Image Processing Final Project Report:
Image Watermarking

葉偉良	林奕君	彭思安	安本林
L091189	309540009	0616110	0616336

1. INTRODUCTION

1.1 Image Watermarking

In recent times, due to the great developments in computer and internet technology, some of the online images are watermarked to protect images from illegal copying, modifying, and redistributing multimedia data. Copyright protection, data authentication, covert communication, and content identification can be achieved by watermarking.

An image watermark is a pattern of bits inserted into a digital that identifies the file copyright information. The bits representing the watermark must be scattered throughout the image in such a way that they cannot be identified or manipulated.

As shown in Figures 1 and 2, the image watermark can be roughly divided into two types: visible and invisible watermarks.

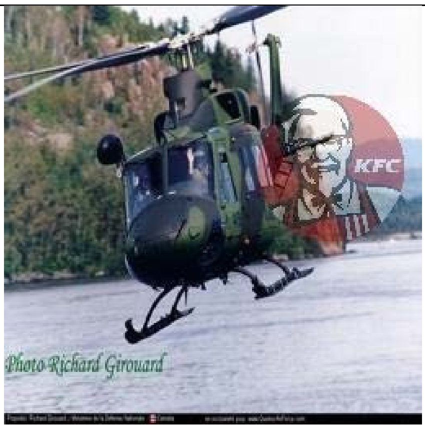
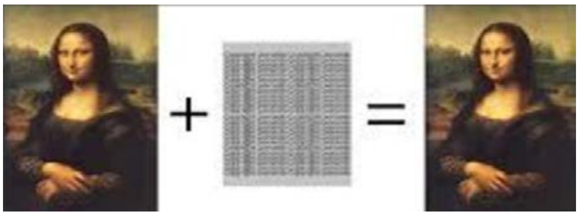
	

Figure 1. Visible Watermark	Figure 2. Invisible Watermark

1.2 History of Image Watermark

The term "watermark" probably originated from the German term "wassermarke", which means the marks resemble the effect of water on paper. The first watermarks appeared in Italy during the 13th century, but their use rapidly spread across Europe. By the 18th century, watermarks on paper in Europe and America had been used as trademarks, to record the manufactured date, or to indicate the size of original sheets. Watermarks continue to be used today as manufacturer's marks and to prevent forgery.

1.3 Applications of Image Watermark

A. Copyright Protection

The copyright information can be embedded as a watermark into the new production. Once there is a dispute on the ownership, the watermark can be extracted to provide evidence of who is the owner of this product.

B. Content Authentication

The watermark is embedded to detect if the images have been modified or not, this process can be used for authentication.

C. Owner Identification

To achieve owner identification, there was a traditional form for intellectual ownership verification which was a visual mark. However, nowadays, this is easily overcome by the use of some software that modifies images. For example, the images with the copyright registration symbol c which has this mark are removed by specialized software. To solve this problem, invisible watermarks are used to overcome the problem.

D. Fingerprinting

The main purpose of fingerprinting is to protect customers. If someone got a legal copy of a product but redistributed it illegally, fingerprinting can prevent this. This can be achieved by tracing the whole transaction by embedding a unique robust watermark for each recipient. Thus, the owner can identify who redistributed this product by extracting the watermark from the illegal copy.

E. Copy Control

The watermark contains owner data and specifies the corresponding amount of copies allowed. This presupposes hardware and software for updating the watermark whenever it has been used. It also provides copy tracking for unauthorized distribution since the owner of data is embedded in the watermark.

2. LIFE CYCLE PHASES

As shown in Figure 3, a watermarking system is usually divided into three distinct steps:

