Hybrid Method based Improved Steganography

Falath M. Mohammed

Al Anbar University/ College of computer

falathm@yahoo.com/

Abstract

Since ancient times Steganography was the best way to transfer secret data from one person to another. The third parties don't know about the transferred information because it is hidden in another media like image, sound, text or video. Unlike encryption, confidential information is open to hackers but cannot be used because it is encrypted.in this paper a new data hiding method has been proposed. In this method the digital image will split into one hindered areas or windows, the standard deviation for each window has computed to choose the smallest fifty values of standard deviation for hiding the data inside this windows. In each window zigzag bath has used to choose the required pixels to hide the secret bits inside it, the first or the second bit of the binary value of the blue component of the pixels in that path has chosen for embedding.

KEYWORD: Steganography, image, pixel, information, embedding, PNSR, embedding

المستخلص

طريقة هجينة لتحسين الستيغانوغرافي منذ العصور القديمة كان ستيغانوغرافيا أفضل وسيلة لنقل البيانات السرية من شخص إلى آخر. بحيث لا يعرف الطرف الثالث المعلومات المنقولة لأنها مخفية في وسائط أخرى مثل الصورة أو الصوت أو النص أو الفيديو. على عكس التشفير، المعلومات السرية مفتوحة للقراصنة ولكن لا يمكن استخدامها لأنها مشفرة.في

هذه البحث تم اقتراح طريقة جديدة لإخفاء البيانات. في هذه الطريقة سوف تنقسم الصورة الرقمية إلى مئة منطقة أو نافذة ، الانحراف المعياري سيحسب لكل نافذة لاختيار اقل خمسين قيمة الانحراف المعياري لإخفاء البيانات داخل هذه النوافذ. في كل نافذة نختار مسارمتعرج لاختيارالبكسلات المطلوبة لإخفاء البتات السرية داخلها ثم يتم اختيار البت الاول أو الثاني من القيمة الثنائية للمكون الأزرق للبكسل الموجود في هذا المسار من اجل الاخفاء

1. INTRODUCTION:

Now in this time computer and internet have been improved and become the major media of communication to exchange a hug information among different parts of the world, but the need of safety and secret communication still an issue, the development of Steganography solve this problem and provide a secret schema to transfer confidential data [4]. Steganography is the art of covered confidential information to send it between two parties in a secret manner, this manner was used by Greek were they called 'covered writing' as a vast array of secret communications methods that hill the message's existence [1]. As long as Steganography was a branch of cryptography when it tries to conceal the secret massage within others medias, avoiding the perception that a message there, as a covered file Steganography use image, sound or text to archives this process [2]. Steganography is an ancient subject started when where two prisoners wish to communicate in secret to create an escape plan, their connotation was passed through the warden who will throw them in solitary imprisonment when he should guess any covert communication [5]. The warden may be passive or active, the passive one who geek and test the message if it contents any confidential information then he will send a report to the higher party and lets the message going. While the active warden will try to change the content of the massage before let it going to another prisoner who doesn't know if the message was detected [6]. Steganography is complementary to the encryption process, therefore using Steganography behind encryption will improve its work because there are problem when sending the encrypted message it still exists as data, and if someone has enough time may decrypt the data, in this case Steganography will provide a secure cover for this information and no one can detect it [3].

2. RELATED WORKS:

Based on LSB (least significance bit) embedding there are many techniques proposed in order to provide security and robust for embedding operation. In 2013 an algorithm proposed to improved transfer confidential letter, after encrypted the message using a key the algorithm's work is to divide the image into blocks size (8*8) and then calculate values standard deviation (STD) for each block, are then finding less, the largest and median value of a standard deviation then isolate sections where the value of the standard deviation less than median value and adopt this sections for embedding all bit of message into the (LSB) for each section [11]. Naziha M. AL– Aidroos and Marghny H. Mohamed, proposed algorithm tends to produce stego similar than the cover image with high embedding capacity, it is summarized by dividing the cover image pixels into two groups smooth and edge area according to the difference value between three pixels adjacent to the target pixel the all inside one block, the embedding process done when if there is a similarity between the message bits and the bits of pixel in smooth area else in the 3LSB of pixel in the edge area and so on[12]. Autade

