Journal of AL-Qadisiyah for computer science and mathematics
Vol.9 No.1 Year 2017

Page 132 - 143

Steganography: Applying LSB Algorithm to Hid Text in Image

Ali Fattah Dakhil
Department Computer Science
Gollege of Computer Science & Information Technology
University of Sumer
allee@programmer.net

Recived : 2\4\2017 **Revised : 25\4\2017** **Accepted : 27\4\2017**

Abstract

The method as well as procedure of concealing correspondences between two energy is called Steganography. In reality, steganography features a significant function and plays a substantial role in security as well as data protection. It applies a method in which making these kinds of communication is stashed by hiding data within other media. At this time there are three parts of Steganography; cover-media which holds the secrete message, additionally the secrete message and third stegano media which is the last result of combining the secrete message & hosting media. Probably the most useful algorithm that implemented here's the Least Significant Bit (LSB). Images are the objective media used here to cover a text inside it using LSB algorithm.

1. Introduction

Data as well as information is exceptionally fundamental asset to us. Along these lines, securing data turns into all of the more essential for our association. Hiding information plays big role [1] today mainly because it supplies encryption making sure that such details would be invisible. In this paper, a technique is assessed and applied utilizing hiding data from an entity media straight into another. Data exchanging among any possible assets, must be protected as well as done under high secure ecosystem in order to get rid of any tampering [1].

2. Proposal Study

As the point of reality is that there is no reliability over the medium, by which the data is transmitted, it's to express the nature of medium is not protected. Therefore, it requires methods so that is hard enough for unwanted users to debrief data. Many aspects that guided us for using hiding data:

1- Critical data.
2- Hiding criminal traces.
3- Trade secrets.
4- Avoiding data abusing.
5- Exclusive and confidential data.
6- Future study and development.
7- Preventing human error, damage of data, and an incidental deletion.
8- Pecuniary purposes.

2.1 Modern Related Work

The primary benefit of utilizing Steganography over the other popular techniques is because of its easy security mechanism since steganographic email is integrated invisibly and also covered inside some other harmless sources. Different research completed has demonstrated the point that the ways that are employed in the spatial domain are faster and simpler to apply than sandals that work within the change url and that is even more powerful in

term of opposition to attacks. In Spatial Domain, data or message being transferred is embedded directly into pictures being utilized as protection item whereas, in transform domain name as its title suggests, pictures are first transformed before the information or maybe information being transferred is lodged into it. Image steganography can be implemented using Transfer domain and Spatial domain which implements any of these three methods [2]:

- Non Filtering: This strategy deals with embedding the information into the cover item by beginning from the very first pixel of the pictures being used as protection object.

- Randomized: In this technique both sender and also receiver of the picture use password denominated stego key which is used as the seed for pseudo random number generator, which in turn produces sequence that's used as index to possess a chance to access the picture pixel.

- Filtering: In this particular technique, the algorithm cleanses the cover picture by implementing a default air filter and hides info in the places that purchase a much better rate.

2.2 A New Selected LSB Algorithm

In Selected Least Significant Bit Algorithm, both the image and the data used as cover item are converted from pixel format to binary. Probably The Least Significant Bit of a single colour (BLUE) which created a Pixel is substituted with the share of the information being transferred. This will mirror the message that has be hidden. Just the Least Significant Bit of a single colour in a Pixel is flipped through the bits of the information to hide. Only one third (1/3) of the bits on the picture can be used [two]. Hiding Data making use of Selected Least Significant Bit requires extra pixels of pictures when compared with probably the Least Significant Bits method of secret details, because just the very last colour of probably the Least Significant Bit is gon na be changed. As an outcome, the human eye can't perceive the changes - therefore this can make the information being properly hidden and inconspicuous on the human eye.

