International Journal of Trend in Scientific Research and Development (IJTSRD)
Volume: 3 | Issue: 4 | May-Jun 2019 Available Online: www.ijtsrd.com e-ISSN: 2456 - 6470

A Review on Stegnography Data Hiding using Color Images

Gagandeep Singla[1], Chamkour Singh[2]

[1]M. Tech Scholar, [2]Assistant Professor
[1,2]Guru Kashi University, Talwandi Sabo, Punjab, India

How to cite this paper: Gagandeep Singla | Chamkour Singh "A Review on Stegnography Data Hiding using Color Images" Published in International Journal of Trend in Scientific Research and Development (ijtsrd), ISSN: 2456-6470, Volume-3 | Issue-4, June 2019, pp.889-893, URL: https://www.ijtsrd.com/papers/ijtsrd23556.pdf

IJTSRD23556

Copyright © 2019 by author(s) and International Journal of Trend in Scientific Research and Development Journal. This is an Open Access article distributed under the terms of the Creative Commons Attribution License (CC BY 4.0) (http://creativecommons.org/licenses/by/4.0)

ABSTRACT

Nowadays, network has necessary roles for transferring knowledge accurately and quick from supply to a destination. The info isn't secure enough to transfer extremely confidential. The protection of data has become one in every of the principle challenges of resource sharing with electronic communication over network. Cryptography and Steganography square measure to strategies for shielding knowledge from intruders whereas transferring over an open channel network. Cryptography could be a technique to cipher knowledge and steganography is that the art and science of concealing secret message in an exceedingly cowl image. The digitally shared knowledge between the users ought to be born-again to some unclear format which cannot be tampered by the intruders. To fulfill these necessities the technique Steganography will be used. During this technique we tend to use completely different mediums to cover the info that square measure text, images, audio, video etc. this paper is that specialize in encrypting of knowledge by exploitation image steganography.

Keywords: *Stego, Stegnography, image, hiding, color etc*

I. INTRODUCTION

Advanced steganography is the craftsmanship and exploration of concealing correspondences; a steganographic framework along these lines implants mystery information in broad daylight cover media so as not to excite a meddler's doubt. A steganographic framework has two primary perspectives: steganographic limit and intangibility. In any case, these two qualities are inconsistent with each other.

Besides, it is very hard to expand the steganographic limit and at the same time keep up the impalpability of a steganographic framework. Furthermore, there are still extremely constrained techniques for steganography to be utilized with correspondence conventions, which speak to offbeat yet encouraging steganography mediums. Advanced picture steganography, as a strategy for mystery correspondence, intends to pass on a lot of mystery information, generally to the extent of cover picture, between conveying parties. Moreover, it plans to keep away from the doubt of non-conveying gatherings to this sort of correspondence [5]. Consequently, this examination addresses and proposes a few strategies to enhance these key parts of advanced picture steganography. Consequently, a few attributes and properties of computerized pictures have been utilized to expand the steganographic limit and improve the stego picture quality (imperceptibility).This section gives a general prologue to the exploration by first clarifying the examination foundation. At that point, the primary inspirations of this examination and the exploration issue are characterized and talked about. Next, the exploration point is recognized in light of the built up meaning of the examination issue and inspirations.

II. INFORMATION SECURITY AND STEGANOGRAPHY

Basically, PC and system security have a few necessities that ought to be tended to so as to get secure frameworks. Consequently, with a specific end goal to decide the execution of a security innovation, three key ideas ought to be broke down: classification, uprightness, and accessibility. Distinguishes these ideas as takes after:

1. "Classification manages securing, distinguishing, and stopping the unapproved exposure of data". The primary objective of cryptography is to jumble a plaintext message such that exclusive the proposed beneficiary can read it. This is unequivocally the objective of privacy.
2. "Respectability manages averting, recognizing, and dissuading the unapproved change of data". An uprightness assault is conceivably more hazardous than a secrecy assault. Cryptography tends to honesty by playing out a computerized signature check crosswise over data.
3. "Accessibility identifies with counteracting, distinguishing, or preventing the refusal of access to basic data". Cryptography can counteract secrecy and uprightness assaults, yet it cannot avert accessibility assaults. Cryptography, similar to some other system security innovation, isn't a silver shot. Subsequently, it must be joined with different strategies to accomplish vigorous security arrangement.

Notwithstanding the three key ideas of security, two other security objectives are basic with respect to cryptography: confirmation and non-revocation [10].