1. Embedding Phase
2. Distortion Phase
3. Detection Phase

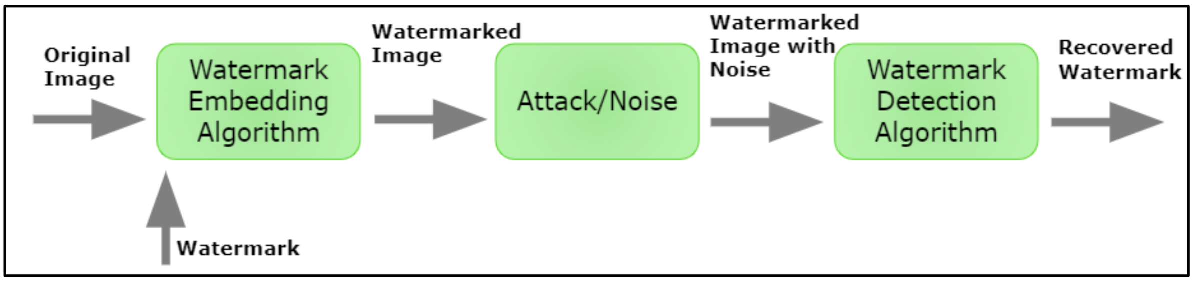

Original Image
Watermark Embedding Algorithm
Watermarked Image
Attack/Noise
Watermarked Image with Noise
Watermark Detection Algorithm
Recovered Watermark
Watermark

Figure 3. Life Cycle of Image Watermarking

2.1 Embedding Phase

An embedding algorithm and a secret key are used for embedding the watermark in the original image and producing the watermarked image. The secret key used is to enforce the security of the watermark.

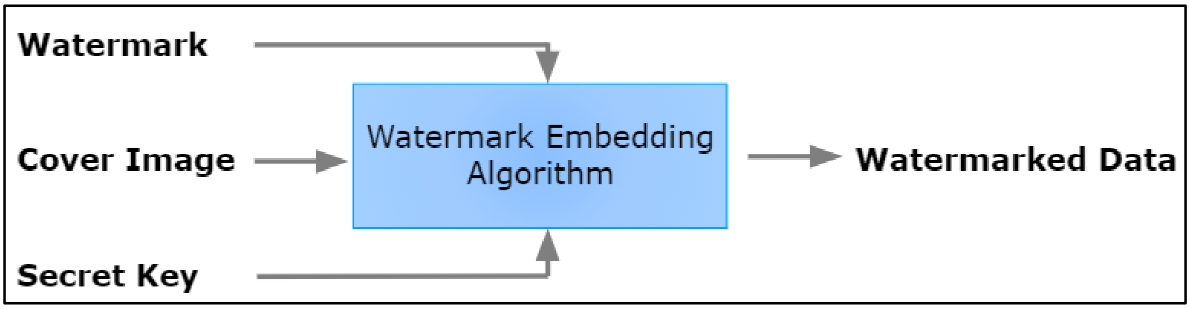


Figure 4. Embedding Phase

2.2 Distortion Phase

The watermarked image might be shared with another person. If this person makes a modification to the image, this is called an attack. The modification may not be malicious, it just aims to remove the watermark. There are many possible ways of attack, such as lossy compression of the image, cropping an image, or inserting noise.

2.3 Detection Phase

Detection algorithm and secret key are used to detect the watermark, even the noise added is also detected.

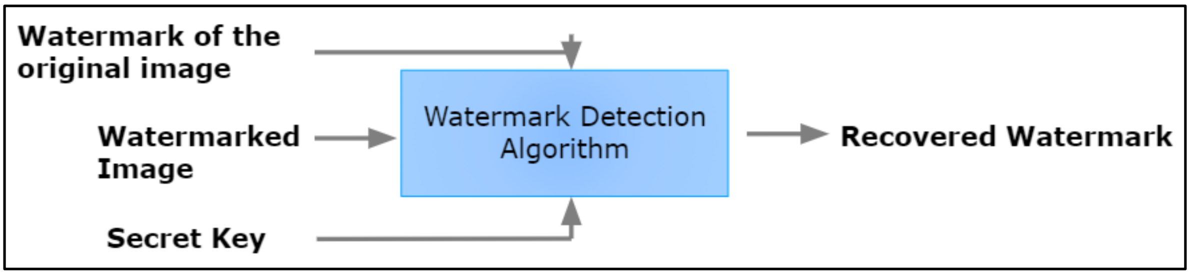

Watermark of the original image
Watermarked Image
Secret Key
Watermark Detection Algorithm
Recovered Watermark

Figure 5. Detection Phase

3. WATERMARKING TECHNIQUES

As shown in Figure, the watermarking techniques can be divided into two types depending on their domain: the spatial domain techniques and the frequency domain techniques.

