IJARESM
INTERNATIONAL JOURNAL OF ADVANCED RESEARCH IN ENGINEERING, SCIENCE & MANAGEMENT

# SURVEY OF IMAGE STEGANOGRAPHY TECHNIQUES

**Roshni Solanki[1], Monika Chuahan[2], Madhavi Desai[3]**
U.G.Student, CSE., SNPIT & RC, Umrakh/ GTU, Bardoli/Surat, Gujarat, India[1]
U.G.Student, CSE., SNPIT & RC, Umrakh/ GTU, Bardoli/Surat, Gujarat, India [2]
Professor, CSE., SNPIT & RC, Umrakh/ GTU, Bardoli/Surat, Gujarat, India [3]

***Abstract:*** ***Steganography is the art and science of invisible communication. This can be accomplished by the hiding information in other information. It is sometimes not enough to keep the contents of a message secret; it may necessary to maintain an existence of the message secret. So the technique used to implement this, is called steganography. Many different carrier file formats (text, digital image, audio, video, protocol) can be used, but digital images are the most popular carrier because of their frequency on the internet. For hiding secret information in images, there exists a large variety of steganography techniques based on a spatial domain, transform domain, spread spectrum techniques, distortion techniques, masking, and filtering. In this paper, we have presented a brief survey of different image steganography techniques.***

*Keywords:* **Communication, Image, Message, Redundant bits, Embedding, Extraction, Steganography, Security**

## I. INTRODUCTION

**Information hiding in digital images has been most popular and has drawn much attention in recent years. In today's information age, information sharing and transfer has increased exponentially. The threat of an intruder accessing secret information has been an ever existing concern for the data communication experts. "Cryptography" and "Steganography" are the most widely used techniques to overcome this threat [1].**

**Cryptography involves converting a message text into an unreadable cipher. On the other hand, Steganography embeds message into a cover media and hides its existence. Both these techniques provide some security of data neither of them alone is secure enough for sharing information over an unsecure communications channel and are vulnerable to intruder attacks [1]. Steganography is not intended to replace cryptography but rather to supplement it. If a message is encrypted and hidden with a steganographic method, it provides an additional layer of protection and reduces the chance of the hidden message being detected.**

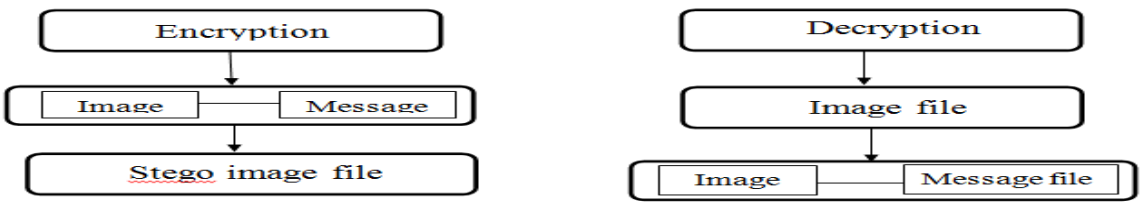


**Figure 1: Block Diagram for Steganography[3]**

A stego-key is used for hiding/encoding process to restrict detection or extraction of the embedded data. In the Steganography system scenario, before the hiding process, the sender must select the appropriate message carrier (i.e image, video, audio, text) and select the effective secret messages as well as the robust password (which supposed to be known by the receiver) **[2]**.

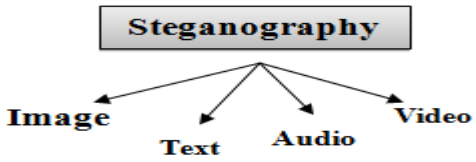


**Figure 2: Carriers for Image Steganography[2]**

Carriers for image steganography are: text, image, audio, and video. Hiding information in text is the most important method of steganography. However, text steganography using digital files is not used very often because the text files have a very small amount of redundant data **[2]**. Images are used as the popular cover objects for steganography. A message is embedded in a digital image through an embedding algorithm, using the secret key **[3]**. On the other side, it is processed by the extraction algorithm using the same key. During the transmission of stego image, unauthenticated persons can only notice the transmission of an image but can't guess the existence of the hidden message **[3]**.