2.3 PROPOSED ALGORITHM FOR NEW SELECTED LEAST SIGNIFICANT BIT

In this particular method, a brand new steganography algorithm that's grounded on choosing probably the Least Significant Bit of the 2 colors (Blue and green) in every pixel is suggested, since pictures in a computer are represented as arrays of values. These values represent the intensities of the 3 colors R (Red), G (Green B and) (Blue), where value for every one of the 3 colours talks about a pixel. Every pixel is combination of 3 components (Red, Blue and green). In this particular system, the pieces of previous 2 elements (Blue and green) of Pixels of picture were replaced with Data Bits. The blue colour is selected due to a research performed by Hecht [three], that reveals the visible perception of extremely Blue objects is much less unique compared to the perception of items of Green and red. Green is chosen in combination with Blue because it gives more room for the length of the data to be embedded

2.4 Normal LSB and Selected LSB Comparison

In this paper we only discussed the direct way of how to apply LSB algorithm on gray image technically by software trying to make handy for readers who are looking for an easy executed code.

No big difference with the selected LSB, because we deal with only one layer (gray level), and so the SLSB use only one layer also (red or green or blue).

3 Information Hiding Characteristics

There are some features that any information concealing shall have [4]:

1- Capacity - This is donating to the quantity of data which would be hidden inside cover media. That amount of data is conducted under principle that rules for the information should not entirely modify the original media in order to prevent unintentional user alertness.
2- Robustness - This is the ability of avoiding any negative or noticeable alteration of both the hosted media as well as the actual information.
3- Security - Hiding data needs high security implemented. So, it means that only the desired user/assets could reach the embedded data which is hid inside cover media. This point is to allow other party to have credentials to extract information.
4- Perceptibility - Once a hiding method applied, it must consider some criteria by which hidden information perceptually is ambiguous and mysterious.

4. Used Tool for Implementation

MATLAB application is utilized by millions of scientific researchers and engineers for design, evaluation and system controlling all across the word. As MATLAM is a matrix primarily based language, thus, it's commonly considered as the world's many nature connate technique to do mathematics operation and a lot of computational theories as well as exercises. MATALB is additionally provided with a built in graphics software program and mechanism to put in visualization as well as image processing. Consequently, MATLAB was used by us to achieve the mission of ours for implementing LSB algorithm [5].

5. Understanding Steganography

Steganography used to transport data from one place to other place through open divert in undercover way. Steganography shrouds the very presence of a message so that if fruitful it by and large draws in no doubt by any means. Steganography implies concealing a mystery message inside a bigger one (source cover) such that an onlooker cannot identify the nearness of substance of the shrouded message. Various bearer file formats can be utilized, yet computerized pictures are the most well known in view of their recurrence on the Internet. For concealing mystery data in pictures, there are exists a substantial assortment of Steganography systems some are more perplexing than others and every one of them have particular solid and frail focuses [6].

6. Information Security Techniques

Remembering the ultimate objective to achieve the information security objective there are number of procedures which are used for information security. The **Cryptography** is one of the methods which are used to ensure information or data in against any uncover to the data. Honestly, cryptography is the workmanship and craft of protecting information from undesirable individuals by changing over it into a shape non-prominent by its aggressors while set away and transmitted. Data cryptography on a very basic level is the scrambling of the substance of data, for instance, content, picture, sound, video and so forth to make the data stirred up, imperceptible or unfathomable in the midst of transmission or limit called Encryption. The crucial goal of cryptography is keeping data secure from unapproved aggressors. The modify system for data encryption is called data decryption.

Second, **Hiding information**, the term of cover information is the path toward covering the release message or information sight and sound records to guarantee there is no other social affair can disclose or evolving it. Under this point we can drive two frameworks which are used to cover information one is progressed watermarking is the route toward embedding information into an electronic movement in a way that is difficult to clear, the banner may be sound, pictures, video or substance records; its for the most part used for demonstrate the authorized advancement rights reason, for instance, including copy right logo or substance (maker signature) for sight and sound reports.

