Implementing image steganography: future Research challenges

Akshay Shinde[1] , Ankush Shinde[2], Prerana Nitalikar[3], Alkesha Pund[4] Mayur Chaudhari[5]
MCA II year student, Sinhgad Institute of Management And Computer Application(SIMCA), Narhe #First-Third Department

***Abstract*— Steganography derives from the Greek word steganos, meaning covered or secret, and graphy (writing or drawing).**

Innovation of technology and having fast Internet make information to distribute over the world easily and economically. This is made people to worry about their privacy and works. Steganography is a technique that prevents unauthorized users to have access to the important data. The steganography and digital watermarking provide methods that users can hide and mix their information within other information that make them difficult to recognize by attackers. In this paper, we review some techniques of steganography and digital watermarking in both spatial and frequency domains. Also we explain types of host documents and we focused on types of images.

This research paper describe how can we send a message secretly to the destination.

- **Using steganography, information can hidden in carriers such as images, audio files, text files, videos and data transmissions.**
- **In this study, I proposed a new framework of an image steganography system to hide a digital text of a secret message.**

***Keywords*— Steganography, digital text**

Introduction:

In today's world, communication is needed for transmitting the information. Everybody needs the security and secret of the conveying information. So as to send the information in a disguised way two systems are for the most part utilized. These techniques are Cryptography and Steganography. In cryptography, the information is encrypted utilizing the encryption key which is known to sender and receiver as it were. The message can not be gotten to by anybody without utilizing the encryption key. The encoded message can be changed, tempered or decoded by the attacker. Along these lines, to conquer the weaknesses of the cryptographic strategies, steganographic procedures have been sent. Steganography shrouds the information such that nobody can identify its nearness. In steganography, the covering up of the information inside any mixed media substance, for example, picture, video is alluded as "Implanting‖. So it is also known as the art of ―covered writing‖. Digital steganography is practice of secretly encoding information within the cover medium as a part of covert communication. Like the many security fields,steganography is the discipline where the steganographer attempts to hide the information and steganographic attacker tries to retrieve the hidden text.

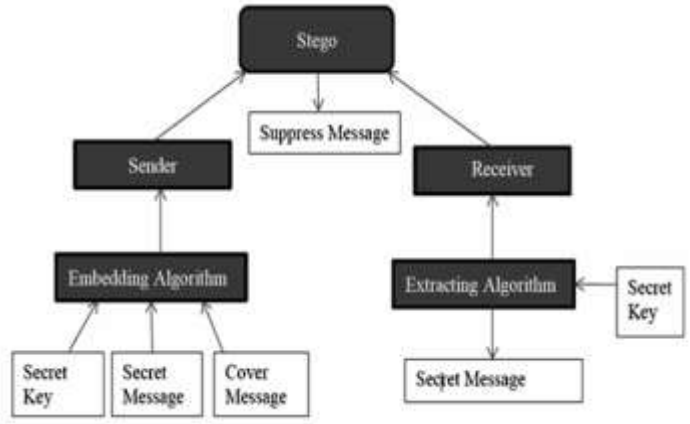
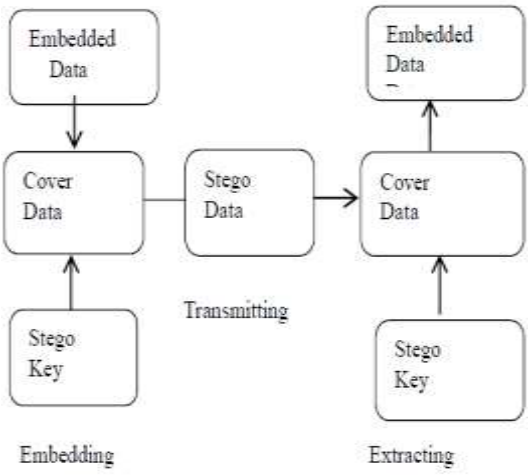


Fig. Steganography process flow

[II]: Steganography Model

Steganography comprises of the two terms that is the message and the cover picture in which the information is to be hided . Message is the secret data and the cover image act as the carrier for hiding the data. Together the cover media and the embedded message creates a stego-carrier. For example , when a crucial data(secret message) is hidden within a cover image, the resulting product is the stego-image. The possible formula of the process is

represented as- Cover media + embedded message + stego key = stego-medium.



