

修士学位論文

題目

**3D Watermarking Secret Direction Scheme for Volumetric  
DICOM Images**

指導教員

Prof. Mario Köppen

報告者

Ajif Yunizar Pratama Yusuf

2018/2/14

九州工業大学大学院 情報工学研究院 情報創成工学専攻

# Contents

<b>1</b>	<b>Introduction</b>	<b>2</b>
<b>2</b>	<b>3D Watermarking Secret Direction Scheme</b>	<b>3</b>
2.1	3D Watermarking . . . . .	3
2.2	Secret Direction Scheme . . . . .	3
2.2.1	Bresenham Algorithm . . . . .	3
2.2.2	Randomized Halton Sequence . . . . .	4
<b>3</b>	<b>Methodology</b>	<b>5</b>
3.1	Pre-Watermarking . . . . .	5
3.1.1	Encryption of the logo . . . . .	5
3.1.2	Slicing process by selection point for $(X, Y)$ secret direction . . . . .	6
3.1.3	Scrambling row for $t$ -secret direction . . . . .	10
3.2	Encode Watermark Process . . . . .	12
3.3	Decryption of the logo . . . . .	12
<b>4</b>	<b>Experiment Result</b>	<b>14</b>
4.1	Analysis the watermarked frame of secret direction . . . . .	14
4.2	Analysis the watermarked of volumetric DICOM images . . . . .	15
4.2.1	Analysis point selection type 1 : $(1, 1)$ to $(512, 512)$ . . . . .	16
4.2.2	Analysis point selection type 2 : $(51, 1)$ to $(335, 512)$ . . . . .	17
4.2.3	Analysis point selection type 3 : $(352, 1)$ to $(352, 512)$ . . . . .	17
4.2.4	Analysis point selection type 4 : $(1, 32)$ to $(512, 433)$ . . . . .	18
4.2.5	Analysis point selection type 5 : $(1, 105)$ to $(512, 105)$ . . . . .	18
4.3	Analysis of decryption of the logo . . . . .	19
<b>5</b>	<b>Conclusion</b>	<b>20</b>
<b>6</b>	<b>Acknowledgement</b>	<b>21</b>

# 1 Introduction

Image security is one of the most questionable issues when medical images along with patient information are transmitted to the public network. With the service system in obtaining patient medical images gradually expanding with the provision of health care delivery, consideration in image security is no longer limited in transit but also storage. Medical image security can be categorized into three main issues; privacy, authenticity, and integrity [1].

Digital watermarking is a technique for protecting or securing the integrity of medical images. The advantage of using watermarking is to secure authentic information that is visually invisible to the human eye [2].

There has been much research in improving the integrity and authenticity of watermarking techniques, especially in medical images. However, most of them in their applications so far have only one frame in mind and do not offer a satisfying solution to the case of multiple frames, such as X-ray angiography (XA), or intravascular ultrasound (IVUS) [3].

Digital Imaging and Communication in Medicine (DICOM) is standard for image communication in medicine. The watermarking technique for volumetric DICOM images has been enhanced by several studies [1],[2],[3],[4].

Dou et al.[4] have proposed an improved tamper detection and localization scheme for volumetric DICOM images.

## 2 3D Watermarking Secret Direction Scheme

### 2.1 3D Watermarking

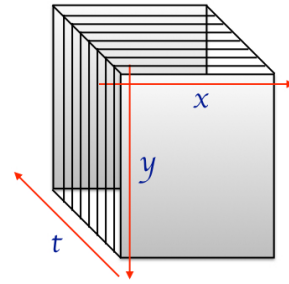
3D watermarking is watermarking on three-dimensional objects. Currently, the three-dimensional graphical objects are so rapidly evolving that they require security in protecting copyright. Distribution through the Internet which is a public network is very unsafe, so it needs a method in protecting the copyright. And the technique that has been good at protecting copyright on an object is watermarking.

### 2.2 Secret Direction Scheme

View the DICOM medical image frames as three-dimensional structures.



(a) A volumetric of DICOM images.



(b) Three-Dimensional form.

Figure 1: A series of DICOM images is three-dimensional form.

Here, the  $x$ -axis is represented as a column of DICOM image, the  $y$ -axis is represented as a row of DICOM images, and the time  $t$ -axis is represented as a Dicom series of images per time  $t$ .

For the  $XY$ -secret direction, Bresenham algorithm is used, and for the  $t$ -secret direction, the Randomized Halton sequence is used.

#### 2.2.1 Bresenham Algorithm

Bresenham algorithm is an algorithm for drawing an approximate line. This algorithm was proposed by Jack Elton Bresenham in 1962.

In here, we will describe how the Bresenham algorithm works. At first, choose two endpoint of a line from  $(X_0, Y_0)$  to  $(X_1, Y_1)$ . The point of  $x$  represents a column, and the point of  $y$  represents a row. To select the points between  $(X_0, Y_0)$  and  $(X_1, Y_1)$ , The Eq.(1) is used. At this time, the initial values of  $x$  and  $y$  are  $X_0$  and  $Y_0$ . Increasing the value of  $x$  by one, the value of  $y$  is derived.

$$y = \frac{Y_1 - Y_0}{X_1 - X_0} (x - X_0) + Y_0 \quad (1)$$

As seen in the figure below how Bresenham algorithm works to select the next point.

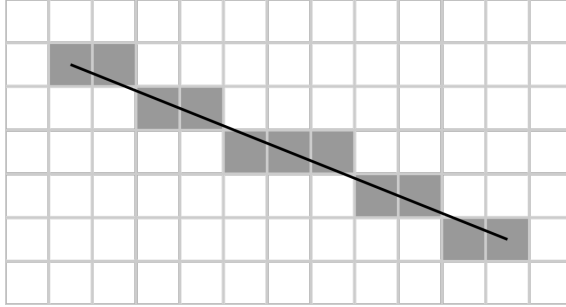


Figure 2: The drawing line concept using Bresenham algorithm[5].

### 2.2.2 Randomized Halton Sequence

The Halton sequence is a sequence that is obtained by breaking the unit interval continuously based on chosen point-p.

