Improving ZOH Image Steganography Method by using Braille Method

Abdelmged A. A.
Computer Science Department
Minia University, Egypt

Tarek A. A.
Computer Science Department
Minia University, Egypt

Al-Hussien Seddik Saad
Computer Science Department
Minia University, Egypt

Shaimaa M. H.
Computer Science Department
Minia University, Egypt

ABSTRACT

Steganography is considered one of the branches of data hiding. It is the science of hiding sensitive information in a cover such as image, audio, video to achieve secure and secret communication. The word steganography derived from two Greek words: steganos means covered and graphien means writing and often refers to secret writing. The most common use of steganography is to hide a file inside another file. In this paper we modify the secret message that embedded into the cover not the technique of embedding of the previously proposed image steganography method using Zero Order Hold zooming (ZOH) by using LSBraille image steganography method that can represent the secret message characters by 6 bits only not 8 bits as binary representation. The proposed method provides MHC and PSNR more than the previously proposed method ZOH.

Keywords

Steganography, Zero Order Hold (ZOH) Method, Peak Signal-to-Noise Rate (PSNR), Mean Square Error (MSE).

1. INTRODUCTION

In recent years, the rapid growth of information technology and digital communication has become very important to secure information transmission between the sender and receiver. This growth of information encourages researchers to develop security techniques to secure data transmission between sender and receiver from attacker's .Therefore, steganography introduces strong way to hide information and to communicate a secret data in an appropriate multimedia carrier, e.g., image, text, audio and video files [1].

The idea of information hiding is not new to history. As early as in ancient Greece there were attempts to hide a message in trusted media to deliver it across the enemy territory. In ancient time, secret information is hidden in the back of wax that covered tablets, scalp of the slaves etc. In the modern world of digital communication, there are several techniques used for hiding information in any medium. One of such technique is steganography, the word steganography derived from two Greek words: steganos means covered and graphien means writing and often refers to secret writing or data hiding [2].

Steganography aims to embed secret data into a digital cover media, such as digital audio, image, video, etc., where the hidden message will not be apparent to an observer. The major goal of it is to increase communication security by inserting secret message into the digital image and is recently become important in a number of application areas especially military. The most cover media used for steganography is image. The reason is that the large amount of redundant data present in the images can be easily altered to hide secret messages inside them without attracting attention to human visual system (HVS).

Cryptography and Steganography achieve the same goal via different means; Cryptography encodes the data into an unreadable format. Steganography differs from Cryptography in the sense that where cryptography focuses on keeping the contents of a message secret, whereas steganography focuses on keeping the very existence of the message secret. By using steganography there is a chance to send messages so that nobody can detect the existence of the message.

There are a number of Image steganography techniques that hide message in an image; these techniques can be classified according to the format of the cover image or the method of hiding. There are two popular types of image steganography techniques; spatial domain techniques and transform domain techniques [3].

In spatial domain techniques, the secret messages are embedded directly in the image. , the most common and simplest steganography method is the least significant bits (LSB) insertion method. Other spatial domain techniques include contrast adjustment, noise insertion, etc.

In transform domain pixel values are transformed and then processing is applied on the transformed coefficients. The first step is to transform the cover image into different domain. Then the transformed coefficients are processed to hide the secret information. Finally, these changed coefficients are transformed back into spatial domain to get the stego image. The transformed coefficients are obtained by applying transforms, such as Discrete Cosine Transformation (DCT) and Discrete wavelet transformation (DWT) to the image. In DCT, after transforming the image in frequency domain, the data is embedded in the least significant bits of the medium frequency components and is specified for loss compression while In DWT, secret messages are embedded in the high frequency coefficients resulted from Discrete Wavelet Transform and provide maximum robustness. [11].

