Information Hiding Using Chain Code Technique

Zuheir H.Ali
Al-Mustansiriyah university - College of Education
Department of computer science

Abstract

In world where privacy is a right, many people try to find a way to hide information especially when it comes to sensitive documents and files. Steganography is a technique of hiding information, which could be defined as the art and science of communicating which hides the existence of communication. The proposed system use chain code to hide the information where first generate a chain code and store it in the image then store the embedded text in the image according to the generated chain code. The main goal of Steganography was fulfilled since the resulted image did not drown any suspicion.

المستخلص :

أخفاء المعلومات باستخدام تقنية سلسلة الرموز

زهير حسين علي - الجامعة المستنصرية / كلية التربية / قسم علوم الحاسبات .

تعد السرية حق في العالم ، بعض الاشخاص يحاولون ايجاد طريقة لاخفاء المعلومات وخاصة عندما تكون وثائق وملفات حساسة ، الكتابة المخفية هي تقنية لاخفاء المعلومات ويمكن تعريفها بانها فن وعلم الاتصالات الذي يخفي وجود المعلومات المرسلة، النظام المقترح يستخدم تقنية سلسلة الرموز لاخفاء المعلومات حيث يتم اولا توليد سلسلة الرموز وخزنها في الصورة وبعد ذلك يتم خزن النص المرسل في الصورة اعتمادا على سلسلة الرموز الموجودة، وقد تم تحقيق هدف الاخفاء لان النتيجة من النظام كانت عبارة عن صورة لاتثير الشك.

References

[1] Stallings W., **"Cryptography and Network Security"**, Principles and Practice, 3rd Edition, Prentice Hill, 2002.

[2] Ashish Patel and Ajay Kumar Garg, **"Study and Implementation of Cryptographic Algorithms"**, 2008.

[3] K. Anup Kumar and S. Udaya Kumar, **"Block cipher using key based random permutations and key based random substitutions"**, March 2008.

[4] Lars Ramkilde Knudsen, **"Block Ciphers Analysis, Design and Applications"**, PhD thesis, Aarhus University, Denmark, July 1, 1994.

[5] T. Shirai and K. Shibutani, **"On Feistel Structures Using a Diffusion Switching Mechanism"**, Springer- Verlag, 2006.

[6] Microsoft Help and Support, **"Overview of the compatibility considerations for 32- bit programs on 64-bit versions of Windows"**, http://support.microsoft.com/kb/896456#XSLTH3120121124120121120120

[7] Scott oaks, **"JAVA Security"** 2nd Edition, 2002, O'Reilly & Associates, Inc.

[8] H. M. Deitel, P. J. Deitel, S. E. Santry, **"Advanced Java 2 Platform How To Program"**, 2001 by Prentice-Hall, Inc.

[9] A.Menezes, P.van Oorschot and S.Vanstone, **"Handbook of Applied Cryptography "**, Y 1997 by CRC Press, Inc.

[10] Jonathan B. Knudsen, **"Java Cryptography"**, First Edition May 1998.

[11] W. Mao, **"Modern Cryptography Theory and Practice"**, Prentice Hall PTR, July 25, 2003.

1- Steganography

1-1 Definition

The word steganography literally means covered writing as derived from Greek. It includes as vast array of methods of secret communications that conceal the very existence of message. Among these methods are invisible inks, microdots, character arrangement (other than the cryptographic methods of permutation and substitution), digital signatures, covert channels and spread-spectrum communications [1].

Stegaongraphy is the art and science of communicating in a way which hides the existence of the communication. In contrast to cryptography, where the enemy is allowed to detect, intercept and modify messages without being able to violate certain security premises guaranteed by a cryptosystem, the goal of steganography is to hide messages inside other harmless messages in a way that does not allow any enemy to even detect that there is a second secret messages present[2].

1-2 Introduction

Steganography is one of the oldest arts that people were eager to have since they started communication with each other.

Two areas of research which are generally referred to as “information hiding”, steganography and watermarking as shown in figure (1).

