New Image Steganography Method using Zero Order Hold Zooming

Abdelmgeid A. A. Tarek A. A. Al-Hussien Seddik Saad Shaimaa M. H.

ABSTRACT
Steganography is a branch of information hiding. It allows the people to communicate secretly. Steganography word is classified into two parts: Steganos which means “secret or covered” (where you want to hide the secret messages) and the graphien which means “writing". It aims to embed secret data into a digital cover media, such as digital audio, image, video, etc., without being suspicious looking. In This paper a new image steganography method that hides the secret message inside the cover image using zero order hold (ZOH) is considered. The main goal of this method is to hide a secret message in the pixels of the cover image in such a way that the human eyes are not able to differentiate between the original and the stego-image.

Keywords
Image Steganography, Peak Signal-to-Noise Ratio (PSNR), Maximum Hiding Capacity (MHC), Zero Order Hold (ZOH).

1. INTRODUCTION
Over the last two decades, the rapid development of internet requires confidential information that needs to be protected from the unauthorized users. This is accomplished through data hiding. It is a method of hiding secret messages into a cover file [1].

Steganography techniques are used to secure the secret message transmitted over an open communication channel such as the internet. But message transmission over the internet is facing some problems. So securing communication channel for transmitting data over the internet is needed. Two schemes are used to protect secret messages from being stolen during transmission. The first scheme is a cryptography which is a well-known method in which the information is encrypted by using a key and then sent over the channel and only the right person with a right key can decode and recover the original information successfully. The second one is a steganography (which is the point of research) is a method in which the secret information is hidden inside a carrier file [2] [9].

Steganography is often confused with cryptology because the two methods are similar in the way that they both are used to protect important information. The difference between them is that steganography involves hiding information so it appears that no information is hidden at all. If a person sees the object that has hidden information, he will not expect or notice that any data in it. Therefore the person will not attempt to decrypt the information [2] [13].

Steganography literally means "covered writing" which is derived from the Greek words steganos and graphien. Steganography is defined by Markus Kahn [10] as follows, "Steganography is the art of concealing the existence of information within seemingly innocuous carriers". However, in the hiding information the meaning of steganography is hiding secret messages into media file such as image, text, sound, and video [1] [7].

Steganography ancient origins traced back to 440 BC. It was started by the Greeks by shaving the head of a messenger and tattooed a message on the messengers head. After allowing his hair to grow, the message would be undetected until the head was shaved again [11]. As well as, the invisible ink used for hiding the secret messages by the American revolutionaries during the USA Revolution. Also it was used in both World Wars by German army [4].

The main terminologies used in steganography systems are: the cover file, secret message, stego file, embedding algorithm and extraction algorithm. The cover file is defined as the original file such as image, video, audio, text, or some other digital media used to embedding the secret message. The secret message is defined as the message you want to embed inside the cover file, it is called payload. Stego file is defined as the file after embedding the secret message in the cover file; it should have similar properties to that of the cover. The embedding algorithm is the method that used to embed the secret message in the cover image. The extraction algorithm is the method that retrieves the secret message from the stego image [7] [14].

In the Steganography system, before the hiding process, the sender must select the carrier (i.e. image, video, audio or text) [12] then select the secret message. The effective and appropriate Steganography algorithm must be selected that able to encode the message in more secure technique. Then the sender may send the Stego file by email or chatting, or by other techniques. After receiving the message by the receiver, the message can be decoded by using the extracting algorithm [7]. The Steganography system is shown in Figure (1) [12].

