ContinuingEducationProgram
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

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

Data Security is one of concern for all user who using the internet network. Nowadays, hackers threat all data and hangs it like a Damocles sword. The transmission data through any communication channel needs strong encryption techniques in purpose of the data security. The trends of development in information technology is needed to safe, secure, and protect the transmission of data. Conventional encryption technique methods give failed desired result of data protection. However, unique ID and password, and combination between symbol, alphabets & numerical will give a good impact to account security. One technique to protect any information is Steganography. [1]

Steganography is one of technique for hide information such that the presence of data that can't be detected easily. A message is encrypted with an algorithm that hide any secret information or message inside an object. Steganography combine communication methods, so it can be used to carry out hidden exchanges. Trithemius is author of Polygraphia and Steganographia, invented the word of Steganography and the word is written from Geek words. Steganos, meaning "covered".

Meanwhile graphien, meaning "to write". One of evidence on Steganography being used to transfer messages is the Heredotous story. The story describes about slaves and their shaved heads. Nowadays, encryption method is the most discussed problem, it's because the method with cipher text are very doubtful. Steganography mission is to create a secret channel with totally un-detectable way to evade drawing suspicion on the transporting data. Steganography methods with a secret messages can be embedded into different cover media like image, audio, video, and text.

Among the methods, the hidden message is hard to be detected using Steganography techniques in a text file compared with a picture, markup language, or sound file. One of technique in Steganography is Digital Watermarking. [2]

As an effective way in order to protect digital media copyright is using Digital Watermarking. Digital Watermarking technique has attract the attention of many people and today we have a lot of algorithms in order to use Digital Watermarking. In digital images, the process of embedding accomplished in either spatial domain or frequency domain. It's shown that better compromise of robustness and level of robustness is obtained using frequency domain scheme. [4]

Digital Watermarking is one of technique which used to hidden a message with watermarking technique. On this ISAS, it will describe about one of technique in digital watermarking called Algorithm of Morphological Haar Wavelet Transform (MHWT).

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, readingonline 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 observationtechniques,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 Digital Watermarking Process

Digital watermarking has some process. First choose a picture that want to be embedded with watermark. After that with algorithm the image RGB Channels will be decomposed. The main aim why needs to be decomposed because to make the watermark easy to embed in the picture. After the picture decomposed, it will be embedded between the image and the watermark. The process of embedding will use a good algorithm of embedding to hidden a watermark information inside a picture. The watermark can also be visible watermark instead invisible watermark. For the full process, see the figure below.

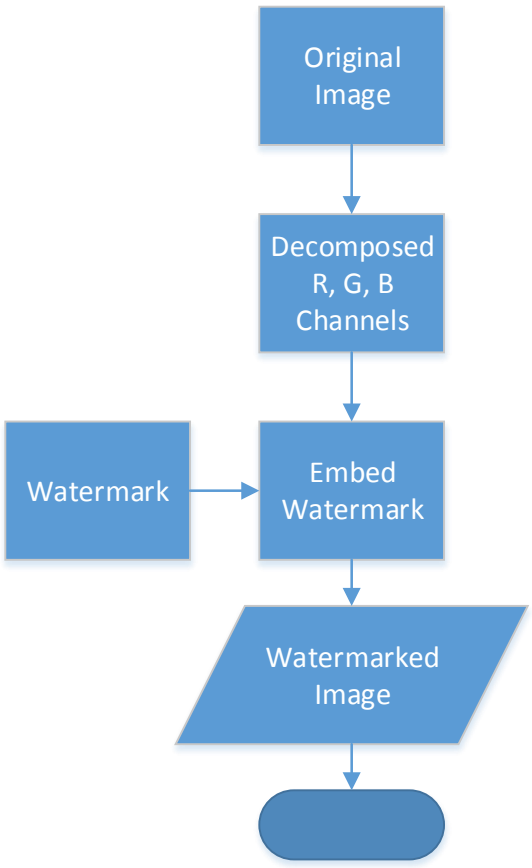

Figure 2.1 Flowchart Digital Watermarking Process

II.2 Arnold Transform Scrambling Algorithm

Arnold Transform Algorithm is a technique of two-dimensional mapping which transform each coordinate (x,y) in the logo image to new coordinate (x',y').

The function of Arnold Transform algorithm is to increase the security of picture which ready to be embedded with watermark. Because it will mapping from original coordinate into the new coordinate.

II.3 Haar Wavelet Transform

Haar Wavelet Transform is one of wavelet transform implementation which use a discrete set of the wavelet scales and translations obeying some defined rules. This transform decomposes the signal into mutually orthogonal set of wavelets, which is the main difference from the continuous wavelet transform (CWT), or its implementation for the discrete time series. It can be called discrete-time continuous wavelet transform (DT-CWT).

