Review of Different Techniques of Image Steganography

Ravi Saini
Lecturer, C.M.R.A., GP Sanghi(Rohtak)

***Abstract*— Today, secure communication is the need of the society. Steganography and Cryptography are most popular techniques used for secure communication in the present era. Steganography is used hide the existence of data within some cover media like image file, audio file, video file, text file etc. But the most commonly used media for steganography is image file. There are many techniques of image steagnography like LSB Method, Parity Checker Method and Matrix Determinant Method. In this paper, I have reviewed various image steganography techniques.**

***Keywords*— Steganography, Cryptography, Cover Image, Stego Image etc.**

I. INTRODUCTION

Steganography [1] is the art and science of writing Hidden messages in such a way that no one, apart from the sender and intended recipient, suspects the Existence of the message, a form of security through obscurity. The word steganography is of Greek origin and means "concealed writing" from the Greek words steganos meaning "covered or protected", and graphein meaning "to write". The first recorded use of the term was in 1499 by Johannes Trithemius in his Steganographia, a treatise on cryptography and steganography disguised as a book on magic. Generally, messages will appear to be something else: images, articles, shopping lists, or some other covertext and, classically, the hidden message may be in invisible ink between the visible lines of a private letter. The term Steganography refers to the art of covert communications. By implementing steganography, it is possible for sender to send a secret message to receiver in such a way that no-one else will know that the message exists. Typically, the message is embedded within another object known as a cover Work, by tweaking its properties [2]. The resulting output, known as a stegogramme is engineered such that it is a near identical perceptual model of the cover Work, but it will also contain the hidden message. It is this stegogramme that is sent between sender and receiver. If anybody intercepts the communication, they will obtain the stegogramme, but as it is so similar to the cover, it is a difficult task for them to tell that the stegogramme is anything but innocent.

One of the oldest examples of steganography dates back to around History. Herodotus, a Greek historian from the 5th Century BC, revealed some examples of its use in his work entitled "The Histories of Herodotus". One elaborate example suggests that Histaeus, ruler of Miletus, tattooed a secret message on the shaven head of one of his most trusted slaves. After the hair had grown back, the slave was sent to Aristagorus where his hair was shaved and the message that commanded a revolt against the Persians was revealed [3]. In this example, the slave was used as the carrier for the secret message, and anyone who saw the slave as they were sent to Aristagorus would have been completely unaware that they were carrying a message. As a result of this, the message reached the recipient with no suspicion of covert communication ever being raised. Steganography can be viewed as akin to cryptography. Both Steganography and Cryptography have same goals i.e. to send data securely 440 BC in Greek. AS AN EXAMPLE, THE COVER TEXT:

I'm feeling really stuffy. Emily's medicine wasn't strong enough without another febrifuge.

hides the sentence "Meet me at nine" if the reader retains the second letter of each word in sequence [4].

Steganography can also be achieved by embedding secret data in an unsuspecting medium like image, video or audio, in such a way that the human-perceived quality of the unsuspecting medium is not altered [5]. The idea was first described by Simmons in 1983 [6]. More comprehension theory of steganography is given by Anderson [7]. Steganography is different from Cryptography which is about concealing the content of the message whereas steganography is about concealing the existence of the message itself [8]. Images provide excellent carriers for hidden information and many different techniques have been introduced [9].

In case of image steganography [5,10,11], if the secret data could be encrypted first and then embedded into a cover image then we get the better results. The image into which the encrypted data is embedded is called stego image. The difference between original image and stego image is very small that the human eye cannot distinguish the difference [8,12]. Secret information can also be hidden within HTML Tags [13] since they feature case insensitivity. Shifting text lines vertically and shifting words horizontally [14] may help in hiding some information. Abbreviations and spaces steganography can hide very little information in the text [15]. To protect hidden information among electronic retyping

