Continuing Education Program
Center for Computing and Information Technology
Faculty of Engineering
University of Indonesia

ISAS (Information Search and Analysis Skill)

“Digital Watermarking”

Group 2

Muhamad Hudya Ramadhana

Mutia Ayu Dianita

Faculty :

Fachran Nazarullah S.Kom

Class : 4SC1 (PNJ)

Faculty of Engineering University of Indonesia

Depok 16424

Preface

First, Let us give praise to Allah S.W.T who give guidance to us untill we can complete our ISAS entitled "Digital Watermarking". As author write this article, author get a lot of support from various parties. Among others are :

1. Our parents, who always help in the form of spirit and material.
2. Dr. Aries Subiantoro, M.Sc as director of CCIT Faculty of Engineering, University of Indonesia.
3. Mr. Fachran Nazarullah S.Kom, as our faculty who have provided guidance and support and referrals to us so that we can finish ISAS.
4. Our friends who always give the information that they know, exchange ideas and give encouragement to us in writing this article.

Author know that the results of this article is far from perfect and there are still many shortcomings, author hope readers will give comments and suggestions in building this article in order to become better. We hope this article can be useful for those who read or hear, especially for CCIT students of the Faculty of Engineering UI.

Our ISAS titled "Digital Watermarking" is One of Technique in Steganography to secure the message inside watermark. We hope with this ISAS people will understand about introduction of Code Igniter Framework.

Depok, February 2017

Author

TABLE OF CONTENTS

TABLE OF FIGURES

CHAPTER 1

INTRODUCTION

I.1 Background

Based on Ponemon Institue researchers, around 432 Million account hacked in this world. Hackers have exposed personal information of 110 Million American people. The hacked account roughly half are the nation's adults. It happened in the last of 12 Months alone.

The security data is one of biggest attention in the world. Because every country secret should be protected with high security. The main of security data not only to protect the important information, but also to protect any disruption from unauthorized people. The security data have so many technique. There are several technique in security data such as Cryptography and Steganography.

Steganography is one of technique in security data to hidden the message inside or above the object. It can be images, video, and text. With Steganography, any message which send by the sender will be decrypted using technique. There are several technique in Steganography, one of the technique is Digital Watermarking.

Digital Watermarking is one of technique in Steganography. The main of this invention is to hidden the message above the watermark. With the watermark above the picture it will be encrypted with the algorithm to hidden and protect the message inside the watermark. Watermark will hide a message related to the actual content of the digital signal, while in steganography the digital signal has no relation to the message, and it used as a cover to hide the real message. As example, Sender sent a picture. The condition of a picture is on the mountain with all of the high view. At the right bottom of the picture there are a watermark for signify the owner of the photo (person who takes it). If we see it normally, there are no wrong with the pictures. It's only high view at the mountain with a watermark at the right bottom of the picture. But at the real condition, the sender give a message inside the

watermark that only can be decrypted with someone who knows the algorithm. The point is to protect the message inside the picture.

Digital Watermarking is one of interesting technique in Steganography. The purpose is to study about Security Data with Digital Watermarking technique.

1.2 Writing Objective

The purpose of this ISAS are :

1. Definition of Steganography.
2. Definition of Digital Watermarking.
3. History of Digital Watermarking.
4. Classification of Digital Watermarking.

1.3 Problem Domain

Accordance with the title of ISAS "Architecture Technology of Code Igniter" We will discuss about :

1. Advantages and Disadvantages of Digital Watermarking
2. Technique of Image Watermarking

1.4 Writing Methodology

The method which used in this ISAS is the method of browsing from internet, reading online journal, and make a survey in problem domain.

1.5 Writing Framework

The paper was written by systematic as follows :

CHAPTER I : INTRODUCTION

1.1 Background

Discusses the result of research in security data, briefly description about steganography , and briefly description about digital watermarking.

1.2 Writing Objective

The purpose of this article is to understand about steganography, digital watermarking, advantages and disadvantages, and technique of image watermarking.

1.3 Problem Domain

First, tell about the advantages and disadvantages of digital watermarking, it's a comparison between benefit and deficit. Second, tell about the technique of image watermarking which used to protect and hidden a message inside the picture.

1.4 Methodology Writing

To get data which needed, this paper use the method of observing or direct observation techniques, author reads famous repository online journal.