Steganography is the art of hiding information in ways that prevent the detecting of hiding information messages. Digital steganogrphy or information hiding, schemes can be characterized by utilizing the theories of communication . The parameters of information hiding such as the amount of data bits that can be hidden, the perceptibility of the message, and its

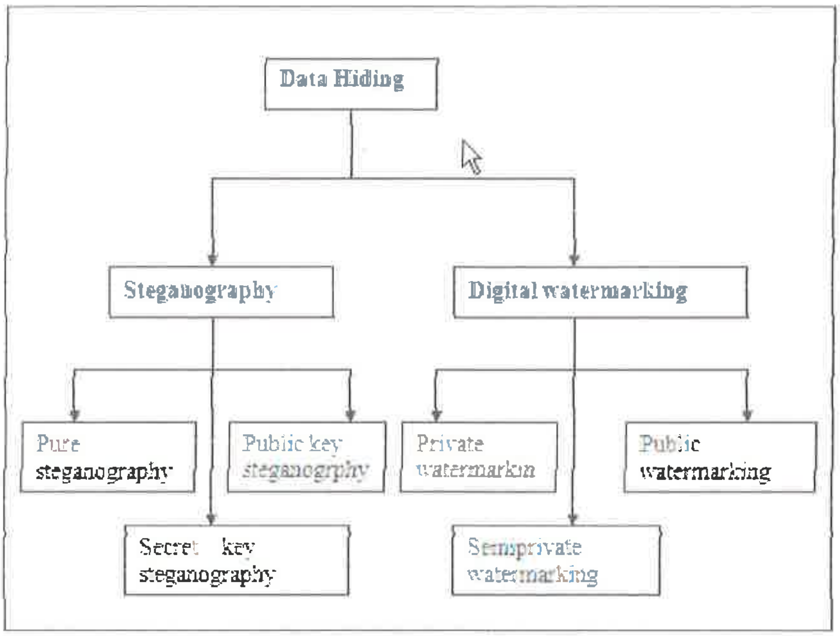


Figure (1) data hiding classification

Robustness to removal can be related to characteristics of communication system, capacity, signal to noise ratio (SNR), and jamming margin.

The notion of capacity in data hiding indicates the total number of bits hidden and successfully recovered by the steganography. The SNR serves as a measure of detect ability.

Recent advances in computing power and recent interest in privacy has led to development of techniques to hide messages in otherwise innocuous computer files such as digital pictures and digitized audio. Using steganography someone who knows about a secret message and no one else will even know that the message is there .

1-3 Use of steganogrphy

Steganogrphy can be used anytime you want to hide data. There are many reasons to hide data but they all boil down to the desire to prevent unauthorized persons from becoming aware of existence of message. In the business world steganogrphy can be used to hide a secret chemical formula or plans for a new invention. Steganography can also be used for corporate espionage by sending out trade secrete without anyone at the company being any the wiser. Steganography can also be used in the non-commercial sector to hide information that someone wants to keep private. Spies have used it since the time to pass messages undetected . The healthcare industry and especially medical imaging systems may befit from information hiding techniques the use standard such as DICOM (digital imaging and communication in medicine) which separates image data from caption, such as the name of picture is lost, thus embedding the name of the patient in the image could be useful safety measure [3].

2-Chain code

Chain code introduced by Freeman in 1961 that is known as Freeman Chain Code (FCC) [4]. This code follows the contour in counter clockwise manner and keeps track of the directions as we go from one contour pixel to the next. The codes involve 4–connected and 8–connected paths. Figure 2(a) shows 4-connected and Figure 2(b) shows 8-connected of FCC

In the 8-connected FCC each code can be considered as the angular direction in multiple of 45 that we must move to go from on contour pixel to the next. A code scheme must satisfy three objectives

1- Faithfully preserve the information of interest

2- It permits compact storage and convenient for display

3-It facilitates any required processing.