Likewise, **Steganography**, the third procedure is the workmanship and investigation of composing shrouded messages such that nobody, aside from the sender and proposed beneficiary, associates the presence with the message. Since, the principle use for steganography is to send secure messages between gatherings, then it is mean to keep the message being recognized by some other gathering [7].

7. Types of Steganography

Although the formats those're with a lot of redundancy would be far more appropriate, steganography is usually utilized for those computerized file formats. Redundancy is usually characterized as the pieces of an object which offer precision far more visible than would usually be suitable for the object 's

show and utilization. The unneeded bits of an item are those bits that may be modified without the shift being distinguished effectively. Sound files and picture particularly consent to this particular demand, while inquire about has also revealed additional documents which could be used for information stowing away. You will find 4 classifications of documents which may be used for Steganography came out in fig. one. Because, photos are mainstream cover or maybe transporter objects used for Steganography. In the area of skilled photos distinct photo documents are existed; the vast majority are accessible for particular purposes [8].

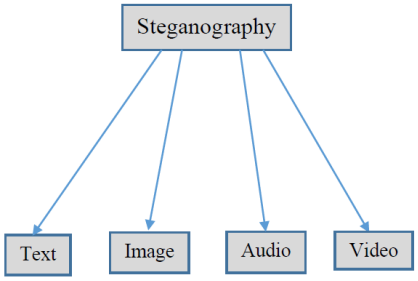

Fig 1 Types of Steganography

1. Text Steganography
2. Audio Steganography
3. Video Steganography
4. Image Steganography

8. Image Steganography Algorithms

While steganography can be achieved utilizing some covering media, we're worried with concealing info in computerized images. The elements expected of a stego medium are heartiness and indistinctness, to ensure that the unknown message is known simply on the planned beneficiary and moreover the stego medium having the capability to resist assaults from interlopers. The way of measuring mystery message implanted must be with the objective it doesn't decrease the dynamics of the stego picture.

This theme moves for concentrate the distinct procedures used in steganography for implanting info. The goal of steganography is usually to implant mystery info right into a protective cover so that no one separated from the sender and also planned beneficiaries even admit there's mystery info [nine]. There are several algorithms readily available to apply on image:

A. Discrete Cosine Transform (DCT)
B. Discrete Wavelet Transform (DWT)
C. Spread Spectrum
D. Hash-Least significant Bits (Hash-LSB)
E. Least Significant Bit Substitution Technique

9. LSB Algorithm

In LSB steganography, the least significant bits of the covering media 's digital info are used to conceal the message. The least hard of the LSB steganography methods is LSB substitution. LSB substitution steganography flips the final slice of every one of the info qualities to mirror the idea that must be covered up [10].

Consider a 8 bit grayscale bitmap image where every pixel is stored as being a byte speaking to a dim scope an incentive as been seen in fig two. Believe the initial 8 pixels of the first picture like following info.

10010110
01010111
00100110
11010001
11000110
11010111
01000110
10010101

To conceal the letter W for instance, whose binary information is 01110111, we have to modify the final bits at the very first to have the following information:

10010111
01010110
00100111
11010000
11000111
11010110
01000111
10010100

Therefore, we can see

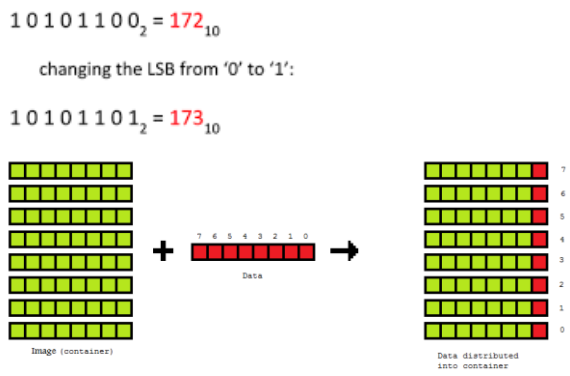

Figure 2 LSB algorithm Technique

10. Pixels and Bitmaps Images

Computerized pictures are made from pixels (short for image components). Every pixel speaks on the shading (or maybe dim level for increased contrast photographs) with a solitary thing in the picture, therefore a pixel looks like a tiny dab associated with a certain shading [11]. By calculating the shade of an image at huge, we are able to generate a computerized estimation of the photograph from which another of the 1st could be reproduced. Pixels are like grain particles in a regular photographic picture, yet masterminded in a regular illustration of columns and rows and store information to some degree in a surprise way.

