# Metamorphic Cryptography

Namrata Singh
AKTU

## ABSTRACT
In today's digital world the ways communication are getting better day by day which in turn giving rise to one major problem which is the security of the data transmission, for protecting the secret information from the intruder the existence of the data should be hidden from others for increasing the security we can also make the secret data unreadable which can be done by using various steganographic techniques along with the cryptographic techniques. Steganography hides the existence of the information whereas cryptography makes the data unreadable making the communication robust.

## Keywords
Cryptography, Steganography, Crypto-Steganography.

## 1. INTRODUCTION
Steganography is the art of concealing the secret information in a cover object the cover can be an image, video, text or audio. Steganography hides the existence of the message which removes the chances of leak of information but if the existence is known then the security of the information is compromised. In case of cryptography the message is made unreadable by converting it into cipher text or any other format but it can be decoded if the method is known the security is compromised. What if we combine these two techniques of secure communication to increase the robustness of the communication system. In this survey paper the steganography will be used alongside cryptography for increasing the security of communication.

## 2. STEGANOGRAPHY
When existence of a message/information is hidden by concealing it in a cover file (Image, Video, Audio, Text, Network Headers etc that process is called steganography. In steganography the changes are done in the cover file without amending or distorting the message here the cover file undergoes changes. So if the existence is compromised then the secret information is also compromised. Fig. 1 shows the flowchart for the steganographic process.[2].

In the above Fig.1 Key is introduced which is used to encode/decode the secret message where the stego object is the file obtained after concealing the secret information in the cover file.[1] At the time of decoding the secret information original cover file is required to regenerate the secret message. There are various types of steganography based on the type of cover file used : [6]

- Image Steganography : Here an image is used as the cover file the LSB of the each RGB component of the image is replaced with the secret message.
- Video Steganography : In this type video is used as the cover file increasing the payload of the system which means we can hide more data in video as a video comprises of multiple frames and audio.
- Audio Steganography : In this steganography the audio file is used as the cover file. Concealing message in audio is typical as the range of frequencies audible to human are vast so this method is challenging.
- Text Steganography : In this steganography the secret message is hidden in the text. It can be done by any means by adjusting the vertical spacing between the lines or between the words or even adjusting the vertical and horizontal length of alphabets.
- Network Steganography : In this Steganography the network header is used as the cover for the secret information.

Above mentioned are the type of steganography now their are various techniques of steganography shown in the Fig. 2 below :[1]

