International Journal on Data Science and Technology
2017; 3(5): 45-51
http://www.sciencepublishinggroup.com/j/ijdst
doi: 10.11648/j.ijdst.20170305.11
ISSN: 2472-2200 (Print); ISSN: 2472-2235 (Online)

A Review Study on Unique Way of Information Hiding: Steganography

Muhammad Zeeshan, Sibghat Ullah, Saadia Anayat, Rabia Ghulam Hussain, Nayab Nasir

Faculty of Computer Science & Information Technology, Virtual University of Pakistan, Lahore, Pakistan

Email address:
ms150400558@vu.edu.pk (M. Zeeshan), ms150400753@vu.edu.pk (S. Ullah), ms150401012@vu.edu.pk (S. Anayat), ms150400912@vu.edu.pk (R.G. Hussain), ms150400522@vu.edu.pk (N. Nasir)

To cite this article:
Muhammad Zeeshan, Sibghat Ullah, Saadia Anayat, Rabia Ghulam Hussain, Nayab Nasir. A Review Study on Unique Way of Information Hiding: Steganography. *International Journal on Data Science and Technology*. Vol. 3, No. 5, 2017, pp. 45-51. doi: 10.11648/j.ijdst.20170305.11

Received: July 19, 2017; **Accepted**: August 17, 2017; **Published**: September 26, 2017

Abstract: Internet communication become the need of entire world, today internet is like a recourse of power that is used to run human life. The users, as a layman, may not know that internet, a way of communication, as the use of internet is increasing also data and information that is traveling through internet is increasing by every passing day every minute. In an internet environment where every user need security about their data and information that they want to share with other, such environment requires secrecy and security to safeguard the privacy. There are many approaches available that can be adopted to provide user data security, Steganography is one of the techniques which offer sufficient platform to tackle this aspect in a suitable way. The working is very easy; the information (data) can be hidden inside the other information (data) while viewers may see the cover and hidden data will be known to intended viewers only that know the way of decryption that is adopted at sender side. In simple world two images are selected, one as cover and other as message carrier, but the view and size of original image may not be changed. This paper discusses certain technique and algorithms in context to Least Significant Bit (LSB) and ascertains possible depth of LSB usage where the distortion of image starts and attracts the attacker/ hacker. It became a unique way of information hiding by merging images with cipher data or plain text.

Keywords: Steganography, Algorithms, LSB, Depth of LSB, Distortion of Image

1. Introduction

The communication arrangement has made so many things easy in the daily life, where use of internet become a business and need of internet is growing by passing of the day. That business need more transfer of data between different client and users of the internet, although the information travels from one point to another in a friction of seconds it's a speedup of the communication. That's the beauty lies in the security aspects of its structure. The information is valuable till the time it is intact, unhindered, unamended and secured in all respect, because if someone knows the other user information that a big problem for the user so to keep in mind the use of internet the security is also a valuable aspect. As technology is growing and become faster to facilitate the user of the internet the speed of information hacking is also increased, Now-a-days there are number of ways through which the hackers/ attackers either get the information for their use or infect it with some malware, a program that run on users machine and send back information to its operator of its founder. To safe the business need and secure the information along with that media through which it has to travel is also necessary. The growth of business or internet is depended its user security and privacy of their data. The vulnerability has considerably increased in the present scenario because hacker can adopted many ways to stolen the information. Here we discuss the protection and security of information (message) only. To secure the information there are number of ways available which provide solution to the problem. These are cryptography, coding, steganography etc. Among all such methods, Steganography has gained popularity in the recent few years as in [1].

Steganography, a unique way of information hiding, provide the opportunity to the users to hide their messages from all non-concerned people and only intended receivers to receive the messages securely, although a hacker if receive any Stig-Image he/she cannot be able to read the hidden message that why a unsecure medium is used for traveling of data. No doubt that cryptography serves the purpose but everyone has knowledge that an encrypted message is in air and hackers do try to decrypt the message because its reality the thing in air is no longer secure from intended users, But in case of Steganography, the system is altogether different; message (data) can be hidden in text, graphics, video clips or sounds and other than intended receivers, no one guess out about any hidden message because it is impossible to recover the adopted fashion by intended receiver, only correct receiver can get back the hidden message. Steganography is a Greek word which means "concealed writing" as in [1], is presented a new information hiding techniques that is very interesting in such a manner that transmitting a message on a busy channel where other traffic is also running by the other user in an unsecure manner. Steganography is declared by [1] the developed way of information is unique and batter than other the main theme of this technique is that no one except information hider and selected recipient can get secrete message presence in the viewed image. Video or any other type of file.