or OCR usage problems of the previous shifting approach, semantic [16] and character feature [17] In recent years, normous research efforts have been invested in the development of digital image steganographic techniques [18]. The major goal of steganography is to enhance communication security by inserting secret message into the digital image, modifying the nonessential pixels of the image [10]. Until recently, information hiding techniques received very much less attention from the research community and from industry than cryptography, but this has changed rapidly [19]. The search of a safe and secret manner of communication is very important now a days, not only for military purposes, but also for commercial goal related to the market strategy as well as the copyright rights. To find other forms to communicate covertly is important. In this context, the steganography has great significance because it is based on the obscurity to keep the secrecy [20]. With the rapid growth of the Internet and multimedia systems in distributed environments, it is easier for digital data owners to transfer multimedia documents across the Internet. Therefore, there is an increase in concern over copyright protection of digital contents [21, 22, 23, 24]. Traditionally, encryption and control access techniques were employed to protect the ownership of media. These techniques, however, do not protect against unauthorized copying after the media have been successfully transmitted and decrypted. Recently, watermark techniques are utilized to maintain the copyright [25, 26, and 27]. Invisible ink has been in use for centuries—for fun by children and students and for serious espionage by spies and terrorists [28, 29].

Cryptography is a method of storing and transmitting data in a form that only those it is intended for can read and process. It is a science of protecting information by encoding it into an unreadable format. Cryptography is an effective way of protecting sensitive information as it is stored on media or transmitted through network communication paths [30]. Although the ultimate goal of cryptography, and the mechanisms that make it up, is to hide information from unauthorized individuals. Cryptography became very common place in the middle ages. Secret writing was employed by the Catholic Church in its various struggles down the ages and by the major governments of the time. Steganography was normally used in conjunction with cryptography to further hide secret information [31, 32].

The first encryption methods date back to 4,000 years ago and were considered more of an ancient art. As encryption evolved, it was mainly used to pass messages through hostile environments of war, crisis, and for negotiation processes between conflicting groups of people. Throughout history, individuals and governments have worked to protect communication by encrypting it. Cryptography protects the contents of a message, steganography can be said to protect both messages and communicating parties. [33]

Watermarking is defined as a process of embedding information like owner name, company logo etc. in the host data. Digital watermarking embeds a signal into the original element such that the signal uniquely identifies the owner. Watermarking has become the key method for protecting digital elements such as image, audio and video [34].Fingerprinting is the user-unique markings of the data for the purpose of tracing the origin of a discovered, illegal copy of data [35]. The core idea of fingerprinting is that each user receives a copy of the object in question, containing a unique marking [36]. Biometric systems make use of fingerprints, hand geometry, iris, retina, face, hand vein, facial thermo grams, signature, voiceprint, palm print, etc. to establish a person's identity [37, 38]. While biometric systems have their limitations [39], they have an edge over traditional security methods in that it is significantly difficult to lose, steal or forge biometric traits.

II. LITERATURE SURVEY

In this paper, I have reviewed various techniques of image steganography.The details of some popular techniques is given in the next section.s Table 1 shows the different techniques with their features, advantages and disadvantages in ascending order.

TableI

Authors	Year of Publication	Features	Advantages	Disadvantages
Neil F. Johnson & Sushil Jajodia[40]	1998	Spatial Domain Technique Uses LSB of pixel	Simple to implement 100 % chances of insertion.	Not immune to noise and compression technique Not Secure
Wang *et.* al.[41]	2001	Genetic Algorithm	Stego pixel is closer to host pixel	Huge Computational time & bijective mapping function solution is not optimal
Chan & Chang[42]	2001	Uses Moderate significant bits	Improve sensitivity to modification	Degrade quality of stego image
Chang *et.* al[43]	2002	Uses dynamic programming strategy	Reduced computational time	
Wu & Tsai[44]	2003	Pixel value difference is used	High hiding capacity & outstanding	Hiding capacity is not optimal

