ISSN 2286-4822
www.euacademic.org

EUROPEAN ACADEMIC RESEARCH
Vol. III, Issue 2/ May 2015

Impact Factor: 3.4546 (UIF)
DRJI Value: 5.9 (B+)

A Novel Approach for Hiding Huge Data in Image

ZAINALABIDEEN ABDUAL SAMAD RASHEED
ZAINA HUSSAN KADIM
SAMI KADHEM ALTHABHAWI
Education College
Kufa University, Najaf, Iraq

Abstract:

Steganography is an important area of research in recent years involving a number of applications. It is the science of embedding information into the cover images viz. text, video, and images. Various Steganography methods have been applied in terms of robustness, Imperceptibility (stego-image), and capacity. However, most of hiding image in image focus on capacity and Imperceptibility (image quality) and most of them need cover image to be 8 times bigger than secret image, for that reason this project focus on apply new techniques to reduce the size of cover image requiring by insert 4 bits in each pixel instead of one with mention to image quality. The quality of cover image is considered high due to the inserting process by add the message or inverse of message. Moreover, selecting a suitable pixel within the same block case less change to the cover image and keep quality of cover image too.

Key words: Least significant bit (LSB), Digital image Steganography, capacity, image quality.

1- Introduction

In terms of security data there are two general systems which be used for most people; cryptography and Steganography. The main purpose of Steganography, which means ‘writing in hiding' is to hide data in a cover digital media so that others will not be able to notice it (Figure 1). However, cryptography is about protecting the content of messages; Steganography is about concealing their very existence. The applications of information hiding systems mainly range over a broad area from military, intelligence agencies, online elections, internet banking, medical-imaging and so on. These variety of applications make Steganography a highly interest topic for study. Different carrier file formats can be used to be a cover medium. Moreover, the cover is usually Chosen to keeping in mind the type and the size of the secret message. Recently, digital images are the most popular carrier/cover files that can be used to transmit secret information. Steganography can be achieved using different digital cover media .while this paper concerning to apply steganography in digital image.

The features expected of a stego-medium are imperceptibility and robustness, so that the secret message is known only to the intended receiver and also the stego-medium being able to with stand attacks from intruders. The capacity of secret message embedded should be such that it doesn't less the quality of the stego image. The main idea of steganography is to embed secret data into a cover in such a way that no one expected the intended recipient can collect the secret message or even changed. However, the steganography is based on many factors like Imperceptibility, robustness and capacity;

1. Imperceptibility: Imperceptibility is the property in which a person should be unable to distinguish the original and the stego-image.
2. Embedding Capacity: Refers to the amount of secret information that can be embedded without degradation of the quality of the image.
3. Robustness: Refers to the degree of difficulty required to destroy embedded information without destroying the cover image.

Lately, steganography has come to be commonly used in the improvement of information security. Digital media can be used to hide secret information such as image, video, audio, text etc.

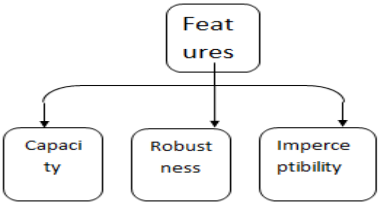


Figure -1: Information-hiding system features.

2- Steganography Techniques

2.1 Classification of Steganography Categories

Steganography is classified into 3 categories,

- Pure steganography where there is no stego key. It is based on the assumption that no other party is aware of the communication.
- Secret key steganography where the stego key is exchanged prior to communication.This is most susceptible to interception.
- Public key steganography where a public key and a private key is used for secure communication **[1]**

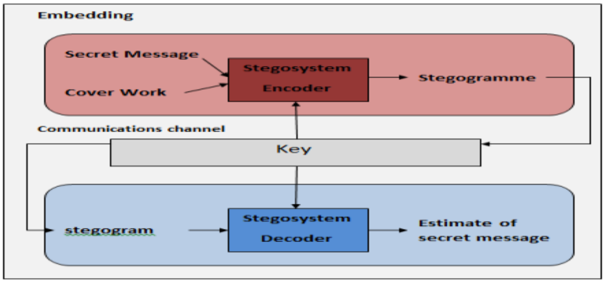


Figure 2. Steganography process [2]

2.2 Uses of Steganography

1. Steganography can be a solution which makes it possible to send news and information without being censored and without the fear of the messages being intercepted and traced back to us.