The paper is organized in various sections. In section II, steganograhic as a whole is described. In section III, algorithms which are in use to perform steganograhy are highlighted. In Section IV, algorithmic time complexities are analysed. In section V, variable depth of least significant bit (LSB) data hiding techniques are discussed. In section VI, the discussion will be concluded.

2. Related Work

In a digital world need of data encryption is very important to protect the user data from intended user, Steganography and Cryptography was the two technique that make secure the data from intended user that want to threat the normal user by many side like harm the user or keeping eyes on others working/progress. Both Steganography and Cryptography are excellent but it is a fact that no one of the technique is batter or trustable because that's technique are broken in many cases where hacker do Cryptanalysis in long term fashion to get break the strong encryption techniques. That why many expert of internet security prefer to add multiple layers of security and uses both technology. In the alphanumeric world to increase the security level from the unwanted users of network Steganography is used, and also high encryption mean to secure a message as long term mean it need strong and cryptanalysis to break any technique because it is a fact both Steganography and Cryptography can be broken in many cases. The most popular data formats that widely available on internet used are. bmp, doc, gif, jpeg,

Mp3, txt and wav because it is difficult to identify which particular file contain any hidden information and it is difficult to identify which tool of steganography is use these data formats to brock the technology. To keep high user security and privacy, it is real fact that the Steganographic technologies plays an important role in the future of Internet security in a network communication system mode. Many government organisations have present laws to make security level increase for information communication security or proscribe cryptosystems completely for user security. Unluckily shrubberies the common of the Internet community either with comparatively feeble and a lot of the times breakable encryption algorithms.

As about 440 BC, the King Darius of Susa remove the hair from the head of his one slave and write a message on the head than after a time when his hair grow up he was sent to the Miletus undetected area, to get back message they remove or cut the hair and read the original message.

Romans used invisible inks, it is difficult to read the message where it is written in a long paper or a bundle of papers, that ink is also used in modern word but in limited manner. It was based from fruit juices and milk and other natural substances [12]. Between 1883 and 1907) a book named "Auguste Kerckhoff" related to Cryptography can clear the foundation of the Steganography and more significantly to watermarking techniques.

1992 to present we are in the modern global digital world where for the sake of user security Steganography is widely used all over computer systems and network based environment like internet. Many of new tools and technologies have been developed that gives us advantage of old steganographic techniques in new fashion, such as null ciphers technique, technique of coding in images for stego-image, audio, video and microdot.

Steganography protocols: in general there are three steganography protocols that are

a. Pure steganography.
b. Secrete key steganography.
c. Public key steganography.

A. Pure steganography: Pure steganography is defined as a striate forward steganographic technique that work without any password that is stego-key in order for the receiver to read the message, it is open technique for secrete messaging. That technique of information hiding is not much secure by nature because both sender and receiver can took their eyes on an assumption that no one can assess their messages. Only sender and receiver ca know the secret mechanism that is adopted.

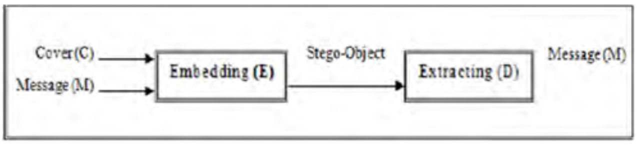

Figure 1. Pure steganography diagram [6].

B. Secrete key steganography: Secret Key Steganography is the best technique of Steganography because it is much secure than other little bit better than before, because a secret key is also used with embedding stage where as if a third person can interfere or get access to stego-image he/she can never get rollback the process because it is require a secrete key. To get back secret message any user/person how have access the message and stigo-key can read only by completion this reverse process. There are much benefit to Secret Key Steganography, like if someone access any message/cipher text or stigo-image without key he/she cannot read original message that is hidden within any image.

