Singular Value Decomposition and Discrete Cosine Transform Based Image Watermarking

S.M. Rafizul Haque
This thesis is submitted to the Department of Interaction and System Design, School of Engineering at Blekinge Institute of Technology in partial fulfillment of the requirements for the degree of Master of Science in Computer Science. The thesis is equivalent to 20 weeks of full time studies.

Contact Information:
Author:
S.M. Rafizul Haque
E-mail: rafizulku@yahoo.com

Advisor(s):
Guohua Bai
Email: gba@bth.se
Department of Interaction and System Design

Department of Interaction and System Design
Blekinge Institute of Technology
Box 520
SE – 372 25 Ronneby
Sweden

Internet : www.bth.se/tek
Phone : +46 457 38 50 00
Fax : + 46 457 102 45
Acknowledgement

I would like to express my sincere and heartiest gratitude to my honorable supervisor Dr. Guohua Bai for his continuous help, guidance, constant support and enduring patience throughout the progress of this thesis.

I would like to extend my special appreciation and gratitude to my parents and my friends for their encouragement, endless love and understanding of my spending lots of time on this work.
Abstract

Rapid evolution of digital technology has improved the ease of access to digital information enabling reliable, faster and efficient storage, transfer and processing of digital data. It also leads to the consequence of making the illegal production and redistribution of digital media easy and undetectable. Hence, the risk of copyright violation of multimedia data has increased due to the enormous growth of computer networks that provides fast and error free transmission of any unauthorized duplicate and possibly manipulated copy of multimedia information. One possible solution may be to embed a secondary signal or pattern into the image that is not perceivable and is mixed so well with the original digital data that it is inseparable and remains unaffected against any kind of multimedia signal processing. This embedded secondary information is digital watermark which is, in general, a visible or invisible identification code that may contain some information about the intended recipient, the lawful owner or author of the original data, its copyright etc. in the form of textual data or image. In order to be effective for copyright protection, digital watermark must be robust which are difficult to remove from the object in which they are embedded despite a variety of possible attacks. Several types of watermarking algorithms have been developed so far each of which has its own advantages and limitations. Among these, recently Singular Value Decomposition (SVD) based watermarking algorithms have attracted researchers due to its simplicity and some attractive mathematical properties of SVD. Here a number of pure and hybrid SVD based watermarking schemes have been investigated and finally a RST invariant modified SVD and Discrete Cosine Transform (DCT) based algorithm has been developed. A preprocessing step before the watermark extraction has been proposed which makes the algorithm resilient to geometric attack i.e. RST attack. Performance of this watermarking scheme has been analyzed by evaluating the robustness of the algorithm against geometric attack including rotation, scaling, translation (RST) and some other attacks. Experimental results have been compared with existing algorithm which seems to be promising.

Keywords: Image Watermarking, SVD, DCT
Contents

Chapter One
Introduction.................................................................1
1.1 Intellectual Property and the Digital Age..........................1
1.2 Information Hiding Techniques......................................2
1.3 Digital Image Watermarking Framework............................2
1.4 Types and Applications of Watermarks.............................4
1.5 Applications of Digital Watermarking..............................6
1.6 Properties of Watermarks............................................7
  1.6.1 Robustness............................................................7
  1.6.2 Fidelity...............................................................8
  1.6.3 Computational cost................................................8
  1.6.4 False positive rate.................................................9
1.7 Attacks on Watermarks................................................9
  1.7.1 Removal attacks...................................................9
  1.7.2 Geometric attacks...............................................10
  1.7.3 Cryptographic attacks..........................................10
  1.7.4 Protocol attacks................................................10

Chapter Two
Background.....................................................................11
2.1 Singular Value Decomposition (SVD).................................11
2.2 SVD example................................................................12
2.3 Properties of SVD........................................................12

Chapter Three
Problem Definition and Goals.............................................15
3.1 Criteria of effective watermarking....................................15
3.2 RST invariant watermarking..........................................15
3.3 RST transformations....................................................15
3.4 RST and other attacks on image.....................................16
3.5 Goal of this thesis.......................................................18

Chapter Four
Literature Review.............................................................19
4.1 Pure SVD based algorithms............................................19
  4.1.1 Non block based algorithms......................................19
  4.1.2 Block based algorithms............................................19
4.2 SVD and transforms domain based algorithms....................20
  4.2.1 SVD and DCT based algorithm................................20
  4.2.2 SVD and DWT based algorithm.................................21
  4.2.3 SVD and FHT based algorithm.................................21
  4.2.4 SVD and Zernike moments based algorithm...............22

Chapter Five
Proposed Watermarking Scheme.........................................23
5.1 Developed watermarking scheme...................................23
5.2 Steps of the algorithm................................................24
  5.2.1 Embedding of watermark........................................24
  5.2.2 Preprocessing before extraction...............................25
  5.2.3 Extraction of watermark.........................................25
5.3 Enhanced Robustness Due to the Preprocessing...............26
Chapter Six
Analysis of experimental results .................................................. 27
6.1 Conducted experiment.............................................................. 27
6.2 Resilience against Attacks....................................................... 28

Chapter Seven
Conclusion ..................................................................................... 32
7.1 Scopes for future works............................................................ 32

References ....................................................................................... 34
List of figures

1.1 Steganography vs. Cryptography………………………… 2
1.2 A typical watermarking system…………………………… 3
1.3 Classification of watermarking techniques………………… 5
1.4 Different attacks on watermark…………………………… 9
2.1 Original and Gaussian blurred image……………………… 13
3.1 Original image…………………………………………… 16
5.1 Mapping of DCT coefficients to four blocks……………… 24
6.1 Original cover image and watermark image………………. 27
List of tables

Table 2.1  Singular values of two images  ………………….  13
Table 3.1  Attacked images…………………………………  17
Table 6.1  Extracted watermarks and value of correlation coefficient for different attacks……………  30
Table 6.2  Values of correlation coefficient of two methods…….  30
Chapter 1

Introduction

1.1 Intellectual Property and the Digital Age

Rapid evolution of digital technology has improved the ease of access to digital information. Digitizing of multimedia data has enabled reliable, faster and efficient storage, transfer and processing of digital data [16]. It also leads to the consequence of illegal production and redistribution of digital media. Duplication and modification of such digital data has become very easy and undetectable. Hence the risk of copyright violation of multimedia data has increased due to the enormous growth of computer networks that provides fast and error free transmission of any unauthorized duplicate and possibly manipulated copy of multimedia information. One way to protect multimedia data against illegal recording and distribution is to embed a secondary signal or pattern into the image, video or audio data that is not perceivable and is mixed so well with the original digital data that it is inseparable and remains unaffected against any kind of multimedia signal processing [15]. This embedded secondary information is digital watermark which is, in general, a visible or invisible identification code that may contain some information about the intended recipient, the lawful owner or author of the original data, its copyright etc. in the form of textual data or image. The information to be hidden is embedded by manipulating the contents of the digital data, allowing someone to identify the original owner, or in the case of illegal duplication of purchased material, the buyer involved. This digital watermark can be detected or extracted later to make an assertion about the data. Digital watermarks remain intact under transmission / transformation, allowing us to protect our ownership rights in digital form. Absence of a watermark in a previously watermarked image would lead to the conclusion that the data content has been modified.

