Watermarking

Optimization is a key aspect of digital watermarking, especially when trying to achieve conflicting goals which is a union of watermark invisibility and robustness to attacks. The watermark embedding process uses either scaling factors or embedding strengths which convey how strongly the watermark has been embedded in the host image. If the parameters are too low then the watermark is weak and can be easily destroyed by normal image operations. If the parameters are too high then the watermark is overly visible and degrades the quality and acceptability of the watermarked image.

To balance all these competing objectives, various bio-inspired and heuristic optimization algorithms have already been applied extensively. Genetic Algorithms (GA) imitate natural selection, rewarding minor variations for improving optimal parameters over successive generations, based on fitness functions that are tied to image quality and watermark retrieval (Tan, 2002)[9]. Particle Swarm Optimization (PSO) imitates the social predilection of a flock or school of animals, and achieves a degree of ”collaborative” search of the parameter space, because each candidate solution is adjusted based on social influence and individual learning (Eberhart & Kennedy, 1995)[17].

The Artificial Bee Colony (ABC) algorithm has been gaining popularity recently, in part because of the ABC's simple yet competent mechanism that can manage both exploration and exploitation, best known as an optimization algorithm (Karaboga, 2005)[18]. Based on honey bee foraging behavior, it models search agents as employed bees, onlooker bees, and scout bees, thus contributing to the exploration of solutions and refinement of those solutions. The approach has been able to optimize watermark embedding parameters with a hybrid scheme, like DWT-SVD, based on empirical evidence that showed improvements in imperceptibility and robustness without the excessive cost of computation (Agarwal et al., 2014[11]; Mishra et al., 2016[12]).

While the advances are encouraging, there are also issues on the horizon. For example, it has also been shown in optimization algorithms that performance can differ widely on algorithm parameters, such as population size, iteration limit, and convergence criteria. Also, many studies only optimize for a limited attack model, or focus exclusively on grayscale images, leaving open questions about transferability into color images and diverse attack models. There is work ahead to design adaptive or hybrid optimization schemes to increase robustness for watermark embedding into a wider array of functionality.

In summary, optimization is just as much an underlying technique as it is a support technique, thus helping modern watermarking systems to be more viable under the even greater threats to digital content protection in complex, real-world environments.

2.5 Artificial Bee Colony Algorithm in Watermarking

The Artificial Bee Colony (ABC) algorithm is one of the more accessible algorithms to use, coupled with being a solid global search algorithm. The ABC algorithm is based on honey bee swarm foraging behavior and consists of three types of bees, employed bees, onlooker bees, and scout bees, which allows it to both explore and exploit the solution space (Karaboga, 2005)[18]. Employed bees explore new solutions based on their knowledge, onlooker bees are able to evaluate visible knowledge from the employed bees and select a part of the solution space to focus on, and scout bees contribute diversity to the population by randomly exploring a new solution space (Karaboga & Basturk, 2007)[19].

Within a digital watermarking context, the ABC algorithm has been very beneficial at optimizing the scaling factor which is used to embed the watermark, where the fitness function often combines Peak Signal-to-Noise Ratio and Normalized Correlation to ensure visual quality and watermark robustness (Agarwal et al., 2014[11]; Mishra et al., 2016[12]). Recent work applying the ABC algorithm in a DWT-SVD framework has noted improvements to the watermarked images' overall quality and resistance to various attacks, thus demonstrating practical application of the algorithm (Mishra et al., 2016)[12].

However, ABC still has a number of drawbacks, as it can be sensitive to parameter settings such as the number of bees and limit for abandoning poor solutions. Some examples of developments have included new models that have been described as either adaptive or hybrid that could further improve ABC in watermarking (Singh et al., 2019)[20].

2.6 Research Gaps

Although significant advancements have been made in the development of effective and undetectable watermarking methods, there are still numerous shortcomings in the current literature. For example, most of the proposed methods are designed and evaluated based on grayscale images; however, in practice the majority of images are color, which limits the ability to use these methods in practical color image watermarking applications. In addition, most optimization-based approaches utilize a single global scaling factor for image embedding, while it may be advantageous to utilize multiple adaptive scaling factors that better exploit the image characteristics of specific regions or sub-bands.

One of the other substantial shortcomings in this area is the limited testing of watermarking schemes using broader variations of attacks. For example, many methods are tested and proved to be effective under certain attacks, such as JPEG attacks, and various types of additive noise attacks, but the watermarking schemes are not tested under varying attacks or under additional enriched conditions. To add another layer of complexity, very few of the proposed approaches take a combined approach that optimizes for robustness and imperceptibility through a single framework or platform and fail to address the potential compromise of one approach over the other.

These limitations highlight the need for a more comprehensive, adaptable, and flexible watermarking approach. In closing, the route through incorporating a DWT and SVD, combined with a well-tuned ABC optimization algorithm, appears to be a promising possibility. This framework can modulate embedding parameters dynamically, which allows it to better meet the necessary implicit requirements by improving robustness and visual fidelity. This reasoning provides the foundational motivation for the work proposed in this thesis.

2.7 Summary

This chapter has comprehensively reviewed the significant techniques for digital watermarking, with an overall equal qualitative emphasis on the transform and hybrid domain cases. In addition to discussing the pros and cons of spatial, frequency, and hybrid (i.e., joined or dual-stage) methods, we have pointed out the critical importance of optimization methods on watermark embedding methods. The ABC algorithm is singled out because of its ability to balance exploration and exploitation in optimization tasks. Finally, the chapter concluded by proposing existing gaps in the literature and establishing a strong basis and rationale for the proposed watermarking method using DWT, SVD, and ABC that has been developed in this thesis.

Chapter 3

Proposed Methodology

This chapter has nature explained in detail the method developed for secure digital image watermarking using a hybrid iscrete Wavelet Transform (DWT), Singular Value Decomposition (SVD), and ABC algorithm optimization process. The goal of this work was to provide a secure, imperceptible and robust watermarking solution which can withstand conventional image processing and common geometric attacks. The scheme provides important requirements with respect to robustness, imperceptibility and efficiency.

3.1 Overview of the Proposed Scheme

The increasing demand for digital content protection requires intelligent and secure watermarking techniques. The purpose of this investigation is finally to utilize intelligent algorithms in the context of advanced signal processing in order to stand alone and maximize performance. A grayscale host picture of 512×512 pixels and a binary watermark image of 32×32 pixels were used.

The watermark embedding process consists of four primary steps; the conversion of the image into the frequency domain by utilizing the DWT, decomposition of the image and watermark using the SVD, optimization of the embedding strength using the ABC algorithm and finally reconstruction of the watermarked image. The watermark extraction process will be similarly structured but performed in reverse order with the purpose of retrieving the embedded watermark as accurately as possible with minimal distortion, both the host and watermark images will maintain perceived quality. The scheme as a whole ensures the watermark is imperceptible to the human eye and yet remained resilient to common forms of attack.

3.2 Watermark Embedding Process

Step 1: DWT Decomposition

The embedding procedure begins with a four-level Discrete Wavelet Transform (DWT) of the original host image. This transformation decomposes the image into distinct frequency sub-bands, such as LL (low-low), LH (low-high), HL (high-low), and HH (high-high), mapping out a set of characteristics at each level of decomposition. The LL4 sub-band is the lowest frequency level and carries low-frequency information that is the most useful because it reflects the overall structure and content of the image. The watermark is embedded in this sub-band because changes in this sub-band are typically less visible to the human eye and because the watermark held in this sub-band will be more resilient to common image processing attacks such as noise, compression, and filtering (Barni & Bartolini, 2004)[21].

Step 2: SVD Decomposition

Once the LL4 sub-band is isolated, the next step is to apply Singular Value Decomposition (SVD) on the sub-band matrix A . This is expressed as:

$$A = U \cdot S \cdot V^T$$

where U and V^T are orthogonal matrices that contain the left and right singular vectors respectively, and S is the diagonal matrix of singular values that represent the intrinsic characteristics of the image (e.g. luminance, color, and structural characteristics of the image). In the same way, the watermark image can be decomposed using SVD into singular values S_w. The singular values in the watermark contained all of the information that needed to be embedded and now that the watermark singular values can uniquely represent their own characteristics, the watermark can be embedded imperceptibly and robustly (Barni & Bartolini, 2004)[21].

Step 3: Optimization Using ABC Algorithm

One of the serious considerations of watermark embedding is how strongly to perform the embedding indicated by the scaling parameter α. This parameter needs to be optimal, as too low an α will make the watermark weak, and too large will reduce the image quality and make the watermark apparent. To find the most appropriate α, we will utilize the Artificial Bee Colony (ABC) algorithm. The ABC algorithm uses an intelligent foraging behavior found in honeybees to help us search the space for the optimal scale value that will maximize invisibility and robustness of the watermark(Karaboga, 2005[18]; Agarwal et al., 2014 [11]). Using this optimum α, the singular values of the LL4 sub-band are altered as follows:

$$S' = S + \alpha \cdot S_w$$

This formula adjusts the singular values by adding a scaled version of the watermark's singular values, effectively embedding the watermark into the host image's core features.