CHAPTER III
PROBLEM ANALYSIS

III.1 Arnold Transform

Expression of Arnold Transform can be shown as the following equation:

$x' = a_1x + a_2y + mod L$

$y' = a_3x + a_4y + mod L$

The parameters may fulfill, a1 * a4 – a2 * a3 = ± 1 and the parameter L x L is the size of the logo image. Scrambled image can be get from an adaptive logo-scrambling performs with iterative procedure. However, Arnold Transform only valid for square images. The Arnold Transformation is used to scramble the digital images and has many applications, especially in digital watermarking.

This technique can rotate logo for angles 90, 180, 270. The ability to scramble and descramble may increase the security in watermarking.

Figure 3.1 Logo Image of Size 64x64

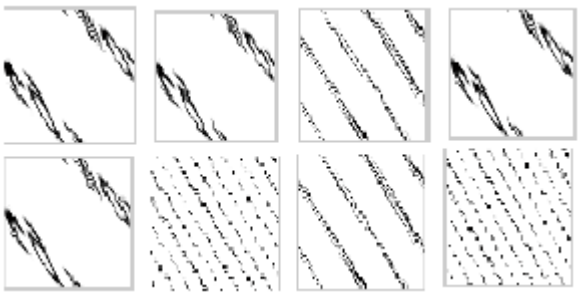

Figure 3.2 Results of Arnold Transform applied on logo image size of 64x64

III.2 Morphological Haar Wavelet Transform

In mathematics, expression of Haar transform matrix shown as the following:

$T = HFH^T$

F = N x N image matrix

H = N x N transformation matrix

T = the result of Haar Transform

H contains the Haar basis function, its $h_k(z)$, it is defined in a continuous closed interval of $z \sum [0,1]$.

$k = 0,1,2,\ldots N-1$.

$N = 2^n$.

To generate H matrix, define an integer variable *k*, as $k = 2p + q - 1$ ($0 \leq p \leq n - 1$ when p = 0, q = 0 or 1).

Define of Haar basis function:

$$h_0(z) = h_{00}(z) = \frac{1}{\sqrt{N}}, z \in [0,1]$$

And

$$h_k(z) = h_{pq}(z) = \frac{1}{\sqrt{N}} \begin{cases} 2^{p/2} & (q-1)/2^p \leq z < (q-0.5)/2^p \\ -2^{p/2} & (q-0.5)/2^p \leq z < q/2^p \\ 0 & \text{others}, z \in [0,1] \end{cases}$$

To embed a pictures we refer to two section of synthesis operators, a family of ω^s_j of signal synthesis operator and a family of ω^s_j which detail synthesis operators mapping $V_j + 1$ back into V_j. The equation define as:

$$\psi^a_j(x)(m,n) = \min(x(2m,2n), x(2m+1,2n), x(2m+1,2n), x(2m+1,2n+1))$$

$$\omega^a_j(x)(m,n) = (\omega^a_{j,v}(x)(m,n), \omega^a_{j,h}(x)(m,n), \omega^a_{j,d}(x)(m,n))$$

$\psi^a_j, \omega^a_{j,v}, \omega^a_{j,h}, \omega^a_{j,d}$ represent the scaled signal and the vertical, horizontal, and diagonal detail signals, which are given by below equation:

$$\omega^{a}_{j,v}(x)(m,n)=1/2((x(2m,2n)-x(2m,2n+1)+x(2m+1,2n)-x(2m+1,2n+1))$$

$$\omega^{a}_{j,h}(x)(m,n)=1/2((x(2m,2n)-x(2m+1,2n)+x(2m,2n+1)-x(2m+1,2n+1))$$

$$\omega^{a}_{j,d}(x)\,(m,n)=1/2((x(2m,2n)-x(2m+1,2n)-x(2m,2n+1)+x(2m+1,2n+1))$$

The synthesis operators are now given by below equation:

$$\psi^{S}_{j}(x)(2m,2n)=\psi^{S}_{j}(x)(2m,2n+1)=\psi^{S}_{j}(x)\,(2m+1,2n)=\psi^{S}_{j}(x)\,(2m+1,2n+1)=x(m,n)$$

And

$$\omega^{S}_{j}(y)(2m,2n)=\max(y_V(m,n)+y_h(m,n),\,y_V(m,n)+y_d(m,n),\,y_h(m,n)+y_d(m,n),0)$$

$$\omega^{S}_{j}(y)(2m+1,2n)=\max(y_V(m,n)-y_h(m,n),\,y_V(m,n)-y_d(m,n),\,-y_h(m,n)-y_d(m,n),0)$$

$$\omega^{S}_{j}(y)(2m,2n+1)=\max(y_h(m,n)-y_V(m,n),\,-y_V(m,n)-y_d(m,n),\,y_h(m,n)-y_d(m,n),0)$$

$$\omega^{S}_{j}(y)(2m+1,2n+1)=\max(-y_V(m,n)-y_h(m,n),\,y_d(m,n)-y_V(m,\,n),\,y_d(m,n)-y_h(m,n),0)$$

III.3 Watermark Embedding

First, using Arnold Scrambling Algorithm to improve the security of watermark. As example, picture with 64x64 pixel grayscale Baboon image as the watermark is used.

