**International Journal of Technical Research and Applications e**-ISSN: 2320-8163,
www.ijtra.com Volume 2, Issue 4 (July-Aug 2014), PP. 72-75

# A NOVEL APPROACHES TOWARDS STEGANOGRAPHY

**Geeta D. Rote[1], Dr. A. M. Patil[2]**

[1] Research Scholar
[2]HOD of Electronics and Telecommunication
J.T.M College of Engineering, Faizpur

***Abstract*— For increase network security of messages sent on internet the steganography is mostly preferred. To transmit data secretly steganography is used in open system environment. In this paper discussed the reviews of image steganography and the general framework of image steganography using different method. Steganography is nothing but art of hide information behind the other information without leaving remarkable track on original message.**

***Keywords*— Cryptography, Steganography, Watermarking, LSB, DCT, etc**

## I. HISTORY OF STEGANOGRAPHY

Steganography is nothing but the concealed communication. This technique is used for data hiding under the cover information, hidden information recover by particular key without any awareness of original information [**1].**

While Cryptography also used for data hiding. This is started before 4000 years ago by Egyptian people. But it allows only the privacy, in contrast steganography provides secrecy, [2] Privacy you need when you use your credit cards on internet that means you don't want your credit card number revealed to the public that time you used cryptography. That means hacker can see you have sent a message because that code may be unbreakable. But in contrast steganography having true secrecy, you do not want anyone to know you are sending a message at all. Actual message can hide behind the cover message without any suspicion. During the 1980's, Margaret Thatcher wants to find out that from where cabinet documents leaks from press. So she had the word processors programmed to predetermine their uniqueness in the word spacing, so that unfaithful ministers could be traced [3].

In 1983, steganography is termed as a prisoner's problem, where two prisoners A and B want to escape from jail. They wants to communicate each other but one warden was observe there communication. So they embed there secrete message with the covert text, warden can see the cover message but cannot even predict that some message hidden behind it [4] [5].

In steganography information can be hidden in carriers such as images, audio files, text files, and video and data transmissions. When message is hidden in the carrier a stego carrier is formed for example a stego-image. Hopefully it will be perceived to be as close as possible to the original carrier or cover image by the human senses. Images are the most widespread carrier medium. They are used for steganography in the following way. The message may firstly be encrypted. The sender embeds the secret message to be sent into a graphic file. This results in the production of what is called stego-image. Additional secret data may be needed in the hiding process e.g. a stego-key etc. This stego-image is then transmitted to the recipient. The recipient extractor extracts the message from the carrier image. The message can only be extracted if there is a shared secret between the sender and the recipient. This could be the algorithm for extraction or a special parameter such as stego-key. A Steganalyst or attacker may be tried to intercept the stego image [6].

In steganography our secure data is embed with the cover image. Data embedding is really invisible due to the human vision system and it cannot understand original host signal and host signal with hidden data. Such a blind tests are used to evaluate the perceptual simplicity of data embedding process [7].

*1) Types Of Steganography*

There are four different types of steganography those are text, audio, video and Image steganography. In text steganography line shift coding, word shift coding and feature coding as well as syntactic/ semantic methods are used for data hiding. This type of data hiding is done by changing the formatting or look of the file, by modifying spacing between the lines, modifying words or the sizes of the letters but this type of modifications can be easily visible to eye or sometimes it changes the meaning of sentences because of that text files have a small amount of redundant data

Audio steganography is also most difficult technique to encode the secret message because of the human auditory system. Audio steganography, the hiding of messages in audio "noise" (and in frequencies which humans can't hear), is another area of information hiding that relies on using an existing source as a space in which to hide information. Audio steganography can be problematic, however, since musicians, audiophiles, and sound engineers have been reported to be able to detect the extra high-frequency information encoded in messages. In addition to store information in non-audible frequencies or by distorting the audible signal to include additional noise [8, 6].

As per [9] Image steganography is relatively easy and protected way for transmitted information over the internet. This type of steganography is mostly used to hide secret message in digital images because of the limited power of human vision. LSB encoding is the most popular technique used for digital images. In LSB we can store 3 bits of data in each pixel for 24 pixels that means this type of steganography can hide large amount of data as compare to others, secondly it cannot differ in cover image as well as stego image so hackers cannot predict that some data is hidden behind that image. If hacker do not having any special extracting method or secrete key then he or she cannot extract the hidden message. Rather than when we apply image compression and image processing on the stego image that time also the message recovery rate is higher.

