# MULTIPLE STENOGRAPHY METHOD FOR PROTECTED INFORMATION TRANSFER

Harsh Saki
harshsaki.atc@acropolis.in

Sumit Jain
sumit.cse2005@gmail.com

Deepak Patidar
deepak.patidar.atc@acropolis.in

Department of Computer Science & Engineering,
Acropolis Technical Campus, Indore.

***Abstract* - With the spread of computerized information around the globe through the web, the security of the information has raised a concern to the individuals. Numerous techniques are heading up to shield the information from going under the control of the unapproved individual. Steganography and cryptography are two separate systems for information security. The fundamental reason in cryptography is to make message idea muddled, while steganography expects to stow away mystery message. Computerized pictures are amazing bearers of shrouded data. We propose a technique for joining steganography and cryptography for mystery information correspondence. In this paper, we propose a superior JPEG steganography alongside a substitution encryption system. The methodology utilizes the procedure which utilized as a part of the recurrence space for stowing away scrambled information inside picture. Test results demonstrate that the visual and the measurable estimations of the picture with scrambled information before the insertion are like the qualities after the insertion consequently lessens the shot of the secret message being identified and empowers mystery correspondence. The viability of the proposed technique has been evaluated by figuring Mean square lapse (MSE) and Peak Signal to Noise Proportion (PSNR).[1]**

***Index Terms***— Mean square lapse (MSL) , Peak Signal to Noise Proportion (PSNR), Steganography,Cryptography, image hiding

## I. INTRODUCTION

The In the computerized world, information is the heart of PC correspondence and worldwide economy. To guarantee the security of the information, the idea of information covering up has pulled in individuals to concoct innovative answers for shield information from falling into wrong hands. Advanced information can be conveyed over PC systems starting with one spot then onto the next with no blunders and obstruction. The dispersion of advanced media raised a worry throughout the years as the information are assaulted and controlled by unapproved individual [2]. Computerized information can be duplicated with no misfortune in quality what's more, substance. In this manner it represents an enormous issue for the security of information and insurance of savvy property privileges of copyright proprietors. The Internet gives a system for correspondence as a intends to disperse data to the masses. As an aftereffect of spreading of Internet around the world, inspiration of concealing mystery message in diverse sight and sound and secure correspondence through Web is expanded. Strategies for data covering up are expanding step by step with additional advanced methodology. The computerized media which are utilized for mystery correspondence incorporates content, pictures, sound and features which give fantastic transporters to concealed data. Because of the development of information correspondence over PC system, the security of data has turned into a real concern. Accordingly to shield information from unapproved get to and utilize, the information privacy furthermore, honesty are needed.[3]

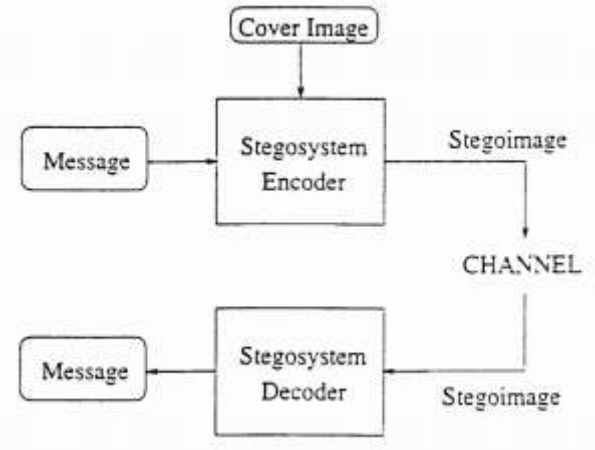


**Figure 1.Steganographic flow**

Steganography and cryptography are the two diverse data concealing strategies which give privacy and honesty of information. Steganography system expects to transmit a message on a channel, where some other sort of data is now being transmitted. The objective of steganography is to conceal messages inside other "safe" computerized media in a manner that does not permit any individual to try and recognize the vicinity of mystery message. The fundamental objective of steganography is to impart safely so as to abstain from attracting suspicion to the transmission of a concealed information [4]. Cryptography conceals the substance of a mystery message from an unapproved individual however the substance of the message is unmistakable. In cryptography, the structure of a message is mixed so as to make it good for nothing and ambiguous way. Fundamentally, cryptography offers the capacity of transmitting data between persons as it were that keeps an outsider from understanding it [5].