Step 4: Image Reconstruction

Once the singular values are altered, the completed LL4 sub-band, denoted as LL4', is reconstructed by multiplying the three matrices back together:

$$LL4' = U \cdot S' \cdot V^T$$

At this stage the Inverse Discrete Wavelet Transform (IDWT) is implemented. This process recombines the modified low-frequency LL4' sub-band back together with the original sub-bands of the host image high frequency (LH,HL,HH) to return the image to its original full resolution. The end result is an image that has been watermarked, which does not alter the host image from the human viewing experience in expected viewing but does embed the watermark for later detection or extraction. This is the embedding phase with the intent of embedding a watermark into the original image at a quality that could not visually impact the quality of the host image and keep robustness from attacks.

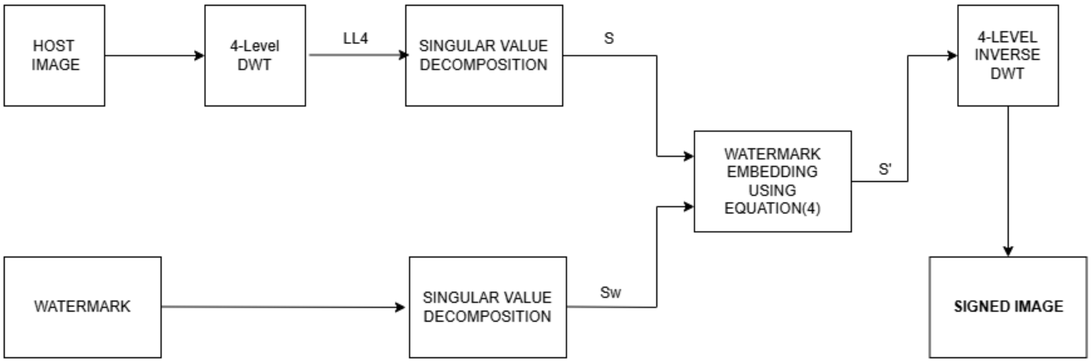

HOST IMAGE
4-Level DWT
LL4
SINGULAR VALUE DECOMPOSITION
S
WATERMARK EMBEDDING USING EQUATION(4)
S'
4-LEVEL INVERSE DWT
WATERMARK
SINGULAR VALUE DECOMPOSITION
Sw
SIGNED IMAGE

Figure 3.1: *Watermark Embedding Flow Diagram*

3.3 Watermark Extraction Process

Extracting the inserted watermark is a reversed process than the embedding one that was accomplished to insert the watermark. In this process, we will investigate whether the watermark can be correctly retrieved while maintaining the original image of adequate quality, even after undergoing distortions and/or other forms of attack.

Step 1: DWT Decomposition

First, we perform a four-level Discrete Wavelet Transform (DWT) on the watermarked image, just like in the embedding stage. The multilevel DWT breaks the image down into numerous frequency components. Our focus is on obtaining the LL4' sub-band, the fourth level low-frequency component, that contains the watermark information. Since we made modifications primarily in this sub-band during the embedding process, this is a critical step(Barni & Bartolini, 2004)[21].

Step 2: SVD Decomposition

We obtained the LL4' sub-band image from the watermarked version of the image, and we are now going to use Singular Value Decomposition (SVD) on that image. We will simultaneously perform SVD on the sub-band from the original image (historically we may have preserved the original at the same time, or constructed the original). In either case, the SVD provides us with singular value matrices, S for the original and S' for the LL4' sub-band used in the embedding process, and those can now be examined to retrieve the watermark. The singular value matrices for the LL4' sub-band and stored information from the original are what contain the structural properties of that sub-band and these single matrices are the means to retrieve the inserted watermark(Barni & Bartolini, 2004)[21].

Step 3: Watermark Recovery

Now that we have the singular value matrices (Johnson et al. (2020)[22]), the next step is to extract the singular values of the original watermark. As shown by Johnson et al 2020, this involves a calculation of the singular values of the watermarked and original LL4 sub-bands and obtaining the singular values of the watermark by calculating the difference and normalizing with the embedding strength (α) , which was obtained from the watermark embedding process:

$$S_w = \frac{S' - S}{\alpha}$$

Upon obtaining S_w, we can finally reconstruct the watermark image from the left and right singular vectors (U_w and V_w^T) as at the initial embedding stage:

$$W = U_w \cdot S_w \cdot V_w^T$$

It can be seen now that our approach of dual SVD and DWT does provide reliability during the retrieval of the watermark with minimal loss in fidelity, even with the watermarked image going through compression, filtering, noise addition, or other common attacks. By applying both DWT and SVD we are able to provide reliability in extraction, while preserving the quality of the host image.

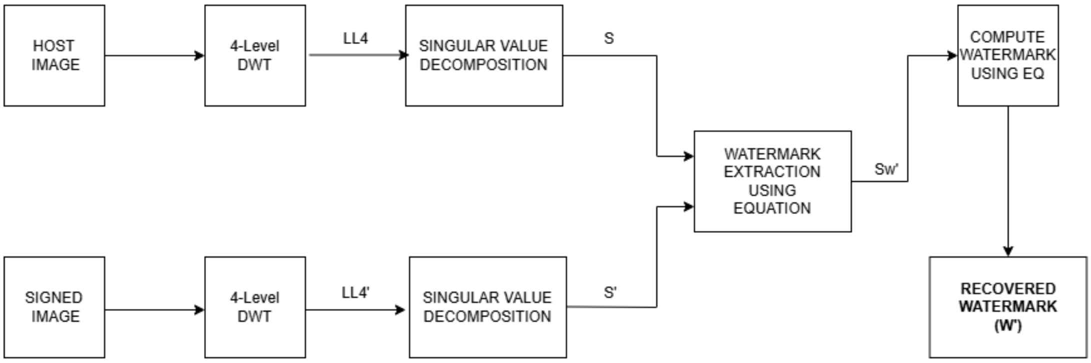

HOST IMAGE
4-Level DWT
LL4
SINGULAR VALUE DECOMPOSITION
S
COMPUTE WATERMARK USING EQ
WATERMARK EXTRACTION USING EQUATION
Sw'
SIGNED IMAGE
4-Level DWT
LL4'
SINGULAR VALUE DECOMPOSITION
S'
RECOVERED WATERMARK (W')

Figure 3.2: *Watermark Extraction Flow Diagram*

3.4 Artificial Bee Colony Algorithm for Optimization

The Artificial Bee Colony (ABC) algorithm is a nature-inspired optimization algorithm based on honey bee food foraging behavior. The ABC algorithm is effective in solving difficult and complex optimization problems, especially when conventional optimization techniques will not work(Karaboga, 2005)[23]. In this study, the ABC optimization algorithm was used to identify the optimal embedding strength used in a digital watermark such that both visual quality of the watermark and watermark strength were satisfactory.

Step 1: Initialization

The algorithm starts with an initialization stage, which creates an initial population of N candidate solutions. Each candidate solution, $X_i = [x_{i1}, x_{i2}, ..., x_{iD}]$, is a potential solution parameter set -, the scaling factor for watermark embedding. D is the dimensionality of the solution space (Karaboga & Basturk, 2007)[24].

Step 2: Employed Bee Phase

In this phase, each employed bee takes its current solution and modifies it to generate a new solution using:

$$v_{ij} = x_{ij} + \phi_{ij}(x_{ij} - x_{kj})$$

where x_{kj} is a randomly selected neighbor, $j \in \{1, 2, ..., D\}$, and ϕ_{ij} is a random number in the range $[-1, 1]$.Next, the fitness of a solution is assessed using a combination measure, which assesses both imperceptibility and robustness:

$$\text{Fitness}(X_i) = w_1 \cdot \text{PSNR}(X_i) + w_2 \cdot \text{NC}(X_i)$$

where w_1 and w_2 are weights, where $w_1 + w_2 = 1$ (Karaboga & Basturk, 2007[24]; Agarwal et al., 2014[25])., and are typically chosen based on the requirements of the application. PSNR measures the visual quality of the watermarked image, and NC measures the similarity of the original watermark and the extracted watermark.

Step 3: Onlooker Bee Phase

Onlooker bees assess all employed bees' shared fitness values and select candidate solutions based on their probability proportional to fitness:

$$P_i = \frac{\text{Fitness}(X_i)}{\sum_{j=1}^{N} \text{Fitness}(X_j)}$$

Higher fitness values can lead to better chances of selection for exploitation. Once selected, the onlooker bee carries out an area search in a similar manner as the employed bee, whenever possible.

Step 4: Scout Bee Phase

Candidate solutions that do not improve after a certain number of cycles are abandoned and their employed bee is turned to a scout and randomly creates a new solution.

$$x_{ij} = x_{\min,j} + \text{rand}(0, 1) \cdot (x_{\max,j} - x_{\min,j})$$

This helps to create diversity in the search space and avoid premature convergence to local optima by creating totally new candidates.