C. Public key steganography: is also a unique way of secrete information communication transfer technique where public, private key concepts is used between the parties wanting to communicate secretly, this type of data hiding is much secure and many cases if implemented properly give a batter performance. A person how want to communicate securely use a public key of the partner which he use as encapsulation stage. A message/ image is encrypted with public key must be decrypted with private key of the receiving partner. If a third person or hacker how get access to a stigo-image can never rollback the process to get secrete message back because without complete process of private key is unable to break the system.

3. Steganography – The Approach to Work

There is a need of two image files; one for cover image and other for hiding data after necessary compression. Encryption and embedding is done and at the time of retrieving the data the decryption is carried out. The process is explained in subsequent paragraphs.

3.1. Image Files

The computer takes on everything as data, so a photograph or image is converted into data and saved in a computer. The data is saved in an array of numbers which shows the light intensities at different points. These points are known as pixels which make up the image data. These images are saved in 8-bit or 24-bit files. Figure. 2 and figure. 3 shows 8-bit colour and 24-bit colour display in the computer as in [2].

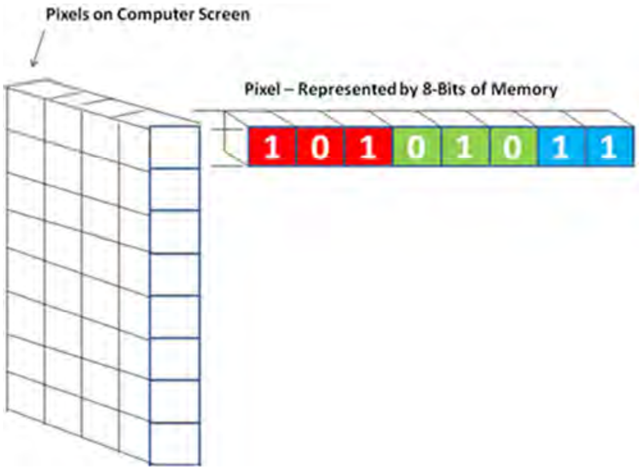
Pixels on Computer Screen
Pixel – Represented by 8-Bits of Memory
1 0 1 0 1 0 1 1

Figure 2. *8-bit.*

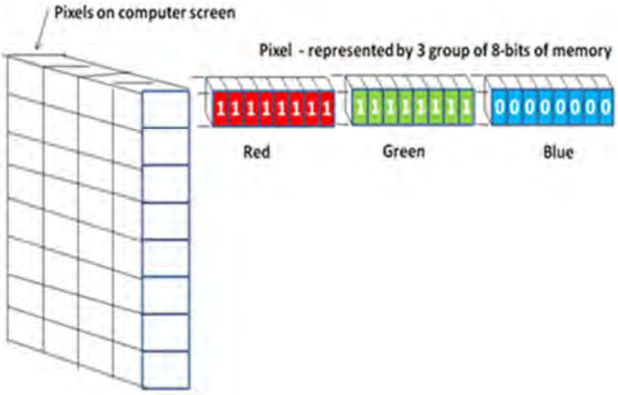
Pixels on computer screen
Pixel - represented by 3 group of 8-bits of memory
11111111
11111111
00000000
Red
Green
Blue

Figure 3. *24-bit.*

There are three primary colours namely Red, Green and Blue which are presented by 1 byte. The distribution of 8-bit colour is done as 3 bits of red, 3 bits of green and 2 bits of blue. But it is different in 24-bit as these are distributed as 8 bits of red, 8 bits of green and 8 bits of blue. Here the image uses 3 bytes per pixel. Hexadecimal, decimal and binary can be used to present these 3 bytes. Since there is much more space in 24-bit therefore it is commonly used as explained in [3]. Figure 4 shows the working of composite RGB (red, green, blue) colour by adding them together and getting true colour as in [4].

