ISSN No. 0976-5697

Volume 5, No. 3, March-April 2014

International Journal of Advanced Research in Computer Science

RESEARCH PAPER

Available Online at www.ijarcs.info

A Critical Study of Image based Steganographic Techniques for Information Hiding

Vandana Yadav*
M.Tech, Computer Science & Engineering
Galgotia University
Gr. Noida, UP, India

Amandeep
M.Tech, Computer Science & Engineering
Galgotia University
Gr. Noida, UP, India

Neeraj Rai
M.Tech, Automation & Robotics
Ajay Kumar Garg Engineering College
Ghaziabad, UP, India

*Abstract***:** In present scenario the security of the confidential information has become an important issue. It has become a challenge as the large amount of data is exchanged on the internet. To protect these data from unauthorized access and tampering various methods for data hiding like cryptography, hashing, authentication, watermarking, etc. have been developed and are in practice today. In this paper we will be discussing one such data hiding technique called Steganography. Steganography is a tool for hiding information inside an image. For hiding secret data in digital images, large varieties of steganographic techniques are available, some are more complex than others, and all of them have their respective pros and cons. This paper intends to give thorough understanding and evolution of different existing digital image steganography techniques of data hiding in spatial, transform and compression domains. It covers and integrates recent research work without going in to much detail. The survey results show that the steganography has played a very beneficial role in various applications. It increased the level of information security with a wide use of its techniques. It would be very useful and provide a better platform for the beginners who want to work in steganography.

Keywords: Steganography; digital image steganography; cover image; stego image; data hiding; information security.

I. INTRODUCTION

In the present scenario the communication of the multimedia data has increased to a large extent. With this increase of multimedia communication the security of these data becomes important; as because there is the huge rise of World Wide Web. And as we know that the internet users frequently need to store, send, or receive data and information, this calls up for the creation of methods to protect these digital information against unauthorized access and manipulation.

Information security means protecting information and information systems from unauthorized access, use, disclosure, disruption, modification or destruction. The terms information security, computer security and information assurance are being used frequently interchangeably. These fields are interrelated and share the common goals of protecting the confidentiality, integrity and availability of information.

There are various available techniques for protecting the data and information, these are:

(a). Cryptography
(b). Hashing
(c). Steganography, etc.

These are very different in practice.

A. Cryptography:

In cryptography we basically do the complete conversion of our original data into a new unreadable format so that intruders cannot find original data.

B. Hashing:

In hashing we use some mathematical functions and transformations to irreversibly encrypt our original data and information [1].

C. Steganography:

But, Steganography is basically the art of writing hidden messages in such a way that no one other than the sender and authorized recipient knows the existence of the message.

This is basically the form of security through obscurity [2].

The key concern of this paper is to critically review the different data hiding and steganography techniques using digital images as shown in the figure 1. The motivation for this work includes provision of protection of information during transmission without any detection of information. Keeping the key focus as pivot this study proceeds in different sections: section I provide the brief introduction of the technique, section II reviews the literature work, section III provides different steganographic techniques, section IV concludes the study and finally, section V gives the references cited in this study.