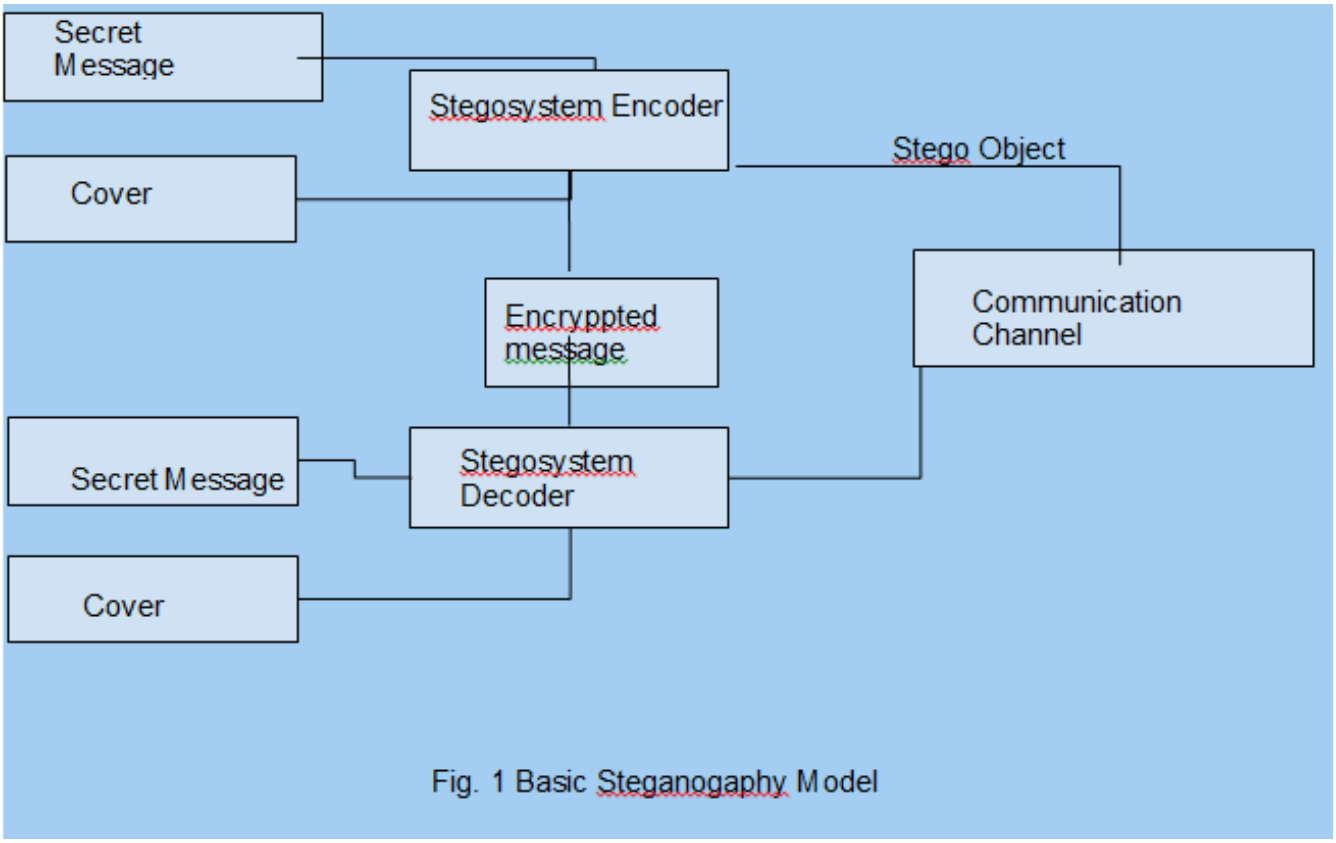


Fig. 1 Basic Steganogaphy Model

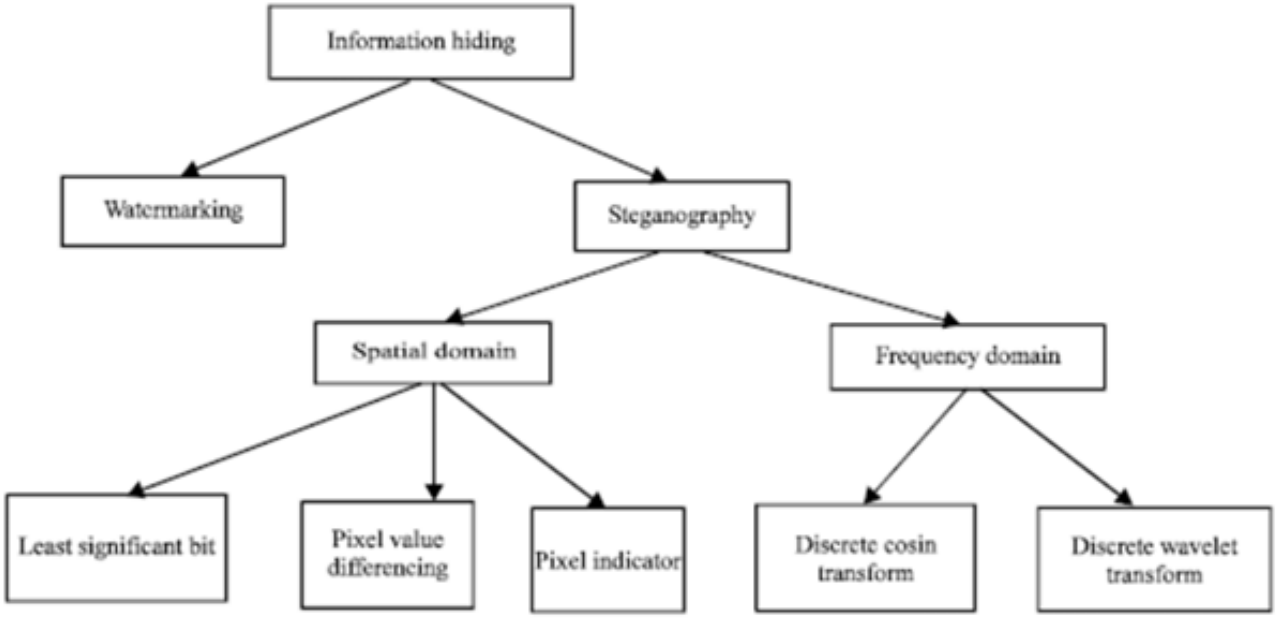


Fig.2 Types of Steganography

## 3. CRYPTOGRAPHY

In cryptography the message is disguised or distorted using different methods to make it unreadable which can only be decoded using the key used. In this technique not the word whole message is converted in cipher or other form.

The main aim of cryptography is make the message unreadable. In cryptography a key is required for both encryption and decryption. Fig. 3 below shows the basic model of the cryptography.[2,3]

Cryptography is categorised on the bases of the key used for encryption: [3,4]

- Asymmetric Key : In this two different keys are used for the encryption and decryption of the information one can keep a key public keeping one secret.
- Symmetric Key : In this one key is used for both encryption and decryption this key should be kept secret as it is used for the decryption of the information.

One Way : It uses no key to encrypt the information it is also known as hash function cryptography it is mostly used for generating digital signature as it is very fast as compared to other methods

## 3.1 Comparison Between Cryptography And Steganography

Cryptography and Steganography are two different ways for a secure communication cryptography focuses on disguising the information whereas steganography focus on hiding the existence/presence of the secret information. Both of them has their own limitation cryptography will be compromised if the disguise is blown and steganography is compromised if the existence is blown. Table 1 shows a comparison between the steganography and cryptography by considering various parameters.[1,3,5]

