An Overview of Image Steganography: Survey and Analysis

Arun Kumar Singh
arunsingh86@gmail.com

I) Introduction: Steganography is the specialty of concealing information in cover medium and the cover medium could be pictures, sound or video record. Any critical information could be covered up inside a computerized transporter picture. Steganography gives preferred administrations over cryptography. Reason is that cryptography conceals the substance of the message yet not the presence of the message. So nobody separated from the approved sender and beneficiary will know about the presence of the mystery information. Steganographic messages are frequently first encoded by some conventional means and afterward a cover picture is adjusted somehow to contain the scrambled message. The recognition of steganographically encoded bundles is called steganalysis.

***Keywords**: Digital Image, Secret Message, Cover, Stego Image, Encryption, Decryption, Steganography, Watermarking*

*****

I. LITERATURE SURVEY:

In this paper, we propose three proficient Steganography methods that are utilized for concealing mystery messages. They are LSB based Steganography, Steganography utilizing the last two critical bits and Steganography utilizing inclining pixels of the picture. Symmetric and awry key cryptography has been utilized to encode the message.

Information security over the systems is a vital test for scientists and PC engineers for quite a long time. Web is an awesome comfort which offers secure information correspondence of vital messages, mystery data, assortment of pictures and records. Keeping in mind the end goal to keep the unapproved access of imperative messages and pictures from vindictive fraudsters, one have to make it more secure by sending the scrambled messages over the systems. To fulfill and assemble such secure frameworks, numerous information covering up and encryption methods have been proposed over the most recent couple of decades. Both the information stowing away and encryption strategies are observed to be the primary instruments in information security. Be that as it may, utilization of previous component has been expanding as of late because of a few negative marks have been found in the later instrument. [2]

II. PROPOSED METHODOLOGY AND DISCUSSION

The formal instrument of information encryption utilizes the strategy to change over a message into a ciphertext message by utilizing some encryption calculation and the ciphertext message is then sent to the beneficiary who has the approval to get and get the first message. To get the first message which has been sent by the sender, beneficiary uses a key to get the decoded message. Any pernicious client who does not have the key can't break the security of ciphertext which resembles some inane code. In spite of the fact that information encryption is turned out to be a protected technique to shroud information, it has a few shortcomings. For instance, now and again appearance of ciphertexts could give an unmistakable motivation to an unapproved client and this may prompt unapproved access to the first substance by breaking it. Therefore the first collector would not have the capacity to get the figure writings sent