Steganography does not modify the structure of the mystery message, however shrouds it inside a medium so that the change is not noticeable. As such, steganography keeps a unintended beneficiary from suspecting that the information exists and the security of the steganography framework depends on mystery of the information encoding framework . When the encoding framework is known, the steganography framework is vanquished. While cryptography shields messages from unapproved individual by changing the

 

importance, steganography strategies empower covering of the way that a message is being sent through computerized media. Steganography is the imperceptible correspondence between the sender and the collector. In Steganography, just the sender and the beneficiary know the presence of the message, while in cryptography the presence of the scrambled message is noticeable to the world. Consequently, steganography uproots the undesirable consideration going to the media in which the message is concealed.[6]

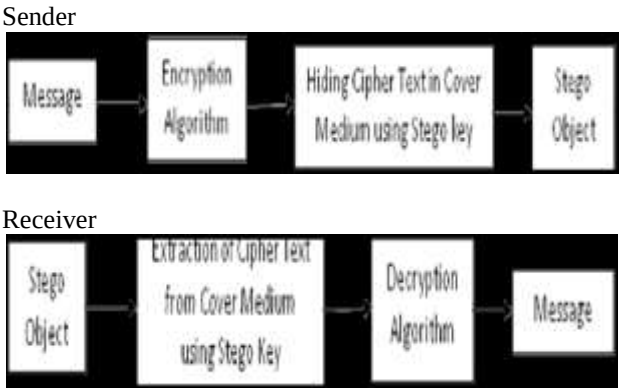


**Figure 2: Secure Communication**

Steganography and Cryptography are distinctive in their method for information concealing however they are truth be told corresponding methods. Regardless of how solid the encryption calculation may be, if mystery message is found, it will be liable to cryptanalysis. In like manner, how well a message is covered inside an advanced media there is probability of the concealed message to be found by the outsider. By consolidating Steganography and Cryptography we can accomplish better security by covering the presence of a scrambled message. The subsequent stego-article can be transmitted without uncovering that mystery data is being traded. Moreover, regardless of the possibility that an aggressor were to distinguish the message from the stego-object, he at first need to unravel the message from advanced media and after that he would even now require the cryptographic calculation to decode the scrambled message [7].

## II. Related Study

Iris Biometric Cryptography For Identity Document", this paper exhibit a way to deal with create an extraordinary and more secure cryptographic key from iris format. The iris pictures are prepared to deliver iris format or code to be used for the encryption and decoding errands. AES cryptography calculation is utilized to scramble and decode the character information.

[8]. Furthermore „Two New Approaches For Secured Image Steganography Using Cryptographic Techniques And Type Conversions" This paper give data about Cryptography & Steganography, This paper presents two new techniques wherein cryptography and Steganography are joined to scramble the information and also to conceal the scrambled information in another medium so the way that a message being sent is concealed

.[9] Next paper is "A New Image Steganography Technique" it incorporates different picture Steganography procedures like Text-Based Steganography, Audio Steganography, Steganography in OSI Network Model, Image Steganography and so forth

[10] "Outlining Of Robust Image Steganography Technique Based On LSB Insertion And Encryption" This paper examines the outline of a vigorous picture Steganography procedure in light of LSB (Least Significant Bit) insertion and RSA encryption strategy. Steganography is the term used to depict the stowing away of information in pictures to evade identification by aggressors.

[11] "Multilevel Network Security Based on Iris Biometric", In this paper A novel security Mechanism is produced here for high security arranges by consolidating IRIS biometric procedures with cryptographic and Steganography mechanisms.

[12] Hiding data in pictures is a primitive strategy and with the progression computerized innovation clear way to many types of steganographic techniques [

## III. Problem Domain

The A few works have been introduced towards both steganography, cryptography and consolidating the methods for better information security. Despite the fact that the exploration of Steganography at first was completed as an issue of concealing information behind spread pictures, as the innovation has advanced more perplexing structures of steganography has advanced.