## 3.2 Crypto- Steganography

Cryptography and steganography both have their own limitations which can be overcome by using them together one is good in making the information unreadable and another excels in hiding the existence of the secret information. Once they are used together they'll increase the robustness of the communication system. For the crypto-steganography the secret data first encrypted using a key and converted into unreadable cipher text after that the encrypted data is embedded in a cover file and the transmitted over a communication channel.[1,6] This increases the secureness of the information removing the two limitations as they are fulfilling the limitation of each other because of the cryptography the data is encrypted and unreadable and because of steganography presence of secret information is hidden. Fig. 4 shows a basic flowchart for the crypto-steganography system.[1,3,5]

Bases On the combination of the steganography with other techniques it is categorised into three types :[1,6]

- Pure Steganography : When steganographic technique is used without any other process.
- Secret Key Steganography : When steganography is used with the secret key cryptographic technique.
- Public Key Steganography : When steganography is used with the public key cryptography technique.

For Increasing the robustness we can also bring on other encryption algorithms in use for example RSA algorithm, AES etc.[3,4]

# 4. LITERATURE REVIEW

In [1] this paper author has described the steganography and cryptography individually along with the terminologies and types. Author also explained the term crypto-steganography.

In [2] this paper author explained steganography and cryptography and used a approach in crypto-steganography where he used AES algorithm for increasing the robustness of the system.

In [3] this paper author explained various steganographic techniques and data hiding techniques along with various types and techniques of steganography.

In [4] this paper author explained various cryptographic techniques along with the use of RSA algorithm.

In [5] survey paper author explained the difference between cryptography and steganography.

In [6] this paper author pointed the different types of Steganography and cryptography along with their limitations and comparison