For flexibility, robustness and higher security in image steganography combines with cryptography. In cryptography data is hide in unreadable format, but it increase the curiosity of the hacker to get that message. And if we hide that unreadable data by using steganography no one can recognize the hidden

data, so we can increase the security by combining these two methods [10].

## II. GENERAL FRAMEWORK

Figure 1 shows the block diagram of steganography mechanism.

1. Encrypt: The secret data is encrypt behind the original message.
2. Embed: Embedding the information along with Least Significant Bit method along with stego key which is mandatory for sender and receiver. By using stego key it forms stego object

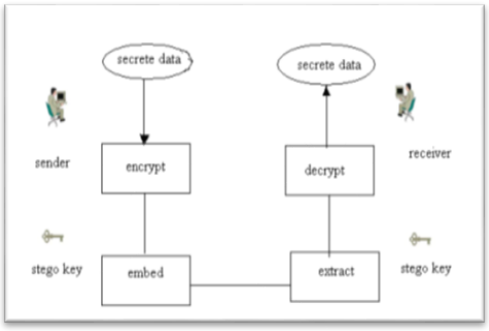


**Figure 1 Block diagram of Steganography by [11].**

3. Extract: At the receiver side that stego object is separates by stego key. The same stego key is required to extract the secret data.
4. Decrypt: At last the original message and hidden data is separate at the receiver side and receiver gets the secret data.

*A. Steganography Techniques:*

Watermarking and steganography are similar techniques which used for data hiding. In watermarking technique information hides in data object but that is not easily modify or it will corrupt the quality of image. Steganography is the technique, where modification in cover message may corrupt the hidden information. [12]

In watermarking data hide into multimedia data by any unnoticeable modification in data. In steganography normal carrier is used to hide data without enlightening its presence. [13]

In Data Insertion technique unique signature is created of stego image by using different steganography tools. By using camouflage tool steganography algorithm is easy to detect. Compare with jpegx tool, it adds particular fixed signature before adds with secrete message. [14]

Least Significant Bit technique secrete message is hide behind the cover message after that remaining data is replaces by all 0's or all 1's. At the time of detection first consider the LSB's of data and then search for block of 0's or 1's. In LSB technique data is hidden behind the cover image, it creates one stego image for communication. Images may be 24 bit or 8 bit image; if image is 24 bit then it is capable to hide 3 bits of data per pixels. For 8 bit image it can hide one bit per pixel. So by changing these bits of information do not affect the cover image and so it cannot easily attract attention of hackers.

Discrete Cosine Transform technique data embed in spatial domain and it's difficult to detect the hidden data. DCT uses basically two different methods, large number of coefficients customized slightly to contain data of payload another is customized small number of insignificant coefficients by data of payload. [4]

Transformation technique is used for embedding the data in large amount, but in this technique generates more noise in stego image, compare with this LSB is used to reduce noise. In wavelet transformation technique data stored in small memory space because of that data can be easy to transfer. In transformation techniques, spatial domain to frequency domain conversion also possible by using DCT, Fast Fourier transforms or wavelets etc [15]

Decompositions in data hiding are performing by DCT, DFT, hadamard and sub band transform. DFT is better as compare to other decomposition. [16]

In steganography video and image data can also hide behind video. Video is nothing but series of high motion images [17]**.** That conceal data is distribute over wide range of frequencies of cover data. Discrete cosine or discrete wavelet transform coefficient is used for conceal data. In DCT technique two bits of conceal data can hide behind cover data.

J. J. Chae and B. S. Manjunath [18] presents a technique that conceal image and cover video convert using the 8 × 8 DCT. Conceal coefficients quantized and then encoded using multidimensional lattices and then inserted into cover DCT coefficients.

As per [19] LSB is implemented by using spatial domains in which secrete data bits are replaced by least significant bits of the cover image to form a stego image. As well as in DCT & DWT algorithms are implemented by frequency domain in which frequency domain convert to spatial domain of stego image & hidden data bits embed into frequency components of cover image

In Spread Spectrum image steganography is another technique of hiding information within noise signal. If kept at level, it's not observable to human vision and susceptible to computer analysis except the cover image. [20]

## III. RELATED WORK

Steganography is the technique to conceal the data in secure manner, that means hide a data behind the other data. Original information hides at the back of cover information.

Steganography is nearly similar to cryptography difference is that in cryptography is convert the original information in non-readable format and no one can understand the information. And the steganography is the technique which no one can understand that any information is hiding behind the existing data. That means the data is unobtainable to unauthorized users the person intended to get message even knows a secret message exist. In steganography we can hide information like text, image, audio and video [2, 8, 21, 22].

