ENHANCING SVD-BASED IMAGE WATERMARKING STRATEGIES BASED ON DIGITAL CHAOS

WAFA’ HAMDAN SULEIMAN ALSHOURA

UNIVERSITI SAINS MALAYSIA

2022

ENHANCING SVD-BASED IMAGE WATERMARKING STRATEGIES BASED ON DIGITAL CHAOS

by

WAFA’ HAMDAN SULEIMAN ALSHOURA

Thesis submitted in fulfilment of the requirements for the degree of Doctor of Philosophy

August 2022

ACKNOWLEDGEMENT

First and foremost, I have to thank Allah for somehow to help me and make everything going from hard into easy. I would like to thank my supervisor Associate Professor Dr Zurinahni Zainol for his patience and continued support during my study, he gave me all the cognitive and advisory support all the time about contributions and writing. These few words do not meet the size of appreciation and respect for him. Also, I would like to thank my co-supervisor Dr Je Sen Teh for his continued help in discussing ideas and research papers. I would like to extend my special thanks to the Dean and all staff members of the School of Computer Science, USM. There is no word to express my deep feelings to my lovely mother, husband, sister, brothers, and my little daughters (Lenda and Lama) for their feeling and hopes.

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

LIST OF ABBREVIATIONS

BCR	Bite Correction Rate
BPNW	Back Propagation Neural Network
CT	Comparison and Threshold
DCT	Discrete Cosine Transform
DTCWT	Dual-Tree Complex Wavelet Transform
DW	Direct Watermarking
DWT	Discrete Wavelet Transform
EPR	Electronic Patient Record
EPR	Electronic Patient Record
FPP	False Positive Problem
HVS	Human Visual System
IPR	Intellectual Property Right
IWT	Integer Wavelet Transform
LBP	Local Binary Pattern
LSB	Least Significant Bit
MOACO	Multi-Objective Ant Colony Optimization
MSB	Most Significant Bit
MSE	Mean Square Error
MSF	Multiple Scale Factor

NC	Normalized Correlation
NSCT	Non-Sub-Sampled Contour Let Transform
ODFA	Opposition and Dimension Modified Firefly Algorithm
PC	Principle Component
PE	Differential Evolution
PSNR	Peak-Signal-Noise Ratio
PSO	Particle Swarm Optimization
RDWT	Redundant Discrete Wavelet Transform
RIDWT	Redistributed Invariant Discrete Transform
SIFT	Scale-Invariant Feature Transform
SSF	Single Scale Factor
SVC	Singular Value and Comparison
SVD	Singular Value Decomposition
SVMW	Singular Value Matrix Watermarking

PENAMBAHBAIKAN STRATEGI-STRATEGI PENANDAAN IMEJ BERASASKAN KEKACUAN DIGITAL

ABSTRAK

Imej digital adalah media sejagat yang membawa maklumat sensitif dan berkembang pesat dalam beberapa tahun kebelakangan. Skema penanda air adalah teknik yang digunakan untuk melindungi gambar digital dan kandungan lain seperti audio, video, dan teks. Skema penanda air gambar mempunyai kemampuan untuk memasukkan maklumat pemilik ke dalam gambar asal dengan cara yang tidak dapat dilihat, dan dapat diekstrak kemudian pada fasa pengesanan. Baru-baru ini, skema penanda air berdasarkan dekomposisi nilai tunggal (SVD) berdasarkan domain frekuensi telah mendapat perhatian. adalah kerana SVD mempunyai kestabilan dan sifat kuat yang menjadikannya tahan terhadap serangan terkenal yang berbeza. Walau bagaimanapun, skema SVD hibrid yang ada tidak memenuhi beberapa syarat penandaan air yang kritikal seperti pertukaran yang berjaya antara ketahanan dan ketidaklihatan, kapasiti besar, dan keselamatan yang tinggi. Oleh itu, mereka menghasilkan hasil yang tidak berkesan yang tidak mantap dan terdedah kepada pelbagai serangan. Kajian ini bertujuan untuk merapatkan jurang dengan mengembangkan skema watermarking gambar berasaskan SVD hibrid untuk memenuhi syarat penandaan air yang disebutkan di atas. Dalam skema yang dicadangkan, nombor rawak dan strategi penyisipan baru digunakan untuk mengatasi masalah ini serta menjadikan skema yang dicadangkan fleksibel dan mudah dilaksanakan. Kajian ini mencadangkan tiga skema baru yang dapat dilaksanakan pada format gambar yang berbeza (gambar kelabu dan warna). Elemen reka bentuk dan konstruksi novel yang digabungkan dalam skema yang dicadangkan memastikan bahawa ia melebihi skema yang ada. Akhirnya, skema baru dinilai seca-

ra eksperimen berdasarkan pelbagai metrik keselamatan yang biasa digunakan yang merangkumi rintangan terhadap serangan masalah positif palsu, ketahanan, ketidaklihatan dan keupayaan penyisipan. Rintangan terhadap pelbagai serangan terkenal telah diuji untuk menunjukkan kekukuhan menggunakan Normalized Correlation (NC) dan imperceptibility diuji menggunakan Peak Signal to Noise Ratio (PSNR). PSNR tertinggi direkodkan ialah 58.12 DB, manakala skor NC tertinggi ialah 0.99712 selepas serangan garam dan lada. Beberapa imej tera air telah dibenamkan dalam satu imej hos dengan PSNR 58.84 DB tinggi, 8 imej tera air dengan saiz 256×256 telah dibenamkan dalam imej hos satu warna dengan saiz 512×512. Perbandingan antara skim yang dicadangkan dengan skim terkini yang dikenal pasti dalam kesusasteraan dijalankan untuk menunjukkan keunggulan mereka berbanding rakan sebaya mereka.

