



IMAGE STEGANOGRAPHY USING LEAST SIGNIFICANT BIT ALGORITHM

Vedansh Sharma¹, Deepak Singh²

^{1,2}Student, Department of Information Technology,
IMSEC, Ghaziabad, Uttar Pradesh, India

Abstract: To increase the safety of messages sent over the web steganography is employed. This paper discussed a technique supported the LSB (least important bit) and a brand new cryptography algorithmic rule. By matching data to the image, there is less chance of associate degree attacker having the ability to use steganalysis to recover information. Before hiding the information in a picture the application first encrypts it.

Keywords: Steganography, LSB (least significant bit), Encryption, Decryption, Information hiding, Stega Image.

1. Introduction

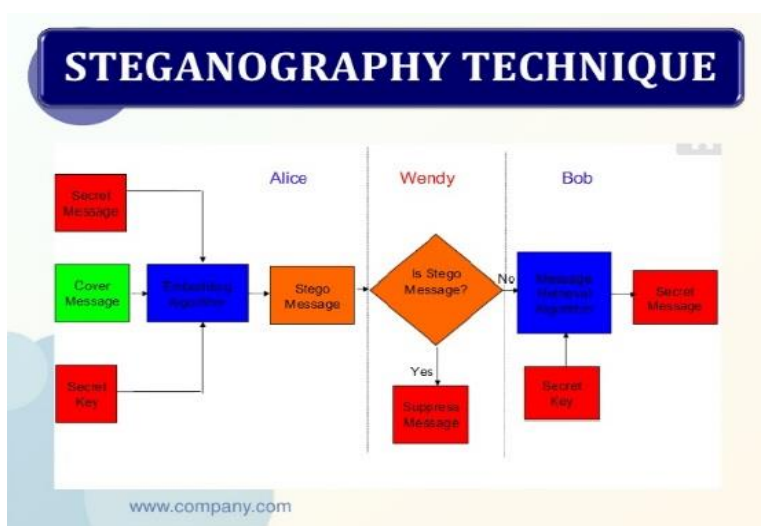


Figure 1: Generic steganography systems [11]

Since the rise of the net, one of the foremost important factors of data technology and communication is that the security of data. Cryptography has been used as a technique for securing the secrecy of communication, and many completely different strategies are developed to code and decode information so as to stay a message secret. Steganography attempts to hide the existence of communication [1]. However, it is not enough to stay the contents of a message secret, it may even be necessary to stay the existence of the message secret. The used technique to satisfy that is called steganography.

In computer science, steganography is the science of concealing information inside a file.

Electronic communications may embrace the transport layer, document file, image file, program or protocol. Steganography is the art of hiding the very fact that communication is happening, by hiding data in different data. It is the art of concealing a message during a cover while not exploit an interesting track on the initial message. The word steganography is derived from the Greek words stegos that means cowl and grafia meaning writing [8] shaping it as lined writing.

There are many techniques to conceal data within cover-image. The spatial domain techniques manipulate the cover-image picture element bit values to insert the secret data. The secret bits are written on to the duvet image picture element bytes. Consequently, the spatial domain techniques are easy and simple to implement. The Least Significant Bit (LSB) is one among the most techniques in spacial domain image steganography. In this work, a new technique of LSB steganography has been proposed that is associate impermanent version of 1 bit LSB technique.

It is best (in term of information hiding) method of image steganography. Because the intensity of image is solely modification by one or zero once concealment the knowledge. Change in intensity is either zero or one as a result of the modification at last bit.

Two different technologies that are closely connected to steganography are watermarking and procedure. These technologies are primarily involved with the protection of intellectual property. But steganography is concern with the concealment of text in another data like image, text, audio and video.

