國立臺灣大學電機資訊學院資訊工程學研究所

碩士論文

Department of Computer Science and Information Engineering
College of Electrical Engineering and Computer Science
National Taiwan University

Master Thesis

基於直方圖預測誤差的兩位嵌入可逆數據隱藏法及其於醫學圖像平滑區域的應用

Two-bit embedding Histogram-Prediction-Error based Reversible Data Hiding for Medical images with Smooth Area

楊謦羽

Ching-Yu Yang

指導教授：吳家麟 博士

Advisor: Chia-Lin Wu, Ph.D.

中華民國 110 年 5 月

May, 2021

doi:10.6342/NTU202101171

口試委員審定書

國立臺灣大學碩士學位論文
口試委員會審定書

基於直方圖預測誤差的兩位嵌入可逆數據隱藏法及其於醫學圖像平滑區域的應用

Two-bit embedding Histogram-Prediction-Error based Reversible Data Hiding for Medical images with Smooth Area

本論文係楊聲羽君（學號 R08922145）在國立臺灣大學資訊工程學系完成之碩士學位論文，於民國 110 年 5 月 26 日承下列考試委員審查通過及口試及格，特此證明

口試委員：

吳家麟

陳俊良（指導教授）

周承復

陳駿丞

系主任 洪士灝

doi:10.6342/NTU202101171

國立臺灣大學碩士學位論文
口試委員會審定書

基於直方圖預測誤差的兩位嵌入可逆數據隱藏法及其於醫學圖像平滑區域的應用

Two-bit embedding Histogram-Prediction-Error based Reversible Data Hiding for Medical images with Smooth Area

本論文係楊謦羽君（學號R08922145）在國立臺灣大學資訊工程學系完成之碩士學位論文，於民國 110 年 5 月 26 日承下列考試委員審查通過及口試及格，特此證明

口試委員：吳家麟

張瑞澎（指導教授）

系主任 洪士灝

doi:10.6342/NTU202101171

中文摘要

近年來，病人隱私權保護日益受到重視。病人在治療過程中，多處可能涉及個人私密，例如醫院對病人所拍攝的醫療影像以及相關病情或健康資訊依法不得無故對外洩漏。

可逆式隱寫術 (reversible data hiding) 是一種能將元資料 (meta data) 嵌入影像，並且可無失真回完全復原始影像的資料隱藏技術。本研究旨在提出一個適合於醫學影像的完全可逆並具有高資訊容量的隱寫術 (Steganography)演算法。

醫學影像的 Region of Interest (ROI)為整張影像中具有重要醫學資訊的部分，一般而言醫學影像需要高解析度以分析影像中細微的變化。本研究利用分布圖位移 (histogram Shift) 及預測差異 (prediction error) 技術，再輔以醫學影像中的非 ROI 區域所具像素平滑之特性，設計出所謂“兩位元嵌入”之演算法，並將嵌入資料藏於影像中的非 ROI 區域。此算法的最大優點是“完全可逆”且擁有“高資訊容納量”並同時達到將醫學影像中 ROI 因資料嵌入所造成之失真度降至最低的目的。

為了驗證本研究提出方法的有效性，我們測試了三種 DICOM 格式的醫學影像，分別為 X 光攝影像 (X-ray)、電腦斷層攝影像(CT)以及核磁共振影像 (MRI)。結果顯示，隱藏資訊大多會被嵌入於醫學影像中的非 ROI 區域，且此方法較其他類似方法具有更高的資訊容納量。

關鍵字：隱寫術、可逆式隱寫術、分佈圖位移、預測差異、醫學影像、ROI、病人隱私權

doi:10.6342/NTU202101171

ABSTRACT

In recent years, patients' privacy attracts extensive attention worldwide. During the treatment, personal privacy is involved. Medical images or health information must not be leaked without reason. Reversible data hiding is a technique that embeds meta data into an image and can be recovered without any distortion after the hidden data have been extracted. This thesis targets at proposing a two-bit embedding reversible data hiding algorithm with large hiding capacity for medical images.

Medical image can be partition into the region of interest (ROI) and region of noninterest (RONI). ROI is an important information in the medical image, and cannot tolerant subtle changes. Hence, reducing distortion in ROI is our primary goal. We observe that RONI is a smoother area in medical image. In this thesis, we utilize histogram shifting and prediction error to embed meta data into RONI. In addition, our embedding algorithm minimize the side effect to ROI and completely can be recovered when required.

In order to verify the proposed method in this thesis, we used three types of medical images in DICOM format, namely X-ray photography (X-ray), computer tomography (CT), and magnetic resonance imaging (MRI). Experiment results show that most of the hidden data have been embedded in RONI, and the performance achieve high capacity and less distortion to the ROI.

Keywords: Data Hiding, Reversible Data Hiding, Histogram Shifting, Prediction Error, Medical Image, ROI, Patient's Privacy

doi:10.6342/NTU202101171

CONTENTS

doi:10.6342/NTU202101171

doi:10.6342/NTU202101171

LIST OF FIGURES

doi:10.6342/NTU202101171

LIST OF TABLES

doi:10.6342/NTU202101171

Chapter 1

Introduction

1.1 Motivation

Over the past two decades, data hiding has developed rapidly because of strong demand for secure communication and copyright protection. This technology can be applied in multimedia, such as text, image, audio, video. Data hiding use the redundancy of the cover data to hide information imperceptibly. In this thesis, we use image as our cover data. However, in the distortion-sensitive application such as military and medical fields, the integrity of the data is very important. Reversible data hiding was first proposed by Barton [1] which allows information to be extracted and the cover image can be recovered when required. As a result, reversible data hiding is widely used in the medical and military fields.

Data hiding is mainly divided into two major categories, that is, Digital Watermarking [15] and Steganography 錯誤！找不到參照來源。. Digital Watermarking technology embeds copyright-related information (author information, company trademark, etc.) into the cover data in order to protect the copyright and prove the authenticity. Steganography technology also embeds information into the cover data but it is imperceptible to unauthorized access or adversary. The purpose of steganography is to protect hidden data. The difference between cryptography and steganography is that cryptography make the encrypted secret message looks like error

doi:10.6342/NTU202101171

codes. When the adversary receives the encrypted data, he knows the existence of the secret message. However, steganography makes embedded data imperceptible. Therefore, after the adversary get the cover data, he does not know the existence of the hidden information, so it can reduce the possibility of being attacked.

Data hiding is widely used in various application, such as video, audio, and image. In this thesis, the issue we discussed is application for medical image. In the hospital, patient may take several medical images and meanwhile, medical data related to patient are recorded in these images. However, if the hospital's database administrator accesses these images, the medical data are leaked, and “medical data breach” are happened. The hypothetical scenario is illustrated in Fig. 1-1.

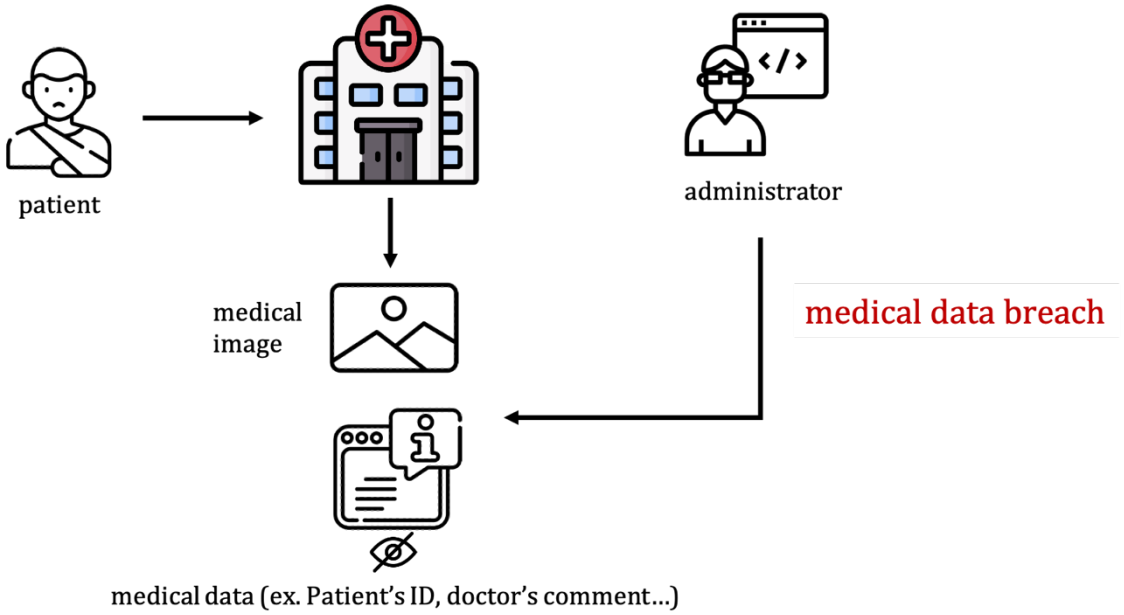


Fig. 1-1 Overview of the hypothetical scenario

In order to deal with the problem mentioned above, our scheme embed data into medical image. Since the medical image is distortion-sensitive, patients may be misdiagnosed due to any subtle changes of image, so we use reversible data hiding technique to recover the original image after hidden data have been extracted. The

doi:10.6342/NTU202101171

overview of the application scenario is shown in Fig. 1-2.