Audio stenography is masking, which exploits the properties of the human ear to hide information unnoticeably **[3]**. An audible, sound can be inaudible in the presence of another louder audible sound. This property allows to select the channel in which to hide information. Video Steganography is a technique to hide any files or information into digital video format **[2]**. Video (combination of pictures) is used as carrier for hidden information. Generally discrete cosine transform (DCT) alter values (e.g., 8.667 to 9) which is used to hide the information in each of the images in the video, which is not noticeable by the human eye **[2]**.

## II. IMAGE STEGANOGRAPHY

As stated earlier, images are the most popular cover objects used for steganography. In the domain of digital images many different image file formats exist, most of them for specific applications. For these various image file formats, different steganographic algorithms exist.

### *A. Evaluation Parameters for Image Steganography:*

All the algorithms for image steganography have different strong and weak points, and it is important to ensure that one uses the most suitable algorithm for an application. The most important requirement is that a steganographic algorithm has to be imperceptible.

These criteria are as follows:

1) ***Payload capacity*:** Unlike watermarking, which needs to embed only a small amount of copyright information, steganography aims at hidden communication and, therefore, requires sufficient embedding capacity.
2) ***Robustness*:** In the communication of a stego image by trusted systems, the image may undergo changes by an active warden in an attempt to remove hidden information. Image manipulation, such as cropping or rotating, can be performed on the image before it reaches its destination. It is preferable for steganographic algorithms to be robust against either malicious/bad or unintentional changes to the image.

3) ***Invisibility*:** The invisibility of a steganographic algorithm is the most important and foremost requirement since the strength of steganography lies in its ability to be unnoticed by the human eye. The moment that one can see that an image has been tampered with, the algorithm is compromised.
4) ***Independent of file format:*** With many different image file formats used on the Internet, it might seem suspicious that only one type of file format is continuously communicated to two parties. The most powerful steganographic algorithms thus possess the ability to embed information in any file. This also solves the problem of not always being able to find a suitable image at the right moment, in the right format to use as a cover image.
5) ***Robustness against statistical attacks:*** Statistical steganalysis is the practice of detecting hidden information through applying statistical tests to image data. Many steganographic algorithms leave a 'signature' when embedding information that can be easily detected by statistical analysis. To be able to pass by a warden without being detected, a steganographic algorithm must not leave such type of mark in the image as be statistically significant.
6) ***Unsuspicious files:*** This requirement includes all characteristics of a steganographic algorithm that may result in images that are not used normally and may cause suspicion.

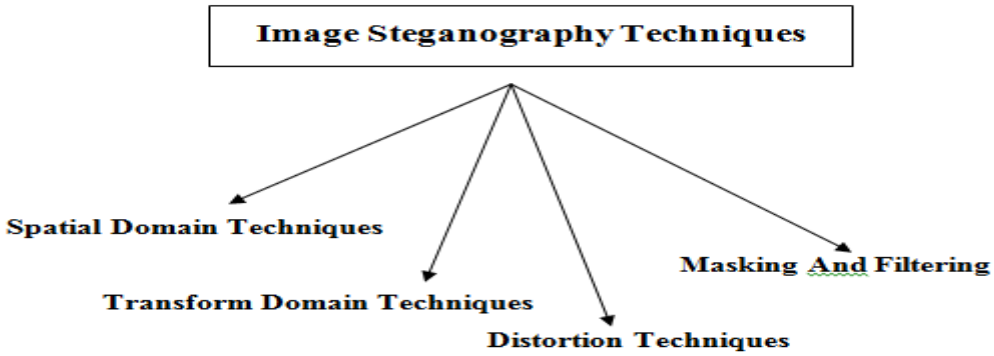


Figure 3: Types of Image Steganography Techniques

*B. Spatial Domain Methods:*

There are many versions of spatial steganography, all directly change some bits in the image pixel values in hiding data. Least significant bit (LSB)-based steganography is one of the simplest techniques that hides a secret message in the LSBs of pixel values without introducing many perceptible distortions **[2]**. Changes in the value of the LSB are imperceptible to human eyes. Spatial domain techniques are broadly classified into:

1. Least significant bit (LSB)
2. Pixel value differencing (PVD)
3. Edges based data embedding method (EBE)
4. Random pixel embedding method (RPE)
5. Mapping pixel to hidden data method
6. Labeling or connectivity method
7. Pixel intensity based method
8. Texture based method
9. Histogram shifting methods

