IJCRT.ORG ISSN : 2320-2882

INTERNATIONAL JOURNAL OF CREATIVE RESEARCH THOUGHTS (IJCRT)

An International Open Access, Peer-reviewed, Refereed Journal

Steganography for Public Security

Asha Durafe
Electronics Department
Shah & Anchor Kutchhi Engineering College

Ritika Desai
Electronics Department
Shah & Anchor Kutchhi Engineering College

Anushka Kashyap
Electronics Department
Shah & Anchor Kutchhi Engineering College

Suraj Gupta
Electronics Department
Shah & Anchor Kutchhi Engineering College

Pushkar Bagul
Electronics Department
Shah & Anchor Kutchhi Engineering College

Abstract - As technology is stepping up the ladder with each day, we need to find ways to transfer crucial data from one point to another in a secure manner. With the evolution of internet, it has become inevitable to store information in an electronic format. Our daily work is highly dependent on transmitting data over a network. Security of this information has become a major concern. To prevent unauthorized access of digital information, numerous data sharing techniques have been introduced. Cryptography and steganography are the most widely used techniques for securing the transmitted data.

Keywords – Steganography, Image, Cryptography, RSA Algorithm

I.INTRODUCTION

Steganography is obtained from the Greek word 'Steganos' meaning concealed or hidden and 'Graphia' meaning writing. Hence Steganography is a technique of hidden communication. In Steganography, the secret/important information such as text, audio, video or image is embedded into another multimedia file with the help of a key. Steganography disguises the information in the spare or non-essential bits of the cover file. It hides the fact that communication is taking place. Steganography is carried out so cleverly that an intruder cannot detect the existence of a hidden message inside the cover object.

In cryptography, the information is encrypted with the help of an encryption key. Cryptography makes the information illegible for an intruder. However, this encoded message can be meddled with or decoded by the intruder. This is why steganography is preferred over cryptography. A simply encrypted message can draw attention to itself, but steganography conceals the fact that there is a secret message. Our project intends to use Steganography to securely transfer criminal information (photo and information) from one CBI node to another. The image is hidden using Steganography and the information is password protected with a QR code. The two files are zipped with a password and mailed to the receiver using Raspberry Pi. The OTP is sent as a text message using GSM Module

II. TYPES OF STEGANOGRAPHY

a. Text Steganography

Commonly used methods in text steganography are number of tabs, white spaces, capital letters & every nth letter of a word to hide the message.
Even emoticons can be used to conceal secret information.

b. Audio Steganography

Phase coding, spread spectrum & low-bit encoding to embed secret information in audio steganography.

c. Video Steganography

Videos are generally a combination of images and audio which is advantageous as video signals carry a large amount of data enabling us to hide a lot of data in it.

d. Image Steganography

The cover image is bigger in size than the secret image. The unimportant bits of the cover image are used to embed the secret image.

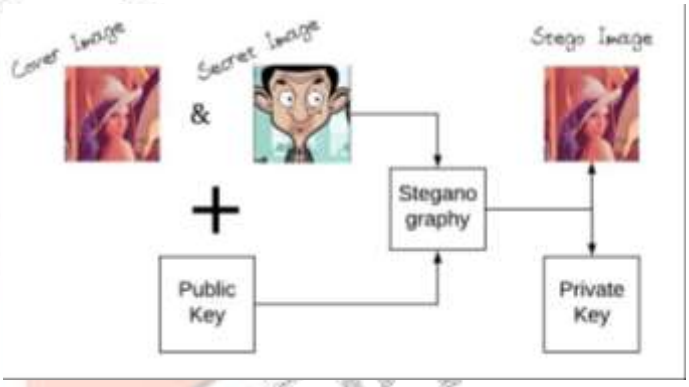
III. CHARACTERISTICS

- Capacity: This is the size of data that is hidden within the cover object. If the capacity is increased, a smaller cover object can be used. Thus higher capacity decreases the bandwidth required to transmit the image.