1.5 Writing Framework

This paper Writing Framework consists of four Chapter, the first chapter is introduction which tells the background, writing objective, several problem domain, methodology writing and writing framework of this paper.

Chapter II Basic of Theory

In chapter II, paper written several sub chapter. The first sub chapter is to tell about definition of Steganography. The second sub chapter is to tell about Definition of Digital Watermarking. The third sub chapter is to tell about History of Digital Watermarking. The fourth sub chapter is to tell about Classification of Digital Watermarking.

Chapter III Problem Analysis

Analyzing and solve the problem that contained in problem domain.

Chapter IV Conclusion and Suggestion

Conclude and suggest related to this paper.

CHAPTER II
BASIC THEORY

II.1 Security System

In general, security is “the quality or state of being secure to be free from danger”. In other words, protection against adversaries from those who would do harm, intentionally or otherwise is the objective. National security, for example, is a multilayered system that protects the sovereignty of a state, its assets, its resources, and its people. Achieving the appropriate level of security for an organization also requires a multifaceted system.

A successful organization should have the following multiple layers of security in place to protect its operations:

1. Physical security, to protect physical items, objects, or areas from unauthorized access and misuse
2. Personnel security, to protect the individual or group of individuals who are authorized to access the organization and its operations
3. Operations security, to protect the details of a particular operation or series of activities
4. Communications security, to protect communications media, technology, and content
5. Network security, to protect networking components, connections, and contents
6. Information security, to protect the confidentiality, integrity and availability of information assets, whether in storage, processing, or transmission. It is achieved via the application of policy, education, training and awareness, and technology.

The Committee on National Security Systems (CNSS) defines information security as the protection of information and its critical elements, including the systems and hardware that use, store, and transmit that information.

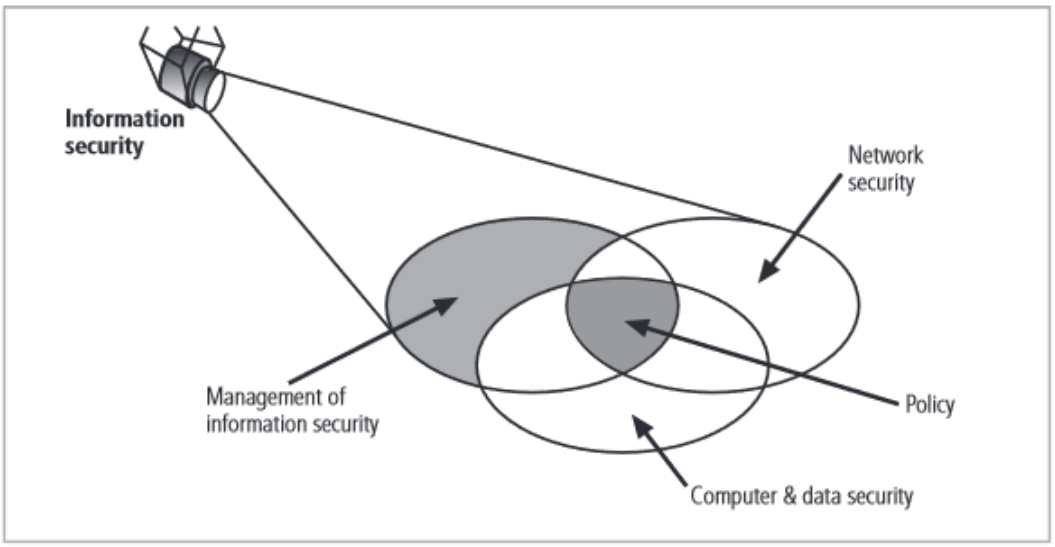

Figure 2.1 Components of Information Security (REF: [1])

Figure 2.1 shows that information security includes the broad areas of information security management, computer and data security, and network security. The CNSS model of information security evolved from a concept developed by the computer security industry called the C.I.A. triangle. The C.I.A. triangle has been the industry standard for computer security since the development of the mainframe. It is based on the three characteristics of information that give it value to organizations: confidentiality, integrity, and availability. The security of these three characteristics of information is as important today as it has always been, but the C.I.A. triangle model no longer adequately addresses the constantly changing environment. The threats to the confidentiality, integrity, and availability of information have evolved into a vast collection of events, including accidental or intentional damage, destruction, theft, unintended or unauthorized modification, or other misuse from human or nonhuman threats. This new environment of many constantly evolving threats has prompted the development of a more robust model that addresses the complexities of the current information security environment.[1]

II. 2 Definition of Encryption

Encryption is one of the principal means to guarantee security of sensitive information. Encryption algorithm performs various substitutions and transformations on the plaintext (original message before encryption) and transforms it into cipher text (scrambled message after encryption). Many

encryption algorithms are widely available and used in information security. Encryption algorithms are classified into two groups: *Symmetric-key* (also called secret-key) and *Asymmetric-key* (also called public-key) encryption [2].

