ISSN:0975-9646

Information Hiding in an Image File: Steganography

Harsh Prayagi, Tushar Srivastava, Gyanendra Ojha, Sunil Chaurasia

Department of Computer Science & Engineering,
Institute of Technology & Management, GIDA,
Gorakhpur, UP (India),
Gautam Buddh Technical University,
Lucknow, Uttar Pradesh , India

Abstract- Steganography plays an important role in information security. Since the rise of the Internet one of the most important factors of information technology and communication has been the security of information. It is the art of hiding the fact that communication is takes place, by hiding information in other information. Many different file formats can be used, but digital images are the most popular because of their frequency on the Internet. For hiding secret information in images, there exist a large variety of steganographic techniques some are more complex than others and all of them have respective strong and weak points. 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 graphei meaning "writing". The first recorded use of the term was in 1499 by Johannes Trithemius in his Steganographia, a treatise on cryptography and steganography disguised as a book on magic. Generally, messages will appear to be something else: images, articles, shopping lists, or some other covertext and, classically, the hidden message may be in invisible ink between the visible lines of a private letter. Steganography is the science that involves communicating secret data in an appropriate multimedia carrier, e.g., image, audio, and video files. It comes under the assumption that if the feature is visible, the point of attack is evident, thus the goal here is always to conceal the very existence of the embedded data. Steganography has various useful applications. However, like any other science it can be used for ill intentions. It has been propelled to the forefront of current security techniques by the remarkable growth in computational power, the increase in security awareness by, e.g., individuals, groups, agencies, government and through intellectual pursuit.

Keywords— Steganography, Cryptography, Encryption, Decryption, Steganalysis, Watermarking

I. INTRODUCTION

Steganography is the science that involves communicating secret data in an appropriate multimedia carrier, e.g., image, audio, and video files. It comes under the assumption that if the feature is visible, the point of attack is evident, thus the goal here is always to conceal the very existence of the embedded data. Steganography has various useful applications. However, like any other science it can be used for ill intentions. It has been propelled to the forefront of current security techniques by the remarkable growth in computational power, the increase in security awareness by, e.g., individuals, groups, agencies, government and through intellectual pursuit. Steganography's ultimate objectives, which are undetectability, robustness (resistance to various image processing methods and compression) and capacity of the hidden data, are the main factors that separate it from related techniques such as watermarking and cryptography. This paper provides a state-of-the-art review and analysis of the different existing methods of steganography along with some common standards and guidelines drawn from the literature. This paper concludes with some recommendations and advocates for the object-oriented embedding mechanism. Steganalysis, which is the science of attacking steganography, was not the focus of this survey but nonetheless has been briefly discussed.

In this paper a novel method is proposed to provide more security for the key information with the combination of image compression and data encryption method. This method requires less memory space and fast transmission rate because of image compression technique is applied. Steganography plays an important role in information security. Since the rise of the Internet one of the most important factors of information technology and communication has been the security of information. It is the art of hiding the fact that communication is takes place, by hiding information in other information. Many different file formats can be used, but digital images are the most popular because of their frequency on the Internet. For hiding secret information in images, there exist a large variety of steganographic techniques some are more complex than others and all of them have respective strong and weak points. Many applications have different requirements of the steganography technique used. Some applications may use absolute invisibility of the secret information, but others require a larger secret message to be hidden. This method has been implemented and tested on varies images and data. It provides better security for encrypted data and no distortion in the image quality. While Digital watermarking is the process of embedding information into a digital signal which may be used to verify its authenticity or the identity of its owners, in the same manner as paper bearing a watermark for visible identification. In digital watermarking, the signal may be audio, pictures, or video. If the signal is copied, then the information also is carried in the copy. A signal may carry several different watermarks at the same time

II. PROBLEM STATEMENT

Although steganography is an ancient subject, the modern formulation of it comes from the prisoner's problem proposed by Simmons, where two prisoners named Alice and Bob wish to communicate in secret to hatch an escape plan. All of their communication passes through a warden named Eve who will throw them solitary confinement if she suspects any type of secret communication. So they must find out some way of hiding their secret message which gives the birth of steganography. The warden is free to examine all communication exchanged between Alice and Bob can either be active or passive. An active warden will try to alter the communication with the suspected hidden information deliberately in order to remove the information where as a passive warden takes the note of covered communication, informs the others and allows the message to pass through .An assumption can be made based on this model is that if both the sender and receiver share some common secret information then the corresponding steganography protocol is known as then the secret key steganography where as pure steganography means that there is none prior information shared by sender and receiver. If the public key of the receiver is known to the sender, the steganographic protocol is called public key steganography. Although all digital file formats can be used for steganography, but the image and audio files are more suitable because of their high degree of redundancy.