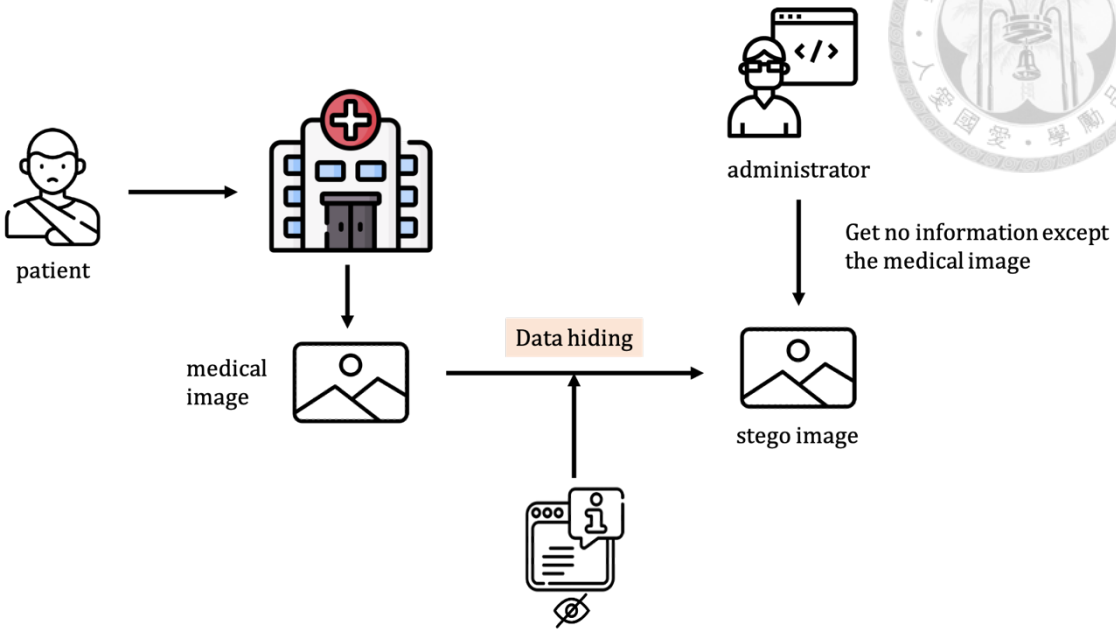


Fig. 1-2 Overview of the application scenario

We categorize reversible data hiding method into three domains, that is, spatial domain, frequency domain, and compression domain. Spatial domain method embed data into the least significant bit (LSB) of pixel in the image, which has good concealment. Since no additional transformation is required, the computational complexity is low, but the disadvantages are poor security and robustness. Frequency domain method transform the cover data into the frequency domain, such as using Fourier Transform. Then, hidden data are embedded in the frequency domain, and transform back to the spatial domain. The advantage is that it has good robustness to the shearing attack, but it requires extra time for the transformation. Reversible data hiding in the compressed domain such as JPEG, decodes the JPEG to get the decoded image first, and embed the data into it. Finally encode the image with the hidden data into JPEG format. The disadvantage is that the performance of this method is greatly related to the nature of the image.

doi:10.6342/NTU202101171

Most of the reversible data hiding is applied in spatial domain, because of the intuitive algorithm and low computation cost. The methods of spatial domain include Difference Expansion (DE), Histogram Shifting (HS), and LSB Modification, etc. More detailed discussion is in the Chapter 2. Our proposed algorithm is based on histogram shifting.

1.2 Basic characteristic of data hiding

According to the purpose of data hiding, the characteristics are mentioned below [2]:

(a) Imperceptibility

After the data hiding is processed, the quality of cover data must be maintained, and the embedded data cannot be detected by human sensory system. This is the most basic characteristic of data hiding.

(b) Undetectability

Embedded data and cover data have some data characteristics, such as noise distribution, entropy, etc. Even through the analysis of data characteristics, unauthorized receiver cannot know whether there is embedded information or not.

(c) Capacity

It is also called the embedding rate or effective payload, which is the maximum amount of information can be embedded in the host data.

(d) Efficiency

The efficiency here means to consider the time required to perform reversible data hiding

However, it is difficult for any data hiding algorithm to take into account all characteristics, because these characteristics are contradictory. For example, if we want

doi:10.6342/NTU202101171

to achieve a high capacity, we need to modify the cover data by a large, which will increase the noise and may lose the imperceptibility. Considering to the characteristics of medical image, we mainly focus on capacity and imperceptibility. The goal of our research is to maximize capacity without losing imperceptibility.

1.3 Evaluation metric of proposed scheme

As mentioned above, our goal is to achieve high capacity and imperceptibility, so we use following evaluation metrics to verify our algorithm.

(a) Capacity

We measure the maximum amount of data that can be embedded in the medical image.

(b) Peak signal-to-noise ratio (PSNR)

PSNR is the most common and widely used objective measurement for image quality assessment which is defined by Mean Square Error (MSE). Given an $m \times n$ reference image *I* and a noisy image *K*, MSE is defined as (1-1):

$$\mathrm{MSE} = \frac{1}{\mathrm{mn}} \sum_{\mathrm{i}=0}^{\mathrm{m-1}} \sum_{\mathrm{j}=0}^{\mathrm{n-1}} [\mathrm{I(i,j)\text{-}K(i,j)}]^2 \qquad (1\text{-}1)$$

Then, PSNR is defined as (1-2):

$$\mathrm{PSNR} = 10 \times \log_{10}(\frac{\mathrm{MAX_I^2}}{\mathrm{MSE}}) \qquad (1\text{-}2)$$

$\mathrm{MAX_I^2}$ is the maximum value of the image.

However, according to many experimental results, the PSNR score cannot be exactly match the Human Vision System (HVS), so we also use another method SSIM mentioned below to make the experiment more complete.

(c) Structural similarity index measure (SSIM)

doi:10.6342/NTU202101171

The basic idea of SSIM is to evaluate the similarity of two images *x*, *y*, through the luminance (*l*), contrast (*c*) and structure (*s*) defined as (1-3), (1-4), (1-5):

$$l(x,y) = \frac{2\mu_x\mu_y + c_1}{\mu_x^2 + \mu_y^2 + c_1} \tag{1-3}$$

$$c(x,y) = \frac{2\sigma_x\sigma_y + c_2}{\sigma_x^2 + \sigma_y^2 + c_2} \tag{1-4}$$

$$s(x,y) = \frac{\sigma_{xy} + c_3}{\sigma_x\sigma_y + c_3} \tag{1-5}$$

μ_x is the average of *x*, and μ_y is the average of *y*. σ_x^2 is the variance of *x*, and σ_y^2 is the variance of y. σ_{xy} is the covariance of *x* and *y*. c_1, c_2, and c_3 are constants to avoid dividing by zero.

Then, SSIM is defined as (1-6):

$$SSIM(x,y) = \frac{(2\mu_x\mu_y + c_1)(2\sigma_{xy} + c_2)}{(\mu_x^2 + \mu_y^2 + c_1)(\sigma_x^2 + \sigma_y^2 + c_2)} \tag{1-6}$$

According to many experimental results, the evaluation performance of SSIM is closer to the human visual system than PSNR.

We implement above three methods to compare with other papers. More detailed discussion is in the Chapter 4.

1.4 Contribution

In our work, we design a novel reversible data hiding scheme that utilizes smooth area of medical image to embed data. We apply proposed scheme to MRI images, CT images, and X-ray images. The major contributions of this thesis are listed as follows.

(a) We present a novel two-bit embedding algorithm for reversible data hiding, that used medical image as inputs and achieve high capacity and less distortion.

(b) We propose a local complexity function that suitable for our two-bit embedding

doi:10.6342/NTU202101171

algorithm to select which pixel embedded first. Results show that our algorithm embed most of hidden data in RONI of medical image, and causes less distortion in ROI.

(c) Since there are several types of medical image. We used three common types, such as MRI, CT, X-ray to verify feasibility of our algorithm. Experiment results show that our algorithm achieve a good performance and suitable for these types of images.

1.5 Thesis Organization

In Chapter 1, we have introduced the motivation of our work which aims to propose a novel two-bit embedding reversible data hiding using histogram shifting and achieves good results in the medical image with smooth area. We have also discussed the main application and basic characteristic of data hiding technology. The evaluation metric of our scheme and the contributions of this thesis are also mentioned above. The rest of the thesis are organized as follows:

In Chapter 2, we are going to introduce several related works of data hiding and some famous method in spatial domain. First, digital watermarking and steganography are presented. In addition, we will compare the goal and application scenario of these two techniques. Moreover, we are going to discuss some mechanisms of reversible data hiding in spatial domain. Last but not the least, we will list several advantages and disadvantages of these methods.

In Chapter 3, we will present a comprehensive description of our proposed reversible data hiding algorithm in detail. In the beginning, we are going to introduce the prediction error histogram and its benefits. After that, we will give an overview of

doi:10.6342/NTU202101171

the histogram-prediction-error based two-bit embedding reversible data hiding scheme proposed in this thesis. Then, embedding algorithm and how to perform extraction and recovery will be introduced. Finally, we will describe the pipeline of encoder and decoder.

In Chapter 4, we will introduce several public databases, which include CT-type, MRI-type, X-ray type medical images and other commonly used images. Then, we are going to describe several evaluation metrics used in this thesis. Finally, we will present the experimental results of our proposed two-bit embedding method in comparison with other state-of-the-art histogram-based frameworks on medical images.

In Chapter 5, we will discuss the experimental results and conclude the contributions of this thesis. Finally, we are going to bring up a discussion on the future work.

doi:10.6342/NTU202101171

Chapter 2

Related Work

In this chapter, we are going to introduce some existing applications of data hiding. That is, steganography and digital watermarking which are categorized by the purpose of these application. Next, we will introduce common several approaches of reversible data hiding.

2.1 Steganography and Digital Watermarking

(a) Steganography

Steganography technique hides secret message in cover data. The same purpose of steganography and cryptography is to protect secret message. In cryptography, the secret message after encryption called ciphertext, and the cover image which has been embedded secret message by steganography called stego-image. The main difference is that ciphertext looks like an error code (see Fig. 2-1). After the attacker receives the encrypted message, he already knows that it exists secret message. On the contrary, steganography makes secret message imperceptible, so attacker cannot detect the existence of secret message (see Fig. 2-2).

doi:10.6342/NTU202101171

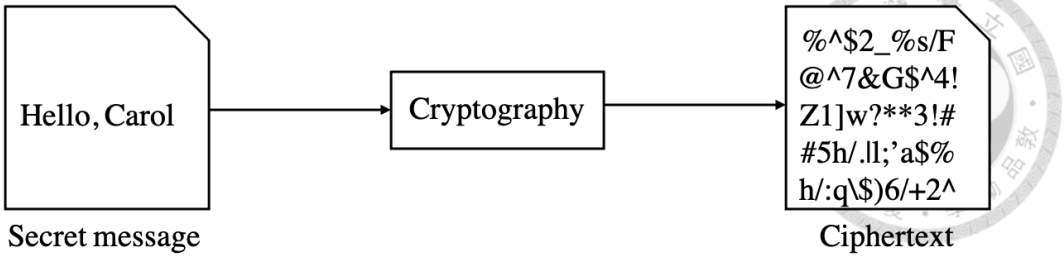


Fig. 2-1 Framework of cryptography

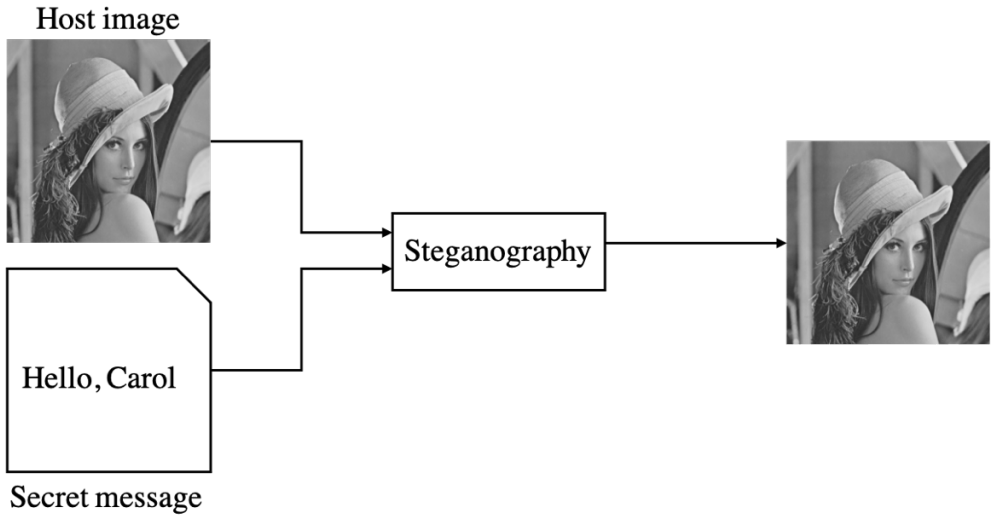


Fig. 2-2 Framework of steganography

(b) Digital Watermarking

Digital watermarking is a branch of data hiding, and it also embeds data into cover media. The purposes of digital watermarking are protecting copyright of digital work, proving the authenticity, tracking piracy, and so on. Therefore, digital watermarking focus on hiding some specific information into digital work, such as author information, company trademarks, product numbers. According to the different scenario, digital watermarking can be visible or invisible. Since digital works may be illegally operated by others, so robustness of digital watermarking is the most important.