10.1 Binary Images

A binary image is an image in which every pixel accepts one of just two discrete qualities. Basically, these two qualities compare to on and off as in fig 3.

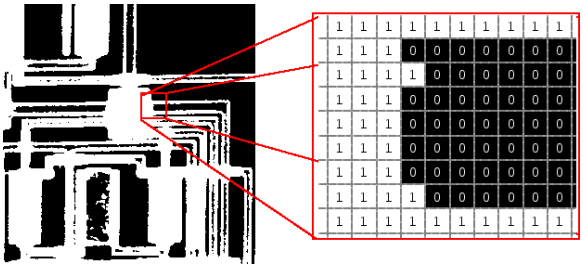

Fig 3 Binary Image Bits Data

10.2 Gray Image

A gray (or dark level) photo is essentially 1 where the primary tones are shades of dim. The goal behind separating such photographs from any other type of shading photo would be that much less details must be accommodated each pixel. Honestly a "dark" shading is 1 where the white, blue and green areas each have risen to run in RGB area, so it's simply crucial that you establish a solitary force an incentive for each pixel, rather than the 3 powers likely to show each pixel inside a total shading picture. Like in fig four, gray pictures are exceptionally natural, to some degree because a great deal of modern show and photo catch equipment can easily merely bolster 8 bit pictures. Also, gray pictures are totally sufficient for a few errands hence there's no compelling reason to use harder-to-process and convoluted more shading pictures.

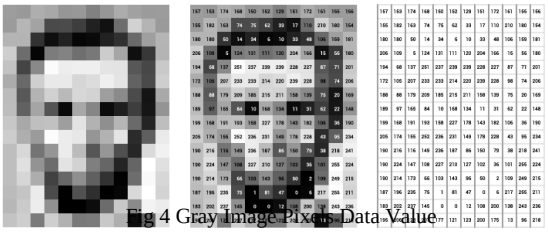

Fig 4 Gray Image Pixels Data Value

11. Implementing LSB Algorithm

After talking about couple of theories about protection, steganography and image processing solutions, so as it's typically known that this particular subject concentrates on applying and actually use such software. Consequently, we will use the prior strategies which are being mentioned in prior things. This subject is to legitimate exercise for our LSB algorithm and also the right way to undertake it in authentic with Matlab. Generally, the Matlab application is our preferred technology/language by which LSB algorithm is applied by us, so that, we are able to show such capabilities.

11.1 Implementing LSB Algorithm by Matlab

It is time to code and put hand experience on our LSB algorithm. Now, we include the code that apply LSB algorithm.

```
clc
clear
j=imread('rosegrey.jpg')
[r c] = size(j)
imageBIN = dec2bin(j,8)
[rbin cbin] = size (imageBIN);
text='hi'
ascm=double(text)
binasc=dec2bin(ascm,8)
[rtbin ctbin] = size (binasc)
 for i=1:1:rtbin*ctbin
   imageBIN(i,8) =binasc(i);
 end
imagewithtext=uint8(reshape(bin2dec(imageBIN),r,c));
subplot(1,2,1)
imshow(j)
subplot(1,2,2)
imshow(imagewithtext);
camp = colormap('gray');
p=ind2gray(imagewithtext, camp);
imwrite(p ,'imhitxt.png','png');
```

As displayed in the code above, you can find couples of lines have to be defined as numbered:

