Concealment of Information and encryption by Using Fuzzy Technique

Fatma Hassan Al-Rubbaiy
University of Al Mustansuraia

Abstract

Concealment of Information is the science that involves communicating secret data in an appropriate multimedia carrier, e.g., image,audio, and video files.This scince called steganography. It comes under the assumption that if the feature is visible, the point of attack is evident, thus the goal here is always to conceal the very existence of the embedded data.

Steganography's ultimate objectives, which are undetectability, robustness (resistance to various image processing methods and compression) and capacity of the hidden data.

In this research we suggest method of secret message hiding inside a cover-image by enhanced the classical *LSB* method by split cover-image into subimages and select only even subimages to hide information.

Also We suggest encrypted secret message by using standard fuzzy functions before embedded process to increasing hidden robustness.

We are use classical LSB method to obtain the large space for information hidding.

Key words (Concealment of Information, Fuzzy functions).

1. Introduction

In a world where privacy is aright, many people try to find away to hide information especially when it comes to sensitive documents and files. A person would like to send an email or file with no fear that a person asid from the recipient will read the message. Also, with all information that is on the Internet, owners of such information must protect themselvse from unwanted spying, copying ,thef and false representation. One technique of information hiding is steganography.[1]

Steganography is the art and scince of communicating in a covert fashion, it utilizes the typical digital media such as text, image, video and multimedia as a carrier for hiding private information [2].

The purpose of steganography is to achieve security, privacy, undetectability and to avoid drawing suspicion to transmission of a hidden message [3,4].

Steganography, like cryptography, is a means of providing secrecy. Yet, steganography dose so by hiding the very existence of the communication.

While cryptography dose so by scrambling a message so it cannot be understood. Acryptography message can be intercepter by an eavesdropper, but the eavesdropper may not even known a steganographic message exists.[5]

Steganography conceals a message where the hidden message is object of the communication, It is an invisible to the human eye, and must not be known.Steganography tools hide large blocks of informationa.

2.General Model of Embedding-data and Extraction-data

Figure (1) shows the generallyaccepted model of a Steganography system (or stego-system for short), the sender of a secret message embeds *embedded-data* into *cover-data* using a *key*, and sends the result, stego-data, to the recipient. The recipient then extracts the *embedded-data* from stego-data using a *key* that may not equal to the one used in embedding. [6]

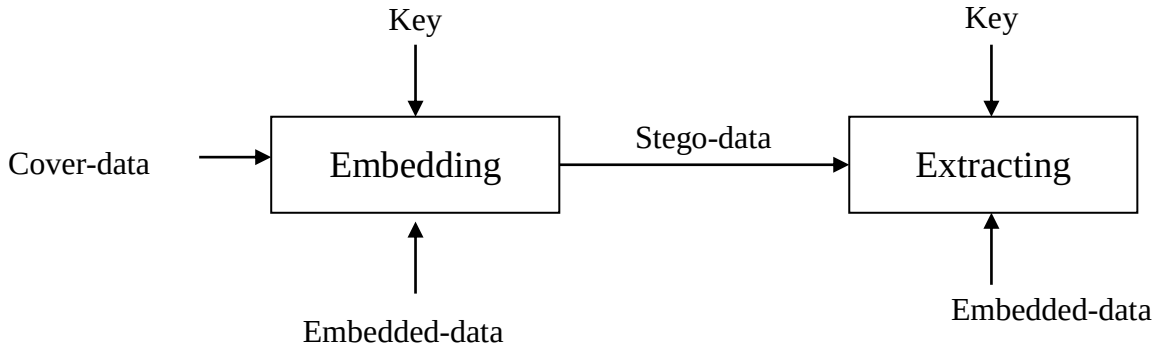

Figure (1) Basic model of Embedding-data and Extraction-data

A secret key steganography system is similar to symmetric cipher: the sender choose a cover and embeds the secret message into cover using secret key. If the key used in the embeding process is known to the receiver, he can reverse the process and extract the secret message. Any one who dose not know the secret key should not be able to obtain evidence of the encoded information. Again, the cover and the stego-object can be perceptually similar [7].

