ISSN:0975-9646

# Dual Stenography Approach For Secure Data Communication

Kirti Shukla[1], Asst. Prof. Priyanka Vijaywargiya[2]

[1]*PG Scholar Department of Computer Science Engineering*
*Shri Vaishnav Institute Of Technology & Science, Indore (M.P.),India*

[2]*Associate Prof. Department of Computer Science Engineering*
*Shri Vaishnav Institute Of Technology & Science, Indore (M.P.),India*

***Abstract*** **- Steganography is the dim cousin of cryptography, the utilization of codes. While cryptography gives security, steganography is planned to give mystery. Steganography is a system for secretly conveying. Steganography is a process that includes concealing a message in a proper bearer for instance a picture or a sound document. The transporter can then be sent to a collector without any other person realizing that it contains a concealed message. This is a procedure, which can be utilized for instance by social liberties associations in severe states to impart their message to the outside world without their own particular government being mindful of it. In this article we have attempted to explain the diverse methodologies towards usage of Steganography utilizing "interactive media" record (content, static picture, sound and feature).[1] Steganalysis is a recently developing limb of information preparing that looks for the distinguishing proof of steganographic spreads, and if conceivable message extraction. It is like cryptanalysis in cryptography. The system is antiquated developing beast that have increased unchanging recognize as it have recently entered the universe of computerized correspondence security. Target is to keep the message being perused as well as to conceal its presence.[2]**

**Keywords— Steganography, Cryptography, image hiding, least-significant bit (LSB) method**

## I. INTRODUCTION

The The late development in computational force and innovation has pushed the requirement for exceptionally secured information correspondence. One of the best strategies for secure correspondence is Steganography-an undercover composition. It is a specialty of concealing the very presence of imparted message itself. The methodology of utilizing steganography as a part of conjunction with cryptography, called as Dual Steganography, builds up a strong model which includes a great deal of difficulties in recognizing any concealed and scrambled information. Utilizing cryptographic systems to scramble information before transmission may prevent any sort of security issues. Be that as it may the disguised appearance of scrambled information may stimulate suspicion. Along these lines utilizing steganography inside steganography, offer climb to enhanced form of double steganography which will give better security. This paper exhibits a procedure for concealing information with two level of security to install information alongside great perceptual straightforwardness and high payload limit. Here the mystery information is not limited to pictures just additionally appropriate to any content, sound or feature.[3]

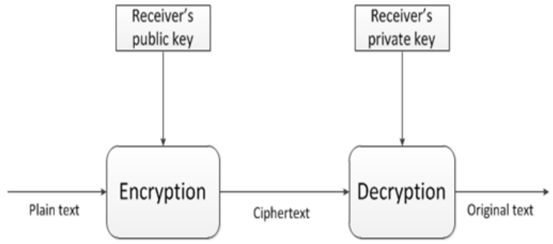

**Fig 1: Cryptographic flow**

Steganography is the investigation of undetectable correspondence which shrouds any private information inside a blameless looking spread item. The statement Steganography is gotten from the Greek words "stegos" signifying "spread" and "grafia" signifying "composition" characterizing it as "secured written work" .Steganography is not quite the same as cryptography. The objective of cryptography is to give secure interchanges by changing the information into a structure that can't be caught on. Steganography procedures, then again, conceal the presence of the message itself, which makes it awkward for a third individual to figure out the message. Not at all like steganography, sending scrambled data may draw consideration. Steganography today, then again, is altogether more complex, permitting a client to conceal a lot of data inside picture and sound documents. [4]