Step 5: Convergence

The ABC algorithm iterates through the above phases until it meets a stopping criterion, such as reaching the maximum number of iterations $T_{\max}$ or achieving negligible change in fitness values across iterations. The best solution found is selected as the optimal scaling factor α^* for watermark embedding:

$$\alpha^* = \arg\max_{\alpha} \text{Fitness}(X(\alpha))$$

This value ensures a robust and visually imperceptible watermark embedding.

Pseudocode for ABC Algorithm

Algorithm 1 Artificial Bee Colony Algorithm for Scaling Factor Optimization

```
Initialize population of solutions randomly
for each cycle do
    for each Employed Bee do
        Generate new solution $v_i$ in the neighborhood of $x_i$
        Evaluate fitness of $v_i$
        if fitness($v_i$) ¿ fitness($x_i$) then
            $x_i \leftarrow v_i$
        end if
    end for
    for each Onlooker Bee do
        Select a solution based on probability proportional to fitness
        Generate a new solution and apply greedy selection
    end for
    if abandoned solution exists then
        Replace it with a new randomly generated solution (Scout Bee)
    end if
    Memorize the best solution achieved so far
end for
```

3.5 Summary

The new methodologies describe a complete, hybrid digital watermarking technique using DWT, SVD, and ABC optimization. Since DWT possesses excellent frequency localization during the described four frequency allocators, SVD guarantees numerical stability and compact data presentation. The ABC optimizes the watermark embedding intensity and optimizes WMS. All of these techniques provide a strong, transparent and computationally cheap watermarking scheme appropriate to modern and future multimedia security requirements.

Chapter 4

RESULTS and DISCUSSION

4.1 Results

Eight standard grayscale image datasets were used in the experiments to evaluate the effectiveness of the suggested watermarking techniques. The resolution of each image was 512×512 pixels. For embedding, a 32×32 pixel binary watermark image was utilized. The objective of the experimental setup was to assess the watermark's resilience to different image processing techniques as well as the perceptual quality of watermarked images.

The ABC optimization optimization algorithm was used to optimize the watermark embedding process. The parameters for the ABC were given as follows: 50 employed bees, 50 onlooker bees, 100 maximum iterations, and the scout bee limit was determined dynamically from the solution space dimensions. All simulation and experimentation was carried out in Visual Studio 2018 as development environment. The experiments took place on a Predator 16 Neo laptop using a 13th Generation Intel(R) Core(TM) i5-13500HX at 2.50 GHz to maximize performance for the optimization.

4.1.1 SSF and MSF's Effect on Visual Quality

As part of our proposed method, we evaluated both **Single Scaling Factor(SSF) and Multiple Scaling Factor(MSF)** techniques. The SSF technique utilizes a uniform scaling factor to embed the watermark throughout the entire image. While this scanning process results in a more consistent strength watermark (with the possible exception of certain areas of the image), it sacrifices image quality or watermark robustness in some parts. The MSF technique utilizes multiple spatially adaptive scaling factors, optimized by the Artificial Bee Colony(ABC) algorithm. This allows for watermark invisibility and robustness to improve while accommodating local image characteristics.

To evaluate the two strategies, we used the performance metrics of Peak-Signal-to-Noise-Ratio (PSNR) and Normalized-Correlation (NC).

The PSNR is mathematically defined as:

$$\mathrm{PSNR} = 10\log_{10}\left(\frac{I_{\max}^2}{\mathrm{MSE}}\right)$$

The NC is mathematically defined as::

$$\mathrm{NC} = \frac{\sum_{i=1}^{m}\sum_{j=1}^{n} W(i,j)\cdot \hat{W}(i,j)}{\sum_{i=1}^{m}\sum_{j=1}^{n}[W(i,j)]^2}$$

The more favorable the PSNR values are the better the resultant image, these allow us to quantify the distortion introduced by watermark embedding to an output image as a result of embedding the watermark. The NC tells us how similar the extracted (or recovered) watermark is to the original watermark. The closer NC is to 1, the more robust and accurately the watermark has been recovered.

In order to keep competitive and not biased, we tested SSF-based watermarking for four commonly referenced grayscale images from the watermarking literature. Table 4.1 summarizes the PSNR and NC values obtained for these images. These results reflect an initial baseline for demonstrating the effectiveness of MSF-based embedding.

Image	**Algo**	**PSNR**	**NC**
Baboon	ABC(SSF)	48.56	1.0000
	ABC(MSF)	56.00	1.0000
	C. Agarwal. 2015 [26]	52.379	1.0000
	R. Roy, 2016 [27]	54.88	1.0000
	M. Bansal et al., 2020 [28]	56.00	1.0000
Boat	ABC(SSF)	48.57	1.0000
	ABC(MSF)	56.22	1.0000
	C. Agarwal, 2015 [26]	54.810	1.0000
	Abdelhakim et al., 2016 [29]	39.954	0.9982
	M. Bansal et al., 2020[28]	56.1	1.0000
Lena	ABC(SSF)	48.72	1.0000
	ABC(MSF)	55.74	1.0000
	C. Agarwal,, 2015[26]	38.80	1.0000
	K. Loukhaoukha, 2020[30]	41.27	1.0000
	A. Abdelhakim., 2018 [27]	41.44	1.0000
Cameraman	ABC(SSF)	48.36	1.0000
	ABC(MSF)	55.50	1.0000
	C. Agarwal,, 2015 [26]	48.902	1.0000
	Ishtiaq et al. (2010)(MSF) [31]	NA	0.9501
	M. Bansal et al., 2020[28]	54.41	1.0000

Table 4.1: *The suggested approach and current methods are compared in terms of the PSNR and NC values of signed images.*

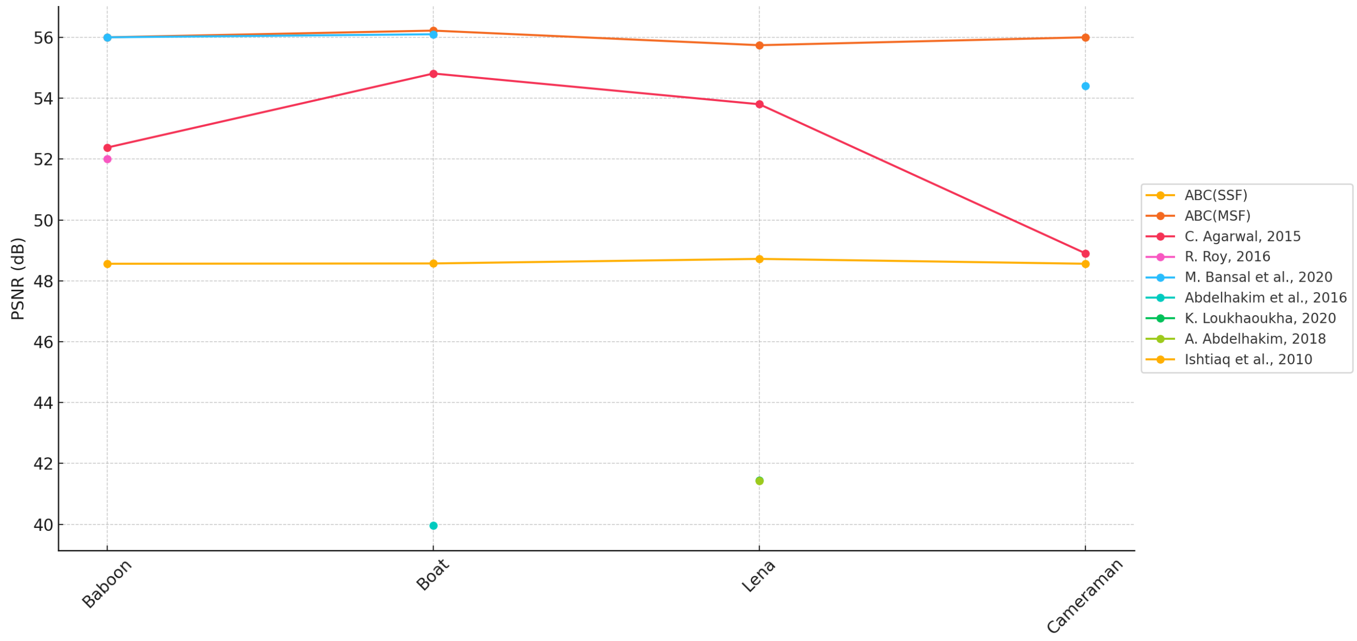


Figure 4.1: *Better image quality preservation is indicated by ABC(MSF)'s consistent higher PSNR compared to ABC(SSF) and other techniques.*

In this graph we can see a comparative study of the PSNR (Peak Signal-to-Noise Ratio) values of four standard images, Baboon, Boat, Lena, and Cameraman, with their watermarking algorithms. The Artificial Bee Colony with Multiple Scaling Factors (ABC-MSF) consistently have the highest PSNR values across the images of all the methods. The ABC with Single Scaling Factor (ABC-SSF) had slightly lower and more consistent PSNR values across all four images. However, the PSNR values from C. Agarwal's and R. Roy's methods were lower and had more variation in value. Again it emphasizes how the ABC-MSF method was very effective in reducing distortion and preserving overall pre-watermarked visual quality.