3. Fuzzy Logic Concept

Fuzzy Logic is basically a multivalued logic that allows intermediate values to be defined between conventional evaluations like yes/no, true/false, black/white, etc. and a continuous range of truth values in the interval [0,1] notions like rather warm or pretty cold can be formulated mathmatically and processed by computers[8,9,10].

4. Fuzzy Logic Applications

- Control (Robotics, Automation, Tracking, Consumer Electronics)
- Information system (DBMS, Information Retrieval).
- Pattern Recognition (Image Processing , Machine Vision).
- Decision Support (Adaptive HMI, Senor Fusion) .[9]

5. Fuzzy Logic Benefits:

- Simplified and reduced development cycle.
- Ease of implementation.
- Can provide more "user- friendely" and efficient performance.[10]

6. Steganography Methods:

The following formula provides a very generic description of the pieces of the steganographic process[11]:

cover_medium + hidden_data + stego_key = stego_medium

In this context, the *cover_medium* is the file in which will hide the *hidden_data*, which may also be encrypted using the *stego_key*. The resultant file is the stego_medium (which will, of course. be the same type of file as the cover_medium). The cover_medium (and, thus, the *stego_medium*) are typically image or audio files. In this article, I will focus on image files and will, therefore, refer to the *cover_image and stego_image*.

Before discussing how information is hidden in an image file, it is worth a fast review of how images are stored in the first place. An image file is merely a binary file containing a binary representation of the color or light intensity of each picture element (pixel) comprising the image.

Images typically use either 8-bit or 24-bit color. When using 8-bit color, there is a definition of up to 256 colors forming a palette for this image, each color denoted by an 8-bit value. A 24-bit color scheme, as the term suggests, uses 24 bits per pixel and provides a much better set of colors. In this case, each pix is represented by three bytes, each byte representing the intensity of the three primary colors red, green, and blue (RGB), respectively. The Hypertext Markup Language (HTML) format for indicating colors in a Web page often uses a 24-bit format employing six hexadecimal digits, each pair representing the amount of red, blue, and green, respectively. The color orange, for example, would be displayed with red set to 100% (decimal 255, hex FF), green set to 50% (decimal 127, hex 7F), and no blue (0), so this system would use "#FF7F00" in the HTML code.

The size of an image file, then, is directly related to the number of pixels and the granularity of the color definition. A typical 640x480 pix image using a palette of 256 colors would require a file about 307 KB in size (640 • 480 bytes), whereas a 1024x768 pix high-resolution 24-bit color image would result in a 2.36 MB file (1024 • 768 • 3 bytes). To avoid sending files of this enormous size, a number of compression schemes have been developed over time, notably Bitmap (BMP), Graphic Interchange Format (GIF), and Joint Photographic Experts Group (JPEG) file types. Not all are equally suited to steganography,

however.GIF and 8-bit BMP files employ what is known as *lossless compression*, a scheme that allows the software to exactly reconstruct

the original image. JPEG, on the other hand, uses *lossy compression*, which means that the expanded image is very nearly the same as the original but not an exact duplicate. While both methods allow computers to save storage space, lossless compression is much better suited to applications where the integrity of the original information must be maintained, such as steganography. While JPEG can be used for stego applications, it is more common to embed data in GIF or BMP files.

The simplest approach to hiding data within an image file is called *least significant bit (LSB*) insertion. This method can take the binary representation of the hidden_data and overwrite the LSB of each byte within the cover_image. If the system is using 24-bit color, the amount of change will be minimal and indiscernible to the human eye. As an example, suppose that have three adjacent pixels (nine bytes) with the following RGB encoding:

10010101 00001101 11001001
10010110 00001111 11001010
10011111 00010000 11001011

Now suppose want to "hide" the following 9 bits of data (the hidden data is usually compressed prior to being hidden): 101101101. If overlay these 9 bits over the LSB of the 9 bytes above, the following get (where bits in bold have been changed):

10010101 0000110**0** 11001001
1001011**1** 0000111**0** 1100101**1**
10011111 00010000 11001011

Note that have successfully hidden 9 bits but at a cost of only changing 4, or roughly 50%, of the LSBs.

