International Journal of Innovative Research in Advanced Engineering (IJIRAE) ISSN: 2349-2163
Issue 9, Volume 2 (September 2015) www.ijirae.com

AN ENHANCED APPROACH TO STEGANOGRAPHY : OBSCURITY

Tiyasa Gupta[1] , Assouma Alassane Mouhamadou Hafifou[2] ,Ramachandra Tawker[3] ,**Vaidhehi V.**[4]
[1], [2], [3] PG Scholar Department of Computer Science, Christ University, Bengaluru, India
[4]Associate Professor, Department of Computer Science, Christ University, Bengaluru, India

Abstract— Steganography is a method where a secret message is hidden inside another file. Cryptography is a method of encrypting and transmitting data in such a way so that only those for whom it is intended can read and process it. Cryptography doesn't require any carrier medium like Steganography. This paper describes about the research work where the art of steganography is implemented using f5 algorithm where the secret message is scattered all over the carrier file. An image file is used as a carrier file and any document be it in .txt, .doc etc. format and the file is hidden inside the image so that no one can guess the presence of any hidden information. As for the method of cryptography, AES algorithm is used for encryption. This paper also highlights the comparison between different algorithms in this domain.

Keywords—image steganography, key, encryption, decryption

I. INTRODUCTION

Gatecrashers/Programmers are fruitful today in light of the data they get from a framework which they can read and break down. In the wake of gaining such individual data they may uncover it to an individual or any association or may utilize this data to dispatch an assault. One of the best answers for this issue is the utilization of steganography. Steganography is the method of concealing data in computerized media. Dissimilar to cryptography it is not to keep others from knowing the data that is concealed however to keep others from imagining that the data even exists.

Steganography is a rising idea nowadays as a great many individuals join the internet insurgency consistently. Steganography is the technique for concealing data in ways that data is not really noticeable to the external world and there can be diverse sorts of Steganography to conceal the message from being seen. Because of headway in Data and Correspondence Innovation (ICT) or IT, all the data is kept electronically. In light of this security concern is a noteworthy issue nowadays. Aside from cryptography, Steganography is likewise utilized for concealing information and data.

In cryptography, the message is encoded utilizing distinctive systems. The message will at present be obvious to others yet in a scrambled structure. So if any interloper can figure the encryption procedure or the example, they can without much of a stretch split the message. Yet, in Steganography, the message will be installed in an advanced host before going it through the system, so an interloper can't even get an insight about the presence of the message. Aside from concealing the data for secrecy, it can likewise be utilized to shroud data in various types of advanced media, for example, sound, feature and images. Because of trade of a lot of information and data over the system, a large portion of them being some essential and mystery information, there is a need to network security. Information respectability and privacy is presupposed amid transmission of such information to avert unapproved get to and utilization. Because of this, there is a tremendous development in the field of information covering up.

Information stowing away is a rising examination range, which involves applications like watermarking, fingerprinting, copyright insurance for advanced media, steganography and so forth. In watermarking applications, the message is implanted with some data, for example, proprietor distinguishing proof and a computerized time stamp, which is for the most part utilized for copyright insurance.

In finger impression applications, the proprietor sets up a serial number that extraordinarily recognizes the client of the information to be transmitted. This includes copyright data with the goal that it can keep a track of any unapproved client and just permit the approved client to peruse the information.

In steganography applications, a message will be scrambled in another advanced document before transmitting it over the system. The sender will change over the information in a manner that it stays imperceptible to any individual who sees it following the example. Some components, such as multi-leveled equations, graphics, and tables are not prescribed, although the various table text styles are provided. The formatter will need to create these components, incorporating the applicable criteria that follow.

