**Available Online at www.ijcsmc.com**

International Journal of Computer Science and Mobile Computing

**A Monthly Journal of Computer Science and Information Technology**

**ISSN 2320–088X**

***IJCSMC, Vol. 4, Issue. 7, July 2015, pg.150 – 155***

**RESEARCH ARTICLE**

# MULTI LEVEL STENOGRAPHY METHOD FOR PROTECTED DATA TRANSFER

**Mr. Mrigank Yadav**
Research Scholar, Dept. of CSE, Oriental University indore( india)
yadav.mrigank2@gmail.com

**Mr. Harsh Saki**
Asst. Prof., Dept. of CSE, Oriental University indore (india)
harshneema@gmail.com

***Abstract - Steganography is a part of cryptography, the usage of codes. While cryptography gives security, steganography is wanted to give secret. Steganography is a framework for furtively passing on. Steganography is a procedure that incorporates covering a message in a fitting conveyor for occasion a photo or a sound archive. The transporter can then be sent to a gatherer with no other individual understanding that it contains a disguised message. This is a methodology, which can be used for example by social freedoms relationship in extreme states to grant their message to the outside world without their own specific government being aware of it. In this article we have endeavored to clarify the different systems towards utilization of Steganography using "intuitive media" record (content, static picture, sound and feature)[1]. Steganalysis is an as of late creating appendage of data setting up that searches for the recognizing verification of steganographic spreads, and if possible message extraction. It is similar to cryptanalysis in cryptography. The framework is out of date creating monster that have expanded constant perceive as it have as of late entered the universe of modernized correspondence security. Target is to keep the message being examined and in addition to cover its presence[2].***

***Keywords— Steganography, Cryptography, Image hiding***

## I. INTRODUCTION

The late advancement in computational power and development has pushed the prerequisite for outstandingly secured data correspondence. One of the best systems for secure correspondence is Steganography-a covert piece. It is a forte of hiding the very vicinity of conferred message itself. The approach of using steganography as a piece of conjunction with cryptography, called as Dual Steganography, develops an in number model which incorporates a lot of troubles in perceiving any disguised and mixed data. Using cryptographic frameworks to scramble data before transmission may keep any kind of security issues. In any case the hidden appearance of mixed data may animate suspicion. Thusly using steganography inside steganography, offer move to upgraded type of twofold steganography which will give better security. This paper displays a system for hiding data with two level of security to introduce data nearby extraordinary perceptual straightforwardness and high payload limit. Here the secret data is not restricted to pictures just furthermore fitting to any substance, sound or feature.[3]

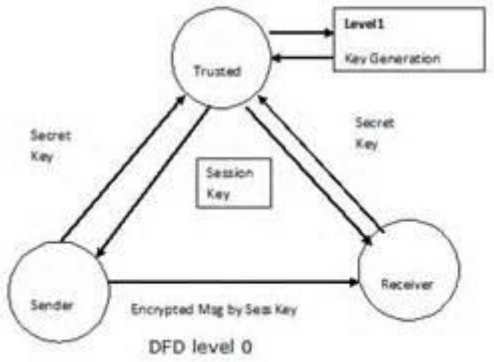

**Fig 1: Cryptographic flow Diagram**

Steganography is the examination of imperceptible correspondence which covers any private data inside a chaste looking spread thing. The announcement Steganography is gotten from the Greek words "stegos" implying "spread" and "grafia" connoting "piece" describing it as "secured composed work" .Steganography is not exactly the same as cryptography. The goal of cryptography is to give secure trades by changing the data into a structure that can't be gotten on. Steganography methodology, on the other hand, cover the vicinity of the message itself, which makes it unbalanced for a third individual to make sense of the message. Not in any way like steganography, sending mixed information may draw thought. Steganography today, on the other hand, is by and large more perplexing, allowing a customer to hide a considerable measure of information inside picture and sound reports.[4]

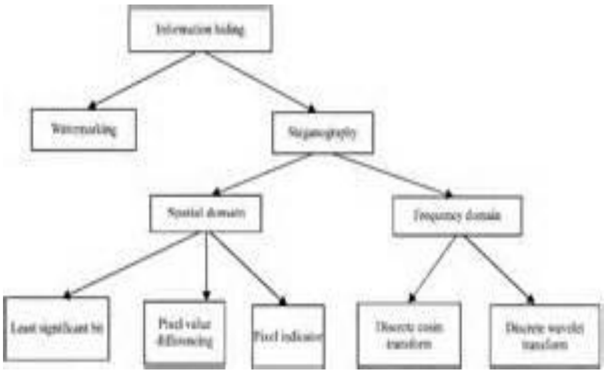

**Fig 2: Steganography flow**

These sorts of steganography consistently are used as a piece of conjunction with cryptography so that the information is doubly secured; first it is encoded and a short time later covered so that a foe needs to first discover the information (an often troublesome task independent from anyone else) and a while later interpret it. Properly, cryptography is not the immense response for secure correspondence yet simply bit of the course of action. Both techniques can be used together to better guarantee information .