In order to be effective for copyright protection, digital watermark must be robust, recoverable from a document, provide the original information embedded reliably, be non-intrusive and also removable by authorized users. Robust watermarks are those which are difficult to remove from the object in which they are embedded despite a variety of possible attacks by pirates including compression such as JPEG, scaling and aspect ratio changes, rotation, translation, cropping, row and column removal, addition of noise, filtering, cryptographic and statistical attacks, as well as insertion of other watermarks. Here cryptographic techniques and statistical properties of pseudo-random numbers play an important role.
1.2 Information Hiding Techniques

There are several techniques for information hiding into digital media. They are used for several purposes as well as copyright protection. Two basic methods of information hiding are cryptography and steganography. The concept of digital watermarking is derived from steganography. The term steganography means “cover writing” and cryptography means “secret writing”. Cryptography is a widely used method for protecting the digital content of the media. The message is encrypted before transmission and decrypted at the receiver end with the help of a key. No one can access the content without having the true key. The message is called the plain text and the encrypted message is called the cipher text [15]. The information is protected before the time of transmission. But, after decryption, the information becomes unprotected and it can be copied and distributed. The schematic representation of the cryptography is given in Figure 1.1 (b).

In steganography, the message is embedded into the digital media rather than encrypting it in such a way that nobody except the sender and the intended recipient can even realize that there is a hidden message. The digital media content, called the cover, can be determined by anybody; but, the message hidden in the cover can be detected by only the person having the actual key. Thus steganography actually relates to covering point-to-point communication between two parties. That’s why steganography methods are usually not robust against modification of the data, or have only limited robustness. The schematic representation of the steganography is given in Figure 1.1 (a).

![Steganography vs. Cryptography](image)

Figure 1.1 Steganography vs. Cryptography [15].

1.3 Digital Image Watermarking Framework

Image Watermarking, as mentioned earlier, is the process of embedding a secondary signal into an image such that the signal can be detected or extracted later to make an assertion about the image. In general, any watermarking scheme consists of the following three parts:

- The watermark signal,
- Watermark embedder that embeds the watermark into the media
• Watermark detector that verifies the presence of watermark

Figure 1.2: A typical watermarking system [7]

Figure 1.2 is a conventional watermarking system [7] consists of watermark embedder and watermark detector. The inputs to the watermark embedder are the watermark, the cover media data and the embedding security key. The watermark can be a number sequence, a binary bit sequence or may be an image. The key is used to enhance the security of the whole system. The output of the watermark embedder is the watermarked data. The inputs to the watermark detector are the watermarked data, the security key and, depending on the method, the original data and/or the original watermark. According to Cox et al. [16], a watermark detector includes two-step process. The first step is to extract watermark that requires one or more pre-processes to extract a vector referred to as extracted mark. In this process, original unwatermarked image may be used or may not be used depending on the algorithm. If the detector does not require the original copy, watermarking scheme is called public watermarking or blind watermarking, if the detector requires the original image, then, it is called private watermarking or non-blind watermarking [17]. If the original image is used, the watermark can be extracted in its exact form (if the image is not corrupted). If it is a blind detection, we can determine whether a specific given watermarking signal is present in an image.

Then, the second step is to determine whether the extracted mark contains the original watermark or not. The second step usually involves with comparing the extracted mark with the original watermark and the result could be some kind of confidence measurement representing the possibility of the original watermark being present in the document. Correlation method is used for this purpose. The correlation function computes the correlation value and the computed correlation are compared with a detection threshold. If the correlation value exceeds the threshold value, the image is believed to be watermarked. For some watermarking algorithms, the extracted mark can be further decoded to get the embedded message for various purposes such as copyright protection.
Suppose that a watermark is defined as $W$, $D$ is the host data, and $K$ is the security key. In watermarking, an embedding function $e(.)$ takes the watermark $W$, the host data $D$, and the security $K$, as the input parameters, and outputs the watermarked data $D' [7]:$

$$D' = e(D, W, K).$$

The watermark is considered to be robust if it is embedded in a way such that the watermark can remain unaffected even if the watermarked data $D'$ go through different attacks. The watermark detection procedure is stated as follows:

$$W' = d(D', K, . . . ),$$

where $d(.)$ is the detection function. $D$ and $W$ are the optional inputs for the detection function.

Watermark detection can be considered as watermark extraction when the watermark contains only one bit information indicating whether the original watermark is present in the work or not.

1.4 Types and Applications of Watermarks

Watermarking techniques can be classified according to the application domain, according to the type of document, according to the human perception and according to the application [15, 17]. Classification of watermarking techniques is shown in Figure 1.3.

Watermarks can be embedded into the multimedia content in spatial domain or in frequency domain. Frequency domain watermarking methods may use several different domains, such as discrete cosine transformation (DCT) domain, discrete Fourier transformation (DFT) domain, discrete wavelet transformation (DWT) domain, fast hadamard transform (FHT) domain etc. In the literature, it has been affirmed that the frequency domain techniques are more robust then spatial domain techniques [14].

The watermarking algorithms can be named according to the embedded multimedia content, such as text, image, audio and video watermarking.
Human perception is also used as a criterion to classify the watermarking techniques. Visible and invisible watermarks are of this type. Logos are the examples of the visible watermarks that indicate the owner of the content [18]. An usual way of visible image watermarking is to print “©date,owner” mark onto the image. One disadvantage of visible watermarks is that it can be easily removed from the digital cover image. Invisible watermarks alter the media in a way that they are perceptually unnoticeable. They can only be detected by using an appropriate detection method. They identify the owner of the digital media. Unlike visible watermarks, the invisible watermarks could not be removed from the media because they became an integral component of the content after being embedded. However, they can be made undetectable by some manipulations and distortions called “attacks”. The watermark, ideally, must be resilient to all possible attacks. Proof of ownership is another application area for invisible watermarks; however, it needs a higher level security than owner identification. Craver et al. [19] proposed a watermarking scheme that can be applied on a watermarked image, to allow multiple claims of rightful ownership. The two types of invisible watermarks are robust and fragile watermarks. Purpose of the robust algorithms is
the endurance of watermark after possible distortions such as possible compressions, filtering and noise additions. However, the fragile watermarks are used to detect if there is any manipulation or modification on the digital content. These modifications would change or destroy the watermark. Fragile watermarks can be used for content authentication such as trustworthy camera. A watermark is embedded into the frame when it is captured by the camera. The watermark will be lost if any altering made so verifying if the frame is the original captured one or not. The invisible robust watermarks are divided into two categories as private and public watermarks, as described in previous section. The private algorithms need the original content to detect the watermark where the public watermarks do not need.