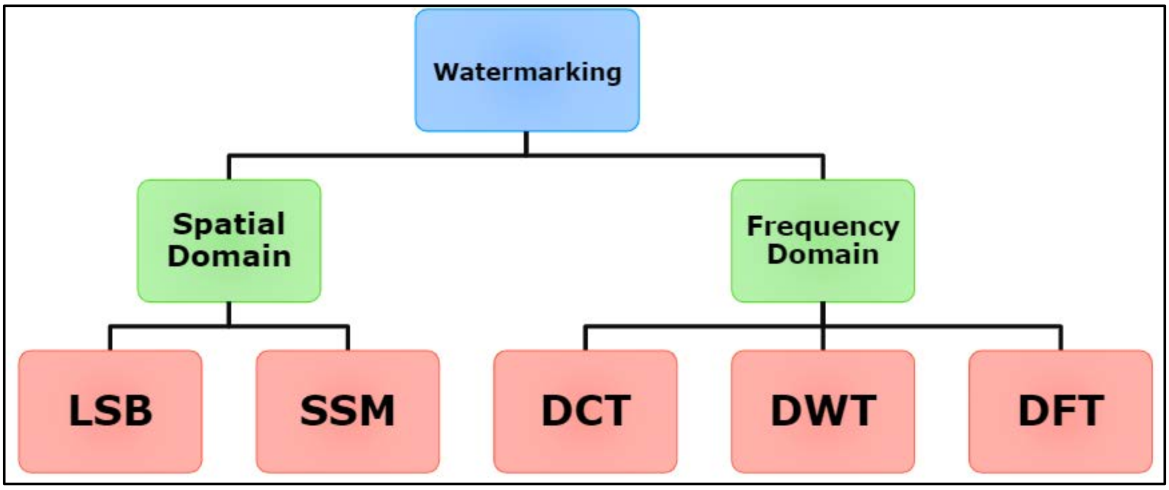


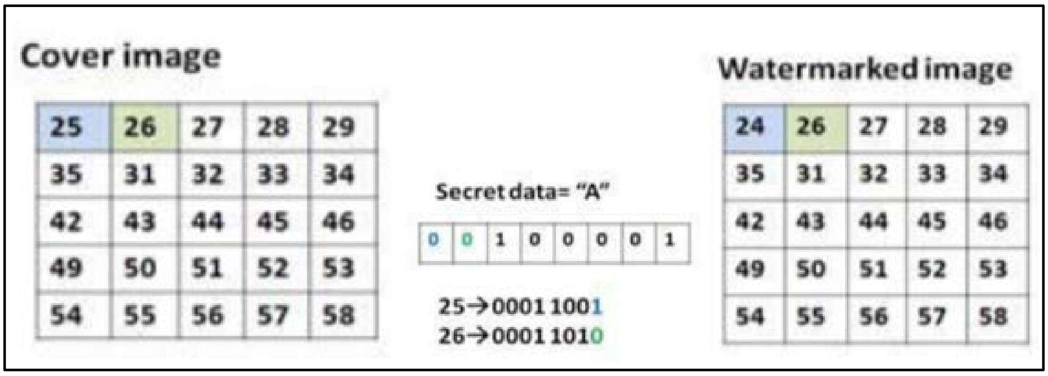
Figure 6. Watermarking Techniques

3.1 Spatial Domain Techniques

Spatial Domain Techniques involve changing the values, intensity and the color of selected pixel pixels in the image. Those techniques are used because of their simplicity, their low computational complexity and their rapidity.

3.1.1 Least Significant Bits (LSB)

The LSB technique might be the most popular among all spatial domain techniques. It requires changing the least significant bit of a selected pixel into the desired bit of watermark information. To illustrate, let’s consider the 5x5 cover image below into which we want to insert the secret data watermark “A”. The first 2 bits of the watermark will replace the least significant bit of the first two upper left pixels, resulting in a slight change of pixel values in the watermarked image.



Cover image

25	26	27	28	29
35	31	32	33	34
42	43	44	45	46
49	50	51	52	53
54	55	56	57	58

Secret data= “A”

0	0	1	0	0	0	0	1

25→0001 1001
26→0001 1010

Watermarked image

24	26	27	28	29
35	31	32	33	34
42	43	44	45	46
49	50	51	52	53
54	55	56	57	58

Figure 7. Least Significant Bit

3.1.2 Spread Spectrum Modulation (SSM)

SSM is another spatial domain technique with a slightly more complex algorithm than LSB. In this technique, the cover image undergoes a perceptual analysis that produces a perceptual mask of the image. The mask is multiplied by a pseudorandom sequence and the result is feeded to an SSM block, alongside a secret key and a discrete watermark message. The output is then added to the original image to produce the final watermarked image. SSM can be used over LSB because it produces better output images with data integrity, reduces noise, and the embedded watermark is harder to detect.

