International Journal of
Emerging Research in Management &Technology
ISSN: 2278-9359 (Volume-3, Issue-5)

Research Article | **May 2014**

Data Security with Image Clustering using Steganography

Mitali Garg, Vikas Wasson
Research scholar, Computer Science Department
Chandigarh University, India

Abstract—

Steganography is art of invisible Communication. It strives to hide the existence of communicated message in appropriate medium i.e. Image, Audio or Video. So as not to arouse an eavesdropper's suspicion. Various techniques with Objectives of robustness, Payload and Undetectability are available and have their respective pros and cons. Various Steganography Techniques are employed depending on requirements of application for which they are designed.

Keywords—Steganography, Data Hiding, Cover Object, Cryptography, Steganalysis

I. INTRODUCTION

In the modern era, computers and the internet are major communication media that connect the world. As a result, people can easily exchange information and distance is no longer a barrier to communication. The safety and security of long-distance communication remains an issue [19]. Data transfer and data Sharing is a part of high speed Internet Technology. Intruders try to access the Secret Information. So Information Security is needed to be applied and modified exponentially. Cryptography and Steganography are used for information security to reduce intruder accessing. Cryptography is used to encrypt data and make it unreachable for unauthorized person. Encryption process marks message as "Secret" information, and encrypted message becomes subject to attack [20]. Steganography is technique that is used to hide secret information and to prevent any attackers to use the Information in illegal form. Steganography is the art and science of hiding the secret information in some carrier data without leaving any evidence of data alternation. Data Hiding is another name for Steganography. The Goal of Steganography is that Data should be hidden in such a way that even if viewed by User should not gain Focus from the Viewer. Block Diagram for general form of Image Steganography.

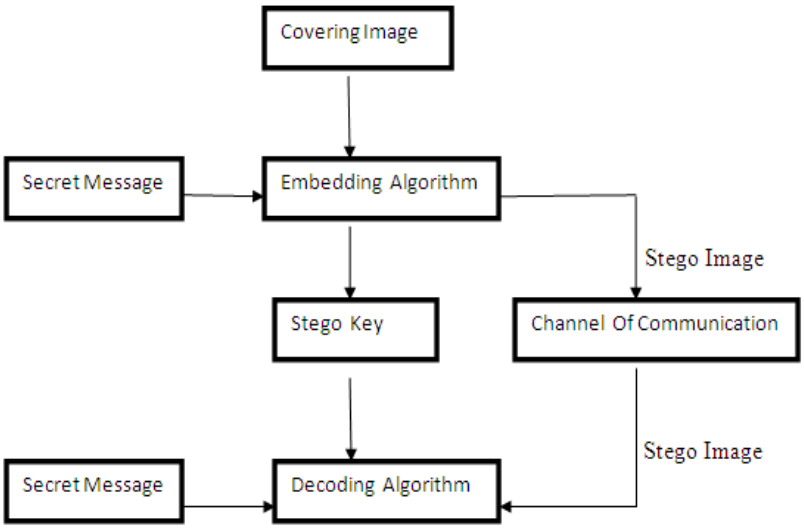


Figure 1: Block Diagram for general form of Image Steganography

The general model of Steganography uses a Cover Image (any image that can be used to hold secret information inside), the secret message (the private information that is to be sent secretly), a stego key that is used to encode the secret message so that detection becomes difficult and a Steganography algorithm/technique (the procedure to hide secret message). The outcome of the process is the stego Image that has the secret message hidden inside. This stego object is sent to the receiver where receiver will get the secret data out from the stego image by applying decoding algorithm/technique [21]. A good technique of image Steganography aims at following aspects.

1. Imperceptibility to a Human Visual System: The difference between stego image and original image should be minimal such that the unauthorized person cannot detect Secret information. If more information is hidden inside the carrier image, it will lead to degradation of stego image

2. Robust: Stego image should remain unchanged even if it undergoes transformation, sharping, filtering, scaling, blurring, cropping and other modification etc. It should produce the original image after reversal of processes. This makes sure that the message to be hidden remains safe even if it gets attacked and manipulated.
3. Simplicity of detection and extraction for an individual who possesses the private key to retrieve the message, it should be easy to extract it. For others who don't have a key, it should be very complicated to unlock its contents. This ensures that the watermarking is perfect and can be only deciphered by rightful individual.
4. High information capacity the watermarked image should be able to carry large information without burdening the channel or the original image. This property describes how much data should be embedded for proper carriage [22].