ENHANCING SVD-BASED IMAGE WATERMARKING STRATEGIES BASED ON DIGITAL CHAOS

ABSTRACT

A digital image is a universal medium that carries sensitive information and has proliferated in recent years. The watermarking scheme is a technique used for protecting digital images and other content such as audio, video, and text. Image watermarking schemes have the ability to embed the owner's information into a host image in an imperceptible manner, and can be extracted later in the detection phase. Recently, the hybrid singular value decomposition (SVD)-based watermarking schemes in the frequency domain have received considerable attention. The interest is as a result of SVD having stability and robust properties which makes it resistant to different well-known attacks. However, existing hybrid SVD schemes do not meet some critical watermarking requirements such as successful trade-offs between robustness and imperceptibility, large capacity, and high security. Hence, they produce ineffective results which are not robust and are prone to a variety of attacks. This study aims to bridge the gap by developing enhanced hybrid SVD-based image watermarking schemes to fulfil the aforementioned watermarking requirements. In the proposed schemes, random numbers and new embedding strategies are leveraged upon to address these issues as well as making the proposed schemes flexible and easy to implement. This study proposes three new schemes that can be implemented on different image formats (gray and color image). The design elements and the novel constructions incorporated in the proposed schemes makes sure that they surpass the existing schemes. Finally, the new schemes are experimentally evaluated based on a wide variety of commonly used security metrics which include resistance against false positive problem attacks, robustness, imperceptibility and embedding capacity. Resistance against various well-known attacks was tested to indicate robustness using Normalized Correlation (NC) and imperceptibility was tested using Peak Signal to Noise Ratio (PSNR). The highest PSNR recorded was 58.12 DB, whereas the highest NC score was 0.99712 after a salt and pepper attack. Several watermark images were embedded in one host image with high PSNR 58.84 DB, 8 watermark images with size 256×256 were embedded in one color host image with size 512×512. A comparison between the proposed schemes with state-of-the-art schemes identified in literature are carried out to show their superiority over their peers.

CHAPTER 1

INTRODUCTION

1.1 Overview

The growth of mobile and fixed communications technologies, coupled with the increase in storage capacity devices and computing have increased the usage and exchange of digital content, thus opening new frontiers for today's information-driven society. Our important day-to-day life applications such as social networks, email, e-banking, e-commerce create, generate and process massive amounts of digital content which have made people more concerned about security and privacy issues than before. Hence, it is of vital importance to protect and secure digital content by incorporating confidentiality and authenticity in order to prevent misuse of digital information.

Intellectual property rights (IPR) is one of the techniques that has been developed for protecting digital content from illegal use and manipulations. Other techniques that have gained attention include; verification of the source, origin of the content and identification of authorized and unauthorized parties that initially share digital images. Approaches such as watermarking are leveraged to protect copyright and identification of ownership. Some special form of watermarking embed hidden watermarks which are imperceptible to the human eye in the digital content. The hidden watermarks can only be detected using a detector device that has a knowledge of the locations and shapes of the watermarks. For instance, image content can be watermarked by making some pixels in some frames faintly lighter on a copy and darker on another copy. The user will be unable to determine if he is viewing a watermarked copy or not but the detector can tell if it a copyrighted version and trace/detect who is responsible for the piracy for legal action to take place. Other approaches such as collusion-resistant fingerprinting can help protect copyrighted digital content against piracy. This technique appends fingerprints to the content to distinctively link specific copies to specific users in order to detect any user/pirate who shares or leaks their copies to other users. In digital fingerprinting, an unique identification information is embedded in the shared content. For example, there is an attack called a collusion attack where a group of purchasers collaborate as part of a coalition. A detectable location is a content segment that the colluders have at least two distinct copies of. The fingerprint must thus withstand both ordinary distortions (compression, filtering, data conversion, and channel noise) and malicious user collusion attacks.

Most of the digital image contents very sensitive multimedia data that cannot tolerate any errors, such as courtroom reports, medical images, telemedicine, military, photo-journalism, fingerprinting and so forth (Agarwal et al., 2019). The importance of digital content has pulled many researchers and specialists into proposing diverse approaches for the security of digital information, particularly free digital image content.

Digital image watermarking is the art and science that protects the ownership rights of digital images, and it is an alternative approach to IPR protection. Watermark signal is embedded into digital images and distributed to the users on the Internet where everyone and anyone can see. The embedded watermark is undetected to the public and only the owner can detect and extract it during the detection/extraction phase. Currently, millions of digital images are produced and uploaded to the Internet and are easily available online (Garg and Kishore, 2020; Ray and Roy, 2020). This accessibility is made easier by free Web hosting sites and message exchange. Image collections are downloaded, stored, uploaded, and updated every day. Hence, the ownership protection of digital images from unauthorized parties, to curtail illegal copying and distribution of images has become extremely important as the year progresses.

Digital image watermarking can be fundamentally classified into spatial-domain and transform-domain methods (Assini et al., 2018). The spatial domain method is a straightforward technique that was popular in the early days of the introduction of watermarking as they address values in the content. In the spatial domain technique, the content of the watermark is embedded in the host image by modifying the pixel values. It has the advantage of easy implementation, low-cost benefits, and low complexity in terms of computation. The common techniques used in this domain include the least significant bit (LSB), spread spectrum and correlation-based methods. However, the spatial domain technique is very weak to different visual distortions, mostly fragile to image-processing operations and produce low-quality images that can be observed by the human visual system (HVS). In contrast, the representative transform-domain technique which is also referred to as the frequency-domain embeds the watermark by modulating the magnitude of coefficients in a transform domain. The frequency-domain technique is known to be better, more robust, and more realistic in watermarking techniques. Examples of the transform-domain techniques include, the discrete cosine transforms (DCT), discrete wavelet transforms (DWT), integer wavelet transforms (IWT), singular value decomposition (SVD) and others (Ray and Roy, 2020).