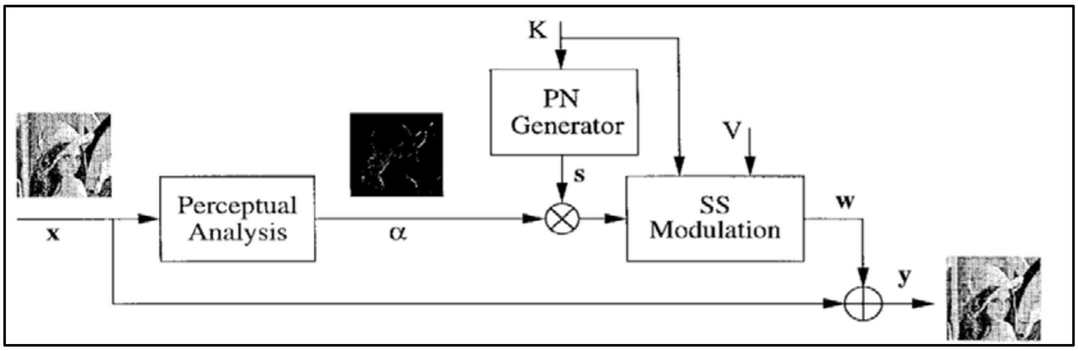


Figure 8. Spread Spectrum Modulation flowchart

3.2 Frequency Domain Techniques

Images can also be viewed as frequencies, since the intensity values repeat at a given frequency in an image. Contrast this to the spatial domain techniques, where the image is viewed as an array of values, and the frequency domain methods provide an entirely different view of the file system.

3.2.1 Discrete Cosine Transform (DCT)

The Discrete Cosine Transform remains a popular method not only of image watermarking, but also data compression. Similar to the Fourier Transform, which decomposes a signal into combinations of periodic functions, the DCT breaks a signal down into a combination of only cosine functions. The image is first split into blocks, (e.g. 8x8 subimages) and different frequency components are separated. Then the forward transform is applied to each block. Coefficients are selected and subsequently modified. These coefficients are embedded in such a way as to embed the actual watermark into the larger image.

3.2.2 Discrete Wavelet Transform (DWT)

The Discrete Wavelet Transform method splits the signal into high and low frequency sections. The low frequency sections are then further subdivided, and so on until the signal is entirely decomposed. The signals are further decomposed because most values live in the low frequency part of the signal. This method provided more pleasing results and is more robust than other compression methods, but it incurs a higher computational cost, as is common to frequency domain techniques.

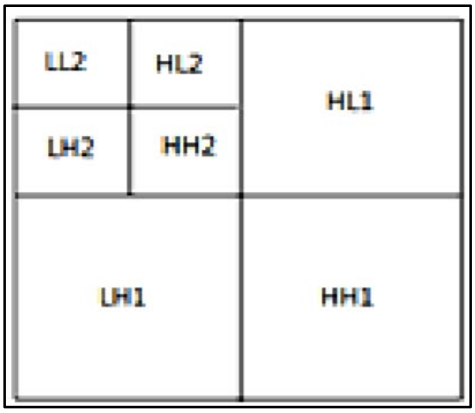


Figure 9. Subdividing the images in the discrete

3.2.3 Discrete Fourier Transform (DFT)

The Fourier methods involve decomposing a signal into a combination of sine and cosine functions. This transformation is more robust than others in the frequency domain against geometric attacks, which involve cropping, scaling, or otherwise distorting the image. We again wish to change the phase coefficients to embed the watermark. There are two types of DFT, direct embedding and template-based. In direct embedding, the magnitude and phase coefficients are directly modified. The template-based approach uses structures which are embedded in the frequency domain to find the appropriate transformation. The computational cost of DFT compared to other frequency domain techniques such as DCT means that in practice DFT is used less frequently.