1- This is clearing up the work area window and structure just for the brand new results.
2- This is clearing out the possible values in the mind from last use.
3- This command is reading and publish a picture file into a handler known as J. The picture rosegey.jpg' is a grey structure. We may use a colored picture, nonetheless, we have to change it for grey structure via this performance ---> rgb2gray(rosegey.jpg');
4- Here we look at the size and learn the number of Columns and Rows on the J image.
5- Now, we produce a binary image data since it was known as imageBIN, from the performance dec2bin(j,8). This feature makes use of the J picture (with decimal data) and also use eight bits format. In reality, the real image as following:

```
j =

   68   61   63   91
   53   45   50   87
   54   43   46   83
   61   50   50   83
```

Whereas this image data was transformed into binary format as below:

```
imageBIN =

01000100
00110101
00110110
00111101
00111101
00101101
00101011
00110010
00111111
00110010
00101110
00110010
01011011
01010111
01010011
01010011
```

6- This is to identify the size of the binary image imageBIN by its Rows (rbin) and Columns (cbin).

```
rbin =

    16
```

7- Set the text which will be hidden inside the image.

```
cbin =

     8
```

8- Getting the equivalence ASCII number for each letter in the text, as h=104 and i= 105.

```
text =

hi


ascm =

   104   105
```

9- Find the binary format for the new matrix which we got from the previous step in 8 bits. We can notice that h = 104 = 01101000 and i = 105 = 01101001.

```
binasc =

01101000
01101001
```

10- Determine the Rows and Columns for the new binary image.

```
rtbin =

     2


ctbin =

     8
```

11- Now, we begin to use the particular LSB algorithm method along with its approach. Up to now, we've the binary structure for the initial image (host) as well as the binary format of the book letters. A loop operator has been done by us, so that, we implement the LSB algorithm for every preferred bit. Thus, the iteration was repaired for one --> (rtbin*ctbin) that is sixteen in the example of ours, as we have to preserve sixteen bits of the 2 letters (eight for each)Here, we replace the content of binacs matrix (binary format of text) with the last bit of each row in imageBIN (binary format of the image).

12- That is the end of the loop. Bellow in fig 5, explanation about the LSB mechanism.

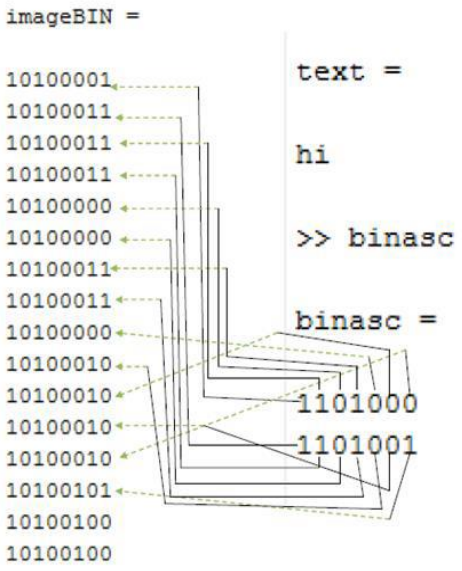

Fig 5 LSB Algorithm Mechanism

14- This command is to create the host image with the hidden text, we used bin2dec(imageBIN) to transform binary format back to decimal. As such, we apply reshaping technique by reshape(bin2dec(imageBIN),r,c) regarding to r and c dimensions. Then we used uint8(reshape(bin2dec(imageBIN),r,c)) in order to set the capabilities of 8- bits format. After that we go the image **imagewithtext** with its value as shown below with little differences.

```
imagewithtext =

   68   61   63   90
   52   45   51   86
   55   42   46   82
   61   50   50   83
```

Now it is clear to notice the few differences in matrix (image) values as comparing with original one:

```
j =                              imagewithtext =

    68    61    63    91            68    61    63    90
    53    45    50    87            52    45    51    86
    54    43    46    83            55    42    46    82
    61    50    50    83            61    50    50    83
```

15- Preparing a displaying window to indicate the 2 images as in fig 6.