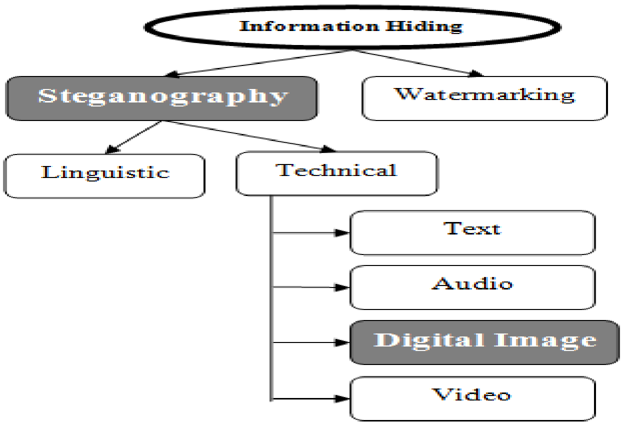

Figure.1. Different information hiding techniques

D. *Data hiding and Steganography:*

Data hiding is a method of hiding secret messages into a cover-media such that an unintended observer cannot know the existence of the hidden messages. Steganography is the practice of hiding secret message within any media. Steganography is often confused with cryptography because the two are similar in the way that they both are used to protect secret information. If both the techniques: cryptography and steganography is used then the communication becomes double secured. The word "steganography" is basically of Greek origin which means "hidden writing". The word is classified into two parts: steganos which means "secret" and "graphic" which means "writing". However, in hiding information, the meaning of steganography is hiding text or secret messages into another media file such as image, text, sound or video. The primary objective of steganography is to avoid drawing attention to the transmission of hidden information. Steganographic techniques allow communication between two authorized parties without an observer being aware that the communication is actually taking place [3].

The basic terminologies used in the steganography systems are:

a. Cover message,
b. Secret message,
c. Secret key, and,
d. Embedding algorithm.

The cover message is the carrier of the message such as image, video, audio, text or some other digital media. The secret message is the information which is needed to be hidden in the suitable digital media. The secret key is usually used to embed the message depending on the hiding algorithms. The embedding algorithm is the way or the idea that usually used to embed the secret information in the cover message.

In steganography, the possible cover carriers can be:

(a). Images,
(b). Audio,
(c). Video,
(d). Text, or,
(e). Some other digitally representative code.

The hidden message may be:

(a). Plaintext,
(b). Cipher text,
(c). Images, or,
(d). Anything that can be embedded into a bit stream.

In steganography, before the hiding process, the sender must select an appropriate message carrier, an effective message to be hidden as well as a secret key used as a password. A robust steganographic algorithm must be selected that should be able to encrypt the message more effectively. The sender then may send the hidden message to the receiver by using any of the modern communication techniques. The receiver after receiving the message decrypts the hidden message using the extraction algorithm and a secret key.

For example, when a secret message is hidden within a cover image, the resulting product is a stego-image. A possible formula of the process may be represented as:

cover medium + embedded message + stego key = stego-medium

E. *Advantage of Steganography:*

The advantage of steganography is that it can be used to secretly transmit messages without the fact of the transmission being discovered. Often, using encryption might identify the sender or receiver as somebody with something to hide. For example, the picture of our cat could conceal the plans for our company's latest technical innovation.

F. *Limitations of Steganography:*

If we only use Steganography, data become invisible, but methodical analysis of all possible files, will lead to disorder of data and searching for hidden data, would make it possible to uncover the data.

G. *Application of Steganography:*

It finds its main application in the field of secret communication. It can be used by intelligence agencies across the world to barter highly confidential data in a secret media, e.g. a secret agent can hide a map of a terrorist camp in a photograph using image steganographic software and post it on a forum. An officer from the head office could download the photograph from the forum and easily retrieve the hidden map. These techniques have many Army applications in the defensive information warfare arena, such as hidden communication, in-band captioning, and tamper proofing.

II. LITERATURE REVIEW

History of steganography dates back to 440 B.C. this technique was initiated by ancient Greeks, they shave the heads of their slaves and write the messages on their heads, after the hair had grown back, the slaves were sent to their allies without the enemies knowledge. Steganography was also used by Germans during the World War I and II. Also during the American Revolution, invisible ink was used by the revolutionaries for communication purposes. The motto behind developing steganographic methods was its application in secret communication between the members of an organization involved in mission critical situations like wars; also it can be used for communication between intelligence agencies etc.

The field of information security has grown and evolved significantly in recent years. It offers many areas for specialization including: securing networks and allied infrastructure, securing applications and databases, security testing, information systems auditing, business continuity planning and digital forensics science, etc.

The introduction of the various processes of the last decades have continuously pointed out towards the security requirement levels, especially since the massive utilization of personal computers, networks and the internet with its availability. Many techniques have been developed for avoiding theft of data, controlling quantities of possible copies. These techniques used for data hiding are: Cryptography, Digital Watermarking, Steganography, etc.