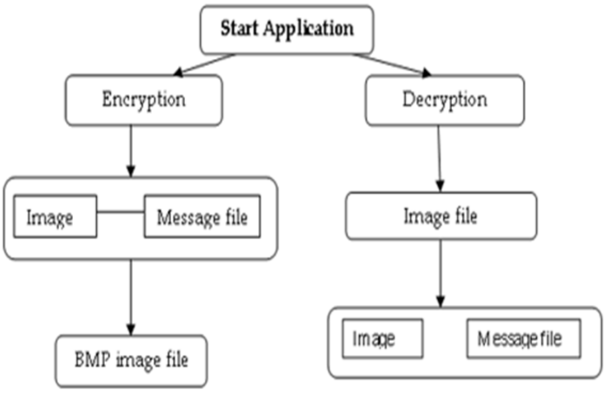

**Fig 2: Steganography flow**

These types of steganography regularly are utilized as a part of conjunction with cryptography so that the data is doubly secured; first it is encoded and afterward shrouded so that an enemy needs to first find the data (a frequently troublesome assignment all by itself) and afterward decode it. Appropriately, cryptography is not the great answer for secure correspondence yet just piece of the arrangement. Both procedures can be utilized together to better ensure data .

The model comprises of Carrier (C), Secret Data (D), and Stego Key (K). Transporter is the spread question in which the mystery message is implanted. Mystery information can be any sort of secret information i.e. plain content, figure content or other picture. Key primarily used to guarantee that just beneficiary having the interpreting key will have the capacity to recover the mystery message from the spread article. With the assistance of installing calculation, the mystery information is inserted into the spread question in a manner that does not change the first picture in a human noticeable manner. At long last, the stego object which is the yield of the methodology is only the spread article with installed mystery information.[5]

## II. RELATED STUDY

The exploration of securing an information by encryption is Cryptography though the strategy for concealing mystery messages in different messages is Steganography, so that the mystery's extremely presence is covered. The term "Steganography" depicts the system for concealing cognitive substance in an alternate medium to keep away from location

by the interlopers. This paper presents two new strategies wherein cryptography and steganography are consolidated to scramble the information and in addition to shroud the scrambled information in an alternate medium so the way that a message being sent is hidden. One of the systems demonstrates to secure the picture by changing over it into figure message by S-DES calculation utilizing a mystery key and hide this content in an alternate picture by steganographic system. An alternate strategy demonstrates another method for concealing a picture in an alternate picture by encoding the picture straightforwardly by S-DES calculation utilizing a key picture and the information got is hidden in an alternate picture. The proposed technique keeps the potential outcomes of steganalysis too.

[6] Shilpa Gupta, Geeta Gujral and Neha Aggarwal developed an enhanced LSB algorithm which embeds the secret data only in one i.e. blue component instead of all RGB components. With this new technique, the performance of LSB has been improved which leads to the minimization of the distortion level that is negligent to human eye. This will increase the robustness but will decrease the payload capacity.

[7]Shailender Gupta, Ankur Goyal and Bharat Bhushan developed a technique for hiding data using LSB steganography and cryptography where the secret information is encrypted using RSA or Diffie Hellman algorithm before embedding in the image with the help of LSB method. With the proposed technique, time complexity is increased but high security is achieved at that cost. Tanmay Bhattacharya, Nilanjan Dey and S. R. Bhadra Chaudhuri proposed a DWT based Dual steganographic technique. By using DWT, a cover image is decomposed into four subbands. Two secret images are hidden within HL and HH subbands respectively by usage of a pseudo random sequence and a session key. By this technique fair amount of information is transferred in a secured way with an acceptable level of imperceptibility.

[8] K.Sakthisudhan and P.Prabhu proposed a dual steganography approach in which the secret data is firstly converted to encrypted form and then LSB technique of steganography is used to embed it within cover object. By this method, message is transferred with utmost security and can be retrieved without any loss of data.

[9] Rosziati Ibrahim and Teoh Suk Kuan developed a SIS (Steganography Imaging System) in which two layers of security are used, firstly username and password are required and once login done, key is used to embed the secret data. Due to this, integrity and privacy is maintained.