II. LITERATURE REVIEW

[1] Talks about the accessibility of generally reasonable computerized items combined with the guarantee of higher transfer speed and nature of administration (QoS) for both wired and remote correspondence systems have made it conceivable to make, repeat, transmit, and circulate advanced information with no misfortune in quality. In such a situation steganography has gotten immense consideration from the examination group round the globe, as it has been discovered helpful for data security and under spread correspondence. Steganography alludes to secretive correspondence for exchange of classified data over a correspondence channel. This paper introduces a high limit stenographic procedure in which mystery information is inserted in Middle Critical Bit planes of the spread image. The information to be implanted is separated in squares of generally diminishing lengths and every piece is inserted in the spread media under control of an exceptionally secure key. This work shows alluring results as for indistinctness and limit when contrasted and a couple reported procedures notwithstanding giving satisfactory information security.

[2] States that in today's reality the craft of sending & showing the shrouded data particularly out in the open spots, has gotten more consideration and confronted numerous difficulties. Consequently, distinctive routines have been proposed so far for concealing data in diverse spread media. In this paper a system for covering up of data on the board showcase is displayed. It is surely understood that encryption gives secure channels to imparting elements. In any case, because of absence of clandestineness on these channels, a spy can recognize scrambled streams through measurable tests and catch them for further cryptanalysis. In this paper we propose another type of steganography, on-line covering up of data on the yield screens of the instrument. This system can be utilized for declaring a mystery message openly put. It can be stretched out to different means, for example, electronic publicizing board around games stadium, railroad station or airplane terminal. This technique for steganography is fundamentally the same to image steganography and feature steganography. Private stamping framework utilizing symmetric key steganography system and LSB strategy is utilized for concealing the mystery data.

[3] Says that the exploration of securing an information by encryption is Cryptography while the system for concealing mystery messages in different messages is Steganography, so that the mystery's extremely presence is covered. The expression "Steganography" portrays the strategy for concealing subjective substance in another medium to maintain a strategic distance from recognition by the interlopers. This paper presents two new techniques wherein cryptography and steganography are joined to encode the information and additionally to shroud the scrambled information in another medium so the way that a message being sent is hidden. One of the systems demonstrates to secure the image by changing over it into figure content by S-DES calculation utilizing a mystery key and disguise this content in another image by steganography strategy. Another strategy demonstrates another method for encrypting so as to con an image in another image the image straightforwardly by S-DES calculation utilizing a key image and the information acquired is disguised in another image. The proposed strategy keeps the potential outcomes of steganalysis too.

[4] Says that Steganography is specialty of undetectable Correspondence. It endeavors to conceal the presence of imparted message in proper medium i.e. Image, Sound or Feature. So as not to excite a spy's suspicion. Different systems with Goals of heartiness, Payload and Imperceptibility are accessible and have their separate advantages and disadvantages. Different Steganography Procedures are utilized relying upon prerequisites of utilization for which they are outlined.

II. COMPARISONS WITH THE EXISTING SYSTEMS

In most of the existing systems, Least Significant bit (LSB) is used which is simple and most common insertion approach to embed information in an image and mainly focus on encryption of text rather than hiding of the text. This makes it easier for an intruder to guess the presence of a message**.** Though the existing systems are inexpensive to implement and but are used for grey scale images.

When a particular text has to be embedded in an image, and the steganography algorithm is applied on the image, the quality of the image deteriorates and sometimes it can be easily guessed that the image has hidden information. In the proposed F5 algorithm is used which uses permutative straddling for scattering the secret message over the whole carrier medium is used.

The straddling mechanism used in this system shuffles all coefficients using a permutation first. It doesn't change the number of coefficient it only changes it values. It totally depends on the key derived from a password. Here not only grey scale but also colored images can be used. As the message is scattered all over the carrier image, it doesn't affect the quality of the image. So, an intruder can guess it so easily.

III. METHODOLOGY

F5 employs permutative straddling to uniformly spread out the changes over the whole steganogram.

1. Start JPEG compression. Stop after the quantization of coefficients.
2. Initialize a cryptographically strong random number generator with the key derived from the password.
3. Instantiate a permutation (two parameters: random generator and number of coefficients).
4. Determine the parameter k from the capacity of the carrier medium, and the length of the secret message.
5. Calculate the code word length $n = 2k - 1$.
6. Embed the secret message with $(1, n, k)$ matrix encoding.