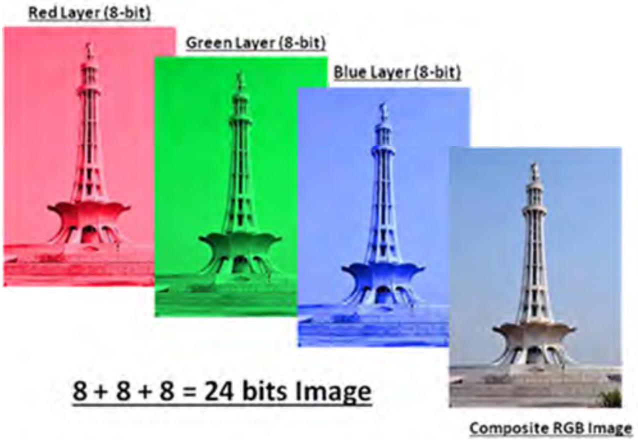

Figure 4. *Composite RGB.*

3.2. File Compression

The compression is carried out in two ways namely lossless and lossy as in [2].

1. *Lossless Compression:* After the process of hiding the image into another image through bit replacement method then compression is done to the image. Once it reached at its destination and data has to be retrieved then it is uncompressed. This process is done through the Lossless compression which has the capability to reconstruct the image in its real form. This is the reason it is commonly in use.
2. *Lossy Compression:* Lossy means once done is retrieved there is a chance of loss of data. The image once reconstructed then it is not in its original form

therefore it is not possible that the receiver gets the information and data has to be discarded.

3.3. Embedding Data

For the purpose of data embedding two image files are used. One file holds the data and other file provides the cover. The data may be of any kind like plaintext/ ciphertext, graphical image or voice etc it can be easily embedded in a bit stream. Once the cover image and message are combined then outcome will be called stego-image.

3.4. More Details – The Approach to Work

The message is converted into the bit streams and divided into 8-bit blocks. The cover image which will be used for covering is also divided into the 8-pixel blocks and each pixel corresponds to each bit in the 8-bit block. This technique is applied to the whole message and the LSB Substitution.

Once the process of converting message into bit streams and further dividing into 8-bit blocks is done then each bit is embedded into the LSB of the pixels. The pixel value is changed by one and it does not have any significant change in the image quality as in [5]. Figure. 5 shows the one LSB change and figure. 6 shows the two LSB change. Here the quality of image got less affected in figure. 4 and more affected in figure. 6.

1	0	0	1	0	0	0	1

Figure 5. *Last One Bit changed - With Change (Right), Without Change (Left).*

1	0	0	1	0	0	0	1

Figure. 6. *Last Two Bit changed- With Change (Left), Without Change (Right).*

4. Algorithms Used for Steganography

As per the experiments carried out on a human eye, it is evident that it reacts differently to three colours namely Red, Green and Blue. Human eye is very less sensitive to blue colour and less sensitive to green colour. But it is more sensitive to red colour. One can say that sensitivity slides downwards from red to green to blue. The image steganography gets the advantage of this limitation of human eye and Steganography algorithms are based on the theory of human visual system (HVS) as in [6]. There are three common ways used to perform the task of hiding the data into the image as in [3], namely:-

1. Least Significant Bit (LSB) Insertion.
2. Masking and Filtering.
3. Discrete Cosine Transform (DCT).

Above mentioned techniques are reasonably practicable and in use, however, there results are different. All these have number of problem areas which are inherited within their own spheres. They are discussed in detail in following paragraphs:-

4.1. LSB Insertion

In a cover file the data is hidden very conveniently and retrieval is also easy as far as lossless compression technique is concerned. But in case of lossy compression, the message is of no use because of some data loss at the stage of retrieval.

4.2. Masking and Filtering

It works like water-marking and normally uses the 24-bit or gray-scale images. The message is hidden as water-marks which are printed on the image file. Such marking is hidden by changing the luminance of the image area where the marks are present. This is done in accordance with the luminance of the whole image area. The degree of increase or decrease is at a level where human eye can't see the water-marking. Masking and filtering is more vigorous and robust as compared with LSB insertion.