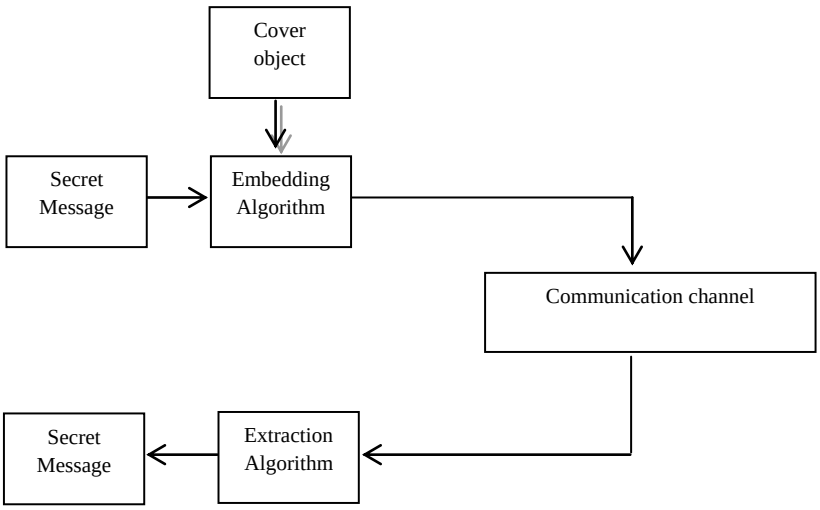

Fig 1: The Steganography system

Many carrier messages can be used in the recent technologies, such as Image, text, video and many others. The image file is the most popular used for this purpose because it is easy to send during the communication between the sender and receiver that makes the information more secure.

In this paper a new method that hides the secret message inside the cover image using Zero order hold Zooming method (ZOH). It is also known as zoom twice [3].

2. ZERO ORDER HOLD METHOD

There are many methods for zooming image, Zero order hold is one of this. In zero order hold method, two adjacent elements are picked from the rows respectively and then the average value between two pixel (add them and divide the result by two then take the integer value) is calculated, and their result is placed in between those two elements. First, this row is done wisely and then the result is taken and do this column is don wisely as the same way [3].

For example let's take an image of the dimensions of 2 rows and 2 columns and zoom it using Zero Order Hold Method.

4	6
7	8

First zoom it row wise

First row, two pixels is (4, 6) , average (4+6)/2 =5.

Second row, two pixels is (7, 8) , average (7+8)/2 =7.

4	5	6
7	7	8

Second zoom it column wise

First column, tow pixels is (4, 7) , average (4+7)/2 =5.

Second column, tow pixels is (5, 7) ,average (5+7)/2=6.

Third column, tow pixels is (6, 8), average (6+8)/2=7.

4	5	6
5	6	7
7	7	8

3. LSB METHOD

There have been many techniques for hiding information or messages in images such as Least Significant Bit (LSB) is a simple approach to embedding information in spatial domain image steganography. The simplest Steganography techniques embed the bits of the message directly into least significant bit plane of the cover-image in a deterministic sequence. Modulating the least significant bit does not result in human perceptible difference because the amplitude of the change is small. [2].

This is one of the simplest and easiest methods of hiding the data in images. In this method, the binary data form is hidden into the LSBs of the carrier bytes or in pixels of image. The overall change to the image is so small that human eye would not be able to discover. In 24-bit images each 8-bit value refers to the red, green and blue color. But in 8–bit images each pixel is of 8-bits, so each pixel stores maximum 256 colors [6].

For example, suppose hiding a message in 24-bit color image whose RGB components are separated and the original image pixels are:

(00100111 11101000 11001000)
(00100111 11001001 11101001)
(11001000 00100111 11101000)

Suppose hiding character “S” within the image whose binary representation is 01010011 within the image using LSB of each RGB component. After hiding the resulting image pixels are:

(00100110 11101001 11001000)
(00100111 11001000 11101000)
(11001001 00100111 11101000)

In each pixel only one bits of character are hidden by changing the LSB of blue channel bits of a pixels of the image.