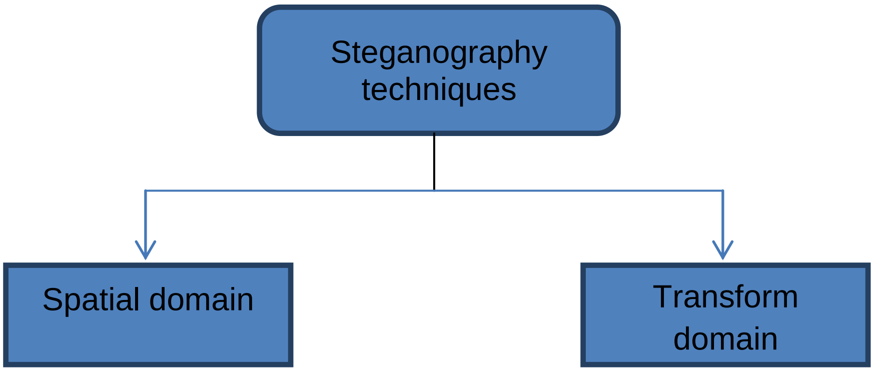

Fig. 1: Techniques of Steganography

The major objective of steganography is to prevent some unintended observer from stealing or destroying the confidential information. There are some factors to be considered when designing a steganography system:

• Invisibility: Invisibility is the ability to be unnoticed by the human.

• Security: Even if an attacker realizes the existence of the information in the stego object it should be impossible for the attacker to detect the information.

• Capacity: The amount of information that can be hidden relative to the size of the cover object without deteriorating the quality of the cover object.

• Robustness: It is the ability of the stego to withstand manipulations such as filtering, cropping, rotation, compression etc. [12].

For implementation of the steganography system, two algorithms are needed to be designed: one for embedding data and the other to extract this successfully. The embedding algorithm is concerned with hiding a secret message in the cover without attracting any attention. The extraction algorithm is a much simpler process and can be achieved by inversing the steps of embedding algorithm, where the secret message is retrieved at the end.

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. RELATED WORK

In [14] authors proposed a new encoding technique that is called Mobile Phone Keypad encoding (MPK) for secret message that represent each character in the secret message by two digits only not three digits as ASCII encoding, and they constructed a full characters' table that contains small letters (a ... z), capital letters (A ... Z), digits (0 ... 9) and special characters (@, -, +, ...) and this proposed MPK encoding technique saved one third of the required space for embedding which in turn enhanced the Maximum Hiding Capacity (MHC) of the cover image, as a result of this the PSNR values have been enhanced too.

In [5] the authors proposed new image steganography method using zero order hold zooming (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.

In [6] the authors proposed a method that hides the secret message inside the cover image 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. The proposed method is using the Braille method representations of the characters as each character is represented by only 6 dots using the 6 – dots matrix which called (Braille Cell). The method will start by representing these characters (dots) as binary digits each of which consists of 6 bits only, not eight bits as in original LSB embedding method which uses the binary representation from the ASCII table. So, by using this representation one-fourth of the MHC for each cover image can be saved which will increase the MHC and enhance the PSNR.

In this paper, we modify the secret message itself before embedding it in the cover image has been done instead of modifying the embedding technique.

3. PROPOSED METHOD

In the proposed method we modify the secret message of the previously proposed image steganography method using Zero Order Hold Zooming (ZOH) by using LSBraille image steganography method to increase MHC.

In LSBraille method the first step was to represent the letters as show in table 1 by 6 bits only not 8 bits as in original binary representation from the ASCII table. So, through using this representation 2 pixels are saved from each secret byte embedding process or more than one-fourth of the maximum hiding capacity for each cover image, So that it will increase the maximum hiding capacity (MHC) and PSNR of the stego image.

Table 1. Braille characters representation.