- Embedding efficiency: When inverse steganography is performed, the probability of error measured is called the embedding efficiency.
- Perceptual Transparency: When steganography is performed, some amount of noise is added to the cover object. Now, this distortion should not be visible to an intruder. When the original image and the cover image are kept side by side, the distortion should not be visible.
- Robustness: If a steganalysis attack is performed, the stego-object should be able to resist it.

IV.IMAGE STEGANOGRPAHY

In image steganography, the secret image is hidden in a cover image. The cover image is always bigger in size than the secret image so that the unused bits of the cover image can be used to conceal the secret image. The steganography is performed using a public key. The resultant image is called stego-image. Another key, called the private key, is also generated which is used by the receiver to perform inverse steganography to obtain the secret image from the stego-image. Steganalysis attack is a technique to determine the existence of a secret image.



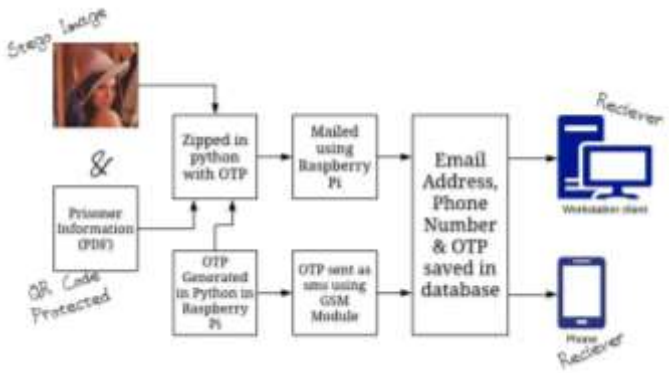
We use a matlab code to perform both, steganography as well as inverse steganography. We use the RSA algorithm.

V.RSA ALGORITHM

Ronald Rivest, Adi Shamir, and Leonard Adleman developed the RSA system. The RSA cryptosystem is a public-key cryptosystem that offers both encryption and digital signatures.

There are three steps in the RSA Algorithm:
1. Key Generation: Key generation RSA involves a public key and a private key.
2. Encryption: The public key can be known by everyone and is used for encrypting messages.
3. Decryption: Messages encrypted with the public key can only be decrypted in a reasonable amount of time using the private key.

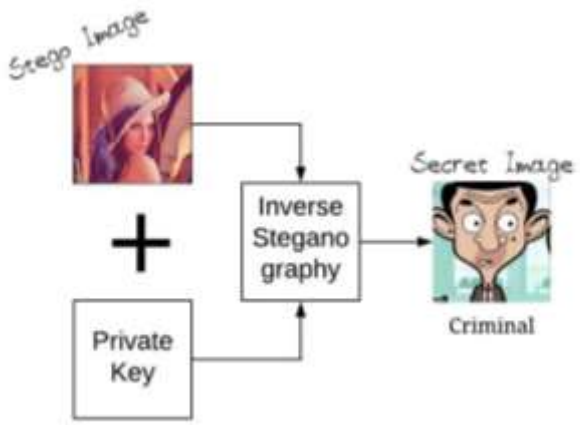
VI.TRANSMISSION PROCESS



The criminal information is QR code protected. The stego image and the QR code are zipped in the Raspberry Pi using a python code with a One Time Password. Using the Raspberry Pi mailing function and a python code, the zipped file is mailed to the recipient. The OTP generated is sent as a sms using the GSM Module integrate with the Raspberry Pi. The Email, Address, Phone Number & OTP is saved in the database of the system.

VII.INVERSE STEGANOGRAPHY

We now use the private key to obtain the secret image from the stego-image.