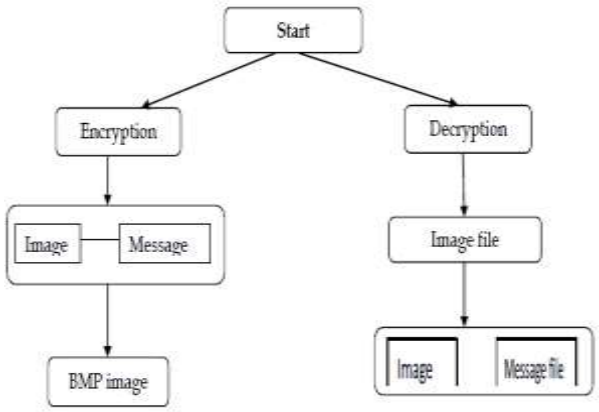
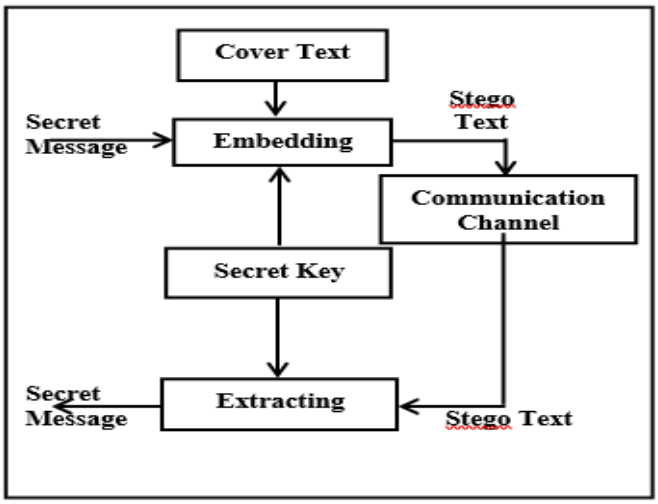


Figure: Block diagram for Steganography



Steganography Technique:

Pure steganography: Pure steganography is the process of embedding the data into the object without using any private keys. This type of steganography entirely depends upon the secrecy. This type of steganography uses a cover image in which data is to be embedded, personal information to be transmitted, and encryption decryption algorithms to embed the message into image.

[III]: Advantages/Disadvantages

Advantages:

1. Original image is very similar to altered image. Embedded data resembles Gaussian noise.
2. The hash is encrypted and sent with the message. When the recipient receives the message it is decoded. If the hash from the decoded message does not match the hash from the encrypted message, both the sender and recipient of the message know that it has been tampered with.
3. Hiding Information: - Steganography can also be used to protect identities and valuable data from theft, unauthorized viewing, or potential sabotage by concealing the message within a unsuspicious image.
4. E-commerce allows for an interesting use of steganography. In current e-commerce transactions, most users are protected by a username and password, with no real method of verifying that the user is the actual card holder. Biometric finger print scanning, combined with unique session IDs embedded into the fingerprint images via steganography allow for a very secure option to open ecommerce transaction verification.

Disadvantages:

1. Huge number of data, huge file size, so someone can suspect about it.
2. If this techniques is gone in the wrong hands like hackers, terrorist, criminals then this can be very much dangerous.
3. The three biggest areas of illegitimate steganography evolve around terrorism, pornography and data theft.
4. how much image/sound distortion is tolerable, before the user starts noticing something weird.
5. how much image/sound distortion is tolerable before the message is lost in the noises.
6. The confidentiality of information is maintained by algorithms, and if the algorithms are known then this technique is of no use.
7. Password leakage may occurs and it leads to the unauthorized access of data.
8. Someone else with steganography detection and cracking tool could expose this message.

[IV]: Applications:

Steganography can be used anytime you want to hide data. There are many reasons to hide data but they all boil down to the desire to prevent unauthorized persons from becoming

aware of the existence of a message. With these new techniques, a hidden message is indistinguishable from white noise. Even if the message is suspected, there is no proof of its existence. In the business world steganography can be used to hide a secret chemical formula or plans for a new invention.

Steganography can also be used for corporate espionage by sending out trade secrets without anyone at the company being any the wiser. Terrorists can also use steganography to keep their communications secret and to coordinate attacks. All of this sounds fairly nefarious, and in fact the obvious uses of steganography are for things like espionage. But there are a number of peaceful applications. The simplest and oldest are used in map making, where cartographers sometimes add a tiny fictional street to their maps, allowing them to prosecute copycats. A similar trick is to add fictional names to mailing lists as a check against unauthorized resellers. Most of the newer applications use steganography like a watermark, to protect a copyright on information. Photo collections, sold on CD, often have hidden messages in the photos which allow detection of unauthorized use. The same technique applied to DVDs is even more effective, since the industry builds DVD recorders to detect and disallow copying of protected DVDs.