1. Confirmation: "In many exchanges you should have the capacity to authenticator approve that the general population you're managing are who they say they are".

2. "Non-revocation manages the capacity to demonstrate in an official courtroom that somebody sent something or marked something carefully". Without non revocation, computerized marks and contracts would be futile. Steganography, as a mystery specialized strategy, accomplishes the greater part of these prerequisites since there is no technique that can address all security ideas . Along these lines, the key ideas of security that applies for steganography and similarly think about the fundamental standards of data security prerequisites (talked about above) are as per the following:

1. Classification: Cryptography accomplishes the privacy by averting unapproved people, who can see the data, from accessing this data. With steganography, unapproved individuals don't know there is mystery information there.
2. Survivability implies that all information preparing happens amongst sender and recipient does not annihilate the shrouded data. Moreover, this got data must be extractable and meaningful.
3. No Detection: Steganography fizzles in the event that somebody can without much of a stretch distinguish where you conceal your data and discover your message. In this way, regardless of whether somebody knows how the steganography strategy installs the mystery data, he or she can't without much of a stretch discover that you have implanted information in a given record [10].
4. Perceivability: The stego record must be imperceptible and there must be no noticeable changes to the stego document. The primary objective of steganography is precisely the classification of inserted information. Not at all like cryptography which shrouds the substance or importance of the mystery information, steganography conceals the very presence of this information. In this manner, unapproved individuals don't know there is mystery information there. From a secrecy point of view, steganography gives a more elevated amount of data insurance than cryptography.

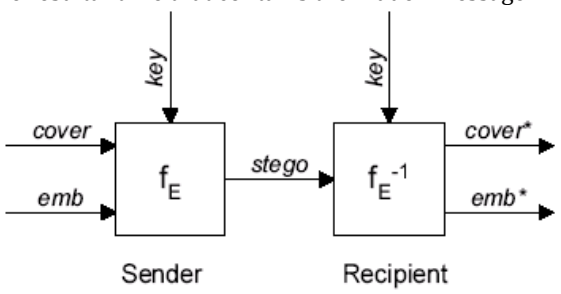
To some degree, the survivability of information speaks to the honesty of this information since them two (survivability and trustworthiness) are intending to keep the control of the transmitted information. In our examination and proposed strategies, similar to the greater part of other steganography methods, think about the uninvolved superintendent situation.

The inactive superintendent is confined from altering the substance of stego documents amid the correspondence procedure and he/she has the privilege to anticipate or allow the message conveyance [11]. Along these lines, if the stego document is gotten, at that point it will be precisely the record which is sent with no adjustment or changes included amid the transmission procedure. Most steganography inquire about is worried about such sort of situations which expect that the uprightness of mystery information is protected between the sender and the recipient. In this manner, keeping up the honesty of mystery message implies that the implanted message by the sender is the very same message separated by the collector (in place mystery message). Notwithstanding, the trustworthiness of the stego picture implies that the stego picture sent by the sender is precisely the same stego picture got by the recipient (indistinguishable and have comparable measurable properties).

The objective of steganography is mystery correspondence. In this manner, steganography plans to keep others from feeling that such correspondence is occurring. Basically, steganographic frameworks ought to distinguish the repetitive (insignificant)bits of cover documents or medium. Consequently, any adjustments to these excess bits ought not demolish the honesty of these mediums. Therefore, saving the uprightness of cover records upgrades the undetected capacity of steganography [5]. More often than not, concealing mystery information utilizing steganography adds as light change to the stego document properties. This makes the recognition of steganography nearness troublesome or relatively unthinkable. Furthermore, regardless of whether the concealing strategy utilized is publically known, no one ought to have the capacity to demonstrate the presence of shrouded information. Be that as it may, imperceptibility could be fundamentally accomplished by adding no noticeable changes to the cover document. After the information concealing procedure, individuals need to see no unmistakable follows in the stego document. Consequently, in the event that somebody can tell or demonstrate that a given document (i.e. stego document) has been adjusted somehow then the steganography is unsuccessful. For picture based steganography, the devotion (i.e. PSNR) of the stego picture is normally used to quantify and assess the imperceptibility of steganography strategy utilized. Be that as it may, Fidelity alludes to our capacity to distinguish contrasts between cover picture and stego picture. Hence, on the off chance that we can't recognize any contrast between these two pictures then this steganography strategy is impalpable. In any case, the honesty of the cover picture isn't saved with steganography since a few sections of the cover document ought to be changed or adjusted so as to shroud the mystery message and get the stego record [13].

