REVIEW OF STEGANOGRAPHY TECHNIQUES

Shivani Yadav[1], Deepak Goyal[2]
[1,2] *Department of Computer Science and Engineering,*
Vaish College of Engineering,
Rohtak-124001, India
[1] shivaniyadav17@gmail.com
[2] deepakgoyal.vce@gmail.com

Abstract-- **Steganography is the most popular technique for securing the information in the present era. Steganography 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". In this paper, we have reviewed various techniques of steganography with their advantages and disadvantages.**

KeyTerms -- **Steganography, Cryptography, Cover Image, Stego Image etc.**

I. INTRODUCTION

Steganography is a technique to hide the message in digital objects such as image, video, music, or any other computer file. This idea was first described by Simmons in 1983. More comprehension theory of steganography is given by Anderson [1]. Steganography is hiding secret information within a medium in an invisible manner. It is one such pro-security innovation in which secret data is embedded in a cover [2]. Steganography and cryptography are closely related. Cryptography is about protecting the content of messages while steganography is about concealing their very existence [3].

Steganography means Cover medium + Secret message + Stego key. The general model of data hiding can be described as follows. The embedded data is the message that one wishes to send secretly. The message is hidden in a cover-text or cover-image or cover-audio as appropriate, producing the stego-text or other stego-object. A stego-key is used to control the hiding process so as to restrict detection and /or recovery of the hidden data to parties who know it [4].

The objective of steganography is to embed the information into the cover image such that the existence of payload in the cover image is imperceptible to the human beings [5]. In any case, once the presence of hidden information is revealed or even suspected, the purpose of steganography is defeated, even if the message content is not extracted or deciphered [6]. According to Johnson & Jagodia [1], "Steganography's main purpose in security is to supplement cryptography, not replace it. If a hidden message is encrypted, it must also be decrypted if discovered, which provides another layer of protection."

Watermarking and Fingerprinting are two different applications of steganography used for different purposes as atermarking allows a person to provide hidden copyright notices or software piracy and fingerprinting uses each copy of the content and make it as unique to the receiver [7]. Digital watermarking is the special case of information hiding and Febriano, Italy is considered as its birth place [8]. Tirkel et al [9] introduced the world "water marks" which became "watermarks" later on, digital water marking is the process of embedding information into digital media content such that the information (the watermarks) can later be extracted or detected for a variety of perposts including copy prevention and control. Digital watermarking is becoming an important area of research and development. It helps in addressing some of the challenges faced by the rapid explosion of digital content. Water marking is emerging as an efficient method for protecting digital elements such as image, video and sound [8], [9], [10]. Finger printing technique was introduced to prevent the piracy of digital objects or we can say, illegal copying of digital objects such as software, multimedia objects. In this technique, a fingerprint (a distinct mark) is inserted in each digital object, which is some way related to buyer. In future, if an unauthorized copy of digital object is found then its origin can be recovered by retrieving the unique fingerprinting contained in it. The fingerprint is embedded into digital a object which makes it difficult for buyers to make any changes in it. This technique has emerged with some problems which were firstly introduced by Wagner [11] and still the work is going on for making it best technique.

II. HISTORY

In ancient times, steganography was messy and was sent on foot. For secret communication, you had two options i.e. have

Herodotus (485-525BC)

the messenger memorize it, or hide it on the messenger. According to Greek historian Herodotus, the famous Greek tyrant Histiaeus, while in prison, for sending the message to his son-in-law, shaved the head of a slave to tattoo a message on his scalp. Hisatiaeus then waited until the hair grew back on slave's head prior to sending him off to his son-in-law. Wooden tablet covered with wax was also used for secret communication. Pliny the Elder explained how the milk of the thithymallus plant dried to transparency when applied to paper but darkened to brown when subsequently heated, thus recording one of the earliest recipes for invisible ink. The Ancient Chinese wrote notes on small pieces of silk that they then wadded into little balls and coated in wax, to be swallowed by a messenger and then retrieved [12].

In middle age Johannes Trithemius was considered as the founders of modern cryptography. His three volume work Steganographia, described an extensive system for concealing secret messages within innocuous texts and in the 16th century Steganographia was only circulated privately until publication in 1606. The earliest actual book on steganography was a four hundred page work written by Gaspari Schott in 1665 and called Steganographica. His idea was to send the message without the knowledge of the messenger that he is carrying the message. He also described hiding the message in living creature, for example by feeding a letter in meat to a dog and then killing him to retrieve it. Later, chemical effected sympathetic inks were developed.