[10] Weiqi Luo, Jiwu Huang and Fangjun Huang proposed a technique in which the secret data is embedded in the edges of the objects of an image. With the proposed scheme, embedding regions are selected according to size of secret message and difference between two consecutive pixels in cover image. Here, LSB matching revisited is used which uses a pair of pixels as embedding unit. Sharper images are selected for hiding data so that good security and visual quality is increased.

[11] Mazen Abu Zaher developed a modified LSB method in which 8 bit ASCII codes of secret message are converted into 5 bit codes with the aid of encryption algorithm and then embedded in the cover image by using LSB method. So with this scheme, more amount of information can be hidden with a level of protection.Shabir A. Parah, Javaid A. Sheikh, Abdul M. Hafiz and

## III. PROBLEM DOMAIN

The The objective of this examination work is to investigate double steganography and its applications in secure, continuous way. Steganography is the procedure of concealing a mystery message inside a bigger one such that the vicinity of the mystery message can't be distinguished. For this situation, client verification data will be installed in crude sound information in a system. This can be fulfilled by utilizing the slightest critical bit of a LSB test to store one bit of an encoded message. With a fitting decoder, the mystery message can be separated from an alternate LSB test while the ordinary client would have no clue that it exists. In the proposed plan, double picture steganography is utilized. The purpose for utilizing picture steganography is that pictures are more prominent among the web clients. In this work, 4 bit LSB substitution method falling under the class of spatial space is utilized by which high security is attained to for mystery information alongside great measure of impalpability and additionally high payload limit.[12]

## IV. PROPOSED SOLUTION

This 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.

This process is based on two components

1) Data hiding

2) Data processing

**Data Hiding:**

The block diagram for the proposed data hiding technique is shown in Fig.1. Here two cover images are used i.e. cover image1 and cover image2. For providing more security two stego keys are used which are different from each other. The stego key used is of 10 bit in length. The key can be made of numbers, characters, and symbols but should be of 10 bit length. These keys are hidden in the cover image during the hiding process. This should be known at the receiver side during the decoding process for retrieving the secret file.As shown in Fig.; the secret data has been embedded inside the cover image1 with the help of 4 bit LSB embedding algorithm along with the stego key1 mainly used for security purpose from which stego image1 is generated. Next, the stego image1 is considered as the secret data and hidden inside the cover image2 using 4-bit LSB algorithm and stego key2 after which final stego image is generated.

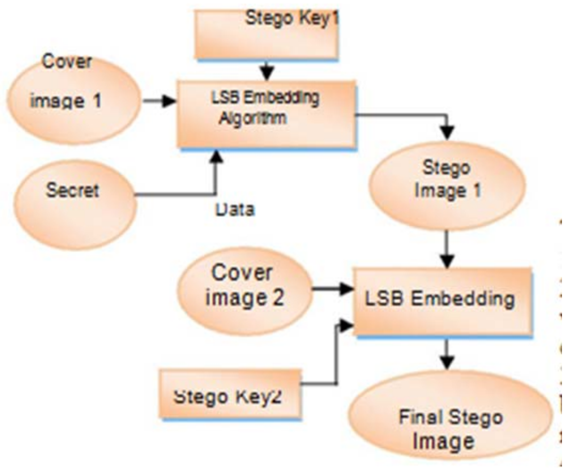

**Fig.4-Sender end Steganography**

The algorithm works as follows:

1) Cover image1 is separated into RGB planes.

2) Secret data taken is then converted into binary form.

3) Those values are separated into upper and lower nibbles which are embedded in two separate planes of the cover image1.

4) Upper nibbles are embedded in green plane and lower nibbles in red plane.

5) Stego key is embedded inside the blue plane.

6) After which, all the three planes are combined to generate stego image1.

7) Stego image1 is then interpreted as secret data and embedded in the cover image2 using the same algorithm and thus the final stego image is generated.