Parimal and Katariya S. S proposed method to choose the pixels for hide the secret bits, this method summarized by convert the massage into binary bytes after encrypt it using twelve square substitution to get cipher text, then transform the cover image pixels into binary form, each pixel becomes one byte, p is the index variable of bits in the pixel (byte), If the current value p = 0 hides the two bits of the code text in the sixth and seventh bit locations of the current pixel, and the following value p is 1 for the next pixel. If the current value p = 1 hides the two bits of the code text in the bit locations 7 and 8 of the current pixel, and the following value p is 2 for the next pixel. If the current value of p = 2 hides the two bits of the code text at the location of the sixth and eighth bits of the current pixel (byte), and the following value p is 0 for the next pixel. This method gives a robust distribution that resists analysis [13]. An algorithm has been purposed as a modifier of the Kekre algorithm (MKA). This algorithm increases the capacity of the hiding information depending on the least important bit concept and the pixel intensity value, the basis of the algorithm is to divide the image pixels into ranges based on the pixel intensity. The number of secret bits which will embed in each pixel ranges from 1 to 5 bit depend on the range corresponding to that pixel [14].

3. STEGANOGRAPHY TECHNIQUES

There are several techniques to perform the Steganography process each technique depends on the importance of the embedded data and what is the intent of the process. Here are some of these techniques.

3.1. LEAST SIGNIFICANT BIT METHOD (LSB):

This method is based on a confidential message that must be covered in another medium such as digital images to produce what called "stego image", in this case, the data must be delivered with all security and confidentiality without change. Figure 1 illustrates this process.

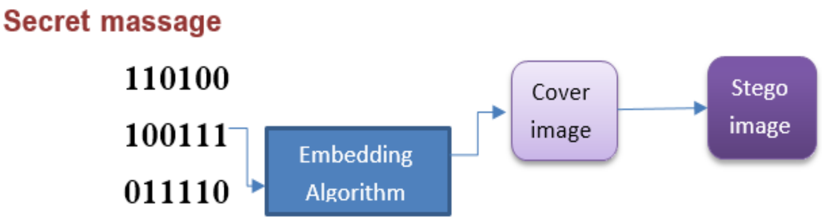


Fig.1 Least significant bit method

Digital image used as cover to include the secret massage, an image is a two-dimensional signal. It is defined by the mathematical function f(x, y) where x is a horizontally coordinate and y is vertical coordinate. Digital image content of pixels which is the smallest thing in the image and the value of the pixel at any point on the image is gives by the function f(x, y) and it is ranging between 0 and 255.

There are several types of digital image like binary (monochrome), gray and color image, the pixel value in the monochrome image either 1 or 0 that mean it two colors only (white or black). In gray one value of pixel ranging between 0 and 255, it has 256 different colors between white and black color.

In the third type of Digital image (color image) any pixel has three color component (blue, red, green), each component has ranged between 0 and 255 in its own color, that means each pixel has 256 × 256 × 256 number of different color, therefore the digital image is suitable to hide a large amount of data without the ability of detection this data because the huge number of colors in the image.

Least significant bit method is one of the easiest ways to embed secret data in the cover object and is used so far efficiently, this process is summarized in following steps:

a) Selecting a specific pixel for embedding,

b) reading this pixel color value and converting it to binary mode,

c) Selecting the Least significant bit (th8).

d) Changing the value of th8 bit by bit from the secret message

e) Returning the process to the rest of the image pixels until the end of the secret message.

The change in a th8 bit of cover image will not be detected by the human eye because the effect of this bit on the color value of pixels is very small and not affect the image's quality.

3.2. DIGITAL WATERMARKING METHOD (DW):

DW a widespread technique used in many applications, in this method, the embedding information is unchanged hides in digital objects like text, image or video. The process of extracting this information leads to the destruction of the original information. Therefore this technique is used in many areas such as proving ownership because the copy process will take all the information in that objects including the secret information contained in it, this process will prevent illegal use of original information.

There are two types of digital watermarking (visible and invisible) in a visible watermark, the data is visible as it is a company logo on the video or image. The TV channels often have logos indicating that the information on the channel is protected. No one is allowed to use this data without permission from the channel, An invisible watermarking is information added to a digital multimedia object, the invisible information is mixed with a digital object which should look like the original object, the most important applications of an "invisible watermark" is copyright protection [7].