For example, if we choose 2; it will generate the sequence by breaking the unit interval by 2 continuously until the number of sequence values that we want is reached. The first unit interval is  $(0,1)$  and the first number of sequence is  $1/2$ . The second interval is  $(0,1/2)$  and the second number of sequence is  $1/4$ . The third interval is  $(1/2,1)$  and the third number of sequence is  $3/4$ . It is performed repeatedly until the number of sequence values that we want is reached. The result of sequence becomes like Eq.2

$$\frac{1}{2}, \frac{1}{4}, \frac{3}{4}, \frac{1}{8}, \frac{3}{8}, \frac{5}{8}, \frac{7}{8}, \dots \quad (2)$$

Randomized Halton sequence will be used to encrypt the logo by randomizing row and column and to get  $t$ -secret direction by randomizing row of the frame that we get from  $XY$ -secret direction.

### 3 Methodology

In the previous section, the scheme of 3D watermarking by secret direction was introduced. And in this section the watermarking embedding with 3D secret direction will be explained. Figure 3 shows the flowchart of the 3D watermarking process with secret direction.

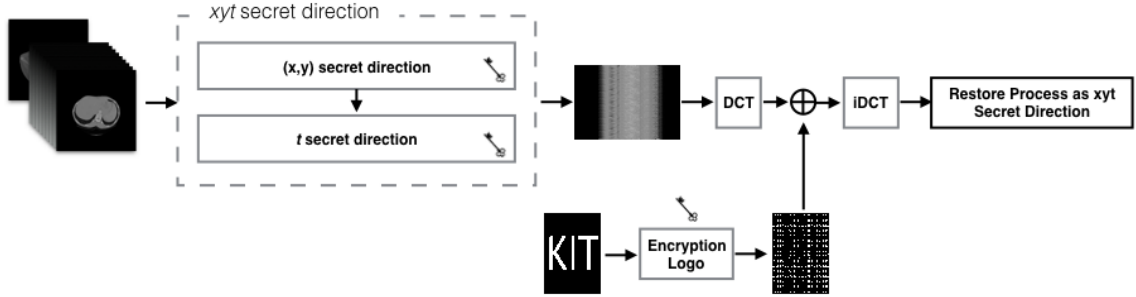


Figure 3: Flowchart of 3D watermarking secret direction scheme.

Embedding the watermark logo will be done after the message encryption process, the line slicing process on the  $XY$ -slice and the method of randomizing the line on the time  $t$ -axis. It aims to secure messages or watermark logos into levels challenging to detect.

Encrypting the watermark logo using Halton sequence is the first step of pre-watermarking. Halton sequence is a well-known multi-dimensional low-discrepancy sequence that can be relied upon to encrypt the watermark logo [1].

Next is the slicing process by selection point for  $XY$ -secret direction.

We use Bresenham algorithm to determine pixel selection and form a line extending over the DICOM image per-time  $t$ . In this experiment, five types of image slicing will be executed.

The scrambling row to get  $t$ -secret direction also uses Halton sequence for encryption.

#### 3.1 Pre-Watermarking

Pre-watermarking is part of the preparation before embedding a watermark logo. There are three preparations; encrypting the logo, slicing the image for  $XY$ -secret direction, and scrambling the row for  $t$ -secret direction.

##### 3.1.1 Encryption of the logo

An encryption system is based on the Halton series. Encryption and decryption are determined by a key that will be the basis of the calculation of the Halton sequence itself.

The algorithm for encryption using Halton sequence is below;

1. Read the logo image.
2. Resize the logo became  $64 \times 45$  (Fig.4a).
3. Convert image to binary image, based on threshold.
4. Choose based = 2.78. It means the unit interval is broken into 2.78 equal parts, each subinterval into two equal parts, each sub-sub-interval, etc. And also, it will be became secret key.
5. Generate Halton sequence. The logo size 64 row and 45 column so that we will generate 109 sequence.
6. Sort the sequence of row by series of smallest numbers to largest and exchange the row.
7. Sort the sequence of column by series of smallest numbers to largest and exchange the column (Fig.4b).



(a) Original Logo.



(b) Encrypted Logo.

Figure 4: Encrypt logo process.

Figure 4b will then be used for the encoded watermark process.

### 3.1.2 Slicing process by selection point for $(X, Y)$ secret direction

To get the line connected two points between  $(X_0, Y_0)$  and  $(X_1, Y_1)$ , which  $(X_0, Y_0)$  is the beginning point and  $(X_1, Y_1)$  is the end point, we will use Bresenham algorithm. Here is the algorithm :

1. Input the two end-points;  $(X_0, Y_0)$  and  $(X_1, Y_1)$ .
2. Calculate the constant  $dx$ ,  $dy$ ,  $2dy$ , and  $(2dy - 2dx)$  which is

$$dx = X_1 - X_0$$

$$dy = Y_1 - Y_0$$

and get the first value for the decision parameter as

$$parameter = 2dy - dx$$

.

3. At each  $X_k$  along the line, starting at  $k = 0$ , perform the following test if pixel  $p_k < 0$ , the next point to plot is  $(x_k + 1, y_k)$  and

$$p_{k+1} = p_k + 2dy$$

Otherwise,

$$(x_k, y_k + 1)$$

$$p_{k+1} = p_k + 2dy - 2dx$$

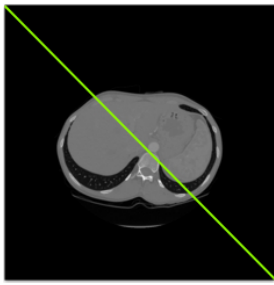
.

4. Repeat step 4 with  $(dx - 1)$  times. For  $dy/dx > 1$ , find out whether you need to increment  $x$  while incrementing  $y$  each time. After solving, the equation for decision parameter  $P_k$  will be very similar, just the  $x$  and the  $y$  in the equation gets interchanged.