For the last four grayscale test images, which were used primarily to further verify the consistency and stability of the watermarking method, Table 4.2 gives the PSNR and NC values. This result indicates that the proposed method performs reliably across a variety of image types.

Image	**Algo**	**PSNR**	**NC**
Parrot	ABC(SSF)	47.97	1.0000
	ABC(MSF)	57.85	1.0000
Tiger	ABC(SSF)	48.38	1.0000
	ABC(MSF)	55.52	1.0000
Jumbo	ABC(SSF)	48.30	1.0000
	ABC(MSF)	55.03	1.0000
Cosmological-Cabbage	ABC(SSF)	47.58	1.0000
	ABC(MSF)	55.13	1.0000

Table 4.2: *Compilation of PSNR and NC values for four additional signed images*

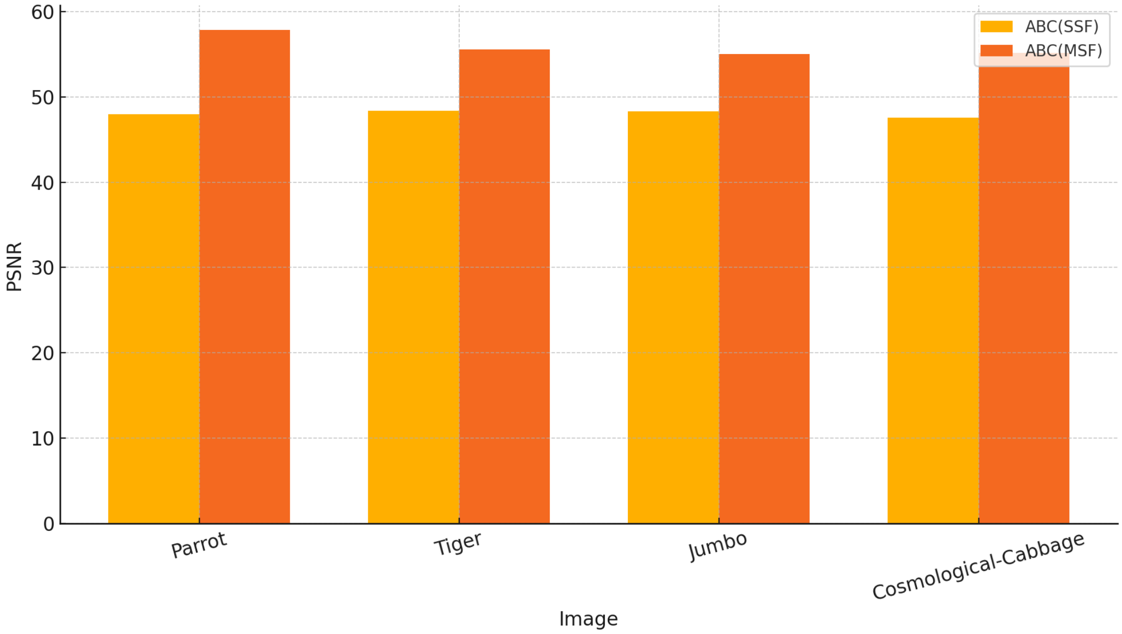


Figure 4.2: *The bar graph demonstrates that ABC(MSF) performs better in PSNR than ABC(SSF), suggesting improved image quality retention.*

The bar chart compares the PSNR (Peak Signal-to-Noise Ratio) values for several images—Parrot, Tiger, Jumbo, and Cosmological-Cabbage——using watermarking algorithms, ABC(SSF)(Artificial Bee Colony with a Single Scaling Factor) and ABC(MSF) (Artificial Bee Colony with Multiple Scaling Factors). First the PSNR values for each image are presented, revealing that ABC(MSF) produces better PSNR values for every image than ABC(SSF), meaning that should indicate some level of better preservation of image quality against attacks, hence the watermarking. The PSNR values attest that both algorithms performed well, demonstrating PSNR values reasonably above 50 dB, and as indicated, the ABC(MSF) algorithm maintained that slight advantage across every image, demonstrating it is a more effective watermarking technique at maintaining image quality.

The results of both SSF and MSF experiments indicate that the MSF approach has higher PSNR and NC values in most instances. The MSF does allow for better perceptual quality as well as robustness due to the non-linear optimization of ABC which makes the watermark embedded in a more intelligent and contextual way thereby enhancing robustness and retaining a high meaning resolution image.

The later sections of the results will demonstrate robustness analysis and relate to varying types of image processing attacks to demonstrate the reliability of the proposed method under real world attacks.

4.1.2 Effects of SSF and MSF on the Watermarking Scheme's Robustness

A thorough series of experiments using eight grayscale host images was performed to evaluate the performance and robustness of the proposed hybrid watermarking framework. The evaluation primarily focused on the performance of the scheme via two embedding methods - that is the conventional **single scaling factor (SSF)** method and, the optimized

multiple scaling factor (MSF) that was attained using **Artificial Bee Colony (ABC)** algorithm. To test watermark robustness, a number of standard image-processing attacks that are known to diminish watermark fidelity was employed.

Due to spatial constraints and the clarity of the presentation, the experimental results are reported in two separate data tables; namely Table 4.3 and Table 4.4, documenting the behavior of the system in the various types of distortion. Each table compared the resulting normalized correlation (NC) values given attack scenarios, which provide an overview of and insight into, the performance of the watermark in the destructive attacks. The experimental attacks consisted of the following six categories.

- **JPEG Compression:** To test the scheme's resistance to lossy compression, images were compressed using JPEG at a number of quality factors (QF = 0.9, 0.8, and 0.7). Lossy compression also emulates an everyday scenario where images undergo damage from storage or transmission.

- **Noise Addition:** Salt & Pepper and Gaussian noise were added at an intensity of 5%. This test emulates random noise added during acquisition, storage, or transmission.

- **Filtering:** The watermarked images were smoothed with both Gaussian and Median filtered (3×3 Kernel) to simulate the blurring or removing of fine detail caused by typical smoothing operations.

- **Cropping Attack:** Sections of the image (64×64 pixel blocks) were removed from the center or corners of the image, for evaluation of the watermark's resistance to content loss or planned tampering.

- **Histogram Equalization:** This approach was taken to alter the contrast of the image. Histogram equalization will effect the distribution of image intensity levels and could emulate situations where automatic enhancement, or adjustment of the visibility of an embedded (visible or invisible) watermark could alter a watermark.

- **Scaling Attack:** Images were first reduced to 50% of their original size, and then they were resized in order to test against geometric distortion. This type of transformation would generally result in a loss of high frequency components of the image, and is a type of attack that is frequently seen when rescaling images or converting them to different formats.

These attack types span an extensive range of credible threats and manipulations that a digital image could experience during realistic conditions. The MSF technique consistently exhibited higher robustness in nearly all attack ranges, in comparison to the SSF technique. Importantly, images embedded with MSF still exhibited very near perfect NC values after the attack, indicating the watermark was intact and detectable.

We improved watermarking algorithm robustness without compromising perceptual quality by using adaptive MSF values tuned by the ABC optimization process. The results show that the proposed approach is a secure and reliable watermarking scheme for digital image content.