According to the applications, the watermark could be classified as source based and destination based watermarks. In the source based algorithms, all the copies are watermarked with a unique watermark and used for ownership identification or authentication. The watermark identifies the owner of the content. However, the destination based watermarks (fingerprints) are embedded individually to each copy and used to mark out the buyer in the case of an unlawful operation. Fingerprints can be used for broadcast monitoring. A unique watermark is embedded into each video or audio-clip before broadcasting. Automated computers monitor the broadcast and detect when and where each clip is appeared [18]. Another application area of the watermarks is copy control. The digital media can be copied without sacrificing quality. To check this, a watermark can be inserted in a media such that a recorder would not copy it if it detects a watermark that indicates copying is illegal. However, this could be successful if all the manufactured recorders can implement watermark detection algorithms.

1.5. Applications of Digital Watermarking

Digital watermarking systems are developed based on the applications. Following are the common applications of watermarking [23]:

1) Copyright Protection. One of the main applications of watermarking is copyright protection. Information about the copyright owner is embedded into the data to prevent other people from claiming to be the legal owners of the data. The watermarks used for that purpose are supposed to be very robust against various attacks intended to eliminate the watermark.

2) Content Authentication. In order to be able to validate the content, any change to or manipulation with the content should be detected. This can be achieved through the use of “fragile/semi-fragile watermark” which has low robustness to the modifications of the host image. The semi-fragile watermarking can also serve the purpose of quality measurement. The extracted watermark can not only notify the possible tampering with the host image, but also provide more information about the degradation of the host image, such as Peak Signal
to Noise Ratio (PSNR) of the degraded host image. This can be very useful for broadcasting or network transmission, since sometimes the original reference is not available at the receiver side. The degradation of the transmitted media can be further used to evaluate the quality of service (QoS) of the transmission or the congestion of the network.

(3) Copy and Usage Control. Users can have different privilege (play/copy control) on the object due to different payment for that object. It is expected in some systems to have a copy and usage control mechanism to check illegal copy of the content or limit the number of times of copying. A watermark can be used for this purpose.

(4) Content Description. The watermark can contain some descriptive information about the host image such as labeling and captioning. For this kind of application, the capacity of the watermark should be relatively large and there is usually no strict necessity for the robustness.

1.6 Properties of Watermarks

Main properties of the watermarks are robustness, fidelity, computational cost and false positive rate [18]. However, a watermark may not satisfy all of these properties. Moreover, that may be not required for all types of watermarks. For a visible watermark, fidelity is not a concern, however, for an invisible watermark it is one of the most important issues. The watermark is designed to satisfy the required properties according to the type of the application. On the other hand, one property may confront with another. Increasing the strength of the watermark can increase the robustness but it decreases the fidelity. There must be a trade-off between the requirements and properties of the watermarking schemes depending on the applications. In this section, those properties will be investigated.

1.6.1 Robustness

For most of the watermarking applications, the marked data is expected to be processed in some way before it reaches to the watermark receiver. For example, in television and radio broadcast, the watermarked media should be resilient to lossy compression, D/A-A/D conversion applied on the transmitter and receiver side, and some small amount of horizontal and vertical translations. Moreover, noise can be added due to the transmission medium. Sometimes compression techniques are applied on images and videos on the web, so if a watermark is present in these objects, it must be resistant to compressions. Sometimes, one may need to use only some portion of the multimedia content, and thus crops and removes the other parts which require robustness against cropping. The images may be printed and distributed as hardcopy. In this case, geometrical modification and some noise may occur on the image. The distributed copies have different watermarks in broadcasting applications.
One may use these copies to provide an unwatermarked copy by averaging all copies which is called collusion attack. A robust watermark must be invariant to possible attacks and remains detectable after attacks are applied. However, it is probably impossible, up to now, for a watermark to resist all kind of attacks, in addition, it is unnecessary and extreme. The robustness criterion is specific for the type of application. On the other hand, the concept of fragile watermarks conflicts with the robustness criteria. In these applications, the watermark must be changed or lost after any applied attack. In many applications, when the signal processing between embedding and detection is unpredictable, the watermark may need to be robust to every possible distortion. This is the case for owner identification, proof of ownership, fingerprinting, and copy control. It is also true for any application in which hackers might want to eradicate the watermark.

1.6.2 Fidelity

Fidelity is a major concern for invisible types of watermarks. High fidelity means that, the amount of degradation caused by the watermark in the quality of the cover image is unnoticeable for the viewer. However, in most applications increasing the robustness by embedding a more powerful watermark signal may cause loss of fidelity. In this case a trade-off must be made and fidelity or robustness may be settled to a required level. Some watermarking algorithms use visual masking property of the Human Visual System (HVS) and embed the watermark to imperceptible regions in the cover object. This means embedding the most of the watermarks in the spotted regions of the image. For visible watermarks, it is worthless to talk about fidelity. However, in this case the watermark may be extended in a large or important area of the image in order to prevent its removal by clipping. As for example, a video signal, transmitted over National Television System Committee (NTSC), is not supposed to have very high quality. Hence, the watermark fidelity is not a big problem for the transmission using NTSC and can be low relatively. However, in High Definition Television (HDTV) and DVD video, the signals have very high quality and require much higher fidelity watermarks.

1.6.3 Computational Cost

Speed of the watermark embedding operation is a very important issue especially in broadcast monitoring applications where it must not slow down the media production and the watermark detector must work in real-time while monitoring the broadcasts. This would require practical watermarking schemes, which would not generate a lot of computational work. On the other hand, it is not very critical for a detector used for proof of ownership, because such a detector will only be used during ownership disputes.
1.6.4 False Positive Rate
A watermark detector may find a wrong watermark in the media or may not find the watermark, even if there is. These phenomena are called false positives. The false positive rate is the number of false positives expected to take place in a given number of detector runs.

1.7 Attacks on Watermarks

According to the watermarking jargon, an attack is any processing that may mess up detection of the watermark or communication of the information provided by the watermark. The processed, watermarked data is then called attacked data. Robustness against attacks is an important issue for watermarking schemes. The usefulness of an attacked data can be measured by its perceptual quality and the amount of watermark destruction can be measured by criteria such as miss probability, probability of bit error, or channel capacity. An attack may succeed in defeating a watermarking scheme if it distorts the watermark beyond tolerable limits while maintaining the perceptual quality of the attacked data [14]. The wide class of existing attacks can be divided into four main groups: removal attacks, geometrical attacks, cryptographic attacks and protocol attacks [23]. Figure 1.4 summarizes the different types of attacks.