 ISSN: 2321-8169
330 – 332

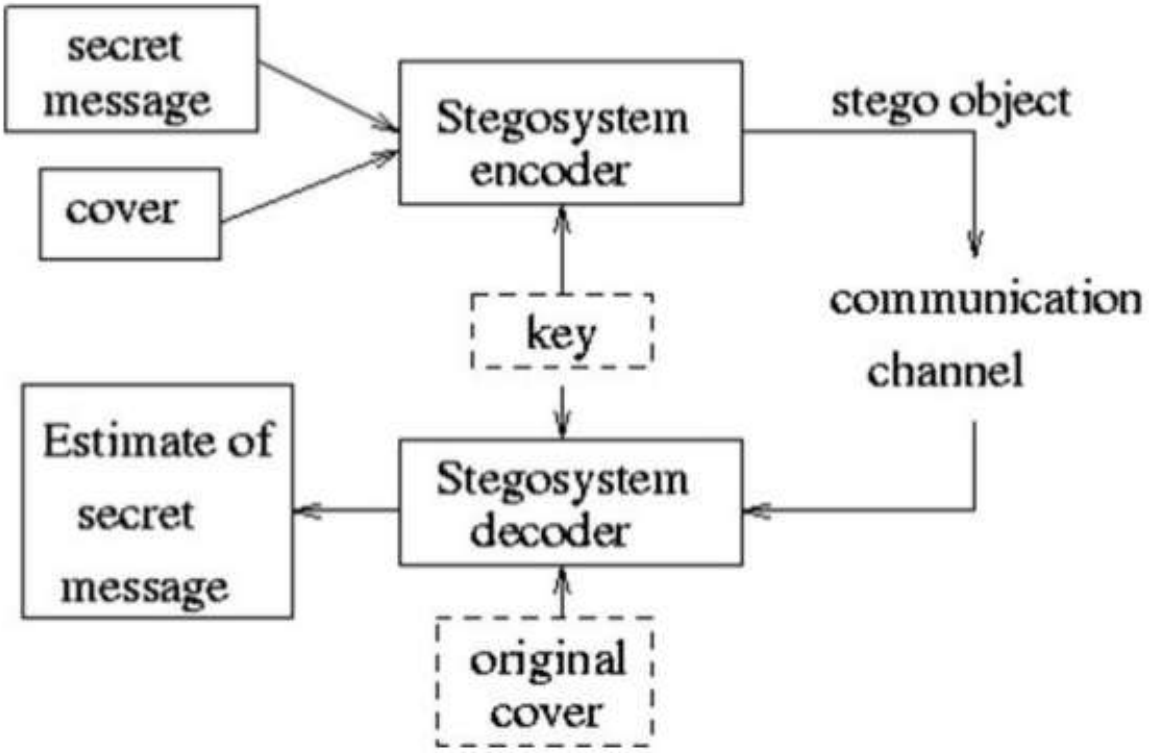

Fig:1 Steganography in Digital Images [3]

by the sender. Frequently unapproved clients may exploit by devastating the figure content when it can't be recuperated. Another real downside to encryption is that the presence of information is not covered up. Information that has been encoded, albeit mixed up, still exists as information. On the off chance that sufficiently given time, somebody could in the long run decode the information. Thus inquire about on information covering up has been expanding as of late. An answer for this issue is information covering up. Information concealing procedures could assume a noteworthy part to install critical information into mixed media records, for example, pictures, recordings or sounds. Since computerized pictures are obtuse to human visual framework, in this way pictures could be great cover bearers. Information stowing away has two noteworthy applications – watermarking and steganography. Watermarking only develops the cover source with additional data. Steganographic methods are utilized to store watermarks in information. Steganography is an antiquated craft of concealing messages for making the messages not perceivable to pernicious clients. For this situation, no substitution or change was utilized. The concealed message is plain, yet unsuspected by the peruser. Steganography's aim is to conceal the presence of the message, while cryptography scrambles a message so it can't be caught on. Steganography has been generally utilized, incorporating into late recorded circumstances and the present day. Conceivable changes are interminable and known illustrations include: (i) shrouded messages inside wax tablets, (ii) concealed messages on delegate's body, (iii) shrouded messages on paper written in mystery inks, under different messages or on the clear parts of different messages, and (iv) specialists utilized photographically

Types of Steganography:

1)Secret Key Steganography

2)Public Key Steganography

3)Linguistic Steganography

4)Semagrams:

5)Visual Semagrams

6)Text Semagrams

7)Open Code

8) Technical Steganography:

9) Frequency Domain:

10) Audio Steganography:

REFERENCES

[1] A. Cheddad, J. Condell, K. Curran and P. Mc Kevitt,"Digital Image Steganography: Survey and Analyses of Current Methods".Signal Processing, Volume 90, Issue 3, March 2010, Pages 727-752.

[2] Maiti C., Baksi D., Zamider I., Gorai P., Kisku D.R. (2011) Data Hiding in Images Using Some Efficient Steganography Techniques. In: Kim T., Adeli H., Ramos C., Kang BH. (eds) Signal Processing, Image Processing and Pattern Recognition. Communications in Computer and Information Science, vol 260. Springer, Berlin, Heidelberg

[3] https://www.slideshare.net/manikaarora589/steganography-48398473