*C. Transform Domain Techniques:*

This is a more complex way of hiding information in an image. Various algorithms and transformations are used on the image to hide information in it **[2]**. Transform domain embedding can be termed as a domain of embedding techniques for which a number of algorithms have been suggested. The process of embedding data in the frequency domain of a signal is much stronger than embedding principles that operate in the time domain. Most of the strong steganographic systems today operate within the transform domain techniques have an advantage over spatial domain techniques as they hide information in areas of the image that are less exposed to compression, cropping, and image processing **[2]**. Some transform domain techniques do not seem dependent on the image format, and they may outrun lossless and lossy format conversions. Transform domain techniques are broadly classified into:

1. Discrete Fourier transformation technique (DFT).
2. Discrete cosine transformation technique (DCT).
3. Discrete Wavelet transformation technique (DWT).
4. Lossless or reversible method (DCT)
5. Embedding in coefficient bits

*D. Distortion Techniques:*

Distortion techniques need knowledge of the original cover image during the decoding process where the decoder functions to check for differences between the original cover image and the distorted cover image in order to restore the secret message. The encoder adds a sequence of changes to the cover image. So, information is described as being stored by signal distortion **[2]**. Using this technique, a stego object is created by applying a sequence of modifications to the cover image. This sequence of modifications is use to match the secret message required to transmit. The message is encoded at pseudo-randomly chosen pixels.

*E. Masking and Filtering:*

These techniques hide information by marking an image, in the same way as to paper watermarks. These techniques embed the information in the more significant areas than just hiding it into the noise level **[2]**. The hidden message is more integral to the cover image. Watermarking techniques can be applied without the fear of image destruction due to lossy compression as they are more integrated into the image.

## III. LITERATURE SURVEY

A lot of Research has been carried out on Steganography. The main purpose of this literature is to present a survey on various steganography techniques used in recent years. It has been relatively difficult to find sufficient articles on steganography since it is not a much-researched discipline. Furthermore, the Google search engine proved to be a valuable tool for our research.

**In 2001, Great scholar James C. Judge[4]** in his work 'Steganography: Past, Present, Future', has observed and conclude that steganography is applied to any number of processes in which we can hide a message within an object, and the hidden message will not be detected by anyone. **James** also stated about past, present work and future of different steganographic techniques.

**In 2003,** One of the researches by **Muhalim bin Mohamed Amin et al [5],** in 'Information Hiding Using Steganography' has proposed and implemented one technique to enhance the compression rate using LSB technique. They have done this by randomly

dispersing the bits of the message in the image. This technique was extremely harder for unauthorized people to detect the original message.

**In 2004, Zhi and Fen [6]** have proposed and developed a new method of LSB image steganography, which was used a method called detection of random LSB. They have used passive steganalysis method for the detection of secret message from the stego image. This method used the concept of RS, that means (Regular And Singular). In this technique, the secret message was inserted in selected part of an image randomly rather than fixed or predefined manner. By this, steganalysis becomes difficult. In this method, gradient energy of an image is analyzed theoretically based on steganalysis detection method known as GEFR.

**In 2004, Potdar and Chang [7]** have introduced and implemented a new method in which First element of the bit stream is mapped to the first selected pixel in the cover image. This will provide better performance and greater security. This technique is useful in server security, network data security and industry scale system.

**In 2005, Raja, *et al*.,[8]** have proved and stated that 'Without any password, images are transferred securely with low Mean Square Error (MSE) and Bit Error Rate (BER).

**In 2007, [9]** authors have introduced and developed a new data hiding technique where the dark area of an image will be found out first, and then data will be hidden using LSB. Then it converts it to the binary image, and then each object will be labeled using 8 pixel connectivity scheme for hiding data bits. However, this method required high computation to find dark region. The data hiding capacity of this technique totally depends on the texture of an image.

**In 2008, [10]** author have proposed and implemented a new pixel indicator technique that uses variable bits. Firstly, it chooses one channel among red, green and blue channels. Then it embeds data into variable LSB of the chosen channel from that 3 channels. Intensity of the pixel decides the number of variable bits of data to be embed into the cover image. The selection of a channel process is sequential, and its capacity depends on the cover image's channel bits. Their proposed method has almost same histogram of cover image and stego-image, so it is not detected by visual attacks.