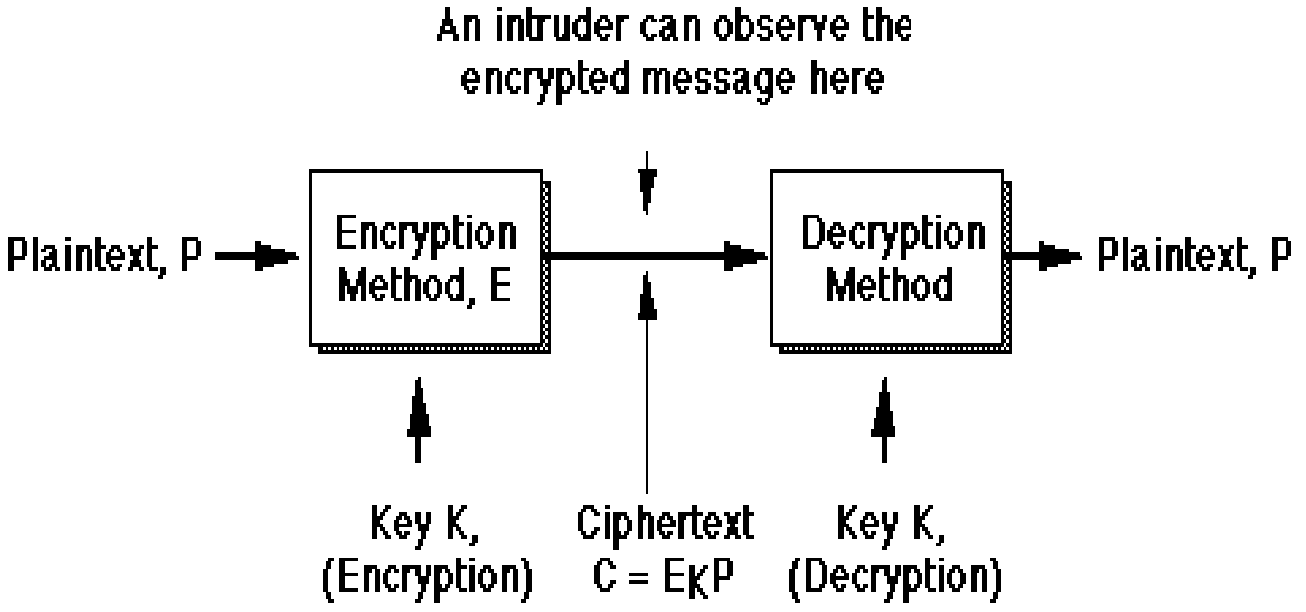


**Fig.3 Basic Model of Cryptography**

**Table 1 Comparison between Steganography and Cryptography**

| S.no | Steganography | Cryptography |
|---|---|---|
| 1. | Existence of secret information is hidden | Secret message is disguised or written secretly |
| 2. | Key is not necessary for encryption | Key is required for encryption |
| 3. | Various Cover files are Used (Audio, Video, Text etc) | It is text based as the message is encrypted |
| 4. | Still Under Development for other formats | Most of the algorithms are known |
| 5. | Here the cover file is altered keeping secret message intact | Here the message is altered to give it a disguise or make it unreadable |
| 6. | Compromised once known about the existence | Compromised once known about the technique used |
| 7. | Doesn't require high computing power for decoding | Require high computing cost for decoding |