4.3. DCT

There are number of algorithms available which compress and hide the data in an image. Jpeg-Jsteg also known as JPEG software is the good example which combines the message and cover image. The compression is achieved by using the discrete cosine transform (DCT). Here the compression is lossy as the values of cosine can't be calculated exactly. Encryption can be used to the data and it can be spread over the whole image and making it like noise. The major benefit of DCT is that the data is more secured. In case the attackers get hold of the data then they have to decrypt the data to understand it. White Noise Storm is one of the best software available for the said purpose.

5. Algorithm Complexity

The algorithms are famous and in use according to their computational cost. The time taken and space occupied matters while performing the embedding and then extracting the data to and from the image respectively. The algorithm complexity increases once use of number of LSBs is increased. The Hoffman code is used in the algorithms which use the permutation and it has linear time complexity *O (n)*. The F5 algorithm works on these lines as in [7].

Whatever the number of bits used, the time taken will be *O (n)* because a single execution of algorithm will be required. It means the bit changing process will be done at the same time on both the cover image and the message. This directs the execution to a small linear complexity as in [6].

The steganography algorithm complexity is established by time complexity and the capacity required by the number of bits. While doing so following are the meters by which the efficacy of the algorithm is judged as experimented at the platform of MATLAB and defined in [8]:-

5.1. Time Complexity

It is an important factor which determines the time spent over the algorithm to complete. The time taken by embedding and then extracting the data is calculated. It is noticed that time increases once number of bits increases. Time consumption increases with the increase of bits which are to be replaced. Now it is clear that time complexity is directly proportional to the increase of number of bits. Figure. 7 shows the increase in the time complexity with the increase in the number of bits as explained in [8].

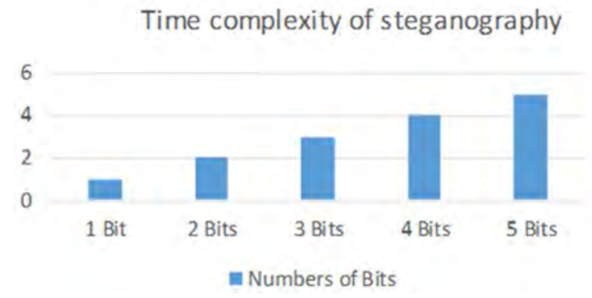

Figure 7. *Time Complexity Increase with Bits Increase.*

5.2. Capacity

The space once gets the data in increasing number then an exponential increase is observed. There is a lot space needed for the data which is to be embedded. Figure. 8 shows the increase in capacity with the bits increase as explained in [8].

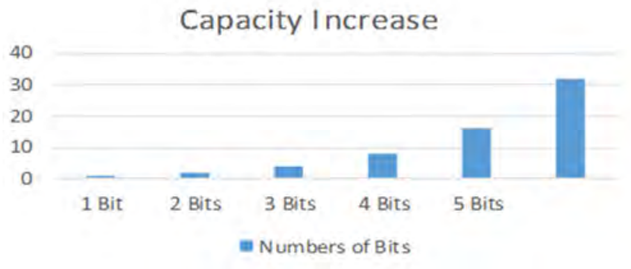

Figure 8. *Capacity Increase with Number of Bits Increase.*

6. Variable Depth LSB Data Hiding

The image will be vulnerable once more number of bits are replaced in the cover image. The image will be distorted and blur as well. Now it has to be determined that at how many bits changing the image's vulnerability is challenged. In this paper it will be analysed that at what maximum depth of LSB the cover image's cover is no more for the hackers or attackers. At what stage the image is distorted enough to attract the viewers to observe some change in the cover image as discussed in [9]. The details as under:-

6.1. One LSB Replacement

The one LSB is concerned it is very evident from the cover image that there is no change observed. The image is same as the original one. Due to no change is seen, no one can guess out any difference. In the one LSB replacement, the message is stored in the right most LSB of only one colour of RGB value or in the parity bit of entire RGB value. Once such change take place then the palette will be having new colours. Now the palette's recommended size should be less than 128 pixels. There is a benefit of this replacement and that is there is no change at all to the cover image. But there is a big drawback and that is a very small size of data can be hidden in the cover image. If a large amount of data is to be hidden then more number of cover images are needed. Figure. 9 shows the one LSB of one colour replacement.