			imperceptibility for the stego image	
Chan & Chang *et.* al[45]	2004	Optimal pixel adjustment process is used	Less Worst Mean Square Error	Hiding capacity is not optimal
Potdar, & Chang[46]	2004	Gray level value of pixel is used	Chances of insertion of data are optimal. Easy to implement.	Vulnerable to steganalysis. Not immune to noise and compression
Manchanda, *et.* al[47]	2004	Image is divided in a contiguous and disjoint regions	Uniform distribution of Message	Less hiding capacity
Ko Chin Chang *et.* al[48]	2008	Three different directional edges are used Optimal approach for selection of reference point is used	Superior embedding capacity & better secrecy protection	
Bhattaacharyya & Sanyal[49]	2009	Eight neighborhood of each selected pixel are used for insertion.	Independent of the nature of the data Produces a stego image with minimum degradation	Less Embedding Capacity
Yadav et.al [50]	2010	Parity of pixel bits are used for message insertion & retrieval	Easy to implement	Not immune to noise & compression
Yadav et.al[51]	2010	6^{th} , 7^{th} & 8^{th} bit are used for message insertion	Chances are message insertion are 85.49%	Hiding capacity is less
Yadav et.al[52]	2011	Pixel is divided into two parts & their difference is used for insertion & retrieval	Change in image quality is less	Not immune to noise & compression
Yadav et.al[53]	2011	Image is divided into equal sizes blocks and message is inserted into central pixel of the selected block using cyclic combination of last three bits	Uniform distribution of message & chances of message insertion are 100%	Hiding capacity is not optimal
Das. et. al[54,58]	2012	LSB:-32bit secret key Blind extraction ASCII HVS	Efficient Method & embedded information is completely invisible	
Mare et. al[55,58]	2012	LSB:- RGB images Payload Adaption	Stronger steganographic model, size of jump table for extraction reduces	Jump table cannot be stored in noisy areas
Jose and Abraham[56,58]	2013	Image encrypation Chaotic sequence	High embedding capacity	
Kadam et. al[57,58]	2013	AES:128 bit key, 32 bit words, LSB, 128 bit cipher	Increased data security and intruder interference	Memory required for implementation should be as small as possible.

III. PARAMETERS OF STEGANOGRAPHY

There are many parameters that affect steganography techniques. These parameters include hiding capacity, perceptual transparency (or security), robustness, complexity, survivability, capability and detect ability [11,59,60,61].

- **Hiding Capacity**

Hiding capacity is the size of information that can be hidden relative to the size of the cover. A larger hiding capacity allows the use of a smaller cover for a message of fixed size, and thus decreases the bandwidth required to transmit the stego-image.

- **Perceptual Transparency**

The act of hiding the message in the cover necessitates some noise modulation or distortion of the cover image. It is important that the embedding occur without significant

degradation or loss of perceptual quality of the cover. In a secret communications application, if an attacker notices some distortion that arouses suspicion of the presence of hidden data in a stego-image, the steganographic encoding has failed even if the attacker is unable to extract the message. Preserving perceptual transparency in an embedded watermark for copyright protection is also of paramount importance because the integrity of the original work must be maintained.

- **Robustness**

Robustness refers to the ability of embedded data to remain intact if the stego-image undergoes transformations, such as linear and non-linear filtering, addition of random noise, sharpening or blurring, scaling and rotations, cropping or decimation, lossy compression, and conversion back to digital form (such as in the case when a hard copy of a stego-image is printed and then a digital image is formed by subsequently scanning the hardcopy.)

- **Tamper Resistance**

Beyond robustness to destruction, tamper-resistance refers to the difficulty for an attacker to alter or forge a message once it has been embedded in a stego-image, such as a pirate replacing a copyright mark with one claiming legal ownership. In a copyright protection application, achieving good tamper resistance can be difficult because a copyright is effective for many years and a watermark must remain resistant to tampering even when a pirate attempts to modify it using computing technology decades in the future.

- **Other Characteristics**

Computational complexity of encoding and decoding is another consideration and individual applications may have additional requirements. For example, for a copyright protection application, a watermark should be resistant to collusion attacks where many pirates work together to identify and destroy the mark.

IV. Popular Techniques of Image Steganography

A. LSB TECHNIQUE [40]

The popular and oldest method for hiding the message in a digital image is the LSB method. In LSB method we hide the message in the least significant bits (LSB's) of pixel values of an image. In this method binary equivalent of the secret message is distributed among the LSBs of each pixel.

For example data bits 01100101 are tried to hide into an 8 bit color image. According to this technique 8 consecutive pixels from top left corner of the image are selected. The binary equivalent of those pixels may be like this

00100101 11101011 11001010 00100011 11111000 11101111 11001110 11100111

Now each bit of data 01100101 are copied serially (from left hand side) to the LSB's of equivalent binary pattern of pixels, resulting the bit pattern would become

00100100 11101011 11001011 00100010
11111000 11101111 11001110 11100111

The problem with this technique is that it is very vulnerable to attacks such as image compression and quantization of noise.

Advantages of LSB

1. 100 % chances of insertion.
2. Easy to implement

Disadvantages of LSB

1. 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.
2. Not immune to noise and compression technique.