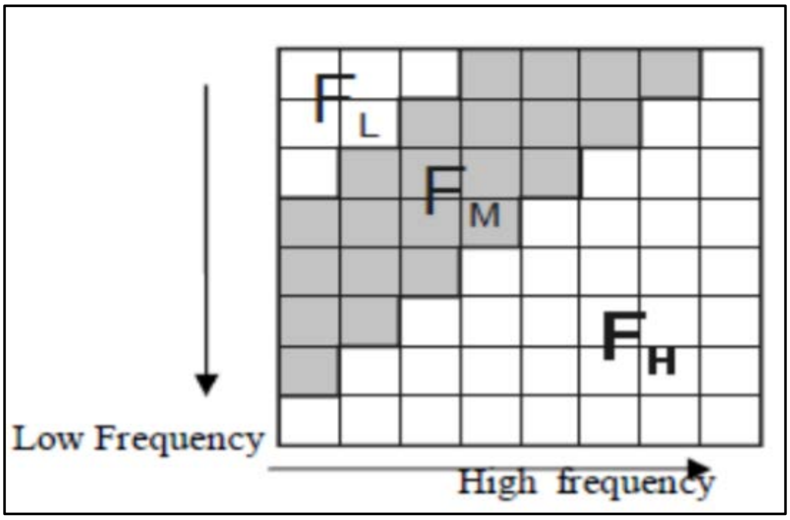
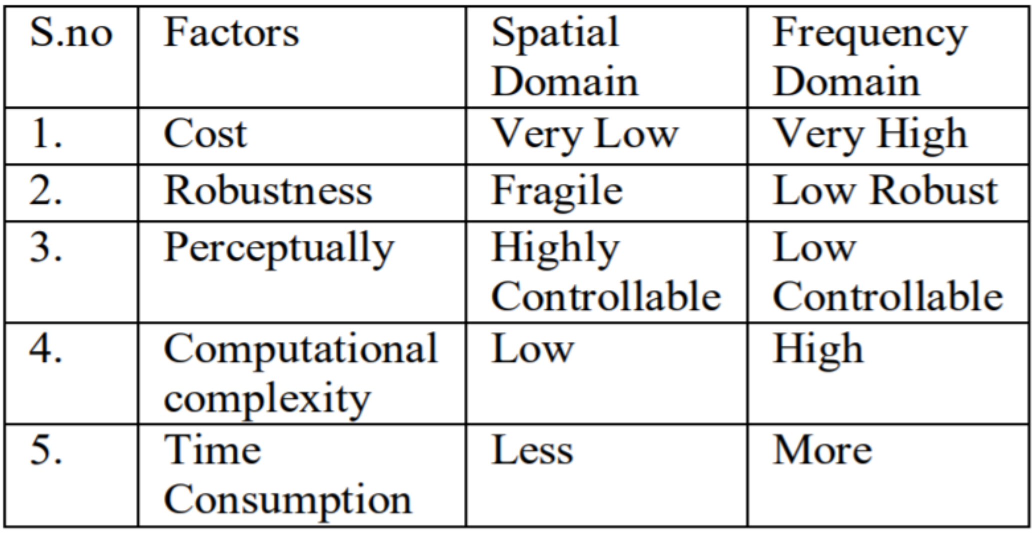


Figure 10. Splitting frequencies in a block into high frequency and low frequency components.