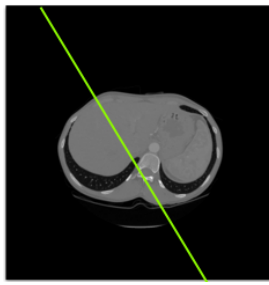
Based on the Bresenham algorithm, we are dealing with 5 types of selection point;

1. Point Selection Type 1 :  $(1, 1)$  to  $(512, 512)$
2. Point Selection Type 2 :  $(51, 1)$  to  $(335, 512)$
3. Point Selection Type 3 :  $(352, 1)$  to  $(352, 512)$
4. Point Selection Type 4 :  $(1, 32)$  to  $(512, 433)$
5. Point Selection Type 5 :  $(1, 105)$  to  $(512, 105)$

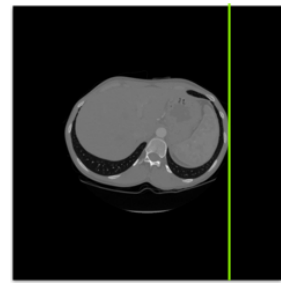




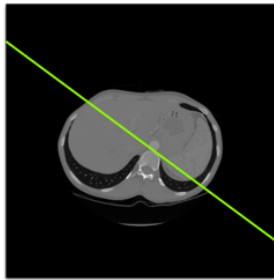
(a)  $(1, 1)$  to  $(512, 512)$ .



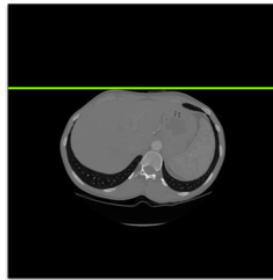
(b)  $(51, 1)$  to  $(335, 512)$ .



(c)  $(352, 1)$  to  $(352, 512)$ .



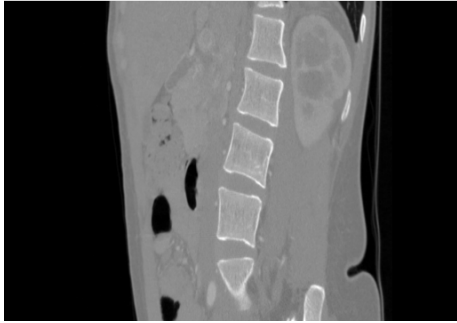
(d)  $(1, 32)$  to  $(512, 433)$ .



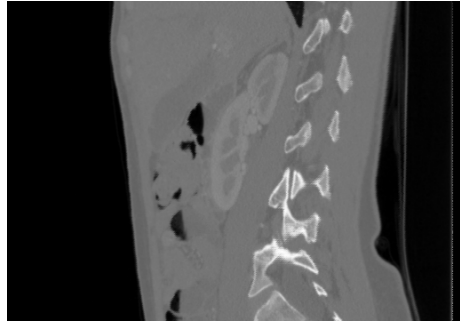
(e)  $(1, 105)$  to  $(512, 105)$ .

Figure 5: Five types of line slicing image.

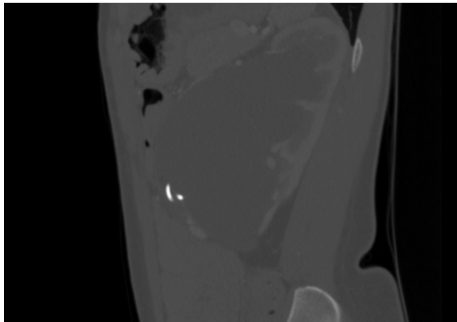
As seen in the figure 6, those are every type of line slicing.



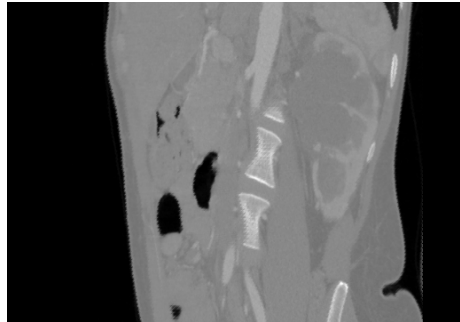
(a) The slices type 1.



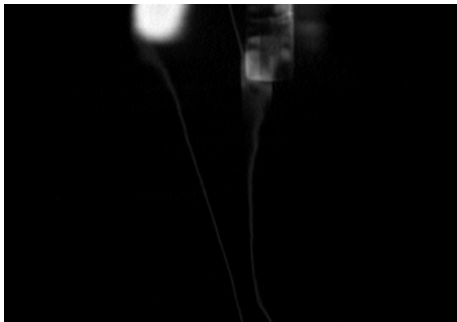
(b) The slices type 2.



(c) The slices type 3.



(d) The slices type 4.



(e) The slices type 5.

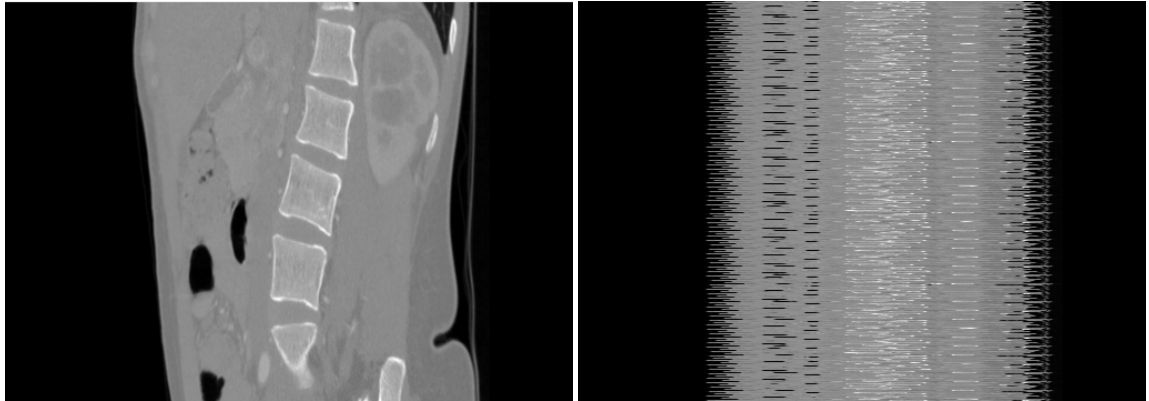
Figure 6: Five types of slicing image, with the resolutions  $360 \times 520$  for each type.