Most digital image watermarking schemes achieve their main targets and improve their performance by combining two or more transforms; such schemes are referred to as hybrid schemes. The main reason behind the combination of more than one transform is to correct the defects of an individual transform, which consequently results in an effective scheme (Zear et al., 2018). The intuition behind the development of new hybrid schemes is to use the characteristics of the combined transforms to achieve the desired objectives of the targeted system. To achieve the desired objectives, watermarking schemes based on SVD in the frequency domain have been developed over the last few years, due to the fact that SVD yields attractive characteristics, such as stability and robustness (Assini et al., 2018; Makbol et al., 2017a; Zear et al., 2018).

1.2 Motivation

Nowadays, with the growth of the Internet and communications technology around the world, the accessibility and use of electronic information have increased dramatically. Anyone can handle, transfer and store digital products more easily than ever before. However, this advantage raises security issues that have emerged in the form of unlimited duplication, manipulation and illegal distribution of multimedia. Hence, ownership protection and digital content verification have become important concerns. Watermarking is known to be a popular strategy among the current strategies used to address these problems.

Images represent a significant element of multimedia content and include descriptive diagrams, virtual arts, and legacy of cultural boards in digital photography and digitized form. Distributed images on open channels have led to an increase in warnings about copyright violation and content integrity. Moreover, various image processes such as copying, updating, modifying and sharing, have become seamless over the Internet. Therefore, digital content security strategies are needed and image watermarking is one of them.

With improvements in the quality of smartphone cameras, there are many digital images (photos) taken each year. Figure 1.1 shows the number of photos taken from 2013 to 2022. The number of photos decreased in 2020 and 2021 due to the global Covid-19. In 2022, the number of photos taken sharply increased because restrictions have been lifted and people started travelling more again. The number of photos taken and shared will continue to grow in the coming years. The photos are taken by owners are kept as digital images in their own phones or devices. Many images are posted online or in personal correspondences. Figure 1.2 shows the number of images are stored in Google in four years. The number of images is still expected to increase in the coming years. The process of protecting the ownership of images is of utmost importance and requires quick and reliable techniques. Image watermarking is one of the main solutions to provide ownership protection.

Image watermarking has been widely studied and numerous research perspectives and innovations have been published in recent years. The two major motives being the availability of too many images on the Internet at no cost and the high demand for the security of those images from illegal infringements and the claim ownership (Singh, 2018; Singh and Bhatnagar, 2019). Image watermarking utilizes an embedding strategy to protect the distributed image without a significant loss of visual quality, signal or digital information (owner information) is used as watermark information. Finally, depending on its application, a watermark image might be visible or invisible.