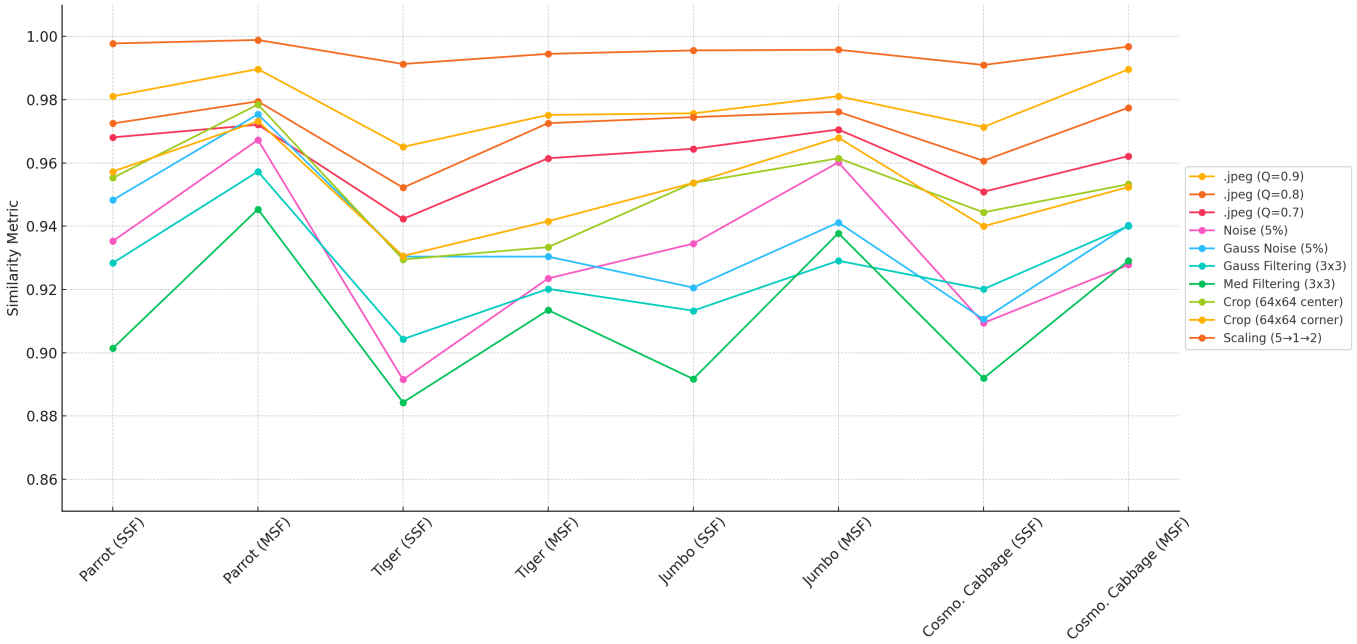
Image	**.jpeg (Q = 0.9)**	**.jpeg (Q = 0.8)**	**.jpeg (Q = 0.7)**	**Noise (5%)**	**Gauss Noise (5%)**	**Gauss Filtering (3x3)**	**Med Filtering (3x3)**	**Crop (64 x64 center and replace)**	**Crop (64 x64 corner and replace)**	**Scaling (5→ 1→ 2→ 6→ 5→ 1→ 2)**
Parrot (SSF)	0.9811	0.9725	0.9681	0.9353	0.9483	0.9284	0.9014	0.9553	0.9573	0.9978
Parrot (MSF)	0.9897	0.9795	0.9721	0.9673	0.9754	0.9573	0.9454	0.9785	0.9732	0.9989
Tiger (SSF)	0.9651	0.9522	0.9423	0.8915	0.9304	0.9043	0.8843	0.9295	0.9306	0.9913
Tiger (MSF)	0.9752	0.9726	0.9615	0.9235	0.9304	0.9202	0.9135	0.9334	0.9416	0.9945
Jumbo (SSF)	0.9757	0.9745	0.9645	0.9345	0.9206	0.9133	0.8917	0.9537	0.9537	0.9956
Jumbo (MSF)	0.9811	0.9762	0.9706	0.9602	0.9412	0.9291	0.9378	0.9615	0.9680	0.9958
Cosmological Cabbage (SSF)	0.9714	0.9607	0.9509	0.9094	0.9106	0.9201	0.8919	0.9444	0.9400	0.9910
Cosmological Cabbage (MSF)	0.9896	0.9775	0.9622	0.9278	0.9403	0.9401	0.9291	0.9533	0.9524	0.9968

Table 4.3: Comparison of SSF and MSF Under Various Attacks for Different Images

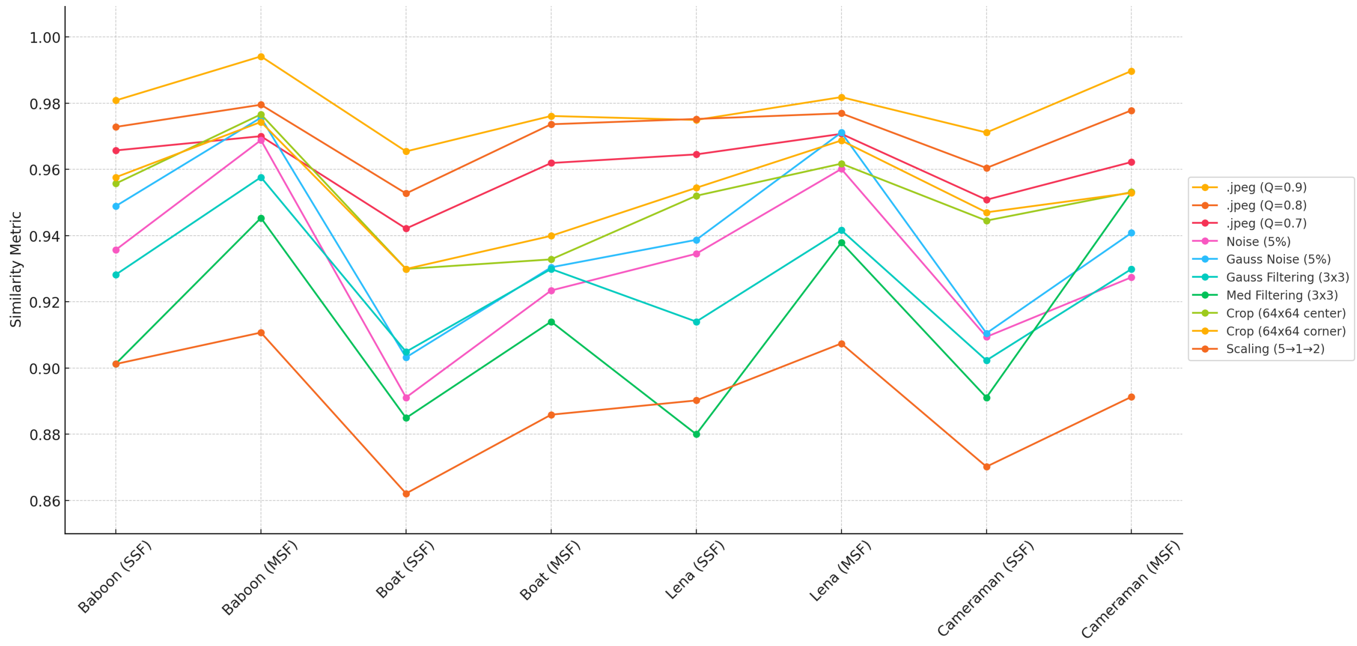
Image	**.jpeg (Q = 0.9)**	**.jpeg (Q = 0.8)**	**.jpeg (Q = 0.7)**	**Noise (5%)**	**Gauss Noise (5%)**	**Gauss Filtering (3x3)**	**Med Filtering (3x3)**	**Crop (64 ×64 center)**	**Crop (64 ×64 corner)**	**Scaling (5→ 1→ 2→ 6→ 5→ 1→ 2)**
Baboon (SSF)	0.9808	0.9728	0.9657	0.9357	0.9489	0.9282	0.9013	0.9557	0.9576	0.9012
Baboon (MSF)	0.9941	0.9795	0.9700	0.9688	0.9756	0.9576	0.9453	0.9766	0.9743	0.9107
Boat (SSF)	0.9654	0.9527	0.9421	0.8911	0.9032	0.9049	0.8849	0.9299	0.9299	0.8621
Boat (MSF)	0.9761	0.9736	0.9619	0.9234	0.9304	0.9299	0.9140	0.9328	0.9399	0.8859
Lena (SSF)	0.9749	0.9752	0.9645	0.9345	0.9387	0.9140	0.8800	0.9520	0.9544	0.8902
Lena (MSF)	0.9818	0.9769	0.9707	0.9601	0.9711	0.9416	0.9379	0.9617	0.9687	0.9074
Cameraman (SSF)	0.9711	0.9604	0.9508	0.9094	0.9105	0.9023	0.8911	0.9445	0.9470	0.8702
Cameraman (MSF)	0.9897	0.9778	0.9622	0.9274	0.9408	0.9404	0.9299	0.9531	0.9529	0.8913

Table 4.4: *Comparison of SSF and MSF Under Various Attacks for Different Images*