In modern era, during 1883 and 1907, Auguste Kerckhoff (author of Cryptographic Militaire) and Charles Briquet (author of Les Filigranes) books can be attributed to the foundation of some steganographic systems and more significantly to watermarking techniques. Photography permitted a great reduction in images, so a page could be made very small. This technique was successfully used during World War II for secret communication. During World War II, Great Britains BBC generally used steganography as phrase in their radio as "The chair is against the wall" were interspersed within radio broadcasts. Only groups or individuals who knew that the phrase "The chair is against the wall" meant that Allies were expecting to bomb a particular city tomorrow were able to decode the information. Simmon was first to present a paper in 1983, about secret communication regarding prisoners communication [13]. Adelson described a method of data hiding that exploits the human visual system's varying sensitivity to contrast versus spatial frequency. He substituted high-spatial frequency image data for *hidden* data in a pyramid-encoded still image. While he was able to encode a large amount of data efficiently, there was no provision to make the data immune to detection or removal by typical manipulations such as filtering and rescaling [14]. Bender modified Adelson's technique by using *chaos* as a means to encrypt the embedded data, deterring detection, but providing no improvement to immunity to host signal manipulation [15]. The use of Steganography techniques for hiding copyright marks, tamper proofing information and annotations in sound and images is studied by [16]. [17] proposed another approach for embedding in spatial domain. In their method, noise that statistically resembles common processing distortion, e.g., scanner noise, or digital camera noise, is introduced to pixels on a random walk. The noise is produced by a pseudo random noise generator using a shared key. A parity function is designed to embed and detect the message signal modulated by the generated noise.

III. CRITERIA OF STEGANOGRAPHY

Any Steganographic technique is judged on basis of following criteria [18]:

A. Invisibility – 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 [19].

B. *Payload capacity* – Information, Steganography requires sufficient embedding capacity [20].

C. *Robustness against statistical attacks* – Many Steganographic algorithms leaves a "signature" when embedding information that can be easily detected through statistical analysis. A Steganographic algorithm must not leave such a mark in the cover data as be statistically significant [21].

D. *Robustness against cover data manipulation* –The cover data may undergo changes by an active warden in an attempt to remove hidden information. Depending on the manner in which the message is embedded, these manipulations may destroy the hidden message. It is preferable for Steganographic algorithms to be robust against either malicious or unintentional changes to the image [21].

E. *Independent of file format* –The most powerful Steganographic algorithms thus posses the ability to embed information in any type of 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 [21].

F. *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.

Unfortunately hardly any algorithms fulfill these requirements. Thus a trade off will exist in most cases, depending on which requirements are more important for the specific application [22].

IV. LITERATURE SURVEY

Authors	Year of Publication	Technique	Advantages	Disadvantages
R.Chandramouli et.al.[23]	2001	Adaptive Steganography	Imperceptibility	Not optimal Data Hiding
Hideki Noda et.al.[24]	2002	BPCS steganography with compressed images	Image Quality is Good	Effected by various types of noises
Po-Chyi et.al.[25]	2003	Steganography in JPEG 2000 compressed images	Controllable distortion Can embed high Volume data.	Complexity is high
Zhicheng Ni et.al.[26]	2004	Lossless Data Hiding	No salt pepper Noise Can resist JPEGcompression 1024/512 bits	Other noise can effect hidden data
H. Motameni et.al.[27]	2007	LSB substituting on Dark region of Image	Useful for smooth region with solid boundary of object based dataset	High computation required and not tested on high texture areas
M. Tanvir Parvez and A. Abdul-Aziz Gutub [28]	2008	Pixel indicator with variable LSB substitution	Almost Same histogram of stego-image against cover image	Hidden capacity depended on Cover image pixel intensities
H. Zhang Et.al.[29]	2009	PVD with Adaptive LSB	Histogram of cover and stego image is almost same	Dataset for Experiments is too small
Fangjun Huang and Jiwu Huang[30]	2010	Edge adaptive scheme which can choose the embedding regions	Enhance the security significantly	Less data Hiding
Yadav et.al[31]	2010	Parity of pixel bits are used for message insertion & retrieval	Easy to implement	No Noise Control
Zhihua Xia, et al [32]	2011	LSB matching steganography in gray images	Reliable detection ability	Intruder can easily distort the message
Rajkumar Yadav et al.[33]	2011	A novel approach for image steganography In spatial domain	Limited changes In cover-image.	Effected by various types of Noises

		using last two bits of pixel value		
S.Shanmuga Priya et. al [34]	2012	Embedding done in the sharper edge regions using a threshold	Better performance in terms of distortion and resistance against existing steganalysis	Non adaptive technique has more PSNR & less MSE than adaptive technique.
P.Thiyagarajan et.al [35]	2013	Scheme using 3D geometric models.	Resistance against uniform affine transformations such as cropping, rotation & caling.	High Complexity
Jose and Abraham[36,37]	2013	Image encryption Chaotic sequence	High embedding capacity	More Computation Time

V. IMAGE STEGANOGRAPHIC TECHNIQUES

Image steganography techniques can be divided into following domains.