2. It is also possible to simply use Steganography to store information on a location. For example, several information sources like our private banking information, some military secrets, can be stored in a cover source. When we are required to unhide the secret information in our cover source, we can easily reveal our banking data and it will be impossible to prove the existence of the military secrets inside.

3. Steganography can also be used to implement watermarking. Although the concept of watermarking is not necessarily Steganography, there are several stenographic techniques that are being used to store watermarks in data. The main difference is on intent, while the purpose of Steganography is hiding information, watermarking is merely extending the cover source with extra information. Since people will not accept noticeable changes in images, audio or video files because of a watermark, stenographic methods can be used to hide this.

4. E-commerce allows for an interesting use of Steganography. In current e-commerce transactions, most users are protected by a username and password, with no real method of verifying that the user is the actual card holder. Biometric finger print scanning, combined with unique session IDs embedded into the fingerprint images via Steganography, allow for a very secure option to open ecommerce transaction verification.

5. Paired with existing communication methods, Steganography can be used to carry out hidden exchanges. Governments are interested in two types of hidden communications: those that support national security and those that do not. Digital Steganography provides vast potential for both types.

Businesses may have similar concerns regarding trade secrets or new product information.

6. The transportation of sensitive data is another key use of Steganography. A potential problem with cryptography is that eavesdroppers know they have an encrypted message when they see one. Steganography allows to transport of sensitive data past eavesdroppers without them knowing any sensitive data has passed them. The idea of using Steganography in data transportation can be applied to just about any data transportation method, from E-Mail to images on Internet websites**. [3]**

2.3 Steganography techniques:

Steganography can be applied in both S.D and F.D, in this paper our force on S.D, especially in capacity and quality of stego- image. The comparative will be between our proposal and LSB method.

1- Abdelfatah A. Tamimi, Ayman M.[4] use an algorithm that use variable number of LSBs from each pixel of the cover image for hiding .The number of bits chosen from each pixel colour (red, green, and blue) is different. The actual number of bits changes according to neighbourhood information of each pixel colour. When the resemblance between the neighbours of a pixel colour entry is low, the pixel entry is located in a non-smooth area where change will not be detected easily. Therefore, the number of bits used for hiding is chosen to be proportional to the neighbours' XOR value for each pixel colour entry. The XOR is computed for the value of each one of these pixels' four neighbours: left, right, above, and below. This comparison measures the smoothness of the pixel's neighbourhood so that the number of hiding bits can be determined**.**

2- In LSB replacement technique, the bit of binary top-secret memo is used to over mark the LSB of the protection image pixel. I.e. firstly, the secret message is transformed to binary bit watercourse. Secondly, the cover pixel value is converted to binary stream bit also. Finally, LSB of cover pixel is substituted by bit of secret message. As shown in Figure 1 the first three pixels value of cover image converted to binary bits and secret message convert to bits too. The first bit from secret message replace with LSB of first cover pixel ,second bit from secret message replace with LSB of second pixel and The third bit from secret message replace with LSB of third pixel[5][6]

3- Shilpa Gupta et al proposed a system that try to reduce the distortion in Least Significant Bit because it make a more distortion when the information hidden in the LSB of the three colour components in the pixel of the colour cover image by proposing Enhanced LSB algorithm that works in the spatial domain that suppose message to be hidden in Blue component only of the colour cover image.[7]

4- The conventional LSB method limits the size of the secret data to eighth of the size of the cover. LSB steganography least n-bits for increasing the capacity of the secret information n/8 the size of the Cover image. The writer increase n and that will distorts stego-image, where in each run, random data are embedded in the n least significant bits, where 1≤n≤7. [8]

5- The author supposes that the cover image of 24 bit colour image and two methods are described in that proposal. In first method, last 2 LSB of each plane (red, green and blue) of cover image is replaced by 2 MSB of secret image. In the second method, last LSB of each red plane is replaced by first MSB of secret image, last 2 LSB of each green plane by next 2 MSB of secret image and then last 3 LSB of blue plane is replaced by next 3

MSB of secret image. That means the total 6 bits of secret image can be hide in 24 bit colour image. [9]

2.4 Proposed system

Our proposed system can hide a secret image that have critical information in a cover image and to hide a secrete image with large size.