II. RELATED WORK

In [2], the authors have proposed a methodology that hides the key message within the quilt image by representing the key message characters by mistreatment Braille methodology of reading and writing for blind those that will save quite one- fourth of the specified area for embedding. The proposed methodology used the Braille methodology representations of the characters wherever every character is diagrammatic by solely six dots mistreatment the six – dots matrix that referred to as (Braille Cell). The method starts by representing these characters (dots) as binary digits, each of that consists of vi bits solely instead of eight bits as in original LSB embedding methodology that uses the binary illustration from the American Standard Code for Information Interchange table. Therefore, by using this illustration, two pixels are saved from every secret computer memory unit embedding method or additional than twenty-five percent of the most concealing capability for every cowl image. Therefore, the maximum concealing capability (MHC) has been accumulated and also the PSNR of the LSB embedding technique has been increased. In [3], a new approach for hiding message in digital image in special domain has been conferred. According to work of this paper, a method that embeds 2 bits of knowledge in a very pel, and alters one bit from one-bit plane has been introduced. However, the message does not essentially place within the least important little bit of the pel, the second less significant bit plane, the fourth less significant bit plane may also host the message, and only one alteration bit is allowed to be happen. In [4], a new steganography technique has been proposed. According to this method, nine bits of message will be hidden in a very single pel. A true image consists of three parts R, G, and B elements in every component three bits of message hidden. So a total of 9 bits is embedded in to one pel, i.e. more than one character (usually eight bits are accustomed represent the American Standard Code for Information Interchange price of a character). Therefore, the message is not only embedding within the least important bit (LSB), but additionally the second LSB, third LSB, and the fourth LSB are at risk of amendment. However, during every method of embedding solely 2 bit of every element are modified. To have additional security, this method changes solely the even columns of pixels. In [5], the authors have introduced best approach for least significant bit (LSB) that based mostly on image steganography that enhances the present LSB substitution techniques to boost the protection level of hidden info. The new security conception hides secret info among the LSB of image wherever a secret key encrypts the hidden information to defend it from unauthorized users. Hidden information is hold on in totally different position of LSB of image counting on the key. Therefore, a bit of hidden information placed in either LSB of inexperienced or Blue matrix of a particular pel, which set by the secret key. The cover image is split into 3 matrices (Red, Green and Blue). The secret is converted into one, 0 array of bit stream. Secret key and Red matrix are used solely for deciding to interchange hidden info into either inexperienced matrix or Blue matrix. Each bit of secret is XOR with every LSB of Red matrix. The resulting XOR price decides that the one bit of hidden info are going to be placed with either LSB of inexperienced matrix or Blue matrix (i.e. if the XOR value is one, then the LSB of Green matrix is replaced by the initial little bit of hidden info. If the XOR value is zero, then the LSB of Red matrix is replaced by the first little bit of hidden information). The same process are going to be continuing till the hidden info is finished.

III. PROPOSED WORK

Structure of image files is that an image is created from pixels that any pixel created from three colors (red, green and blue said RGB) each color of a pixel is one byte information that shows the density of that color. Merging these three color makes every color that we see in these pictures. We know that every byte in computer science is created from 8 bit that first bit is Most-Significant-Bit (MSB) and last bit Least-Significant-Bit (LSB), the idea of using Steganography science is in this place; we use LSB bit for writing our security information inside pictures. Although 24 Bit images are best for hiding information due to their size. Some people may choose 8 Bit BMP" s or possibly another image format such as GIF [2]. So if we just use last layer (8st layer) of information, we should change the last bit of pixels, in other hands we have 3 bits in each pixel so we have $3 \times \text{height} \times \text{width}$ bits memory to write our information. But before writing our data we must write name of data (file), size of name of data & size of data. We can do this by assigning some first bits of memory (8st layer). All color variations for the pixels of a 24-bit image are derived from three primary colors: red, green and blue, and each primary color is represented by 8 bits [9]. Thus in one given pixel, there can be 256 different quantities of red, green and blue [10].