There are various applications of steganography described as follows:

- Secret data storing
- E-Commerce
- Media
- Database Systems
- Digital Watermarking
- Protection of data alteration
- Confidential Communication

[V]: Literate Review:

Abusukhon (2012) focused a novel method for data encryption which is able to transformation file into an image file on both sides of system that is client and server. They have analyzed their algorithm by exploring the number of all possible key permutations.

Seetaiah Kilaru (2013) [2] describe that security is the main principle in any field. With the
successive attacks , it is a major test for the clients to secure the advanced pictures which are transmitting over web. Solitary Value Decomposition (SVD) gives an answer up to a more prominent degree.

Mostaghim (2014) [3] focuses making the visual cryptography more robust which can able to share sent and the received data with the generated message and will combine to the received share to reveal the hidden message. Their proposed scheme is evaluated in terms of Histogram, correlation coefficient, key sensitivity and key space. Their results are found to be improved in comparison to the traditional technique.

Hassan (2015) [4] described a secure communication scheme. It is a most identified system used as a carrier for the encoded data to be transmitted. At the transmitter end, two diverse disorganized frameworks are coupled and used to build another most identified framework. One of the yields of the most identified framework is utilized as a carrier for the disperse information.

Apoorva Shrivastava and Lokesh Singh (2016) describes three fundamental routines for secured correspondence accessible , in particular, cryptography, steganography and watermarking [5]-[7] . The researchers also describes the different methodologies for cryptography and steganography. They also focuses on problem identification and finding out that security is the main key for more robust.

[VI]: Future Scope:

• The scope of the research paper is to limit unauthorized access and provide better security during message transmission. To meet the requirements, I use the simple and basic approach of steganography.

• In this research paper, the proposed approach finds the suitable algorithm for embedding the data in an image using steganography, which provides the better security pattern for sending messages through a network.

• In the near future, the most important use of steganographic techniques will probably be lying in the field of digital watermarking. Content providers are eager to protect their copyrighted works against illegal distribution and digital watermarks provide a way of tracking the owners of these materials.

• Steganography might also become limited under laws, since governments already claimed that criminals use these techniques to communicate.

• The possible use of steganography technique is as following:

- Hiding data on the network in case of a breach.
- Peer-to-peer private communications.
- Posting secret communications on the Web to avoid transmission.

- Embedding corrective audio or image data in case corrosion occurs from a poor connection or transmission.

[VII]: Conclusion:

The researcher have studied for improving the steganalysis performance and also analyzing the hiding capacities of the existing research work. The steganalysis performance of state-of-the-art detectors is near-perfect against current steganographic schemes. A novel, robust and secure hiding schemes that can resist steganalytic detection must be implemented. Hiding schemes are characterized by three complementary requirements- security against steganalysis, robustness beside distortions in the transmission channel, and capacity in terms of the embedded method. This work would be able to be extended for different formats of images. This work may be extended using other transforms methods also.

In the present world, the data transfers using internet is rapidly growing because it is so easier as well as faster to transfer the data to destination. So, many individuals and business people use to transfer business documents, important information using internet.

• Security is an important issue while transferring the data using internet because any unauthorized individual can hack the data and make it useless or obtain information unintended to him.

• The future work on this project is to improve the compression ratio of the image to the text. This project can be extended to a level such that it can be used for the different types of image formats like .bmp, .jpeg, .tif etc., in the future. The security using Least Significant Bit Algorithm is good but we can improve the level to a certain extent by varying the carriers as well as using different keys for encryption and decryption.

[IX]: References:

[1] Abusukhon A, Talib M. A novel network security algorithm based on private key encryption. International conference on cyber security, cyber warfare and digital forensic (CyberSec) 2012 (pp. 33-7). IEEE.
[2] Kilaru S, Kanukuntla Y, Chary KB. An effective algorithm for image security based on compression and decomposition method. International Journal of Advanced Computer Research. 2013; 3(8); 289-94.
[3] Mostaghim M, Boostani R. CVC: chaotic visual cryptography to enhance steganography. International ISC conference in information security and cryptology (ISCISC) 2014 (pp. 44-8). IEEE.
[4] Hassan MF. Synchronization of hyperchaotic systems with application to secure communication. In IEEE international systems conference (Sys Con) 2015 (pp. 121-6). IEEE.
[5] Elbirt AJ, Paar C. An instruction-level distributed processor for symmetric-key cryptography. IEEE Transactions on Parallel and Distributed Systems. 2005: 16(5):468-80.
[6] Diffie W. Hellman ME. New directions in cryptography. IEEE Transactons on Informaton Theory. 1976;22(6):644-54.
[7]William S. Stallings W. Cryptography and network security, 4/E. Personal education India; 2006.
[5]https://en.wikipedia.org/w/index.php?title=Steganography&oldid=878881535