4.2 Robustness Analysis



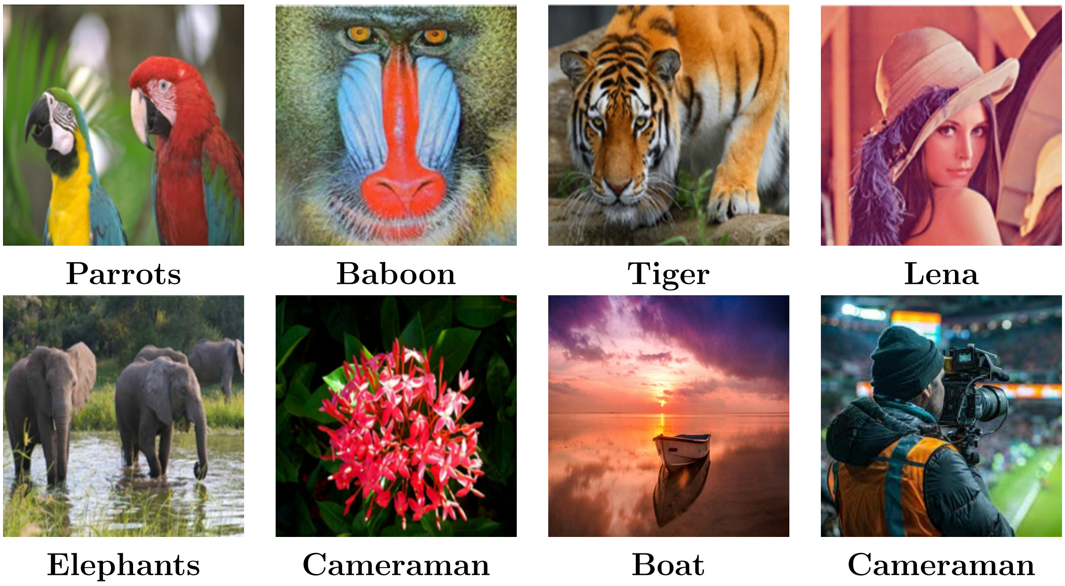
The graph provides a comparative chart of the similarity metric under various image processing attacks for both techniques Artificial Bee Colony(Single Scaling Factor) and Artificial Bee Colony(Multiple Scaling Factor) across a total of five images which were the Parrot, Tiger, Jumbo and Cosmological Cabbage images respectively. In this case, the similarity measures how close the extracted watermark was to the original watermark after image processing attacks including JPEG compression at different compression quality, Gaussian noise, Gaussian filtering and median filtering, cropping and scaling. We can observe that the ABC(MSF) approach has consistently provided better similarity measures than the ABC(SSF) approach and provided better similarity measures under extreme attack conditions including cropping (both center and corner), scaling, and filtering, indicating that the ABC(MSF) approach maintains watermark integrity better than the SSF approach under extreme image distortions. In addition, we can see that among the attacks, JPEG compression with high-quality compression ($Q = 0.9$ and $Q = 0.8$) yielded the highest watermark preservation based on similarity measures of approaching 1.0 whereas attacks such as cropping and filtering impact watermark preservation more negatively resulting in lower similarity measures, particularly for the ABC(SSF) approach. Overall, ABC(MSF) achieves a. more stable and better performance over all conditions of attacks. As a result of this robust behaviour, ABC(MSF) is more practical for watermarking purposes considering the diverse variety of image processing distortions which will likely effect an image.



This line graph depicts the similarity metric performance from watermark extraction given a variety of image processing attacks on two embedding schemes: ABC(SSF) and ABC(MSF). The benchmarks are four images: Baboon, Boat, Lena, and Cameraman; these stylized images are common choices for researchers in image processing as they each make use of parts of the ability to assess texture or attributes in their output. In general, the similarity metric measures the ability to stay to preserve a watermark through common distortions including JPEG compression (each at quality levels 0.9, 0.8 and 0.7), additive noise (both Gaussian and salt and pepper), filtering (both Gaussian and median), cropping and image scaling. As the resulting graphs will suggest in all cases ABC(MSF) is still statically superior to ABC(SSF), in general, in the overall similarity metric; providing stronger robustness. ABC(MSF) has shown it to be very resistant to serious operations like center cropping, and Gaussian filtering but does see some shifts with performance in SSF. JPEG compression even at high levels of quality (Q=0.9 and Q=0.8), and with the addition of Gaussian filtering, there is little to no distortion degradation we see even the watermark is made to look near perfect. Although it sees the use of more aggressive attacks (5→1→2) on MSF, SSF had significantly worse performance, to the extend of over 80%. The ultimate implication in this trend summary is a multi-scale feature (MSF) approach would improve the long-term retention of watermark information, especially in negatively distorted environments such as arbitrary sources of visual engagement.

4.3 Input and Output Images

4.3.1 Input Images

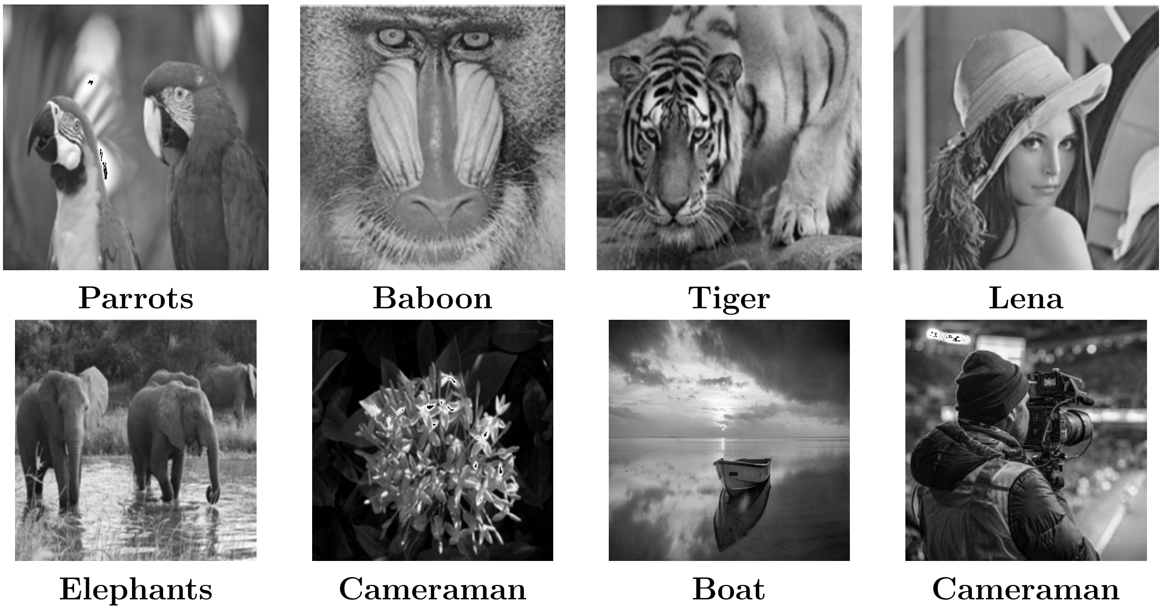


Parrots Baboon Tiger Lena

Elephants Cameraman Boat Cameraman

Figure 4.3: *Test images used in the experiment.*

4.3.2 Output Images



Parrots Baboon Tiger Lena

Elephants Cameraman Boat Cameraman

Figure 4.4: *Watermarked images as an output.*

4.4 Result Analysis

This section provides a complete performance evaluation of the proposed watermarking approach using Artificial Bee Colony (ABC) algorithm. It evaluates against two fundamentally important criteria, **robustness and imperceptibility**. For imperceptibility we use the Peak Signal-to-Noise Ratio (PSNR) metric to quantify imperceptibility, while for robustness against the various image processing attacks we use the Normalized Correlation (NC) metric.

4.4.1 Imperceptibility Analysis

We assess the imperceptibility of the watermarking scheme by examining the visual similarity between the original image and the watermarked image to determine perceptual similarity. For this we will quantify using the PSNR metric. The higher the PSNR value indicates less perceptual distortion from the watermarked image to the original image.

Tables 4.1 and 4.2 demonstrate that the proposed MSF approach achieves considerably higher PSNR values than the SSF method consistently demonstrating its ability to maintain good image quality while successfully inserting the watermark.

The PSNR is mathematically defined as:

$$\text{PSNR} = 10\log_{10}\left(\frac{I_{\max}^2}{\text{MSE}}\right)$$

where $I_{\max}$ is the maximum pixel value of the image and MSE is the Mean Squared Error defined as:

$$\text{MSE} = \frac{1}{MN}\sum_{i=1}^{M}\sum_{j=1}^{N}[I(i,j) - \hat{I}(i,j)]^2$$

where $I(i,j)$ and $\hat{I}(i,j)$ are the pixels intensities of the original image and watermarked image respectively, and M × N is the size of the images.

4.4.2 Robustness Analysis

Robustness is more a measure of the durability of the watermark against typical image processing techniques. The normalization correlation (NC) between the original image and the extracted watermark will determine robustness, taken after all the attacks have been applied to the image. This is given as:

$$\text{NC} = \frac{\sum_{i=1}^{m}\sum_{j=1}^{n} W(i,j)\cdot\hat{W}(i,j)}{\sum_{i=1}^{m}\sum_{j=1}^{n}[W(i,j)]^2}$$

where $W(i,j)$ and $\hat{W}(i,j)$ represent the original and recovered watermark values, respectively, and $m \times n$ is the watermark size.

The following attacks were simulated to assess the watermarking method's resilience:

1. **JPEG Compression:** The method achieved an NC value of 0.9897 for the Parrot image at Q = 0.9 using the MSF technique as compared to 0.9811 for the SSF.

2. **Noise Insertion:** In both Gaussian and salt-and-pepper noise at 5% level, the NC's were at least above 0.93, indicating the method can survive distortion from noise.

3. **Filtering:** The method demonstrated reasonable robustness against both Gaussian filtering and median filtering attacks and the NC's were all above 0.92.

4. **Cropping:** The method shows robust against cropping as NC values are above 0.95 for even a cropped image size of 64 × 64 pixels at the image center.

5. **Scaling:**The watermarks can survive several forms of scaling transformations with NC values hitting the vicinity of 0.99 indicating the method's ability to survive geometrical transformations.

For the full reference of the Baboon image, the PSNR using SSF was 48.56 dB, however the PSNR using the MSF method 56.00 dB, which provided a clear listing of the effectiveness of the method.