Cryptography is the practice and study of hiding information. The word cryptography is derived from the Greek word kryptos, which means hidden. The origin of cryptography is usually dated from about 2000 BC. The first known use of a modern cipher was by Julius Caesar (100 BC to 44 BC) [4], who did not trust his messengers when communicating with his governors and officers. For this reason, he created a system in which each character in his messages was replaced by a character three positions ahead of it in the Roman alphabet. In modern times, cryptography is considered a branch of both mathematics and computer science and is affiliated closely with information theory, computer security and engineering. Cryptography is used in applications present in technologically advanced societies. Its examples include the security of ATM cards, computer passwords and electronic commerce, which all depend on cryptography.

Digital watermarking involves embedding of an invisible structure in a host signal to mark its ownership. It may be comprised of copyright or authentication codes or a legend essential for signal interpretation. The existence of these watermarks within a multimedia signal goes unnoticed except when passed through an appropriate detector. Common types of signals to watermark are still images, audio and digital video. To be effective a watermark must be:

a. Unobstructive,
b. Easily extracted, and,
c. Robust or fragile to incidental and unintentional distortions.

We are currently in an evaluation phase of the technology in which researchers are developing general guidelines for effective watermarking algorithm design, improving reliability within the constraints of computational complexity and tailoring to the constantly changing needs of multimedia industries. Although there are commercially available digital watermarking systems, the area is still in its infancy. Traditionally, it takes a cryptographic system ten to twenty years to be adopted for general use. What makes watermarking a formidable problem is the urgency to incorporate it within the disparate objectives of multimedia applications. There is the limitation of watermarking i.e. if someone is interested in breaking the security mechanism imposed in watermarking can easily accomplish it by just replacing lines, replacing words or reshaping characters.

Steganography is a very old method of passing messages in secret. This method of message cloaking goes back to the time of the ancient Greeks. The historian Herodotus [3] has written about how an agent wrote a message warning of an invasion on the wood part of a wax tablet. Since, messages were normally inscribed in the wax and not the wood, the tablet appeared blank to a common observer. There is also the story of a messenger during the Persian Wars who shaved his head and had a message tattooed on it. He waited until his hair grew back to make his journey. When he arrived at his destination, he shaved his head to reveal the message [5]. During World War II, spies on both sides used “invisible” inks. These inks were fluids such as milk, fruit juice or urine that would darken when heated. They also sent messages with very small punctures above characters in a document that formed a message when combined. Almost all digital file formats can be used for steganography [6], but the formats that are more suitable are those with a high degree of redundancy. Redundancy can be defined as the bits of an object that provide accuracy far greater than necessary for the object’s use and display. The redundant bits of an object are those bits that can be altered without the alteration being detected easily. Image and audio files especially comply with this requirement, while research has also uncovered other file formats that can be used for information hiding.

In past few years a large number of algorithms for Image Steganography have been developed. A broad range of embedding algorithms goes from simple Least Significant Bit (LSB) methods to various spread spectrum schemes. We will now discuss different image steganographic techniques.

III. STUDY OF STEGANOGRAPHIC TECHNIQUES BASED ON DIGITAL IMAGES

In today’s scenario almost all digital file formats can be used for steganography, however only those with a high degree of redundant bits are preferred. The steganographic techniques are classified based on the types of cover files as shown in fig2.

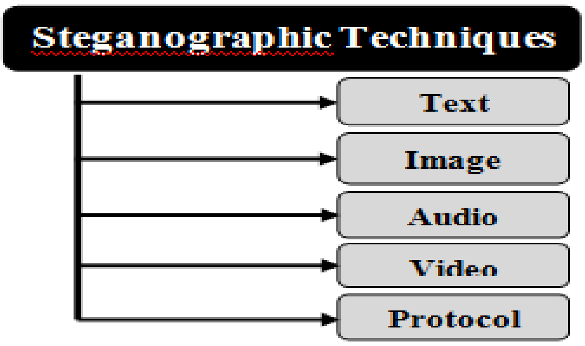

Figure.2. Different steganographic techniques

In this paper we will focus only on the Image based steganographic techniques. The larger size of audio and video files makes them less popular as compared to images. The term protocol steganography refers to embedding information within network protocols such as TCP/IP.