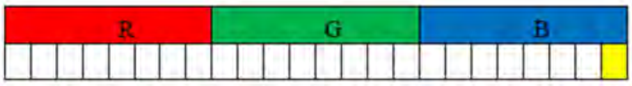

Figure 9. *One Bit LSB Replacement.*

6.2. Two LSB Replacement

In this scenario where two LSB are taken again it is very evident from the cover image that there is not much of change observed. The cover image is same as the actual one. As there is no change observed therefore viewers could not guess out any difference. There is no change from one bit replacement but the storage space is doubled. Two LSBs can be utilized of any colour of RGB value of pixels. A 64 colour palette is required for the production of 192 new colours. In each colour there are two new colours available for every existing colour in the image. Although the space is doubled for the storage of data but again this space is not sufficient enough to hide a large amount of data. If a large data is stored in more than two cover images and in case one image is lost then whole the message cannot be gathered. The receiver cannot make out about the message contents. Figure. 10 shows the two LSB of one colour replacement.

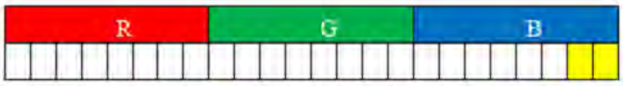

Figure 10. *Two Bit LSB Replacement.*

6.3. Three LSB Replacement

At the level of three LSB replacement, the cover image distortion starts but still viewers with less or no knowledge would not be able to make out any significant difference. Three LSBs can be utilized of any colour of RGB value of pixels for storing the data. A 32 colour palette would be required which allow the production of 224 new colours. Now in each colour there are three colours available for every existing colour in the image. The accessible space will be three times from the previous ones. Figure. 11 shows the three LSB of one colour replacement.

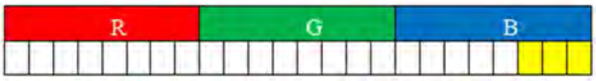

Figure 11. *Three Bit LSB Replacement.*

6.4. Four LSB Replacement

In this situation four LSBs of any one colour of RGB are replaced where 16 colour palette will be required which could produce 240 new colours. Now in each colour there are four colours available for every existing colour in the image. The 16 colour palette is the smallest and beyond this smaller palette is not possible. This aspect limits the usage of colours but about 16 colour variations are sufficient enough to obtain handsome amount of texture mitigation. At this level there is a noteworthy amount of distortion and noise will be observed by the viewers. Figure. 12 shows the four LSB of one colour replacement.

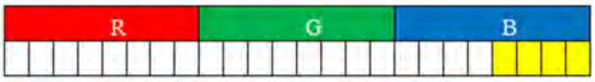

Figure 12. *Four Bit LSB Replacement.*

6.5. Cycling of Colour

There are number of software which can detect the hidden data among the stego – images. These software are based on LSB steganography detection algorithm as explained in [10]. There are two types of modes which can be utilized for detection, these are:-

1). *Simple Mode Detection.* In a cover image any pixel is selected randomly. Image which is selected for hiding purpose is embedded in the cover image's lower bits with upper left corner at the selected pixel. Selected corner's location, bits used for hiding and original image's dimensions are used as a secret key for decryption.

2). *Shuffle Mode Detection*. Here the cover image and image to be hidden are divided into rows and columns. The rows and columns are selected to embed the image. The indices of selected rows and columns are used as decryption key.

The above detection can be avoided by cycling of colour values in each pixel. Data which is to be hidden can be embedded by rotating the RGB colour values. Now the detection would be more challenging and difficult for the attackers. It is difficult because there is no set pattern of hiding the data. The one of the sequences could be first bit replaces Blue LSB, second bit replaces Green LSB, and third bit replaces Red LSB as discussed in [11]. Figure. 13 shows the cycling of colour replacement.

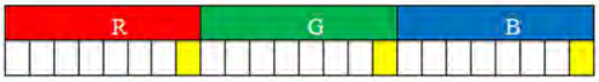

Figure 13. *Cycling of Colour.*

7. Conclusion

This paper has discussed Steganography in detail. The algorithms which are used in carrying out the process, determine the required time and space involved in the process. The complexity in terms of time and capacity has been elaborated. Furthermore with the increase of number of bits what effects could be visible over the image is also highlighted. Least significant bit (LSB) involvement with variable depth is also discussed in detail. The development of the paper is for the beginners who are the learners and interested into the basic knowledge of Steganography.