VIII.MERITS

- Draws no attention to the message
- High capacity
- Confidentiality
- Accurateness
- Imperceptibility

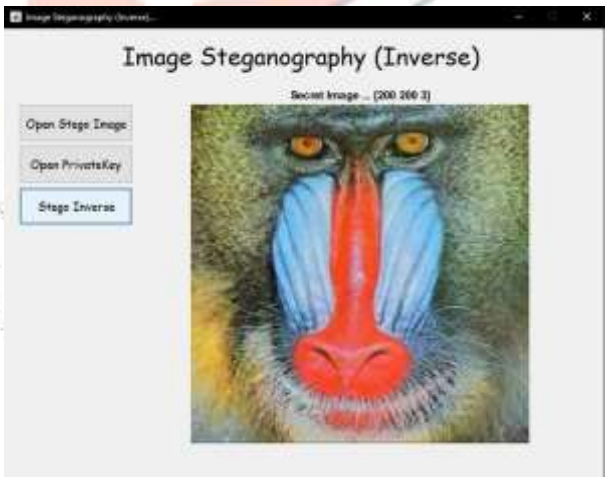
IX.DEMERITS

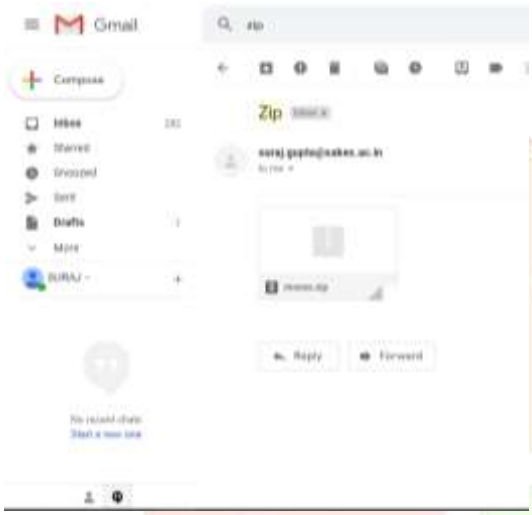
The three biggest areas of illegitimate steganography evolve around terrorism, pornography and data theft. During the research for this website the illegitimate uses of steganography were also found to be on a global scale, involved national security or were done on an academic basis in order to better understand the potential danger of steganography if created by individuals with ill-intentions.

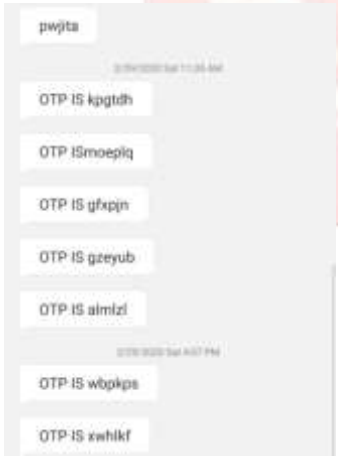
X.APPLICATIONS

- Secret data storing and sharing
- E-Commerce
- Media
- Database Systems
- Digital Watermarking
- Protection of data alteration
- Confidential Communication
- ID cards where the details are embedded in their photograph

XI.OUTPUTS







XII. CONCLUSION

In a nutshell, secure transmission of data is the rising concern with the advancements in technology. Steganography has its own pros and cons but is a better choice for sending secret information from one point to another without getting detected.

XIII. REFERENCES

[a] *Rina Mishra, Praveen Bhanodia*, "A Review on Steganography and Cryptography", 2015 International Conference on Advances in Computer Engineering and Applications

[b] *Mehdi Hussain, Ainuddin Wahid, Anthony T.S. Ho, Ki-Hyun Jung*, "Image Steganography in Spatial Domain: A Survey", ResearchGate

[c] *Abbas Cheddad, Joan Condell, Kevin Curran, Paul Mc Kevitt*, "Digital Steganography: Survey & Analysis of Current Methods", www.elsevier.com/locate/sigpro

[d] *Yashika Garg, Amneet Kaur*, "A Case Study on Steganography & it's Attacks", International journal of Engineering Trends & Technology (IJEET) – Vol 46 No. 8 May 2017

[e] *S. Nanda Kishor, Dr. Kodanda Ramaiah, Dr. S.A.K. Jilani*, "A review on steganography through multimedia", 2016 International Conference on Research Advances in Integrated Navigation Systems