**In 2008, [11]** author has introduced a Pixel value difference (PVD) and simple least significant bits scheme are used to achieve high adaptive least significant bits data embedding. In pixel value differencing (PVD), the size of the hidden data bits can be calculated by the difference between two consecutive pixels in the cover image using the simple relationship between two pixels. This PVD method provides a good imperceptibility by obtaining the difference between two consecutive pixels that determine the depth of the embedded bits. Proposed technique provides both larger capacity and high visual quality of an image. However, this method is more complex due to adaptive k generation for substitution of LSB.

**In 2008, [12]** authors have proposed and developed a method of Multi-Pixel Differencing (MPD). This method uses more than two pixel to estimate the smoothness of each pixel for data embedding. Then it calculates the sum of the difference value of four pixels block. Note that, for small difference value it uses the LSB otherwise for the high difference value it uses MPD method for data embedding. Strength of this method is its simplicity of an algorithm, but experimental dataset is too limited.

**In 2009, [13] Babita *et al*** uses 4 LSB of each RGB channel to embed data bits, and then apply median filtering technique to enhance the quality of the stego image. Then

encoding will be done by the difference of cover and stego image as key data. In decoding phase, the stego-image is added with key data to extract the hidden data. Proposed scheme has high secret data hiding capacity but has to manage the stego-key.

**In 2009, [14] Hamid *et al*** have proposed and developed a texture based image steganography. Firstly, this texture analysis technique divides the texture areas into two groups namely, simple texture area and complex texture area. The simple texture is used to hide the 3-3-2 LSB (3 bits for Red, 3 bits for Green, 2 bits for Blue channels) method. On the other hand, over complex texture area 4 LSB embedding technique is applied for information hiding. The above-presented method used the both (2 to 4 LSB for each channel) methods depending on texture classification for increasing better visual quality. The proposed method has high hidden capacity with considering the perceptual transparency measures e.g., PSNR, etc.

**In 2009, [15]** authors have proposed and implemented a new LSB based image hiding method. In this technique, a common pattern bits (stego-key) are used to hide data. Then the LSB's of the pixel are modified based on the (stego-key) pattern bits and the secret message bits. Where, the pattern bits are combination of M*N size rows and columns (of a block) and with random key value. In embedding phase, each and every pattern bit is matched with message bit, if satisfied it modifies the 2nd LSB bits of the cover image otherwise it will remain the same. This technique targets to achieve higher security of hidden message in stego-image using a common stego-key. However, this proposed method has very low hidden capacity because the single secret bit requires a block of (MxN) pixels.

**In 2009, Yang et al.[16]** proposed and implemented an adaptive LSB substitution based data hiding method for image steganography. To achieve better visual quality of stego-image, it takes care of noise sensitive area for embedding. This proposed method differentiates and takes advantage of normal texture and edges area for embedding. This method firstly analyzes the edges, brightness and texture masking of the cover image for calculation of number of k-bit LSB for secret data embedding. The value of k is high at non-sensitive image region and over sensitive image area, the k value will remain small to balance overall visual quality of an image. The overall result shows a good high hidden capacity, but it has very few dataset for experimental results.

**In 2009, [17]** author has proposed and implemented another pixel value differencing method. This technique uses the 3 pixels for data embedding that are near to the target pixel. It also uses simple k-bit LSB method for embedding of secret data where number of k-bit is estimated by near 3 pixels with high difference value. To obtain better visual quality of image and high capacity, it simply uses optimal pixel adjustment method on target pixels. The main advantage of this method is that the histogram of stego-image and cover-image is almost same, so it can not be easily detected by visual attacks, but dataset for experiments are too small.

**In 2010, [18]** authors have introduced and developed a high capacity of hidden data utilizing the LSB technique and hybrid edge detection scheme. For the computation of edge, two types of canny and fuzzy edges detection method are applied. Then the simple LSB substitution method is used to embed the hidden data. This scheme is successful to embed data with higher peak signal to noise ratio (PSNR) with normal LSB based embedding. However, the proposed scheme is tested on limited images dataset. This method is not tested on extensive edges based images.

**In 2010, [19] Madhu *et al*** proposed and implemented an image steganography method, based on LSB substitution. In this technique, random pixels will be selected from the image area. This method is targeted to improve the security of technique where password for embedding and extraction is added by LSB of pixels. It generates the random numbers and selects the region of interest where secret message has to be hidden. The strength of this method is its high security of hidden message into the stego-image, but this method does not consider any perceptual transparency.