Figure 2.2 Encryption (REF: http://www.tectrade.com/wp-content/uploads/2015/10/encryption.jpeg)

Symmetric key encryption is a form of cryptosystem in which encryption and decryption are performed using the same key. It is also known as conventional encryption.

Asymmetric encryption is a form of cryptosystem in which encryption and decryption are performed using the different keys – one a public key and one a private key. It is also known as public-key encryption [3].

A Key is a numeric or alpha numeric text or may be a special symbol. The Key is used at the time of encryption takes place on the Plain Text and at the time of decryption takes place on the Cipher Text. The selection of key in Cryptography is very important since the security of encryption algorithm depends directly on it. The strength of the encryption algorithm relies on the secrecy of the key, length of the key, the initialization vector, and how they all work together [4].

Asymmetric encryption techniques are about 1000 times slower than Symmetric encryption which makes it impractical when trying to encrypt large amounts of data. Also to get the same security strength as symmetric, asymmetric must use a stronger key than symmetric encryption technique [5].

II.3 Definition of Steganography

Steganography deals with hiding messages in a cover signal so that they can be extracted at the receiving side with the help of a secret key. Applications of steganography include covert communications, watermarking and fingerprinting that seem to hold promise for copyright protection, tracing source of illegal copies, etc.

Figure 2.3 Steganography (REF: http://www.jjtc.com/Steganography/steg05.jpg)

There are several issues to be considered when studying steganographic systems. One among the key performance measures used to compare different message embedding algorithms is *steganography capacity*. In a general sense, it is the maximum message size that can be embedded subject to certain constraints [6].

II.4 Definition of Digital Watermarking

Digital Watermarking is a branch of information hiding which is used to hide proprietary information in digital media like photographs, digital music, or digital video. The ease with which digital content can be exchanged over the Internet has created copyright infringement issues.

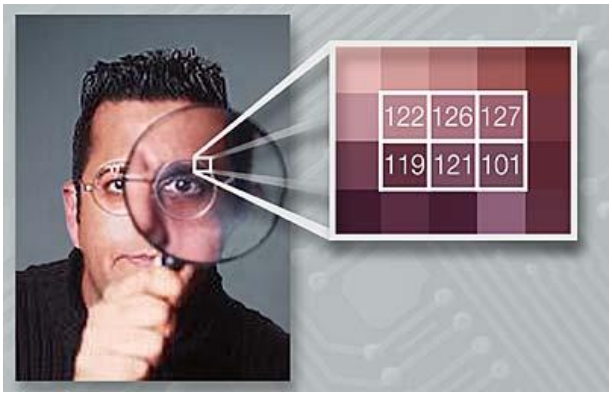

Figure 2.4 Digital Watermarking (REF: http://wiki.cas.mcmaster.ca/images/d/d1/Stegwatermark.png)

Copyrighted material can be easily exchanged over peer-to-peer networks, and this has caused major concerns to those content providers who produce these digital contents. In order to protect the interest of the content providers, these digital contents can be watermarked. In this paper we provide a survey of the latest techniques that are employed to watermark images. Image watermarking techniques can be applied to digital videos as well [7].

II.5 History of Digital Watermarking

Although the art of papermaking was invented in China over one thousand years earlier, paper watermarks did not appear until about 1282, in Italy. The marks were made by adding thin wire patterns to the paper molds. The paper would be slightly thinner where the wire was and hence more transparent. The meaning and purpose of the earliest watermarks are uncertain. They may have been used for practical functions such as identifying the molds on which sheets of papers were made, or as trademarks to identify the paper maker. On the other hand, they may have represented mystical signs, or might simply have served as decoration. By the eighteenth century, watermarks on paper made in Europe and America had become more clearly utilitarian. They were used as trademarks.