This description is meant only as a high-level overview. Similar methods can be applied to 8-bit color but the changes, as the reader might imagine, are more dramatic. Gray-scale images, too, are very useful for steganographic purposes. One potential problem with any of these methods is that they can be found by an adversary who is looking. In addition, there are other methods besides LSB insertion with which to insert hidden information.

7. The proposed system

The proposed system is trying to hide secret message inside a cover image in specific manner that doesn't change the viewing of cover image to everyone.

7.1 Embedding Process Algorithm

Step1:Load cover image from the image file.
Step2: Divide the image into sub images of size 10X10 pixel.
Step3: Split image pixels color to array of Red, Green and Blue colors(RGB).
Step4: load the text from temp file

Step5: Convert text character to ASCII codes.

Step6: Cipher ASCII codes by using fuzzy standard functions[12]:

If x <= a then F(x,a,c)=0

If x>c then f(x,a,c) =1

If (a<x) and (x<= (a+c)/2) then

$F(x,a,c)=2\ ((x-a)/(c-a))^2$

If (((a+2)/2)<x) and (x<=c) then

$F(x,a,c)= 1-2((c-x)/(c-a))^2$

Where x refer to ASCII value , a refer to the start point and c refer to the end point

Step7:Convert the result of Fuzzy function into binary stream.

Step 8: Get number of each sub image and then select only even sub image to hide information in it.

Step9:Hide the binary stream of text in the Last signaficant Bit (LSB) in the even sub images only until the binary stream complete.

Step10:End.

The flowchart diagram of the embedding process is shown in figure (2)

7.2 Extracting Process Algorithm

Step1:Load information hiding image from Internet.

Step2: Divide the image into sub images of size 10X10 pixel.

Step3: Split image pixels color to array of Red, Green and Blue colors(RGB).

Step4: Extract the binary steram of information hiding from LSB in the even sub images only.

Step5: Convert the binary stearm in to ASCII codes.

Step6: Decipher ASCII codes by using Defuzzy standard functions[12]:

$$\text{Output}= \frac{\sum_i \mu_A(y_i)\times y_i}{\sum_i \mu_A(y_i)} \quad \textit{where } \mu_A, y_i \textit{ prametars of inverse fuzzy function}$$

Step7: Convert the result of Defuzzy into plain text.

Step 8: End.

The flowchart diagram of the Extraction process is shown in figure (3)