**In 2010, [20]** authors have proposed and developed an adaptive least significant bit spatial domain embedding method. Firstly, this method divides the image pixels ranges (0-255) and then generates a stego-key by which it will be encrypted. The strength of this proposed method is its integrity of secret hidden information in stego-image and high hidden capacity. The limitation is that we need to hide extra bits of signature with hidden message for maintaining its integrity purpose. It has also proposed a method for color image, and we just have to modify the blue channel with this scheme for information hiding. This method is targeted to achieve high hidden capacity, as well as high security of hidden message.

**In 2010, [21]** One another research by **Namita Tiwari et al** entitled 'Evaluation of Various LSB based methods of Image Steganography on GIF File Format ' has proposed and conclude by their observations that many different carrier file formats can be used, but digital images are the most popular because of their frequency on the Internet.

**In 2011, [22]** Prominent research scholar **Yongzhen Zheng et al** in their work on ' Identification of Steganography Software based on Core Instructions Template Matching ' proposed and developed a new approach, which was based on the principles of LSB Replacement Steganography algorithm. This approach that was used to identify steganography software by Core Instructions Template Matching. It had higher performance as compared to simple LSB replacement technique.

**In 2012, Mare, et al.,[23]** ] introduced and developed a new technique based on LSB:- 9 LSBs, for RGB images, and Payload adaptation. The main advantage of this technique is that it is a very Stronger steganographic model, It is also noticed that the size of jump table for extraction is reduced, and it leaves more space for secret data to be hidden. The only disadvantage is that the Jump table cannot be the store in noisy areas.

**In 2013, [24]** Research scholars **Dipesh Agrawal & Samidha Diwedi** in their research on ' Analysis of random bit image steganography techniques' propounded and stated that many steganography techniques can be used like least significant bit (LSB), layout management schemes by replacing only 1's or only zero 0's from lower nibble from the byte for hiding secret message in an cover image.

**In 2013, Geetha, *et al*.,[25]** proposed and developed a new technique based on LSB, Edge Detection Method, Multiple Edge Detection Method:- Gaussian filter, 2-dimensional convolution filter, Multiple Error Replacement, and Variable Embedding Ratio. This technique has very good visual qualities, highest embedding capacity as well as higher security that prevents it from attacks.

**In 2013, Ramaiya, *et al*.,[26]** have introduces and implemented technique consisting of LSB technique:- 2-bit, DES for encryptions:- 64-bit,16 rounds, S-Box: - 6-bit as input and 4- bit output, 4*16 definition tables,0-15 decimal values. In presented paper, high level of security is provided. It is observed that the variation in two LSB of each pixel will not affect

 

the quality of the cover image. The only disadvantage of this technique is that Small modification to an S-Box could significantly weaken DES; hence it will become less secure.

**In 2014, Mamta Juneja and Parvinder Singh Sandhu [27]** have introduced and developed an Improved LSB based Steganography Techniques for Color Images in Spatial Domain. This research paper aims to propose an additional information security using Hybrid Feature detection technique; Two Component-based Least Significant Bit (LSB) Substitution Technique and Adaptive LSB substitution technique for data hiding. Furthermore, an Advanced Encryption Standard (AES) is used to provide Two Tier Security; Random Pixel Embedding makes it more resistant to statistical and visual attacks and Hybrid Filtering makes it more immune to various disturbances like noise.

**In 2014, M.RAJKAMAL, B.S.E. ZORAIDA, [28]** They have proposed and developed a new technique of image steganography. In this technique, they have used Hash-LSB with RSA algorithm for providing more security to data as well as to data hiding method. The developed technique uses a hash function for generation of a pattern for hiding data bits into LSB of RGB pixel values of the carrier image. This technique ensures that the data has been encrypted first before embedding it into a carrier image.

**In 2014, Sunny Dagar [29]** proposed and developed in his paper a new approach of image steganography. In which, he uses two secret keys to randomize the bit hiding process. This selection of 2 keys enhances the additional level of security of secret information. This approach uses red, green and blue values of a pixel and then performs some calculation on it. Based on this calculation, the bits of the secret information will be placed at the random position of the pixels. This approach maintains high data hiding capacity like LSB substitution do, but it maintains a much better security level than simple LSB substitution as we know that LSB substitution technique is predictable.