The term watermark seems to have been coined near the end of the eighteenth century and may have been derived from the German term *wasser-marke* (though it could also be that the German word is derived from the English. The term is actually a misnomer, in that water is not especially important in the creation of the mark. It was probably given because the marks resemble the effects of water on paper.

About the time the term watermark was coined, counterfeiters began developing methods of forging watermarks used to protect paper money. In 1779 Gentleman's Magazine reported that a man named John Mathison. John Mathison was hanged. Counterfeiting prompted advances in watermarking technology. William Congreve, an Englishman, invented a technique for making color watermarks by inserting dyed material into the middle of the paper during papermaking.

The resulting marks must have been extremely difficult to forge, because the Bank of England itself declined to use them on the grounds that they were too difficult to make. A more practical technology was invented by another English-man, William Henry Smith. This replaced the fine wire patterns used to make earlier marks with a sort of shallow relief sculpture, pressed into the paper mold. The resulting variation on the surface of the mold produced beautiful watermarks with varying shades of gray. This is the basic technique used today for the face of President Jackson on the $20 bill

In 1951, Emil Hembrooke of the Muzak Corporation filed a patent for watermarking musical Works. An identification code was inserted in music by intermittently applying a narrow notch filter centered at 1 kHz. The absence of energy at this frequency indicated that the notch filter had been applied and the duration of the absence used to code either a dot or a dash. The Identification signal used Morse code.

It was probably 1990s the term digital watermarking really came into vogue. About 1995, interest in digital watermarking began to mushroom. In the late 1990s several companies were established to market watermarking products. Most recently, a number of companies have used watermarking technologies for variety applications.[8]

II.6 Types of Digital Watermarking

There are 5 types of digital watermarking according Chawla, Saini, Yadav & Kamaldeep:

1. Division Based on Human Perception

   This is sub-divided into visible watermarks and invisible watermarks.

   a. Visible Watermarks

      These watermarks can be seen clearly by the viewer and can also identify the logo or the owner. Visible watermarking technique changes the original signal. The watermarked signal is different from the original signal.

Visible watermark embedding algorithms are less computationally complex. The watermarked image cannot with stand the signal processing attacks, like the watermark can be cropped from the watermarked image.

Figure 2.5 Visible Watermarked Image (REF: [9])

Spreading the watermark throughout the image is a best option, but the quality of the image is degraded which prevents the image from being used in medical applications.

b. Invisible Watermarks

These watermarks cannot be seen by the viewer. The output signal does not change much when compared to the original signal.

Figure 2.6 Invisible Watermarked Image (REF: [8])

The watermarked signal is almost similar to the original signal. As the watermark is invisible, the imposter cannot crop the watermark as in visible watermarking. Invisible watermarking is more robust to signal processing attacks when compared to visible watermarking. As

the quality of the image does not suffer much, it can be used in almost all the applications.

2. Division Based on Application

Based on application watermarks are sub-divided into fragile, semi-fragile and robust watermarks.

a. Fragile Watermarks

These watermarks are very sensitive. They can be destroyed easily with slight modifications in the watermarked signal

Figure 2.7 Fragile Watermarked Images (REF: [9])

b. Semi Fragile Watermarks

These watermarks are broken if the modifications to the watermarked signal exceed a pre-defined user threshold. If the threshold is set to zero, then it operates as a fragile watermark. This method can be used to ensure data integrity and also data authentication.

c. Robust Watermarks

These watermarks cannot be broken easily as they withstand many signal processing attacks. Robust watermark should remain intact permanently in the embedded signal such that attempts to remove or destroy the robust watermark will degrade or even may destroy the quality of the image. This method can be used to ensure copyright protection of the signal

3. Division Based On Level Of Information Required To Detect The Embedded Data

Based on the level of required information all watermarks are sub-divided into blind watermarks, semi-blind watermarks and non-blind watermarks

a. Blind Watermarks

These watermarks detect the embedded information without the use of original signal. They are less robust to any attacks on the signal.