3. One of the basic techniques so more vulnerable to Steganalysis.

B. GLM (GRAY LEVEL MODIFICATION) METHOD[46]

Gray level modification Steganography is a technique to map data (not embed or hide it) by modifying the gray level values of the image pixels. GLM Steganography uses the concept of odd and even numbers to map data within an image. It is a one-to-one mapping between the binary data and the selected pixels in an image. From a given image a set of pixels are selected based on a mathematical function. The gray level values of those pixels are examined and compared with the bit stream that is to be mapped in the image.

Initially, the gray level values of the selected pixels (odd pixels) are made even by changing the gray level by one unit. Once all the selected pixels have an even gray level it is compared with the bit stream, which has to be mapped. The first bit from the bit stream is compared with the first selected pixel. If the first bit is even (i.e. 0), then the first pixel is not modified as all the selected pixels have an even gray level value. But if the bit is odd (i.e. 1), then the gray level value of the pixel is decremented by one unit to make its value odd, which then would represent an odd bit mapping. This is carried out for all bits in the bit stream and each and every bit is mapped by modifying the gray level values accordingly.

Advantages of GLM

1. Chances of insertion of data are optimal.
2. Easy to implement.

Disadvantages of GLM

1. Vulnerable to steganalysis.
2. Not immune to noise and compression.

C. PARITY CHECKER METHOD [50]

In this method the concept of even and odd parity by using the parity checker has been used by Rajkumar et al. As it is already known that even parity means that the pixel value contains even number of 1's and odd parity means that the pixel value contains odd number of 1's. Proposed method inserted '0' at a pixel value where pixel value had odd parity and if odd parity is not present over there than we made the odd parity by adding or subtracting '1' to the pixel value. Similarly, we inserted '1' at a pixel value if it had even parity. In case, if even parity is not present at that location then we made even parity over that location by adding or subtracting '1'. In this way we can insert '0' or '1' at any location. For Retrieval of message, again we used the parity checker. If odd parity is present at the selected location then , '0' is message bit, else message bit is '1'. Retrieval process was repeated for all locations where message bits were hidden. In this way, we retrieved the message bits from all the locations where the message bit were inserted.

D. MATRIX DETERMINANTMETHOD [62]

In this Method, Rajkumar used the concept of determinant of matrix for insertion and retrieval of message. Firstly, he extracts the four least significant bits of selected pixel value (i.e. intensity). Now, make the (2x2) square matrix from the extracted bits. We can insert 0 at a pixel position if the determinant of (2x2) square matrix designed is 0. If the determinant of designed matrix is not 0 and we want to insert 0 at that point value then change the least significant bits in increasing order of weight age such that determinant of designed matrix becomes 0. Similarly, we can insert 1 at a pixel position if the determinant of (2x2) square matrix designed is not equal to 0. If the determinant of designed matrix is and we want to insert 1 at that pixel value then change the least significant bits in increasing order ofwe made the semi pixel difference equal to odd number by adding or subtracting 1 to the pixel value. The pixels for insertion of watermark information are selected by using Pseudo-Random Number Generator that is seeded with a secret key.

E. HIDING DATA IN 6th, 7th & 8th BIT OF PIXEL VALUES[51]

In this approach data is hidden in 6th, 7th and 8th bit of pixel values. In this method 6th, 7th and 8th bits of the image pixels are used to hide the message. Since this method involves 8th bit for hiding the message, intruder can easily change 8th bit of all image pixels and this may result in the loss of message. To avoid this, time factor has been introduced, i.e. at some time t1, sender sends the cover object with message and at some other time t2 sender sends the cover object without message. Sender and recipient agree on this time factor initially before starting any communication. The advantage of introducing time factor (slot) is that if least significant bits of all pixels are changed by the intruder even then the message can be retrieved by comparing the two cover objects, i.e. one containing the message and the other not containing the message.

Advantages

1. The probability that the message bit will be inserted at the pseudorandom location at first chance is 85.93%.
2. The advantage of introducing time factor (slot) is that if LSBs of all pixels are changed by intruder even then the message can be retrieved.
3. It can be easily detected if intruder makes some changes because changes will be of +2/-2 range.

Disadvantages

Chances of insertion are not optimal (100 %) at first instance.