4. PROPOSED METHOD

In the proposed method, the secret message in the image is embedded using zero order hold method (ZOH). In this method the pixel of the image is modify if the end of the average of two adjacent pixels are not equal to the bit of the message, But the pixel of the image doesn't change if the end

of the average is equal to the bit of the message. In extraction, the image will be zoomed using ZOH method pick two adjacent elements from the rows respectively then add them and divide the result by two, and place their result in between those two elements. First do this row wise and then do this column wise then extract the pixel from the image as show in extraction algorithm and save it.

Using this method there is a high security and high PSNR and approximately MHC compared to the LSB method.

4.1 ZOH Embedding Algorithm

Input: Cover Image C; Secret Message M.

Output: StegoImage S.

Steps:

1) Split C into 3 channels Red (R), Green (G), and Blue (B).
2) Convert image (B) to one column x.
3) Split M into characters.
4) Take m from M.
5) Convert m into binary bin.
6) Take pixel 1 from bin.
7) Calculate average of x (count) and x (count+1).

If end (average)! =end (bin) then x (count+1) = x (count+1) +2

8) Add 1 to count.
9) Repeat steps from 4 to 8 until the whole M has been embedded in C.
10) Merge the 3 channels R, G, y again to construct the StegoImage S.

4.1.1 ZOH Extraction Algorithm

Input: StegoImage S, size of message W.

Output: Secret Message M.

Steps:

1) Split S into 3 channels Red (R), Green (G), and Blue (B).
2) Zoom the image

   i) In rows: calculate the average between two row respectively and place the result between them.

   ii) In columns: calculate the average between two column respectively and place the result between them.
3) Merge the 3 channels R, G, B again to construct the image after zooming(V)
4) Split V into 3 channels Red (R), Green (G), Blue (B).
5) Calculate size of the image R(rows),C(columns).
6) Convert image (B) to column x .
7) Count=2.
8) For t=1:W
   y=dec2bin(x(count))
   M(t)=y(end)
   if ((mod(count+1+C))=0)
   count=count+C+1
   end
   count=count+2
   end
9) Convert M from binary to character.

5. EXPERIMENTAL RESULTS

In this section, the proposed method (ZOH) has been tested by taking different messages with different lengths and hiding them in some cover images. The results that are obtained from these experiments are recorded and can be summarized in the following tables.

Table 1. Comparison between (LSB-3) and (ZOH) Methods

Cover images	Message Capacity	PSNR	
		LSB – 3	ZOH
Boat	8,160	39.1132	49.9386
Bird	8,160	39.0955	49.9167
Flinstone	8,160	39.1188	49.9513

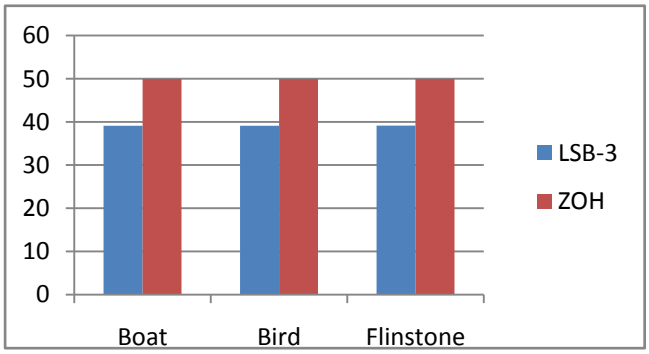

Fig 2: Comparison between PSNR values of Table1

As shown in Table 1 and Fig 2, after hiding the same message length 8,160 bytes in the cover images (Boat, Bird, Flinstone) with size (256 x 256), using the (LSB-3) and (ZOH) methods, it has been found that, the (ZOH) method has higher PSNR values than the (LSB-3).