Image based steganographic techniques are classified into three main parts as shown in fig3.

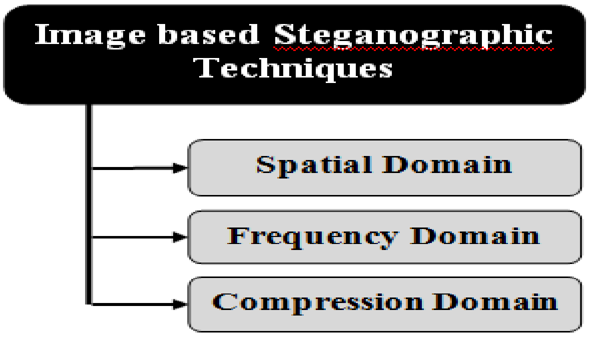

Figure.3. Image based steganographic techniques

A. Spatial domain based image steganographic techniques:

In Spatial domain, cover-image is first decomposed into bits planes and then least significant bit (LSB) of the bits planes are replaced with the secret data bits. Several Spatial domain based image steganographic techniques are shown in fig4.

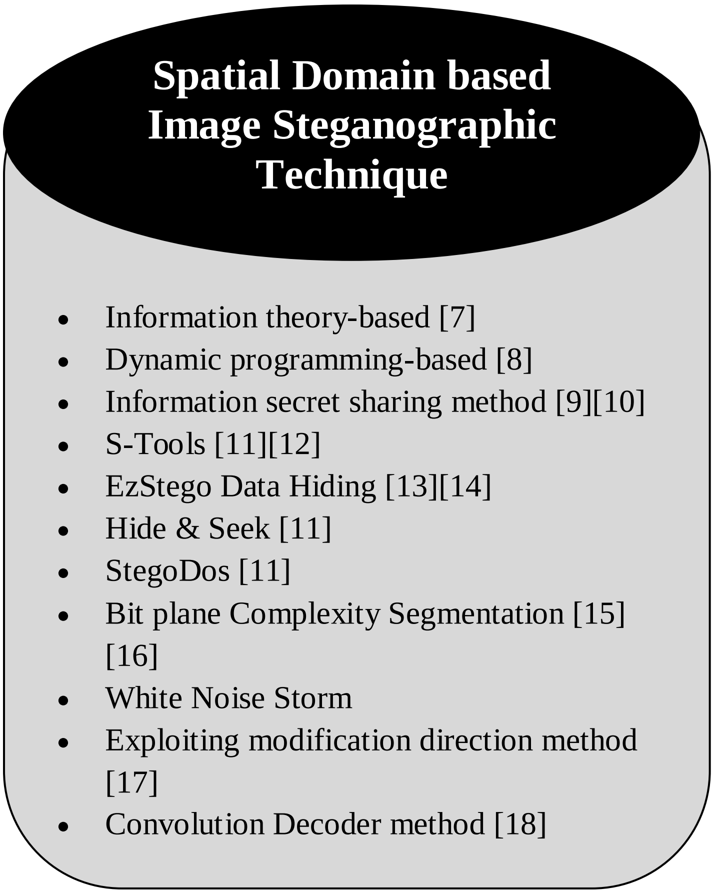
Spatial Domain based Image Steganographic Technique
Information theory-based [7]
Dynamic programming-based [8]
Information secret sharing method [9][10]
S-Tools [11][12]
EzStego Data Hiding [13][14]
Hide & Seek [11]
StegoDos [11]
Bit plane Complexity Segmentation [15] [16]
White Noise Storm
Exploiting modification direction method [17]
Convolution Decoder method [18]

Figure.4. Spatial Domain based image steganographic technique

B. Frequency domain based image steganographic techniques:

In Frequency domain embedding techniques, firstly the cover-image is transformed into its frequency domain and then the secret data is embedded in frequency coefficients. Several Frequency domain based image steganographic techniques are shown in fig5.