(a) Fill a buffer with *n* nonzero coefficients.
(b) Hash this buffer (generate a hash value with *k* bit-places).
(c) Add the next *k* bits of the message to the hash value (bit by bit, xor).
(d) If the sum is 0, the buffer is left unchanged. Otherwise the sum is the buffer's index 1 . . . *n*, the absolute value of its element has to be decremented.
(e) Test for shrinkage, i. e. whether we produced a zero. If so, adjust the buffer (eliminate the 0 by reading one more nonzero coefficient, i. e. repeat step 6a beginning from the same coefficient). If no shrinkage occurred, advance to new coefficients behind the actual buffer. If there is still message data continue with step 6a.

7. Continue JPEG compression (Huffman coding etc.).

REQUIREMENTS SPECIFICATION

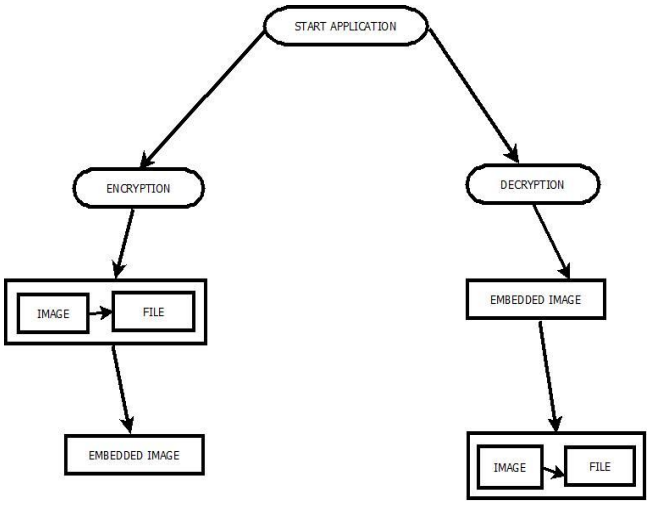
Functional specification of this application states that it include information about the various facilities, users can easily access the application from any location, the secret files/text to be sent is not shared with the outside world, users can encrypt and decrypt using a password (public key).

The non-functional specifications includes SPACE CONSTRAINT which states that in image steganography the size of encrypted file is increased during the process of encryption when any data file is encrypted with an image file for instance when an text file which has a size of 70KB and an image file which is 1.5MB and after the encryption process is completed the size of encrypted file comes up to 9-10MB, TIME CONSTRAINT, which states that the time taken when transferring the encrypted data file depends on the size of the file; if the file size is larger, then uploading the file will take more time and vice versa, SECURITY, which states that the password or the public key will be exchanged only between authorized users, REUSABILITY, which states that the same application is used by both the sender and the receiver and PERFORMANCE, which states that the application does not require much of memory space and internet is not mandatory.