Table 2. Comparison between (Modified LSB-3) and (ZOH) Methods

Cover images	Message Capacity	PSNR	
		Modified LSB – 3	ZOH
Boat	8,160	42.4163	49.9386
Bird	8,160	42.4062	49.9167
Flinstone	8,160	42.2932	49.9513

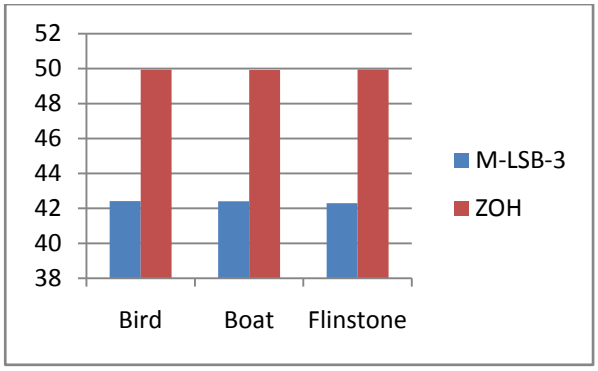

Fig 3: Comparison between PSNR values of Table2

Also in Table 2 and Fig 3, after hiding the same message length 8,160 bytes in the cover images (boat, bird, flinstone) with size (256 x 256), using the (Modified LSB-3) and (ZOH) methods, it has been found that, the (ZOH) method has higher PSNR values than the (Modified LSB-3).

Table 3. Comparison between (MSLDIP) and (ZOH) Methods

Cover images	Message Capacity	PSNR	
		MSLDIP	ZOH
Boat	8,160	47.77530	49.9386
Bird	8,160	47.61975	49.9167
Flinstone	8,160	47.61975	49.9513

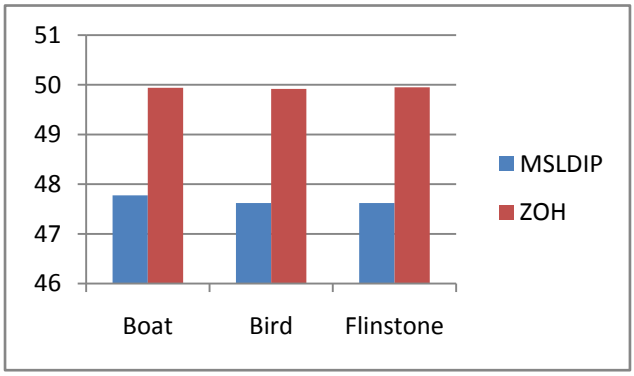

Fig 4: Comparison between PSNR values of Table3

Also in Table 3 and Fig 4, after hiding the same message length 8,160 bytes in the cover images (boat, bird, flinstone) with size (256 x 256), using the (MSLDIP) and (MSLDIP-MPK) and (ZOH) methods, it has been found that, the (ZOH) method has higher PSNR values than the (MSLDIP) and (MSLDIP-MPK).

Table 4. Comparison between MSLDIP-MPK and (ZOH) Methods

Cover images	Message Capacity	PSNR	
		MSLDIP-MPK	ZOH
Boat	8,160	49.36969	49.9386
Bird	8,160	49.54604	49.9167
Flinstone	8,160	49.25001	49.9513

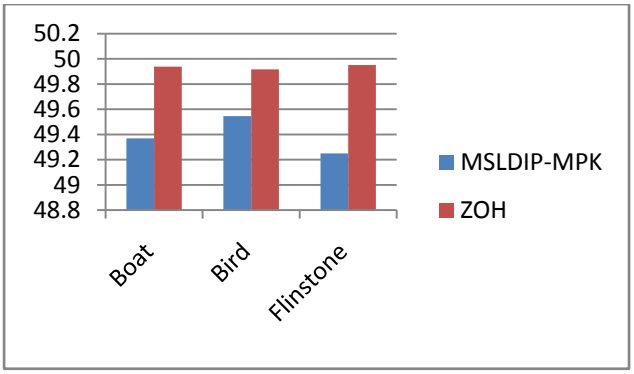

Fig 5: Comparison between PSNR values of Table2

Also in Table 4 and Fig 5, after hiding the same message length 8,160 bytes in the cover images (boat, bird, flinstone) with size (256 x 256), using the (MSLDIP-MPK) and (ZOH) methods, it has been found that, the (ZOH) method has higher PSNR values than the (MSLDIP-MPK).