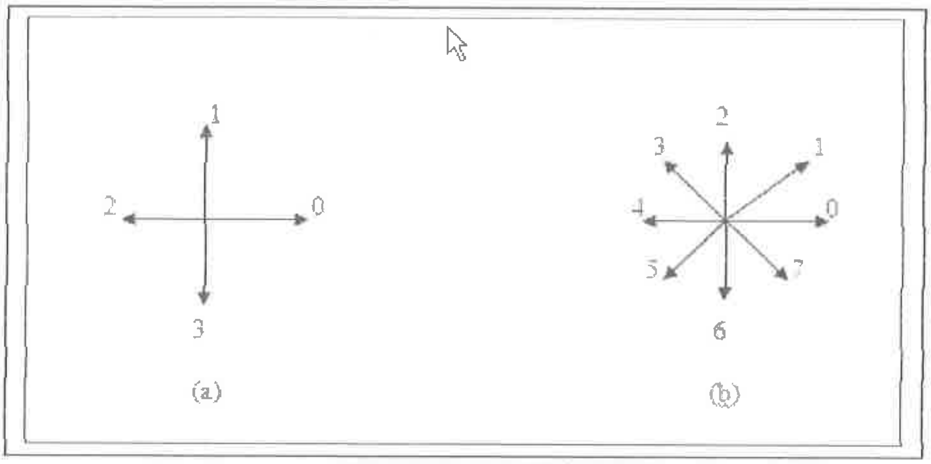
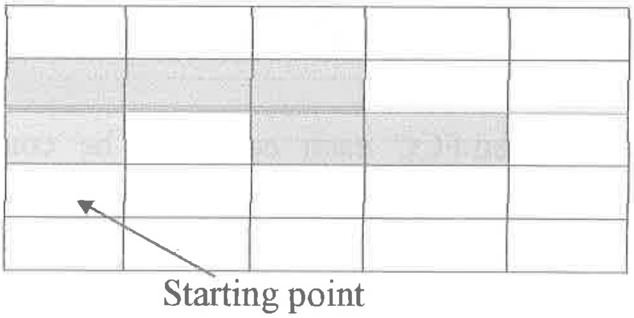
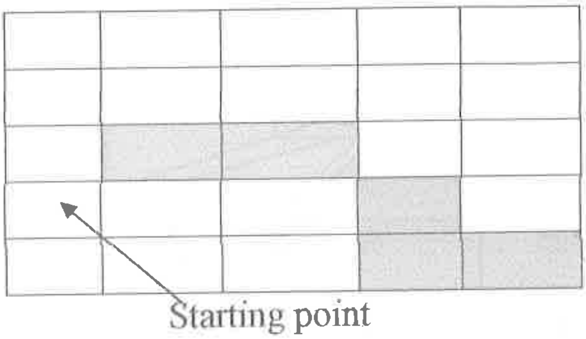


Figure (2) Neighbor Direction of Fcc

To represent the 4-connected and 8-connected we need (2)and(3) bits respectively[5]. The code for 4- connected is as follows 00,01,10,11 for 0,1,2,3 and the code for 8-connected is 000,001,010,011,100,101,110,111 for 0,1,2,3,4,5,6,7 respectively. The following examples illustrate the 4-connected and 8-connected, consider the code 01,01,00,00,11,00



The shadow cell represents the path in which we follow. To illustrate the 8-connected consider the code 001,000,111,110,000



In the 8-connected we can move to the 8-neighbor pixel.

3- The Proposed system

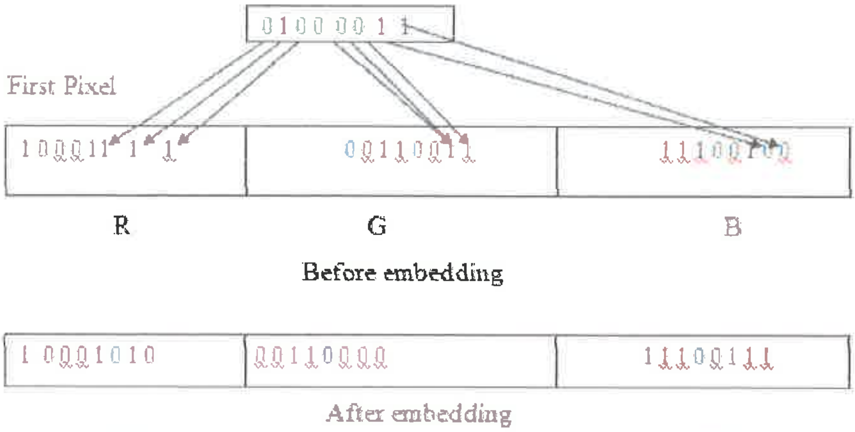
In the new proposed system the first pixel in the image specify the location of starting point to begin with it, The second pixel contain the length of secret message where each character need 8 bits for representation. We divided the image into two section the first half contain the chain code which represent the map of secret message and the second half include the secret message which the sender pass. For example consider the embedded text is as follow