F. PVD (PIXEL VALUE DIFFERENCING METHOD)[44]

The pixel value differencing (PVD) method proposed by Wu and Tsai (2003) can successfully provide both high embedding capacity and outstanding imperceptibility for the stego-image. The pixel value differencing (PVD) method segments the cover image into non overlapping blocks containing two connecting pixels and modifies the pixel difference in each block (pair) for data embedding. A larger difference in the original pixel values allows a greater modification.

G. COVER REGION AND PARITY BITS METHOD[47]

In this technique, the image is divided in a minimum of L (m) contiguous and disjoint regions and their use are defined by a pseudo-random number generator (PRNG). The parity of the region is calculated by using equation 3.1.

$$P(I) = \sum_{j \in i} LSB(C_j) \bmod_{2.} \text{----------} (3.1)$$

It is necessary only one LSB flipping of any pixel of the region to change the parity region value.

V. CONCLUSION AND FUTURE SCOPE

In this paper, I reviewed some existing techniques of the image steganography. We have reviewed various existing techniques like LSB, GLM, Parity Checker technique, PVD Method etc. with their advantages and disadvantages. Every research leaves some space for some improvement. So, in future I will try to develop some new techniques which provide us robustness and highly embedding capacity and remove the disadvantages associated with the existing techniques.

REFERENCES

[1] N. Johnson and S. Jajodia, "Exploring steganography: seeing the unseen," IEEE Computer, pp. 26-34, February 1998.
[2] Soumeyendu Das, Subhendu Das , Bijoy Bandhopadhyay , Sugata Sanyal, "Steganography and Steganalysis:Different approaches".
[3] Provos, N., Honeyman, P. "Hide and Seek: An Introduction to Steganography",
[4] Eugene, T.L. and Edward, J.D.(2006), "A Review of Data Hiding in Digital Images", Video and Image Processing Laboratory (VIPER), Indiana.
[5] Amirtharajan Rengarajan, Ganesan Vivek, Jithamanyu R, Rayappan John Bosco Balaguru, "An Invisible Communication for Secret Sharing against Transmission Error", Universal Journal of Computer Science & Engineering Technology, 1 (2), 117-121, Nov – 2010.
[6] Simmons G. J, "The Prisoners Problem and the Subliminal Channel", Proceedings of crypto '83, Plenum Press, pp 51-67, 1983.
[7] Anderson R. J, "Stretching the Limit of Steganography", In Information Hiding, Springer Lecture Notes in Computer Science, Vol. 1174, pp 39-48, 1996.
[8] Anderson, R.J. and Petitcolas, F.A.P. (1998), "On the Limits of Stegnography", IEE Journal on selected Areas in Communications, Vol. 16 No 4, pp 474-481
[9] NEIL F. JOHNSON, ZORAN DURIC, S. G. J. Information Hiding : Steganography and Watermarking - Attacks and Countermeasures (Advances in Information Security, Volume 1). Kluwer Academic Publishers, February 15, 2001.
[10] Cheddad, A., Condell, J., Curran, K. and Kevitt, P.M. (2010), "Digital image steganography: Survey and analysis of current methods Signal Processing 90 :727–752
[11] W. Bender, D. Gruhl, N. Morimoto, A. Lu,"Techniques for data hiding", IBM Syst. J. 35 (3&4) (1996) 313–336.
[12] Anderson R. J, "Stretching the Limit of Steganography", In Information Hiding, Springer Lecture Notes in Computer Science, Vol. 1174, pp 39-48, 1996.
[13] Hassan, M. and Shahreza, M. (2006) "A New Approach to Persian/Arabic Text Steganography," 5th IEEE/ACIS International Conference on Computer and Information Science (ICISCOMSAR 06), pp. 310- 315.
[14] Bennett, K. (2004), "Linguistic Steganography: Survey, Analysis, and Robustness Concerns for Hiding Information in Text", Purdue University, CERIAS Tech. Report 2004-13.
[15] Low, S.H., Maxemchuk, N.F., Brassil, J.T. and O'Gorman, L.(1995), "Document marking and identification using both line and word shifting", Proceedings of the Fourteenth Annual Joint Conference of the IEEE Computer and Communications Societies (INFOCOM '95).
[16] Chan, C.K. and Chen, L.M. (2004), "Hiding data in images by simple LSB substitution", Pattern Recognition 37 (3) 469–474.
[17] Judge, J.C. (2001),"Steganography: Past, Present and Future", Sans Institute.