Protecting the hidden data is the main purpose of steganography, while digital

doi:10.6342/NTU202101171

watermarking protects the cover data, Table 2-1 shows the major differences between steganography and digital watermarking. The goal of this thesis is to embed the information into the medical image which is related to the patient privacy. Therefore, we utilized steganography technique to implement reversible data hiding.

Table 2-1 Differences between steganography and digital watermarking.

Technique	steganography	digital watermarking
Objective	Focus on maintaining existence of a message secret, or secret communication.	Focus on marking the digital works with copyright-related information to avoid illegal access.
Visibility	Invisibility.	Invisibility or visibility depending on the requirements.
Security	The hidden message is imperceptible.	Verify the authenticity or integrity of the digital works.

2.2 Approaches of Reversible Data Hiding

Before we introduce our proposed framework, we present several state-of-the-art reversible data hiding algorithms first. These algorithms are LSB substitution, Difference expansion (DE) and Histogram shifting (HS).

2.2.1 LSB substitution

The least-significant-bit (LSB) substitution embeds the secret message in the LSB of pixels. Typical approaches include Wang [3], Chan [4], and Celik et al. [5]. The general operation of LSB substitution method is described below. For example, given a 3×3, 8-bit grayscale image, then convert it into binary representation as follows:

doi:10.6342/NTU202101171

01100110	01010101	01001011
11001011	10100010	01010111
11101110	11111101	00101010

Now we have a secret message 101100010, which is embedded into the LSBs of this grayscale image. The result is shown as follows, and the underlined bits have been modified.

0110011**1**	0101010**0**	01001011
11001011	10100010	0101011**0**
11101110	1111110**0**	00101010

The advantage of this method is that the algorithm is intuitive, and the distortion of the cover image is small, which satisfies the imperceptibility. However, the hidden message may be lost through image processing. The disadvantage is that it is not robust and vulnerable to attack.

2.2.2 Difference expansion

Difference expansion was proposed by Tian [6] in 2003. The algorithm utilizes pair of the pixel (x, y) in grayscale image, and calculate the difference $h = x\text{-}y$. Then, the secret message will be hidden in the LSB of h. The general operation of DE method is described as follow. For example, we have a pair of pixels (x, y). Assume $x = 206$, $y = 201$, and the hidden bit $b = 1$. First, we calculate the average l and difference h of x and y.

doi:10.6342/NTU202101171

$$l = \lfloor (x + y)/2 \rfloor = \lfloor (206 + 201)/2 \rfloor = 203$$

$$h = x\text{-}y = 206\text{-}201 = 5$$

Next, we transfer the value h into binary representation $h = (101)_2$. Then we append the hidden bit b to h, and get the new difference h'.

$$h' = (101b)_2 = (1011)_2 = 11.$$

Based on new value h' and average l, we calculate new value of pair of pixels (x', y').

$$x' = 203 + \lfloor (11 + 1)/2 \rfloor = 209$$

$$y' = 203\text{-}\lfloor 11/2 \rfloor = 198$$

When we need to extract the hidden message, we compute the difference h' and average l'. Then we can retrieve the hidden message by the LSB of h'.

$$h' = 209\text{-}198 = 11$$

$$l' = \lfloor (209 + 198)/2 \rfloor = 203$$

$$b = \mathrm{LSB}(h') = 1$$

$$h = \lfloor h'/2 \rfloor = 5$$

Finally, we can recover the original pair of pixels (x, y).

$$x = 203 + \lfloor (5 + 1)/2 \rfloor = 206$$

$$y = 203\text{-}\lfloor 5/2 \rfloor = 201$$

The advantage of this method is that the algorithm is simple and capacity is high. Due to h' in the algorithm, the pixel value will move to both sides in the histogram, and the change of the pixel value is uniform. However, the disadvantage is that because difference value is multiplied by 2, it may cause significant distortion of visual quality.

2.2.3 Histogram shifting

Histogram shifting was proposed by Ni et al [7] in 2006. The general operation of

doi:10.6342/NTU202101171

histogram shifting method is described as follow [8]. First, we find the peak point of image histogram as shown in Fig. 2-3.

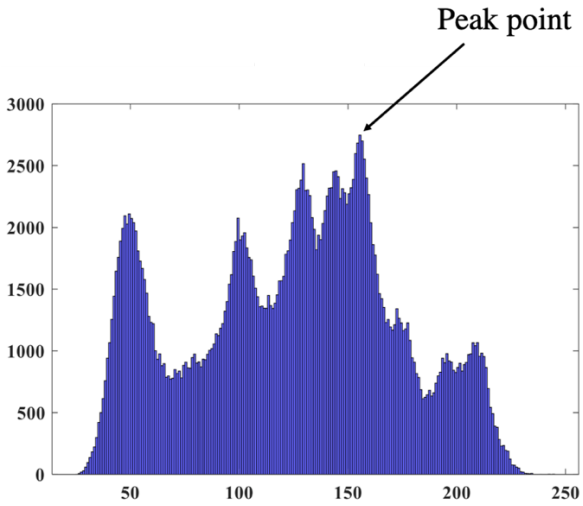
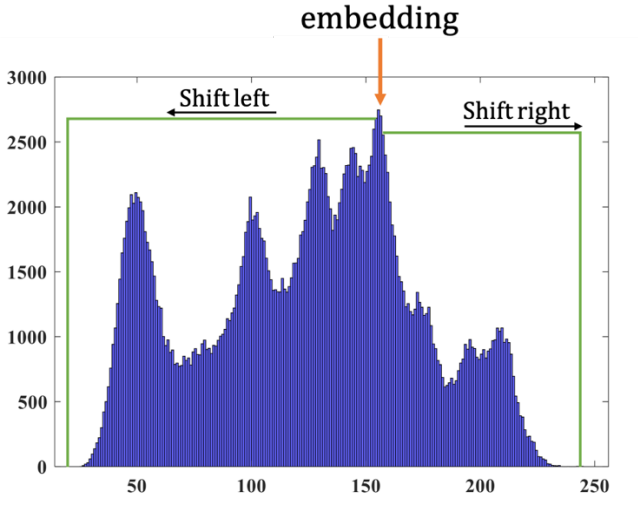


Fig. 2-3 Histogram of Lena

Then the embedding function defined as (2-1)

$$p' = \begin{cases} p + b & \text{if } p = k \\ p\text{-}b & \text{if } p = k\text{-}1 \\ p + 1 & \text{if } p > k \\ p\text{-}1 & \text{if } p < k\text{-}1 \end{cases} \qquad (2\text{-}1)$$

$b \in \{0,1\}$ is the hidden bit, and k is the peak value. p is value of the original pixel, and p' is value of modified pixel. The implementation of the histogram shifting is shown in Fig. 2-4



doi:10.6342/NTU202101171

Fig. 2-4 Histogram shifting

Capacity of this method is limited by the peak point of the histogram. In order to solve this problem, prediction error of adjacency pixels instead of pixel value is used [11]. Prediction-error-based methods significantly improve the capacity. The advantages of histogram shifting are high payload and invisible to the distortion. Our proposed method utilize histogram shifting to implement the reversible data hiding which will be described in detail in Chapter 3.

doi:10.6342/NTU202101171

Chapter 3

Proposed Method

In this chapter, we investigate a novel two-bit embedding reversible data hiding method based on the framework proposed by Kim et al. [14], which utilizes even and odd embedding. In Kim et al.'s work, pixels are divided into even and odd set. If the sum of a pixel's horizontal and vertical position is even value, it will be categorized into even set. On the contrary, if the sum is odd value, it will be categorized into odd set.

Firstly, we present the prediction error histogram which can be used to embed hidden data based on the even and odd embedding. Next, we are going to comprehensively introduce the proposed reversible data hiding framework, which aim to embed the secret message into smooth area of medical image. We utilized the local complexity function to help embedding message in the RONI. In addition, our method achieves high capacity and keeps the ROI almost unchanged.

3.1 Prediction Error Histogram

The original histogram shifting method has the limitation of the capacity which is dominated by the peak point of histogram. In order to deal with this problem, we transform histogram into prediction error domain, such as prediction error histogram (PEH). First, we use four neighboring pixel values {N, W, S, E} (Fig. 3-1) to calculate the prediction value $\hat{p}$ by the follow equation (3-1):

doi:10.6342/NTU202101171

$$\hat{p} = \left[\frac{(N + W + S + E)}{4}\right] \quad (3\text{-}1)$$

Then, we compute prediction error p_e by the follow equation (3-2):

$$p_e = p\text{-}\hat{p} \quad (3\text{-}2)$$

Finally, we generate the prediction error histogram (see Fig. 3-2). As shown in the figure, after doing conversion, the peak point gathers around 0 value. We are going to use this feature to embed the data in the zero position. More details of the algorithm will be described in the next section.