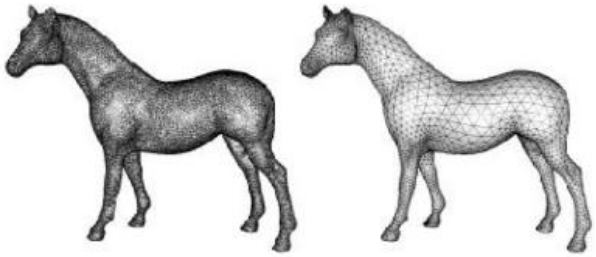

Figure 2.8 Blind Watermarks (REF: https://image.slidesharecdn.com/applicability-of-tracability-technologies-for-3d-printing-robust-blind-watermarking-ucl-150217034026-conversion-gate02/95/applicability-oftracabilitytechnologiesfor3-dprintingrobustblindwatermarkingucl-12-638.jpg?cb=1424145020)

b. Semi Blind Watermarks

These watermarks require some special information to detect the embedded data in the watermarked signal.

c. Non Blind Watermarks

These watermarks require the original signal to detect the embedded information in the watermarked signal. They are more robust to any attacks on the signal when compared to blind watermarks.

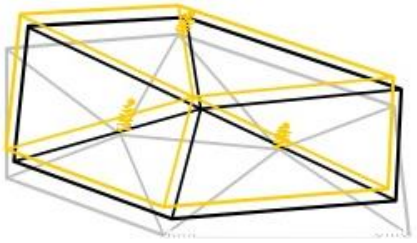

Figure 2.9 Non Blind Watermarks (REF: https://image.slidesharecdn.com/applicability-of-tracability-technologies-for-3d-printing-robust-blind-watermarking-ucl-150217034026-conversion-gate02/95/applicability-oftracabilitytechnologiesfor3-dprintingrobustblindwatermarkinguc l-12-638.jpg?cb=1424145020)

4. Division Based On User's Authorization To Detect The Watermark

   This is sub-divided into public watermarks and private watermarks

   a. Public Watermarks

      In this watermarking, the user is authorized to detect the watermark embedded in the original signal.

   b. Private Watermarks

      In this watermarking, the user is not authorized to detect the watermark embedded in the original signal.

5. Division Based on Knowledge of The User on The Presence of The Watermark

   This is sub-divided into steganographic watermarking and non-steganographic watermarking.

   a. Steganographic Watermarking

      The user is not aware of the presence of the watermark.

   b. Non-Steganographic Watermarking

The user is aware of the presence of the watermark

CHAPTER III
PROBLEM ANALYSIS

III.1 Techniques of Digital Watermarking

Digital Watermarking techniques can be classified into two domains:

1. Spatial Domain Watermarking
2. Frequency Domain Watermarking

A. Spatial Domain Watermarking

Spatial Domain Technique is a technique of watermark embedding achieved by directly modifying the pixel values of the host image. There are two techniques in SDW:

1. Least Significant Bit (LSB) Technique

   LSB is one of old popular technique embeds the watermark in the least significant bit of pixels. This method is easy to implement and doesn't generate serious distortion to the image. However, this techniques is not robust from attack.

   This technique of watermark may be embedded inside the picture. The embedding of the watermark is performed choosing a subset of image pixels and substituting the least significant bit of each of the chosen pixels with watermark bits.

   For example, in the binary number: 10111001, the least significant bit is the far right 1.