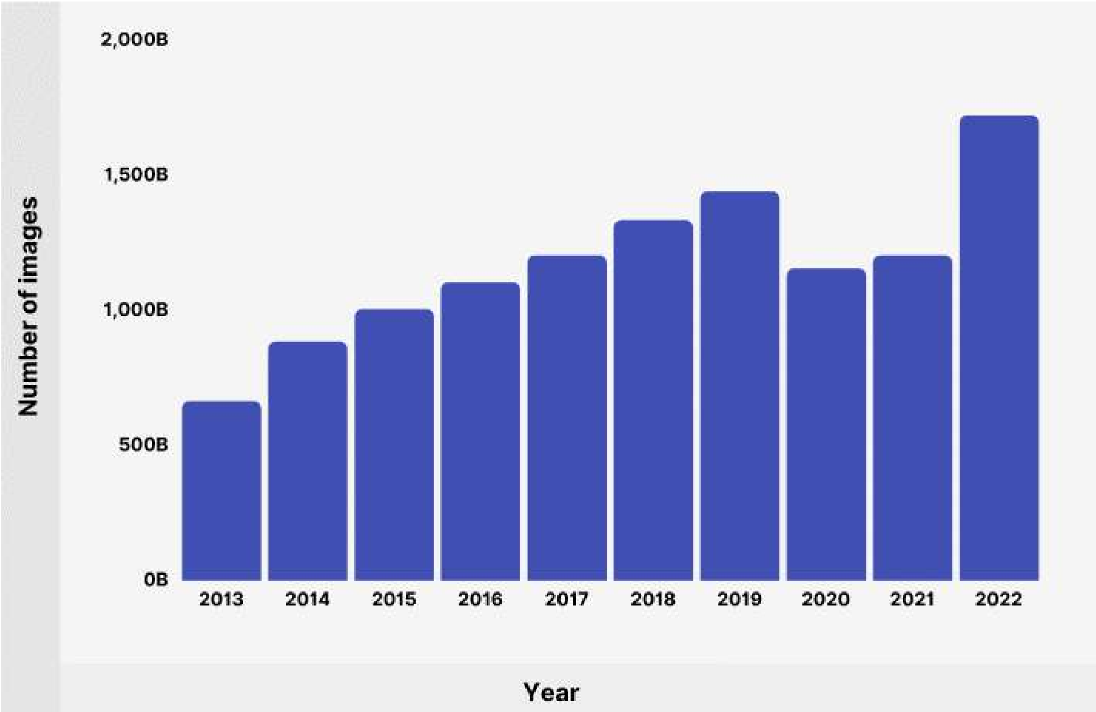

Figure 1.1: Number of photos taken each year

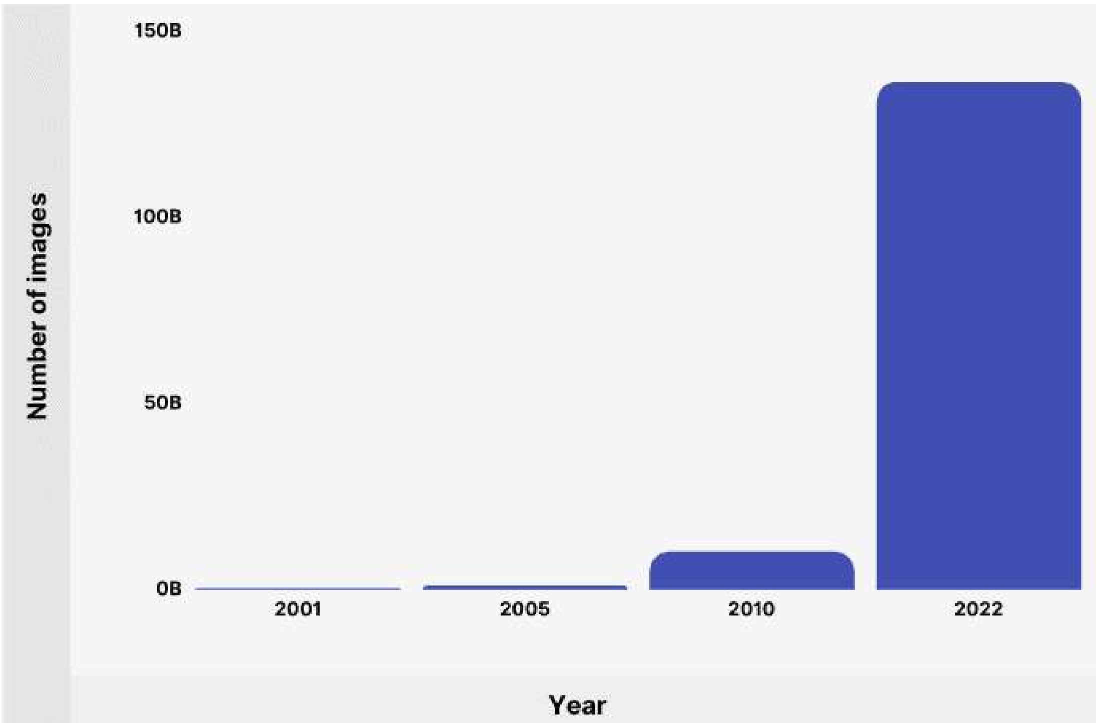

Figure 1.2: Number of images on Google

Image watermarking is been used in many applications such as copyright protection, authentication, tampering, ownership identification, access control, and so forth (Singh et al., 2018). Researchers working in digital image watermarking confront obstacles in developing new techniques with appropriate characteristics (requirements) to meet desired purposes. The most desirable characteristics important to any watermarking technique are robustness, imperceptibility, capacity, and security. Trade-offs between these characteristics have always attracted a significant number of researchers to obtain the best results (Kazemivash and Moghaddam, 2017; Thakur et al., 2019). For instance, lower imperceptibility findings will lead to high watermark robustness due to higher watermark content on the host image. In addition, a larger embedded capacity would weaken its imperceptibility and make more changes to the host image in the embedding process. Also, it reduces watermark robustness because more changes have a direct effect on the extracted watermark. Therefore, developing new image watermarking methods generally requires achieving a good balance between the mentioned contradictory criteria (Singh, 2018).

Security is a core characteristic required for protecting digital images from malicious attacks through extracting fake watermarks and claiming ownership. Invisible watermark is one of the security technologies that ensure attackers do not have access to sensitive data to delete or modify them. Most of the existing schemes do not take into consideration the security and reliability, thus they are unable to extract and detect relevant watermarks within certain attacks, consequently, failing to protect copyright. Furthermore, a number of security vulnerabilities have been discovered in existing image watermarking schemes, especially the SVD-based image watermarking scheme (Zhang and Wei, 2019).

Without the protection of digital images (especially those that have value as intellectual property) and with images widely shared in social media and in other forms of correspondence, the resulting impact can be summarized as follows:

- Legal courts cannot separate disputes over image ownership without digital watermarking technology.
- Legal legislation is based on watermark technology in enacting its laws.

1.3 Problem Statement

Digital images are a major component of multimedia content because these digital images hold sensitive information. With increased Internet speed and hardware memory, many digital images are captured every day and shared over various networks. These digital images are susceptible to being copied, modified or manipulated. Therefore, techniques to protect digital content are necessary (Singh and Bhatnagar, 2019).

Ownership and copyright protection are very necessary to protect digital images against unauthorized parties to change the ownership. Image watermarking is the best technique used to protect the ownership of digital images. An image watermarking scheme protects the sensitive information in the digital image by embedding owner information into the host image without noticeable degradation in visual quality. Consequently, a watermark image is produced and marked as generic or shared with users. The owner uses extraction technology, to protect the watermark image against the opponent claiming ownership of the image (Liu et al., 2021).

To protect the ownership of digital images, there are four necessary requirements - robustness, imperceptibility, security, and capacity. Hence, a trade-off always exists among them. Research in the area is divided into two main categories. The first develops image watermarking based on spatial domain, while the second uses the frequency domain to embed the owner's watermark in the host image. In spatial domain, image pixels are changed directly using watermark information. Thus, the spatial domain has many problems, including not being able to protect the watermark image against different distortions such as salt and pepper, JPEG attacks (Shi et al., 2021). On the other hand, the frequency domain has shown better properties than spatial domain. Frequency domain converts a host image from spatial to the frequency coefficients to do the embedding process, the embedding is done by simple mathematical equations. A watermark image is embedded and then inverted it to recover the watermarked image. The frequency domain shows high results and good trade-off between watermark requirements compare to spatial domain. However, there are certain flaws with frequency-based watermarking schemes, such as selecting a proper frequency transform and extracting embedded watermark information with good visual quality (Khare and Srivastava, 2021).