In steganography technique for hiding information can be used many formats such as .bmp, .doc, .gif, .jpeg, .mp3, .txt .au and .wav. Information concealing is not capable in text as well as audio as compare to images. In day to day life images are more secure data type for hide the information. When we use the computers that images are made up of number of pixels, by combination of that pixels form a complete image. In this digital world for use with steganography 8-bit and 24-bit per pixel image files are representative 8-bit image can represents only 256 colors those are the grey-scale colors, this colors have minor changes because of that hidden data cannot predict easily. Similar to 24- bit images have number of colors which can hide data easily and cannot obtainable to human vision system, advantage of 24-bit images can hide much larger data as compare to 8-bit digital image. Disadvantage of 24-bit digital image is larger is required as compare to 8-bit digital

images when we used it at internet [6, 23]. Grayscale images are the best cover images. When uncompressed scans of photographs or images achieve a high number of colors are optional and highly secure for data hiding [24] [40]

According to Hsiang-Kuang Pan, Yu-Yuan Chen, and Yu-Chee Tseng [25] binary images which consist only two colors black and white also conceal the data more securely as well as more efficiently. Much data can conceal behind binary images without affect quality of cover image.

In image steganography if we take the image or video (nothing but the frames of images) after image processing it can be images, this image nothing but set of pixels which represent the light intensities. [26]

Image compression technique is used to reduce the size of existing images by removing excess image data. There are two types of image compressions; lossy compression and loseless compression. Lossy compression reduces the size of digital image and it mostly used in 24-bit digital image. It's not exactly similar to original images it removes the redundant data and has approximation to real image. Lossy compression technique is used in JPEG format. Lossless compression technique recommend that, keeps original data as it is. Because of that lossless compression technique is mostly prefer. Lossless compression technique is mostly used for GIF and BMP formats [27, 6].

In image steganography Least Significant Bit (LSB) method is used for hiding messages. LSB technique depends on the fact that digital images nothing but the set of color and intensities. In LSB insertion is move toward to embedding data in a cover image by place the data at LSB of each picture of cover image. By using LSB method doesn't change the quality of image to human observation. [28, 29, 30]

BMP format data is capable to conceal large amount of information. But BMP is preferred when focus is on amount of data is to be transmitted instead of secrecy, similar to this data type PNG format used for image steganography. GIF format is used in LSB when embedding a reasonable amount of data in grayscale image. [31].

Multimedia files are mostly use to embed large amount of information such as video bmp and audio wav files. MPEG, JPEG, MP3 also use for steganography. [32]

In LSB algorithms having two embedding systems those are sequential and scattered. In sequential embedding that bits of message changes one by one of the image. Where as in scattered embedding there is no sequence to control the embedding sequence. In LSB 3 bits from each pixel can be hiding of each byte of 24 bit image [11].

As per the [33] image smoothness is define by statistical distribution of difference between current pixel value and neighborhood average pixel value. Spatial LSB steganography is proposed message embedding with LSB plane flipping for image smoothness.

In LSB steganography having some demerits that for extraction of secrete data requires exact binary sequence because of noisy transmission, cropping, color conversion may lost the hidden data. [34, 35]

BPCS (Bit Plane Complexity Segmentation) steganography also used for embed as much data as in cover message in bitmap format [36].

## IV. STEGANOGRAPHY APPLICATIONS

There are many applications for digital steganography of image, including copyright protection, feature tagging, and secret communication. Copyright notice or watermark can embedded inside an image to identify it as intellectual property. If someone attempts to use this image without permission, we can prove by extracting the watermark.

In feature tagging, captions, annotations, time stamps, and other descriptive elements can be embedded inside an image. Copying the stego image also copies of the embedded features and only parties who possess the decoding stego-key will be able to extract and view the features.

As proposed in paper [10] that combination of cryptography and steganography used for better security as biometric images and password in voter system. Fingerprint images taken as biometric image for steganography and password for voter account.

Mohammad Shirali-Shahreza [17] proposed that in mobile banking system data can hide by using the steganography for increase the security purpose. Secret data hide in a picture and then address of this image is given to user. When user enter correct password then only secret message can be visible to authorized user.

Data confidentiality issues can occur from increase sources such as healthcare records, criminal justice investigations and proceedings, financial institutions and transactions, residence and geographic records [21].

Typical uses of steganography are of surveillance, industrial or military. Steganalyst may be company scanning outgoing mails to avoid leaking of proprietary information, or an intelligence gatherer hoping to detect communication between adversaries [26].