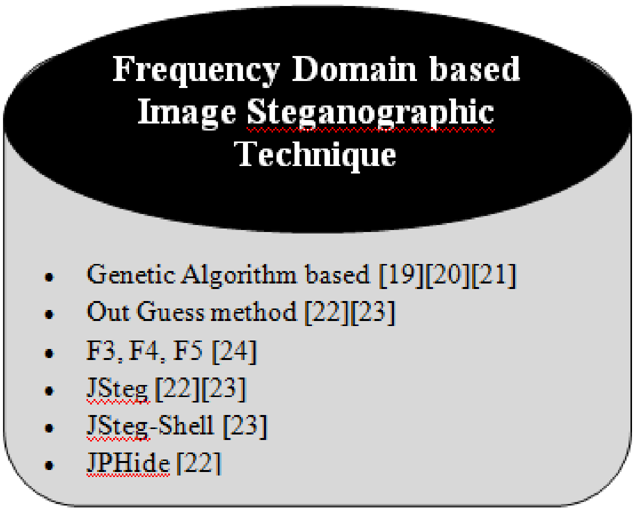
Frequency Domain based Image Steganographic Technique
Genetic Algorithm based [19][20][21]
Out Guess method [22][23]
F3, F4, F5 [24]
JSteg [22][23]
JSteg-Shell [23]
JPHide [22]

Figure.5. Frequency Domain based image steganographic technique

C. Compression domain based image steganographic techniques:

In compression domain, secret data is embedded into compression codes of the cover-image which is then sent to the receiver. It is of paramount importance where bandwidth requirement is a major concern. Several compression domain based image steganographic techniques are shown in fig6.

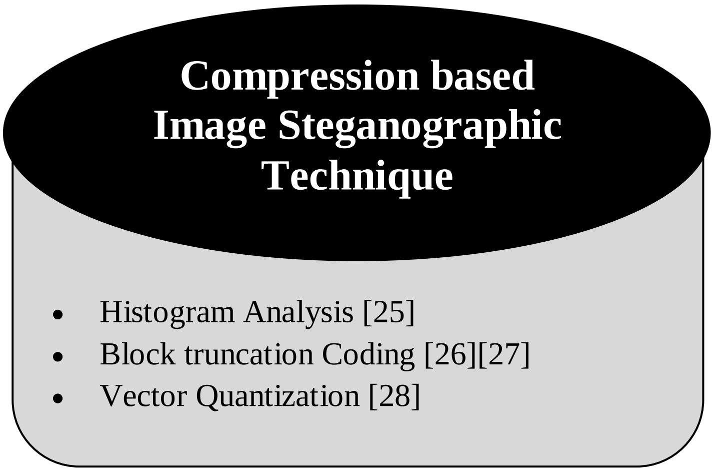
Compression based Image Steganographic Technique
Histogram Analysis [25]
Block truncation Coding [26][27]
Vector Quantization [28]

Figure.6. Compression domain based image steganographic technique

Some other important techniques proposed in recent past are as follows:

a. In 2013, C.R. Geetha, et.al. Proposed a variable load image steganography using multiple edge detection and minimum error replacement method. It is advantageous as it gives good visual qualities and highest embedding capacity with high security [29].
b. In 2013, S. Mahato, et.al. Proposed a modified approach to text steganography using HTML. It is advantageous as steganography is achieved easily by HTML as HTML is rich in code and very less chance to check its source code and easily communicated through internet [30].
c. In 2013, M.K. Ramaiya, et.al. had given an improvisation of security aspect in steganography using DES. It is advantageous as high level of security is provided and variation in only two LSB bits of each pixel do not affect the quality of the cover image [31].
d. In 2013, S. Thenmozhi, et.al. Proposed a novel approach for image steganography using non-linear chaotic map. It is advantageous as it provides high capacity and good invisibility as the secrete message cannot be extracted. And also it removes the outlines of the encrypted images completely [32].
e. In 2012, S. Das, et.al. Proposed a secured key-based digital text passing system through color image pixels. It is advantageous as through digital colour images hidden text passing is very efficiently done and embedded text is completely invisible in the encrypted images [33].
f. In 2012, A. Sanchez, et.al. Proposed a new approach to relatively short message steganography. It is advantageous as the sending of message and receiving of the original message are treated equally [34].
g. In 2011, M. Nosrati et.al. Proposed a steganographic technique in which the secret message was embedded in 24-bit color image using the concept of the linked list data structures. In this the random embedding of data in image was done

and the data was linked together. It is advantageous as because the attacker is unable to guess the next message as the data is not hidden sequentially. Also, without the password it is not possible to access the hidden data [35].