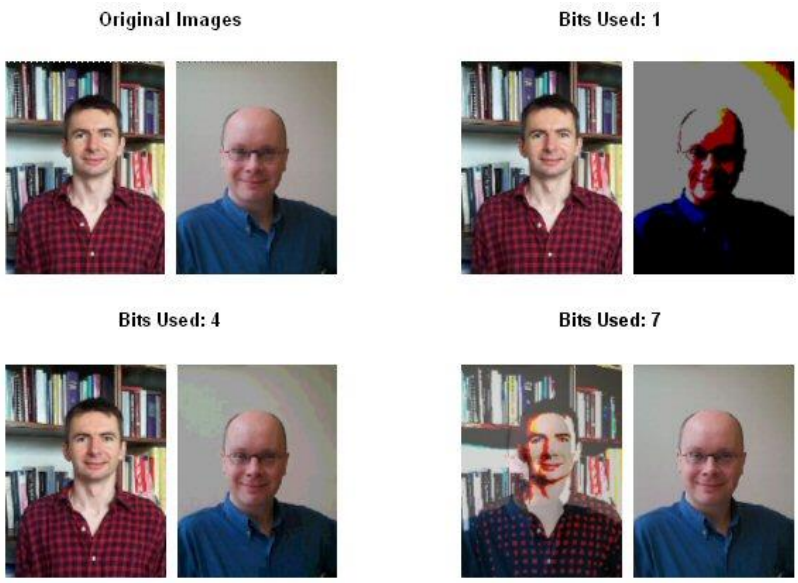

Fig 3.1 *Example of Bit used in LSB*

Source: www.bham.ac.uk

2. Correlation-Based Techniques

   Correlation-Based is the correlation properties of additive pseudo-random noise patterns as applied to an image. To retrieve the watermark, the same pseudo-random noise generator algorithm is seeded with the same key, and the correlation between the noise pattern and possibly watermarked image computed. If he correlation exceeds a certain threshold T, the watermark is detected, and a single bit set. This method can easily be extended to a multiple-bit watermark by dividing the image up into blocks, and performing the above procedure independently on each block.

B. Frequency Domain Watermarking

This technique is also known as transform domain. In this technique values of certain frequencies are changed from original values. There are various methods which are used in transform technique.

1. Discrete Wavelet Transforms (DWT)

Wavelet Transform is a modern technique frequently used in digital image processing, compression, watermarking etc. The transforms are based on small waves, called wavelet, of varying frequency and limited duration. The wavelet transform decomposes the image into three spatial directions, i.e. horizontal, vertical, and diagonal. Hence wavelet reflect the anisotropic properties of HVS more precisely. Magnitude of DWT coefficients is larger in the lowest bands (LL) at each level of decomposition and is smaller for other bands (HH, LH, and HL). The DWT is used in a signal processing applications such as audio and video compression and simulation of wireless antenna distribution. DWT is preferred because it provide both a simultaneous spatial and frequency spread of watermark within the host image.

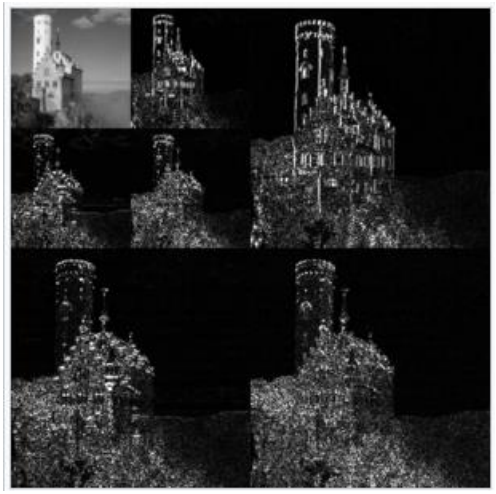

Fig 3.2 *an example of the 2D discrete wavelet transform that is used in JPEG 2000*.

Src: Wikipedia.com

2. Discrete Cosine Transform

DCT like a Fourier transform, it represents data in terms of frequency space rather than an amplitude space. This is useful because that corresponds more to the way humans perceive the light, so that the part are not perceived can be identified and thrown away. DCT based watermarking techniques are

robust compared to spatial domain techniques. Such algorithms are robust against simple image processing operations like low pass filtering, brightness, and contrast adjustment, blurring etc. However they are difficult to implement and are computationally more expensive. At the same time they are weak against geometric attacks like rotation, scaling, cropping etc.

Fig 3.2 *Image which build with DCT Technique*

Src: sourceforge.net

3. Discrete Fourier Transform

   Transforms a continuous function into its frequency components. It has robustness against geometric attacks like rotation, scaling, cropping, translation etc. DFT shows translation invariance. Spatial shifts in the image affects the phase representation of the image but not the magnitude representation, or circular shifts in the spatial domain don't affect the magnitude of the Fourier transform.

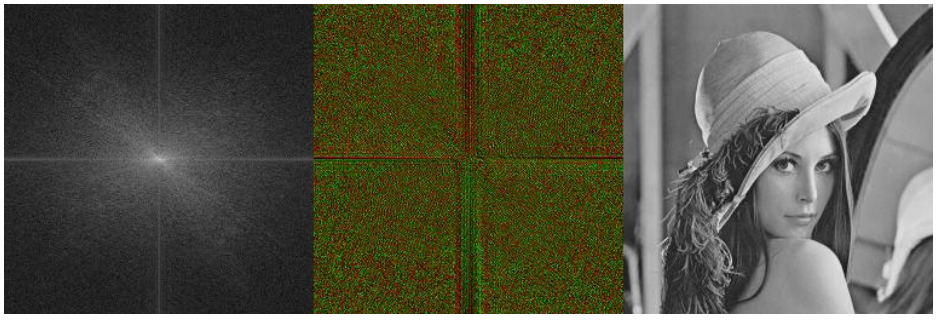

Fig 3.3 Left: Magnitude of DCF. Middle: Phase of DCF. Right: Input image

src: http://boofcv.org

III.1 Advantages and Disadvantages of Digital Watermarking

Digital Watermarking has some of advantages. Besides Digital Watermarking also have some of disadvantages