16- This is to show the first image on the previous window.

17- Set the other window location over the display window.

18- This is showing the host image.

19- This command is to set and figure out the style map and colors routes for a picture, therefore, in our example, we used gray color format.

20- This line is to tell this picture will be in the gray scale color.

21- Now, it's quite essential step to apply the LSB algorithm. We used a command here imwrite to save/create the new image with its new values along with specifying its extension and name as found it was.png file.

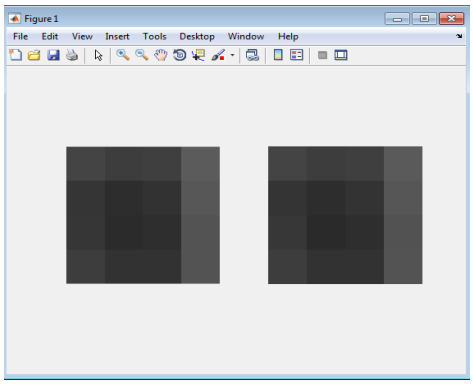

Fig 6 Gray Image Before and After Steganography

11.2 Retrieving Text from Host Image

This portion is the second primary job in steganography mission. We might claim that steganography is meaningless unless we're able to retrieve the secret information. There are several essential issues that we need to understand about the host picture as following:

- How many Columns and rows of the concealed text.
- Where we began preserving the text 's bits in image 's bits.

Today, we've the code to access back the hidden copy from the host picture as shown below:

```
1  imagewithtext=imread('imhitxt.png')
2  imgbin=dec2bin(imagewithtext,8)
3  textbin=imgbin(1:16,8)'
4  shapetextbin = reshape(textbin ,2,8)
5  ascimessage=bin2dec(shapetextbin)
6  message = char(ascimessage)
```

1- This command is to read the host image and save into **imagewithtext**. We can see that this host image is exactly same the saved one as it is.

```
imagewithtext =

    68    61    63    90
    52    45    51    86
    55    42    46    82
    61    50    50    83
```

2- This is to transform the decimal format of image to binary as 8-bits capability.

```
imgbin =

01000100
00110100
00110111
00111101
00111101
00101101
00101010
00110010
00111111
00110011
00101110
00110010
01011010
01010110
01010010
01010011
```

3- This step is quite important to collect and select the LSB bit. Look, we use a technique to read the last bit (8 as stated) when an iteration starts from 1 -- > 16 (2 * 8 referring to Rows and Columns respectively).

```
textbin =

0011110011000001
```

4- Here we apply reshaping on the previous matrix **textbin** which has 1 row and 16 columns. After this, we got this result:

```
shapetextbin =

01101000
01101001
```

5- This step is to find the decimal values of the matrix **shapetextbin** from the binary format. We can see the result that 01101000 = 104 and 01101001 = 105

```
ascimessage =

   104
   105
```

6- Here we get the actual character letter from the **ascimessage** matrix.

```
message =

hi
```

12. Performance evaluation factors

To begin with, this particular technique (steganography) doesn't rely on the kind of documents, almost as it depends on real details (bits format) that extracted from that such file (cover media) whatever is was picture, sound, video as well as text. Having segmentation analysis assessment is a prosperous strategy to dissect the functionality of existing algorithms [twelve]. Before one gets more acquainted with the functionality of an algorithm, realizing exhaustively the meanings of these matrices are inescapable. Different performance parameters used for evaluation of picture segmentation are as per the following. Nevertheless, most of them Don't Affect LSB algorithm at many, so we might state these variables have 0 overall performance effecting on LSB algorithm.

12.1 The Rand index (RI)

The Rand index or Rand measure is a measure of the similarity between two data clusters.

12.2 Variation of Information (VOI)

This metric describes the separation between 2 segmentations as the regular restrictive entropy of just one segmentation provided the other, and thus measures the way of measuring haphazardness in a single segmentation which cannot be clarified by the additional.