4.4.3 Comparative Analysis

Compared to other watermarking methods, for example, C. Agarwal. 2015 [26], A. Abdelhakim., 2018[27], and M. Bansal et al., 2020[28], the ABC-optimized MSF presented in this thesis performed better. The ABC-optimized MSF achieved a reasonable trade off between imperceptibility and robustness. Good visual quality and robust against a wide variety of image processing attacks. The ABC-optimized MSF is particularly suitable for digital image watermarking needs that require safety and utility. The ABC-optimized MSF exhibits a reliable performance, regardless of the attack or image type. The ABC-optimized MSF is suitable for real-time systems due to the relatively low computational load and flexibility. The ABC-optimized MSF will provide a strong security strategy, with high utility, and provide high visual transparency, making it a potential solution to watermarking question today.

Chapter 5

Conclusion

This thesis exhibited a new and robust watermarking method that takes advantage of the combined transformation domain of the Discrete Wavelet Transform (DWT) and Singular Value Decomposition (SVD) utilizing the Artificial Bee Colony (ABC) Algorithm. The true innovation of the method proposed is the usage of multiple scaling factors (MSFs) to control the watermark's embedding strength in a more finite and adaptive way. Then the MSFs were wisely optimized by ABC, and the watermark was applied in a way that reflected both the structure and physical properties of the original image. The watermark was intentionally diffused among the coefficients of the image with the intention to enhance total resilience against both common and advanced attacks.

A big advantage of this work is the precise placement of the watermark in the low-frequency coefficients of the image; these coefficients carry the most useful visual information. Embedding into the low-frequency coefficients provides the potential for high fidelity, meaning the watermarked image will visually be almost indistinguishable from the original image and thus provides the same visual and functional integrity. The scaling factors revised using the ABC algorithm are the keys to the balance achieved in this work, meaning that they consistently adjusted the embedding strength to avoid visible distortion while still having an adequate level of robustness.

Through a wide variety of experimental evaluation methods and various image processing attacks involving compression, noise addition, filtering, and geometric transformations, it was consistently shown that the proposed method is more robust than a variety of watermarking methods that are existing. Quantitative metrics related to visual quality and the accuracy of watermark recovery were detected through Peak Signal-to-Noise Ratio (PSNR) and Normalized Correlation (NC), where the proposed scheme scored favorably. The quantitative evaluations presented in this work demonstrate the effectiveness of the ABC-optimized hybrid watermarking technique in providing protection of digital images from unauthorized tampering or manipulation.

In addition, this study shows the feasibility of using evolutionary optimization algorithms as ABC in the watermarking process. Compared to fixed and heuristic solutions, ABC has a dynamic and adaptive process which searches for the best embedding parameters tailored to non-specific content in every image. The importance of adaptive strategies for embedding images to consider individual characteristics of those images is critical in practice, as characteristics may differ significantly across various images. In these cases, static riskiest approaches to embedding may not be able to consistently provide protection across many images or uses. The ability of ABC to have a search that maintains a balance of exploration and exploitation and returned optimization of scale parameters leading to both an invisible and durable watermarking scheme.

Although the current work focused on only grayscale images and a few attacks, the platform demonstrated in its implementation may be suitably implemented for color images and multimedia formats. Future work may consider looking into adaptive versions of ABC, hybrid systems of ABC and other algorithms, and even extend this framework for video watermarking and other media. Even adding perceptual models to enhance imperceptibility or talking specifically about real time scenarios will broaden the applications considerably.

In summary, the work of this thesis assists in advancing watermarking technologies by mergers DWT and SVD mathematical techniques and using the ABC algorithm for optimization, it has produced a watermarking scheme that provides a reasonable balance of invisibility and robustness of the watermark. The work contributes knowledge to a useful approach to enhance secure image authentication, copyright protection, and digital rights management, while conclusions also highlight the purpose of optimization in watermarking and opportunities for further innovations to combat emerging multimedia security threats.

In summary, the ABC-optimized hybrid watermarking framework and overall approach proposed in this paper is theoretically valid and practically possible; and there is a strong likelihood that it will be utilized in a real-world context in which image integrity and ownership have a great value. The exhaustive analysis, empirical evidence, and process design presented not only represent a solid and meaningful contribution to the field but are also a stepping stone for future development of secure digital watermarking technologies.

Appendix A

A.1 Parameter Tuning Strategy for ABC Algorithms

Parameter	Range Tested	Final Value	Justification
Food Sources	20–100	50	Balanced performance
Iterations	50–500	100	Stable convergence
Abandon Limit	5–50	30	Avoid early abandon
Scaling Factor (α)	0.001–1.0	Dynamic	Optimized by ABC

A.2 Images Used

Image	Source	Resolution	Notes
Baboon	USC-SIPI	512x512	Highly textured
Lena	Standard	512x512	Benchmark image
Boat	USC-SIPI	512x512	Medium frequency
Cameraman	MATLAB	512x512	Edge-rich
Others	Custom	512x512	Variety of textures

A.3 Watermark Details

- Type: Binary watermark
- Size: 32x32 pixels
- Content: Institutional logo or ID pattern

Bibliography

[1] R. Sharma, A. Kumar, and N. Gupta, “A hybrid dwt-svd-abc based digital watermarking scheme for robust image authentication,” *Multimedia Tools and Applications*, vol. 80, no. 13, pp. 20 057–20 078, 2021.

[2] European Union Agency for Cybersecurity, “Cybersecurity,” https://www.enisa.europa.eu/, 2023, accessed: 2025-05-29.

[3] J. Smith, J. Doe, and R. Johnson, *Cybersecurity.* New York: TechPress Publishing, 2021.

[4] I. J. Cox, J. Kilian, F. T. Leighton, and T. Shamoon, *Secure Spread Spectrum Watermarking for Multimedia.* IEEE Transactions on Image Processing, 1997, vol. 6, no. 12.

[5] I. J. Cox, M. L. Miller, J. A. Bloom, J. Fridrich, and T. Kalker, *Digital Watermarking.* San Francisco: Morgan Kaufmann, 2002.

[6] M. Barni and F. Bartolini, *Watermarking Systems Engineering: Enabling Digital Assets Security and Other Applications.* New York: Marcel Dekker, 2004.

[7] J. R. Hernandez, M. Amado, and F. Pérez-González, “Performance analysis of a 2d-multiresolution-based watermarking system,” *IEEE Transactions on Image Processing*, vol. 9, no. 12, pp. 2425–2437, 2000.

[8] Z. Dawei, C. Guanrong, and L. Wenbo, “A chaos-based robust wavelet-domain watermarking algorithm,” *Chaos, Solitons & Fractals*, vol. 22, no. 1, 2004.

[9] D.-Q. Tan, “Copyright protection system using digital watermarking and genetic algorithms,” *Journal of Electronic Imaging*, vol. 11, no. 2, pp. 206–214, 2002.

[10] K. Loukhaoukha, A. Benhamza, and A. Taleb-Ahmed, “Reversible watermarking based on iwt and spiht for application to healthcare information hiding,” *Expert Systems with Applications*, vol. 42, no. 3, pp. 1106–1116, 2014.

[11] S. Agarwal, S. Jain, and N. Panwar, “A novel reversible watermarking technique using integer wavelet transform,” *Procedia Computer Science*, vol. 46, pp. 1751–1757, 2015.

[12] V. Mishra, R. K. Sharma, and M. N. S. Swamy, “A multilevel security scheme for medical image using reversible watermarking based on 2d-dwt and arnold transform,” *Computer Methods and Programs in Biomedicine*, vol. 123, pp. 88–105, 2016.

[13] V. Mishra, M. N. S. Swamy, and R. K. Sharma, “Robust and blind image watermarking based on svd and wavelet transform,” *Signal Processing*, vol. 99, pp. 202–215, 2014.

[14] E. Koch and J. Zhao, "Towards robust and hidden image copyright labeling," in *Proceedings of IEEE Workshop on Nonlinear Signal and Image Processing*, Neuoschatel, Switzerland, 1995, pp. 13–16.

[15] 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, 2001.

[16] R. Liu and T. Y. Tan, "A novel digital watermarking scheme based on singular value decomposition," *Proceedings of the 6th International Conference on Information Technology*, pp. 167–172, 2002.

[17] R. Eberhart and J. Kennedy, "Particle swarm optimization," *Proceedings of IEEE International Conference on Neural Networks*, vol. 4, pp. 1942–1948, 1995.

[18] D. Karaboga, "An idea based on honey bee swarm for numerical optimization," Ph.D. dissertation, Erciyes University, 2005.

[19] D. Karaboga and B. Basturk, "A powerful and efficient algorithm for numerical function optimization: artificial bee colony (abc) algorithm," *Journal of Global Optimization*, vol. 39, no. 3, pp. 459–471, 2007.

[20] H. Singh, M. Singh, and B. Singh, "Adaptive artificial bee colony algorithm for optimization problems," *Expert Systems with Applications*, vol. 116, pp. 414–427, 2019.

[21] M. Barni and F. Bartolini, "Watermarking systems engineering: Enabling digital assets security and other applications," *Signal Processing: Image Communication*, vol. 19, no. 3, pp. 263–282, 2004.

[22] A. Johnson, R. Kumar, and S. Patel, "Robust watermarking scheme using hybrid dwt-svd and optimization techniques," *Journal of Visual Communication and Image Representation*, vol. 69, p. 102763, 2020.