[18] Rabah, K. (2004) "Steganography-The Art of Hiding Data", Information Technology Journal, vol. 3, Issue 3, pp. 245-269.
[19] Lee, Y.K. and Chen, L.H. (2000), "A Secure Robust Image Stegnography Model", 10th National Conference on Information Security, Hualien, Taiwan, pp 275-284
[20] Rodrigues, J. M., Rios, J. R. and Puech, W. (2006), "SSB-4 System of Steganography using bit-4".

[21] Piva, A., Bartolini, F. and Barni (2002), M., "Managing copyright in open networks", IEEE Transactions on Internet Computing, Vol. 6, Issue. 3, pp. 18-26.
[22] Lu, C., Yuan, H. and Liao, M. (2001), "Multipurpose Watermarking for Image Authentication and Protection", IEEE Transactions on Image Processing, Vol. 10, Issue. 10, pp. 1579-1592.
[23] Lu, C., Huang, S., Sze, C. and Liao, H.Y.M (2000), "Cocktail watermarking for digital image protection", IEEE Transactions on Multimedia, Vol. 2, pp. 209-224.
[24] Lee, J. and Jung, S. (2001), "A survey of watermarking techniques applied to multimedia", Proceedings IEEE International Symposium on Industrial Electronics (ISIE), Vol. 1, pp. 272-277.
[25] Brainos, II A.C. (2007),"A Study Of Steganography And The Art Of Hiding Information".
[26] Petitcolas, F. (1999), "Information hiding techniques for steganography and digital watermarking Stefan Katzenbeisser", Artech House Books, ISBN 1-58053-035-4.
[27] Eskicioglu, A. and Delp, E. (2001), "An overview of multimedia content protection in consumer electronics devices", Proceedings Signal Processing Image Communication, pp. 681-699.
[28] Krenn, R. (2006)," Steganography and steganalysis".
[29] Brainos, II A.C. (2007),"A Study Of Steganography And The Art Of Hiding Information".
[30] NEIL F. JOHNSON, ZORAN DURIC, S. G. J. Information Hiding : Steganography and Watermarking - Attacks and Countermeasures (Advances in Information Security, Volume 1). Kluwer Academic Publishers, February 15, 2001.
[31] Provos, N. and Honeyman, P.(2003), "Hide and Seek: Introduction to Steganography".
[32] Pal, S.K., Saxena, P.K. and Muttoo, S.K.(2004), "Image steganography for wireless networks using the handmaid transform", Internation Conference on Signal Processing & Communications (SPCOM).
[33] Stalling, W. (2005), "Cryptography and Network Security Principles" Fourth Edition PHI Indian Edition.
[34] Hartung, F. and Kutter, M. (1999), "Multimedia Watermarking Techniques," Proc, IEEE, vol. 87, no. 7, pp. 1079-1107.
[35] Lindkvist, T. and Lofvenberg, J. (2000), "A Binary Fingerprinting Model", LiTH-ISY-R-2257, ISSN 1400-3902
[36] Brassil J, Low S, Maxemchuk N, O'Garman L. (1994), "Electronic Marking and Identification Techniques to Discourage Document Copying". In: Infocom. IEEE. 1278–1287.
[37] Jain, A.K., Bolle, R., and Pankanti S.,"Biometrics: Personal Identification in Networked Society", Kluwer Academic Publishers, 1999.
[38] Wayman, J.L., "Fundamentals of biometric authentication technologies", International Journal of Image and Graphics, vol. 1, no. 1, pp. 93–113, 2001.
[39] Gorman, L.O., "Seven issues with human authentication technologies", in Proc. of Workshop on Automatic Identification Advanced Technologies (AutoID), (Tarrytown, New York), pp. 185–186, Mar 2002.
[40] Neil F Johnson, Sushil Jajodia, "Exploring Stenography: Seeing the Unseen", IEEE Computer, Feb 1998, pp 26-34.
[41] R.Z. Wang, C.F. Lin and J.C. Lin,"Image hiding by optimal LSB substitution and genetic algorithm",Pattern Recognization Vol. 34, pp. 671-683,2001.
[42] Chan, Y. & Chang, C. 2001,"Concealing a secret Image using the breadth first Transversal linear Quadtree Structure "", 3rd international symposia on Cooperative Database systems and applications , 2001
[43] C.C.Chang, J.Y.Hsiao, C.S. Chan,"Finding optimal least significant bit substitution in image hiding by dynamic programming strategy",Pattern Recognization Vol. 36,Issue 7, pp 1583-1595,2003