References

[1] Manini Manasmita and Sangita Roy, "A Novel Approach to Format Based Text Steganography", KIIT University, India, 2011, pp. 511.

[2] Very PDF Knowledge base website. [Online]. Available: http://www.verypdf.com/wordpress/201110/how-can-i-set-color-depth-and-resolution-settings-during-document-to-image-conversion-4898.html

[3] Neil F. Johnson and Sushil Jajodia, "Exploring Steganography: Seeing the Unseen", IEEE, George Mason University, 1998, pp. 26-30.

[4] Yale C/AIM Web Style Guide website "Color Display Primer". [Online]. Available:http://vesta.astro.amu.edu.pl/Library/WWW/Tutorial1/graphics/display_primer.html

[5] Vijay Anand J. and Dharaneetharan G. D., "New Approach in Steganography by Integrating Different LSB Algorithms and Applying Randomization Concept to Enhance Security", Kalasalingam University Srivilliputhur, Tamil Nadu, India, 1989, pp. 474-475.

[6] Samir Kumar Bandyopadhyay et al., "Genetic Algorithm Based Substitution Technique of Image Steganography", University of Calcutta, Kolkata, India, 2011, pp. 63.

[7] Andreas Westfeld, "F5—A Steganographic Algorithm High Capacity Despite Better Steganalysis" Institute for Sys. Arch., Germany, 2001, pp. 296-301.

[8] Surbhi Singhania et. al. "A study on time complexity of least significant bit steganography", Proc. Nat. Conf. "Science in Media 2012", University of Science and Technology, Faridabad, Haryana (India) Dec. 3rd-4th 2012, pp. 125-126.

[9] Namita Tiwari and Dr. Madhu Shandilya, “Evaluation of Various LSB based Methods of Image Steganography on GIF File Format”, Int. Journal of Computer Applications, Vol. 6–No. 2, Sept. 2010, pp. 2.

[10] Ankit Gupta and Rahul Garg, “Detecting LSB Steganography in Images”, 2009, pp. 8-9.

[11] Lip Yee Por et al., “An Enhanced Mechanism for Image Steganography Using Sequential Colour Cycle Algorithm”, The Int. Arab Journal of Info. Tech., Vol. 10, No. 1, Jan. 2013, University of Malaya, Malaysia, 2013, pp. 53.

[12] https://en.wikipedia.org/wiki/Steganography

[13] G. S. a. V. Kumar, “A novel technique for Reversible Information Hiding,” Advances in Computational Sciences and Technology (Research India Publications) ISSN 0973-6107, vol. 10, no. 7, pp. 2069-2078, Number 7 (2017).

[14] Vandana Yadav and Sanjay Kumar Sharma, “A New Approach for Image Steganography Using Edge Detection Method for Hiding Text in Color Images Using HSI Color Model,” *International Journal of Scientific Research in Science, Engineering and Technology,* vol. 3, no. 2, 30 April 2017.

[15] V. I. *. P. L. T. Sivabalan A/L Patiburn, “Text Steganography using Daily Emotions Monitoring,” *International Journal of Education and Management Engineering(IJEME),* May 2017.

[16] V. S. a. J. Fridrich, “EFFECT OF SATURATED PIXELS ON SECURITY OF STEGANOGRAPHIC SCHEMES FOR DIGITAL IMAGES,” in *Image Processing (ICIP), 2016 IEEE International Conference*, Phoenix, AZ, USA, 25-28 Sept. 2016.

[17] S. C. M. P. S. K. a. A. N. Pramod George Jose, “Hash and Salt based Steganographic Approach with Modified LSB Encoding,” *International Journal of Innovative Research in Computer and Communication Engineering,* vol. 4, no. 6, pp. 10599-10610, June 2016.

[18] Harjit Singh, "Analysis of Different Types of Steganography" International Journal of Scientific Research in Science, Engineering and Technology, vol. 2, no. 3, PP. 578-582, 06 June 2016.