International Journal of Computer Sciences and Engineering
Vol.**11**, Issue **1**, pp.**11-13**, January **2023**
ISSN: 2347-2693 (Online)
Available online at: www.ijcseonline.org

ISSN: 2347-2693 (E)

Research Paper

Encrypting Secret Information inside an Image Using Steganography

Udita Bhardwaj[1*], Vikas Singhal[2], Shivani Dubey[3]

[1]Greater Noida Institute of Technology, Greater Noida, India
[2]Greater Noida Institute of Technology, Greater Noida, India
[3]Greater Noida Institute of Technology, Greater Noida, India

**Corresponding Author: dubey.shivani@gmail.com*

Received: 22/Dec/2022; **Accepted**: 03/Jan/2023; **Published**: 31/Jan/2023. **DOI**: https://doi.org/10.26438/ijcse/v11i1.1113

Abstract— Converting information into the image format has become the latest method which can be implemented for encrypting information into colours. Experts have projected different methods to implement this approach to secure data against hackers. Most of the approaches square measuring readily implemented algorithms or putting forward an easy level of the coding execution which makes these methods a risk to break by attackers. A new and emerging method of operations is discussed through this paper so as to build a word-To-picture encrypting approach. The substitution and transposition operations square measure applied into two levels ((characters (bytes) and bits) of the written information to formulate the secret and safe image. Together the given functions provide lots of strength points to fight against hackers. The projected method has been applied and verified across various sets of information; the recorded observations proved the efficiency and correctness of the methodology as an efficient Text-To-Image encrypting approach.

Keywords — Encryption, Cryptography, Stegnography

1. Introduction

This is the new generation of metaverse, everything is revolving around data and technology, sending and accepting digital data among individuals and establishments has become a part of every hour task. Numerous ways and techs have been invented by engineers to safeguard the data over the internet from the evil hackers. Cryptography and steganography are most famous technologies nowadays which is being used to shield the confidential data of high end institutions. While cryptography works on ever changing the initial secret information into a non-recognizable encrypted data. On the other hand, steganography is the way to hide the presence of the confidential data through encrypting the data in some other kind of format which works as a carrier within the case of discovering the presence of the confidential data by hackers, the encryption of the secret information works as the second and last safeguard border against hackers. Therefore, vast efforts square measure defrayment by researchers to develop extremely secure cryptologic systems [1].

2. Training the Algorithms with Two Keys

Traditionally, all encrypting methods are implementing one or both of the two main operations on the confidential data (Text, Image, Audio, and Video) to encrypt it and producing the secure coded data. These two operations are Substitution and Transposition. While substitution involves changing the original values of the confidential information to recent new values, the transposition consists of changing the order of the initial values of the confidential data to latest order. Because these two operations are recognized to all, hence the strength of any well-formed encryption technique is based on the way of the style (manner used) to implement these operations and the key(s) used in the method. The encryption method consists of an algorithm that explains the main steps of implementing the substitution and transposition operations, and key(s) (which kept secret) that represents the secret information on how to implement these steps on the original confidential data to produce encrypted data [2]. Depending on the type and number of keys used in the encryption method, encryption methods are classified into two types:

- **Symmetric key:** which uses the private confidential key in both encrypting and decrypting stages.
- **Asymmetric key:** it applies a pair of differently designed keys (public key and private key). The one type of key is applied in the encryption stage and the other is a secret key is used for the decryption stage.

The most important points that focus on when should be selecting the key(s) are:

- **Size of Key:** the key must be as large as possible so that it is much harder to break hackers.

- **Complexity of Key:** the key must be complicated and random as much as possible to add more and more difficulties in face of hackers.

3. Tools & Technologies

Steganography technique is being pretty much crucial these days due to large scale mass of human is making itself active on the internet world and digital revolution. Steganography is the art of encrypting information in ways that prevents the detection of hidden messages. Steganography includes an array of secret communication methods that hide the message from being seen or discovered. Due to advances in ICT, major part of the data is saved in digital format [4]. Consequently, the security of information has become a fundamental issue. Besides cryptography, steganography can be employed to secure information. In cryptography, the message or encrypted message is embedded in a digital host before sending it over the network, thus the existence of information is not known. Apart from hiding data for the purpose of safety and security, this methodology of information hiding can be extended to copyright protection for digital media: audio, video and images [5]. The growing possibilities of modern communications need the special means of security especially on computer network. The network security is becoming more important as the number of data being exchanged on the internet increases. Therefore, the confidentiality and data integrity requires to protect against unauthorized access and use. This has resulted in an explosive growth of the field of information hiding Information hiding is an emerging research area, which encompasses applications such as copyright protection for digital media, watermarking, fingerprinting, and steganography [6].