A portion of the generally examined and advanced variations of

Steganography are:

1) Hiding Image behind Video
2) Hiding Data behind Video
3) Hiding information behind Audio
4) Hiding Audio behind Video

One of the intelligible necessities of steganography is that the extent of the spread must be higher than that of payload. The higher the size degree, the better covering up achieved.However with proceeds with development of pictures, picture screening for concealing information has likewise been heightened. Thusly the need of Hybrid steganography is expanded. It is a manifestation of steganography where information is first covered up behind one specific kind of payload and the resultant stego article is further taken cover behind another payload prompting more mind boggling installing which is hard to track. This work manages crossover steganography where instant message is taken cover behind Image and the outcome is taken cover behind sound record. The system stress on accomplishing high PSNR for high BPP such that such a model don't require an

excess of additional bits for stegano process.Likewise a content information contains just characters and there is continuously a high resilience for the content information. Regardless of the fact that a few bits are ruined, the content can be translated well. However in instance of utilization exes, even a solitary ruined bit may cause a wrong tying with underneath system which causes the application to crash upon execution. Exe information is for the most part twofold information. An exe document is produced by incorporating a source code with compiler and linker.[13]

## IV. PROPOSED SOLUTION

This Steganography can be utilized at whatever time you need to conceal information. There are numerous motivations to conceal information however they all come down to the craving to keep unapproved persons from getting to be mindful of the presence of a message. With these new methods, a concealed message is indistinct from background noise. Regardless of the fact that the message is suspected, there is no confirmation of its presence.
This procedure is in view of two segments

1) Data covering up
2) Data preparing

The square chart for the proposed information concealing procedure is indicated in Fig.1. Here two spread pictures are utilized i.e. spread image1 and spread image2. For giving more security two stego keys are utilized which are not the same as one another. The stego key utilized is of 10 bit as a part of length. The key can be made of numbers, characters, and images yet ought to be of 10 bit length. These keys are covered up in the spread picture amid the concealing methodology. This ought to be known at the beneficiary side amid the interpreting methodology for recovering the mystery file.As demonstrated in Fig.; the mystery information has been implanted inside the spread image1 with the assistance of 4 bit LSB inserting calculation alongside the stego key1 mostly utilized for security reason from which stego image1 is created. 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 created.

The algorithm works as follows:

1) Cover image1 is divided into RGB planes.

2) Secret information taken is then changed over into double structure.

3) Those qualities are divided 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 joined to produce stego image1.

7) Stego image1 is then translated as mystery information and installed in the spread image2 utilizing the same calculation and consequently the last stego picture is created.

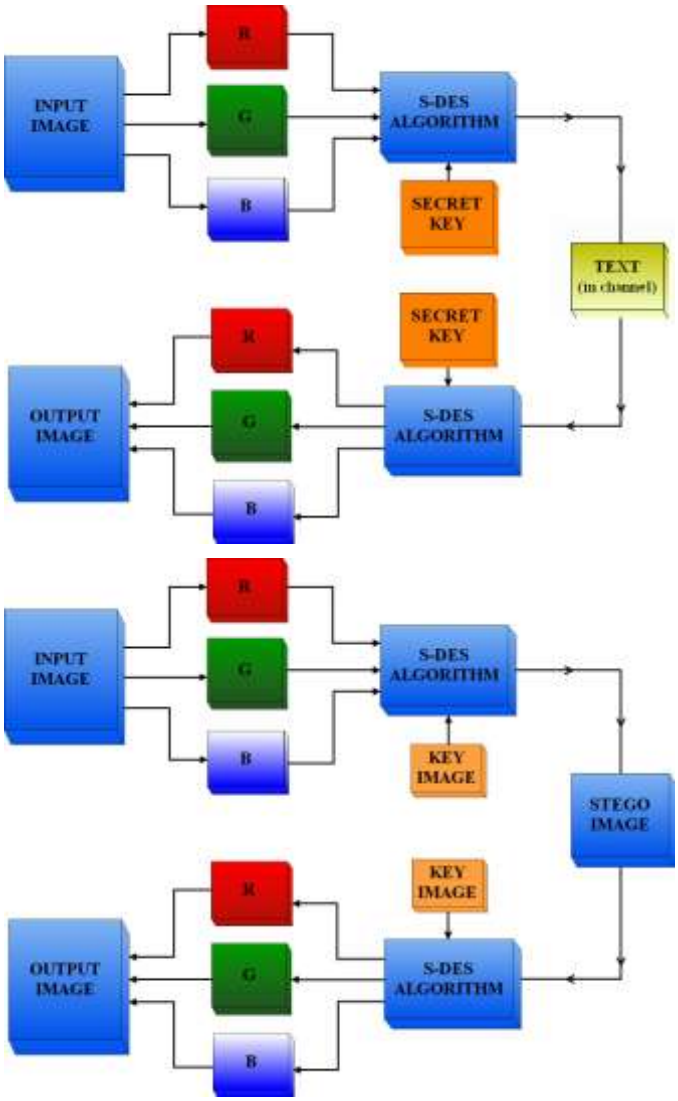


**Figure-3: Flow of proposed idea**

**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 extricated by utilizing stego key2 and

same LSB recuperation calculation. The proposed plan is irreversible one as the spread picture is not recuperated at the collector side.