### 3.1.3 Scrambling row for $t$ -secret direction

To get the unknown  $t$  direction of a number of the frame for the watermarking process, we can use the scrambling row by Halton sequence . The algorithm of scrambling row using Halton sequence is :

1. Read the slicing image from slicing process by selection point using Bresenham algorithm.
2. Choose based = 3.42. It means the unit interval is broken into two equal parts, each subinterval into two equal parts, each sub-sub-interval, etc. And also, it will become the secret key.
3. Generate Halton sequence which the number of sequence values is 360 sequences.
4. Sort the sequence by row and exchange the rows.

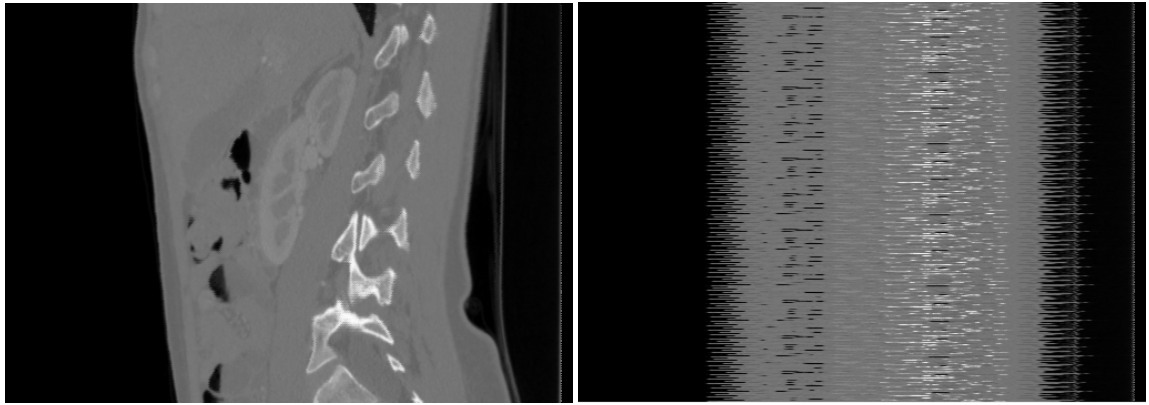
Now we will execute the algorithm of every type of point of selection from the slicing process.



(a) The slice type-1.

(b) After scrambling row.

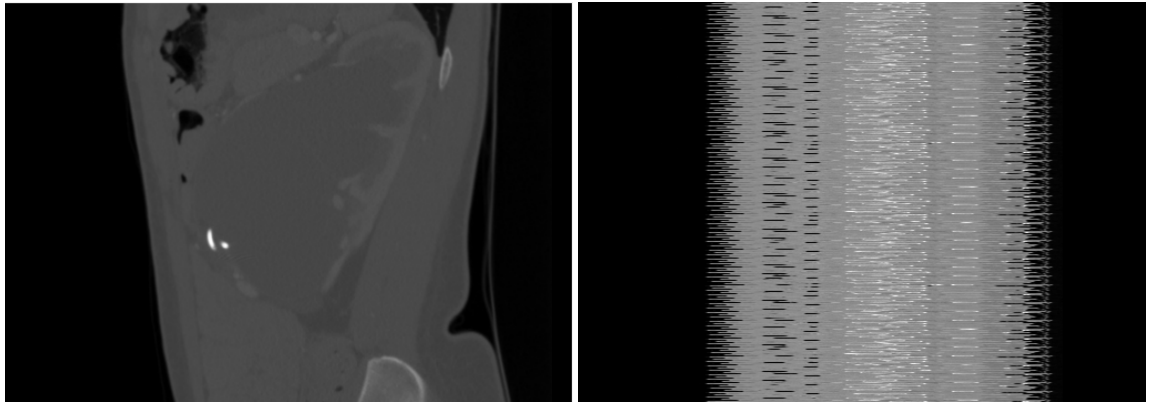
Figure 7: The scrambling slice type-1.



(a) The slice type-2.

(b) After scrambling row.

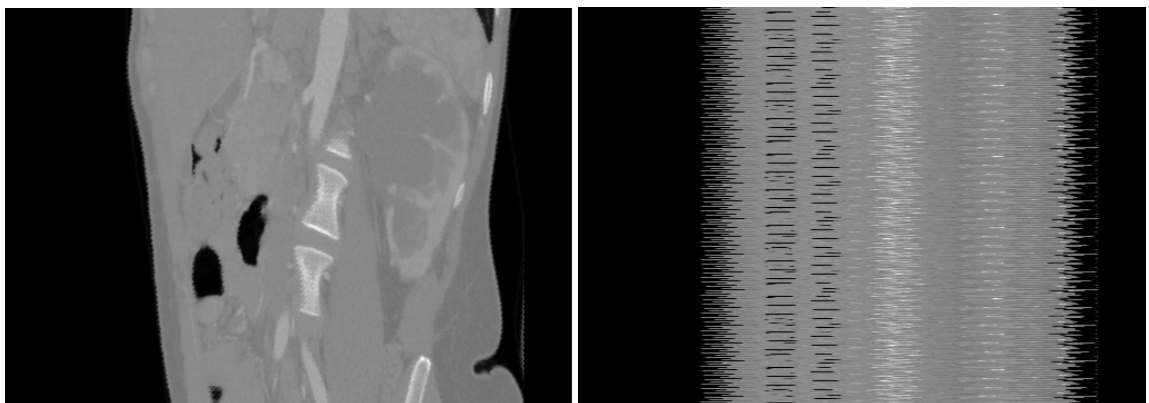
Figure 8: The scrambling slice type-2.



(a) The slice type-3.

(b) After scrambling row.

Figure 9: The scrambling slice type-3.



(a) The slice type-4.

(b) After scrambling row.

Figure 10: The scrambling slice type-4.