To address the limitations of frequency-based watermark schemes, researchers employ hybrid transforms to get improved outcomes and resistance to various attacks. On a host image, a hybrid transform employs two or more frequency transforms, such as DCT, DWT, and others. Each transformation offers advantages that differ from one another. SVD is a frequency transform that has a number of characteristics that make it a more appealing transform than others. Due to its stability and robustness, SVD is employed in many hybrid transformations. However, many of the proposed schemes still have issues and do not achieve the optimal properties of a watermarking scheme (Balasamy and Suganyadevi, 2021; Zermi et al., 2021).

SVD is a matrix decomposition mathematical tool used to simplify the matrix to its component parts in order to make some resulting matrix calculations easier. The intuition behind the SVD-based watermarking method is to determine the SVD of the host image or each block of the host image, which is followed by altering the singular values of the digital image to embed the watermark. It used in a variety of applications; image watermarking is one of such applications which has some of the desired characteristics for watermarking, such as stability, flexible matrix size, and reliable orthogonal matrix (Singh et al., 2020c). The watermark is always embedded after the image has been altered by changing the SVD components. As a result, image watermarking schemes based on SVDs are basic and efficient. On the other hand, the transform domain is utilized to combat piracy and is more resilient in image watermarking techniques than the spatial domain. As a result, methods from the transform domain and SVD decomposition are combined into the frequency domain to generate strong watermarking schemes (Agarwal et al., 2019; Ahmadi et al., 2019). These proposed schemes obtain acceptable outcomes by finding a balance between robustness and imperceptibility, while they fall short of addressing various FPP attacks.

Hybrid SVD watermarking schemes have been proposed which include different frequency transforms such as DCT, DWT, IWT, and others (Agarwal et al., 2019). Most of these existing schemes embedded the watermark after obtaining the transform coefficients to reduce visible distortion. However, the embedding in SVD components has some challenges that make it difficult for proposed schemes to meet the watermarking requirements (robustness, imperceptibility, capacity, and security). Three identified issues have made the hybrid SVD image watermarking strategies to be insecure, not robust, and not maintain the quality of the digital image after the embedding process (Agarwal et al., 2019; Huang et al., 2019; Makbol et al., 2018; Sadek, 2012).

SVD decomposes the image into three components U, S, V, the left, and right are singular vectors that contain the geometry structure of the image and the middle is a singular value that represents the luminance of the image. The host image is transformed by using one or two frequency transforms, the transform coefficient is decomposed by SVD and the watermark signal is embedded in one of the SVD components. Most of the researchers used singular values S in the embedding process because it has stability and it is effective in terms of robustness and imperceptibility (Al-Afandy et al., 2018; Ali et al., 2014a; Hossain and Muhammad, 2016; Roy and Pal, 2017a; Singh et al., 2016). Using the watermark content or S of the watermark after SVD decomposition, the embedding is conducted by modifying S values of the host image and the singular vectors of watermark used as the side information for the extraction process. False Positive Problem (FPP) arises when using S in the embedding process whether S of the host image or a watermark image.

In FPP, a fake watermark is extracted from a watermarked image that has a particular watermark (Ansari et al., 2016). An attacker can demand legal ownership by using other side information in a variety of ways (attacks). Three FPP attacks were proposed to extract fake watermarks from the watermarked image that used S in the embedding process (Makbol et al., 2018). Researchers have proposed a number of solutions to avoid FPP in SVD-based watermarking schemes (Assini et al., 2018; Kang et al., 2018; Najafi and Loukhaoukha, 2019; Zear et al., 2018; Zhang et al., 2019). However, the FPP is still in existence in the recently proposed schemes (Arumugham et al., 2019; Assini et al., 2018; Zear et al., 2018). The usage of the S component in the embedding process and storing the right and left U and V as side information required for the extraction process are the main reasons why these proposed schemes suffer from FPP. This is due to the fact that the U and V components include the majority of the information from the watermark image while the S component contains diagonal information from the embedded watermark. Also, existing solutions do not take into account trade-offs among watermarking requirements, high efficiency and low computation (Hossain and Muhammad, 2016; Jia, 2014; Makbol et al., 2016; Zhang et al., 2019).

Robustness is described as the extraction of an embedded watermark under various geometric and non-geometric attacks with tiny distortions in the extracted watermark. While imperceptibility means preserving the visual quality of the image after embedding the watermark content (tiny distortions in the watermarked image). To obtain a good trade-off between robustness and imperceptibility, scale factor values are used to determine the level degree of embedding in many SVD-based watermarking schemes (Ali and Ahn, 2014a; Moeinaddini and Afsari, 2018). Single scale factor (SSF) is used with contrasting results such as small SFF value which achieves high imperceptibility and low robustness to well-known attacks and vice versa (Jain et al., 2008a). It is hard to select a suitable SSF to get a high trade-off. Therefore, multiple-scale factor (MSF) is used instead of SSF in many SVD-based watermarking schemes (Ansari and Pant, 2017). MSF is a numerical matrix with several values that is multiplied with the watermark matrix. Unlike SSF, which has a single value that is multiplied by all watermark matrix, MSF gives a wider variety of scale factors and help to achieve the trade-off between watermarking requirements. However, the main challenge is how the MSF values are generated.

In MSF, the optimum MSF parameters are generated by using an efficient optimization algorithm (Ali et al., 2015a; Kang et al., 2018; Zear et al., 2018). Each watermark information that is used in the embedding process has optimum MSF parameters by one of the optimization algorithm. Optimum MSF should thus be kept as the secret key for the extraction process (Makbol et al., 2017a). However, optimum MSF strategies are not flexible and require high computation to achieve high trade-offs (Huang et al., 2019).