Advantages

1. It can't be easily understand by the people

   With Digital Watermarking we hidden the message inside the watermark. The message which hidden inside the watermark can't be easily understand by the people. Because there are several techniques to hidden the message inside the watermark and the message is encrypted with a lot of method. The images which encrypted with watermark is just like a normal images with a watermark to sign the creator of the picture owner.

   Imagine, if someone send a picture with watermark and uploaded in a Pinterest. The picture is just like a normal picture. But the fact there are a hidden message inside the picture and it can be understand to people who has role as receiver. People who saw the picture just think about the meaning of the picture and the essence of the picture. But people who has role as receiver will decrypt the message inside the watermark. It can be a camouflage to the people.

2. The cost is cheap

   The cost of digital watermarking are not expensive because it can be easily embedded in the picture. It's only need editor of photo and give some effect there. So the cost of digital watermarking are cheap and easy to do. Imagine if a company want to send a hidden message but scared to be decrypted or hijacked by unauthorized people so they choose digital watermarking to safe their message inside a picture.

Disadvantages

1. The security is not very safety

Because digital watermark can be seen in the picture. Some of several people can guess the mean of the message inside watermark. However if the message is not hidden with a good encryption. It can be easily guess by hackers. Besides if the sender always send the digital watermark with the same style it can also be guess by the hackers that the sender has a message inside the picture.

As example, if the sender upload in a social media such as pinterest. It can be downloaded by the all of the people.

CHAPTER IV
CONCLUSION AND SUGGESTION

IV. 1 Conclusion

Digital Watermarking is one of technique in Steganography in order to protect and hidden a message inside a picture. Digital Watermarking has two of domain techniques, those are Spatial Domain Watermarking and Frequency Domain Watermarking. Digital Watermarking choose because the implementation is quite cheap.

IV.2 Suggestion

1. Choosing digital watermarking to hidden a message can be solution.
2. Choosing a good technique to protect the message should be done with good technique.
3. We should choose the best method to protect message inside the text, picture, and video.

BIBLIOGRAPHY

[1] Bull, R. L. (2013). *Introduction to Information Security.* Melbourne: Cengage.

[2] Singh, G., & Supriya. (2013). A Study of Encryption Algorithms (RSA, DES, 3DES and AES) for Information Security. *International Journal of Computer Applications*, 1.

[2] William Stallings, "Cryptography and Network Security: Principles and Practice", Pearson Education/Prentice Hall, 5th Edition.

[3] E. Thambiraja, G. Ramesh and Dr. R. Umarani, "A Survey on Various Most Common Encryption Techniques", International Journal of Advanced Research in Computer Science and Software Engineering, Volume 2, Issue 7, pp. 226-233, July 2012.

[4] Diaa. Salama Abdul. Elminaam, Hatem Mohamed Abdul Kader and Mohie Mohamed Hadhoud, "Performance Evaluation of Symmetric Encryption Algorithms", IJCSNS International Journal of Computer Science and Network Security, VOL.8 No.12, pp. 280-286, December 2008.

[5] Chandramouli, R., & Memon, N. (2003). Steganography Capacity: A Steganalysis Perspective. *Stevens Institute of Technology Journal*, 1.

[6] M. Potdar, V., Han, S., & Chang, E. (2005). A Survey of Digital Image Watermarking Techniques. *IEEE Explore*, 1.

[7] Cox, I., Miller, M., Bloom, J., Fridich, J., & Kalker, T. (2008). *Digital Watermarking and Steganography 2nd Edition.* Burlington: Elsevier.

[8] Chawla, G., Saini, R., Yadav, R., & Kamaldeep. (2012). Classification of Watermarking Based upon Various Parameters. *International Journal of Computer Applications & Information Technology Vol.1* , 16-18.