**In 2014, Prof. Arjun Nichal, Mr. Abhinav Gorle [30]** have analyzed one technique of steganography. This technique uses steganography along with cryptography it is the main advantage of this technique. They have also analyzed the effect of embedding bits, and they conclude that the effect will be noticeable when the bits exceeds than 4. Evaluation criteria of that technique were PSNR and EC, etc.

## IV. CONCLUSION

Watermarking is used for copyright preserving; cryptography involves converting a message text into an unreadable cipher. On the other hand, Steganography embeds message into a cover media and hides its existence. Both these techniques provide some security of data neither of them alone is secure enough for sharing information over an unsecure communications channel and are vulnerable to intruder attacks.

There are many different techniques for Image Steganography exist and continue to be developed, the most widely used mechanism on account of its simplicity is the least significant bit. However, a simple LSB technique is less secure and robust as compared to LSB which is having use of cryptography also. Most of the strong steganographic systems today operate within the transform domain techniques have an advantage over spatial domain techniques as they hide information in areas of the image that are less exposed to compression, cropping, and image processing.

## ACKNOWLEDGMENT

We are thankfully acknowledged to Mr. J. N. Patel, Chairmain Vidyabharti Trust, Mr. K.N.Patel, Hon. Secretary, Vidyabharti Trust, Dr. H. R. Patel, Director, Dr. J. A. Shah, Principal, Prof. Dhaval Jadhav, Head of CSE Dept., S.N.P.I.T.&R.C.,Umrakh, Bardoli, Gujarat,India for their motivational & infrastructural supports to carry out this research.

## REFERENCES

[01] "VISUAL CRYPTOGRAPHIC STEGANOGRY IN IMAGES", 2011.

[02] "A Survey of Image Steganography" by Sandeep Kaur, Arounjot Kaur, Kulwinder Singh, Ludhiana in IndiaInternational Journal of Computer Applications Technology and Research Volume 3– Issue 7, 479 - 483, 2014.

[03] Morkel, T., Eloff, J. H. P. and Oliver, M. S. ; "An Overview of Image Steganography", Proceedings of the Fifth Annual Information Security South Africa Conference (ISSA), 2005.

[04] James. C. Judge, "Steganography: Past, Present, Future", GSEC Version 1.2f, SANS Institute 2001.

[05] M.M. Amin, .M. Salleh, S. Ibrahim, M.R Katmin (2003), "Information Hiding Using Steganography", 4th National Conference on Telecommunication Technology Proceeding 2003 (NCTT2003), Concorde Hotel, Shah Alam, Selangor, 14-15 January 2003, pp. 21-25.

[06] Zhi, L. and Fen, S.A. ; "Detection of Random LSB Image Steganography", *Vehicular Technology Conference IEEE*, Vol. 3, pp.2113-2117, 2004.

[07] V. M. Potdar, and E. Chang, "Grey level modificationsteganography for secret communication," Industrial informatics, 2004. INDIN '04. 2004 2nd IEEE international conference on 26-26 June 2004,page(s):223-228.

[08] K. B. Raja, C. R. Chowdary, K. R. Venugopal, and L.M. Patnaik, "A secure image steganography using LSB, DCT and Compression techniques on raw images, "Intelligent 14 17 Dec. 2005, page(s):170-176.

[09] H. Motameni, M. Norouzi, M. Jahandar and A. Hatami, "Labeling Method in Steganography", World Academy of Science, Engineering and Technology, France, (2007).

[10] M. Tanvir Parvez and A. Abdul-Aziz Gutub, "RGB Intensity Based Variable-Bits Image Steganography", IEEE Asia-Pacific Services Computing Conference, (2008), pp. 1322-1327.

[11] C.-H. Yang, C.-Y. Weng, S.-J. Wang, Member, IEEE and H.-M. Sun, "Adaptive Data Hiding in Edge Areas of Images with Spatial LSB Domain Systems", IEEE Transactions on Information Forensics and Security, vol. 3, no. (2008) September 3, pp. 488-497.

[12] K.-H. Jung, K.-J. Ha and K.-Y. Yoo, "Image data hiding method based on multi-pixel differencing and LSB substitution methods", Proc. 2008 International Conference on Convergence and Hybrid Information Technology (ICHIT '08), Daejeon (Korea), (2008) August 28-30, pp. 355-358.