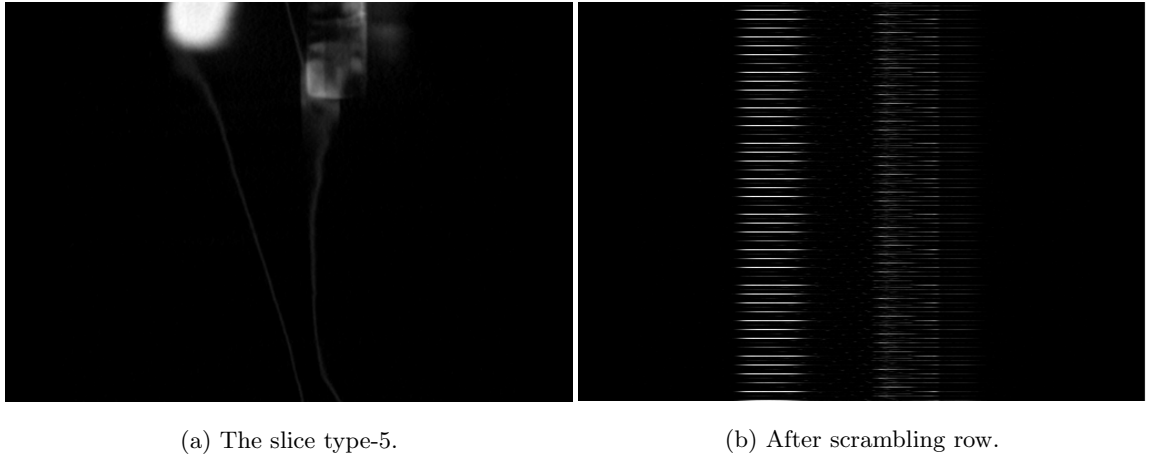


Figure 11: The scrambling slice type-5.

### 3.2 Encode Watermark Process

After going through the process of scrambling images as  $t$  direction above then, we embed the watermark encryption image, with the following algorithm:

1. Read the Scrambling Image  $SI(360 \times 512)$ .
2. Read the Encrypt Watermark  $EW(64 \times 45)$ .
3. The Scrambling Image  $SI(360 \times 512)$  is first divided into square blocks of size  $8 \times 8$  pixels, then the DCT is applied in each block.
4. Embed the Encrypt Watermark  $EW$  using embedding factor.

```

If Encrypt Watermark==0
    DCT Block(8,8) = DCT Block(8,8)+Embedding Factor;
else
    DCT Block(8,8) = DCT Block(8,8)-Embedding Factor;
end

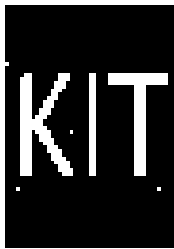
```

5. Compute the inverse DCT of modified block.
6. Repeat the process to compute every type of slice.

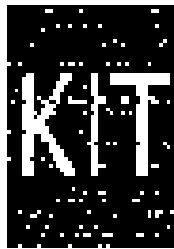
### 3.3 Decryption of the logo

This stage is the final stage in the process of decrypting the logo, where the result is still in the form of an encrypted logo. To decrypt the encrypted logo, we require a key to read or understand messages from the logos that have been implanted in DICOM images.

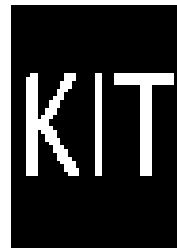
1. Read the logo image.
2. Resize the logo to  $64 \times 45$ .
3. Convert image to binary image, based on threshold.
4. Choose based = 2.78. It means the unit interval is broken into 2.78 equal parts, each subinterval into two equal parts, each sub-sub-interval, etc. And also, it will be became secret key.
5. Generate Halton sequence. The logo size is 64 rows and 45 columns so that we will generate 109 sequences.
6. Sort the sequence of row by series of smallest numbers to largest and exchange the row.
7. Sort the sequence of column by series of smallest numbers to largest and exchange the column.



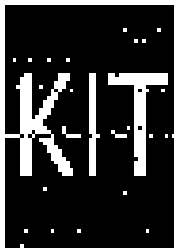
(a) Decryption of the logo  
type-1.



(b) Decryption of the logo  
type-2.



(c) Decryption of the logo  
type-3.



(d) Decryption of the logo  
type-4.



(e) Decryption of the logo  
type-5.

Figure 12: Decryption of the logo of all types.

## 4 Experiment Result

The experiment was done using MATLAB R2016 platform. DICOM images are images of the abdomen that are downloaded for free at <https://www.dicomlibrary.com/> with a resolution of  $512 \times 512 \times 360$ . The resolution of the logo is  $64 \times 45$ . The average time for the watermarking process is 0.21 seconds per frame.

The imperceptibility of the watermark is tested by comparing the watermarked image with the original one. Several tests are used in this regard.

$$\text{Bit Error Ratio } BER = \frac{\text{The number of bit error}}{\text{unit time}} \quad (3)$$

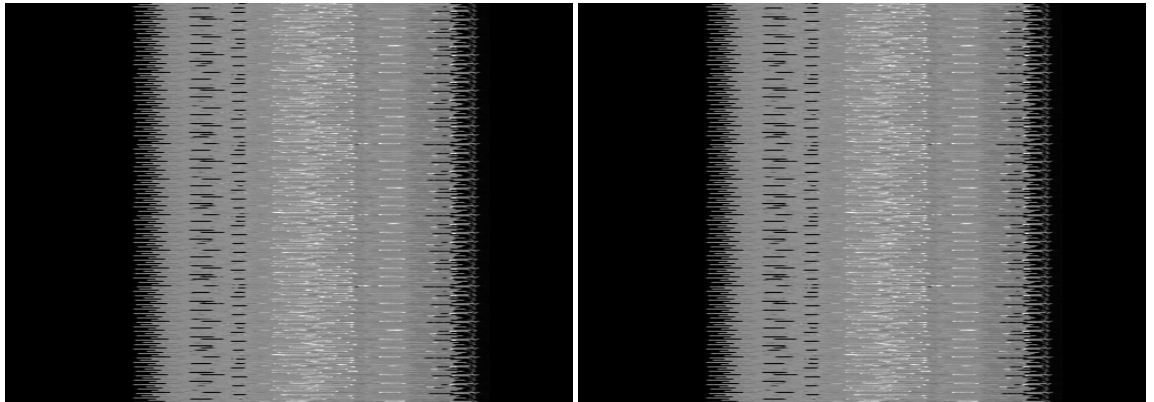
$$\text{Mean Squared Error } MSE = \frac{1}{mn} \sum_{i=0}^{m-1} \sum_{j=0}^{n-1} [I(i, j) - K(i, j)]^2 \quad (4)$$

