A Review Paper on Different Network Security Techniques in Wireless Communication

Brajesh Sharma[1] Mrs. Shikha Singh[2]
[1]M.Tech Student [2]Assistant Professor
[1,2]Department of Electronics & Communication Engineering
[1,2]Dr. C.V. Raman University, Bilaspur, Chhattisgarh-India

Abstract— *Steganography is the network security technique. In which many carrier file formats can be used, but digital images are the most used in the Internet. It is basically used for hiding information in the cover image to form stegoimage. Different applications have different requirements of the steganography technique used. For example in license, Pan card, aadhar card, smart card ,Personal identification card the secret information is hidden in the stegoimage. This is a review paper on image steganography, its uses and techniques.*

Keywords— Cryptography, Steganography, Least Significant Bit

I. INTRODUCTION

In today's world since the rise of the Internet one of the most important factors of information technology and communication has been the security of information. Network is the combination of two or more devices in which information is exchanged. Network security is the important task to provide security to the information exchange between devices in the network. There are two types of network security techniques cryptography and steganography. Cryptography was created as a technique for securing the secrecy of communication and many different methods have been developed to encrypt and decrypt data in order to keep the message secret. Unfortunately it is sometimes not enough to keep the contents of a message secret, it may also be necessary to keep the existence of the message secret. The technique used to implement this, is called steganography. It is often thought that communications may be secured by encrypting the traffic, but this has rarely been adequate in practice.For example an encrypted e-mail message between a known customer to purchaser is not secure only by encryption. So the study of communications security includes not just encryption but also traffic security, whose essence lies in hiding information. An important subdiscipline of information hiding is steganography. While cryptography is about protecting the content of messages, steganography is about concealing their very existence. It comes from Greek roots - literally means "covered writing" and it is usually interpreted to mean hiding information in other information. Examples include sending a message to a spy by marking certain letters in a newspaper using invisible ink, and adding sub perceptible echo at certain places in an audio recording. Today steganography is mostly used on computers with digital data being the carriers and networks being the high speed delivery channels. Steganography differs from cryptography in the sense that where cryptography focuses on keeping the contents of a message secret, steganography focuses on keeping the existence of a message secret . Steganography and cryptography are both ways to protect information from unwanted parties but neither technology alone is perfect and can be compromised. Once the presence of hidden information is revealed or even suspected, the purpose of steganography is partly defeated . The strength of steganography can thus be amplified by combining it with cryptography. Two other technologies that are closely related to steganography are watermarking and fingerprinting. These technologies are mainly concerned with the protection of intellectual property, thus the algorithms have different requirements than steganography. These requirements of a good steganographic algorithm will be discussed below. In watermarking all of the instances of an object are "marked" in the same way. The kind of information hidden in objects when using watermarking is usually a signature to signify origin or ownership for the purpose of copyright protection. With fingerprinting on the other hand, different, unique marks are embedded in distinct copies of the carrier object that are supplied to different customers. This enables the intellectual property owner to identify customers who break their licensing agreement by supplying the property to third parties. In watermarking and fingerprinting the fact that information is hidden inside the files may be public knowledge sometimes it may even be visible – while in steganography the imperceptibility of the information is crucial. A successful attack on a steganographic system consists of an adversary observing that there is information hidden inside a file, while a successful attack on a watermarking or fingerprinting system would not be to detect the mark, but to remove it.

II. LITERATURE REVIEW

Research in steganography has mainly been driven by a lack of strength in cryptographic systems. Many governments have created laws to either limit the strength of a cryptographic system or to prohibit it altogether forcing people to study other methods of secure information transfer. Businesses have also started to realize the potential of steganography in communicating trade secrets or new product information. Avoiding communication through well-known channels greatly reduces the risk of information being leaked in transit. Hiding information in a photograph of the company picnic is less suspicious than communicating an encrypted file.This paper intends to offer a state of the art overview of the different algorithms used for image steganography to illustrate the security potential of steganography for business and personal use. After the overview it briefly reflects on the suitability of various image steganography techniques for various applications. This reflection is based on a set of criteria that we have identified for image steganography. Different kinds of steganography are there.Almost all digital file formats can be used for steganography, 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 [11]. The redundant bits of an object are those bits that can be altered without the alteration being detected easily [5]. Image and audio files especially comply with this requirement, while research has also uncovered other file formats that can be used for information hiding. Figure 1 shows the four main categories of file formats that can be used for steganography.