Figure 1.4: Different attacks on watermark [23]

1.7.1 Removal attacks

These are the attacks that try to weaken or completely remove a watermark from its associated content, still preserving the content so that it is not useless after the attack is over. This category includes denoising, quantization, remodulation, and collusion attacks. Denoising and quantization attacks damage the watermark quality as much as possible, while keeping the quality of the attacked data high enough. Lossy compression has the same effect as denoising. The remodulation attack intends to predict the watermark. It may be
implemented by subtracting the median filtered version of the watermarked image from the watermarked image itself. Then the predicted watermark is removed from the watermarked image, producing the median filtered version of watermarked data. Collusion attacks are possible when many copies of a given data set, each signed with a different watermark, are available to an attacker. In this case, a successful attack can be performed by averaging all copies or taking only small parts from each different copy.

1.7.2 Geometric attacks

Geometric attacks consist of the distortions particular to videos and images including operations as rotation, scaling, translation, cropping etc. In contrast to removal attacks, geometric attacks do not actually remove the embedded watermark, but attempt to deform the watermark detector synchronization with the embedded information. The embedded watermark information can be recovered if the perfect synchronization is regained. However, the complexity of the required synchronization process might be too huge to be realistic. Current watermarking methods intend to endure from these attacks by the use of templates, invariant domains, image feature dependent methods or self synchronizing watermarks to defeat the geometrical transformations imposed by the attacker [15].

1.7.3 Cryptographic attacks

Cryptographic attacks intend to break the security methods in watermarking schemes and thus finding a way to remove the embedded watermark information or to embed deceptive watermarks. Brute-force search for the embedded secret information is one such technique. Another attack in this category is the so-called Oracle attack, which can be used to generate a non-watermarked signal when a watermark detector device is available. High computational complexity has restricted attackers from applying these attacks on watermarks.

1.7.4 Protocol attacks

Craver et al. [19] mentioned an attack, called the watermark inversion attack or IBM attack, which produces a fake watermarking schemes that can be applied on a watermarked image to create doubt about which watermark was inserted first. Copy attack is another kind of protocol attack. In this case, the watermark is predicted by using a watermarked data, and this predicted watermark is embedded into another data by adapting the local features to satisfy its imperceptibility.
Chapter Two

Background

Recently watermarking schemes based on Singular Value decomposition (SVD) have gained popularity due to its simplicity in implementation and some attractive mathematical features of SVD. Here a brief description of SVD and its role in the watermarking schemes have been presented.

2.1 Singular Value Decomposition (SVD)

SVD is an effective numerical analysis tool used to analyze matrices. In SVD transformation, a matrix can be decomposed into three matrices that are of the same size as the original matrix. From the view point of linear algebra, an image is an array of non-negative scalar entries that can be regarded as a matrix. Without loss of generality, if $A$ is a square image, denoted as $A \in \mathbb{R}^{n \times n}$, where $\mathbb{R}$ represents the real number domain, then SVD of $A$ is defined as

$$A = USV^T$$

where $U \in \mathbb{R}^{n \times n}$ and $V \in \mathbb{R}^{n \times n}$ are orthogonal matrices, and $S \in \mathbb{R}^{n \times n}$ is a diagonal matrix, as

$$S = \begin{bmatrix}
\sigma_1 \\
& \sigma_2 \\
& & \ddots \\
& & & \sigma_n
\end{bmatrix}$$

Here diagonal elements i.e. $\sigma$'s are singular values and satisfy

$$\sigma_1 \geq \sigma_2 \geq \ldots \geq \sigma_r \geq \sigma_{r+1} = \ldots = \sigma_n = 0$$

It is noticeable that the unique property of the SVD transform is that the potential $N^2$ degrees of freedom or samples in the original image now get mapped into [1]:

- $S \Rightarrow N$ Degrees of freedom
- $U \Rightarrow N(N-1) / 2$ Degrees of freedom
- $V \Rightarrow N(N-1) / 2$ Degrees of freedom

Totaling $N^2$ degrees of freedom.
SVD is an optimal matrix decomposition technique in a least square sense that it packs the maximum signal energy into as few coefficients as possible. It has the ability to adapt to the variations in local statistics of an image [12].

2.2 SVD Example

As an example to clarify SVD transformation, suppose 

\[
A = \begin{bmatrix}
12 & 23 & 17 \\
34 & 11 & 25 \\
18 & 53 & 29
\end{bmatrix}
\]

If SVD operation is applied on this matrix, then the matrix A will be decomposed into equivalent three matrices as follows:

\[
U = \begin{bmatrix}
-0.3970 & 0.0600 & -0.9158 \\
-0.4667 & -0.8724 & 0.1452 \\
-0.7903 & 0.4851 & 0.3744
\end{bmatrix}
\]

\[
S = \begin{bmatrix}
77.9523 & 0 & 0 \\
0 & 27.5619 & 0 \\
0 & 0 & 1.3349
\end{bmatrix}
\]

\[
V = \begin{bmatrix}
-0.4472 & -0.7332 & 0.5122 \\
-0.7203 & 0.6347 & 0.2798 \\
-0.5303 & -0.2439 & -0.8120
\end{bmatrix}
\]

Here diagonal elements of matrix \( S \) are singular values and we notice that these values satisfy the non increasing order: \( 77.9523 \geq 27.5619 \geq 1.3349 \).

2.3 Properties of SVD

Generally a real matrix \( A \) has many SVs, some of which are very small, and the number of SVs which are non-zero equals the rank of matrix \( A \) [3]. SVD has many good mathematical characteristics. Using SVD in digital image processing has some advantages [5, 11]:

i) The size of the matrices from SVD transformation is not fixed and can be a square or a rectangle.

ii) The SVs (Singular Values) of an image have very good stability, i.e. when a small perturbation is added to an image, its SVs do not vary rapidly;

iii) SVs represent algebraic image properties which are intrinsic and not visual.

As for example, figure 2.1(a) and 2.1 (b) show an image and the same image after Gaussian blur of size 9x9 respectively. The highest five singular values of the original image and the
Gaussian blurred image are presented in the table which clearly shows that the singular values are almost same i.e. the changes in the singular values are very small which demonstrate the good stability of the singular values of an image even after the manipulation on the image.