Working

Modern day steganography mainly deals with hiding information within other files such as music or picture files. These files can "contain perceptually irrelevant or redundant information that can be substituted for hidden messages". Cover is the original picture, audio or video file. Emb is the embedded secret message. Key is the parameter which controls the hiding process of the secret message and stego is the resultant file that contains the hidden message.



III. LITERATURE REVIEW

Pascal Maniriho et.al.[2017] have contemplated Disguising the nearness of correspondence has turned into an extreme worry in this very digitalized world because of the unapproved information access and system arrangement infringement that are rising quickly. These issues have prompted the utilization of cryptography method as a mean for securing information by encoding them. Be that as it may, since the encoded information can be seen by advanced interlopers amid the transmission, this may prompt its doubt which can brings about unapproved get to. Accordingly,

steganography is another system for securing correspondence. Steganography is the act of disguising private data in the codes that make up advanced documents. Not quite the same as encryption, notwithstanding, steganography gives security by camouflaging the nearness of correspondence. In this unique circumstance, this paper shows an enhanced data stowing away executed in view of distinction extension and modulus work. The past strategy has just considered the picture smooth territories where the distinction esteem is 0 or 1 while overlooking different esteems for concealing information. These restrictions may bring about diminishing the installing limit with regards to all pictures having few smooth zones. Thus, another plan that considers both positive and negative distinction esteems to cover mystery information is created. The trial comes about demonstrate that the proposed plot accomplishes preferred outcomes over the current methods. [1]

G.Prashanti et.al.[2017] have examined the sender encodes the mystery message utilizing figure calculation which utilizes a mystery key that ought to be known to both the sender and collector. To give double security the encoded message got from various encryption strategies is covered up in a picture in light of LSB stegnography. From get side the scrambled message is extricated from the picture and is then decoded utilizing unscrambled strategies to get the first mystery message. Matlab is utilized as a test system to execute the strategies of encryption and steganography. Matlab give profoundly registering condition and progressed in fabricated capacity for picture processing. [2]

M. Goljan et.al. [2017] proposed by cryptography, which expects to make correspondence incoherent to the individuals who don't have the privilege keys. Once an outsider can dependably distinguish which pictures contain mystery messages, the stenographic instrument winds up pointless. Another critical factor is the decision of the cover picture. The determination is at the carefulness of the individual who sends the message. Pictures with a low number of hues, PC workmanship, and pictures with novel semantic substance ought to be stayed away from as cover images. [3]

Zhe Wang et.al.[2017] , proposed to distinguish the Least - Significant-Bit (LSB) steganography in the computerized flags, for example, pictures and sound that the length of shrouded information can settle flag tests can be assessed with high accuracy. The new Steganalysis approach depends on some factual measures of test matches that are exceedingly delicate to LSB installing tasks. To assess the heartiness of the proposed Steganalysis approach, limits on estimation blunders are created. The Histogram Characteristic Function (HCF), for the discovery of steganography in shading pictures yet inadequate on dim scale pictures [4].

Anupam Mondal et.al.[2017], proposed the two bits of message is inserted in a pixel in a way that not just the Least Significant Bit (LSB) of picture component is permitted to change yet in addition the second piece plane and fourth piece plane are permitted to be controlled, yet the fact of the matter is in each installing procedure just a single variation in one piece plane is permitted to happen. It is looked at by the strategy LSB-Matching, the outcomes demonstrates this technique has a satisfactory limit of installing information and scarcely is noticeable for Steganalysis algorithm [5].

Q. Huang et.al. [2017] proposed the issue in LSB Matching Revisited (LSBMR) calculation to make areas choice on pictures to discover reasonable region. By depending on every pixel we can choose on the off chance that it ought to be secured. It can enhance the visual subtlety and perceptibility of the LSB coordinating strategy. By altering the parameters of neighbor pixels, the maximum installing limit can be expanded as needed [6].

Chaun Qin et.al.[2017] proposed Steganography is the specialty of composing shrouded messages such that nobody; aside from the sender and planned beneficiary even comprehend there is a concealed message. Adjusting the LSB will just purpose minor changes in shading. While this procedure functions admirably for 24-bit shading picture documents, steganography has not been as effective when utilizing a 8-bit shading picture record, because of restrictions in shading varieties and the utilization of a shading table. Shading table is composed as-the initial three bytes compare to RGB segments and the last byte is held or unused [7].