On the other hand, secret communication does not advertise a covert communication by using steganography. Therefore, it can avoid scrutiny of the sender, message and recipient. This is effective only if the hidden communication is not detected by the others people. In open systems environment steganography used in convert channels, embedded data, and digital watermarking [37].

Steganography technique is possible for the hiding of biometric information for the security purposes. Iris feature can be taken as conceal information. Biometric image of iris is taken by camera and then convert into binary code which is unique for different people. At the time of extraction this code is evaluate with database information. [38]

## V. CONCLUSION AND FUTURE SCOPE

In this review paper shows the steganography technique for information hiding in secure manner, that information may be the text, audio or images but in image steganography we can hide more data as compare to the text or audio steganography. Least Significant Bit embedding method is quite simple for image steganography.

## REFERENCES

[1] Lisa M. Marvel and Charles T. Retter , Charles G. Boncelet,"A Methodology For Data Hiding Using Images", Military Communication Conference, IEEE Volume 3, PP. 1044-1047, 1998.

[2] Vidyasagar M. Potdar, Song Han, Elizabeth Chang, "Fingerprinted Secret Sharing Steganography for Robustness against Image Cropping Attacks", Third IEEE International Conference on Industrial Informatics, PP. 717-724, 2005

[3] R.Anderson and F. Petitcolas, "On the limits of steganography" IEEE Journal of Selected Areas in Communications, Vol. 16, No. 4, PP. 474-48, 1998.