The secrete image firstly arranged as a vector and then divided to sub vectors of length 64 bits and divide the cover image as 4x4 sub image and then the 64 bits as 16 blocks will be accommodate in the sub image in a special way in the 4 LSB. Each block will compare with the best pixels of the 16 pixels in the sub image. The best pixel represents the least value of deference between the pixel of cover image and block in secret message. The comparison will be for every pixel and the deciding the least value to hide in it. The best pixel will be the minimum value of these 16 pixels, and then the second block will compared as above with 15 reminder pixels and soon. The second step after choosing the best pixel is to decide what to choose to hide in the pixel either the block or the inverse of the block according to smallest difference of them with the pixel .And finally after the 16 blocks hide in the 4x4 sub image. The first key of the using of the block or the inverse of it will be hide in the best pixel of the reminder pixels. The second key represents the map of the selection of pixels in the cover image and this key give the robustness of the algorithm. About the capacity in our algorithm the 64 bits will hide in 16 pixels that mean capacity of hiding

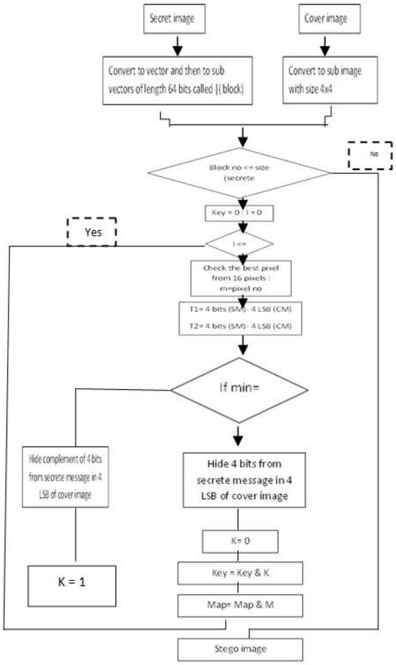
Algorithm

1- Convert the secrete image to vector.
2- Divide the vector to sub vectors of length 16 bits.
3- Each 4 bits in the sub vector called block
4- Take the sub image from cover image with size 4x4
5- Map= 0

```
6-  While ( size(secret message) not terminate)
    Key= 0
    For i=1 to 16
    If i < = 16 then S= Block from secret message
            For j= 1 to 16
                    If p[j] not used then  p[j] = C[j] – S[i]

    next

    Best1 = Minimum (P vector): M= j
    Delete (Best1) from choices list (C vector)
    Best2= Minimum (Best1 – S, Best1 – complement(S) )
    If Best2 = Best1 – S then
            K=0
            Chang the 4 LSB of cover image with the block
    (S)

            Else
            K=1
          Chang the 4 LSB of cover image with the block
          complement (S)

    End if

    Key = Key & K
    Map = Map & M
    Next While
 7-End
```

P[i]	is the value of difference between the 4 LSB of pixel in cover image with 4 bits from Secret message
Key	represent the way used to hide 4 bits from secrete image or the complement of the 4 bits
Map	represent the path used to hide the secret image (the sequence of pixels used)
Best1	the selected pixel
Best2	the selected way of secrete or complement of it

Table 1: Abbreviate of Steganography Algorithm


Secret image
Cover image
Convert to vector and then to sub vectors of length 64 bits called |(block)
Convert to sub image with size 4x4
Block no <= size (secrete
No
Key = 0 : I = 0
Yes
I <=
Check the best pixel from 16 pixels : m=pixel no
T1= 4 bits (SM)- 4 LSB (CM)
T2= 4 bits (SM)- 4 LSB (CM)
If min=
Hide complement of 4 bits from secrete message in 4 LSB of cover image
Hide 4 bits from secrete message in 4 LSB of cover image
K= 0
K = 1
Key = Key & K
Map= Map & M
Stego image