**Data Extraction Process**

In data extraction process we using the final stego image, the stego image1 is extracted using stego key1 and LSB recovery algorithm. Next, from stego image1, secret data is extracted by using stego key2 and same LSB recovery algorithm. The proposed scheme is irreversible one as the cover image is not recovered at the receiver side.

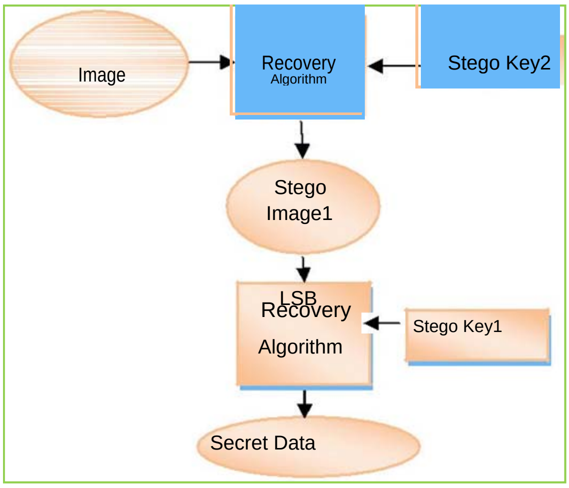

**Fig.5-Receiver end Steganography**

The algorithm works as follows:

1) Final stego image is separated into RGB planes.

2) Stego key which acts as password is entered whichis then verified with the stored key that is embedded in the blue plane of cover image2.

3) If the key is matched then the upper and lower nibbles of binary secret data is extracted from green and red planes respectively.

4) Then the upper and lower nibbles are combined to make the binary form of stego image1.

5) Finally, the original stego image1 is obtained from binary form.

6) Next, using the same algorithm the original secret data is retrieved from stego image1.

## V. EXPECTED OUTCOME

Data hiding system is said to be secured if we have knowledge of hiding data by using algorithm which does not help the eavesdropper to detect hidden data or know the secret data. Stego keys play an important role in improving the security of data hiding technique. As in the proposed work, two different stego keys are used, the system is said to be double protected. In order to enhance the security, in proposed work instead of combining cryptography with steganography, only steganography is used twice. The reason behind this is that National Security Agency (NSA) has developed a quantum computer that could crack most types of encryption algorithms. So if the steganography is partly defeated then secret data becomes visible which can be cracked using quantum computer. Therefore if steganography is used two times, then even if at first level steganography gets defeated then the second level will keep the secret data secured.

## VI. CONCLUSION

Data security has turned into a standout amongst the most huge issues because of the exponential development of web clients. Unapproved access to mystery information can have genuine repercussions like monetary misfortune and so on. Steganography is one of the arrangements whose objective is to conceal the presence of imparted message. In this paper, exceedingly secured information concealing strategy has been exhibited where steganography is utilized inside steganography. The proposed strategy implants information in two spread pictures utilizing Six bit LSB method. The mystery information is covered up in double structure in two spread pictures because of which twofold insurance has been given to classified information which can be any content, sound, feature or picture. The trial results demonstrate that the proposed plan can be a decent option for secure correspondence where two level of security is acquired in conjunction with high payload limit and great subtlety.[13]

## VII. FUTURE WORK

Some problems and concepts that remain unaddressed can be performed in the future. Such as with the help of pre-emptive approach more information can be added for exact, timely analysis with high accuracy. It can also be used for quantitative & qualitative analysis, rank ordering, etc. We also embed the source code of our proposed scheme in Java. In our proposed scheme so as to use the benefits of an approach like open source.

## ACKNOWLEDGMENT

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 SVITS administration for their support & motivation during this research. They also like to give thanks to Dr. Anand Rajavat and Asst.Prof.Priyanka Vijaywargiya for discussion regarding the situational awareness system & for producing the approach adapted for this paper.

## REFERENCES

[1]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

[2] Clair, Bryan, *"Steganography: How to Send a Secret Message",8-*Nov.-2001 www.strangehorizons.com/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]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.

[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.