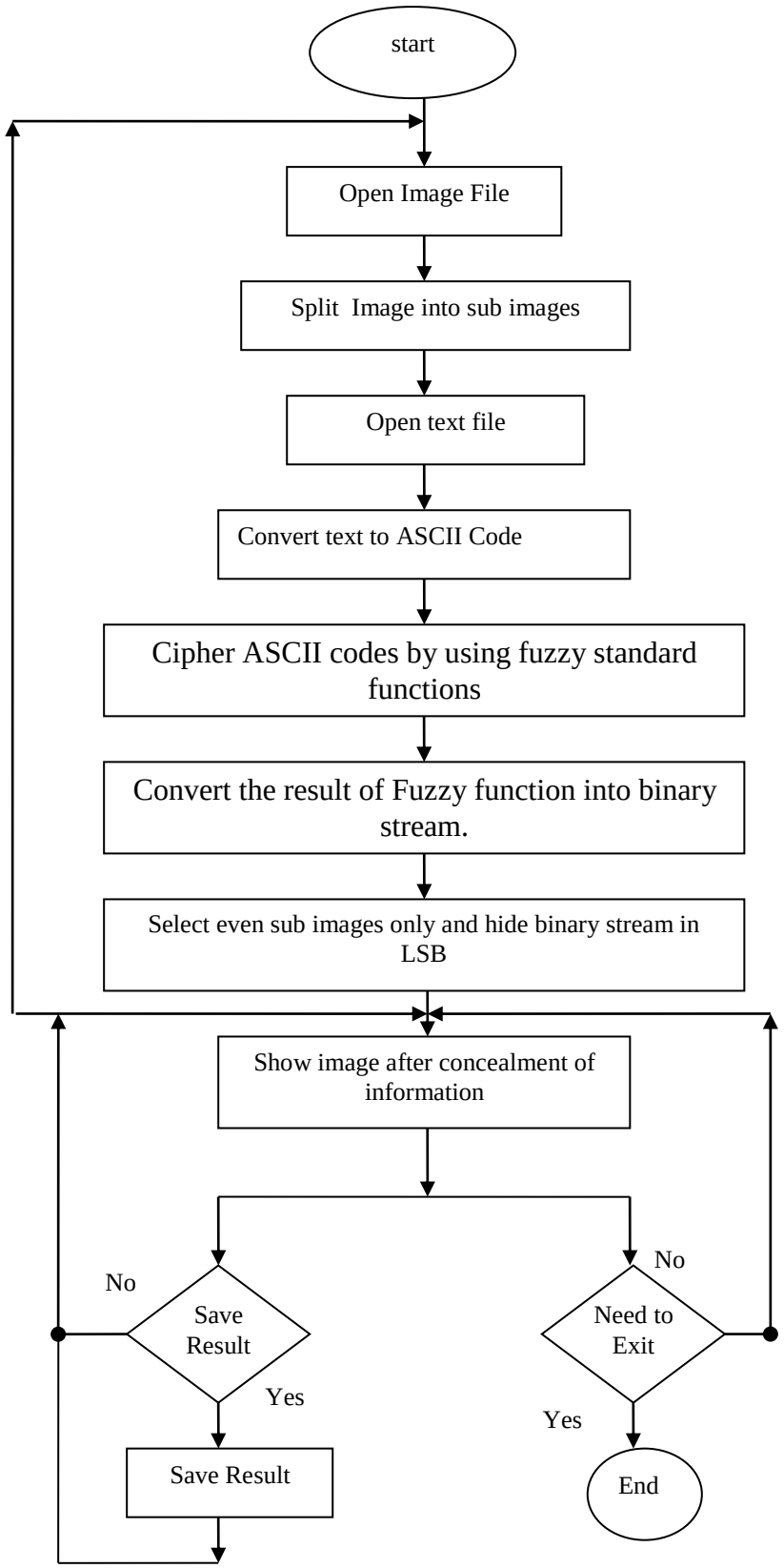

Figure (2) Flowchart of the proposed Concealment of information system

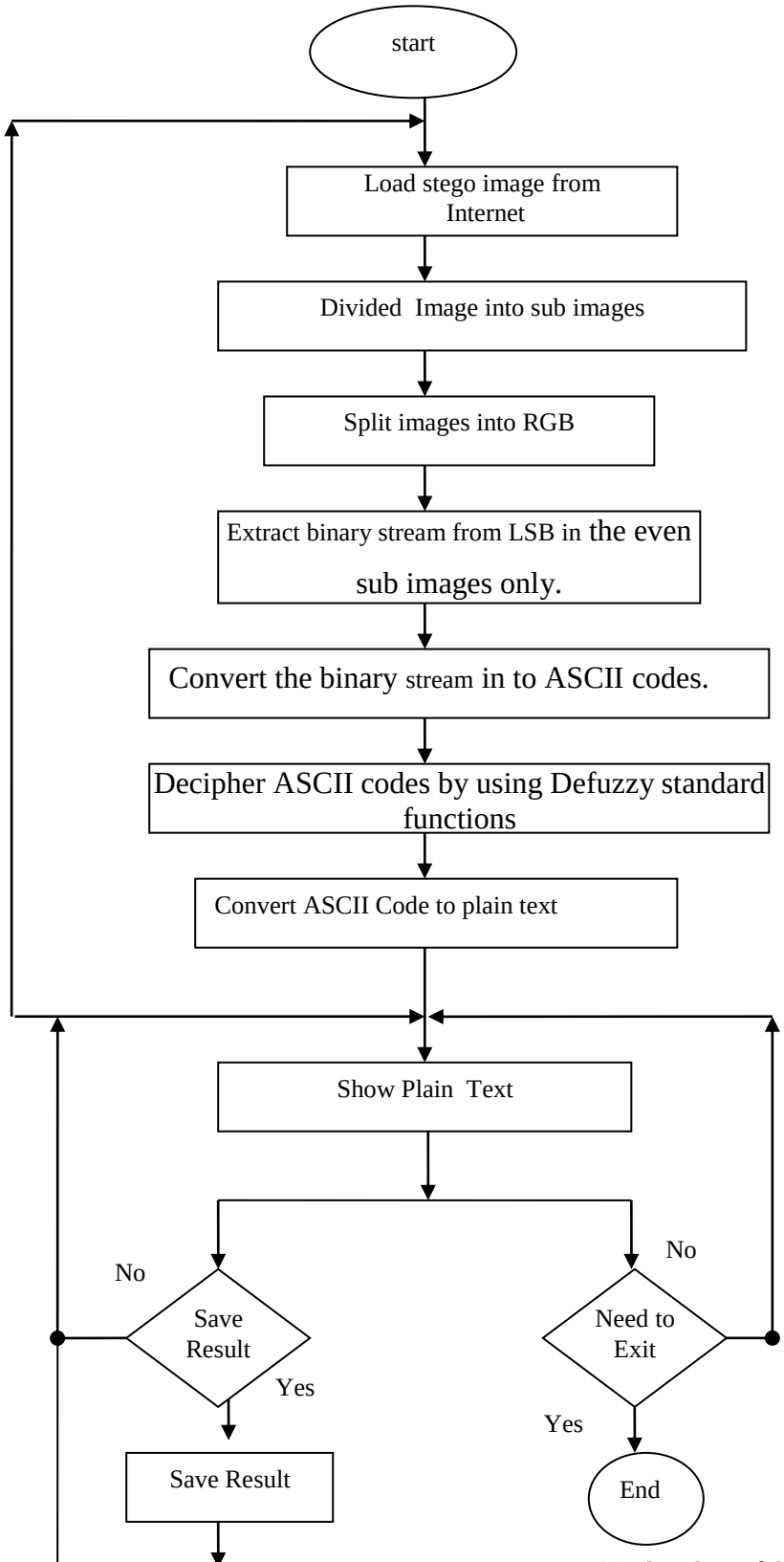

Figure (3) Flowchart of the extraction of information in the proposed system

8: The result discussion :

The are two points can discuss of the result:

1. When the proposed system compared with the LSB classical method ,LSB method concealment information directly in the leas significant bit without any change but in the proposed system must firstly split image into 10X10 pixels and then chosse only even sub images to hide data.
2. The proposed system is applied encryption of secret message by using fuzzy standard function which increased the robustness aginst detection attack.

9: Conclusions :

In the following are some points concluded from this research:

1. Concealment of Information is robustness against detection plaintext by encryption data before embedded in image.
2. Information is encrypted by using fuzzy function is consider new way of ciphering.
3. The high degree of similarity between resulted secret wanted image and the original one that provide resistant against some type of attacks.The proposed system is useful when attacker try to find the plaintext but it's not useful when attacker try to distortion this text without known this text.
4. Fuzzy Logic provides a different way to approach a control or classification problem. This method focuses on what the system should do rather than trying to model how it works. One can concentrate on solving the problem rather than trying to model the system mathematically .on the other hand the fuzzy approach requires a sufficient expert knowledge for the formulation of the rule base, the combination of the sets and the defuzzification.