12.3 Global Consistency Error (GCE)

This measures the degree to which one segmentation can be seen as a refinement of the other.

12.4 Boundary Displacement Error (BDE)

This measures the standard dislodging error of just one limit pixels and also the closest limit pixels in another segmentation [12]. Particularly, it characterizes the error of just one limit pixel as the individual between the pixel as well as the nearest pixel in another limit image.

12.5 Mean absolute error (MAE)

Mean absolute mistake will be the average on the big difference between predicted and legitimate benefit in all of test cases; it's the typical prediction error.

12.6 Peak signal to noise ratio (PSNR)

It measures between the most extreme conceivable power of a signal and the effect of adulterating noise that influences the constancy of image representations.

13. Effecting of Performance

Now, let us have an inspection at those things as well as time complexity metrics on our algorithm (LSB). Set of tables show the overall performance effecting of the algorithm of ours after applying it over particular segments as has been tested all over the preceding factors.

The Rand index (RI)	Time Excu. At sender Per sec.	Time Excu. At Receiver Per sec.
0.512	0.420	0.412
0.831	0.399	0.432
0.668	0.435	0.362
0.512	0.420	0.392
0.831	0.389	0.422

Table 1 Apply LSB on two segments with RI calculated

Variation of Information (VOI)	Time Excu. At sender per sec.	Time Excu. At Receiver Per sec.
0.737	0.230	0.249
2.689	0.244	0.234
0.942	0.275	0.220
1.410	0.218	0.190
0.884	0.253	0.261

Table 2 Apply LSB on two segments with VOI calculated

Global Consistency Error (GCE)	Time Excu. At sender per sec.	Time Excu. At Receiver Per sec.
0.814	0.333	0.413
0.031	0.360	0.384
0.085	0.298	0.410
0.883	0.340	0.385
0.850	0.317	0.402

Table 3 Apply LSB on two segments with GCE calculated

Boundary Displacement Error (BDE)	Time Excu. At sender per sec.	Time Excu. At Receiver Per sec.
5.369	0.673	0.711
3.896	0.712	0.646
4.358	0.636	0.672
3.265	0.646	0.737
5.783	0.673	0.647

Table 4 Apply LSB on two segments with BDE calculated

Mean absolute error (MAE)	Time Excu. At sender per sec.	Time Excu. At Receiver Per sec.
2.369	0.424	0.328
3.896	0.339	0.281
4.358	0.504	0.356
2.265	0.421	0.266
3.783	0.443	0.232

Table 5 Apply LSB on two segments with MAE calculated

Peak signal to noise ratio (PSNR)	Time Excu. At sender per sec.	Time Excu. At Receiver Per sec.
36.459	0.520	0.499
39.079	0.418	0.478
42.763	0.591	0.517
34.272	0.544	0.496
38.746	0.509	0.507

Table 6 Apply LSB on two segments with PSNR calculated

14. LSB is an Independent Algorithm

After proofing that it is algorithm has no effect under any circumstances regards the table 1. The reason behind this is the fact of LSB algorithm applies on how to replace the last bit of image's bytes. Thus, it has to say, that this algorithm depends on the length of text (needed to be hidden).

Let us clarify this point, LSB needs only to have binary data from image, disregard of all other characteristics of that image, as we mentioned above such as size, quality, performance factors and particular block/segment. Three main aspects that LSB approach relies on:

A. Binary format of text.
B. Binary format of image.
C. Replacing bits of text 's letter with last ones of image bytes.

Therefore, LSB mechanism applies on the best way to distributing text 's bit over image at the sender aspect and just how get them also at the receiver facet.