char	Black Dots Index in Cell	Binary Representation (6 bits)					
		1	2	3	4	5	6
a	1	1	0	0	0	0	0
b	1,2	1	1	0	0	0	0
c	1,4	1	0	0	1	0	0
d	1,4,5	1	0	0	1	1	0
e	1,5	1	0	0	0	1	0
f	1,2,4	1	1	0	1	0	0
g	1,2,4,5	1	1	0	1	1	0
h	1,2,5	1	1	0	0	1	0
i	2,4	0	1	0	1	0	0
j	2,4,5	0	1	0	1	1	0
k	1,3	1	0	1	0	0	0
l	1,2,3	1	1	1	0	0	0
m	1,3,4	1	0	1	1	0	0
n	1,3,4,5	1	0	1	1	1	0
o	1,3,5	1	0	1	0	1	0
p	1,2,3,4	1	1	1	1	0	0
q	1,2,3,4,5	1	1	1	1	1	0
r	1,2,3,5	1	1	1	0	1	0
s	2,3,4	0	1	1	1	0	0
t	2,3,4,5	0	1	1	1	1	0
u	1,3,6	1	0	1	0	0	1
v	1,2,3,6	1	1	1	0	0	1
w	2,4,5,6	0	1	0	1	1	1
x	1,3,4,6	1	0	1	1	0	1
y	1,3,4,5,6	1	0	1	1	1	1
z	1,3,5,6	1	0	1	0	1	1
1	1,6	1	0	0	0	0	1
2	1,2,6	1	1	0	0	0	1
3	1,4,6	1	0	0	1	0	1
4	1,4,5,6	1	0	0	1	1	1
5	1,5,6	1	0	0	0	1	1
6	1,2,4,6	1	1	0	1	0	1
7	1,2,4,5,6	1	1	0	1	1	1
8	1,2,5,6	1	1	0	0	1	1
9	2,4,6	0	1	0	1	0	1
0	1,2,3,4,5,6	1	1	1	1	1	1
,	2	0	1	0	0	0	0
;	2,3	0	1	1	0	0	0
:	2,5	0	1	0	0	1	0
.	2,5,6	0	1	0	0	1	1
?	2,6	0	1	0	0	0	1
!	3,4,5,6	0	0	1	1	1	
'	3	0	0	1	0	0	0
-	3,6	0	0	1	0	0	1
“	4	0	0	0	1	0	0
&	1,2,3,4,6	1	1	1	1	0	1
[	1,2,3,5,6	1	1	1	0	1	1
@	2,3,4,6	0	1	1	1	0	1
]	2,3,4,5,6	0	1	1	1	1	1
+	2,3,5	0	1	1	0	1	0
=	2,3,5,6	0	1	1	0	1	1
<	2,3,6	0	1	1	0	0	1
*	3,5	0	0	1	0	1	0
>	3,5,6	0	0	1	0	1	1
/	3,4	0	0	1	1	0	0
)	3,4,5	0	0	1	1	1	0
_	3,4,6	0	0	1	1	0	1
(	4,5	0	0	0	1	1	0
$	4,5,6	0	0	0	1	1	1
%	4,6	0	0	0	1	0	1
Space	Empty cell	0	0	0	0	0	0

LSBraille method will be applied on the ZOH method; the ZOH-Braille will give us a higher capacity than the original method and the maximum number of bytes that can be hidden in any image (MHC).

Table 2. Maximum Hiding Capacity

Image size (Pixels)	Maximum Hiding Capacity (Byte)	
	ZOH	ZOH-Braille
8 x 8	7	9
16 x 16	30	40
32 x32	124	165
64 x 64	504	672
128 x 128	2,032	2,709
256 x 256	8,160	10,880
512 x 512	32,704	43,605
1024 x 1024	130,944	174,592

As show in table 2, after the modification, ZOH-Braille method will has high embedding capacity than the original ZOH.

The proposed method will work as in the following algorithm:-

ZOH-Braille 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) Convert the message(M) using LSBraille MB
5) Take m from MB.
6) Convert m into binary bin.
7) Take pixel 1 from bin.
8) Calculate average of x (count) and x (count+1). If end (average)! =end (bin) then x (count+1) = x (count+1) +2
9) Add 1 to count.
10) Repeat steps from 4 to 8 until the whole M has been embedded in C.
11) Merge the 3 channels R, G, y again to construct the StegoImage S.