TOOLS USED

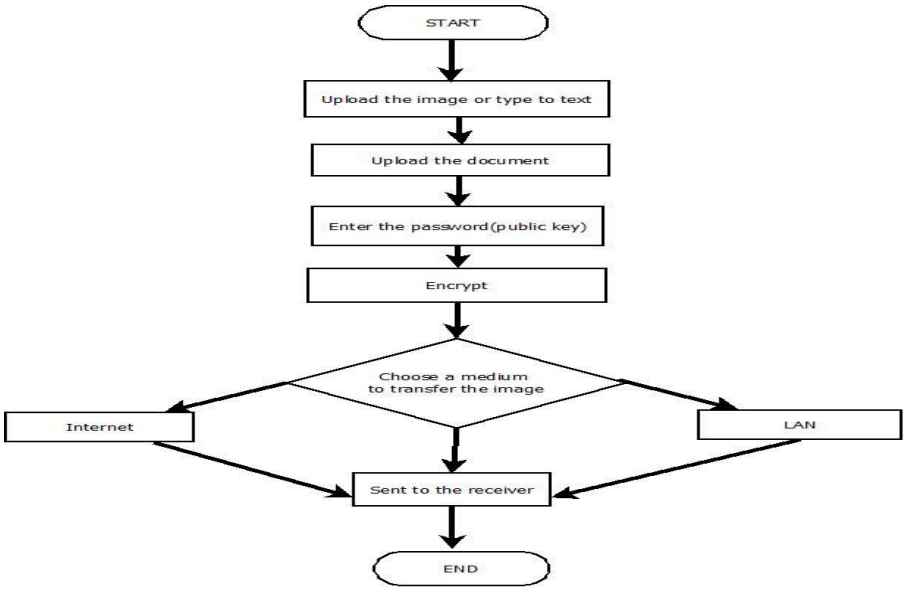
- The hardware requirements of the project includes processor-preferably 1.0 GHz or greater, memory of 1GB and RAM: 512 MB or greater.
- The software requirements of the project includes an operating system like Windows 7, 8 etc. The front end used is C# and the framework used is .NET framework 3.5.

SYSTEM ARCHIETECTURE



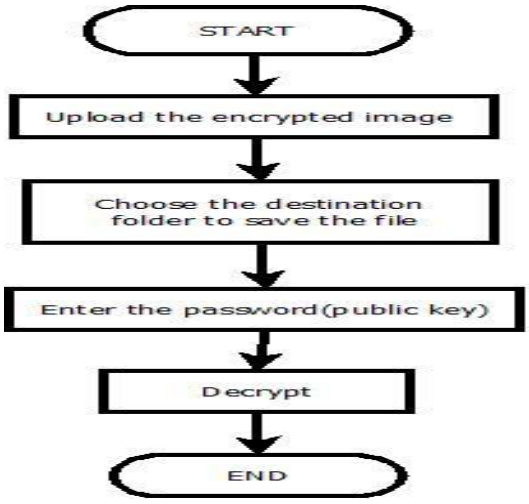
The system is a stand-alone application which is required to be installed in both sender's and receiver's side. The two processes involved are- encryption and decryption. In the encryption process, the sender uploads both the carrier file (image) and the secret file. The secret file is hidden inside the carrier file and we get an embedded image. As for the receiver's side, the decryption process takes place in which the embedded image is decrypted to get back the secret file.

DATA FLOW ON SENDER'S SIDE



In this application, in the sender's side, first he has to upload the image of .jpg, .png, etc. extensions from the local disk, then upload the document file to hide within the image file or enter a text to be encrypted, then set a password for encryption (also called as public key). After entering the password, select the encrypt button which is used to embed the document file into the image file and the image file can be sent to the receiver via any transmission medium (Internet or LAN).

DATA FLOW ON RECIEVER'S SIDE



On the receiver's side, the image file is downloaded and saved by the receiver. Then he has to open the steganography application for decrypting upload the image file in to the application. Once the file is uploaded, select the decryption button for decrypting the file. The receiver can decrypt the file only if he enters the correct password that was used for encryption and a destination folder has to be selected where the document will be extracted to. After the decryption both the image and document is extracted from the encrypted image file. Both the sides should use a common key for the processes, also known as public key.

TABLE I : COMPARISON BETWEEN AES, DES and RSA

A comparison is done between AES, DES and RSA, and among those AES is chosen for encryption of the text is given below: **GLIMPSES OF THE PROJECT INVOLVING THE RESEARCH**