A. *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. Changes in the value of the LSB are imperceptible for human eyes. Spatial domain techniques are broadly classified into[38]:

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

B. *Transform Domain Technique:* This is more complex method of hiding information in an image.Transform domain embedding can be termed as a domain of embedding techniques for which a number of algorithms have been suggested.[39]. Transform domain techniques are broadly classified into:

1Discrete 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

C. *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 [40].

D. . *Masking and Filtering*: These techniques hide information by marking an image. It embeds the information in the more significant areas than just hiding it into the noise level. The hidden message is more integral to the cover image.

VI. CONCLUSION AND FUTURE SCOPE

In this paper, I reviewed different steganographic techniques. Due to the emerging growth of Internet, security is an important issue. So, Steganography is a technique which hides the existence of the message. Every technique after sometime shows the indication of alterations in it. So making a strong steganalysis technique is a continuous process and still going on.

REFERENCES

[1]. N.F.Johnson and S.Jagodia, "Exploring Steganography: Seeing the Unseen", IEEE Computer, Vol. 31, no 2, pp. 26-34, Feb. 1998.

[2]. S.Katzenbeisser and F.A.P.Petitcolas, Information Hiding Techniques for Steganography and Digital Watermarking, Artech House, Norwood, MA, 2000.

[3]. S. Katzenbeiser and F.A.P.Petitcolas, Information Hiding Techniques for Steganography and Digital Watermarking, Artech House, Computer Security Series, Boston, London, 1999.

[4]. F.A.P.Petitcolas, R. J.Anderson and M.G.Kuhn, "Information Hiding – A Survey", in *Proc. Of IEEE*, Special Issue on Protection of Multimedia Content, pp.1062-1078, 1999.

[5]. K.S.Babu, K.B.Raja, K.K.Kumar, T.H.M.Devi, K.R.Venugopal, and L.M.Patnaik, "Authentication of Secret Information in Image Steganography", TENCON 2008 - 2008 IEEE Region 10 Conference, pp 1-6.

[6]. P.Goel, “Data Hiding in Digital Images: A Steganographic Paradigm” M.Tech thesis

[7]. R.Poornima and R.J.Iswarya ,” An Overview Of Digital Image Steganography”, International Journal of Computer Science & Engineering Survey (IJCSES) Vol.4, No.1, pp. 23-31, February 2013.

[8]. T.Y.Nakamura, and K. Matsui, “Embedding secret information into a dithered multilevel image”, in *Proc. Of IEEE Military Communication Conference*, pp. 216-220, 1990.

[9]. K.Tanaka, Y.Nakamura, and K.M. Members, Embedding the attribute information into a dithered image, Syst. Comput. Japan, Vol. 21, no. 7, pp. 43-50, 1990.

[10]. A. Tirkel, G. Rankin, R. Van Schyndel, W. Ho, N. Mee, and C. Osborne, “Electronic water mark”, in *Proc. DICTA*, pp. 666-672, Dec. 1993.

[11]. N.R. Wagner, “ Fingerprinting”, *Proc. Of the Symposium on Security and Privacy, IEEE Comp. Society*, pp. 18-22, 1983.

[12]. G.J.Simmons, *Contemporary Cryptology: The Science of Information Integrity*. Piscataway, NJ: IEEE Press, 1992.

[13]. G.J.Simmon, Prisoners' problem and the subliminal channel. In: *Advances in Cryptology: Proceedings of CRYPTO 83*. D. Chaum, ed. Plenum, New York, 1983, pp. 51-67.

[14]. E. Adelson, *Digital Signal Encoding and Decoding Apparatus*, U.S. Patent No. 4,939,515, 1990.

[15]. W. Bender, “Data Hiding,” News in the Future, MIT Media Laboratory, unpublished lecture notes, 1994.

[16]. W. Bender, D. Gruhl, N. Morimoto and A. Lu, Techniques for data hiding, I.B.M. Systems Journal, Vol. 35, no. 3&4, pp. 313–336, 1996.

[17]. J. Fridrich and M. Goljan, “Digital Image Steganography Using Stochastic Modulation,” in E. Delp (ed.): Proc. SPIE Electronic Imaging, Security, Steganography, and Watermarking of Multimedia Contents V, vol. 5020, pp. 191–202, 2003.