[44] D.C. Wu and W.H. Tsai,"A steganographic method for images by pixel value differencing",Pattern Recognization Letters, Vol. 24, pp 1613-1626,2003
[45] C.-K. Chan, L. M. Cheng, "Hiding data in images by simple LSB substitution," Pattern Recognition Vol. 37, Issue 3, pp. 469-474, 2004
[46] Potdar, V. and Chang, E. (2004), "Gray Level Modification Steganography for Secret Communication", IEEE International Conference on Industrial Informatics, Berlin, Germany.
[47] Manchanda, S., Dave, M. and Singh, S.B. (2004), "Customised and secure Image Steganography Through Random number Logic".
[48] Ko-Chin Chang, Chien-Ping Chang, Ping S. Huang, and Te-Ming Tu," A Novel Image Steganographic Method Using Tri-way Pixel-Value Differencing", JOURNAL OF MULTIMEDIA, VOL. 3, NO. 2, JUNE 2008"
[49] Souvik Bhattacharrya and Gautam Sanyal,"Hiding data in Images using PCP", World Academy of Science, Engineering and Technology,2009
[50] Yadav, Rajkumar, Rishi, Rahul, Batra, Sudhir, "A new Steganography Method for Gray Level Images using Parity Checker", International Journal of Computer Applications (0975-8887) Volume 11-No. 11, December 2010.
[51] Batra, S., Rishi, R., Yadav, R. (2010), "Insertion of message in 6th, 7th & 8th bit of pixel values and retrieval in case intruder changes the least significant bit of image pixels", International Journal of Security and its Applications, Vol . 4, No. 3
[52] Rajkumar Yadav, Gaurav Chawla and Ravi Saini,"Semi-pixel Difference Method for Digital Image Watermarking with Minimum Degradation in Image Quality ",International Journal of Computer Technology & its Applications ,Vol2(5),1297-1314
[53] Rajkumar Yadav,Ravi Saini and Kamaldeep,""Cyclic Combination Method for Digital Image Steganography with uniform distribution of Message",Advance Computing: An International Journal(ACIJ),Vol. 2, No. 6, November 2011
[54] S. Das, P. Bandyopadhyay, Prof. A. Chaudhuri and Dr. M. Banerjee, "A secured key-based digital text passing system through color image pixels, "Advances in engineering, science and management (ICAESM), 2012 international conference on 30-31March 2012,page(s):320-325
[55] 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 May2012,page(s):87-92.
[56] R. Jose, and G. Abraham, "A separable reversible data hiding in encrypted image with improved performance, "Emerging research areas and 2013 international conference on microelectronics, communications and renewable energy (AICERA/ICMiCR), 2013 annual international conference on4-6 June 2013,page(s):1-5
[57] P. Kadam, A. Kandhare, M. Nawale, and M. Patil, "Separable reversible encrypted data hiding in encrypted image using AES algorithm and lossy technique, "Pattern recognition, Informatics and medical engineering (PRIME), 2013 international conference on 21-22 Feb. 2013,page(s):312-316
[58] Sandeep Singh, Aman Singh," A Review on the Various Recent Steganography Techniques", IJCSN International Journal of Computer Science and Network, Volume 2, Issue 6, December 2013 ISSN (Online) : 2277-5420
[59] Titchener, M.R. (1984), " Technical note:Digital encoding by way of new T-codes", IEE Proc. E. Comput. Digit Tech, 131, (4), pp. 151-153.
[60] Chandramouli, R. and Memon, N.D. (2003), "Steganography capacity: A steganalysis perspective", Proc. SPIE Security and Watermarking of Multimedia Contents, Special Session on Steganalysis.
[61] Parvez, M. T. and Gutub, A.(2008), "RGB Intensity Based Variable-Bits Image Steganography", APSCC 2008-Proceedings of 3rd IEEE Asia-Pacific Services Computing Conference, Yilan, Taiwan, 9-12.
[62] Rajkumar Yadav," A New Data Hiding Method using Determinant of 2x2 Matrix", International Journal of P2P Network Trends and Technology-Volume1Issue2- 2011