15. Conclusion and Recommendations

As it's been reviewed and demonstrated over this analysis, we've attempted to present an audit of current info concealing procedures, their advantageous circumstances and burdens. This paper also explained why info stowing away is getting significance today and the goals which should be achieved of any info concealing procedure. Furthermore, we've attempted to state exactly how the important goals of info covering up can be achieved LSB algorithm of information hiding. Additionally, we tried to use LSB algorithm the truth is by MATLAB software. Lastly, we determine and also suggest this investigation will be very convenient to utilize within mobile applications chatting like Viber or WhatsApp to secure higher communications by sending and also receiving innocent photo and images which in reality they will have hidden secret texts.

16. Refrences

[1] C. Yang, C. C and Lin. Chang, Steganography and also watermarking, 1st ed. Hauppauge, New York: Nova Science Publishers, Inc., 2013.

[2] Juan J. and Jesus M. (2009). SLSB: Improving the Steganographic Algorithm LSB. Universidad Nacional de Educación a Distancia (Spain).

[3] Hecht, E. 2006. Optics. Delhi, India: Pearson Education

[4] K. UdhamSingh, "A Survey on Image Steganography Techniques", International Journal of Computer Applications, pp. 10-20, no. 18, vol. 97, 2014.

[5] "MATLAB - Mathworks". Mathworks.com. N.p., 2016. Web. seventeen Apr. 2016.

[6] Fridrich, Steganography in Digital Media, 1st ed. Cambridge: Cambridge Faculty Press, 2009.

[7] P. Wayner, Disappearing cryptography, 1st ed. Amsterdam: Morgan Kaufmann Publishers, 2009.

[8] Mangesh Ghonge, Ankita Dhawale, Atul Tonge, Review of Steganography Techniques, International Journal of Advent Research in Electronics and Computer, No.1, Vol. 1, March 2014

[9] M. Stocchetti, Power and "images in the Digital Age: The political part of electronic visuality", pp. 3-6, no. 2, vol. 2, KOME, 2014

[10] Vijay KumarSharma, Vishalshrivastava, "A Steganography Algorithm for Hiding Images by enhanced LSB substitution by minizedetection."journal of Theoretical and also ISSN: 1992-8645, Vol. 36 No.1, Applied Information Technology, 15th February 2012.

[11] Gonzalez, Rafael C, plus Richard E Woods. Digital Image Processing. Upper Saddle River, N.J.: Prentice Hall, 2008. Print documents.

[12] A. Kicherer, R. Roscher, K. Herzog, W. Förstner and R. Töpfer, "IMAGE BASED Evaluation For the DETECTION OF Cluster Parameters In GRAPEVINE", Acta

Journal of AL-Qadisiyah for computer science and mathematics Vol.11 No.1 Year 2019
ISSN (Print): 2074 – 0204 ISSN (Online): 2521 – 3504

أخفاء المعلومات : تطبيق لخوارزمية الـ LSB لإخفاء نص داخل صورة

علـــي فتـــاح داخـــل
جامعة سومر
كلية علوم الحاسوب و تكنولوجيا المعلومات
قسم علوم الحاسوب
allee@programmer.net

المستخلص :

تعد طريقة أخفاء المعلومات او ما يسمى steganography آلية لآخفاء التراسلات بين طرفين. و مما لا شك فيه ان نطاق عمل اخفاء المعلومات له دور هام و اساسي في مجال امن البيانات. تعمل آلية اخفاء البيانات على تضمين البيانات من اي وسط كانت بداخل وسط آخر بحيث لا يمكن معرفة ذلك من قبل المخترقين. يرتكز مفهوم التضمين على ثلاث مكونات: المحتوى المراد تضمينه او اخفائه، و كذلك الوسط المستضيف او الحامل للبيانات، و ثالثا النتيجة النهائية المكونة من البيانات المخفية و الوسط الحامل لها. في هذا البحث و الدراسة قمنا بتطبيق خوارزمية الـ LSB و التطرق الى تفاصيل عملها و آلية تنفيذها عمليا. كما ان الوسط الذي عملنا به هنا هو الصور باعتباره الوسيط الحامل للبيانات و هذه البيانات عبارة عن نص نريد اخفائه داخل الصورة.