![Original lena image](image1.png) ![Gaussian blurred image](image2.png)

Figure 2.1: Original and Gaussian blurred image

<table>
<thead>
<tr>
<th></th>
<th>Original image</th>
<th>Gaussian blurred image</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>125.5664</td>
<td>125.5488</td>
</tr>
<tr>
<td></td>
<td>20.9847</td>
<td>20.9291</td>
</tr>
<tr>
<td></td>
<td>16.1572</td>
<td>16.0495</td>
</tr>
<tr>
<td></td>
<td>12.8285</td>
<td>12.7591</td>
</tr>
<tr>
<td></td>
<td>11.6343</td>
<td>11.5090</td>
</tr>
</tbody>
</table>

Table 2.1: Singular values of two images

Zhou et al. [20] has presented an analysis of the effects of ordinary geometric distortions on the singular values of an image:

- **Transpose**: Every real matrix \( A \) and its transpose \( A^T \) have the same non-zero singular values.
- **Flip**: \( A \), row-flipped \( A_{rf} \), and column-flipped \( A_{cf} \) have the same non-zero singular values.
- **Rotation**: \( A \) and \( A_r \) (\( A \) rotated by an arbitrary degree) have the same non-zero singular values.
- **Scaling**: \( B \) is a row-scaled version of \( A \) by repeating every row for \( L_1 \) times. For each non-zero singular value \( \lambda \) of \( A \), \( B \) has \( \sqrt{L_1 \lambda} \). \( C \) is a column-scaled version of \( A \) by repeating every column for \( L_2 \) times. For each non-zero singular value \( \lambda \) of \( A \), \( C \) has \( \sqrt{L_2 \lambda} \). If \( D \) is row-scaled by \( L_1 \) times, and column-scaled by \( L_2 \) times, for each non-zero singular value \( \lambda \) of \( A \), \( D \) has \( \sqrt{L_1 L_2 \lambda} \).
• Translation: $A$ is expanded by adding rows and columns of black pixels. The resulting matrix $A_e$ has the same non-zero singular values as $A$. Because of these properties, SVD may be used as a tool to develop semi-blind watermarking schemes.

Due to these properties of SVD, in the last few years several watermarking algorithms have been proposed based on this technique. The main idea of these approaches is to find the SVD of a cover image and then modify its singular values to embed the watermark. Some SVD-based algorithms are purely SVD-based in a sense that only SVD domain is used to embed watermark into image. Recently some hybrid SVD-based algorithms have been proposed where different types of transforms domain including Discrete Cosine Transform, Discrete Wavelet Transform, Fast Hadamard Transform etc. have been used to embed watermark into image.
Chapter Three

Problem Definition and Goals

In a previous chapter different types of applications of image watermarking have been discussed where it has been pointed that all watermarking schemes have some common requirements and some especial criteria are required depending on the type of application these schemes are developed for.

3.1 Criteria of Effective Watermarking

In order to be effective, digital watermark must be robust, recoverable from a document, provide the original information embedded reliably, be non-intrusive and also removable by authorized users. Robust watermarks are those which are difficult to remove from the object in which they are embedded despite a variety of possible attacks by pirates including compression such as JPEG, scaling and aspect ratio changes, rotation, translation, cropping, row and column removal, addition of noise, filtering, cryptographic and statistical attacks, as well as insertion of other watermarks.

3.2 RST Invariant Watermarking

Numerous types of watermarking schemes have been developed so far for different purposes, but no single algorithm has been proved effective and resilient to all types of attacks. Main focus of the watermarking algorithms now is to make it as robust as it can be. Up to now most of the watermarking schemes are not very robust to geometric attacks like rotation, scaling and translation which are called RST attacks in brief. Geometrical distortion can be global or local. Global geometrical distortion affects all the pixels of an image in same manner, while local geometrical distortion affects different portion of an image in different manner. Recently much attention has been paid to make the watermarking algorithms RST invariant i.e. to develop algorithms that can resist RST attacks efficiently because it has been shown that even very small geometric distortions can make the detection of a watermark very difficult or even impossible.

3.3 RST Transformations

Here basic theories of rotation, scaling and translation have been described briefly:

Translation: A translation (or shift) is applied to an image by repositioning it along a straight-line path from one coordinate location to another [22]. A two-dimensional point is translated by adding translation distances, \( x_0 \) and \( y_0 \), to the original coordinate position \( (x, y) \) to move the point to a new position \( (x', y') \).
\[ x' = x + x_0 \]
\[ y' = y + y_0 \]

The translation distance pair \((x_0, y_0)\) is called a translation vector or shift vector.

**Rotation:** A two-dimensional rotation is applied to an image by repositioning it along a circular path in the \(x\ y\) plane. Transformation equations for rotating a point at \((x, y)\) are obtained through an angle \(\varphi\) about the origin clockwise:

\[ x' = x \cos \varphi + y \sin \varphi \]
\[ y' = -x \sin \varphi + y \cos \varphi \]

**Scaling:** A scaling transformation changes the size of an image. We can get the transformation equations by multiplying the coordinate values \((x, y)\) by scaling factors \(a\) and \(b\) to produce the transformed coordinates \((x', y')\):

\[ x' = x \cdot a \]
\[ y' = y \cdot b \]

Scaling factor \(a\) scales images in the \(x\) direction, while \(b\) scales in the \(y\) direction. When \(a\) and \(b\) are assigned the same value, a uniform scaling is produced that maintains relative image proportions.

### 3.4 RST and Other Attacks on Image

In order to demonstrate RST and other attacks on image, original ‘lena’ image (figure 3.1) and attacked image are shown here (table 3.1).

**Figure 3.1:** Original image

| Gaussian Blur | Gaussian noise 0.3 | JPEG compression 30:1 |
Except these attacks there are some other attacks which can destroy or at least distort embedded watermarks. So the problem is to make the watermarking algorithm resistant to these attacks.
3.5 Goal of this Thesis

Objective of this thesis is to develop or modify any existing image watermarking algorithm such that it can resist most of these attacks especially RST attacks efficiently which is currently not resilient to RST attacks. Here emphasis will be on to enhance the resilience against RST attacks but concurrently other attacks will be considered as well.
Chapter Four

Literature Review

In the last few years, numerous schemes have been developed for image watermarking using different types of algorithms. SVD based algorithms are of two types: pure SVD based and hybrid SVD based. In case of pure SVD based algorithms, watermark is embedded in the SVD domain only whereas in hybrid SVD based algorithms, watermark is embedded in the SVD and transform domain. Among them, several algorithms based on SVD have been investigated in this chapter.

4.1 Pure SVD based algorithms

There are two types of pure SVD based algorithms where in some watermarking schemes watermark is embedded into the whole cover image and in some other schemes the cover image is divided into several blocks and the watermark is embedded into each block of the cover image separately.

4.1.1 Non block based algorithms

Many of the earlier algorithms, based on SVD, used to embed the watermark signal directly into the SVD domain. Liu and Tan [1] proposed an algorithm where the watermark image is embedded directly in the SVD domain. A single image is used as watermark which is embedded in the whole image. This algorithm is blind but requires the singular values to or the orthogonal matrices for retrieving the watermark. This algorithm is resistant to some of the attacks like compression, filtering, cropping etc. but is not robust against the attacks including rotation and translation.