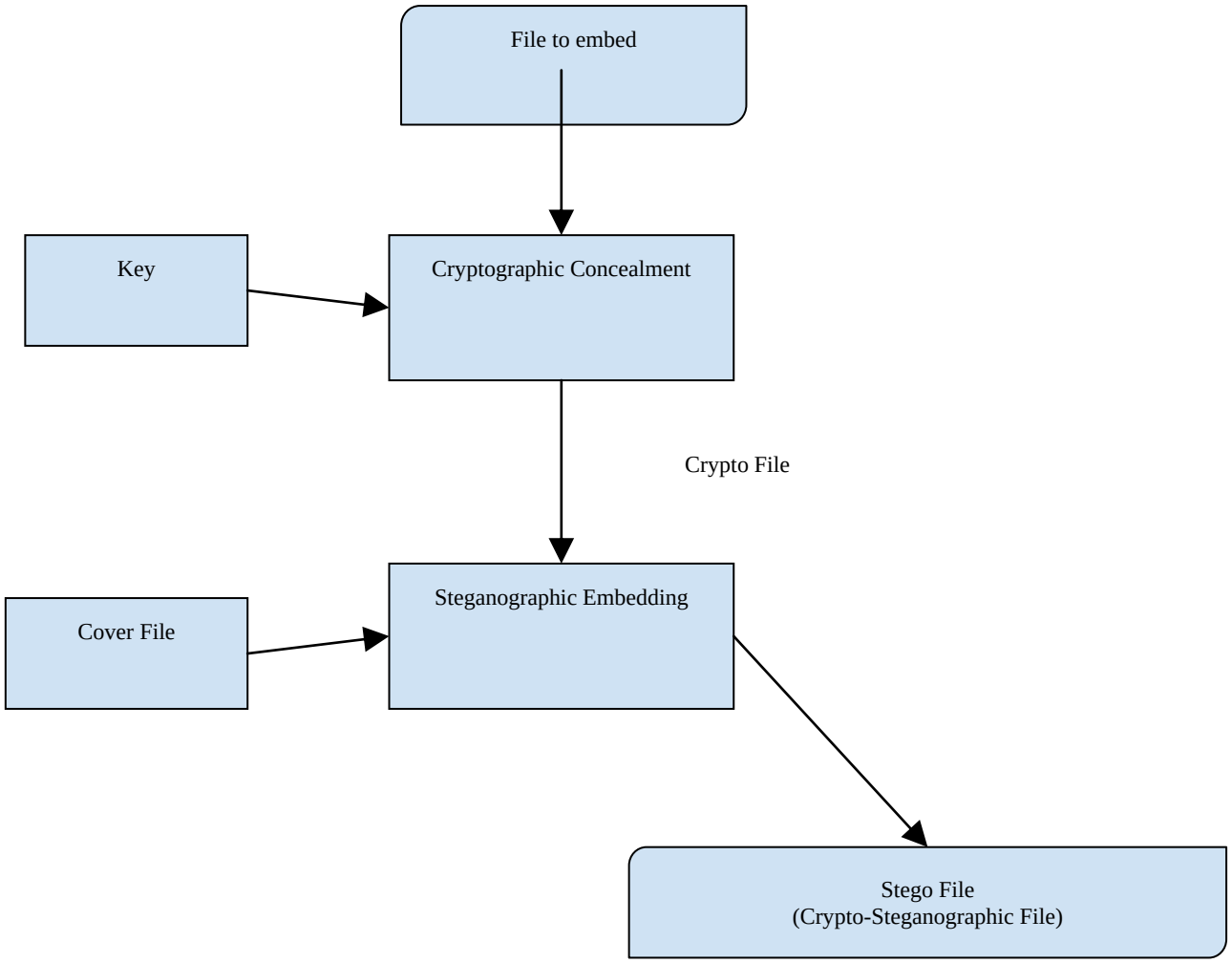


**Fig.3 Basic Model of Cryptography**

## 5. CONCLUSION

Secure communication is a must these days for doing so the techniques used for it must be capable of providing the desired security so that the sensitive information is not mishandled or misused. We came to know that both cryptography and steganography has limitations after combing both the techniques the robustness of the system increased and it became really difficult for a intruder to intercept the information and misuse it. Combination of cryptography and steganography makes the secret information both unreadable and undetectable.

## 6. REFERENCES

[1] Cryptography and Steganography – A Survey, A. Joseph Raphael, Dr. V. Sundaram, A.Joseph Raphael,Dr.V Sundaram, Int. J. Comp. Tech. Appl., Vol 2 (3), 626-630

[2] A Crypto-Steganography: A Survey, Md. Khalid Imam Rahmani, Kamiya Arora, Naina Pal, (IJACSA) International Journal of Advanced Computer Science and Applications, Vol. 5, No. 7, 2014

[3] A Survey on various types of Steganography and Analysis of Hiding Techniques, Navneet Kaur, Sunny Behal, International Journal of Engineering Trends and Technology (IJETT) – Volume 11 Number 8 - May 2014

[4] A Survey on Novel Visual Cryptographic Steganography Techniques, Shailendra M. Pardeshi, International Journal of Computer Applications (0975 – 8887) National Conference on Emerging Trends in Information Technology (NCETIT-2014)

[5] A Survey on Cryptography and Steganography, Niveditha R, International Journal of Science and Research (IJSR) ISSN (Online): 2319-7064

[6] A Survey Paper on Steganography and Cryptography, Z. V. Patel, S. A. Gadhiya, RESEARCH HUB – International Multidisciplinary Research Journal (RHIMRJ) Volume-2, Issue-5, May-2015 ISSN: 2349-7637 (Online)