[13] B. Ahuja, M. Kaur and M. Rachna, "High Capacity Filter Based Steganography", International Journal of Recent Trends in Engineering, vol. 1, no. 1, (2009) May.

[14] M. Hamid and M. L. M. Kiah, "Novel Approach for High Secure and High Rate Data Hidden in the Image Using Image Texture Analysis", International Journal of Engineering and Technology (IJET): 0975-4042, (2009).

 

[15] S. Channalli and A. Jadhav, “Steganography an Art of Hiding Data”, International Journal on Computer Science and Engineering, IJCSE, vol. 1, no. 3, (2009).

[16] H. Yang, X. Sun and G. Sun, “A High-Capacity Image Data Hiding Scheme Using Adaptive LSB Substitution”, Journal: Radioengineering, vol. 18, no. 4, (2009), pp. 509-516.

[17] H. Zhang, G. Geng and C. Xiong, “Image Steganography Using Pixel-Value Differencing”, Electronic Commerce and Security, ISECS '09. Second International Symposium on (2009) May.

[18] W. J. Chen, C. C. Chang and T. H. N. Le, “High Payload Steganography Mechanism Using Hybrid Edge Detector”, Expert Systems with Applications (ESWA 2010), vol. 37, pp. 3292-3301, (2010) April 4.

[19] V. Madhu Viswanatham and J. Manikonda, “A Novel Technique for Embedding Data in Spatial Domain”, International Journal on Computer Science and Engineering, IJCSE, vol. 2, (2010).

[20] Namita Tiwari, Dr.Madhu Shandilya, "Evaluation of Various LSB based methods of Image Steganography on GIF File Format", International Journal of Computer Applications (0975-8887), Volume 6-No.2, September 2010.

[21] Y. K. Jain and R. R. Ahirwal, “A Novel Image Steganography Method With Adaptive Number of Least Significant Bits Modification Based on Private Stego-Keys”, International Journal of Computer Science and Security (IJCSS), vol. 4, (2010) March 1.

[22] Yongzhen Zheng, Fenlin Liu ; Xiangyang Luo ; Chunfang Yang ,"Identification of Steganography Software based on Core Instructions Template Matching," in Multimedia Information Networking and Security (MINES), 2012 Fourth International Conference on, Shanghai , 4-6 Nov. 2011.

[23] S. F. Mare, M. Vladutiu, and L. Prodan, “High capacity steganographic algorithm based on payload adaptation and optimization,”Applied computational intelligence and informatics (SACI), 2012 7th IEEE international symposium on 24-26 May 2012,page(s):87-92.

[24] Dipesh Agrawal & Samidha Diwedi, "Analysis of random bit image steganography techniques" IJCA Proceedings on International Conference on Recent Trends in Engineering & technology 2013 ICRTET, New York, USA, 1-4, May 2013.

[25] C.R Geetha, S. Basavaraju, and Dr. C. Puttamadappa, “Variable load image steganography using multiple edge detection and minimum error replacement method, ”Information & communication technologies (ICT), 2013 IEEE conference on 11-12 April2013,page(s):53-58.

[26] M. K Ramaiya, N. Hemrajani, and A. K Saxena,“Improvisation of security aspect in steganography applying DES,” Communication systems and networktechnologies (CSNT), 2013 international conference on 6-8 April 2013, page(s):431-436.

[27] Mamta Juneja and Parvinder Singh Sandhu , “Improved LSB based Steganography Techniques for Color Images in Spatial Domain”, International Journal of Network Security, Vol.16, No.4, PP.366-376, July 2014.

[28] M.RAJKAMAL, B.S.E. ZORAIDA, “Image and Text Hiding using RSA & Blowfish Algorithms with Hash-Lsb Technique”, IJISET - International Journal of Innovative Science, Engineering & Technology, Vol. 1 Issue 6, August 2014.

 

[29] Sunny Dagar, "Highly Randomized Image Steganography using Secret Keys", IEEE International Conference on Recent Advances and Innovations in Engineering (ICRAIE-2014), May 09-11, 2014, Jaipur, India.

[30] Implementation and Performance Analysis of LSB Based Steganography, Prof. Arjun R. Nichal. International Journal on Recent and Innovation Trends in Computing and Communication ISSN: 2321-8169 Volume: 2 Issue: 4 885 – 889,2014.

[31] http://www.google.com, http://www.wikipedia.com, http://www.ieee.org

 