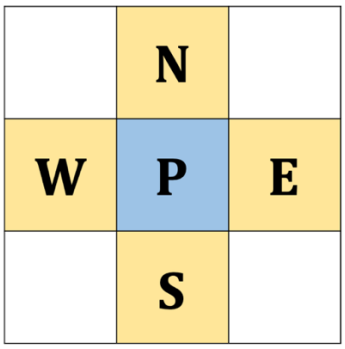


Fig. 3-1 neighboring pixels

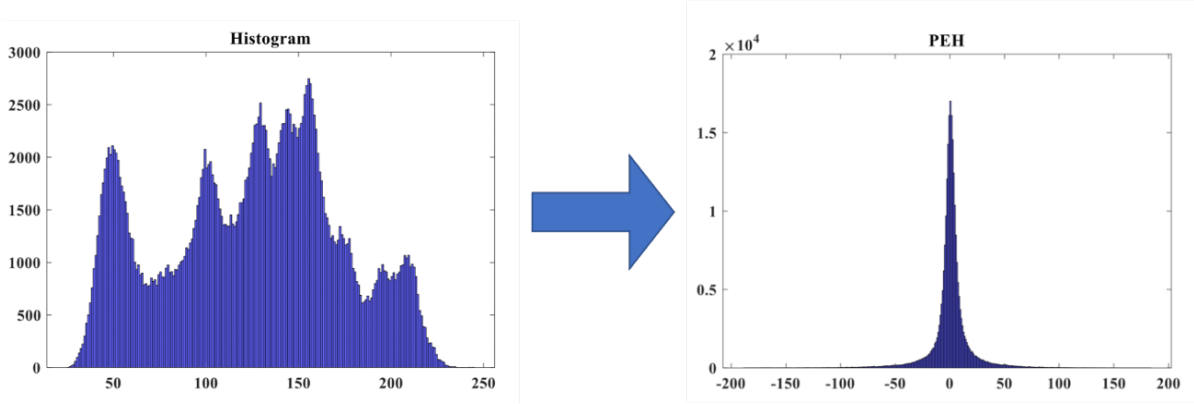


Fig. 3-2 Example of transforming histogram to PEH

doi:10.6342/NTU202101171

3.2 Embedding

Before embedding, we need to mention that medical images contain a lot of pixels with zero value, so the pixel with zero value are directly skipped during the embedding process. Our proposed scheme embeds message based on even and odd embedding. First, we categorize pixels into even set and odd set (see Fig. 3-3). Pixels are categorized into even set which have even sum of its horizontal position value and vertical position value, and vice versa. Note that the two set are independent. Therefore, once the pixel in one set is modified, it won't affect the other set. We can use this property to compute prediction value $\hat{p}$. The algorithm is divided into two rounds, so each pixel is embedded twice through the algorithm. Before performing our algorithm, we convert hidden data into binary.

First round, the prediction error is $p-\hat{p}$, and we embed one message bit in p by follow equation (3-3):

$$p' = \begin{cases} p + b_1 & \text{if } p-\hat{p} = 0 \\ p + 1 & \text{if } p-\hat{p} > 0 \\ p & \text{else} \end{cases} \tag{3-3}$$

where p' is the stego pixel, and $b_1 \in \{0,1\}$ is the embedded message bit in first round. Message bit will be embedded only when prediction error is 0, which means that value of p has the same value as the average of the surrounding pixels. When prediction error is strictly positive, pixels will be shifted positively by 1, and other pixels will remain the same.

Second round, the prediction error is $p'-\hat{p}$, and we embed one message bit in p' by follow equation (3-4):

$$p'' = \begin{cases} p' + b_2 & \text{if } p'-\hat{p} = 0 \\ p'-1 & \text{if } p'-\hat{p} < 0 \\ p' & \text{else} \end{cases} \tag{3-4}$$

doi:10.6342/NTU202101171

where p'' is the stego pixel embedded twice, and $b_2 \in \{0,1\}$ is the embedded message bit in second round. Message bit will be embedded only when prediction error is 0, which means that value of p' is the same as the average of the surrounding pixels. When prediction error is strictly negative, pixels will be shifted negatively by 1, and other pixels will remain the same.

Note that RONI is relatively smooth region in whole image, and our algorithm is designed by this feature. Therefore, we can keep the ROI unchanged. Embedding example in smooth area is described in Fig. 3-4. The main advantage of our algorithm is two-bit embedded in one pixel.

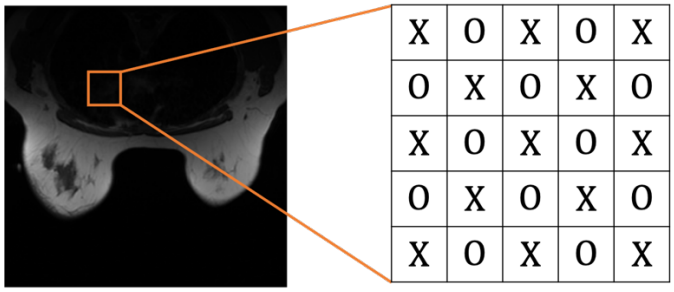


Fig. 3-3 'X' represents even set and 'O' represents odd set

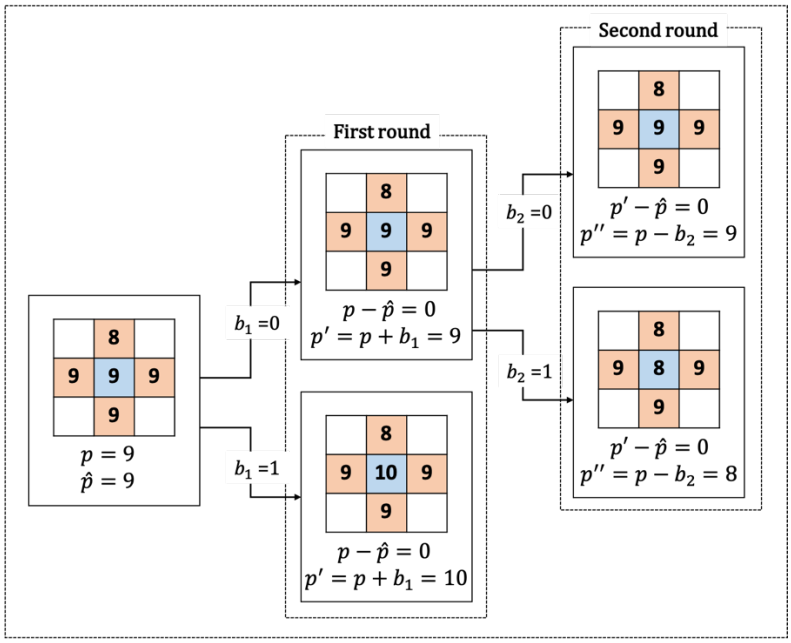


Fig. 3-4 Embedding example in smooth area

doi:10.6342/NTU202101171

3.3 Extraction and Recovery

In this section, we introduce how to extract the hidden data and recover original image. Since the pixel with zero value were skipped during the embedding process. Similarly, in the process of extraction and recovery, pixels with zero value will be skipped, too. Extraction and recovery are done in reverse order of embedding, that is, odd set will be recovered first, then even set. Embedded message bits b_2 in second round is extracted by the following function (3-5):

$$b_2 = \begin{cases} 0 & \text{if } p''\text{-}\hat{p} = 0 \\ 1 & \text{if } p''\text{-}\hat{p} = -1 \end{cases} \tag{3-5}$$

Recovery of p' in second round is done by the following function (3-6):

$$p' = \begin{cases} p'' + 1 & \text{if } p''\text{-}\hat{p} < 0 \\ p'' & \text{else} \end{cases} \tag{3-6}$$

After second round is recover, embedded message bits b_1 in first round is extracted by the following function (3-7):

$$b_1 = \begin{cases} 0 & \text{if } p'\text{-}\hat{p} = 0 \\ 1 & \text{if } p'\text{-}\hat{p} = 1 \end{cases} \tag{3-7}$$

Then, recovery of p in second round can be done by the following function (3-8):

$$p = \begin{cases} p' + 1 & \text{if } p'\text{-}\hat{p} > 0 \\ p' & \text{else} \end{cases} \tag{3-8}$$

Example of extraction and recovery are described in Fig. 3-5.

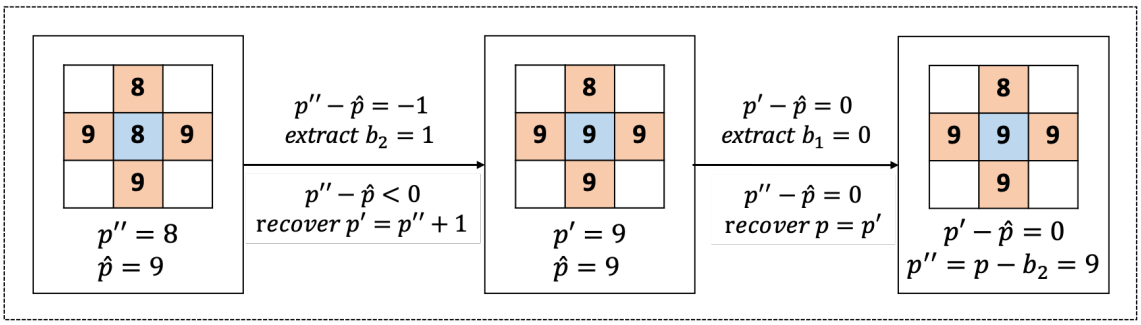


Fig. 3-5 Example of extraction and recovery

doi:10.6342/NTU202101171

Then, even set is recovered and extracted by repeating the same step. Embedding order of each pixel in one set is depending on local complexity function which is going to be presented in next section.

3.4 Local complexity function

Due to the RONI is relatively smooth compared to the ROI, we utilize this feature to select pixel which is embedded first. We designed a local complexity function to deal with pixel selection in order to reduce the distortion in ROI. The main idea is to calculate how smooth of region which surrounding to the pixel. Note that the smaller value of local complexity, the more likely it is a smooth pixel, which is more embeddable. Therefore, pixels with smaller value of local complexity are embedded first. In literature, the four-pixel version of local complexity function is exploited (see Fig. 3-6 (a)). We use an extended version which is able to select a smooth area more precisely.

As Fig. 3-6 (a) shown, we use four neighboring pixels to compute the four-pixel version value f(p) by follow equation (3-9):

$$f(p) = |N\text{-}W| + |W\text{-}S| + |S\text{-}E| + |E\text{-}N| \tag{3-9}$$

Fig. 3-6 (b) shows the context of our proposed extended version. The following function is a description of extended version (3-10):

$$C(p) = f(p) + f(NW) + f(NE) + f(SW) + f(SE) \tag{3-10}$$

doi:10.6342/NTU202101171

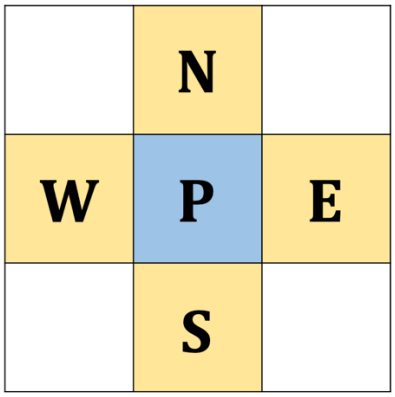


Fig. 3-6 (a) four-pixel version

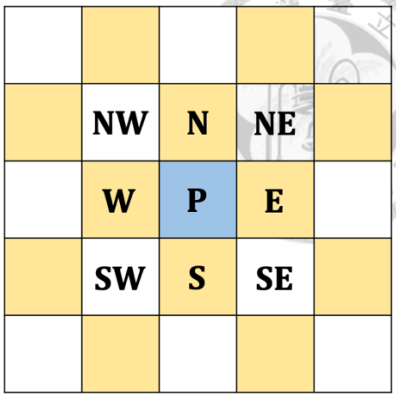


Fig. 3-6 (b) extended version

3.5 Encoder and Decoder

In this section, we are going to present the encoder and decoder. In addition, the side information is comprehensively discussed as follow.