Steganography is implemented by using digital media. Secret message is embedded inside digital cover media like text, images, audio, video or protocols depending upon the requirement or the choice of the sender. Comparatively Image Steganography is most widely used. The reason behind the popularity of Image Steganography is the large amount of redundant information present in the images that can be easily altered to hide secret messages inside them, and because it can take advantage of the limited power of the human visual system (HVS)[22].

Steganography has a wide range of applications. The major application of Steganography is for secret data communication. Security Agencies uses it for spying purposes and to communicate without notification to third party. Steganography provide an ultimate guarantee of authentication that no other security tool can provide. Some modern applications also include Medical Imaging Systems. Here a separation is recommended between patients' image data or DNA sequences and their captions for security or confidentiality reasons, e.g., physician, patient's name, address and other particulars. Hence, embedding the patient's information in the image could be a useful safety measure and helps in solving such problems [19].

II. RELATED WORK

Raman G.S et al. In "Active Steganalysis based on Adapted Lempel-Ziv complexity and Approximate Entropy Estimation" an active Steganalysis proposes method used to detect the existence of stego image.The proposed Steganalysis technique trace embedding rate for approximate entropy estimation and Lempel-Ziv entropy. In this paper the grey-scale stego image is taken and analyzed to calculate the DCT coefficient values.

Cao Hong et al. in "On establishing edge adaptive grid for bilevel image data hiding" experimentally proved an efficient method for edge adaptive data hiding. This is method for authenticating binary host images through establishing a dense edge-adaptive grid along the objective contours. It is efficient than IB4 scheme for images with high resolution clarity and good exemption quality. This method also supports hybrid authentication that integrates data hiding and modern cryptographic techniques**.** Above all, this method is not applied to Bi-level image data hiding.

Shi Ran et al. in "The Objective Evaluation of Image Object Segmentation Quality Ran" propose a new objective quality metric to evaluate the subjective quality of the individual object segmentation. The proposed metric measures the similarity between the ground truth and segmentation result in four aspects: quantity, area, external contour and content. It analyse four types of segmentation errors and verify experimentally that besides quantity, area and contour, the distortion of object content is another useful segmentation quality index. The metric evaluates the similarity between ideal result and segmentation result by measuring these distortions.

Roy.S et al. in "A Text based Steganography Technique with Indian Root" presents a text based Steganography technique based on the Vedic Numeric Code. English alphabets in conjunction with Vedic Numeric Code are used for the Steganography. Hiding a larger message requires large no of words and leads to complexity of sentence.

Chandramouli.R *et al. in* "Analysis of LSB Based Image Steganography Techniques" presents rigorous approach at arriving at the Steganography capacity of LSB based image data hiding techniques. Here Specific technique of Steganography is used which distinguish between Images that carry hidden message and which do not carry hidden message. It derived expression of probability for detection purpose. Here capacity is defined in terms of detectability. Image property and strategy of Steganalyst helps in determining the data hiding capacity for LSB based scheme.

Chanu Jina Yam Bern et al. in "A Short Survey on Image Steganography and Steganalysis Techniques" presents survey on different types of Steganography techniques for image in spatial and transform domains and also Steganalysis techniques for the detection of secret message. In this paper Strong and Weak points of techniques are mentioned so that researcher who works in Steganography has prior knowledge in designing the technique. It also distinguishes between Steganography and Steganalysis .Steganography is the art of hiding data in the medium whereas Steganalysis is art of extracting the hidden message from the medium.

Roy.R et al. in "Evaluating Image Steganography Techniques: Future Research Challenges" evaluates the different algorithms of Steganography both in the spatial and transform domain. Here different Image Steganography Techniques are evaluated based on the degree of security, capacity and factors such as the statistical property of image that they deviate as a consequence of their embedding mechanism. Some of the possibilities of future research in the field of digital Image Steganography are also discussed based on the information gathered. Some important characteristics of a good Steganography system have been put forward.

Ashwin.S et al. in "Novel and Secure Encoding and Hiding Techniques using Image Steganography: A Survey" presents a review on different types of contemporary Steganography techniques for image and Steganalysis techniques. Author says that all the major image file formats have different methods of hiding messages, with different strong and weak

points respectively. Researcher can decide which algorithm to use for data hiding depending upon the type of application to be developed because some lack in payload capacity and others in robustness. Various research trends and challenges are also identified and directions for future research work are also discussed.