In [21], a method based on SVD has been proposed by Liu and Kong. This algorithm uses basic M-sequence as the watermark. Considering the visible quality and robustness criteria, watermark has been embedded in middle singular values maintaining the original order. This algorithm is blind i.e. does not require the original image or any other information of original singular values to detect the watermark. This method can resist some attacks like JPEG compression, median filtering, rescaling, Gaussian low-pass filtering but is not robust against some other attacks including rotation, cropping etc.

4.1.2 Block-based algorithms
An optimal SVD-based watermarking scheme has been proposed by Ganic et al. [9] where the watermark is embedded twice. In the first layer, the cover image is divided into smaller blocks and a piece of the watermark is embedded in each block. The cover image is used as a single block to embed the whole watermark in the second layer. Layer 1 allows flexibility in data capacity and Layer 2 provides additional robustness to attacks. This scheme can resist several attacks including JPEG compression, JPEG 2000, Gaussian blur, Gaussian noise, cropping, rotation and rescaling but after each attack visual quality of the image degrades and the commercial value of the image is lost. In case of rotation operation, small angle has been tested only and this scheme is not robust against translation operation also.

In [6], a SVD based scheme has been proposed by Ghazi et al. where the original image is divided into blocks and then the watermark is embedded in the singular values of each block separately. The watermark can be a pseudo random number or an image. This method is robust against several attacks such as JPEG compression, Gaussian noise, Gaussian blur, cropping, resizing and rotation, though for rotation operation a small angle has been tested and the correlation value for rotation and resizing is not good. This algorithm is not resistant to translation operation.

Zhou et al. [5] has presented an algorithm where the original image is divided into several blocks of size $8 \times 8$ for each block and the watermark is embedded in the SVD domain of each block of the image. Embedded watermark may be binary image, pseudorandom number or gray scale image. If the cover image size is not exactly divisible by 8, then it requires adjustment before embedding of watermark. Experimental result shows that the algorithm is resistant to JPEG compression, noise, filtering, clipping and rotation. Similarity of the original watermark image and the extracted watermark image has been evaluated using the value of correlation coefficient which is not very satisfactory in case of rotation operation. Moreover the algorithm can’t resist scaling and translation operation.

4.2 SVD and transforms domain based algorithms

SVD based algorithms discussed so far are pure SVD based algorithms because in those algorithms watermark is embedded in SVD domain of the cover image. Some algorithms have used different types of transform domain along with SVD domain for watermarking scheme which can be defined as hybrid SVD based algorithm. In this section this type of algorithms will be explored.

4.2.1 SVD and DCT based algorithm

A hybrid method based on DCT and SVD has been proposed by Sverdlov et al. [4]. First, applying the DCT to the whole cover image DCT coefficients are mapped to the four quadrants using the zig zag sequence and then SVD is applied to each quadrant. These four quadrants actually represent frequency bands from the lowest to the highest. Singular values
of the DCT-transformed visual watermark are then used to modify the singular values of each quadrant of the cover image. In this paper, the cover image has been divided into four blocks and as a result the size of the visual watermark is one quarter of the size of the cover image. It has been shown that embedding data in lowest frequencies is resilient to one set of attacks while embedding data in highest frequencies is resilient to another set of attacks. Robustness of this algorithm has been tested against a set of attacks including Gaussian blur, Gaussian noise, JPEG compression, JPEG 2000 compression, rescaling, cropping, histogram equalization, gamma correction etc. Robustness against rotation operation is not very satisfactory which has been reflected by the value of correlation coefficient. This algorithm is not resistant to translation operation.

4.2.2 SVD and DWT based algorithm

A SVD based algorithm using DWT has been presented by Ganic and Eskicioglu [2] which is very similar to the algorithm of Sverdlov et al.[4] discussed previously. The cover image is first decomposed by using DWT into four sub bands and SVD is applied to each sub band image. SVD is then applied on the watermark image and the singular values of the cover image are modified with the singular values of the watermark image. Finally four sets of DWT coefficients are obtained and applying the inverse DWT using the modified DWT coefficients, watermarked image is produced. Robustness of this algorithm has been tested against a set of attacks including Gaussian blur, Gaussian noise, JPEG compression, JPEG 2000 compression, rescaling, cropping, histogram equalization, gamma correction etc. Extracted watermarks from each sub band and the corresponding values of Pearson correlation coefficient with the original watermark image have been reported which shows that extracted watermark from the LL band is the best in visual quality and correlation value. Performance of this algorithm against sharpening, contrasting and histogram equalization is not very good.

4.2.3 SVD and FHT based algorithm

Fast Hadamard Transform (FHT) has been used in a SVD based algorithm presented by Abdallah et al. [10]. This algorithm first divides the cover image into blocks and applies FHT to each block. Then SVD is applied to the watermark image and distributes the singular values of the visual watermark image over the transformed cover blocks. Main features of the algorithm are simplicity, flexibility in data embedding capacity and real time implementation. Robustness of this scheme has been tested against several attacks including Gaussian blur, Gaussian noise, cropping, histogram equalization, gamma correction, sharpening, resizing and rotation. Translation attack has not been considered here, which is an indication of vulnerability of this algorithm against this attack.
4.2.4 SVD and Zernike moments based algorithm

Li et al. [8] has proposed a SVD based watermarking scheme where Zernike moments are used to estimate the rotation angle to make the algorithm rotation invariant. Here also the cover image is divided into blocks and SVD is applied to each image block. This algorithm is robust to rotation for even large angle, scaling and pixel removal attacks. Visual quality of the watermarked image has been measured by Weighted Peak Signal-to-Noise Ratio (WPSNR) and similarity of the original and extracted watermark image has been evaluated by Normalization Correlation.
Chapter 5

Proposed Watermarking Scheme

This chapter discusses the developed watermarking schemes. First, short background of the proposed scheme has been presented and then the detailed scheme has been described.

5.1 Developed Watermarking Scheme

While reviewing number of watermarking schemes based on SVD, it has been noticed that some algorithms are purely SVD based and some others are hybrid SVD based that use different types of transforms domain for embedding watermark. In general, hybrid SVD based algorithms show better performance than the pure SVD based algorithms but most of these algorithms are not truly RST invariant because most of these schemes are not tested against large angle rotation attack and no SVD based algorithm has been found robust to translation attack. Among the hybrid based schemes, Sverdlov et al. [4] has proposed an algorithm where Discrete Cosine Transform (DCT) has been used with SVD for embedding watermark. Experimental results against different types of attacks have been discussed in this paper where it is clear that this algorithm suffers from the lack of robustness against rotation, scaling and translation attacks. It has been tested against rotation attack but the angle is only 20° and it has not mentioned anything about translation attack. In this thesis, a watermarking scheme has been developed which is actually a modification of the algorithm proposed by Sverdlov et al. [4].