Capacity is one of the watermark requirements and measures the amount of embedding in the host image (Zeki et al., 2011). A larger amount of watermark information is desired in terms of the copyright protection algorithms and keep some personal information such as Electronic Patient Record (EPR) (Oueslati and Solaiman, 2018; Zear et al., 2018). In hybrid SVD-based watermarking schemes, the capacity is controlled by the SVD components and the sub-band type used in the embedding process. In the case of increasing the capacity of the embedding in the singular vectors, the imperceptibility will negatively degrade and robustness will be high against attacks (Luo et al., 2019; Singh, 2017; Zhang et al., 2019). On the other hand, a small capacity will contribute to an increase in imperceptibility and low resistance to attacks. Furthermore, embedding in different sub-bands is highly designed to enhance robustness where each sub-band has a specific resistance to different types of attack (Shih and Zhong, 2016; Zear et al., 2018). However, hybrid SVD-based watermarking schemes suffer from a bad trade-off between capacity and other characteristics especially imperceptibility.

In conclusion, hybrid SVD-based image watermarking schemes have three issues that can be written as follows

1. SVD suffers from FPP when using singular values for the embedding process.
2. A trade-off between robustness and imperceptibility on the basis of non-optimum MSF parameters is still poor.
3. SVD-based watermarking schemes that have high capacity perform poorly in terms of imperceptibility.

Researchers introduced many schemes to address SVD-based image watermarking issues. They used several methods to overcome FPP such as encryption, hashing, signature, and embedding singular vectors. However, these methods need additional authentication operations. Thus, FPP without additional authentication operations is still a venue to improve the watermarking schemes. A trade-off between watermarking requirements without optimization algorithms is a challenge and requires further investigation.

1.4 Research Objectives

This study aims to enhance image watermarking schemes based on hybrid frequency transforms and SVD decomposition to meet the desired watermarking requirements. The four design targets that are very important to achieve in an SVD-based image watermarking scheme include FPP avoidance, high robustness against geometrical and signal attacks, preservation of imperceptibility and high embedding capacity.

In this study, a random number-based digital chaos is combined with SVD to achieve the aforementioned design goals. The main goal of this study is success trade-offs (whereby all goals can be achieved simultaneously), each proposed scheme can improve all the essential requirements. Thus, three objectives are identified to address the research problems that have been identified. They are listed as follows:

1. To avoid/solve FPP with low computational overhead using secret key and encryption method.
2. To improve trade-off between watermarking requirements using embedding-based chaotic control.
3. To increase capacity embedding with elevated imperceptibility using direct and indirect embedding.
4. To study and assess the different types of images in the proposed embedding strategies.

1.5 List of Contributions

This section contains a list of contributions that connects the research objectives to the thesis's content. The aim of this thesis is to improve hybrid SVD watermarking schemes and to solve the major issues that have arisen in the existing schemes in recent years. The enhancement is achieved by combining many key components, including chaotic maps, encryption algorithms, and key generation. The chaotic maps are utilized to encrypt the watermark image in the first contribution. The host image and watermark image are used to create a secret key, which is then converted to chaotic variables (initial conditions and control parameters) to generate data sequences with varying ranges. The chaotic data sequences are utilized to encrypt the watermark by transforming it to a highly secure noise image. Additionally, a chaotic map is used to produce MSF with varying ranges at random. Chaotic MSF values are created rapidly and have a high degree of control on the embedding level.

The second contribution employs a secret key to produce chaotic variables, and iteratively generates chaotic data sequences using chaotic maps. Under the chaotic control and chaotic MSF parameters, a watermark image is encrypted and embedded. Eight-bit planes are decomposed and encrypted from the watermark image. Each bit-plane is embedded randomly in the host image's sub-band. The second contribution derived from the previous contribution's strengths while addressing some of its weaknesses, including a flexible secret key, a large capacity, and high results in terms of robustness and imperceptibility. The second contribution generates a hash value to mitigate against FPP attacks, eight bit-planes for high capacity, and chaotic MSF parameters to balance robustness and imperceptibility.

The third contribution introduces a new approach for avoiding FPP attacks by embedding part of the host image's data into a watermark image. This contribution builds on prior contributions by including new strategies to overcome previous contributions' weaknesses, such as side information issues. The third contribution present a new method for encrypting side information in terms of avoiding FPP attacks. Moreover, the authenticated data is embedded into the watermark image is used to as another way to avoid FPP attacks. The chaotic MSF parameters and multiple sub-bands strategies are used to achieve a better embedding scheme.

Table 1.1: A relationship between list of contributions and research objectives

Issues	Research Objective	Contribution
FPP attacks	RO (1): To avoid/solve FPP with low computational overhead using secret key and encryption method.	First (Secret key and encryption based on the chaotic maps) Second (Secret key, encryption bit-planes, and hash value) Third (Secret key, encryption slide information, and authenticated data)
Trade-off	RO (2): To improve trade-off between watermarking requirements using embedding-based chaotic control.	Three contributions (Chaotic MSF parameters)
Capacity	RO (3): To increase capacity embedding with elevated imperceptibility using direct and indirect embedding. RO (4): To study and assess the different types of images in the proposed embedding strategies.	First (double watermark images in different sub-bands of the host image and real-world images) Second (Eight bit-planes embedding, color host image, and real-world images) Third (different watermark images and real-world images)

In summary, three contributions are carefully designed to solve three issues by integrating the proposed primary components of hybrid SVD watermarking schemes. The three contributions address three issues and accomplish the research objectives. The second contribution addressed the first's weaknesses, while the third addressed the previous's. There is, however, a relationship between the list of contributions and the research objectives, as shown in Table 1.1.