The model involves Carrier (C), Secret Data (D), and Stego Key (K). Transporter is the spread question in which the puzzle message is embedded. Riddle data can be any kind of mystery data i.e. plain substance, figure substance or other picture. Key fundamentally used to ensure that simply recipient having the translating key will have the ability to recuperate the secret message from the spread article. With the help of introducing figuring, the secret data is embedded into the spread question in a way that does not change the first picture in a human discernible way. Finally, the stego object which is the yield of the approach is just the spread article with introduced puzzle information.[5]

## II. RELATED STUDY

The investigation of securing a data by encryption is Cryptography however the system for disguising riddle messages in diverse messages is Steganography, so that the puzzle's to a great degree vicinity is secured. The expression "Steganography" delineates the framework for covering psychological substance in a substitute medium to avoid area by the intruders. This paper exhibits two new procedures wherein cryptography and steganography are combined to scramble the data and notwithstanding cover the mixed data in an other medium so the way that a message being sent is covered up. One of the frameworks exhibits to secure the photo by changing over it into figure message by S-DES count using a riddle key and shroud this substance in a substitute picture by steganographic framework. A substitute procedure exhibits another system for disguising a photo in a substitute picture by encoding the photo clearly by S-DES count using a key picture and the data got is covered up in a substitute picture. The proposed strategy keeps the potential results of steganalysis as well.

[6] Shilpa Gupta, Geeta Gujral and Neha Aggarwal built up an upgraded LSB calculation which inserts the mystery information

Next, the stego image1 is considered as the mystery information and covered up inside the spread image2 utilizing 4-bit LSB calculation and stego key2 after which last stego picture is produced.

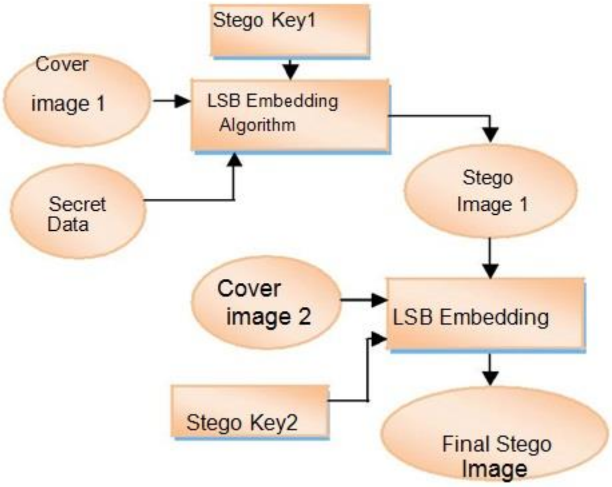

**Fig.4-Sender end  Steganography**

The calculation acts as takes after:
1) Cover image1 is isolated into RGB planes.

2) Secret information taken is then changed over into parallel structure.
3) Those qualities are isolated into upper and lower snack which are inserted in two different planes of the spread image1.
4) Upper snack are implanted in green plane and lower snack in red plane.
5) Stego key is implanted inside the blue plane.
6) After which, all the three planes are consolidated to produce stego image1.
7) Stego image1 is then deciphered as mystery information and installed in the spread image2 utilizing the same calculation and in this way the last stego picture is produced.

**Information Extraction Process :**
In information extraction process we utilizing the last stego picture, the stego image1 is separated utilizing stego key1 and LSB recuperation calculation. Next, from stego image1, mystery information is removed by utilizing stego key2 and same LSB recuperation calculation. The proposed plan is irreversible one as the spread picture is not recouped at the collector side.

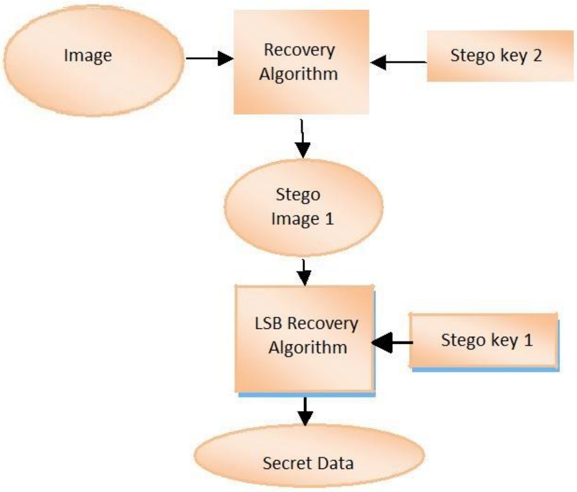

**Fig.5-Receiver end Steganography**

The calculation fills in as takes after:

1) Final stego picture is isolated into RGB planes.
2) Stego key which goes about as secret key is entered whichis then confirmed with the put away key that is installed in the blue plane of spread image2.
3) If the key is coordinated then the upper and lower snack of double mystery information is extricated from green and red planes separately.
4) Then the upper and lower snack are consolidated to make the double type of stego image1.
5) Finally, the first stego image1 is gotten from double shape.

6) Next, utilizing the same calculation the first mystery information is recovered from stego image1.