Figure 3.3 Watermark embedding using Arnold Scrambling Algorithm

Then, composed the original image by L-level MHWT. After that the result can get the approximate subgraph D*l* obtained by the following formula:

$$p(i,\,j)=(1-NVF(i,\,j))\times S_1+NVF(i,\,j)\times S_2$$

NVF is the Noise Visibility Function, S1 and S2 are the maximum allowable distortion values of expected texture region and flat region.

The result of picture is, the approximate multi-scale images retain the basic texture features of the original image by MHWT, so this region can be embedded with watermark. For the concrete steps, it can be following:

1. Composed the original image into L-level wavelet into L-level wavelet to obtain the image Dl with the size of M*l* x N*l*, based on the 2-D MHWT.
2. Do the first step again to obtain the relevant level scale image *Wi*, with the size of *Mi x Ni*.
3. Get the permissible distortion value matrix P from the original image using NVF.
4. Select the maximum *β x M i x N i* values of *p(i, j)* from D*l*, where β is in the range of $[1,2, \ldots., \frac{Ml \; x \; Nl}{Mi \; x \; Ni}]$
5. Select the number of *M i x N i* pixel points from mentioned values above as embedding watermark position, use the generated random sequence under the key K.
6. Corresponding formula, the decomposed watermarks are embedded in the corresponding resolution of the decomposed original image to which the watermark can adapt itself.

   $$D'_l(i, j) = D_l(i, j) + \alpha(i, j) \cdot W_i(i, j)$$

   Where α is the embedding strength of watermark, W*i* (*i, j*) is the relevant information of watermark.
7. Apply Morphological Haar Synthesis Transform on the D*'l* image, include the detail signal images, to produce the watermarked host image.

   The watermark embedding carried out in the above steps is shown in image below.

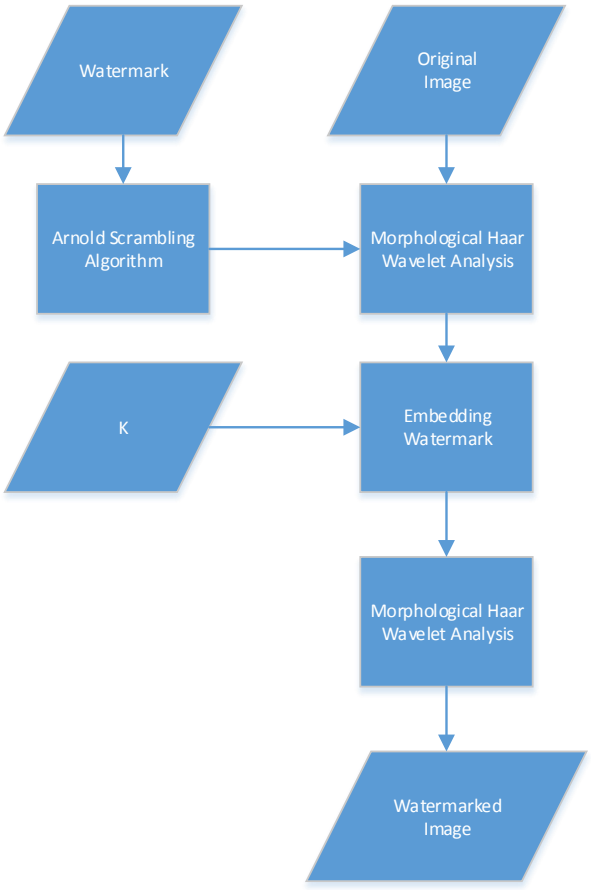

Figure 3.4 Flowchart watermark embedding

III.4 Watermark Detection

The inverse procedure of the watermark embedding is Watermark Extraction. Non-blind watermarking algorithm and the original host image is required to extract the watermark. The similarity between the original watermark and the extracted watermark using the correlation coefficient factor ρ given below in equation:

$$\rho(w,\hat{w}) = \frac{\sum_{i=1}^{N} w_i \hat{w}_i}{\sqrt{\sum_{i=1}^{N} w_i^2}\sqrt{\sum_{i=1}^{N} \hat{w}_i^2}}$$

w & ŵ = the original and extracted watermarks.

N = the number of pixels in watermark.

ρ = the number between [0-1].

