DATA COMPRESSION AND DECOMPRESSION WITH IMAGE STEGANOGRAPHY USING API

Aadesh Garg , Amisha Prajapati, Amisha Linjhara , Ananya Srivastava

ACROPOLIS INSTITUTE OF TECHNOLOGY AND RESEARCH INDORE

INTRODUCTION

With the development of the Internet, information processing technologies and the rapid development of communication, it is necessary to share information resources, and the network has becoming the main means of communication. Nevertheless, the Internet is an open environment so; information security has becoming increasingly important. Today, information security technology has two main branches are cryptography and information hiding. Steganography is the art of hiding information in such a way that prevents the detection of hidden messages. The message is the data that the sender wants to remain confidential. It can be in the form of text, image, audio, video, or any other data that can be represented by a stream of bits. The cover or host is the medium in which the message is embedded. It serves to hide the presence of the message. We can use gray images, videos, sound files, and other computer files that contain perceptually irrelevant or redundant information as a cover image. It is important to note that the hidden data is not detectable in the stego-image.

OBJECTIVES

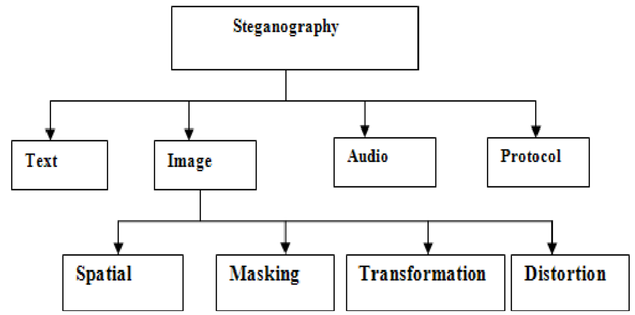
Generally, the study aimed to develop a system Image Steganography of Multiple File Types with Encryption and Compression Algorithms. Specifically, this study aimed to: accept secret file to be hidden; compress secret file using an Algorithm; encrypt and decrypt secret file using Data Encryption Standard Algorithm; embed and extract data file in stego-image using LSB Algorithm; and evaluate the system using a specific standards: functionality, usability, reliability, portability, efficiency, and maintainability.

MATERIAL AND METHODS

The word Steganography is derived from two Greek words- 'stegos' meaning 'to cover' and 'grayfia', meaning 'writing', thus translating to 'covered writing', or 'hidden writing'. Steganography is a method of hiding secret data, by embedding it into an audio, video, image or text file. It is one of the methods employed to protect secret or sensitive data from malicious attacks. Image Steganography – As the name suggests, Image Steganography refers to the process of hiding data within an image file. The image selected for this purpose is called the cover-image and the image obtained after steganography is called the stego-image.

SCOPE

In our thesis work we propose a new approach which give good quality of the image after encoding the original image by using the Least Significant Bit technique because LSB technique has a drawback it affects the resolution the original image after encoding, so that image quality go burst. The future work on this project is to improve the compression ratio of the image to the text. The main intention of the project is to develop a steganographic application that provides good security. The proposed approach provides higher security and can protect the message from stego attacks. The image resolution doesn't change much and is negligible.

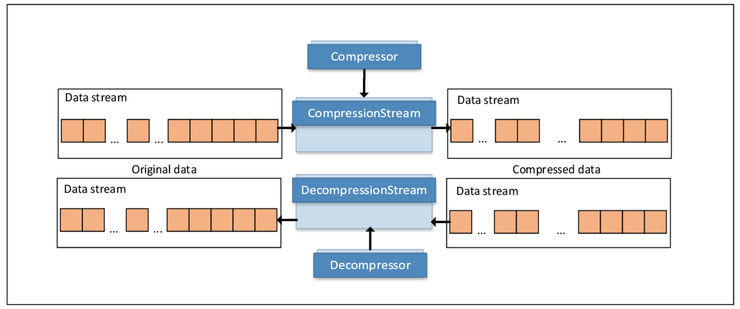


CONCLUSION

The Image Steganography of Multiple File Types with Encryption and Compression Algorithms application developed and described in this research paper may not surpass other higher and well-known steganography application, but the simplicity and the availability of this file security application proves that this application can be developed to fit the needs of an institution without resorting to purchasing expensive software from the market. Since the Image Steganography of Multiple File Types with Encryption and Compression Algorithms application developed by the researcher only used a JPG image as an image cover media, the researcher recommends that other image file types be used as an image cover media to improve flexibility of the application. The following are further recommended: (1) this application could only use an image file to be the cover media of the secret file, the researcher recommends to explore other file types to be the cover media such as video and audio; (2) this application cannot extract the original secret file if the stegophoto .

EXPECTED OUTCOMES

1.Mathematically relating the security and the limit: Security and Capacity exchange off is an imperative issue in steganography. It has been seen that expansion in the limit prompts giving up the security to some degree. 2. Development of Algorithms dependent on items in pictures: As the steganalysis techniques are getting more grounded and in the end most steganographic calculations are falling prey to them, there is a pattern in creating calculations which targets specific parts of pictures for installing.



REFERENCE

[1] Moerland, T. (2014). Steganography and Steganalysis. Leiden Institute of Advanced Computing Science. Retrieved from https://goo.gl/EL2zsp

[2] Wang, H & Wang, S,.(2004). Cyber warfare: Steganography vs. Steganalysis. Communications of the ACM, 47(10)

[3] Silman, J. (2001). Steganography and Steganalysis: An Overview. SANS Institute. [4] Jamil, T. (1999). Steganography: The art of hiding information is plain sight. IEEE Potentials, 18 (01)

[5] Anderson, R.J. & Petitcolas, F.A.P., (1998). On the Limits of Steganography. IEEE Journal of Selected Areas in Communications [6] Artz, D.,(2001). Digital Steganography: Hiding Data within Data. IEEE Internet Computing Journal

RESEARCH POSTER PRESENTATION DESIGN © 2015
www.PosterPresentations.com