Finally, as shown in tables (1), (2) ,(3)and (4), after the comparisons have been done among the proposed method(ZOH) and the methods; LSB–3, Modified LSB–3, MSLDIP and MSLDIP-MPK methods by using the same secret message which consists of 8,160 characters and 3 different cover images (256 x 256) (boat, bird, flinstone) .it is found that the proposed method (ZOH) has more PSNR values than other LSB methods which means the stego image quality of the method will be higher than the quality of other LSB methods.

6. CONCLUSION

As shown in comparison tables, after doing the same experiments using the ZOH, four different methods, the PSNR values of the proposed method (ZOH) were higher than other methods, this means the method's PSNR (stego image quality) is improved successfully. As a future work, we will try to improve Maximum Hiding Capacity (MHC) by improving the secret message using LSBraille image steganography method (Image Steganography Method by Using Braille Method of Blind People). by representing the secret message characters by using Braille method of reading and writing for blind people that can save more than one-fourth of the required space for embedding.

7. REFERENCES

[1] Bret D., "A detailed look at Steganographic Techniques and their use in an Open-Systems Environment", Sans Institute, 1(2002).

[2] Akbas E. A., "A New Text Steganography Method By Using Non Printing Unicode Characters", Eng. & Tech. Journal, VOL.28, NO.1, 2010.

[3] http://www.tutorialspoint.com/dip/Zooming_Methods.htm.

[4] Por L. Y., Delina B., "Information Hiding: A New Approach In Text Steganography" 7th WSEAS int. Conf. on Applied Computer & Applied Computational Science (ACACOS '08), Hangzhou, China, April 6-8, 2008

[5] Abdelmged A. A., Al-Hussien S. S., "Image Steganography Technique By Using Braille Method of Blind People (LSBraille) ", International Journal of Image Processing (IJIP), Vol 7, Issue 1, 2013.

[6] Chutani S., Goyal H. "LSB Embedding In Spatial Domain - A Review Of Improved Techniques". International Journal of Computers & Technology, ISSN: 2277-3061, 3(1),Aug. 2012.

[7] Atallah M. A. "A New Method In Image Steganography With Improved Image Quality". Applied Mathematical Sciences, 6(79), pp. 3907 – 3915, 2012.

[8] Aiad, I. A., "Hiding Data Using LSB - 3 ", J.Basrah Researches (Sciences), Vol. 33, No.4. (81-88), December, 2007.

[9] Ahmed A. R., Ahmed S. and Al-Hussien S. S., " A High Capacity SLDIP (Substitute Last Digit In Pixel ", Fifth International Conference on Intelligent Computing and Information Systems (ICICIS 2011), 30 June - 3 July, 2011, Cairo, Egypt.

[10] Johnson, Neil F., "Steganography", 2000, URL: http://www.jjtc.com/ stegdoc/index2.html

[11] Jagvinder K. and Sanjeev K., "Study and Analysis of Various Image Steganography Techniques", IJCST Vol. 2, Issue 3, September 2011.

[12] Al-Hussien S. S., " Enhancing the (MSLDIP) Image steganographic method (ESLDIP Method) ", International Conference on Graphic and Image Processing (ICGIP 2011), Proc. of SPIE Vol. 8285, 82853I, © 2011 SPIE.

[13] Mohammed A. F., "Image Steganography by Mapping Pixels to Letters ", Journal of Computer Science, 5 (1) : 33-38, ISSN 1549-3636, 2009.

[14] Vipul S., Sunny K.,"A New Approach to Hide Text in Images Using Steganography ", International Journal of Advanced Research in Computer Science and Software Engineering (IJARCSSE), Volume 3, Issue 4, April 2013.