Adnan Gutub et.al. [2017] Image based steganography utilizes the pictures as the cover media. LSB is an ordinarily utilized method in this documented. A few situations of using minimum critical bits inside pictures are accessible. We converge between the thoughts from the arbitrary pixel control techniques and the stegokey ones to propose our work, which utilizes the minimum two noteworthy bits of one of the channels to show presence of information in the other two channels. This work demonstrated alluring outcomes particularly in the limit of the information bits to be covered up with connection to the RGB picture Pixels [8].

Gunjan Nehru et. al. [2017] Steganography is the craftsmanship and study of transmitting shrouded messages. In current correspondences frameworks, this implies concealing data in correspondence media, for example, sound, content, and pictures. In a perfect world, with the exception of the sender and recipient, no outsider ought to try and suspect the presence of such messages. Computerized interchanges frameworks require the utilization of blunder adjusting codes (ECC) to battle clamor, or mistakes, presented by the comparing (Correspondence) channel. Fundamentally, an ECC adds repetition to a message with the goal that the mistakes Presented by the channel can be revised [9].

Mahendra Kumar et.al. [2010] Steganography is the craft of mystery correspondence between two gatherings that conceals the substance of a message, as well as does not uncover the presence of the message. Steganalysis endeavors to recognize the presence of implanted information in a steganographically adjusted cover record. Numerous calculations have been proposed, however so far every ha some shortcoming that has enabled its belongings to be recognized, as a rule through Statistical examination of the image[12]. we propose a novel way to deal with JPEG steganography that gives high implanting limit zero-freak histogram rebuilding. Our calculation, named J3, utilizes stop focuses in its header structure that enable it to reestablish the histogram of JPEG coefficients, making it unthinkable for any first request steganalysis to identify it, notwithstanding expanding its payload contrasted with different calculations. J3 can be utilized to install a lot of information with protection from visual and first request factual assaults. To the extent we know, there is no current calculation that can

furnish as high an inserting payload with finish histogram restoration [10].

Shashikala Channalli, Ajay Jadhav [2009] in this day and age the craft of sending and showing the shrouded data particularly out in the open spots, has gotten more consideration and confronted numerous difficulties. In this way, unique techniques have been proposed so far for concealing data in various cover media. In this paper a strategy for covering up of data on the announcement show is introduced. It is outstanding that encryption gives secure channels to conveying elements. Be that as it may, because of absence of clandestineness on these channels, a meddler can recognize scrambled streams through factual tests and catch them for advance cryptanalysis. In this paper we propose another type of steganography, on-line covering up of data on the yield screens of the instrument. This technique can be utilized for declaring a mystery message in broad daylight put. It can be stretched out to different means, for example, electronic promoting board around sports stadium, railroad station or air terminal. This strategy for steganography is fundamentally the same as picture steganography and video steganography. Private checking framework utilizing symmetric key steganography procedure and LSB system is utilized here for concealing the mystery information. [11]

IV. PROBLEM FORMULATION

From the above literature survey there are different problems that are given below:

- There is Security problem during the transmission of data from sender to the receiver.
- One of the major difficulties encountered in image processing is the huge amount of data used to store an image. Thus, there is pressing need to limit the resulting data volume. Image compression techniques aim to remove the redundancy present in data in a way that makes image reconstruction possible. It is necessary to find the statistical properties of the image to design an appropriate compression transformation of the image; the more correlated the image data are, the more data items can be removed.
- A wavelet transform combines both low pass and high pass filtering in Spectral decomposition of signals. One-Stage Filtering: Approximations and Details For many signals, the low-frequency content is the most important part.
- Lossless compression is preferred for archival purposes and often for medical imaging, technical drawings, maps and logos, where the loss of information is not acceptable. This scheme provides low compression ratio.
- There is bit loss problem during the stego image and data hiding in stego image.

V. RESEARCH METHODOLOGY

It is based upon GUI (graphical user interface) in MATLAB. It is an effort to further grasp the fundamentals of MATLAB and validate it as a powerful application tool. There are basically different files. Each of them consists of m-file and figure file. These are the programmable files containing the information about the images and the DWT technique and Neural Network technique to compress the image. In this work we will firstly upload the image in any extension in the given window**.** Then their will be a button where the DWT and neural network is implemented on the images and gives the results of the compressed images and PSNR and MSE values and Correlation values etc . In modern steganography images are represented in computers as an array of numbers that represent light intensities at various points (or pixels). If a color image is used, then there is such an array for each of the three primary colors, red, green and blue (RGB). Colored image is obtained by superposing these three arrays; each pixel is the sum of these three colors. Since computer files, images, etc. do not use all of the bits inside the file to store the data, an idea of data hiding comes about. One could replace the least significant bit of the original image with the secret bits and the image will not be distorted.