$$\text{Peak Signal to Noise Ratio } PSNR = 10 \cdot \log_{10} \frac{MAX_i^2}{MSE} \quad (5)$$

$$\text{Nomalized Cross-Correlation } NCC = \frac{\sum_{i=1}^N \sum_{j=1}^M W(i, j) W'(i, j)}{\sqrt{\sum_{i=1}^N \sum_{j=1}^M [W(i, j)]^2} \sqrt{\sum_{i=1}^N \sum_{j=1}^M [W'(i, j)]^2}} \quad (6)$$

### 4.1 Analysis the watermarked frame of secret direction

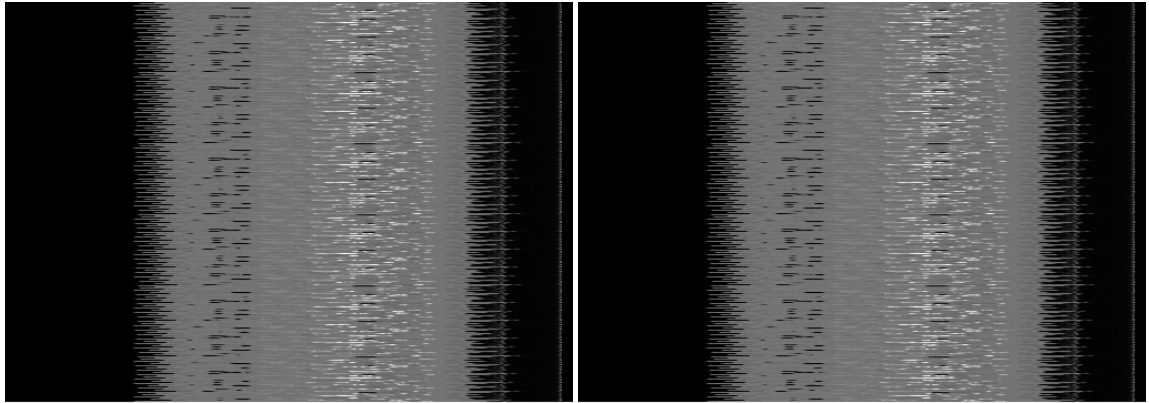
The images from Fig.13 to Fig.14 can be analyzed to see the differences between original and watermarked images.



(a) Before encoding watermark.

(b) After encoding watermark.

Figure 13: The Slice type-1, PSNR = 84.5176.



(a) Before encoding watermark.

(b) After encoding watermark.

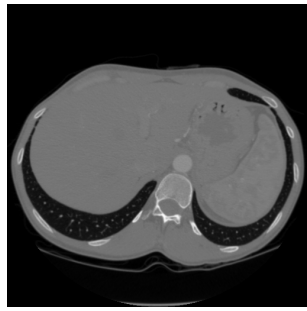
Figure 14: The Slice type-2, PSNR = 84.1935.

For the slice type-3, the PSNR is 84.1585. While the slice type-4, the PSNR is 84.3655. And for the slice type-5, the PSNR is 85.7845.

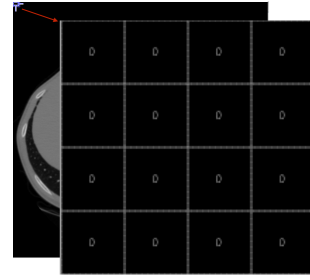
## 4.2 Analysis the watermarked of volumetric DICOM images

In the DICOM image below, it appears that the difference between the original and the embedded watermark

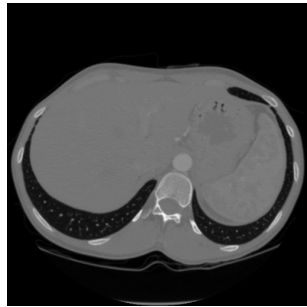




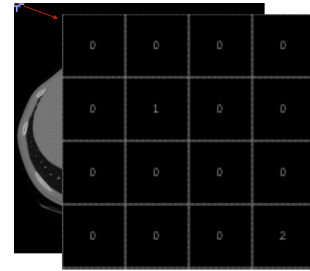
(a) The original frame-1.



(b) The pixelwise of the original frame-1.



(c) The watermarked frame-1.

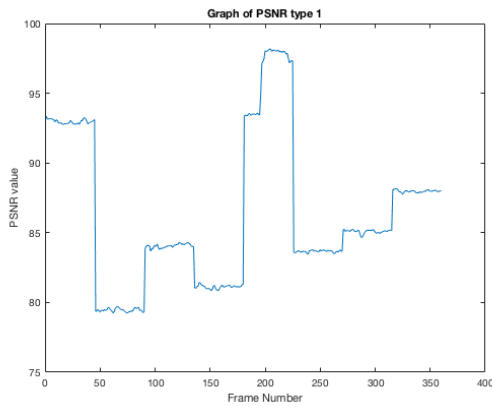


(d) The pixelwise of watermarked frame-1.

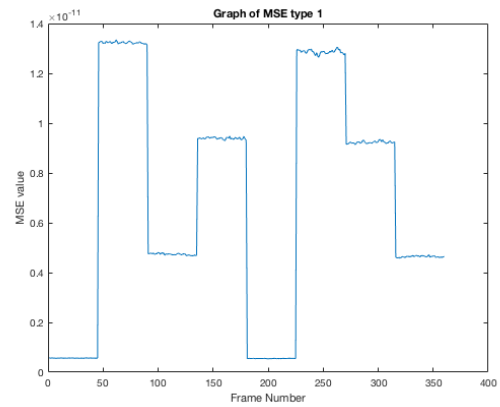
Figure 15: The comparison of frame type 1.