The calculation fills in as takes after:

1) Final stego picture is differentiated into RGB planes.
2) Stego key which goes about as secret key is entered whichis then confirmed with the put away key that is inserted in the blue plane of spread image2.
3) If the key is coordinated then the upper and lower snack of paired mystery information is extricated from green and red planes individually.
4) Then the upper and lower snack are consolidated to make the paired type of stego image1.
5) Finally, the first stego image1 is gotten from paired structure.
6) Next, utilizing the same calculation the first mystery information is recovered from stego image1.

## V. CONCLUSION

Information security has transformed into a champion amongst the most gigantic issues in light of the exponential improvement of web customers. Unapproved access to puzzle data can have bona fide repercussions like money related setback etc. Steganography is one of the game plans whose goal is to hide the vicinity of conferred message. In this paper, exceedingly secured data covering methodology has been displayed where steganography is used inside steganography. The proposed methodology inserts data in two spread pictures using Six bit LSB technique. The puzzle data is concealed in twofold structure in two spread pictures on account of which twofold protection has been given to characterized data which can be any substance, sound, highlight or picture. The trial results show that the proposed arrangement can be an OK alternative for secure correspondence where two level of security is procured in conjunction with high payload farthest point and extraordinary subtlety.[14]

## VI. FUTURE WORK

A few issues and ideas that stay unaddressed can be performed later on. For example, with the assistance of preemptive approach more data can be included for precise, opportune examination with high precision. It can likewise be utilized for quantitative & subjective examination, rank requesting, and so forth. We additionally install 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.

## REFERENCES

[1] M. Hossain, S.A. Haque, F. Sharmin, "Variable Rate Steganography in Gray Scale Digital Images Using Neighborhood Pixel Iriformation", 12th International Conference on Computer and Information Technology (ICCIT 2009) 21-23 December 2009.

[2] Abbas Cheddad, Joan Condell, Kevin Curran, Paul McKevitt, "Digital image steganography: Survey and analysis of current methods", Elsevier, Signal Processing, Vol. 90, pp. 727-752, 18 August 2009.

[3] Shailender Gupta, Ankur Goyal, Bharat Bhushan, "Information Hiding Using Least Significant Bit Steganography and Cryptography", International Journal Modern Education and Computer Science, Vol. 6, pp. 27-34, June 2012.

[4] Md. Rashedul Islam, Ayasha Siddiqa, Md. Palash Uddin, Ashis Kumar Mandal, Md. Delowar Hossain, "An Efficient Filtering Based Approach Improving LSB Image Steganography using Status Bit along with AES Cryptography", 3rd International Conference on Informatics, Electronics & Vision 2014.

[5] K. Sakthisudhan, P. Prabhu, "Dual Steganography Approach for Secure Data Communication", International Conference on Modeling, Optimization and Computing, Elsevier, Procedia Engineering, Vol. 38, pp. 412-417, 2012.

[6] Ali Al-Ataby, Fawzi Al-Naima, "A Modified High Capacity Image Steganography Technique Based on Wavelet Transform", The International Arab Journal of Information Technology, Vol.7, October 2010

[7] R.Amirtharaja, R.Akila, "A Comparative Analysis of Image Steganography", International Journal of Computer Applications, Vol.2, pp. 41- 47, May 2010.

[8] V. Nagaraj, Dr. V. Vijayalakshmi, Dr. G. Zayaraz, "Modulo based Image Steganography Technique against Statistical and Histogram Analysis", IJCA Special Issue on "Network Security and Cryptography" NSC, Vol. 4, pp. 34-39, 2011.

[9] Vikas Tyagi, Atul kumar, Roshan Patel, Sachin Tyagi, Saurabh Singh Gangwar, "Image Steganography Using Least Significant Bit With Cryptography", Journal of Global Research in Computer Science, Vol. 3, pp. 53-55, March 2012.

[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.

[14]Cachin C., "An Information-Theoretic Model for Steganography", Proceedings of 2ndWorkshop on Information Hiding, MIT Laboratory for Computer Science, pp. 306-318, 1998.

 