1.6 Research Scope

This study focuses on developing new hybrid SVD-based image watermarking schemes that can be used in digital applications such as copyright protection and ownership identification. The main design aim of the proposed schemes is to use SVD with carefully chosen frequency transforms to effectively fulfil the necessary requirements of an image watermarking scheme. The trade-off between the three characteristics (robustness, imperceptibility, and capacity) remains a challenge, as well as the ability to prevent an unauthorized person from removing an embedded watermark or falsely claiming ownership of a watermark.

The scope of this research is bounded by the study and proposition of new hybrid SVD-based image watermarking schemes using different digital image formats. Thus, the established frequency tool IWT is leveraged in watermarking schemes in this study as well as classical SVD decomposition. Other frequency tools are not part of the scope of this study. Three image formats used in this study include RGB colour image and grey image. In addition, the proposed new schemes must have the necessary watermark requirements which are highlighted as follows:

- **Imperceptibility**: To preserve the decent visual quality of the image after the embedding phase is done (watermarked image) which is the main aim of any image watermarking scheme. As a consequence, the watermarked image is secure and will not provide any indication that a watermark has been embedded.
- **Robustness**: To be robust against all geometrical, signal and image processing distortion attacks such as JPEG compression and histogram attacks.
- **Capacity**: To embed large watermarks without reducing imperceptibility and retaining high robustness against different attacks. Different ways can be used to achieve this target such as multiple watermarks in different SVD components or sub-bands, repeating the same watermark in different sub-bands or embedding a watermark image in a host image of the same size.
- **Security**: To ensure that the new scheme provides a high level of security by

avoiding FPP attacks, encrypting the watermark, overcoming several malicious attacks, and blind extraction/detection. These security countermeasures help to ensure high reliability for real-life applications.

1.7 Research Methodology

This study is conducted in five phases: Firstly, the existing literature of hybrid SVD-based watermarking schemes is studied to exhibit the shortcomings and difficulties. The weaknesses of these schemes are listed and studied. In addition, the comparison of the existing schemes is introduced to identify the research gap of these schemes. Secondly, the problem statement of this study is identified and the research gab is highlighted. In the third phase, new watermarking schemes are proposed based on the new watermarking strategies such as chaotic image watermarking scheme. To depict the performance and desirable properties of the proposed schemes, evaluation in terms of imperceptibility, robustness, and security are performed in the fourth phase. Also, different image formats are used in this phase. In the fifth phase, discussion and comparison to other existing schemes are performed. Figure 1.3 shows an overview of the steps involved in this study and Table 1.2 provides a summary of the five phases of the research methodology. The association between the sub-problems of the study with the research objectives and contributions is shown in Table 1.3.