3.5.1 Side information

Decoder needs side information to extract the embedded message and recover the stego image to the original one. The following subsection describe side information related to decoder.

3.5.1.1 Preprocessing and Location Map

In order to avoid the overflow problem, we need to preprocess some pixels and record them in location map. For 16-bit medical image, the max pixel value is 65535. However, in the process of embedding, the pixel value may be modified, which cause the pixel value shifted to 65536. Therefore, we have to preprocess the pixel value to avoid overflow problem. However, suppose a pixel's value 1 shift to zero after embedding, it will be skipped during recovery and extraction. Accordingly, we need to shift the pixel value from 1 to 2 and record it in location map before embedding.

doi:10.6342/NTU202101171

Without loss of generality, assuming that k pixels are preprocessed. The location map $M = \{M_1, \dots M_k\}$ is generated and original pixel p_o is preprocessed to p by following equation 錯誤! 找不到參照來源。):

$$M_i = \begin{cases} 0 & \text{if } p_o = 2 \text{ or } 65534 \\ 1 & \text{if } p_o = 1 \text{ or } 65535 \end{cases} \quad (3\text{-}11)$$

$$p = \begin{cases} 65534 & \text{if } p_o = 65535 \\ 2 & \text{if } p_o = 1 \\ p_o & \text{else} \end{cases} \quad (3\text{-}12)$$

We use arithmetic coding to lossless compress location map and append it to the front of hidden data. Given an $n \times m$ image, the size of location map s is defined as $s = \lceil \log_2 n \times m \rceil$ bits. For 512×512 image, the size s is 18 bits.

Then, recovery stage, original pixel p_o is recovered from p using location map M by following equation (3-13):

$$p_o = \begin{cases} 1 & \text{if } M_i = 1 \text{ and } p = 2 \\ 65534 & \text{if } M_i = 1 \text{ and } p = 65535 \end{cases} \quad (3\text{-}13)$$

3.5.1.2 Hidden message length

In order to know when to stop decoding during decoding process, the hidden message length need to be recorded in the LSBs of the border pixels. Therefore, the LSBs of the border pixels are replaced with hidden message length. In addition, the these border pixels will be appended to the front of hidden message, so the pixels can be recovered in the process of decoding. Given an $n \times m$ image, the size of hidden message length l is defined as $l = \lceil \log_2 n \times m \rceil$ bits. For 512×512 image, the size t is 18 bits.

3.5.1.3 LSBs of the border pixels

Hidden message length l is recorded in the LSBs of the border pixels, so we need

doi:10.6342/NTU202101171

to append l LSBs of the border pixel to the front of hidden message and use them during recovery.

3.5.2 Encoder

Encoding process includes embedding messages, which using the following steps:

1. Preprocess and generate location map
2. Sort even set pixels using proposed extended version of local complexity function.
3. Embed hidden message in even set.
4. Sort odd set pixels using proposed extended version of local complexity function.
5. Embed hidden message in odd set.
6. Replace the border pixel.

Fig. 3-7 illustrates the framework of encoder.

doi:10.6342/NTU202101171

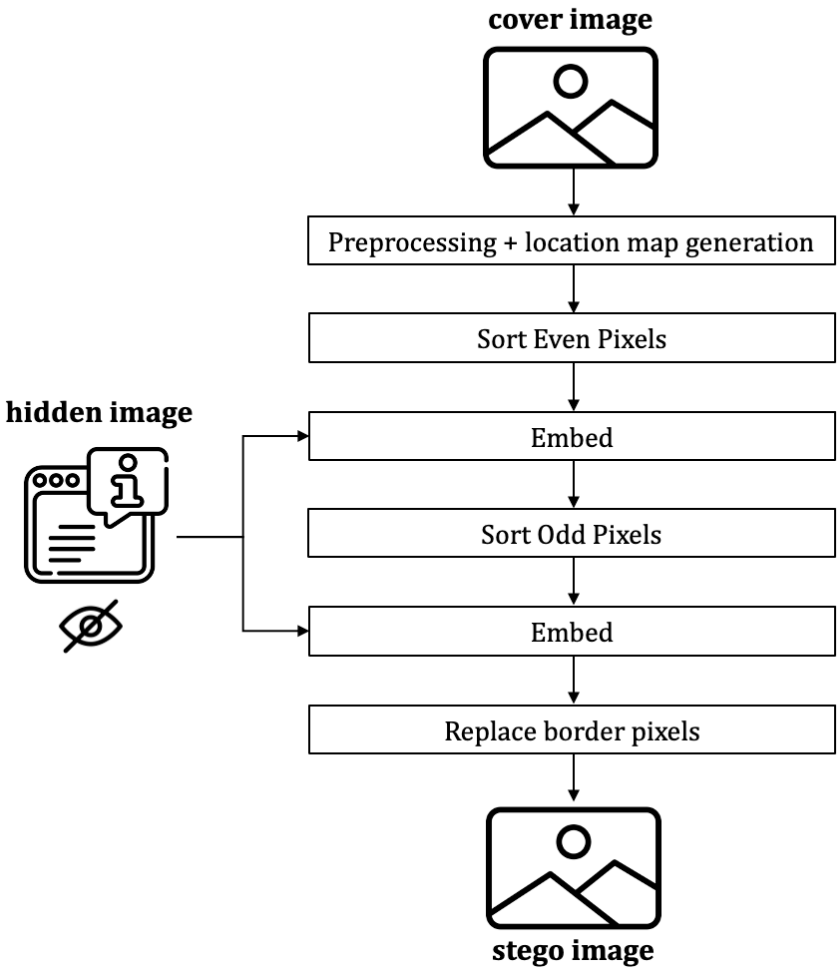


Fig. 3-7 Framework of encoder.

3.5.3 Decoder

Decoding process includes extracting hidden messages and recovering original image, the steps are as follows

1. Get side information from LSBs of border pixels.
2. Sort odd set pixels using proposed extended version of local complexity function.
3. Extract hidden message and recover pixels in odd set.
4. Sort even set pixels using proposed extended version of local complexity

doi:10.6342/NTU202101171

function.

5. Extract hidden message and recover pixels in even set.
6. Replace LSBs of border pixels with original LSBs
7. Decompress location map and undo preprocessing.

Fig. 3-8 illustrates the framework of decoder

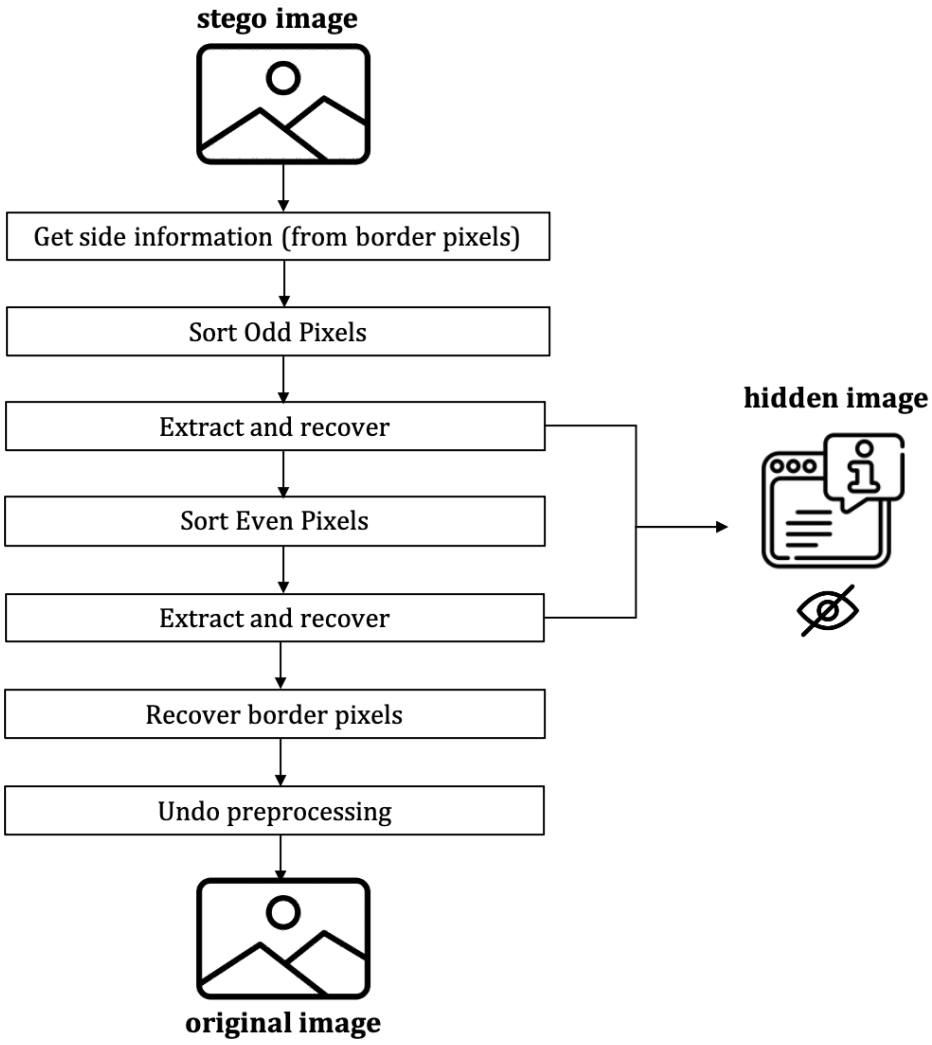


Fig. 3-8 Framework of decoder

doi:10.6342/NTU202101171

Chapter 4

Experiments

Our proposed scheme has been comprehensively introduced in Chapter 3. In this chapter, we compare our method with others by performing experiments on several medical image databases. In order to verify flexibility of our method, we also execute the proposed approach in general image databases. First, we introduce the databases we use, including medical images and general images Next, the evaluation metric that these databases applied will be described. After that, the experimental results will be shown and compared with other state-of-the-art methods.

4.1 Databases

This section describes the database used in our method, including medical images and general images. The details of these databases are as follows.