Jabbar Altaay.A et al. in "An Introduction To Image Steganography Techniques" intends to give an overview of image Steganography, its uses and techniques. Author says that information hiding technology falls into three classes of Steganography, watermarking, and cryptography. Technical Challenges faced during data hiding are also discussed in this paper. A criterion of counted features and restrictions is formed for data embedding algorithm to prove its usefulness. It has stated that data hiding algorithms cannot easily be categorized either in Steganography or watermarking categories as there is no transparent boundary between these two terms and classification relies on application of the algorithm.

Akhtar.N et al. in "An Improved Inverted LSB Image Steganography" an improvement in the plain LSB based image Steganography is proposed. The use of bit inversion technique is used to improve the stego image quality. Two schemes of the bit inversion techniques are proposed and implemented in this paper. The proposed bit inversion technique provides good improvement to LSB Steganography. The improvement in PSNR may be very large for some image as in the case of TestPat image and for some other image, it may be small.

III NEED AND SIGNIFICANCE

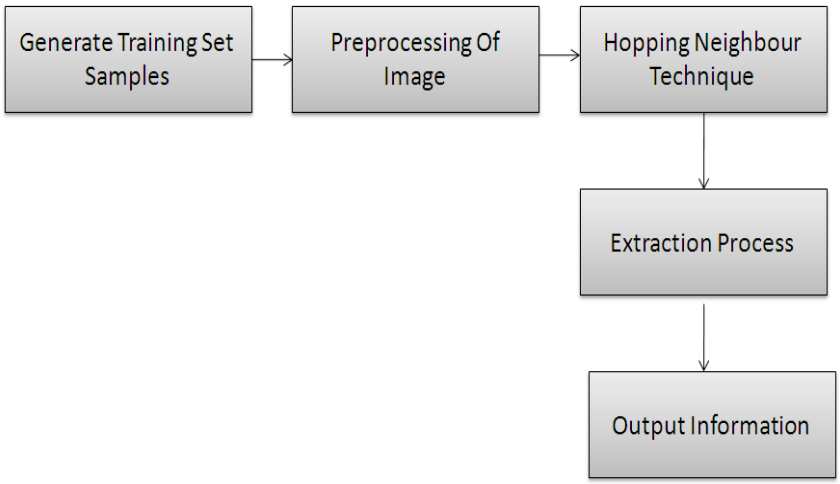
Since the rise of internet, Security of information is important factor. Cryptography is used for Securing the Secrecy of Communication. Various methods have been designed to encrypt and decrypt the data in order to keep the message secret. But sometimes it is not enough to keep the content of message secret, it may also be necessary to keep the existence of message secret. This is done through Steganography. Various Steganography techniques are used to provide some level of access control over the medium. Different mediums are usually images, videos, audio etc. Significance of the Steganography techniques that are employed in information processing algorithms is for data security focusing mainly on images and various properties and characteristics that the Steganography algorithms should posses.

1 Many security level leads to flaws that even with right key incomplete information is extracted.
2 The stego-image has distortion.
3 Low capability of hiding very long secret message in a small stego-image.
4 Already in practice algorithms like bit plane Steganography, embedding algorithm for lcw scheme and embedding algorithm for emd scheme are complex.

IV PROPOSED METHODOLOGY

To full fill the objectives we found as loop holes and missing in the existing technology. We begin the research from the roots of Steganography to tips of the technology. we decided to reach following goals using matlab to increase the threshold of security in the Steganography and at the same time make it so useful and easy when its in right hands with the right key.

1 Generate Training Set Sample. Input the image in which data is to be hidden and the type of data to be secured.
2 Pre-processing of Image to count number of pixels in each cluster. Divide the image into the regions or the parts that are conducive.
3 Securing the data using Hopping Neighbour Method.
4 Extraction process.
5 Output the Information.



V CONCLUSION

Image Steganography is a considerably new dimension in the field of information hiding. Though there have been many active researchers in the field still many research issues are yet to be explored. Some important characteristics of a good

Steganography system have been put forward after the analysis of Information gathered. We have proposed the Hopping Neighbour Technique for this purpose and is much efficient when compared to others.