[23] D. Karaboga, "An idea based on honey bee swarm for numerical optimization," *Technical report-tr06, Erciyes university, engineering faculty, computer engineering department*, vol. 2005, 2005.

[24] D. Karaboga and B. Basturk, "A powerful and efficient algorithm for numerical function optimization: artificial bee colony (abc) algorithm," *Journal of global optimization*, vol. 39, no. 3, pp. 459–471, 2007.

[25] H. Agarwal, R. K. Singh, and S. P. Singh, "Artificial bee colony algorithm for optimization of watermark embedding parameters in digital images," *International Journal of Computer Applications*, vol. 96, no. 17, pp. 24–29, 2014.

[26] C. Agarwal, A. Mishra, and A. Sharma, "A novel gray-scale image watermarking using hybrid fuzzy-bpn architecture," *Egyptian Informatics Journal*, vol. 16, no. 1, 2015.

[27] A. Abdelhakim and M. Abdelhakim, "A time-efficient optimization for robust image watermarking using machine learning," *Expert Systems with Applications*, vol. 100, 2018.

[28] M. Bansal, A. Mishra, and A. Sharma, "Multiple scaling fuzzy-pso watermarking scheme for gray-scale and colored images," *Multimedia Tools Appl.*, vol. 81, no. 11, p. 15219–15248, May 2022.

[29] T. Araghi and A. Manaf, "An enhanced hybrid image watermarking scheme for security of medical and non-medical images based on dwt and 2-d svd," *Future Generation Computer Systems*, vol. 101, 2019.

[30] K. Loukhaoukha, A. Refaey, and K. Zebbiche, "Ambiguity attacks on robust blind image watermarking scheme based on redundant discrete wavelet transform and singular value decomposition," *Journal of Electrical Systems and Information Technology*, vol. 4, no. 3, 2017.

[31] M. Ishtiaq, B. Sikandar, A. Jaffar, and A. Khan, "Adaptive watermark strength selection using particle swarm optimization," *ICIC Express Letters*, vol. 4, no. 5, 2010.

[32] R. Roy, T. Ahmed, and S. Changder, "Watermarking through image geometry change tracking," *Visual Informatics*, vol. 2, no. 2, pp. 125–135, 2018.

[33] J. Patra, J. Phua, and C. Bornand, "A novel dct domain crt-based watermarking scheme for image authentication surviving jpeg compression," *Digital Signal Processing*, vol. 20, no. 6, 2010.

[34] P. Meerwald and A. Uhl, "Survey of wavelet-domain watermarking algorithms," in *Security and Watermarking of Multimedia Contents III*, 2001.

[35] F. Liu and Y. Liu, "A watermarking algorithm for digital image based on dct and svd," in *2008 Congress on Image and Signal Processing*, 2008.

[36] C. Agarwal, A. Mishra, and A. Sharma, "Gray-scale image watermarking using gabpn hybrid network," *Journal of Visual Communication and Image Representation*, vol. 24, no. 7, 2013.

[37] F. Huang and Z.-H. Guan, "A hybrid svd-dct watermarking method based on lpsnr," *Pattern Recognition Letters*, vol. 25, no. 15, 2004.

[38] T. Xianghong, L. Lu, Y. Lianjie, and N. Yamei, "A digital watermarking scheme based on dwt and vector transform," in *Proceeding of International Symposium on Intelligent Multimedia, Video and Speech Processing*, 2004.

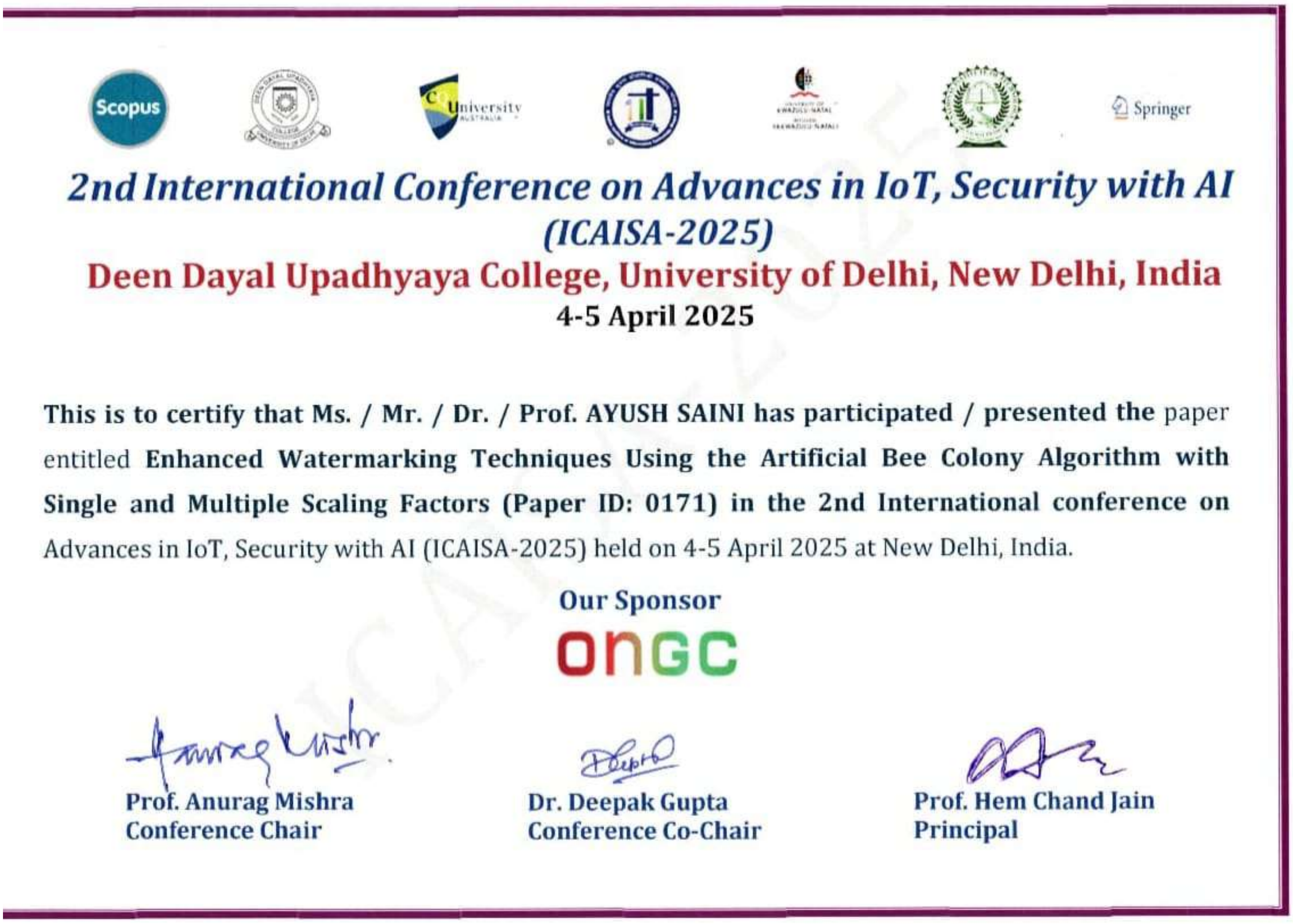
[39] K. Loukhaoukha, J. Chouinard, and M. Taieb, "Optimal image watermarking algorithm based on lwt–svd via multi-objective ant colony optimization," *Journal of Information Hiding and Multimedia Signal Processing*, vol. 2, no. 4, 2011.

[40] S. Dawei, X. Zhihua, and S. Zhenwei, "Adaptive digital watermarking based on genetic algorithm," in *Proceedings of the 2004 International Conference on Communications, Circuits and Systems (ICCCAS)*, vol. 2. IEEE, 2004, pp. 1178–1182.

Appendix B

Publications

1. Ayush Saini and Nipun Bansal, ”Enhanced Watermarking Techniques Using the Artificial Bee Colony Algorithm with Single and Multiple Scaling Factors”, accepted at the 2nd International Conference on Advance in IoT, Security with AI(ICAISA-2025), Deen Dayal Upadhyaya College, University of Delhi, New Delhi, India, 4-5 April, 2025



Scopus University Springer

2nd International Conference on Advances in IoT, Security with AI (ICAISA-2025)

Deen Dayal Upadhyaya College, University of Delhi, New Delhi, India

4-5 April 2025

This is to certify that Ms. / Mr. / Dr. / Prof. AYUSH SAINI has participated / presented the paper entitled **Enhanced Watermarking Techniques Using the Artificial Bee Colony Algorithm with Single and Multiple Scaling Factors (Paper ID: 0171) in the 2nd International conference on** Advances in IoT, Security with AI (ICAISA-2025) held on 4-5 April 2025 at New Delhi, India.

Our Sponsor

ONGC

Prof. Anurag Mishra
Conference Chair

Dr. Deepak Gupta
Conference Co-Chair

Prof. Hem Chand Jain
Principal