4.1.1 Breast-MRI-NACT-Pilot database

Breast-MRI-NACT-Pilot is an MRI-type image database, collecting breast medical images of 64 patients. Some samples are shown in Fig. 4-1 (a)

doi:10.6342/NTU202101171

4.1.2 ACRIN-DSC-MR-Brain database

ACRIN-DSC-MR-Brain database contain MRI-type and CT-type medical images and collect brain medical images. Some samples are shown in Fig. 4-1(b)

4.1.3 NIH Database

NIH is an X-ray type image database, collecting chest medical image. Some samples are shown in Fig. 4-1 (c)

4.1.4 Lung-PET-CT-Dx Database

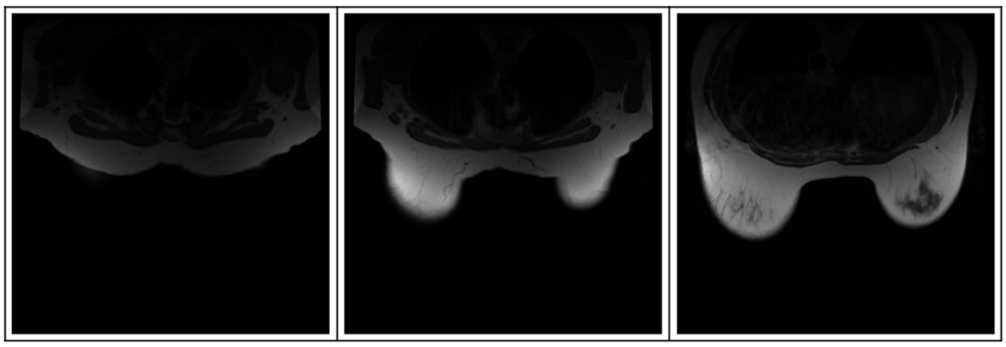
Lung-PET-CT-Dx is an CT-type image database, collecting lung medical image. Some samples are shown in Fig. 4-1 (d)

4.1.5 Prostate-MRI Database

Prostate-MRI database contain MRI-type medical images and collect prostate medical images. Some samples are shown in Fig. 4-1 (e)

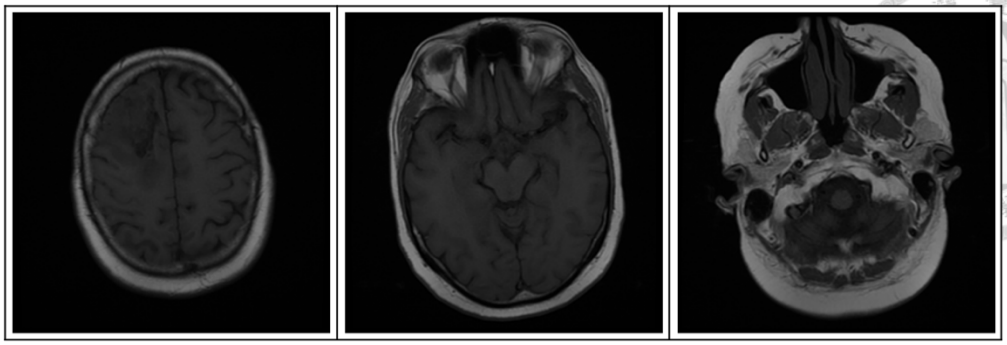
4.1.6 Other grayscale standard images

In order to flexibility of our method, we also test several general images as show in Fig. 4-1 (f)

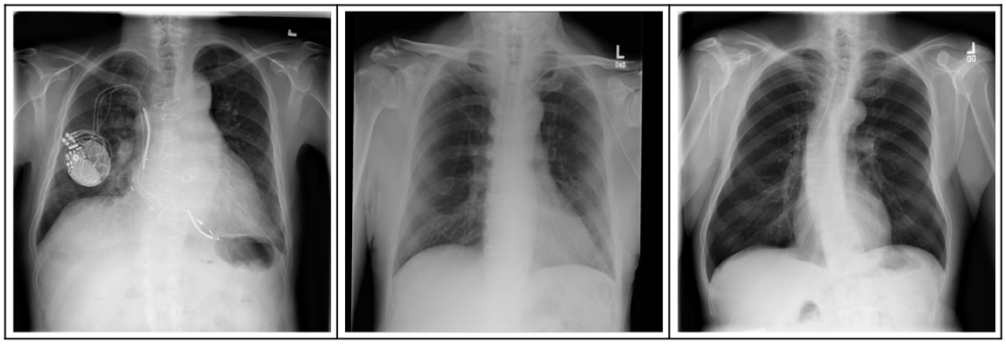


(a) Breast-MRI-NACT-Pilot (breast)

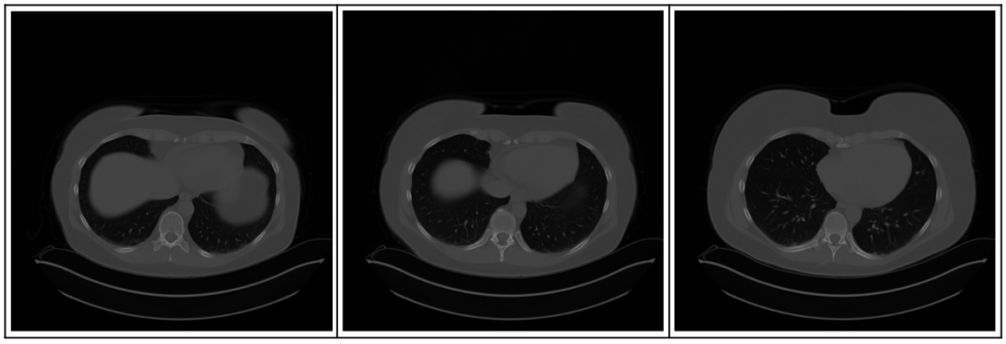
doi:10.6342/NTU202101171



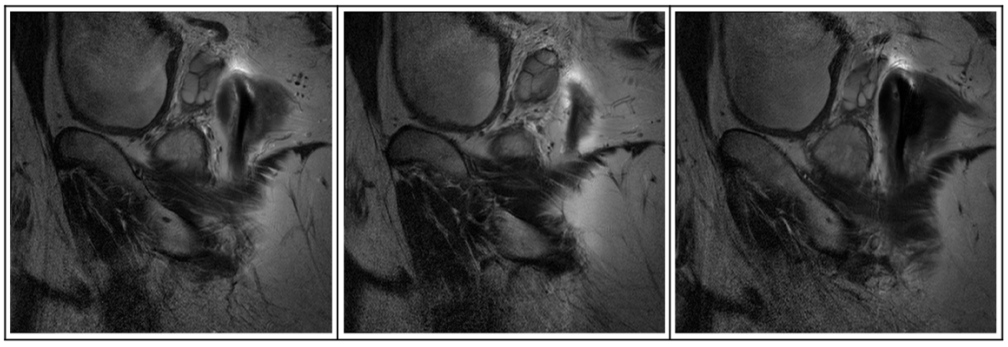
(b) ACRIN-DSC-MR-Brain (brain)



(c) NIH (chest)



(d) Lung-PET-CT-Dx (lung)



(e) Prostate-MRI (prostate)

doi:10.6342/NTU202101171

(f) other grayscale standard images

Fig. 4-1 Example images in several databases

4.2 Evaluation metrics of proposed scheme

In this section, we are going to introduce the evaluation metric that our proposed scheme adopts to measure the performance. Since our scheme is to deal with reversible data hiding in medical image, we focus on imperceptibility and capacity. PSNR (Peak-signal-to-noise-ratio) and SSIM which have been described in Section 1-3 are used to analysis the performance. As we mentioned in Chapter 3, we use local complexity function to select which pixel embedded first, so the modified pixels position will be discussed in following section.

4.3 Experimental Result

In this section, we describe four experiments used to measure the performance of proposed method. The first experiment is that we show stego image and mark the pixels positions which have been modified during the embedding process, as shown in Table 4-1 ~Table 4-6. In order to make modified pixel position have an obvious effect, we set bpp (bit per pixel) rate at 0.05 and 0.025. It can be seen from the results that the local complexity function can distinguish ROI and RONI from most of the medical images,

doi:10.6342/NTU202101171

so modified pixels are gathered in RONI. However, it can be observed that our proposed local complexity function cannot distinguish between ROI and RONI in Prostate-MRI database, due to the relative complexity of the image. Besides, “Modified BPP” represents the proportion of pixels in the image that have been modified. We observed that the performance of "baboon" in grayscale standard images database is poor, because the pixels of the image are relatively complex and it is difficult to select the pixel that are more embeddable by proposed local complexity function. In addition, the modified pixel positions in other grayscale standard images such as Lena and Barbara, are relatively smooth, which verify that our local complexity function is also applicable to general images.

Next, the second experiment test on Breast-MRI-NACT-Pilot database, ACRIN-DSC-MR-Brain database, NIH database and compares max capacity with other methods, as shown in Table 4-7.The method proposed by Kim's is also histogram-based, and the difference from our method is the embedding algorithm and the design of local complexity function. Li's method has been proposed earlier which is also histogram-based method, but it didn’t use prediction error and local complexity function. Therefore, our performance is significantly better than theirs. We can observe that max capacity achieves better performance in NIH database. It’s because the image of NIH database is 1024×1024, however, the image of other databases is 256×256.

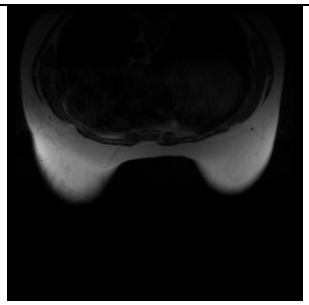
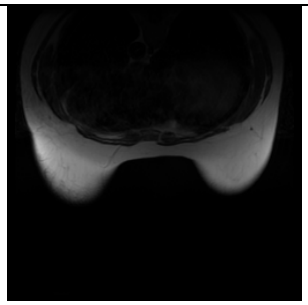
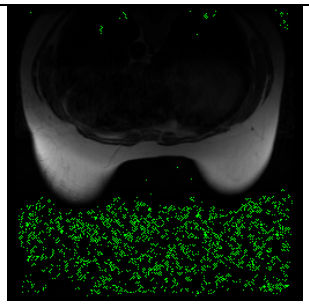
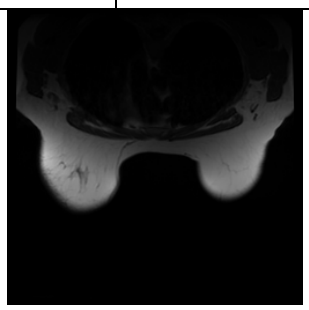
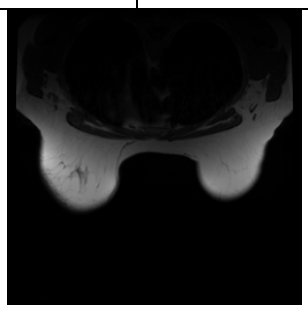
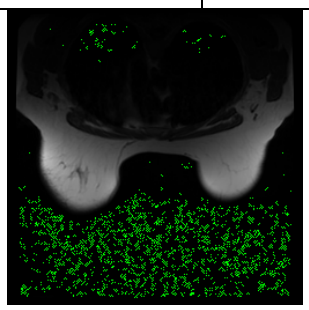
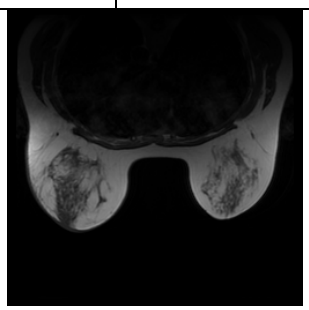
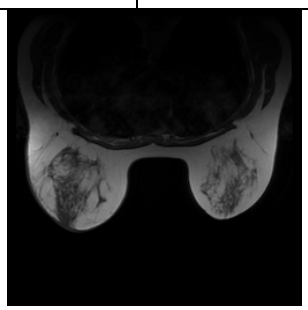
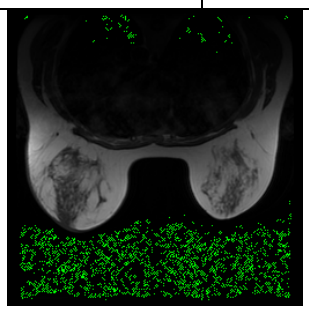
The third experiment was under the condition of a fixed bpp rate. As shown in Table 4-8, we compare the performance of modified pixels number, PSNR and SSIM. The results show that our method is better than others. Note that max capacity of Li's method cannot reach 0.05 bpp on several databases, so we didn’t consider it.