FACTORS	AES	DES	RSA
DEVELOPED	2000	1977	1978
KEY SIZE	128,192,256 bits	56 bits	1024 bits
BLOCK SIZE	128 bits	64 bits	512 bits
CIPHERING & DECIPHERING KEY	Same	Same	different
SCALABILITY	not scalable	it is scalable due to varying key and block size	not scalable
ALGORITHM	symmetric algorithm	symmetric algorithm	asymmetric algorithm
ENCRYPTION	Faster	Moderate	slower
DECRYPTION	Faster	Moderate	slower
POWER CONSUMPTION	Low	Low	high
SECURITY	excellent secured	not secure enough	least secure
DEPOSIT OF KEYS	Needed	Needed	needed
INHERIT VULNERABILITIES	brute forced attack	brute forced attack, linear and differential cryptanalysis attack	brute forced and oracle attack
KEY USED	same key used for encryption and decryption	same key used for encryption and decryption	different key used for encrypt and decrypt.
HARDWARE AND SOFTWARE IMPLEMENTATION	Faster	better in hardware than in software	not efficient
CIPHERING & DECIPHERING ALGORITHM	Different	different	same

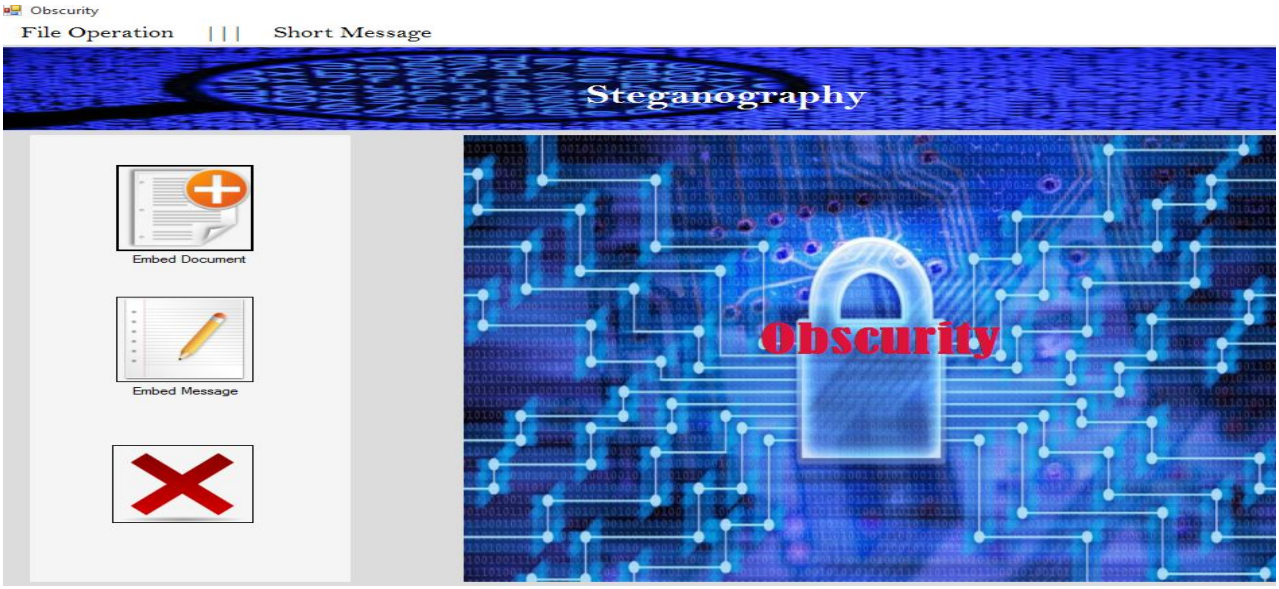


Fig.1 Home Page of our project

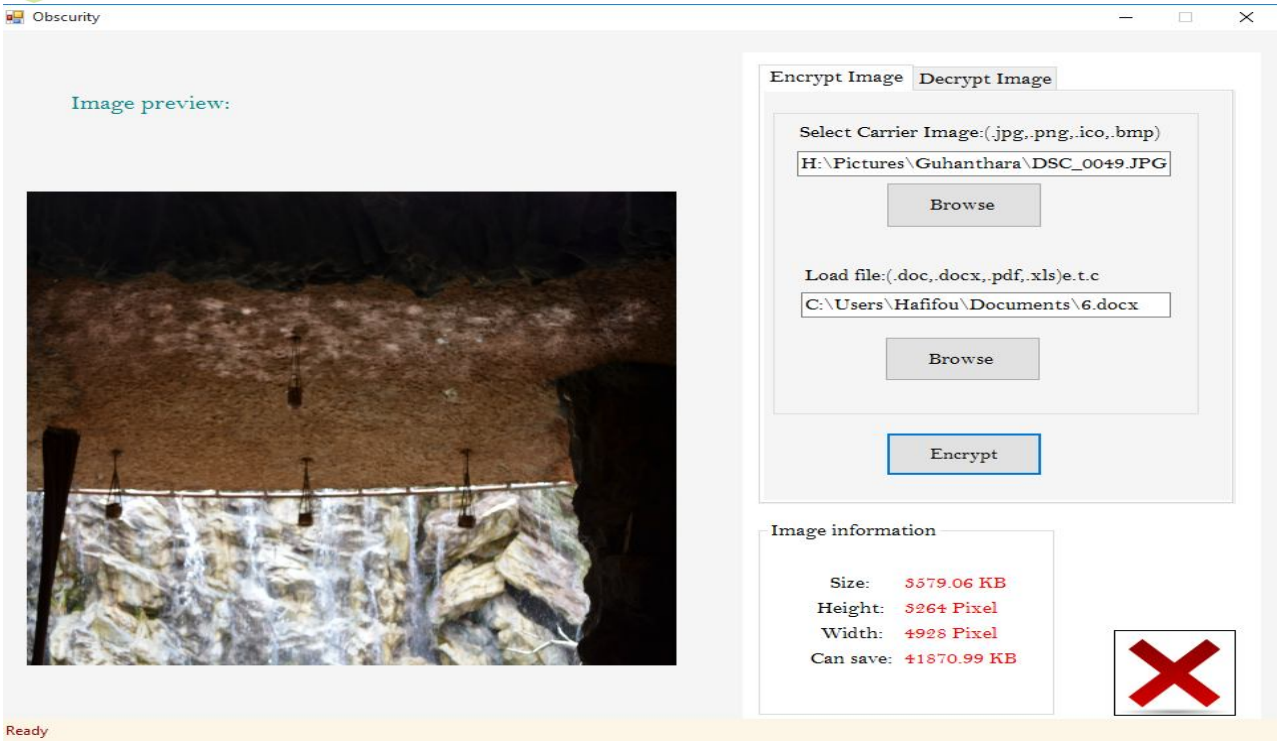


Fig 2: Sender's side (To encrypt)

