Data Compression Decompression and Image Steganography
A Minor Project Synopsis Submitted to

Rajiv Gandhi Proudyogiki Vishwavidyalaya, Bhopal
Towards Partial Fulfillment for the Award of

Bachelor of Technology
(Computer Science and Engineering)

Under the Supervision of

Prof. Priyanka Jangde

Submitted By

Aadesh Garg(0827CS201001)
Amisha Linjhara (0827CS201029)
Amisha Prajapati (0827CS201030)
Ananya Shrivastava (0827CS201032)

Department of Computer Science and Engineering
Acropolis Institute of Technology & Research, Indore
Jan-June 2023

1.Abstract

The goals of this study were to develop a system intended for securing files through the technique of image steganography integrated with cryptography by utilizing ZLIB Algorithm for compressing and decompressing secret files, DES Algorithm for encryption and decryption, and Least Significant Bit Algorithm for file embedding and extraction to avoid compromise on highly confidential files from exploits of unauthorized persons.

The system will be excellently effective based on Functionality, Reliability, Usability, Efficiency, Maintainability and Portability.

The system can be a useful tool for both government agencies and private institutions for it could keep not only the message secret but also the existence of that particular message or file secret maintaining the privacy of highly confidential and sensitive files from unauthorized access.

2.Introduction to the project

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.

3.Objective

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 aspecific standards: functionality, usability, reliability, portability, efficiency, and maintainability.

4.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.

5.Applications

Steganography can likewise be utilized to execute watermarking. In spite of the fact that the idea of watermarking isn't really steganography, there are a few stenographic techniques that are being utilized to store watermarks in data.

The principle distinction is on goal, while the motivation behind steganography is concealing data, watermarking is simply expanding the cover source with additional data. Since individuals won't acknowledge observable changes in pictures, sound or video documents in view of a watermark, Steganography strategies can be utilized to conceal this.

Paired with existing specialized strategies, steganography can be utilized to do shrouded trades. Governments are keen on two sorts of concealed correspondences: those that help national security and those that don't.
Advanced steganography gives huge potential to the two kinds. Organizations may have comparable concerns Regarding prized formulas or new item data.
It is additionally conceivable to just utilize steganography to store data on an area. For instance, a few data sources like our private managing an account data, some military insider facts, can be put away in a cover source.

6.Project Description

The methodology of this system is done through deep research and analysis to achieve data security. This application was done to showcase different techniques and operations used in protecting sensitive information of different file types such as image files, video files, audio files and documents.
The system entitled Image Steganography of Multiple File Types with Encryption and Compression Algorithms is an application that improved file security by integrating the technique of steganography and encryption with the additional feature of compression using the concepts of Least Significant Bit (LSB) algorithm, DES Algorithm for encryption and ZLIB Algorithm for lossless compression.

7.Methodology/Planning of the Project work

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.

Dependencies:

The major requirement of the resources for designing and developing the proposed smart map is as follows.

- HTML
- CSS
- JavaScript
- Java

HTML: HTML stands for Hyper Text Markup Language. It is the standard markup language for creating web pages. It describes the structure of a web page. HTML consists of a series of elements. HTML elements tell the browser how to display the content.

CSS: stands for Cascading Style Sheets. It describes how HTML elements are to be displayed on the screen, paper, or in other media. It can control the layout of multiple web pages all at once and saves a lot of work. External stylesheets are stored as CSS files.

JavaScript: is a scripting language, primarily used on the Web. It is used to enhance HTML pages and is commonly found embedded in HTML code. JavaScript is an interpreted language. Thus, it doesn't need to be compiled. JavaScript renders web pages in an interactive and dynamic fashion.

Java: is a one of the most popular programming languages for many years.
Java is Object Oriented. However, it is not considered as pure object-oriented as it provides support for primitive data types

8.Expected Outcome

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.
3. Improving the steganographic calculations:
It is seen that all steganographic calculations, be that in the spatial area or the change space (recurrence area), eventually adjust factual properties of pictures and because of which they fall prey to measurable steganalysis techniques. In this manner, it is obvious that there still stays sufficient degree for research in creating calculations in picture steganography that will have the capacity to give increasingly anchor highlights to data stowing away.
We can arrange the conceivable upgrades that may be received to assemble future steganographic frameworks as:

- Increasing implanting proficiency
- Decreasing installing mutilation
- Choosing substitute shading spaces
- Choosing alternate colour spaces

9.Resources and Limitations

All the project requires research and analysis investing some time on research and analysis will save much time in future to gather other information.
The main limitation is the maximum size of the embedded data compared to the total data. If a piece of data is already very compressed it might be wholly impossible to embed additional data in it. And even under ideal conditions you will rarely get more than 20% out of the carrier data.
So assume that you use a bunch of image files of moderate compression level as carrier medium. Lets say you get on average 15% out of it, lets say the total batch of images has a size of 1GB.This means that after encrypting and embedding your data, you will be able to transport 75MB of hidden data. This is not a lot. Steganography is in general only used in situations where there is no other alternative because the very fact that A and B are communicating would lead to grave consequences. Trying to swap and share files for example is not such a situation.

There are various requirements (hardware, software and services) to successfully deploy the system. These are mentioned below:

Hardware

- 32-bit, x86 Processing system
- Windows 7 or later operating system
- High processing computer system without GPU or with
- GPU (high performance)

Software

- MySQL
- Hosting domain

10.Conclusion

In the study of Image Steganography of Multiple File Types with Encryption and Compression Algorithms using the Least Significant Bit Algorithm, Data Encryption Standard Algorithm and ZLIB Compression Algorithm, the researcher concluded the following:
(1) in the compression of the secret file, ZLIB Compression Algorithm was used and resulted to a lessened size of the original secret file;
(2) in the encryption and decryption phases, the secret file was primarily secured using the Data Encryption Standard Algorithm;

(3) Least Significant Bit Algorithm was effectively used in embedding and extracting the secret file from the image cover media;
(4) the system was evaluated based on ISO 9126 in terms of functionality, reliability, usability, efficiency, maintainability and portability.

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 of the original secret file is once again embedded as a secret file in another instance of embedding, hence, the researcher recommends to other researchers to further advance this study to solve the said limitation.

11.References

[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