In the last experiment, we analyze the execution time of the encoder and decoder. The specification of this experimental platform is listed in Table 4-10. As shown in

doi:10.6342/NTU202101171

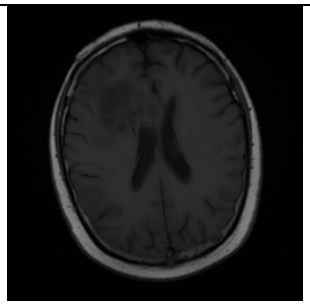
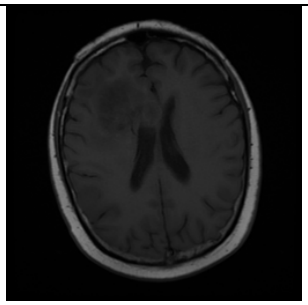
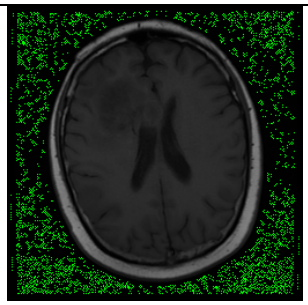
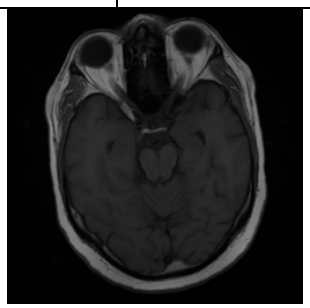
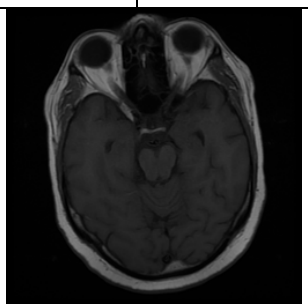
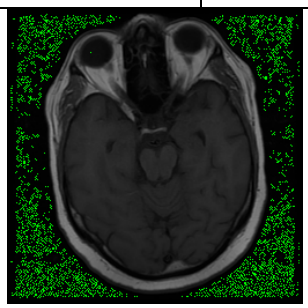
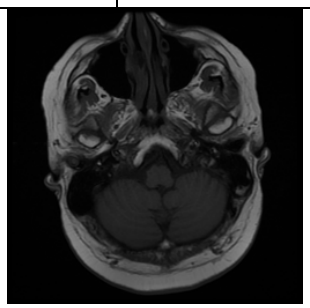
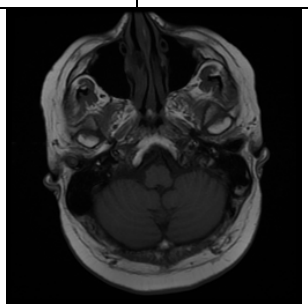
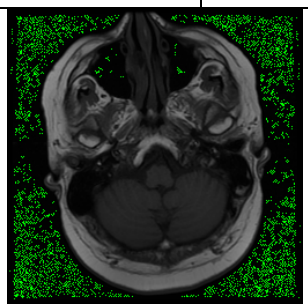
Table 4-10Table 4-10 and Table 4-11, the execution time has the direct correlation with the size of the image, not the bpp, which proves that the local complexity function in our proposed algorithm is the main cause of time-consuming. Since both encoder and decoder use the local complexity function, the execution time results are close.

Table 4-1 Results on Breast-MRI-NACT-Pilot database

Dataset	Original image		Stego image		Modified position	
Breast-MRI-NACT-Pilot						
	BPP	0.05	PSNR	62.08	Modified BPP	0.041
						
	BPP	0.05	PSNR	62.13	Modified BPP	0.041
						
	BPP	0.05	PSNR	62.21	Modified BPP	0.041

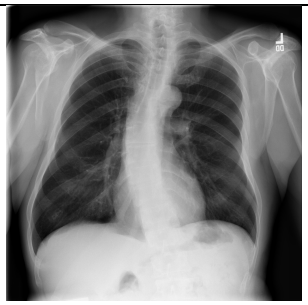
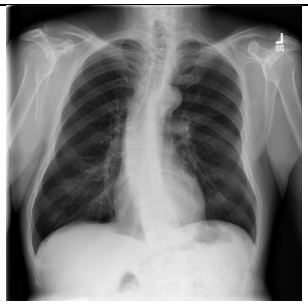
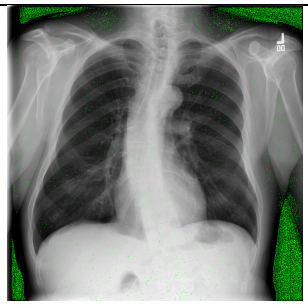
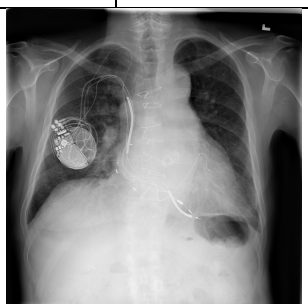
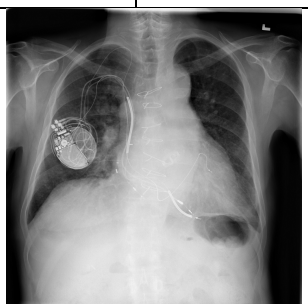
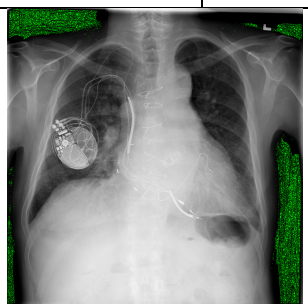
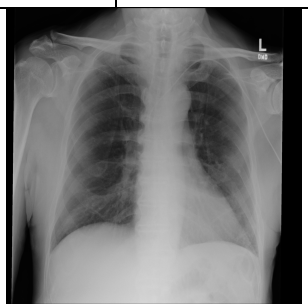
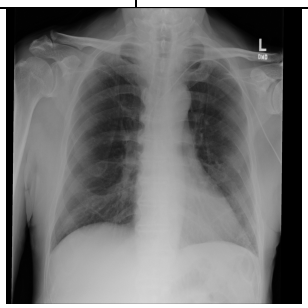
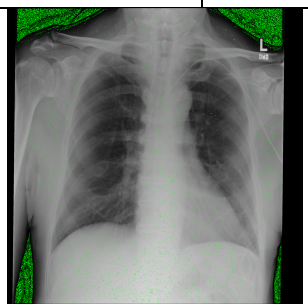
doi:10.6342/NTU202101171

Table 4-2 Results on ACRIN-DSC-MR-Brain database

Dataset	Original image		Stego image		Modified position	
ACRIN-DSC-MR-Brain						
	BPP	0.05	PSNR	60.42	Modified BPP	0.057
						
	BPP	0.05	PSNR	60.85	Modified BPP	0.054
						
	BPP	0.05	PSNR	60.57	Modified BPP	0.058

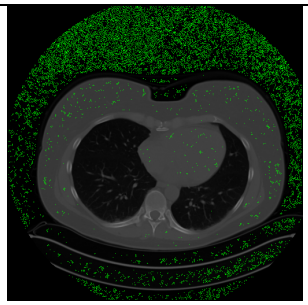
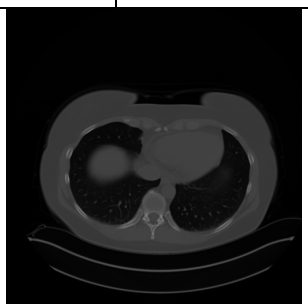
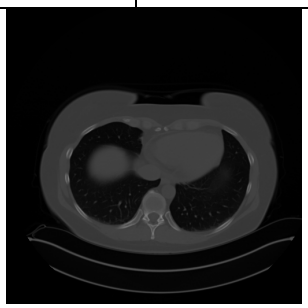
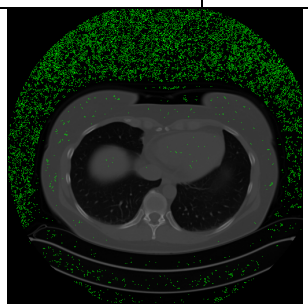
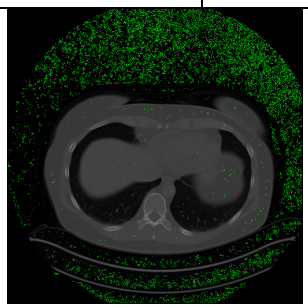
doi:10.6342/NTU202101171

Table 4-3 Results on NIH database

Dataset	Original image		Stego image		Modified position	
NIH						
	BPP	0.05	PSNR	63.56	Modified BPP	0.027
						