4. EXPERIMENTAL RESULTS

In this section, the proposed method (ZOH-Braille) 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 3. Comparison between (ZOH) and (ZOH-Barille) Methods

Cover images (256 x 256)	Message Capacity	PSNR	
		ZOH	ZOH-Braille
Boat	8,160	49.9386	51.1542
Bird	8,160	49.9167	51.1961
Flinstone	8,160	49.9513	51.2214

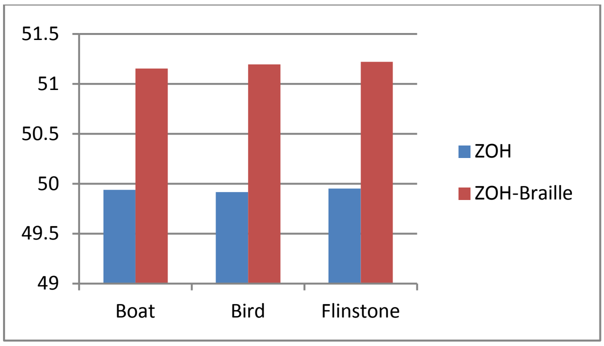

Fig 2: Chart showing comparison between PSNR values of Table3

As shown in Table 3 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 (ZOH) and (ZOH-Braille) methods, it has been found that, the (ZOH-Braille) method has higher PSNR values than the (ZOH).

Table 4. Comparison between (ZOH) and (ZOH-Braille) Methods

Cover images (256 x 256)	Message Capacity	PSNR	
		ZOH	ZOH-Braille
Lena	8,160	49.9175	51.1515
Baboon	8,160	49.8981	51.2217
Peppers	8,160	49.8942	51.1720

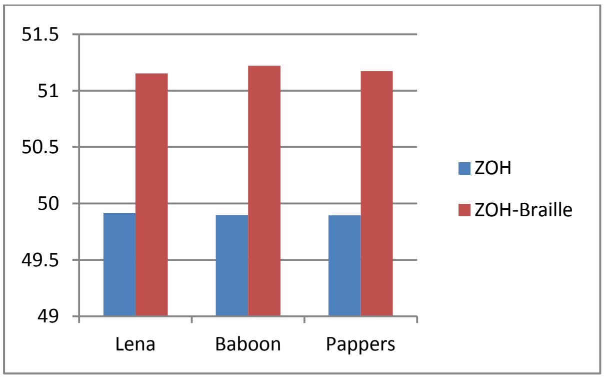

Fig 3: Chart showing comparison between PSNR values of Table4

As shown in Table (4), after hiding the same message length 8,160 bytes in the cover images (Lena, Baboon, Peppers) with size (256 x 256), using the (ZOH) and (ZOH-Braille) methods, it has been found that, the (ZOH-Braille) method has higher PSNR values than the (ZOH).

Table 5. Comparison between (ZOH) and (ZOH-Braille) Methods

Cover images (512 x 512)	Message Capacity (Bits)	PSNR	
		[9]	ZOH-Braille
Lena	4,096	42	69.2555
Lena	10,000	38.38	65.3207
Peppers	4,096	41.87	69.2598
Pappers	10,000	37.78	65.3591

As shown in Table (5), after hiding (4,096 - 10,000 - 4,096 - 10,000) secret bits in 512 x 512 cover images (Lena, Pepper) respectively, using the secure information transmission using steganography and morphological associative memory" method [9] and (ZOH-Braille) methods, it has been found that, the (ZOH-Braille) method has higher PSNR values than the (Four Neighbors) .

Table 6. Comparison between Diagonal Neighbors and (ZOH-Braille) Methods

Cover images	Message Capacity (Bits)	PSNR	
		Diagonal Neighbors	ZOH-Braille
Lena	196,968	43.9590	52.3948
Baboon	220,575	38.8280	51.9115
Peppers	197,379	43.7135	52.3954

As shown in Table (6), after hiding (196,968 - 220,575 - 197379) secret bits in 512 x 512 cover images (Lena, Baboon, Pepper) respectively, using the (Diagonal Neighbors) and (ZOH-Braille) methods, it has been found that, the (ZOH-Braille) method has higher PSNR values than the (Diagonal Neighbors).

Finally, as shown in tables (3), (4) ,(5)and (6), after the comparisons have been done among the proposed method(ZOH-Braille) and the methods; ZOH, [9] and Diagonal Neighbors methods by using different secret message and 3 different cover images (boat, bird, flinstone) .it is found that the proposed method (ZOH-Braille) has more PSNR values than other methods which means the stego image quality of the method will be higher than the quality of other LSB methods.