#### 4.2.1 Analysis point selection type 1 : (1,1) to (512,512)

The Fig.16 illustrates the overall value of PSNR and MSE. The average of PSNR for type 1 is 86.3321%, and the average of MSE is 6.9020.



(a) The graph of PSNR of type 1.

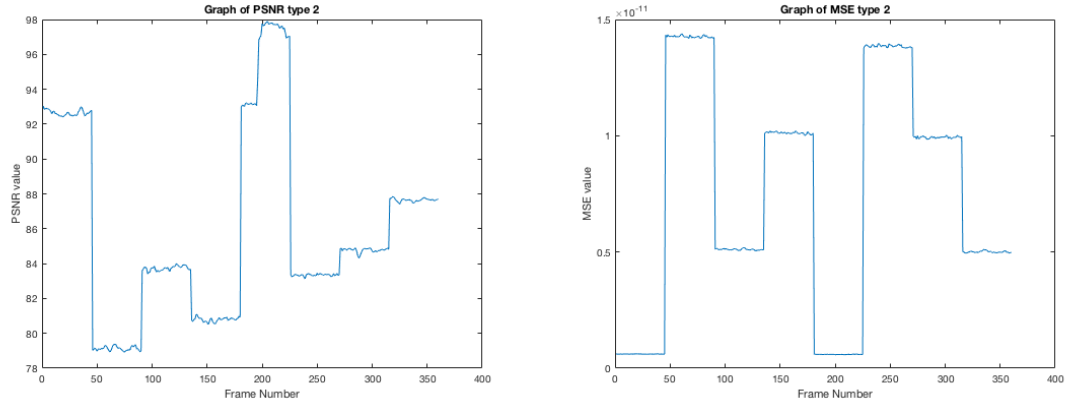


(b) The graph of MSE of type 1.

Figure 16: Analysis of slice type 1.

#### 4.2.2 Analysis point selection type 2 : (51, 1) to (335, 512)

The Fig.17 below illustrates the overall value of PSNR and MSE. The average of PSNR for type 2 is 86.0075%, and the average of MSE is 7.4367.



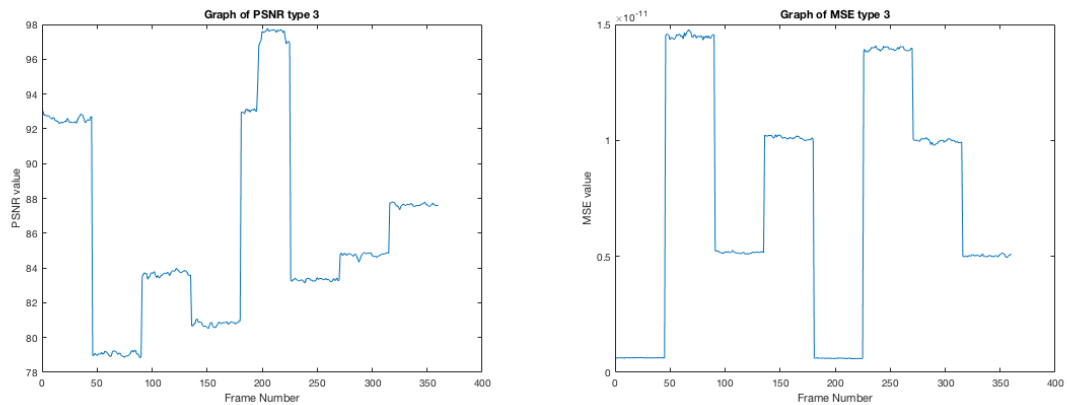
(a) The graph of PSNR of type 2.

(b) The graph of MSE of type 2.

Figure 17: Analysis of slice type 2.

#### 4.2.3 Analysis point selection type 3 : (352, 1) to (352, 512)

The Fig.18 illustrates the overall value of PSNR and MSE. The average of PSNR for type 3 is 85.9616%, and the average of MSE is 7.4968.



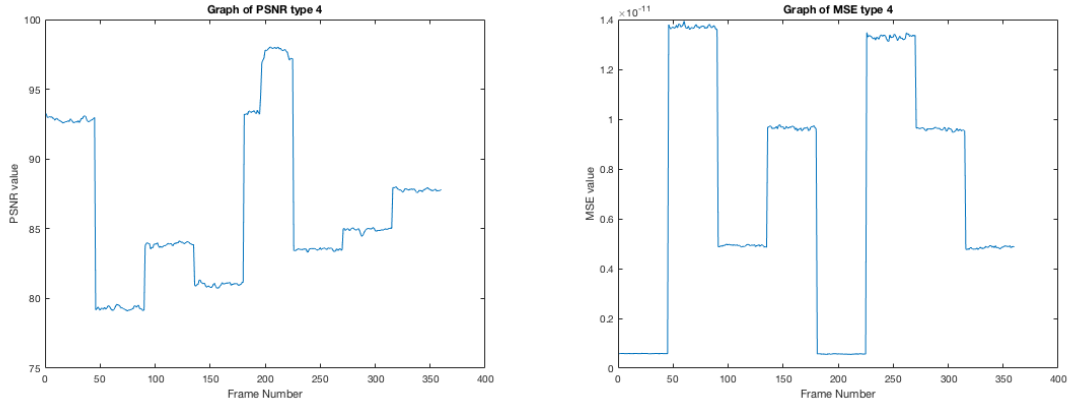
(a) The graph of PSNR of type 3.

(b) The graph of MSE of type 3.

Figure 18: Analysis the slice type 3.

#### 4.2.4 Analysis point selection type 4 : (1, 32) to (512, 433)

The Fig. 19 below illustrates the overall value of PSNR and MSE. The average of PSNR for type 4 is 86.1761%, and the average of MSE is 7.1479.