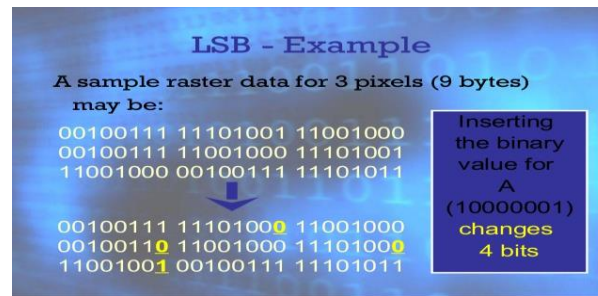
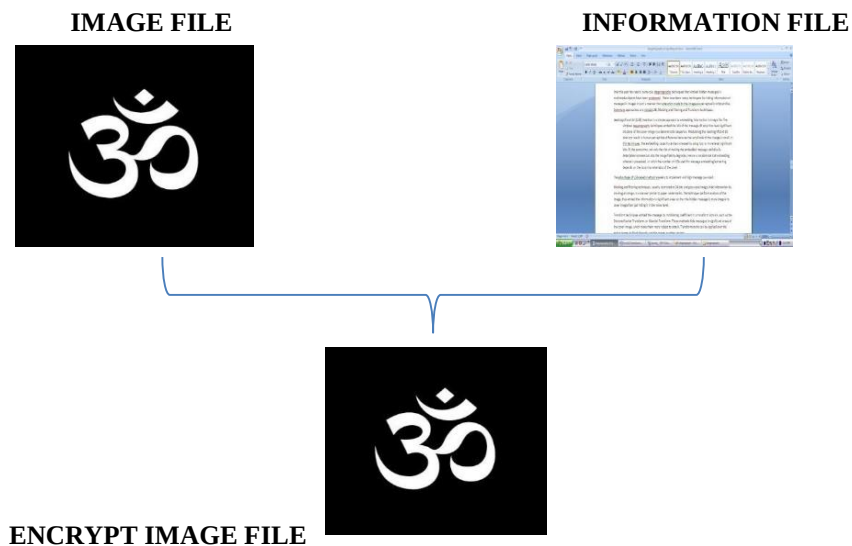
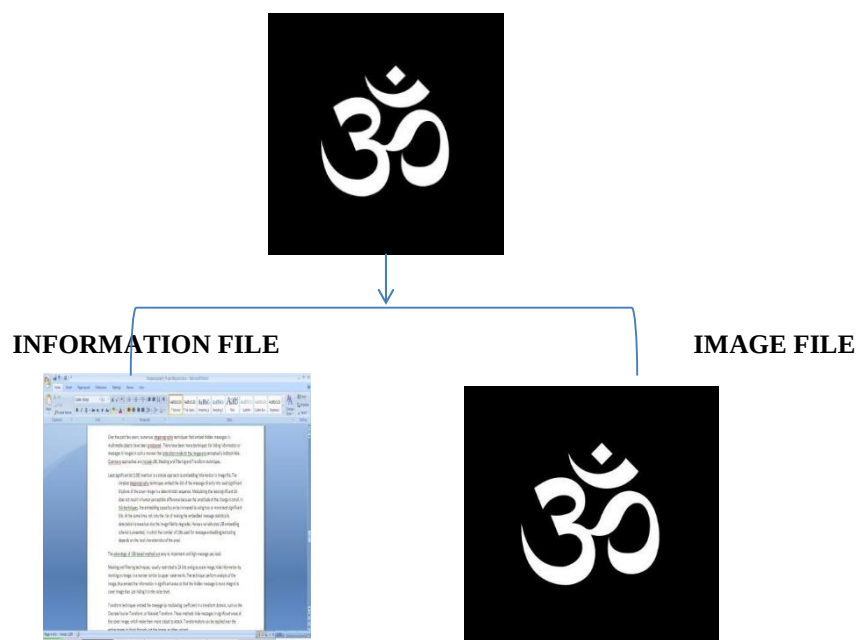


Figure 2: LSB Example
ENCRYPTION PROCESS:



DECRYPTION PROCESS:
ENCRYPT IMAGEFILE



Suppose that we have three adjacent pixels (9 bytes) with the RGB encoding [3]

```

10010101 00001101 11001001
10010110 00001111 11001011
10011111 00010000 11001011
    
```

When the number 300, can be which binary representation is 100101100 embedded into the least significant bits of this part of the image. If we overlay these 9 bits over the LSB of the 9 bytes above we get the following (where bits in bold have been changed)

10010101 00001100 11001000

10010111 00001110 11001011

10011111 00010000 11001010

Here the number 300 was embedded into the grid, only the 5 bits needed to be changed according to the embedded message. On average, only half of the bits in an image will need to be modified to hide a secret message using the maximum cover size.