Fig.2 (visible watermark)

4. IMAGE STEGANALYSIS

The purpose of the steganography is to hide the information in a way that does not occur to the attacker who would be easy to retrieve the embedded information if he knew the inclusion algorithm, so the first thing the attacker does is try to know the algorithm used in the embedding by analyzing the cover image and this is called steganalysis. An attacker can do several things in the picture, such as investigating or destroying embedded information, extracting this information or including other information to mislead the other. The attack can be of two types passive and active. In the first, the attacker only sees the message or in the second the attacker changes or destroy the content of the message.

There are several forms where steganalysis is performed based on information available for analysis, when *stego only available attack* there is no other information available to obtain the secret massage, it is the hardest investigated case, and it needs try every known steganography algorithms which used for embedding.

The second case is called a known cover attack, the available information, in this case, is the cover medium in addition to the stego medium, the attacker will compare the two mediums to identify the steganography algorithm and then retrieve the secret message.

The third case is called Known Message Attack when the secret message is known in addition to the stego image, this case is useful for guessing and predicting the future algorithms.

In another hand when the embedding algorithm is known this case is called targeted (special) steganalysis unlike an unknown embedding algorithm situation, the analyst has to experiment with several algorithms to get the best result, this case is called blind steganalysis [8].

4.1. STATISTICAL ATTACKS

After the embedding of confidential information to the image some of the image characteristics will be change, this change indicates the presence of confidential information inside the image and this will leads the analyst to use many statistical techniques to obtain confidential information based on the available information the Statistical Attacks can be divided Into two kinds Universal and special statistical steganalysis.

4.1.1. SPECIAL STATISTICAL STEGANALYSIS:

These techniques need a detailed knowledge of embedding process, the analyzing of the embedding operating yield very accurate results when used against a target steganography technique, where confidential information can be retrieved. There are many techniques underlying this technique based on the embedding method like LSB embedding steganalysis, LSB matching steganalysis, Spread–spectrum steganography steganalysis, BPCS–steganography steganalysis, JPEG–compression steganography steganalysis, Transform domain steganography steganalysis, Additive noise steganography steganalysis [9].

4.1.2. UNIVERSAL STATISTICAL STEGANALYSIS:

This technique not attack specific embedding method and not need prior information about stenographic methods, it requires estimating the embedding method and constructs the detection model by using different techniques like a neural network, clustering algorithms and other soft computing tools[10].

4.1.3 HISTOGRAM ANALYSIS

In statistics, Histogram is a famous tool in data analysis for its simplicity and clarity for data distribution. A histogram is a representation of tabulated frequencies used to visualize the changes made by embedding to the image, it is shown as adjacent rectangles, erected over limited intervals (bins), with an area equal to the frequency of the observations in the interval. A histogram may also be normalized displaying relative frequencies.The human eye does not notice the changes that occur after you insert images, but the change in the graph of the image can be observed before and after embedding, so it can deduce the existence of confidential information within the image.[15]

5. STANDARD DEVIATION

This measure represents the extent of dispersion and deviation from the arithmetic mean, the square root of the variance, after dividing the image into a blocks, the arithmetic mean will be calculated for each block then calculate the difference between the value of each pixel in the block and the value of arithmetic mean of that block. That is mean that blocks with a High value of standard deviation have many different colors value and I think that is Useful to embedding data which will become unclear to the human eye in this case.

The arithmetic mean (μ) can be calculated as follows:

$$\mu = \frac{1}{N}\sum_{i=0}^{N-1} x_i \qquad \text{......} \ (1)$$

Where *N* is a total number of pixel in the block, *x* is the value of the current pixel.

$$\sigma^2 = \frac{1}{N-1}\sum_{i=0}^{N-1} (x_i - \mu)^2 \qquad \text{...} \ (2)$$

Where σ is a standard deviation.

6. Peak Signal-to-Noise Ratio (PSNR)

Another evaluation method to estimate the changes in image data is the peak signal to noise ratio

Ratio Peak (PSNR). It is a good method to masseur the noise ratio inside the image which occurred when some operations take place to the image like transform, embedding, compression and so on. In the calculation of PSNR, we must first calculate the Square Error Mean (MSE) between the

Hidden image and the cover image. The equation is represented as below.

$$MSE = \frac{\sum_{M,N}[I_1(m,n) - I_2(m,n)]^2}{M * N} \quad \text{........ (3)}$$

I_1 and I_2 respectively represent the pixel intensity of the cover image and the hidden image, N*M for the total number of pixels. Then use the MSE to get the PSNR value of the hidden image

As follows:

$$PSNP = 10\lg\left(\frac{255^2}{MSE}\right) \quad \text{..... (4)}$$

7. THE PROPOSED ALGORITHM

The proposed algorithm in this paper is an expansion of several previous algorithms, it is passed through several steps:

a) In this stage, the image will be divided into blocks each one has (10×10) pixels,

b) Find the standard deviation for each block.

c) Reorder the blocks upward to choose the block that has the highest standard deviation values.