In watermarking applications, the message contains information such as owner identification and a digital time stamp, which usually applied for copyright protection. Fingerprint, the owner of the data set embeds a serial number that uniquely identifies the user of the data set. This adds to copyright information to makes it possible to trace any unauthorized use of the data set back to the user. Steganography hides the secrete message within the host data set and presence imperceptible and is to be reliably communicated to a receiver. The host data set is purposely corrupted, but in a covert way, designed to be invisible to an information analysis. As mentioned in this paper this will increase the number of attempts that are needed by hackers to break the encoded visual where the number of attempts is directly proportional to the number of blocks in the confidential data [7].

4. Methodology

User needs to run the application. The user has two 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 secret information is hiding in with any type of image file. Decryption is getting the secret information from image file [8].

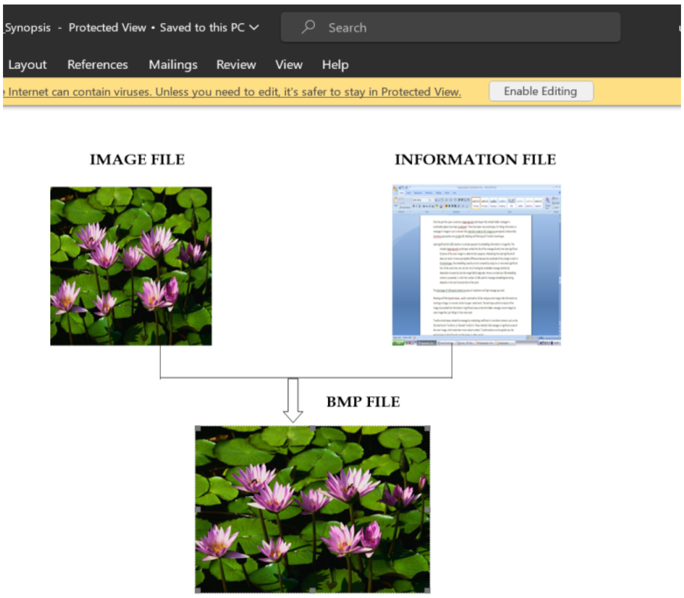
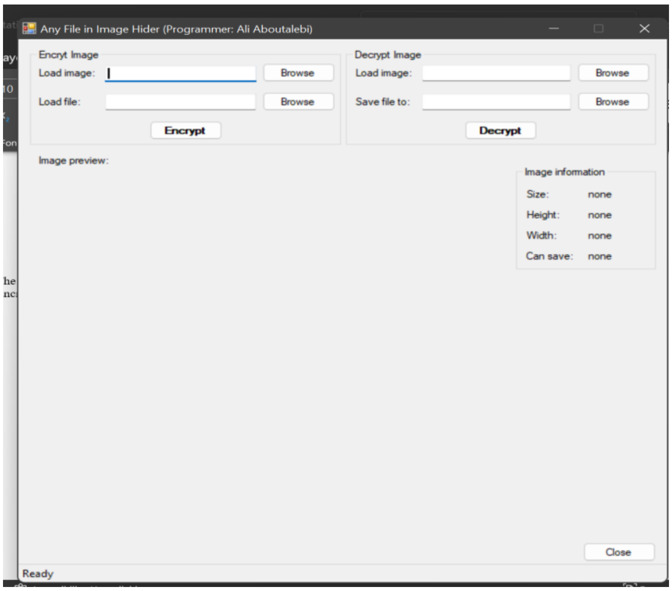

Synopsis - Protected View • Saved to this PC
Search
Layout
References
Mailings
Review
View
Help
Internet can contain viruses. Unless you need to edit, it's safer to stay in Protected View.
Enable Editing
IMAGE FILE
INFORMATION FILE
BMP FILE

Figure.1: Encrypt secret information from image file

The BMP file created is the result obtained in the process of Encrypting the text information to a random image. Given below is the console of the software made with the help of this research paper.