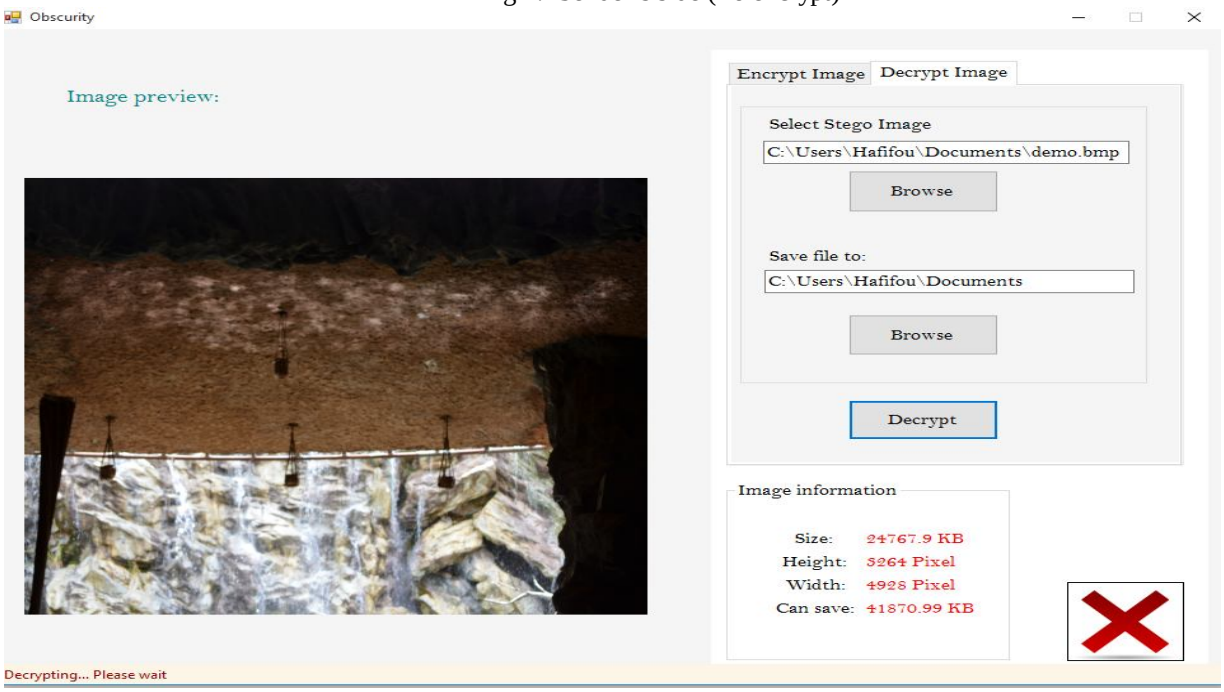


Fig 3: Receiver's side(To decrypt)

IV. CONCLUSION

Steganography can be used for hidden communication. We have explored the benefits of steganography theory and practice. Enhancement of the image steganography system using F5 Algorithm to provide a means of secure communication. A stego-key (commonly known as public key or password) has been applied to the system during embedment of the message into the cover image as well as during extracting the message from the cover image. This steganography application software provided for the purpose to how to use any type of image formats to hiding any type of files inside them. The master work of this application is in supporting any type of images and any type of document file and lower limitation on file size to hide, because of the use of maximum memory space in pictures to hide the file. Some of the future enhancements that can be done includes the use of audio, video etc. as both carrier medium and the file that is required to be hidden. Also there can be different compression techniques applied that can reduce the size of the file to be transmitted.

REFERENCES

[1]. Parah, Shabir A., Javaid A. Sheikh, and G. M. Bhat. "Data hiding in intermediate significant bit planes, a high capacity blind steganographic technique." Emerging Trends in Science, Engineering and Technology (INCOSET), 2012 International Conference on. IEEE, 2012.
[2]. T. Morkel, J. H. P. Eloff, M. S. Olivier, "An Overview of Image Steganography", Information and Computer Security Architecture (ICSA) Research Group, Department of Computer Science,
[3]. Channalli, Shashikala, and Ajay Jadhav. "Steganography an art of hiding data."arXiv preprint arXiv:0912.2319 (2009).
[4]. Narayana, Sujay, and Gaurav Prasad. "Two new approaches for secured image steganography using cryptographic techniques and type conversions." Signal & Image Processing: An International Journal (SIPIJ) Vol 1 (2010).
[5]. Garg, Mitali, and Vikas Wasson. "Data Security with Image Clustering using Steganography."
[6]. N. I. Wu and M. S. Hwang, "Data Hiding: Current Status and Key Issues," International Journal of Network Security, 4(1), pp.1-9. 2010.
[7]. Mehdi Hussain and Mureed Hussain, "Pixel Intensity Based High Capacity Data Embedding Method," International Conference on Information and Emerging Technologies, 1–5, 2010.
[8]. Chen Ming, Zhang Ru, Niu Xinxin,Yang Yixian, "Analysis of current steganography tools: Classification & features" ,Information security center, Beijing University. China.
[9]. R. Chandramouli, M. Kharrazi, N. Memon, "Image Steganography and Steganalysis: Concepts and Practice", International Workshop on Digital Watermarking, Seoul, October 2004.
[10]. William Stallings, Cryptography and Network Security, Principles and Practice, Third edition, PearsonEducation, Singapore, 2003.University of Pretoria, SA.