In modern digital steganography, data is first encrypted by the usual means and then inserted, using a special algorithm, into redundant (that is, provided but unneeded) data that is part of a particular file format such as a JPEG image. Think of all the bits that represent the same color pixels repeated in a row. By applying the encrypted data to this redundant data in some random or non conspicuous way, the result will be data that appears to have the "noise" patterns of regular, no encrypted data. A trademark or other identifying symbol is hidden.

Steps used are:

Begin

1. Plain text
2. Encrypting text
3. upload the RGB image
4. Stegos image
5. Extraction of information
6. Preprocessing
7. Secret message generation
8. Decryption
9. Original image
10. End

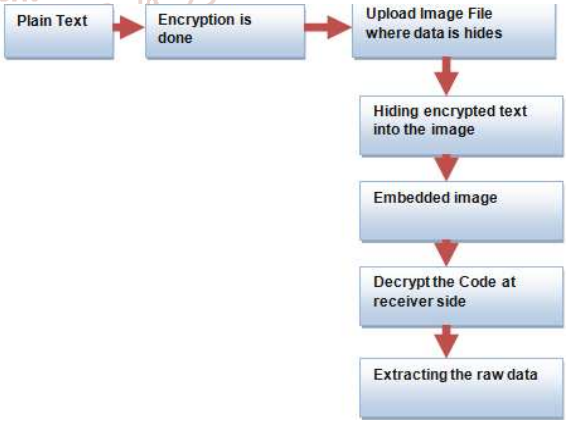


Figure 1: Block diagram of the proposed system

In recent years, a controversy has arisen over so-called strong encryption. This refers to ciphers that are essentially unbreakable without the decryption keys. While most companies and their customers view it as a means of keeping secrets and minimizing fraud, some governments view strong encryption as a potential vehicle by which terrorists might evade authorities. These governments, including that of the United States, want to set up a key-escrow arrangement. This means everyone who uses a cipher would be required to provide the government with a copy of the key. Decryption keys would be stored in a supposedly secure place, used only by authorities, and used only if backed up by a court order. Opponents of this scheme argue that criminals could hack into the key-escrow database and illegally obtain,

steal, or alter the keys. Supporters claim that while this is a possibility, implementing the key escrow scheme would be better than doing nothing to prevent criminals from freely using encryption/decryption.

Sender Side

The proposed scheme uses RSA or Diffie Hellman algorithm to encrypt secret information. To provide higher security the secret information is encrypted first and encrypted ASCII value is converted in binary form. The image pixels at the same time are also converted into binary form. The image is now used as a cover to embed the encrypted information. This process is done by LSB encoder which replaces the least significant bit of pixel values with the encrypted information bits. The modified picture is now termed as Stego image. The whole process is explained in Fig. 1.

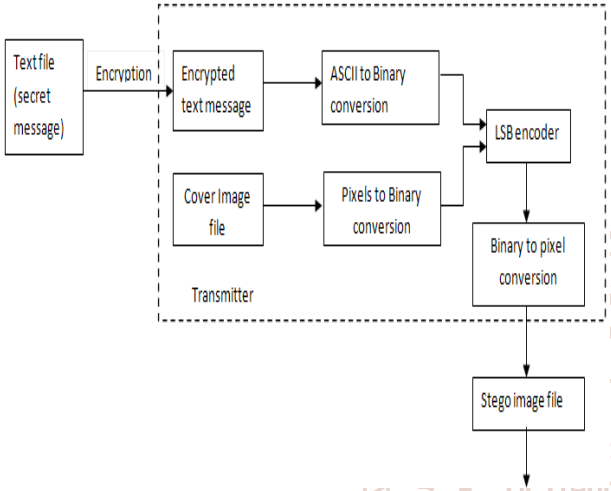


Figure 2: Proposed steganography mechanism for sender

Receiver Side

Upon reception of Stego image the receiver firstly converts the pixels into their corresponding binary values. The LSB decoder then detaches the encrypted data from image pixel values. The encrypted data is decrypted using decryption algorithms. This is how, the plain text is recovered from image. Fig. 2 shows the whole process at the receiver side.