In this developed algorithm watermark is embedded in frequency domain. In all frequency domain watermarking schemes, there is a conflict between robustness and transparency. If the watermark is embedded in perceptually most significant components, the scheme would be robust to attacks but it would be difficult to hide the watermark. On the other hand, if the watermark is embedded in perceptually insignificant components, it would be easier to hide the watermark but the scheme may be less resilient to attacks [2]. This watermarking scheme uses DCT and SVD for embedding watermark. The watermark is a grayscale image. This is a block based algorithm i.e. the cover image is divided into blocks.

A recent paper [13] on DWT-based multiple watermarking claims that embedding a visual watermark in both low and high frequencies results in a robust scheme that can resist to different kinds of attacks. Embedding in low frequencies increases the robustness with
respect to attacks that have low pass characteristics like filtering, lossy compression, and geometric distortions while making the scheme more sensitive to modifications of the image histogram, such as contrast/brightness adjustment, gamma correction, and histogram equalization. Watermarks embedded in middle and high frequencies are typically less robust to low-pass filtering, lossy compression and small geometric deformations of the image but are highly robust with respect to noise adding, and nonlinear deformations of the gray scale. Considering these complimentary advantages and disadvantages, four same visual watermarks are embedded in one image in four sub bands.

Two-dimensional DCT transformation is applied to the whole image but frequency coefficients need to be mapped from the lowest to the highest in a zig-zag order to 4 quadrants (figure 5.1) in order to apply SVD to each block. All the quadrants will have the same number of DCT coefficients. For example, if the cover image is 256x256, the number of DCT coefficients in each block will be 16,384. I label these blocks B1, B2, B3, B4. This process is depicted in Figure 1. The DCT coefficients with the highest magnitudes are found in quadrant B1, and those with the lowest magnitudes are found in quadrant B4. Correspondingly, the singular values with the highest values are in quadrant B1, and the singular values with the lowest values are in quadrant B4. The largest singular values in quadrants B2, B3, and B4 have the same order of magnitude. So, instead of assigning a different scaling factor for each quadrant, I have used only two values: One value for B1, and a smaller value for the other three quadrants.

![Figure 5.1: Mapping of DCT coefficients to four blocks](image)

5.2 Steps of the algorithm

Unlike most watermarking schemes, this algorithm also consists of three steps: Embedding watermark, Preprocessing before extraction and Extraction of watermarks.

5.2.1 Embedding of watermark:

Watermark embedding consists of the following steps:

1. Apply DCT to the whole cover image \( A \) and map the DCT coefficients into 4 quadrants: B1, B2, B3, and B4 using the zig-zag sequence.
2. Apply SVD to each quadrant: \( A^k = U^k A^k S^k V^k \), \( k = 1,2,3,4 \) where \( k \) denotes B1, B2, B3,
and B4 quadrants.

3. Apply DCT to the whole visual watermark $W$ and then apply SVD to the DCT-transformed visual watermark $W$:
   \[ W = U_W \Sigma_W V_W^T. \]

4. Modify the singular values in each quadrant $B_k$, $k = 1,2,3,4$, with the singular values of the DCT-transformed visual watermark:
   \[ \lambda_i^{*k} = \lambda_i^k + \alpha_k \lambda_{wi}, \quad i = 1,\ldots,n, \]
   where $\lambda_i^k$, $i = 1,\ldots,n$ are the singular values of $\Sigma_A$, and $\lambda_{wi}$, $i = 1,\ldots,n$ are the singular values of $\Sigma_W$.

5. Find the 4 sets of modified DCT coefficients:
   \[ A^{*k} = U^k \Sigma^{*k}_A V^k_A, \quad k = 1,2,3,4. \]

6. Map the modified DCT coefficients back to their original positions.

7. Apply the inverse DCT to produce the watermarked cover image.

### 5.2.2 Preprocessing Before Extraction

This step enhances the robustness against rotation and adds resistance to translation attack of the watermarked image. This preprocessing requires following tasks to be followed:

1. Get the size $n \times n$ of the matrix representing the watermarked image.
2. If $n$ is odd, $n = n + 1$
3. Check the values in the whole matrix of the watermarked image for NaN (not a number), Inf (infinity) and –Inf (negative infinity).
4. Replace the NaN, Inf and –Inf values with zero (0).

### 5.2.3 Extraction of Watermarks:

1. Apply the DCT to the whole watermarked cover image $A^*$ and map the DCT coefficients into 4 quadrants: B1, B2, B3, and B4 using the zig-zag sequence.
2. Apply SVD to each quadrant: $A^{*k} = U^k \Sigma^{*k}_A V^k_A$, $k = 1,2,3,4$, where $k$ denotes the attacked quadrants.
3. Extract the singular values from each quadrant $B_k$, $k = 1,2,3,4$:
   \[ \lambda_{wi}^k = (\lambda_i^{*k} - \lambda_i^k)/\alpha_k, \quad i = 1,\ldots,n. \]
4. Construct the DCT coefficients of the four visual watermarks using the singular vectors:
   \[ W_k = W_k = U^k \Sigma^k_W V^k_W, \quad k = 1,2,3,4. \]
5. Apply the inverse DCT to each set to construct the four visual watermarks.
5.3 Enhanced Robustness Due to the Preprocessing

Applying rotation attack on watermarked image increases the size of the matrix which causes problem to divide the matrix into four blocks. As for example, if the size of the watermarked image is $256 \times 256$, $45^\circ$ rotation makes the matrix $365 \times 365$ and as $365$ is odd, the resulting matrix cannot be divided into four matrix. Increasing the dimension of the matrix by one row and one column makes the matrix $366 \times 366$ and it can be divided into four blocks where size of each block is $183 \times 183$.

Translation attack on watermarked image produces blank spaces where the corresponding values in the matrix are –Inf (negative infinity) which prevents applying SVD on that matrix and consequently watermark image cannot be extracted. Here the whole matrix is checked for these values and are replaced by zero(0) which makes the matrix suitable for applying SVD and results in the successful extraction of the watermark image.
Chapter 6

Analysis of Experimental Results

This chapter is for describing the conducted experiment and evaluating the results with comparison to an existing watermarking scheme.

6.1 Conducted Experiment

This watermarking scheme is RST invariant due to its robustness against rotation, translation and scaling attacks. Moreover it is resilient to many other attacks including Gaussian Blur, Gaussian noise, JPEG compression, histogram equalization etc. The cover image used in this experiment is ‘lena.jpg’ (figure 6.1(a)) of size 256 × 256 and the watermark image is ‘scene.jpg’ (figure 6.1(b)) of the same size. This algorithm has been implemented using MATLAB (Release 14). Now- a- days most of the watermarking schemes are implemented using MATLAB.