[4] K.B.Raja,C.R.Chowdary,Venugopal K R, L.M.Patnaik, "A Secure Image Steganography using LSB, DCT and Compression Techniques on Raw Images", Third International Conference on Intelligent Sensing And Information Processing, PP. 171-176, 2005
[5] R. Chandramouli and N. Memon, "Analysis of LSB based image steganography techniques," International Conference on Image Processing, Thessaloniki, Greece, 2001.
[6] Bret Dunbar, "A detailed look at Steganographic techniques and their use in an open systems environment", SANS institute 2002.
[7] Mitchell D. Swanson, Mei Kobayashi, Ahmed H. Tewfik, "Multimedia Data-Embedding and watermarking Technologies", Proceedings of the IEEE, Volume. 86, No. 6, PP. 1064-1087, 1998.
[8] Mr. Vikas Tyagi, Mr. Atul kumar, Roshan Patel, Sachin Tyagi, Saurabh Singh Gangwar " Image steganography using least significant bit with cryptography", Journal Of Global Research In Computer Science, Volume 3, No. 3, March 2012
[9] Chin-Chen Chang, Tung-Shou Chen, Hsien-Chu Hsia, "An Effective Image Steganographic Scheme Based on Wavelet Transformation and Pattern-Based Modification", International Conference on Computer Networks and Mobile Computing, 2003
[10] Manoj Kumar Ramaiya, Naveen Hemrajani, Anil Kishore Saxena, "Improvisation of Security aspect in Steganography applying DES**",** International Conference on Communication Systems and Network Technologies, PP. 431-436, 2013
[11] Garima Tomar, "Effect of noise on image steganography based on LSB insertion and RSA encryption", IOSR Journal of Engineering, Volume 2(3), PP. 473-477, 2012
[12] Niels Provos, Peter Honeyman, "Detecting Steganographic Content on the Internet", Center for Information Technology Integration, 2001
[13] *Chun Shien Lu, "*Dual Security-Based Image Steganography*",* International Conference on Multimedia and Expo Volume 1, PP.489- 492, 2003
[14] Tariq Al Hawi Mahmoudai Qutayri Hassan Barada, "A Testbed For Evaluating Security And Robustness Of Steganography Techniques", In proceeding of Circuits and Systems, IEEE 46th Midwest Symposium on, Volume: 3 PP.1583-1586, 2004
[15] R Praveen Kumar, V Hemanth, MShareef, "Securing Information Using Sterganography", International Conference on Circuits, Power and Computing Technologies, 2013
[16] Mahalingam Ramkumar And Ali N. Akansu, "Capacity Estimates For Data Hiding In Compressed Images", IEEE Transactions On Image Processing, Volume 10, No. 8, PP.1252-1263, 2001
[17] Mohammad Shirali-Shahreza, "Improving Mobile Banking Security Using Steganography", International Conference on Information Technology, 2007
[18] J. J. Chae and B. S. Manjunath, "Data Hiding in Video", 6th *IEEE* International Conference on Image Processing (ICIP'99), Kobe, Japan, Volume 1, PP. *311-315 , 1999*.
[19] Stuti Goel, Arun Rana, Manpreet Kaur, Comparison of Image Steganography Techniques", International Journal of Computers and Distributed Systems Vol.ume No.3, Issue I, PP. 20-30, 2013
[20] Vandana Thakur, Monjul Saikia, "Hiding Secret Image in Video", International Conference on Intelligent Systems and Signal Processing, PP.150-153, 2013
[21] Rosziati Ibrahim and Toeh Suk Kuan, "Steganography Algorithm to hide Secret Message inside an Image", Computer Technology and Application PP. 102-108, 2011
[22] Soumyendu Das, Shubhendu Das, Bijoy Bandyopadhyay, Sugata Sanyal, "Steganography and Steganalysis: Different Approaches", International Journal of Computers, Information Technology and Engineering, Volume 2 No. 1, 2008.
[23] Deshpande Neeta, Kamalapur Snehal, Daisy Jacobs, "Implementation of LSB Steganography and Its Evaluation for Various Bits", Digital Information Management, First International Conference, PP.173-178, 2007
[24] Li Zhi, Sui Ai Fen, "Detection of Random LSB Image Steganography", Vehicular Technology Conference *IEEE* Sixtyth, Vol.3, PP. *2113 - 2117*, September *2004*.
[25] Hsiang-Kuang Pan, Yu-Yuan Chen, and Yu-Chee Tseng, "A Secure Data Hiding Scheme for Two-Color Images", Fifth IEEE Symposium on Computers and Communications, Proceedings ISCC. PP. 750-755, 2000
[26] Nitin Jain, Sachin Meshram, Shikha Dubey "Image Steganography Using LSB and Edge Detection Technique", International Journal of Soft Computing and Engineering (IJSCE), Volume-2, Issue-3, 2012
[27] V. Lokeswara Reddy, Dr A. Subramanyam, Dr. P. Chenna Reddy "Implementation of LSB Steganography and its evaluation for various file formats", Int. J. Advanced Networking And Applications, Volume 02, Issues 05, Pages 868-872, 2011.
[28] Kaustubh Choudhary, "Properties of Images in LSB plane", IOSR journal of computer engineering, Volume 3, Issue 5, pp 08-16 , 2012.
[29] Shailender Gupta, Ankur Goyal, Bharat Bhushan, "Information hiding using Least Significant Bit steganography and cryptography", I.J. Modern Education and Computer Science, pp. 27-34, 2012.
[30] Hsiang-Kuang Pan, Yu-Yuan Chen, and Yu-Chee Tseng, "A Secure Data Hiding Scheme for Two-Color Images ", Fifth IEEE Symposium on Computers and Communications, Proceedings ISCC. PP.750-755, 2000
[31] Erin Michaud, "Current steganography tools and methods", GSEC Practical, Version 1.4b, April 2003.
[32] Richard Zavaleta, Research Associate and Subbarao Wunnava, "Dynamic Steganography Adds Additional Data Security", Proceedings of IEEE SoutheastCon, PP. 3-7, 2004
[33] *Tao Zhang, Yan Zhang, Xijian Ping, Mingwu Song*, "Detection Of LSB Steganography Based On Image Smoothness", International Conference On Multimedia And Expo, PP. 1377-1380, 2006.
[34] Venkatraman.S, Ajith Abraham, Marcin Paprzycki, "Significance of Steganography on Data Security", Proceedings of the International Conference on Information Technology: Coding and Computing (ITCC'04), 2004
[35] Shivendra Katiyar, Kullai Reddy Meka, Ferdous A. Barbhuiya, Sukumar Nandi, "Online Voting System Powered By Biometric Security Using Steganography", Second International Conference on Emerging Applications of Information Technology, PP.288-291, 2011
[36] Smita P. Bansod Vanita M. Mane Leena R. Ragha, "Modified BPCS steganography using Hybrid Cryptography for Improving Data embedding Capacity", International Conference on Communication, Information and Computing Technology, October 2012
[37] Sudantha Gunawardena, Dhananjay Kulkarni, Balachandran Gnanasekaraiyer, "A Steganography based Framework to Prevent Active Attacks during User Authentication", The Eighth International Conference on Computer Science & Education, PP. 383-388, 2013.
[38] Wang Na, Zhang Chiya, Li Xia, Wang Yunjin, "Enhancing Iris-Feature Security with Steganography", Fifth *IEEE* Conference on Industrial Electronics and Applicationsis, PP.2233-2237, 2010
[39] Sorina Dumitrescu, Xiaolin Wu, "A new framework of LSB steganalysis of digital media", IEEE Transactions on Signal Processing, Volume 53, No. 10, 2005.