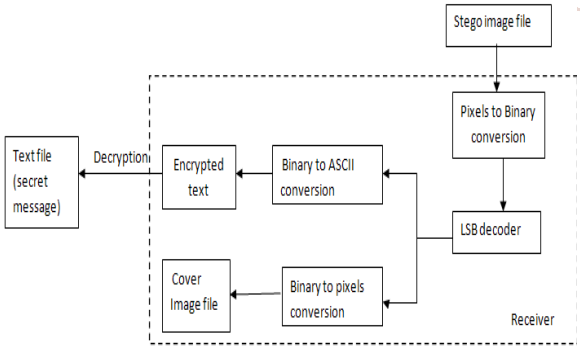


Figure 3: Proposed steganography mechanisms for receiver

VI. CONCLUSION

Because of overwhelming prerequisite of data it is important to guard the information for future references, the information and the use should be possible yet at opposite side there can be sure issues like interlopers, man-in-center assault which makes the computerized transmission to be cautious, the approach with deference the picture stegnography is helpful if the client needs the information to be covered up however in certain way making it secrecy property is taken after. The approach can be extremely valuable for the individual who can be known to the framework and works around the things which may require the privacy to be taken after, the approach is one of the choices so as the information is concealed utilizing some JPEG or BMP pictures which might be helpful secluded from everything the information effortlessly.

REFERENCES

[1] Pascal Maniriho, Tohari Ahmad "Information hiding scheme for digital images using difference expansion and modulus function" Journal of King Saud University – Computer and Information Sciences, Journal of King Saud University – Computer and Information Sciences (2018).

[2] Prashanti, G., B. V. Jyothirmai, and K. Sai Chandana. "Data confidentiality using steganography and cryptographic techniques." In Circuit, Power and Computing Technologies (ICCPCT), 2017 International Conference on, pp. 1-4. IEEE, 2017.

[3] Monies, Dorota, Sateesh Maddirevula, Wesam Kurdi, Mohammed H. Alanazy, Hisham Alkhalidi, Mohammed Al-Owain, Raashda A. Sulaiman et al. "Autozygosity reveals recessive mutations and novel mechanisms in dominant genes: implications in variant interpretation." Genetics in Medicine 19, no. 10 (2017): 1144.

[4] Kang, Kai, Hongsheng Li, Junjie Yan, Xingyu Zeng, Bin Yang, Tong Xiao, Cong Zhang et al. "T-cnn: Tubelets with convolutional neural networks for object detection from videos." IEEE Transactions on Circuits and Systems for Video Technology (2017).

[5] Bhattacharya, Indrani, Satyajit Chakrabarti, Haricharan Singh Reehal, and Vasudevan Lakshminarayanan, eds. Advances in Optical Science and Engineering: Proceedings of the Third International Conference, OPTRONIX 2016. Vol. 194. Springer, 2017.

[6] Yang, Chaowei, Qunying Huang, Zhenlong Li, Kai Liu, and Fei Hu. "Big Data and cloud computing: innovation opportunities and challenges." International Journal of Digital Earth 10, no. 1 (2017): 13-53.

[7] Li, Guo Jie, Kevin D. Hyde, Rui Lin Zhao, Sinang Hongsanan, Faten Awad Abdel-Aziz, Mohamed A. Abdel-Wahab, Pablo Alvarado et al. "Fungal diversity notes 253–366: taxonomic and phylogenetic contributions to fungal taxa." Fungal Diversity 78, no. 1 (2016): 1-237.

[8] Anusuya, R. "A Comparative Study on Pattern Based Image Steganography." International Journal of Computer Science and Engineering Communications 4, no. 2 (2016): 1307-1310.

[9] Pandey, Preeti, Vijay Verma, Gunjan Gautam, Nilima Kumari, Suman Kumar Dhar, and Samudrala Gourinath. "Targeting the β-clamp in Helicobacter pylori with FDA-approved drugs reveals micromolar inhibition by diflunisal." FEBS letters(2017).

[10] Kumar, Mahendra, and Richard Newman. "J3: High payload histogram neutral JPEG steganography." In Privacy Security and Trust (PST), 2010 Eighth Annual International Conference on, pp. 46-53. IEEE, 2010.

[11] Channalli, Shashikala, and Ajay Jadhav. "Steganography an art of hiding data." arXiv preprint arXiv: 0912.2319 (2009)