IV. ALGORITHM

- 1) Select a cover image of size $M \times N$ as an input.
- 2) The message to be hidden is embedded in RGB component only of an image.
- 3) Use a pixel selection filter to obtain the best areas to hide information in the cover image to obtain a better rate. The filter is applied to Least Significant Bit (LSB) of every pixel to hide information, leaving most significant bits (MSB).
- 4) After that Message is hidden using Bit Replacement method.

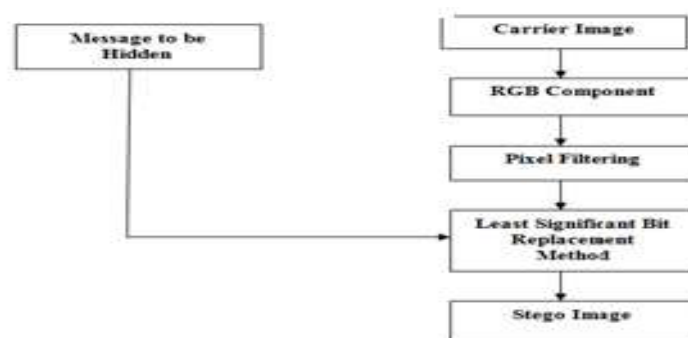


Fig. 3. Algorithm of Least Significant Bit

The LSB is the lowest significant bit in the byte value of the image pixel.

The LSB based image steganography embeds the secret in the least significant bits of pixel values of the cover image (CVR).



Fig. 4: Proposed LSB Algorithm

The concept of LSB Embedding is simple. It exploits the fact that the level of precision in many image formats is far greater than that perceivable by average human vision. Therefore, an altered image with slight variations in its colors will be indistinguishable from the original by a human being, just by looking at it. In conventional LSB technique, which requires eight bytes of pixels to store 1 byte of secret data but in proposed LSB technique, just four bytes of pixels are sufficient to hold one message byte. Rest of the bits in the pixels remains the same.

V. CODE FOR ENCODING

```

01 private byte[] encode_text(byte[] image, byte[] addition,
02     int offset)
03 {
04     if(addition.length + offset > image.length)
05     {
06         throw new IllegalArgumentException("File not long
07         enough!");
08     }
09     for(int i=0; i<addition.length; ++i)
10     {
11         int add = addition[i];
12         for(int bit=7; bit>=0; --bit, ++offset)
13         {
14             int b = (add >> bit) & 1;
15             image[offset] = (byte)((image[offset] & 0xFE) |
16             b );
17         }
18     }
19 }

```

CODE FOR DECODING:

```

01 private byte[] decode_text(byte[] image)
02 {
03     int length = 0;
04     int offset = 32;
05     for(int i=0; i<32; ++i)
06     {
07         length = (length << 1) | (image[i] & 1);
08     }
09     byte[] result = new byte[length];
10     for(int b=0; b<result.length; ++b )
11     {
12         for(int i=0; i<8; ++i, ++offset)
13         {
14             result[b] = (byte)((result[b] << 1) |
15             (image[offset] & 1));
16         }
17     }
18     return result;
19 }

```

VI. CONCLUSION

This method is very easy to implement but this method have following disadvantages One of the major disadvantage associated with LSB method is that intruder can change the least significant bit of all the image pixels. In this way hidden message will be destroyed by changing the image quality, a little bit, i.e. in the range of +1 or -1 at each pixel position. Not immune to noise and compression technique. I will try to solve this disadvantages using enhance or modified LSB method.