5. CONCLUSION

In this paper, an improvement has been made to the previously proposed image steganography method using Zero Order Hold zooming (ZOH) by combining the LSBraille image steganography method with it.

The proposed method was compared with a lot of methods as shown from table 2 to table 6; it has been found that the proposed ZOH-Braille method has more PSNR values than other methods which mean the stego image quality of the proposed method will be higher than the quality of other methods.

This means that this improvement has been succeeded to increase the maximum hiding capacity (MHC) as stated in table 3 while keeping the PSNR values higher than other methods (ZOH,[9], Diagonal Neighbors).

Finally, after checking the results, it can be said that the proposed improvement made the ZOH-Braille method more efficient than the original ZOH and other image steganography methods.

6. REFERENCES

[1] Arun Kumar Singh, Juhi Singh, Dr. Harsh Vikram Singh, "Steganography in Images Using LSB Technique "International Journal of Latest Trends in Engineering and Technology (IJLTET), Vol. 5 Issue 1 January 2015, ISSN: 2278-621X.

[2] Stuti Goel, Arun Rana, Manpreet Kaur,"A Review of Comparison Techniques of Image Steganography", IOSR

Journal of Electrical and Electronics Engineering (IOSR-JEEE) e-ISSN: 2278-1676,p-ISSN: 2320-3331, Volume 6, Issue 1 (May. - Jun. 2013), PP 41-48.

[3] Shikha S., and Sumit B., "Image Steganography: A Review", International Journal of Emerging Technology and Advanced, Vol. 3, Issue 1, January 2013.

[4] Krista B., Linguistic Steganography: Survey, Analysis, And Robustness Concerns For Hiding Information In Text, Center for Education and Research in Information Assurance and Security, Purdue University, West Lafayette, IN 47907-2086, CERIAS Tech Report 2004-13

[5] Abdelmgeid A. A., Tarek A. A., Al-Hussien S. S., Shaimaa M. H., " New Image Steganography Method using Zero Order Hold Zooming ",International Journal of Computer Applications, Vol 133 – No.9, January 2016.

[6] Abdelmgeid 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.

[7] Sara N., Amir M. E., Mohammad S. M.,"Secure Information Transmission using Steganography and Morphological Associative Memory ", International Journal of Computer Applications, Vol 61, No 7, January 2013.

[8] Moazzam H., Sadia A. H., Farhana S., " Variable Rate Steganography in Gray Scale Digital Images Using Neighborhood Pixel Information ", The International Arab Journal of Information Technology, Vol. 7, No. 1, January 2010.

[9] Sara N., Amir M. E., Mohammad S. M.,"Secure Information Transmission using Steganography and Morphological Associative Memory ", International Journal of Computer Applications, Vol 61, No 7, January 2013.

[10] Moazzam H., Sadia A. H., Farhana S., " Variable Rate Steganography in Gray Scale Digital Images Using Neighborhood Pixel Information ", The International Arab Journal of Information Technology, Vol. 7, No. 1, January 2010.

[11] Shweta M., Vishal.," An Improved Novel Steganographic Technique for RGB and YCbCr Colorspace", IJCSMC, Vol. 3, Issue. 5, May 2014, pg.377 – 381, ISSN 2320–088X.

[12] Chandra P. S., Mr. Ramneet S Ch.," A Survey of Steganography Technique, Attacks and Applications ",ijarcsse , Volume 4, Issue 2, February 2014, ISSN: 2277 128X.

[13] Deepa S., Umarani R., " A Study on Digital Image Steganography ", International Journal of Advanced Research in Computer Science and Software Engineering, Vol 3, Issue 1, January 2013.

[14] Abdelmgeid A. A., Al – Hussien S. S., " New Technique for Encoding the Secret Message to Enhance the Performance of MSLDIP Image Steganography Method (MPK Encoding) ", International Journal of Computer Applications, Vol 59, No.15, December 2012.