Flowchart of steganography algorithm

3. Test

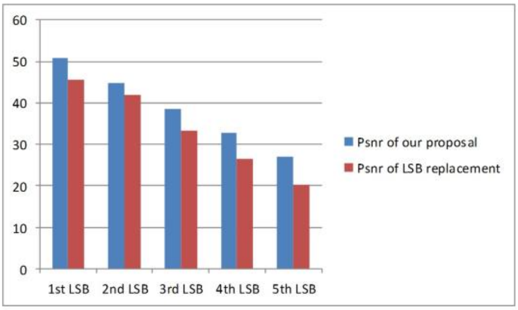


Figure 3: PSNR of two methods (LSB and our proposal methods)

Testing have been done on mat lap 2010, pc core i3,for each time have been inserted 4 bits together into the pixel of cover image starting from (1^{st},2^{nd},3^{rd},4^{th} ^{LSB} then 2^{nd},3^{rd},4^{th},5^{th} ^{LSB} then 3^{rd},4^{th},5^{th},6^{th} ^{LSB} then 4^{th},5^{th},6^{th},7^{th} ^{LSB} finally 5^{th},6^{th} ,7^{th} ,8^{th} ^{LSB}).And it is clear from figure 3: our proposal give us better quality of stego image for each segments due to our inserting process.

4. Conclusion

LSB replacement can be applied in each block with inserting only 16 bits (one bits per pixel with LSB i.e. less change to cover image). However, our proposal 64 bits in 16 pixels together with less change to cover image due to our method by searching the best pixel for inserting and compare which is better the message or the inverse of message.

Within 16 pixels for each block, each pixel will hide 4 bits and 16 segments of secret message each segments has 4 bits, the probability to find the best pixel is too high due to binary system within 4 bits will give us $2^4 = 16$ different probability

Because our project has just 16 segments for each block therefore is highly to find the best position for inserting process.

The comparative, if we have 512* 512 images, each pixel 8 bits we shall need cover at least 8* 512 * 512 = 2,097, 152. While, our proposal =2,097*152/4 = 524,288 and with less change to cover image i.e better quality of stego- image.

REFERENCES

[1] "A Study of Various Steganography Techniques Used for Information Hiding", C.P.Sumathi, T.Santanam and G. Umamaheswari, International Journal of Computer Science & Engineering Survey (IJCSES) Vol.4, No.6, December 2013

[2] A Study on Digital Image Steganography, Deepa S Umarani R, Volume 3, Issue 1, January 2013 ISSN: 2277 128X

[3] "Steganography- A Data Hiding Technique", Arvind Kumar Km. Pooja, Volume 9– No.7, November 2010

[4] “Hiding an Image inside another Image using Variable-Rate Steganography”, Abdelfatah A. Tamimi, Ayman M. Abdalla, Omaima Al-Allaf, (IJACSA) International *Journal of Advanced* Computer Science and Applications, Vol. 4, No. 10, 2013.

[5] Zainalabideen Abdual Samad Rasheed ”Steganography Technique for Binary Text Image” International Journal of Science and Research (IJSR) ISSN (Online): 2319-7064,2015

[6] Zainalabideen Abdual Samad Rasheed, Improving Classical Fibonacci in Steganography, International Journal of Advanced Research in Computer Science and Software Engineering(ijarcsse) ISSN: 2277 128X, 2014

[7] Shilpa Gupta, Geeta Gujral and Neha Aggarwal, “Enhanced Least Significant Bit algorithm For Image Steganography”, IJCEM International Journal of Computational Engineering & Management, Vol. 15 Issue 4, July 2012

[8] Himanshu Gupta, Prof. Ritesh Kumar, Dr. Soni Changlani “Enhanced Data Hiding Capacity Using LSB-Based Image Steganography Method “, International Journal of Emerging Technology and Advanced Engineering , (ISSN 2250-2459, ISO 9001:2008 Certified Journal, Volume 3, Issue 6, June 2013)

[9] Deepesh Rawat, Vijaya Bhandari, “ A Steganography Technique for Hiding Image in an Image using LSB Method for 24 Bit Color Image”, International Journal of Computer Applications (0975 – 8887) Volume 64– No.20, February 2013