The correlation coefficient factor value around 0.75 and above is considered acceptable. The watermark detection is conducted in the steps as shown in below picture.

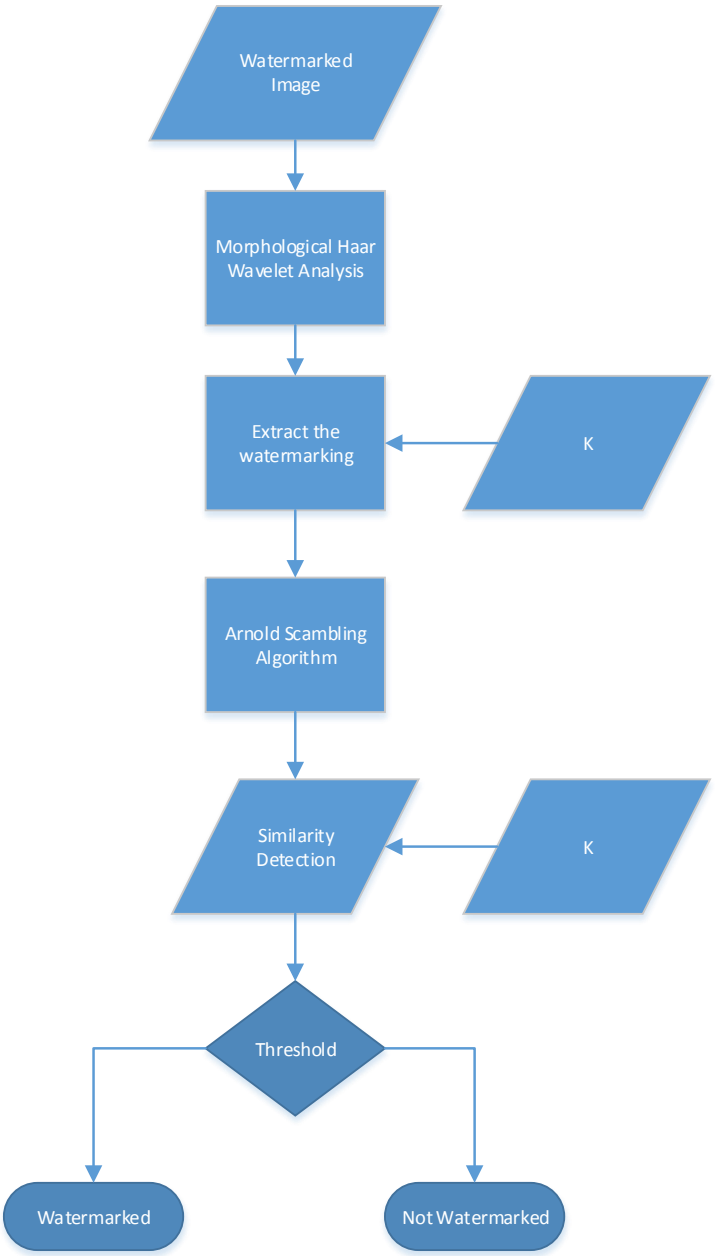

Figure 3.5 Flowchart watermark detection

III.5 Result of Embedding

Combination of Haar Wavelet Transform and Arnold Scrambling Algorithm won't make watermark easy to detect. However, both of Algorithm are dependent each other. Without Haar Wavelet Transform, Arnold Scrambling Algorithm only can make the watermark reducted to detected. Without Arnold Scrambling Algorithm, Haar Wavelet Transform can't make the secure of Watermarked Image.

The reason why Haar Wavelet Transform need Arnold Scrambling Algorithm because it can improve the security to make the watermark hard to detect when it embedded with original image. Arnold Scrambling Algorithm also used in decode the image which want to be decoded. It's because Arnold Scrambling Algorithm will detect the similarity of the image which want to be decoded.

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. To make a watermark on digital images, we should prepare the original image and the watermark image which ready to mix and embed. One of technique to make the watermark security good is to use Arnold transform algorithm. After that Haar Wavelet Transform will be used to mix the watermark and original images.

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]M. Indra Sena Reddy, D. A. (2016). Secured Data Transmission Using Wavelet Based Steganography and Cryptography by Using AES Algorithm. *Procedia Computer Science*, 62-69.

[2] Vidhya P.M, V. P. (2016). A Method for Text Steganography Using Malayalam Text. *International Conference on Information and Communication Technologies*, 524-531.

[3] Xiaosheng Huang, S. Z. (2012). An Adaptive Digital Image Watermarking Algorithm Based on Morphological Haar Wavelet Transform. *International Conference on Solid State Devices and Materials Science*, 568 – 575.

Saikrishna N, R. M. (2016). An Invisible Logo Watermarking using Arnold Transform. *6th International Conference On Advances In Computing & Communications*, 808 – 815.