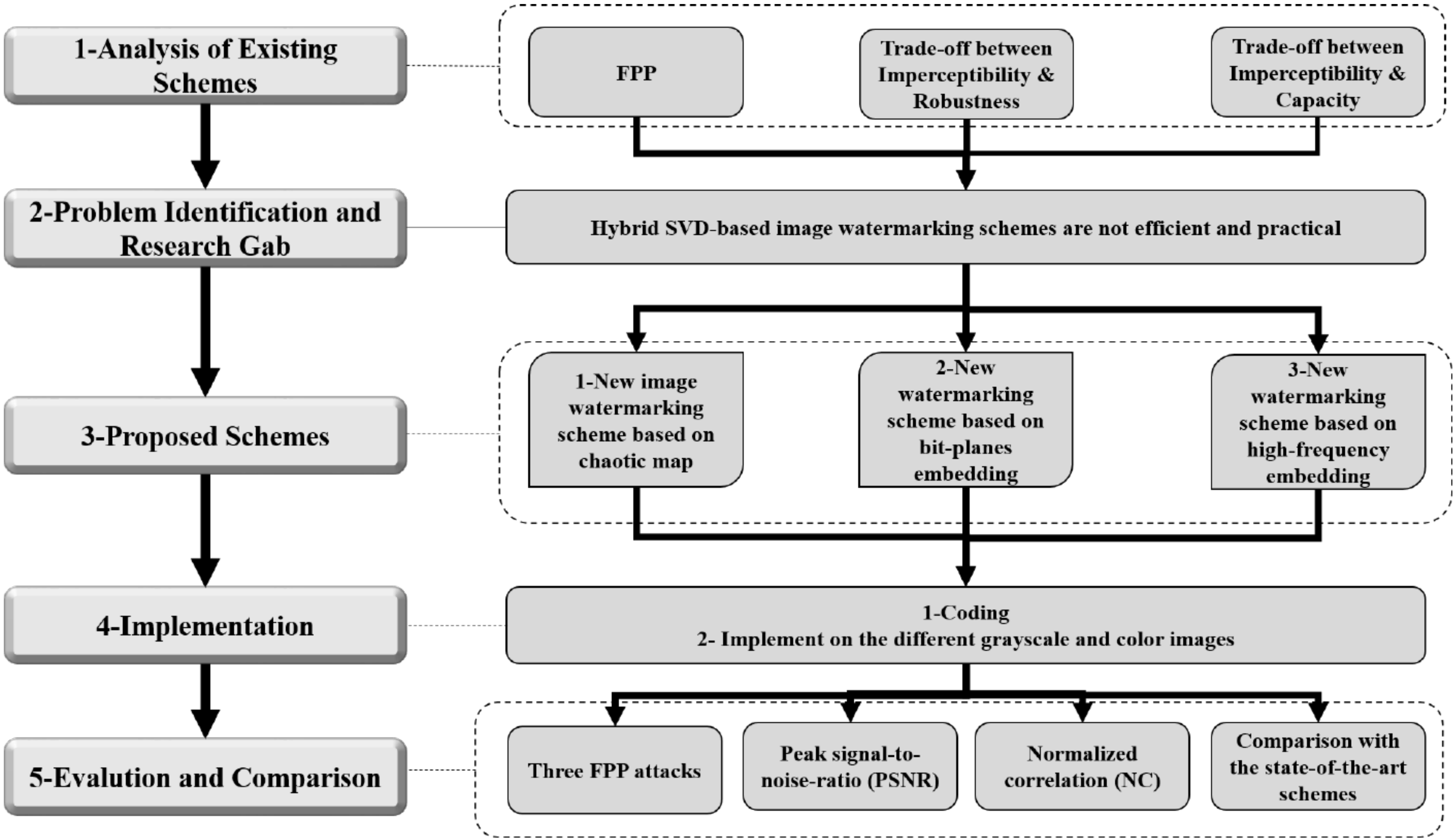

Figure 1.3: The five phases of the research methodology

1.8 Thesis Outline

The thesis is organized into seven chapters. Chapter 1 provides an overview of the concepts, problems, methodology, and contributions of the research. Chapter 2 presents a general overview of the background, related concepts, tools and a thorough description of existing schemes with the main goal of illuminating the gap that exists in the current research which will be filled by the findings of this study. Chapter 3 provides the step by step methodology to build new image watermarking schemes. Chapter 4, 5 and 6 provide three new SVD-based image watermarking schemes with experimental results. These proposed schemes are examined and evaluated using different test images and evaluation methods. Comparative analyses and results with previous schemes are introduced in these chapters. Finally, chapter 7 provides a conclusion of this thesis with open questions pointing to the future directions of the research.

Table 1.2: Research methodology

Phase	Details
1- Analysis of existing schemes	Many schemes which focused on SVD and hybrid frequency methods have been proposed in the literature to enhance image watermarking techniques. This stage of the process sheds light on studying such schemes in current literature, addressing their weaknesses and minimizing them by developing new schemes in terms of security, robustness, imperceptibility, and capacity.
2- Problem identification and research gab	The SVD-based image watermarking schemes still have some unresolved issues, which need to be highlighted first and then carefully studied. The development of image watermarking schemes that strengthen security and balance the trade-off issues synonymous with the SVD-based image watermarking schemes remains a research challenge.
3-Proposed schemes	This phase describes three distinct schemes that can provide solutions to the identified issues facing existing schemes in order to achieve the research objectives. The three proposed schemes, which meet the three research objectives, are a hybrid SVD-based watermarking scheme based on chaotic controls with a frequency transform to avoid FPP attacks with no more authentication processes, hybrid SVD-based watermarking scheme based on a chaos-based scale factor to achieve a high trade-off between robustness and imperceptibility, and hybrid SVD-based watermarking scheme based on direct and indirect embedding strategy to achieve large capacity.
4-Implementation	The proposed schemes that will improve the embedding and extraction performance of digital image watermarking are implemented to achieve the research objectives.
5-Evaluation and comparison	This phase analyses and discusses the quality efficiency of the proposed schemes by assessing the results in terms of image quality, the image under different attacks and security metrics. In addition, comparisons are made in the studies between the proposed schemes and the current state-of-the-art schemes.

Table 1.3: Associate sub-problems with objectives and contributions

Sub-Problems	Objectives	Contributions
• SVD suffers from FPP when using singular values for the embedding process.	• To avoid/solve FPP with low computational overhead using secret key and encryption method.	1. A new SVD-based image watermarking scheme based on extracting the secret key from the host and watermark images. 2. A new SVD-based image watermarking scheme based on extracting hash value from the embedding process as using the secret key. 3. A new SVD-based image watermarking scheme based on integrating a portion of the host image with watermark image before embedding process as using the secret key.
• A trade-off between robustness and imperceptibility on the basis of non-optimum MSF parameters is still poor.	• To achieve a high trade-off between robustness and imperceptibility using embedding-based chaotic control.	1. A new SVD-based image watermarking scheme based on embedding random watermark matrix under control chaos-based MSF. 2. A new SVD-based image watermarking scheme based on embedding multiple bit-planes under control updated chaos-based MSFs. 3. A new SVD-based image watermarking scheme based on embedding high-frequency sub-bands under control three chaos-based MSF parameters.
• Large capacity conducts low imperceptibility and high robustness in SVD-based watermarking schemes.	• To increase capacity embedding with elevated imperceptibility using direct and indirect embedding.	1. A new SVD-based image watermarking scheme based on embedding a watermark with the same size as the host image. 2. A new SVD-based image watermarking scheme based on embedding into multiple sub-bands of the colour host image. 3. A new SVD-based image watermarking scheme based on embedding into six sub-bands of the host image.

CHAPTER 2

BACKGROUND AND LITERATURE REVIEW

2.1 Introduction

Digital data (such as text, video, audio, and image) is transmitted over open channels such as the Internet which invariably makes the protection of private data and IPR to be extremely important in this era (Singh, 2015; Singh and Chadha, 2013) . Digital data types can be easily converted, altered, copied and widely distributed while preserving high quality. It is difficult to save real ownership and copyright of digital data because of an adversary (e.g., hacker, attacker, and pirate) may violate it. An adversary can manipulate, reproduce, alter, modify, re-transmit digital data over the Internet, and prove the ownership. Data or multimedia encryption (cryptography) is a method to protect sensitive data and the ownership of digital data while in storage or transmission. However, encryption focuses on protecting data itself instead of proving ownership (Khan et al., 2014).

In a general context, cryptography provides strong protection for digital content with limited distribution, and authorized parties have the full right to handle secret data after the decryption process (Cox et al., 2007). However, cryptography has faced the challenge of distributing digital data while protecting the ownership/copyright of the content. In order to overcome the challenge of using cryptography in proving ownership, the data hiding method is used to embed the message in the digital content before it is distributed. Hence, data hiding using processes such as watermarking is an intelligent technique that saves the original owner of the digital data by protecting