## V. EXPECTED OUTCOME

Information concealing framework is said to be secured on the off chance that we have learning of concealing information by utilizing calculation which does not help the busybody to distinguish shrouded information or know the mystery information. Stego keys assume an imperative part in enhancing the security of information concealing method. As in the proposed work, two diverse stego keys are utilized, the framework is said to be twofold secured. Keeping in mind the end goal to upgrade the security, in proposed work as opposed to consolidating cryptography with steganography, just steganography is utilized twice. The purpose for this is that National Security Agency (NSA) has built up a quantum PC that could break most sorts of encryption calculations. So if the steganography is somewhat vanquished then mystery information gets to be obvious which can be split utilizing quantum PC. Accordingly if steganography is utilized two times, then regardless of the fact that at first level steganography gets crushed then the second level will keep the mystery information secured.

## VI. CONCLUSION

Information security has transformed into a champion amongst the most colossal issues in light of the exponential improvement of web customers. Unapproved access to puzzle data can have veritable repercussions like fiscal disaster et cetera. Steganography is one of the courses of action whose goal is to hide the vicinity of granted message. In this paper, exceedingly secured data disguising technique has been shown where steganography is used inside steganography. The proposed system inserts data in two spread pictures using Six bit LSB strategy. The secret data is concealed in twofold structure in two spread pictures in view of which twofold protection has been given to ordered data which can be any substance, sound, component or picture. The trial results exhibit that the proposed arrangement can be a respectable alternative for secure correspondence where two level of security is obtained in conjunction with high payload point of confinement and incredible subtlety.[13]

## VII. FUTURE WORK

A few issues and ideas that stay unaddressed can be performed later on. For example, with the assistance of pre-emptive approach more data can be included for precise, auspicious investigation with high exactness. It can likewise be utilized for quantitative & subjective examination, rank requesting, and so forth. We likewise implant the source code of our proposed plan in Java. In our proposed plan in order to utilize the advantages of a methodology like open source.

## VIII. ACKNOWLEDGEMENT

This research work is self financed but recommended from the institute so as to improve the security breaches with current techniques. Thus, the authors thank the anonymous reviewers for their valuable comments, which strengthened the paper. The authors also wish to acknowledge oriental university administration for their support & motivation during this research. They also like to give thanks for discussion regarding the situational awareness system & for producing the approach adapted for this paper.

## REFERENCES

[1] KURAK, C., AND J. MCHUGHES, "*A CAUTIONARY NOTE ON IMAGE DOWNGRADING*", IN IEEE COMPUTER SECURITY APPLICATIONS CONFERENCE 1992, PROCEEDINGS, IEEE PRESS, 1992,PP.153-159.

[2] Clair, Bryan, *"Steganography: How to Send a Secret Message",8*-Nov.-2001/20011008/steganography.shtml.
[3]Moller. S.A., Pitzmann, and I. Stirand, "*Computer Based Steganography: How It Works and Why Therefore Any Restrictions on Cryptography Are Nonsense, At Best*", in Information Hiding: First International Workshop, Proceedings, vol. 1174 of Lecture Notes in Computer Science, Springer,1996,pp.7-21.

[4]Gruhl, D., A. Lu, and W. Bender, "*Echo Hiding in Information Hiding*", First International Workshop, Proceedings, vol. 1174 of Lecture Notes in Computer Science, Springer,1996,pp.295-316.

[5] Sujay Narayana and Gaurav *Prasad "Two new approaches for secured image steganography using cryptographic techniques and type conversions" ,* An International Journal(SIPIJ) Vol.1, No.2, December 2010

[6]van Schyndel, R. G., A. Tirkel, and C. F. Osborne, "A *Digital Watermark*", in Proceedings of the IEEE International Conference on Image Processing, vol. 2, 1994, pp. 86-90.

[7]Johnson, N. F., and S. Jajodia, "Exploring Steganography: Seeing the Unseen", IEEE Computer, vol. 31, no. 2, 1998, pp. 26-34.

[8]Rhodas, G. B., "*Method and Apparatus Responsive to a Code Signal Conveyed Through a Graphic Image*", U.S. Patent5,710,834,-1998.

[9]Swanson, M. D., B. Zhu, and A. H. Tewk, "*Transparent Robust Image Watermarking*", in Proceedings of the IEEE International Conference on Image Processing, vol. 3, 1996, pp.211-214.

[10]Pitas, I., "*A Method for Signature Casting on Digital Images*," in International Conference on Image Processing, vol.3,IEEE-Press,1996,pp.215-218.

[11]Maxemchuk, N. F., "*Electronic Document Distribution*", AT&T Technical Journal, September/October 1994, pp.73-80.

[12]Low, S. H., et al., "*Document Marking and Identifications Using Both Line and Word Shifting*," in Proceedings of Infocom'95,1995,pp.853-860.

[13]Low, S. H., N. F. Maxemchuk, and A. M. Lapone, "*Document Identification for Copyright Protection Using Centroid Detection*", IEEE Transactions on Communications, vol. 46, no. 3, 1998, pp. 372-383.