	BPP	0.05	PSNR	63.65	Modified BPP	0.026
						
	BPP	0.05	PSNR	64.06	Modified BPP	0.026

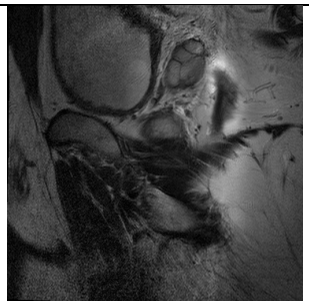
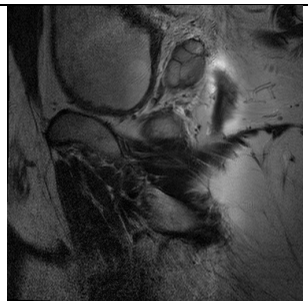
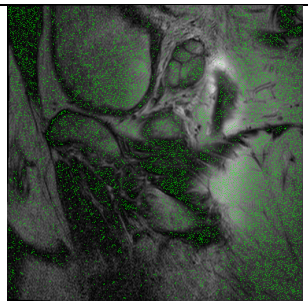
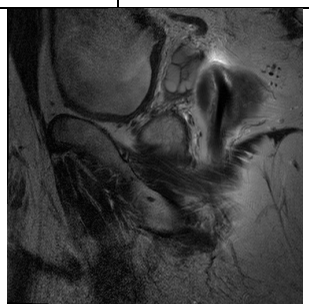
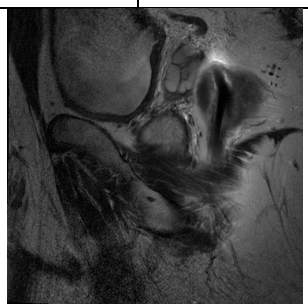
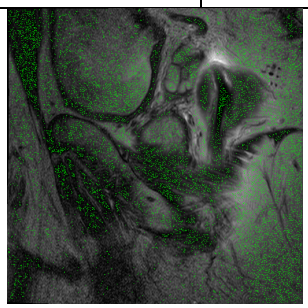
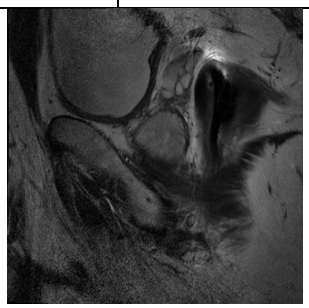
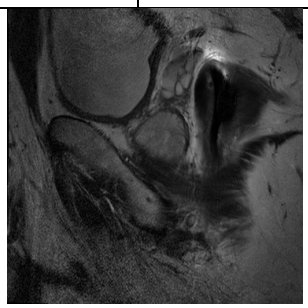
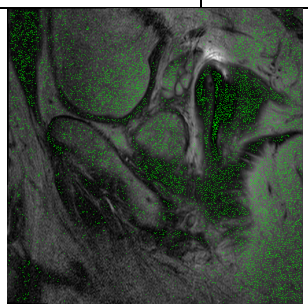
doi:10.6342/NTU202101171

Table 4-4 Results on Lung-PET-CT-Dx database

Dataset	Original image		Stego image		Modified position	
Lung-PET-CT-Dx						
	BPP	0.05	PSNR	61.01	Modified BPP	0.052
						
	BPP	0.05	PSNR	61.49	Modified BPP	0.046
						
	BPP	0.05	PSNR	61.37	Modified BPP	0.047

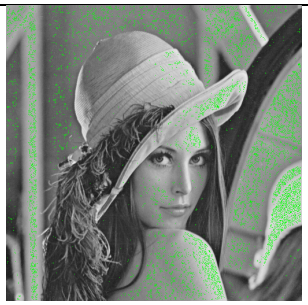
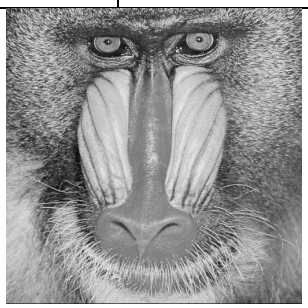
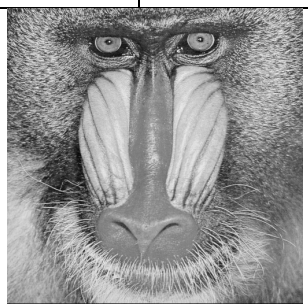
doi:10.6342/NTU202101171

Table 4-5 Results on Prostate-MRI database

Dataset	Original image		Stego image		Modified position	
Prostate-MRI						
	BPP	0.05	PSNR	61.53	Modified BPP	0.046
						
	BPP	0.05	PSNR	61.65	Modified BPP	0.044
						
	BPP	0.05	PSNR	61.95	Modified BPP	0.041

doi:10.6342/NTU202101171

Table 4-6 Results on grayscale standard images

Dataset	Original image		Stego image		Modified position	
grayscale standard images						
	BPP	0.025	PSNR	62.38	Modified BPP	0.038
						
	BPP	0.025	PSNR	62.2	Modified BPP	0.039
						
	BPP	0.025	PSNR	58.43	Modified BPP	0.093

doi:10.6342/NTU202101171

Table 4-7 Max capacity compared with other method

Schemes	Database	Max capacity	BPP
Proposed scheme	Breast-MRI-NACT-Pilot	**14287**	**0.218**
Kim's scheme		10945	0.167
Li's scheme		8257	0.126
Proposed scheme	ACRIN-DSC-MR-Brain	**9633**	**0.147**
Kim's scheme		7340	0.112
Li's scheme		2743	0.042
Proposed scheme	NIH	**282678**	**0.270**
Kim's scheme		204472	0.195
Li's scheme		24909	0.023

doi:10.6342/NTU202101171

Table 4-8 Modified pixels number, PSNR and SSIM compared with other method

Schemes	BPP	Database	Modified pixels number	PSNR	SSIM
Proposed scheme	0.05	Breast-MRI-NACT-Pilot	**2858**	**61.7**	**0.999**
Kim's scheme			4235	60.0	0.999
Li's scheme			23473	52.6	0.999
Proposed scheme	0.05	ACRIN-DSC-MR-Brain	**3763**	**60.5**	**0.999**
Kim's scheme			5646	58.8	0.999
Li's scheme			-	-	-
Proposed scheme	0.05	NIH	**37691**	**62.6**	**0.999**
Kim's scheme			56088	60.8	0.999
Li's scheme			-	-	-
Proposed scheme	0.1	Breast-MRI-NACT-Pilot	**5644**	**58.8**	**0.999**
Kim's scheme			8033	57.2	0.999
Li's scheme			50158	49.3	0.998
Proposed scheme	0.1	ACRIN-DSC-MR-Brain	**8705**	**56.9**	**0.999**
Kim's scheme			11932	55.5	0.999
Li's scheme			-	-	-
Proposed scheme	0.1	NIH	**80952**	**58.5**	**0.997**
Kim's scheme			137641	56.8	0.997
Li's scheme			-	-	-

Table 4-9 Experimental specification

CPU	2.4 GHz Intel Core i5
Memory	16 GB
Operating System	MacOS 10.14.6

doi:10.6342/NTU202101171

Table 4-10 Execution time of encoder

BPP	Database	Image size	Result in seconds
0.05	Breast-MRI-NACT-Pilot	256 × 256	0.803
	Prostate-MRI	512 × 512	4.124
	NIH	1024 × 1024	13.346
0.1	Breast-MRI-NACT-Pilot	256 × 256	0.874
	Prostate-MRI	512 × 512	5.258
	NIH	1024 × 1024	15.427

Table 4-11 Execution time of decoder

BPP	Database	Image size	Result in seconds
0.05	Breast-MRI-NACT-Pilot	256 × 256	0.582
	Prostate-MRI	512 × 512	3.264
	NIH	1024 × 1024	10.26
0.1	Breast-MRI-NACT-Pilot	256 × 256	0.693
	Prostate-MRI	512 × 512	4.101
	NIH	1024 × 1024	12.396

doi:10.6342/NTU202101171

Chapter 5

Conclusions

In this thesis, we propose a novel two-bit embedding architecture for data hiding. The architecture is fully reversible. Most of existing data hiding approaches is not reversible. In contrast, our work is fully reversible. To the best of our knowledge, we are the first to use local complexity function to divide medical image into smooth area and unsmooth area, and our embedding algorithm cause less distortion in ROI. Furthermore, the result shows that the hidden message embedded in stego image is imperceptible.

In the future, algorithm which resist JPEG compression can be developed to improve the robustness. In addition, we can further compare other prediction methods such as block-based approach and steganalysis to our method.

doi:10.6342/NTU202101171

REFERENCE

[1] Barton, J. M. (1997). "Method and apparatus for embedding authentication information within digital data." U.S. Patent 5646997.

[2] W. Bender, D. Gruhl, N. Morimoto, and A. Lu, “Techniques for data hiding,” IBM Syst. J., vol. 35, no. 3–4, pp. 313–336, 1996.

[3] Wang, R.-Z., Lin, C.-F., & Lin, J.-C. (2001). Image hiding by optimal LSB substitution and genetic algorithm. Pattern Recognition, 34(3), 671–683.

[4] Chan, C.-K., & Cheng, L. M. (2004). Hiding data in images by simple LSB substitution. Pattern Recognition, 37(3), 469–474.

[5] Celik, M. U., Sharma, G., Tekalp, A. M., & Saber, E. (2005). Lossless generalized-LSB data embedding. IEEE Transactions on Image Processing, 14(2), 253–266.

[6] Jun Tian. (2003). Reversible data embedding using a difference expansion. IEEE Transactions on Circuits and Systems for Video Technology, 13(8), 890–896.

[7] Z. Ni, Y.Q. Shi, N. Ansari and W. Su, “Reversible Data Hiding”, IEEE Transactions on Circuits and Systems for Video Technology, vol. 16, no. 3, Mar. 2006 , pp. 354-362.

[8] Der-Chyuan Lou, Chen-Hao Hu and Chung-Ching Chiu “Steganalysis of Histogram Modification Reversible Data Hiding Scheme by Histogram Feature Coding” International Journal of Innovative computing Information and Control, Vol 7, No. 11, Nov 2011.

[9] C.W. Lee and W.H. Tsai, “A lossless large-volume data hiding method based on histogram shifting using an optimal hierarchical block division scheme,” J. Inform. Sci. Eng., vol. 27, no. 4, pp. 1265–1282, 2011.

[10] C.-H. Yang and M.-H. Tsai “Improving histogram-based reversible data hiding by

doi:10.6342/NTU202101171

interleaving predictions" IET Image Processing , Dec 2009.

[11] Hong, W., & Chen, T.-S. (2010). A local variance-controlled reversible data hiding method using prediction and histogram-shifting. Journal of Systems and Software, 83(12), 2653–2663.

[12] Tsai, P., Hu, Y.-C., & Yeh, H.-L. (2009). Reversible image hiding scheme using predictive coding and histogram shifting. Signal Processing, 89(6), 1129–1143.

[13] Chen, X., Sun, X., Sun, H., Zhou, Z., & Zhang, J. (2013). Reversible watermarking method based on asymmetric-histogram shifting of prediction errors. Journal of Systems and Software, 86(10), 2620–2626.

[14] S. Kim, X. Qu, V. Sachnev, H.J. Kim, Skewed histogram shifting for reversible data hiding using a pair of extreme predictions, IEEE Trans. Circuits Syst. Video Technol., online published.

[15] I. J. Cox, M. L. Miller, J. A. Bloom, Digital Watermarking, Morgan Kaufmann Publishers, San Francisco, CA, 2001.

doi:10.6342/NTU202101171