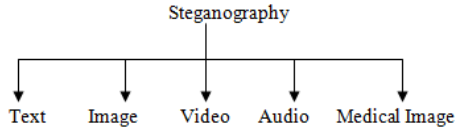

Fig. 1: Categories of steganography

Hiding information in text is historically the most important method of steganography. An obvious method was to hide a secret message in every nth letter of every word of a text message. It is only since the beginning of theText Images Audio/video Protocol Internet and all the different digital file formats that is has decreased in importance [1]. Text steganography using digital files is not used very often since text files have a very small amount of redundant data.Given the proliferation of digital images, especially on the Internet, and given the large amount of redundant bitspresent in the digital representation of an image, images are the most popular cover objects for steganography.This paper will focus on hiding information in images in the next sections.To hide information in audio files similar techniques are used as for image files. One different technique unique to audio steganography is masking, which exploits the properties of the human ear to hide information unnoticeably. A faint, but audible, sound becomes inaudible in the presence of another louder audible sound [1]. This property creates a channel in which to hide information. Although nearly equal to images in steganographic potential, the larger size of meaningful audio files makes them less popular to use than images [8]. The term protocol steganography refers to the technique of embedding information within messages and network control protocols used in network transmission [13]. In the layers of the OSI network model there exist covert channels where steganography can be used [12]. An example of where information can be hidden is in the header of a TCP/IP packet in some fields that are either optional or are never used. A paper by Ahsan and Kundur provides more information on this [13].

III. IMAGE STEGANOGRAPHY

As stated earlier, images are the most popular cover objects used for steganography. In the domain of digital images many different image file formats exist, most of them for specific applications. For these different image file formats, different steganographic algorithms exist.

IV. PROPOSED METHODOLOGY

A. Least Significant Bit

Least significant bit (LSB) insertion is a common, simple approach to embedding information in a cover image. The least significant bit (in other words, the 8th bit) of some or all of the bytes inside an image is changed to a bit of the secret message. When using a 24-bit image, a bit of each of the red, green and blue colour Text Images Audio/ video Protocol Transform Domain. Image Domain JPEG LSB in BMP components can be used, since they are each represented by a byte.

V. CONCLUSION

Although only some of the main image steganographic techniques were discussed in this paper, one can see that there exists a large selection of approaches to hiding information in images. All the major image file formats have different methods of hiding messages, with different strong and weak points respectively. This is the review paper on different network security techniques and there implementation.

REFERENCES

[1] Mrs. Kavitha, Kavita Kadam, Ashwini Koshti, Priya Dunghav/International Journal of Engineering Research and Applications (IJERA) Vol. 2, Issue 3, May-Jun 2012, Steganography Using LeastSignicant Bit Algorithm.
[2] Moerland, T., "Steganography and Steganalysis", Leiden Institute of Advanced Computing Science,
[3] Silman, J., "Steganography and Steganalysis: An Overview", SANS Institute, 2011
[4] Jamil, T., "Steganography: The art of hiding information is plain sight", IEEE Potentials, 18:01, 1999
[5] Wang, H & Wang, S, "Cyber warfare: Steganography vs. Steganalysis", Communications of the ACM, Oct 2014
[6] Anderson, R.J. & Petitcolas, F.A.P., "On the limits of steganography", IEEE Journal of selected Areas in Communications, May 1998
[7] Marvel, L.M., Boncelet Jr., C.G. & Retter, C., "Spread Spectrum Steganography", IEEE Transactions on image processing, 8:08, 1999
[8] Dunbar, B., "Steganographic techniques and their use in an Open-Systems environment", SANS Institute, January 2002
[9] Artz, D., "Digital Steganography: Hiding Data within Data", IEEE Internet Computing Journal, June 2001
[10] Simmons, G., "The prisoners problem and the subliminal channel", CRYPTO, 1983
[11] Chandramouli, R., Kharrazi, M. & Memon, N., "Image steganography and steganalysis: Concepts and Practice", Proceedings of the 2nd International Workshop on Digital Watermarking, October 2003
[12] Currie, D.L. & Irvine, C.E., "Surmounting the effects of lossy compression on Steganography", 19th National Information Systems Security Conference, 1996
[13] Handel, T. & Sandford, M., "Hiding data in the OSI network model", Proceedings of the 1st International Workshop on Information Hiding, June 1996
[14] Ahsan, K. & Kundur, D., "Practical Data hiding in TCP/IP", Proceedings of the Workshop on Multimedia Security at ACM Multimedia, 2002
[15] Johnson, N.F. & Jajodia, S., "Exploring Steganography: Seeing the Unseen", Computer Journal, February 1998
[16] "Reference guide: Graphics Technical Options and Decisions"

[17] Owens, M., "A discussion of covert channels and steganography", SANS Institute, 2002
[18] Johnson, N.F. & Jajodia, S., "Steganalysis of Images Created Using Current Steganography Software", Proceedings of the 2nd Information Hiding Workshop, April 1998
[19] Venkatraman, S., Abraham, A. & Paprzycki, M., "Significance of Steganography on Data Security", Proceedings of the International Conference on Information Technology: Coding and Computing, 2004
[20] Krenn, R., "Steganography and Steganalysis",
[21] Lee, Y.K. & Chen, L.H., "High capacity image steganographic model", Visual Image Signal Processing, 147:03, June 2000
[22] Provos, N. & Honeyman, P., "Hide and Seek: An introduction to steganography", IEEE Security and Privacy Journal, 2003
[23] Bender, W., Gruhl, D., Morimoto, N. & Lu, A., "Techniques for data hiding", IBM Systems Journal, Vol 35, 1996
[24] Petitcolas, F.A.P., Anderson, R.J. & Kuhn, M.G., "Information Hiding – A survey", Proceedings of the IEEE, 87:07, July 1999s