[18]. S.K.Bandyopadhyay, D.Bhattacharyya, D.Ganguly, S.Mukherjee and P. Das, A Tutorial Review on Steganography, IC3-2008 UFL and JIITU, pp. 105-114, 2008.

[19]. Z.Hrytskiv, S.Voloshynovskiy and Y. Rytsav, Cryptography and steganography of video information in modern communication, Electronics and Energetics, Vol 11, No. 1, 115-225. 1998.

[20]. Dean Lewandowski, Mike Palmisano., Steganography

[21]. C. Badgaiyan, A.K. Dewangan, B.K. Pandey, K. Yeulkar and K. K.Sinha, A new steganographic technique: image hiding in mobile application, International Journal of Advanced Computer and Mathematical Sciences, Vol 3, no. 4, pp. 556-562, 2012.

[22]. K. Ahsan, and D. Kundur, “Practical Data hiding in TCP/IP”, *Proc. of the Workshop on Multimedia Security at ACM Multimedia*, 2002.

[23]. R.Chandramouli and N. Memon, Analysis of LSB Based Image Steganography Techniques, IEEE Article, Vol. 3, pp. 1019-1022. Oct. 2001.

[24]. H.Noda, J.Spaulding, M.N.Shirazi and E.Kawaguchi, Application of bit- plane decomposition steganography to JPEG 2000 encoded images, IEEE Signal Processing Letters, Vol 9, no.12, pp. 410-413, Dec. 2002.

[25]. Po-Chyi and C.-C.Jay Kuo, Steganography in JPEG 2000 Compressed Images, IEEE Transactions on Consumer Electronics, Vol. 49, No. 4, pp 824-832, 2003.

[26]. Z. Ni, Y. Q.Shi, N. Ansari, Wei Su, Q. Sun and X. Lin, Robust Lossless Image Data Hiding, ICME, pp 2199-2202, 2004.

[27]. H. Motameni, M. Norouzi, M. Jahandar and A. Hatami, Labeling Method in Steganography, World Academy of Science, Engineering and Technology, Vol. 30, pp. 349-354, 2007.

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

[29]. H. Zhang, G. Geng, and C. Xiong, Image steganography using pixel-value differencing, in Electronic Commerce and Security, 2009. ISECS'09. Second International Symposium on, vol. 2, pp. 109-112, IEEE, 2009.

[30]. F. Huang and J. Huang, Edge adaptive image steganography based on LSB matching, Information Forensics and Security, IEEE Transactions, Vol. 5, No. 2, June 2010.

[31]. R. Yadav, R. Rishi and S. Batra, A new steganography method for gray level images using parity checker, International Journal of Computer Applications, Vol. 11, no. 11, pp. 18-24, December 2010.

[32]. Z. Xia, L. Yang, X. Sun, W. Liang, D. Sun and Z. Ruan, A learning-based steganalytic method against LSB matching steganography, Radio Engineering, Vol. 20, no. 1, pp. 102-109, April 2011.

[33]. R. Yadav, A novel approach for image steganography in spatial domain using last two bits of pixel values, International Journal of Security, Vol. 5, no. 2, pp. 51-61, 2011.

[34]. S. S. Priya, K. Mahesh and Dr. K. Kuppusamy, Efficient steganography method to implement selected least significant bits in spatial domain, International Journal of Engineering Research and Applications, Vol. 2, no. 3, pp. 2632-2637, 2012.

[35]. P. Thiyagarajan, V. Natarajan, G. Aghila, V. P. Venkatesan and R. Anitha, Pattern based 3D image steganography, 3D Research, Vol. 4, no. 1, pp.1-8, 2013.

[36]. R. Jose and G. Abraham, A seperable reversible data hiding in encrypted image with improved performance, “Emerging Research Areas and 2013 International Conference on Microelectronics, Communication and Renewable Energy (AICERA/ICMiCR)”, pp. 1-5, 6 June 2013.

[37]. Sandeep Singh, Aman Singh, A review on the various recent steganography techniques, International Journal of Computer Science and Network, Vol. 2, no. 6, pp. 142-156, December 2013.

[38]. M. Hussain and M. Hussain, A survey of image steganographic techniques, International Journal of Advanced Science and Technology Vol. 54, pp. 113-123, May 2013.

[39]. N. F. Johnson and S. Katzenbeisser, “A Survey of steganographic techniques. in Information Hiding Techniques for Steganography and Digital Watermarking, S. Katzenbeisser and F. Petitcolas, Ed. London: Artech House, pp. 43-78, 2000.

[40]. H. S. Majunatha Reddy and K. B. Raja, High capacity and security steganography using discrete wavelet transform, International Journal of Computer Science and Security, Vol. 3, no. 6, pp. 462-472, 2009.