h. In 2011, M. Naseem et.al. Proposed an optimum modified bit plane slicing LSB algorithm for secret data hiding. In this the pixels are grouped based on their intensity and then the number of bits are to represent the hidden data are chosen. It is advantageous as the bits are grouped based on the intensity of the pixels, more number of darker intensity pixels can be used to represent the hidden data than just the LSB [36].

IV. CONCLUSION

In this paper, we examined the available image based steganographic techniques deployed in spatial, frequency, and compression domains of digital images. We presented some differences between steganography, cryptography, watermarking and hashing. We also surveyed various data hiding techniques in image steganography. In the survey we find that most of the papers used the LSB technique, especially in 2012 and 2013 maximum papers are based on LSB steganography technique, also some researchers used some cryptographic techniques along with steganography techniques and several other techniques were also used. This paper does not act as torch bearer rather it provides some prior knowledge to the beginners who want to work in steganography. Through this paper the beginners will surely get some ideas for the future research in steganography. From this paper it is evident that steganography has numerous useful applications and will remain the point of attraction for researchers in future as well.

V. REFERENCES

[1] Phad Vitthal S., Bhosale Rajkumar S., Panhalkar Archana R. , ‖ A Novel Security Scheme for Secret Data using Cryptography and Steganography‖ in I. J. Computer Network and Information Security, March 2012.

[2] Jayaram P, Ranganatha H R, Anupama H S ―INFORMATION HIDING USING AUDIO STEGNOGRAPHY – A SURVEY‖, The International Journal of Multimedia & Its Applications (IJMA) Vol.3, No.3, August 2011

[3] Herodotus, "The Histories, chap. 5 - The Fifth Book Entitled Terpsichore, 7 - The Seventh Book Entitled Polymnia", J. M. Dent & Sons, Ltd, 1992.

[4] http://en.wikipedia.org/wiki/Cryptography

[5] J. Caldwell, "Steganography", United States Air Force, http:// www.stsc.hill.af.mil /crosstalk/2003/06/caldwell.pdf, June 2003.

[6] http://technology-flow.com/articles/steganography/

[7] Hadhoud, M.M.; Ismail, N.A.; Shawkey, W. & Mohammed, A.Z. Secure perceptual data hiding technique using information theory. In the International Conference on Electrical, Electronic and Computer Engineering (ICEEC), Egypt, 2004, pp. 249-253.

[8] Mielkiainen, J. LSB Matching revisited. IEEE Signal Proc. Letters, 2006, **13**(5), 285-87.

[9] Shamir, A. How to share a secret. Communication of the ACM, 1979, **22**, 612-13.

[10] Lee, C.W. & Tsai, W.H. A new steganographic method based on information sharing via PNG images. In the 2nd International Conference on Computer and Automation Engineering (ICCAE), Singapore, 2010, 807-11.

[11] Johnson, N.F. & Jajodia, S. Exploring steganography:Seeing the unseen. IEEE Computer, 1998, **31**(2), 26-34.

[12] Westfeld, A.; Pfitzmann A. Attacks on steganographic systems breaking the steganographic utilities EzStego, Jsteg, Steganos, and S-tools—and some lessons learned. In the 3rd International workshop on Information hiding, Dresden, Germany, 1999, Springer, pp. 61-76.

[13] Machado, R. EzStego, Stego Online. http://www.stego.com (Accessed on 15 April 2011).