![Original cover Image](image1.png) ![Original watermark image](image2.png)

Figure 6.1: Original cover image and watermark image

According to the algorithm the cover image is divided into four blocks and the watermark image is embedded in each block. Before embedding, the watermark image is reduced to half of its actual size to fit in each block of the cover image. In the extraction phase, all four watermark images from each block is extracted. Quality of the extracted watermark is evaluated visually and using the Pearson correlation coefficient between the original watermark image and extracted watermark image from each block. Pearson correlation coefficient is calculated using the original vector of singular values and extracted vector of singular values for each quadrant. The Pearson product moment correlation coefficient is a dimensionless index that ranges from
-1.0 to 1.0, and reflects the extent of a linear relationship between two data sets which are two images in this case.

6.2 Resilience against Attacks

This watermarking scheme has been tested against several attacks including rotation, scaling, translation, Gaussian Blur, Gaussian noise, JPEG compression, histogram equalization etc. Table 6.1 shows the watermarked image after different attacks and corresponding extracted watermark images and the value of Pearson correlation coefficient.

<table>
<thead>
<tr>
<th>Watermarked Image after</th>
<th>Extracted watermark image</th>
<th>correlation</th>
</tr>
</thead>
<tbody>
<tr>
<td>Gaussian blur 9 × 9</td>
<td></td>
<td>0.9976</td>
</tr>
<tr>
<td>Gaussian noise 0.3</td>
<td></td>
<td>0.9841</td>
</tr>
<tr>
<td>JPEG compression</td>
<td></td>
<td>0.9994</td>
</tr>
<tr>
<td>Watermarked Image after histogram equalization</td>
<td>Extracted watermark Correlation= 0.9711</td>
<td></td>
</tr>
<tr>
<td>---------------------------------------------</td>
<td>------------------------------------------</td>
<td></td>
</tr>
<tr>
<td><img src="image1.png" alt="Image" /></td>
<td><img src="watermark1.png" alt="Watermark" /></td>
<td></td>
</tr>
<tr>
<td>Watermarked Image for 30° angle rotation</td>
<td>Extracted watermark Correlation= 0.7785</td>
<td></td>
</tr>
<tr>
<td><img src="image2.png" alt="Image" /></td>
<td><img src="watermark2.png" alt="Watermark" /></td>
<td></td>
</tr>
<tr>
<td>Watermarked Image for 75° angle rotation</td>
<td>Extracted watermark Correlation= 0.8429</td>
<td></td>
</tr>
<tr>
<td><img src="image3.png" alt="Image" /></td>
<td><img src="watermark3.png" alt="Watermark" /></td>
<td></td>
</tr>
<tr>
<td>Watermarked Image for 135° angle rotation</td>
<td>Extracted watermark Correlation= 0.8047</td>
<td></td>
</tr>
<tr>
<td><img src="image4.png" alt="Image" /></td>
<td><img src="watermark4.png" alt="Watermark" /></td>
<td></td>
</tr>
</tbody>
</table>
Table 6.1: Extracted watermarks and value of correlation coefficient for different attacks

From the figures and correlation value presented in the above table it evident that the watermarking scheme is RST invariant because it can resist rotation, scaling and translation attacks. The scheme has been tested for large values of angle for rotation and large value for scaling which are the improvements over the existing algorithm.

Table 6.2 shows the values of Pearson correlation coefficient of the method proposed by Sverdlov et al. and the developed method. Most of the values of the developed method are better than that of the method proposed by Sverdlov et al which clearly

<table>
<thead>
<tr>
<th>Attacks</th>
<th>Method proposed by Sverdlov et al.</th>
<th>Developed method</th>
</tr>
</thead>
<tbody>
<tr>
<td>Gaussian Blur</td>
<td>0.9894</td>
<td>0.9976</td>
</tr>
<tr>
<td>Gaussian Noise</td>
<td>0.9942</td>
<td>0.9841</td>
</tr>
<tr>
<td>JPEG compression</td>
<td>0.9998</td>
<td>0.9994</td>
</tr>
<tr>
<td>Histogram Equalization</td>
<td>0.9148</td>
<td>0.9711</td>
</tr>
<tr>
<td>Rescaling (256→128→256)</td>
<td>0.9957</td>
<td>1.0</td>
</tr>
<tr>
<td>Rotation 20°</td>
<td>0.7617</td>
<td>0.8366</td>
</tr>
<tr>
<td>Rotation 75°</td>
<td>Not done</td>
<td>0.8429</td>
</tr>
<tr>
<td>Rotation 135°</td>
<td>Not done</td>
<td>0.8047</td>
</tr>
<tr>
<td>Scaling 200%</td>
<td>Not done</td>
<td>0.9966</td>
</tr>
<tr>
<td>Translation to 25, 35</td>
<td>Not done</td>
<td>0.6181</td>
</tr>
</tbody>
</table>

Table 6.2: Values of correlation coefficient of two methods.
shows the improvement over the existing algorithm. The existing algorithm can resist rotation attack only for a small angle whereas the developed algorithm is resilient against rotation for large values of angle. Moreover the developed algorithm can resist scaling and translation attacks successfully from which it can be considered a RST invariant algorithm for watermarking.
Chapter 7

Conclusion

There are several types of algorithms for watermarking. Each type of algorithms has its own advantages and limitations. No method can provide fully perfect solution. Each type of solution has robustness to some type of attacks but is less resilient to some other types of attacks. Main focus of the current research in this field is to make the watermarking algorithms resilient to geometric transformations. In case of practical application, choice of solution type actually depends on the nature of application and requirements. SVD based watermarking is relatively a young field and not that much work has been done so far. Most of the SVD based algorithms are less resilient to geometric distortion including rotation, scaling and translation. So incorporating robustness against RST attacks in the SVD based algorithms is a recent trend of research now. It is not easy because if the techniques for enhancing resilience to RST attacks increase the possibility to make the algorithms less resilient to other usual attacks, then it is not acceptable. Here I have studied several SVD based algorithms and analyzed their relative advantages and limitations. Some of the SVD based algorithms are pure SVD based whereas some others have used different types of transforms in order to enhance the robustness against different types of attacks. Among these transform and SVD based algorithms, I have developed here DCT based algorithm using SVD.

My actual contribution is a modification in an already existing watermarking scheme which has eliminated some of the limitations of this algorithm. Watermarking scheme proposed by Sverdlov et al. [4] has limited robustness against rotation attack and no resilience against scaling and translation attacks which are considered very significant attacks against any watermarking scheme. Here an extra phase has been added as a preprocessing step before the watermark extraction which actually prepares the watermarked image such a way that can resist large angle rotation, scaling and translation attacks. Hence this watermarking scheme can be considered RST invariant.

7.1 Scopes for Future Works

Still there are scopes to improve this work. Though this watermarking scheme is resilient against translation, but the value of correlation coefficient is not very good which I think is a point for further improvement.

For most of the attacks, extracted watermarks from four quadrants are not of the same quality. In most cases, one or two are of the same order of quality due to the different scaling
factors for four quadrants. I think it will be a good idea to devise an algorithm to set the scaling factor for all blocks. In future, I have the plan to work on this point.
References