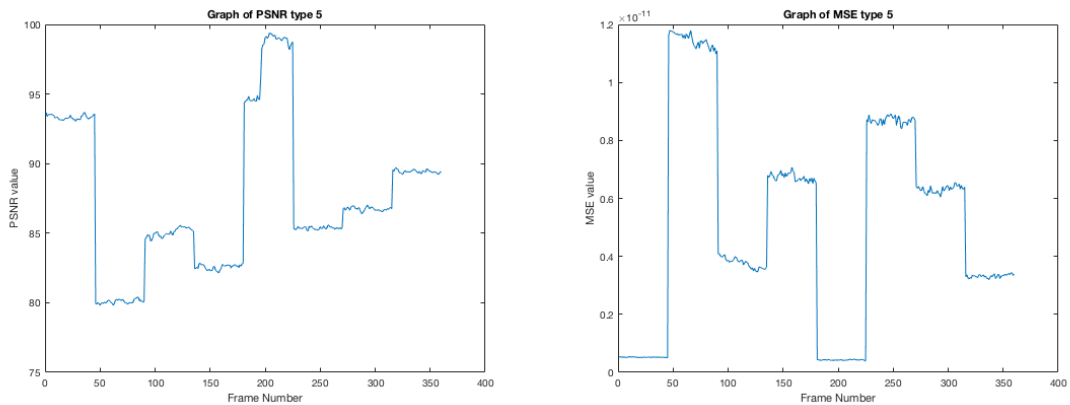
(a) The graph of PSNR of type 4.

(b) The graph of MSE of type 4.

Figure 19: Analysis of slice type 4.

#### 4.2.5 Analysis point selection type 5 : (1, 105) to (512, 105)

The Fig. ?? below illustrates the overall value of PSNR and MSE. The average of PSNR for type 5 is 87.4984%, and the average of MSE is 5.1557.



(a) The graph of PSNR of type 5.






(b) The graph of MSE of type 5.

Figure 20: Analysis of slice type 5.

Table 1

### 4.3 Analysis of decryption of the logo

In the table. 1, we show the decrypted logo from each type

Point selection	Decrypted logo	MSE	BER %	NCC
Type 1		7774.3424	12.0486	1
Type 2		9358.5299	15.2083	-1
Type 3		7638.8736	11.8403	1
Type 4		8341.0976	13.3681	1
Type 5		7638.8736	11.8403	1

## 5 Conclusion

In this thesis, we present the new method; 3D watermarking secret direction scheme for volumetric DICOM images. We studied some effects from various secret directions. Significant changes are visible after the logo is decrypted.

For the  $XY$ -secret direction holds an enormous influence in determining the watermarked logo it has not changed or changed after the logo is decrypted. As for the  $t$ -secret direction also holds control but not as significant as the secret- $XY$  direction.

The experimental results show that the secret scheme of 3D watermarking direction can ensure the integrity of volumetric DICOM images efficiently.

In this thesis, we did not consider how robust the attack might be on the watermarked images of our proposed method. Thus, future work should include any kind of attack that could happen on watermarked DICOM images.

## 6 Acknowledgement

I would like to express my sincere gratitude to my advisor Prof. Mario KÖPPEN for the continuous support of my master study and research, for his patience, motivation, enthusiasm, and immense knowledge. His guidance helped me in all the time of study and writing of this thesis. I could not have imagined having a better advisor and mentor for my master study.

Besides my advisor, I would like to thank the rest of my thesis committee: Prof. Kushiro Noriyuki and Prof. Kenichi Korai.

I thank my labmates: Dwilya Delia, Naohiro Iwamoto, Yuta Okuzono, Sajjad Dadkhah, Andi Arnie, Willa Ariela, Anita Amalia Hak Bisyu for the stimulating discussions, for all the fun we have had in the last two years.

Last but not the least, I would like to thank my family: my parents Muhammad Yusuf Nur and Ani Widya Maharani, and also my stepmother Rosmini Rasyid for supporting me spiritually throughout my life.

18 February 2018

Ajif Yunizar Pratama Yusuf

## List of Figures

1	A series of DICOM images is three-dimensional form. . . . .	3
2	The drawing line concept using Bresenham algorithm[5]. . . . .	4
3	Flowchart of 3D watermarking secret direction scheme. . . . .	5
4	Encrypt logo process. . . . .	6
5	Five types of line slicing image. . . . .	8
6	Five types of slicing image, with the resolutions $360 \times 520$ for each type. . . . .	9
7	The scrambling slice type-1. . . . .	10
8	The scrambling slice type-2. . . . .	11
9	The scrambling slice type-3. . . . .	11
10	The scrambling slice type-4. . . . .	11
11	The scrambling slice type-5. . . . .	12
12	Decryption of the logo of all types. . . . .	13
13	The Slice type-1, PSNR = 84.5176. . . . .	14
14	The Slice type-2, PSNR = 84.1935. . . . .	15
15	The comparison of frame type 1. . . . .	16
16	Analysis of slice type 1. . . . .	16
17	Analysis of slice type 2. . . . .	17
18	Analysis the slice type 3. . . . .	17
19	Analysis of slice type 4. . . . .	18
20	Analysis of slice type 5. . . . .	18

## References

- [1] Zheng Zhou, HK Huang, and BJ Liu. Three-dimensional lossless digital signature embedding for the integrity of volumetric images. In *Proc. of SPIE Vol*, volume 6145, pages 61450R–1, 2006.
- [2] A Ouled Zaid, Achraf Makhloufi, Ammar Bouallegue, and Christian Olivier. Jp3d compressed-domain watermarking of still and volumetric medical images. *Signal, Image and Video Processing*, 4(1):11–21, 2010.
- [3] Luiz OM Kobayashi and Sergio S Furuie. Proposal for dicom multiframe medical image integrity and authenticity. *Journal of digital imaging*, 22(1):71–83, 2009.
- [4] Wenbo Dou, Chueh Loo Poh, and Yong Liang Guan. An improved tamper detection and localization scheme for volumetric dicom images. *Journal of digital imaging*, 25(6):751–763, 2012.
- [5] Bresenham’s line algorithm . [https://en.wikipedia.org/wiki/Bresenham%27s\\_line\\_algorithm](https://en.wikipedia.org/wiki/Bresenham%27s_line_algorithm). [Online accessed 6-February-2018].