Computer

The ASCII code will be as shown

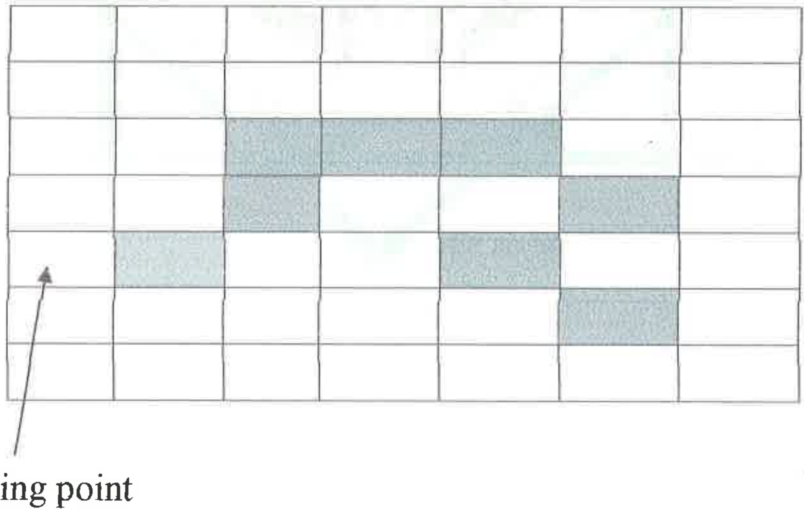
Char	C	o	m	p	U	t	e	r
ASCII	67	111	109	112	117	116	101	114

The first character from embedded text, which is "C" has ASCII value of 67 which can be represented in binary as 01000011 and so as for all characters in the embedded text.



To represent the embedded text suppose the chain code will be stored as follows :

000,001,010,000,000,111,101,111



Where the shadow cell of the path of the embedded text staring from specific point and using 8-connected chain code.

Algorithm 1: this algorithm for hiding the text in the image

step1: we find the length of the embedded text

Step2: select the cover image

Step3: put the starting point and length of chain code in the first two pixel

Step4: generate the chain code such that satisfy the following conditions

A- It do not exceed the image

B- Do not return to any point two times

Step5 : convert the embedded text to ASCII code

Step6 : put the chain code generated in step4 in the beginning of image starting from third pixel

Step7 : Put the ASCII of the embedded text in the image according to the generated chain code starting from start point

4-Extracting the Embedded Text

Extracting the text is done by using the position and length of embedded text stored in the first two pixel and the chain code that was stored in the beginning of image.

Algorithm 2: Extracting text

Step 1: get the start point and length of chain code from the first two pixels.

Step 2 :read the chain code starting from third pixel until reach the end of chain code.

Step 3 : go to the start point in the image.

Step 4 : extract the embedded text in the image by following the chain code

Step 5 : go to step 7 when chain code ended
Step 6 : read the new chain code go to step 4
Step 7 :end of extraction

5-Experimental Result

The *result of the proposed system has been illustrated in the* following example

Example:

The embedded text size is 178 character including space as shown in the following box.

The word steganography literally means covered writing as derived from Greek. It includes as vast array of methods of secret communications that conceal the very existence of message.

Figure (3) shows the cover image before adding the embedded text.

Figure(3) the cover image

Figure number (4) illustrates the cover after adding the text in it using 4- connected chain code

Figure (4) Image after embedding text using 4-chain code

Figure(5) Image after embedding text using 8-connected chain code

6-Conclusions :

1-The proposed system is proved to be a good system to hide text in image.

2- The use of 8-connected chain code gives more flexibility than 4-connected chain code because the move can be done in eight directions rather than 4 directions

3- 4 and 8 connected chain codes gave same results for embedded text because the two method take (3) bits from red, (3) bits from green and (2) bits from blue

4- 4-connected chain code take less bits than 8-connected chain code when store chain code in the image because the 4-connected chain code need only (2) bits when 8-connected chain code need (3) bits.

5- there is a difficulty of implementation because we need to generate chain code and to store embedded text and then extract the embedded text

6- However the difficulty of implementation but it can not be detected since the embedded text was not in adjacent sequence of pixels as more methods that used in information hiding

7-References

1- Johnson, Neil; Duric, Zoran; Jajodia, Sushil (2001). *Information hiding: steganography and watermarking: attacks and countermeasures.*

2- Wayner, Peter (2009). *Disappearing cryptography 3rd Edition: information hiding: steganography & watermarking*. Amsterdam: MK/Morgan Kaufmann Publishers.

3- Kessler, GC (2004). "An Overview of Steganography for the Computer Forensics Examiner". *Forensic Science Communications* .

http://www.fbi.gov/hq/lab/fsc/backissu/july2004/research/2004_03_research01.htm. Retrieved on 2009-09-02.

4- Scott E. Umbaugh (1998), "Computer Vision and Image Processing", Prentice Hall.

5- Milan Sonka, Vaclav Hlavac, Roger Boyle(2008) "Image Processing, Analysis and Machine vision", Second Edition, John wiley