REFERENCES

- [1] K.B.Raja, C.R.Chowdary, Venugopal K R, and L.M.Patnaik," A Secure Image Steganography using LSB, DCT and Compression Techniques on Raw Images" Department of Computer Science Engineering, Bangalore 2005 IEEE.
- [2] A. A. Ali and A. H. Seddik, "Image Steganography Technique By Using Braille Method of Blind People (LSBraille)", International Journal of Image Processing (IJIP), Vol. 7, Issue 1, PP. 81-89, 2013.
- [3] A. Daneshkhah, H. Aghaeinia, and S. H. Seydi, "A more Secure Steganography method in Spatial Domain", Second International Conference on Intelligent System, Modelling and Simulation, IEEE, PP. 189-194, 2011.
- [4] S. A. Raj and T. Soumya, "A Youthful Procedure for Spatial Domain Steganography", Third International Conference on Advances in Computing and Communications, IEEE, PP. 300-303, 2013.
- [5] S. M. M. Karim, M. S. Rahman, and M. I. Hossain, "A New Approach for LSB Based Image Steganography using Secret Key", Proceedings of 14th International Conference on Computer and Information Technology (ICCIT 2011), Dhaka, Bangladesh, PP. 286-291, December -2011.
- [6] V. Lokeshwara Reddy, Dr.A.Subramanyam, Dr. P. Chenna Reddy, "Implementation of LSB Steganography and its Evaluation for Various File Formats", Int. J. Advanced Networking and Applications 868 Volume: 02, Issue: 05, Pages: 868-872 (2011).

- [7] T Markel, JHP Eloff and MS Olivier, "An Overview of Image Steganography," in Proceeding of the Fifth Annual Information Security South Africa Conference (ISSA2005), Sand to SouthAfrica, June/July 2005.
- [8] R.Anderson and F. Petitcolas, "On the limits of steganography" IEEE Journal of Selected Areas in Communications, Vol. 16, No. 4, May 1998.
- [9] An overview of image steganography by T. Morkel, J.H.P. Eloff, M.S. Olivier. Information and Computer Security Architecture (ICSA) Research Group Department of Computer Science University of Pretoria, 0002, Pretoria, South Africa.
- [10] Johnson, N.F. Jajodia, S., "Exploring Steganography: Seeing the Unseen", Computer Journal, February 1998.
- [12] Eric Cole, Ronald D. Krutz, "Hiding in Plain Sight: Steganography and the Art of Covert Communication", Wiley Publishing Inc. (2003).
- [13] David Kahn, "The History of Steganography", Proc. of First Int. Workshop on Information Hiding,
- [14] Cambridge, UK, May30-June1 1996, Lecture notes in Computer Science, Vol.1174, Ross Anderson(Ed.), pp.1-7 Benderr, D. Gruhl, N. Morimoto and A.Lu, "Techniques for Data Hiding", IBM System's Journal, Volume 35, Issue 3 and 4, 1996, p.p., 313-336.
- [15] Artz, D, „Digital Steganography: Hiding data within Data“, IEEE Internet Computing, and May/June 2001.
- [16] Wang, Y., Moulin, P. , "Steganalysis of Block- DCT Image Steganography", Beckman Institute, CSL & ECE Department, University of Illinois at Urbana-Champaign, 2003.
- [17] Cox, I. J., Miller, M. L., Bloom, J. A., Fridrich, J., & Kalker, T. (2008). *Digital Watermarking and Steganography, Second Edition*. Burlington, MA: Morgan Kaufmann.
- [18] Wayner, P. (2009). *Disappearing Cryptography Information Hiding: Steganography & Watermarking, Third Edition*. Burlington, MA: Morgan Kaufmann.
- [19] Vikas Tyagi, Atul kumar, Sachin Tyagi, Saurabh Singh Gangwar, Roshan Patel Image steganography using least significant bit with cryptography, *Journal of Global Research in Computer Science*, Volume 3, No. 3, March 2012.

Acknowledgments

I am very thankful to my guide Prof. Sherish Johri & Prof. Amit Chaurasiya for giving me this opportunity to prepare this paper and also thankful to Prof. N.U Khan H.O.D of Information Technology Department, IMSEC Ghaziabad, Uttar Pradesh, INDIA.