Size: none
Height: none
Width: none
Can save: none

Figure.2: BMP File

5. Conclusion

A new implementation of Text-To-Image encryption method has been proposed in this work to overcome a set of problems that are observed in the previous works. Good results have been achieved through using a compound key and implementing a set of substitution and transposition operations at two levels (bits and bytes). The evaluation of the recorded results from the experiments proved that the proposed Text-to-Image encryption method succeeded to overcome most of the defects in the previous works and provide good protection to the original secret text. Therefore, the Text-To-Image that has been presented in this work represents one of encryption methods that can be used effectively in the field of information security to protect the text data. 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 them. 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".

6. Future Scope

This project is developed for hiding information in any image file. The scope of the project is implementation of steganography tools for hiding information includes any type of information file and image files and the path where the user wants to save Image and extruded file. In the upcoming future, the most important use case of steganographic methods will be lying in the bucket of digital watermarking. As per the observation all steganographic algos are tend to alter statistical properties of images and as a result of which they fall in the net of hackers. Thus, it is pretty sure that there is still a need of improvisation in algorithms of steganographic techniques.

REFERENCES

[1]A. Abusukhon, "Block Cipher Encryption for Text-To-Image Algorithm". International Journal of Computer Engineering and Technology (IJCET), Vol.**4**, Issue.**3**, **2013.**

[2]A. Abusukhon, M. Talib, and H. Almimi, "Distributed Text-to-Image Encryption Algorithm". International Journal of Computer Applications, Vol. **106**, No. 1, **2014**.

[3]M. Chen, N. Memon, E.K. Wong, Data hiding in document images, in: H. Nemati (Ed.). Premier Reference Source– Information Security and Ethics: Concepts, Methodologies, Tools and Applications, New York: Information Science Reference, pp.**438-450, 2008.**

[4]D.C. Lou, J.L. Liu, H.K. Tso, Evolution of information [hiding technology, in H. Nemati (Ed.), Premier Reference Source– Information Security and Ethics: Concepts, Methodologies, Tools and Applications, New York: Information Science Reference, pp.**438-450, 2008.**

[5]Morkel T. , Eloff J.H.P. , M.S. Olivier, "An overview f image]01[steganography", http://mo.co.za/openistegoverview.pdf, on January **2009**.

[6]Diop, S .M Farssi, O. Khouma, H. B Diouf, K .Tall, and K .Sylla, "New Steganographic scheme based of Reed-Solomon codes, International Journal of Distributed and Parallel Systems (IJDPS)", Vol.**3**, Issue.**2**, **2012**.

[7] M. Sutaone and M. Khandare, "Image based steganography using LSB insertion technique", in Conference on Wireless, Mobile and Multimedia Networks, 2008. IET International, Beijing, pp.**146 – 151, 2008.**

[8] N. F. Johnson and S. Jajodia, "Exploring steganography, seeing the unseen", IEEE Computer Magazine, Vol.**31**, Issue.**2**, pp.**26-34, 1998.**

AUTHORS PROFILE

Ms. Udita Bhardwaj is currently pursuing B.Tech in Information Technology from Greater Noida Institute of Technology, Greater Noida, Uttar Pradesh which is affiliated with APJ Abdul Kalam Technical University. She has worked on various projects that go from developing a morse code application in python to a blogging website in her four years of the Engineering program. She has also developed many applications that range from a movie app to a simple quiz application in order to find her specific domain for doing research.

Prof. Vikas Singhal, Head of the Department of Information Technology in GNIOT, Greater Noida. His main research work focuses on Cryptography Algorithms, Network Security, Cloud Security and Privacy, Big Data Analytics, Data Mining, IoT and Computational Intelligence based education. He has more than 22 years of teaching experience and 4 years of Research Experience.

Dr. Shivani Dubey, Associate Professor in Department of Information Technology in GNIOT, Greater Noida has more than 16 years experience in academic and teaching. She has done her doctrate from Ansal University, Gurgaon. Her specialization is in cloud computing, data science, distributed system and supply chain. She has published 42 research papers in reputed conference and journals.