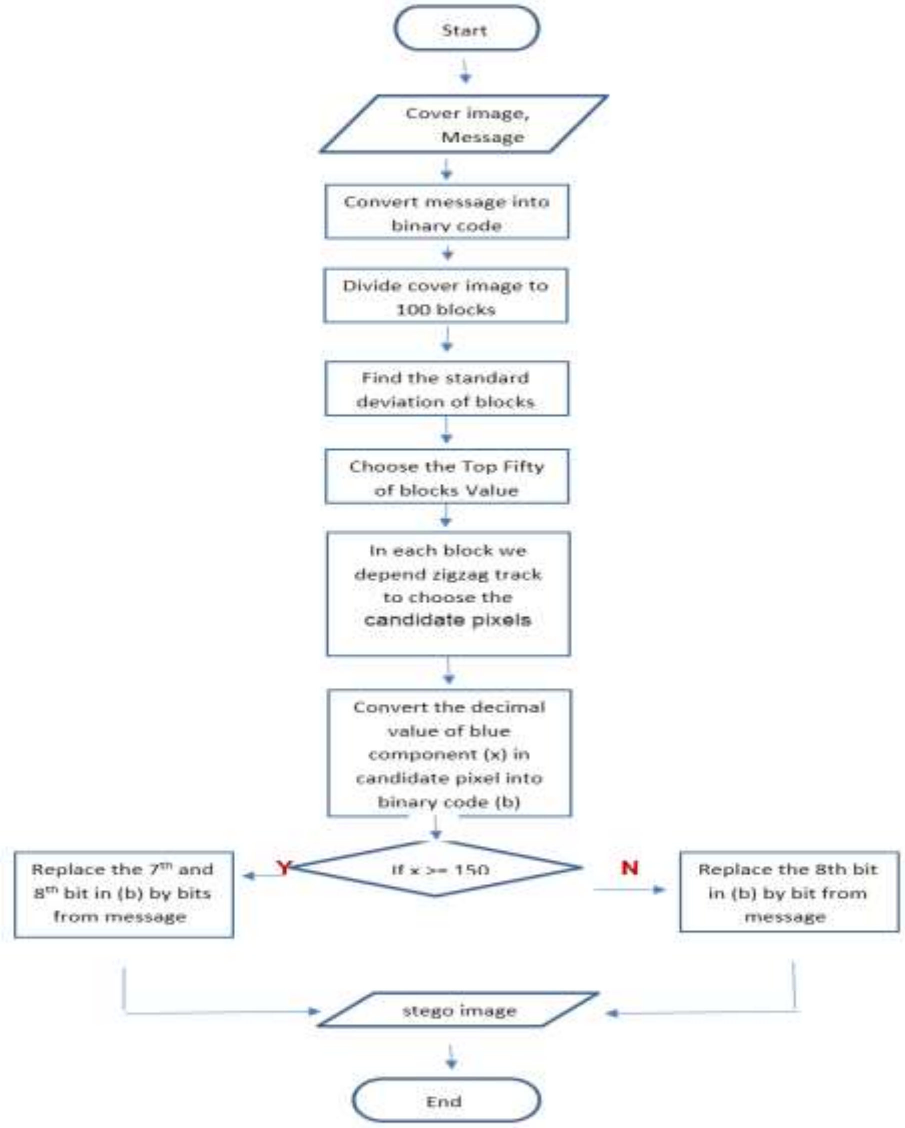
d) Convert the secret massage into binary code to embedding it in the blocks.

e) Each block is an array of 10×10 pixel then we will move in the zigzag path from the pixel with position $(0,0)$ to position $(0,9)$ then go back from position $(1,9)$ to$(1,0)$ and so on.

f) For embedding, the value of the blue component of the color in each chosen pixel will be converted into binary code

g) The 8th and 7th bit in the blue component will be chosen for embedding if the decimal value of the blue component is greater than 150 else the embedding will be in 8th bit only.