ACKNOWLEDGMENT

I would like to express my gratitude to my guide Mr Vikas Wasson for his continous support and guidance. He kindly read my paper and offered invaluable detailed advices on grammar, organization, and the theme of the paper.

REFERENCES

[1] Song.S, "A Novel Secure Communication Protocol Combining Steganography and Cryptography" *Procedia Engineering 15 (2011) 2767 – 2772, Elsevier,* 2011.
[2] Begum.M, "LSB Based Audio Steganography Based On Text Compression" Procedia Engineering 30 (2012) 703 – 710, *Elsevier.* 2012
[3] Biswas.D,"Digital Image Steganography using Dithering Technique" *Procedia Technology 4 (2012) 251 – 255, Elsevier,*2012.
[4] Khamrui.A ,"A Genetic Algorithm based Steganography using Discrete Cosine Transformation (GASDCT)" *Procedia Technology 10 (2013) 105 – 111, Elsevier,*2013.
[5] Majumder.A, "A Novel Approach for Text Steganography: Generating Text Summary using Reflection Symmetry" *Procedia Technology 10 (2013) 112 – 120, Elsevier,*2013.
[6] Roy.S, "A Text based Steganography Technique with Indian Root" *Procedia Technology 10 (2013) 167 – 171, Elsevier,*2013.
[7] Yang.C, "Steganalysis Frameworks of Embedding in Multiple Least-Significant Bits" *IEEE Transactions On Information Forensics And Security, Vol. 3, No. 4,*2008.
[8] SHI.R, "The Objective Evaluation of Image Object Segmentation Quality", @ee.cuhk.edu.hk
[9] Cao.H, "On Establishing Edge Adaptive Grid for Bilevel Image Data Hiding", *IEEE Transactions On Information Forensics And Security,* Vol. 8, No. 9,2013.
[10] Raman.G.S, "Active Steganalysis based on Adapted Lempel-Ziv complexity and Approximate Entropy Estimation", Proceedings of 2013 *IEEE Conference on Information and Communication Technologies,*2013.
[11] Blanes.I, "Pairwise Orthogonal Transform for Spectral Image Coding", *IEEE Transactions On Geoscience And Remote Sensing,* Vol. 49, No. 3, 2013.
[12] Chandramouli.R ,"Analysis Of LSB Based Image Steganography Techniques", *IEEE* International Conference on Image processing, Vol. 3,2001
[13] Chanu Jina.B ,"A Short Survey on Image Steganography and Steganalysis Techniques", *IEEE* National Conference On Emerging Trends And Application In computer Science, p. 52-55,2012.
[14] Roy.R , "Evaluating Image Steganography Techniques: Future Research Challenges" IEEE International Conference On Computing Management And Telecommunication, p. 309-314,2013.
[15] Ashwin.S , "Novel and Secure Encoding and Hiding Techniques using Image Steganography: A Survey" *IEEE* International Emerging Trends In Electrical Engineering And Energy Management, p.1717-177,2012.
[16] Jabbar Altaay.A ,"An Introduction To Image Steganography Techniques"*IEEE* International Conference On Advanced Computer Science Aplications And Technologies, p. 122-126,2012
[17] Akhtar.N , "An Improved Inverted LSB Image Steganography"*IEEE* International Conference On Issues And Challenges In Intelligent Computing Technologies, p. 749-755, 2014.
[18] Mathkour.H, "A New Image Steganography Technique" *IEEE* International Conference On Wireless Communications, Networking And Mobile Computing, p.1-4,2008.
[19] Hamid.N , "Steganography in image files: A survey", *Australian Journal of Basic and Applied Sciences,*2013.
[20] Vipul J Patel , "Uncompressed Image Steganography using BPCS: Survey and Analysis", IOSR *Journal of Computer Engineering* (IOSR-JCE), ISSN: 2278-8727Volume 15, Issue 4,2013.
[21] Faheem Ahmed.H , "Embedding Multiple Images in an Image Using Bit Plane Slicing",*International Journal of Advanced Research in Computer Science and Software Engineering,*Volume 3, Issue 1,2013.
[22] Dr.Husainy.M , "Message Segmentation to Enhance the Security of LSB Image Steganography",*International Journal of Advanced Computer Science and Applications,* Vol. 3, No. 3,2012.