10: Suggestions for Future Works

there are many suggestion point which can be given to enhance the work of the proposed system, these are:

1. improved system by using image compession methods to increase robustness aginst attack.
2. Develop method to enhance the work of the proposed system by increase the powerful of hiding method by choosing the most significat bits of each pixels in image.
3. Improved system to deals with animation images, video images, and audio.

11. Refrences:

1. V. Petricek, "***Information Hiding and Covert Channels***", Charles university, 2001, PDF.
2. S. Areepongsa, Y.F.Syed, N.Kaewkamnerd, and K.R. Rao, ***"Steganography for A Low Bit-Rate Wavelet Based Image Coder"***,

University of Texas at Arlington, 2000, PDF.

3. E. Franz, A. Pfitzman, " ***Steganography Secure Against Cover- Stego – Attacks***", Information hiding, third International workshop, Lecture Notes in computer science, vol. 1768, pp.29-46, Springer, 2000.
4. N. F. Johnson, S. Jajodia " ***Steganalysis of Images Created using Current Steganography Software***", Center of Secure Information Systems, George Mason university, 1998,PDF, [http://issue.gmu.edu/ njhonson/ steganography].
5. N. F. Johnson, Z. Duric, S. Jajodia, ***"Information Hiding Steganography and watermarking- attacks and countermeasures"***, Kluwer Academic pub. 2001, http://www. jjte.com /pub / book2000-ih.htm
6. N. Shin, ***"One-time Hash Steganography",*** Information Hiding, Third International workshop, Lecture Notes in computer science, vol. 1768, pp.17-28, Springer , 2000.
7. S. Katzenbeisser and F. Petitcolas, ***"Information Hiding Techniques for Steganography and Digital Watermarking"***, Artech House pub. 2000, USA, http://www.ifi.unizh.ch/~oppliger/series editor.html.
8. S.D. Kaelhler, ***" Fuzzy Logic and Fuzzy Control"***, Seattle Robotics Society, 2005.
9. A. Bonde, ***"Fuzzy Logic Basics",*** GTE Government System Corp., Needham, MA 02194,2000.
10. J.Foran, ***"Optimisation of a Fuzzy Logic Controller Using Genetic Algorithms",*** M. Eng Project Report, 2002.
11. Gary c. Kessler***, "Steganography : hiding data with in data",***2001.
12. S. A. Ismaeel, H. A. Obeed, ***"Fuzzy Information Modeling in Database"***,Iraqi Commission for Computers and Informatics, 2006.

إخفاء المعلوماتِ والتشفيرِ بإستعمال التقنيةِ المضببة

فاطمة حسن الربيعي

الجامعة المستنصرية

الخلاصة

الكتابة المخفية هو العلم الذي يتضمن توصيل البيانات السرية في حاملة متعددة الوسائط ملائمة ، على سبيل المثال ، الصورة ، الصوت ، وملفات الفيديو.هذا العلم يدعى(Steganography). انها تأتي في ظل الافتراض أنه إذا كان ميزة مرئية ، وجهة الهجوم هو واضح ، وبالتالي فإن الهدف هنا هو دائما لاخفاء وجود البيانات المضمنة.
ان الاهداف الرئيسية للكتابة المخفية هي عدم القدرة على الكشف والمتانة (المقاومة لمختلف اساليب معالجة الصور والضغط).

في هذا البحث نقترح طريقة لاخفاء الرسالة السرية داخل الصورة الغطاء بواسطة تحسين الطريقة التقليدية LSB بتقسيم الصورة الغطاء الى اجزاء من الصورة واختيار فقط الاجزاء الزوجية لاخفاء المعلومات فيها.
ايضا اقترحنا تشفير الرسالة السرية باستخدام الدالة المضببة القياسية قبل عملية الاخفاء لزيادة قوة الاخفاء .
لقد استخدمنا الطريقة التقليدية LSB للحصول على مساحة اكبر لاخفاء المعلومات.

الكلمات المحجوزة (اخفاء المعلومات، الدالة المضببة)