[14] Johnson, N.F. & Jajodia, S. Exploring steganography: Seeing the unseen. IEEE Computer, 1998, **31**(2), 26-34.

[15] Kawaguchi, E. & Eason, R.O. Principle and applications of BPCS-Steganography. In the SPIE Conference on Multimedia Systems and Applications, Boston, 1998, **3524**, pp. 464-73.

[16] Maya, S.T.; Miyatake, M.N. & Medina, R.V. Robust steganography using bit plane complexity segmentation. In the 1st International Conference on Electrical and Electronics Engineering, 2004. Mexico, pp. 40-43.

[17] Zhang, X. & Wang, S. Efficient steganographic embedding by exploiting modification direction. IEEE Communications Letters, 2006, **10**(11), 781-83.

[18] Daneshkhah, A.; Aghaeinia, H. & Seyedi, S.H. A More secure steganography method in spatial domain. In the 2nd International Conference on Intelligent Systems, Modeling and Simulation (ISMS), 2011, pp. 189-94.

[19] Li, X. & Wang, J. A steganographic method based upon JPEG and particle swarm optimisation algorithm. Information Sciences, 2007, **177**(3), 99-109.

[20] Elbeltagi, E.; Hegazy, T. & Grierson, D. Comparison among five evolutionary-based optimisation algorithms. Adv. Engg. Informatics, 2005, **19**(1), 43-53.

[21] Fazli, S. & Kiamini, M. A high performance Steganographic method using JPEG and PSO algorithm. In the IEEE International Multitopic Conference, INMIC 2008.

[22] Provos, N. & Honeyman, P. Hide and seek: An introduction to steganography. IEEE Security Privacy, 2003, **1**(3), pp. 32-44.

[23] Provos, N. & Honeyman, P. Detecting steganographic content on the internet. ISOC NDSS'02, San Diego, CA, 2002.

[24] Westfeld, A. F5—A steganographic algorithm: High capacity despite better steganalysis. In the Proceedings of 4th International Workshop Information Hiding, Springer-Verlag, 2001, pp. 289-302.

[25] Keissarian, F. Using a novel variable block size image compression algorithm for hiding secret data. In the IEEE International Conference on Signal Image Technology and Internet Based Systems, Bali, 2008. pp. 285-292.

[26] Wu, X. & Sun, W. Data hiding in block truncation coding. In International Conference on Computational Intelligence and Security, 2010.

[27] Delp, E. & Mitchell, O. Image compression using block truncation coding. IEEE Trans. Comm., 1979, **27**(9), 1335-342.

[28] Gray, R.M. Vector quantisation. IEEE ASSP Mag., 1984, **1**(2), 4-49.

[29] 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 April 2013,page(s):53- 58.

[30] S. Mahato,D. K Yadav, and D. A Khan,” A modified approach to text steganography using hypertext markup language,” Advanced computing and communication technologies (ACCT), 2013 third international conference on 6-7 April 2013, page(s):40-44.

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

[32] S. Thenmozhi, and M. Chandrasekaran,” A novel technique for image steganography using nonlinear chaotic map,” Intelligent systems and control (ISCO), 2013 7th international conference on 4-5 Jan. 2013,page(s):307-311.

[33] 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 30-31 March 2012,page(s):320-325.

[34] A. Sanchez, A. Conci, E. Zeljkovic, N. Behlilovic, and V. Karahodzic, ”A new approach to relatively short message steganography, ”Telecommunications (BIHTEL), 2012 IX international symposium on 25-27 Oct. 2012,page(s):1-4.

[35] M. Nosrati, R. Karimi, H. Nosrati, and A. Nosrati, “Embedding stego-text in cover images using linked list concepts and LSB technique”, Journal of American Science, Vol. 7, No. 6, 2011, pp. 97-100.

[36] M. Naseem, Ibrahim M. Hussain, M. Kamran Khan, Aisha Ajmal, “An Optimum Modified Bit Plane Splicing LSB Algorithm for Secret Data Hiding”, International Journal of Computer Applications, Vol. 29, No. 12, 2011. Foundation of Computer Science, New York, USA, pp. 36-43.