III. METHODOLOGY

The former methods consist of linguistic or language forms of hidden writing. The later, such as invisible ink, try of hide messages physically. One disadvantage of linguistic steganography is that users must equip themselves to have a good knowledge of linguistry. In recent years, everything is trending toward digitization. And with the development of the internet technology, digital media can be transmitted conveniently over the network. Therefore, messages can be secretly carried by digital media by using the steganography techniques, and then be transmitted through the internet rapidly.

Steganography is the art of hiding the fact that communication is taking place, by hiding information in other information. Many different carrier file formats can be used, but digital images are the most popular because of their frequency on the internet. For hiding secret information in images, there exists a large variety of steganography techniques some are more complex than others and all of them have respective strong and weak points. So we prepare this application, to make the information hiding simpler and user friendly.

User needs to run the application. The user has two tab options – encrypt and decrypt. If user select encrypt, application give the screen to select image file, information file and option to save the image file. If user select decrypt, application gives the screen to select only image file and ask path where user want to save the secrete file.

This project has two methods – Encrypt and Decrypt.

In encryption the secrete information is hiding in with any type of image file.

Decryption is getting the secrete information from image file.

MORE TECHNIQUES OF STEGANOGRAPHY-

Following are the different techniques of steganography:-

1. Physical Steganography- Hidden message within wax tablets, on messenger's body.
2. Digital Steganography- Concealing messages within the lowest bits of noisy images or sound files, image bit-plane complexity segmentation steganography
3. Network Steganography- The concealment of messages in Voice-over-IP conversations.
4. Printed Steganography- The plaintext, may be first encrypted by traditional means, producing a ciphertext. Then, an innocuous covertext is modified in some way so as to contain the ciphertext, resulting in the stegotext.
5. Text Steganography- Data compression.
6. Steganography using Sudoku Puzzle

IV. CONCLUSIONS

Steganography is a really interesting subject and outside of the mainstream cryptography and system administration that most of us deal with day after day.

Steganography can be used for hidden communication. We have explored the limits of steganography theory and practice. We printed out the enhancement of the image steganography system using LSB approach to provide a means of secure communication. A stego-key has been applied to the system during embedment of the message into the cover image. This steganography application software provided for the purpose to how to use any type of image formats to hiding any type of files inside there. The master work of this application is in supporting any type of pictures without need to convert to bitmap, and lower limitation on file size to hide, because of using maximum memory space in pictures to hide the file.

Since ancient times, man has found a desire in the ability to communicate covertly. The recent explosion of research in watermarking to protect intellectual property is evidence that steganography is not just limited to military or espionage applications. Steganography, like cryptography, will play an increasing role in the future of secure communication in the “digital world”.

V. ACKNOWLEDGMENT

We would like to express our deep sense of gratitude to our project guide Mr. Abhishek Srivastava, coordinator Mr. Ajay Kumar & to Mr. Rajeev Ranjan Kumar Tripathi, Head of Department, Computer Science & Engineering/Information Technology, Institute of Technology & Management, Gorakhpur for their effort in putting us on right track & providing the harmonious atmosphere, which is of utmost necessity for being creative.

VI. REFERENCES

[1] Atul Kahate," Cryptography & Network Security", Tata McGraw-Hill Education, 2003.

[2] William Stallings,"Cryptography & Network Security", Pearson Education, Inc.

[3] A.Z. Tirkel, R.G. Van Schyndel, C.F. Osborne, “A digital Watermark” Proceedings of ICIP 1994, Austin Convention. Center, Austin, Texas, Vol. II, 1994, pp. 86–90.

[4] W. Bender, N. Morimoto, A. Lu, “Techniques for data hiding”, IBM Syst. J. 35 (3/4) (1996) 313–336.

[5] Abbas Cheddad , Joan Condell, Kevin Curran and Paul Mc Kevitt“Digital Image Steganography , Survey and Analysis of Current Methods”.