3.3 Comparisons between domains and techniques

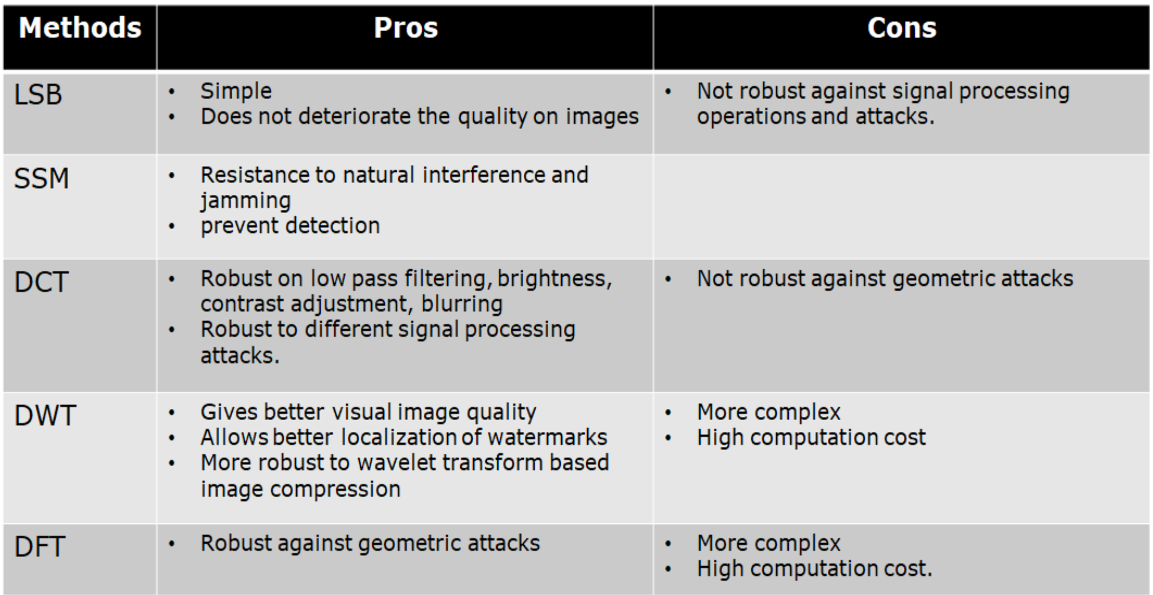


S.no	Factors	Spatial Domain	Frequency Domain
1.	Cost	Very Low	Very High
2.	Robustness	Fragile	Low Robust
3.	Perceptually	Highly Controllable	Low Controllable
4.	Computational complexity	Low	High
5.	Time Consumption	Less	More

Figure 11

In terms of computational cost and complexity, spatial domain techniques are more efficient than frequency domain, since it only involves computation in the spatial domain, whereas frequency domain techniques involve transforms into the frequency domain of an image and embedding watermarks in the spectral coefficients. However, in terms of robustness, frequency domain techniques are more resistant to attacks than spatial domain techniques.

Below figure explains in more detail the attacks the frequency domain techniques are more robust against and other details on their pros and cons.



Methods	Pros	Cons
LSB	• Simple • Does not deteriorate the quality on images	• Not robust against signal processing operations and attacks.
SSM	• Resistance to natural interference and jamming • prevent detection	
DCT	• Robust on low pass filtering, brightness, contrast adjustment, blurring • Robust to different signal processing attacks.	• Not robust against geometric attacks
DWT	• Gives better visual image quality • Allows better localization of watermarks • More robust to wavelet transform based image compression	• More complex • High computation cost
DFT	• Robust against geometric attacks	• More complex • High computation cost.

Figure x

4. CONCLUSIONS

This report focuses on different types and domains of image watermarking techniques. A common application requirement for the watermarks is that they resist attacks that would remove them. Some of the watermarks being attack-resistant may be accidentally removed by unintended attacks such as cropping or compression.

In addition, there is a trade-off between attack-resistant and computation efficiency. However, frequency-domain transformation methods are used widely in digital image compression and digital image watermarking for their robustness over spatial domain methods.

5. REFERENCES

[1] https://core.ac.uk/download/pdf/300420103.pdf
[2] https://www.slideshare.net/nafees321/digital-watermarking-10187496
[3] https://github.com/diptamath/DWT-DCT-Digital-Image-Watermarking/blob/master/paper.pdf
[4] https://www.slideshare.net/qaisarayub/watermarking-inimageprocessing
[5] https://www.slideshare.net/ankushkr007/digital-watermarking-15450208
[6] https://medium.com/swlh/lsb-image-steganography-using-python-2bbbee2c69a2
[7] https://www.pyimagesearch.com/2016/04/25/watermarking-images-with-opencv-and-python/
[8] https://viblo.asia/p/opencv-watermarking-image-1VgZv4or5Aw
[9] https://www.ijarcce.com/upload/2016/april-16/IJARCCE\%20123.pdf
[10] https://pdfs.semanticscholar.org/327e/4aee192e7a270d3876aa1b137ebc7711e1e8.pdf

6. CONTRIBUTIONS

During all the sections of the final project, including preparing content, presentation, and writing reports and ppt, members in this group have contributed equally.