8. THE ALGORITHM FLOWCHART


Start
Cover image, Message
Convert message into binary code
Divide cover image to 100 blocks
Find the standard deviation of blocks
Choose the Top Fifty of blocks Value
In each block we depend zigzag track to choose the candidate pixels
Convert the decimal value of blue component (x) in candidate pixel into binary code (b)
If x >= 150
Y
N
Replace the 7th and 8th bit in (b) by bits from message
Replace the 8th bit in (b) by bit from message
stego image
End

9. EXPEREMENTAL RESULT

As mention in the proposed algorithm the standard deviation used as factor to choose the appropriate block for embedding, the block with highest standard deviation values has been chosen because it has a lot different color values and I see this appropriate to embedding where the human eye cannot distinguish the difference in color value that will occur after the inclusion of classified information within this block, especially when the amount of embedding information was large, in this paper the following massage has been used for embedding (I'm happy to see you again in Iraq my sir) in different images size and type as mention in table 1. The adoption of the standard deviation provides random order for embedding process, and this is Difficult for analyzing.

Table 1

Image	PSNR
	80.1269984229716
320*480	
	80.5498890441324
360 * 640	
	84.4965120332404
1920 * 1200	
	67.8443517941838
224 * 225	
	74.030035888356
190*265	

In the designated block a zigzag bath will be adopted for embedding to increase the difficulty of analyzing operation, then in the designated pixel another algorithm will be adopted to increases the complexity and amount of embedding operation, according to this algorithm the amount of embedding bits depend on the value of color intensity. logically any simple change in the large numbers will have no significant impact on its value of that number, this applies to the colors of the picture, the change in the large color values will not be visible to the human eye, therefore more than one bit will be embed if the color value of the blue component of the pixel is greater than 150 and one bit if the color value is less than 150. The previous table displays PSNR values for different size images after inclusion with the same secret message and obtained high values PSNR which mean the strength of the proposed method, the contrast in the PSNR values between the images due to the size of these images, when the size of the image is large the value of PSNR will be great also.

References

1. F. Johnson, Sushil Jajodia, Exploring Steganography Seeing the Unseen, George Mason University, IEEE, 1998.
2. J. Juan, M.Jesús, SLSB: Improving the Steganographic Algorithm LSB, Universidad Nacional de Educación a Distancia (Spain).
3. Kumar Arvind, Km. Pooja, “Steganography- A Data Hiding Technique”, International Journal of Computer Applications (0975 – 8887), Volume 9– No.7, Nov. 2010.
4. Hamid Nagham, Yahya Abid, “Steganography in image files: A survey”, Australian Journal of Basic and Applied Sciences, 7(1): 35-55, 2013.

5. . Chandramouli, R., Kharrazi, M. & Memon, N., "Image steganography and steganalysis: Concepts and Practice", Proceedings of the 2nd International Workshop on Digital Watermarking, October 2003.
6. Anderson, R.J. & Petitcolas, F.A.P., "On the limits of steganography", IEEE Journal of Selected Areas in Communications, May, 1998.
7. Mustafa Ramadhan," Information Hiding in Images Using Steganography Techniques", Conference Paper, March, 2013.
8. Li Bin, "A Survey on Image Steganography and Steganalysis", Journal of Information Hiding and Multimedia Signal Processing, Volume 2, Number 2, April 2011.
9. Nissar a Arooj, Mir A.H., Classification of steganalysis techniques: A study, Digital Signal Processing 20 (2010).
10. Kaur Manveer, Kaur Gagandeep, Review of Various Steganalysis Techniques, International Journal of Computer Science and Information Technologies, Vol. 5 (2), 2014.
11. Nadia Maan, Ream Jassim," improve LSB method using Standard Deviation measurement", AL Rafidain Journal of Computer Science and Mathematics, volume10, 2013.
12. AL- Aidroos. Naziha M, Mohamed H. Marghny, "data hiding technique based on dynamic LSB",.
13. Parimal Autade, S. S Katariya, "steganography using twelve square substitution cipher and LSB positions", International Journal of Electrical and Electronics Engineering (IJEEE), Vol. 2, Issue 4, Sep 2013.
14. Savita, Juneja Mamta," High Capacity Information Hiding System for Encrypted Text Message Using Pixel Intensity Based LSB Substitution Technique", International Journal (IJCSI) of Computer Science, Vol. 11, Issue 2, No 1, March 2014.
15. M. El-Sayed, Al-Sadi. Azzat, "Pixel-Value Differencing Steganography: Attacks and Improvements",