# SECURITY OF DATA TRANSFER OVER INSECURE CHANNEL THROUGH STEGANOGRAPHY.

Mr. Narshingha P V
Research Scholar , Dept. of Computer Science
MNIT, Allahabad, India.

***Abstract* - In today's world there is a rapid growth in data transmission over the internet but still security is on fly. The security of information has become a core issue. As a challenge to the Researcher most of the research in this area is going on. There two basic techniques are most widely used achieve this goal: Encryption and steganography is one of them. Using Cryptography, the data is transformed into some other gibberish form and then the encrypted data is transmitted. In steganography, the data is embedded in an image file and the image file is transmitted. The implant process is done with help of stego-key, and the detection or reading of implanted information is possible only having this key. The stego-key is used may be user-defined or default not only to facilitate random selection of bytes for hiding message file bits but also is used to encrypt the user data. The encryption method is based on XORing the message bytes with random numbers generated by a pseudo-random number generator whose source is derived from the stego key.**

***Keywords: XORing, Steganography, Data Applications.***

## I. INTRODUCTION

The network security is becoming more important as the amount of data being exchanged on the Internet is increasing. Security requirements are necessary both at the final end-user and at the middleware, especially since the huge utilization of personal computers, networks, and the Internet with its global availability. Throughout time, computational security needs have been focused on different features: secrecy or confidentiality, identification, verification, non repudiation, integrity control and availability. In addition, the rapid growth of publishing and broadcasting technology also requires an alternative solution in hiding information. The copyright of digital media such as audio, video and other media available in digital industry form may lead to large-scale unauthorized copying. The problem of unauthorized copying is of great concern especially to the music, film, book and software publishing industries. To overcome this problem, some invisible information can be embedded in the digital media in such a way that it could not be easily extracted without a specialized technique [2]. Two ways for securing Data independently used. First way is cryptography, where an encryption key is used to jumble the message, this jumbled message is transmitted through the insecure public channel, and the Reconstruction of the original, unencrypted message is possible only if the receiver has the appropriate decryption key. The second method is Steganography, where the secret message is in planted in another message, thus the existence of message is unknown.

## II. CRYPTOGRAPHY

Cryptography is an important element of any strategy to address message transmission security requirements. In Cryptography basically two techniques are used first one is Substitution cipher & Transposition cipher Cryptology is the science underlying cryptography. Cryptanalysis is the science of 'breaking' or 'cracking' encryption schemes, i.e. discovering the decryption key. Cryptographic systems are generically classified along three independent dimensions [1].

### *A. Methodology for transforming plain text to cipher text.*

In substitution method, each element in the plaintext is represented into another element e.g

| Plain text | A | B | C | D |
|---|---|---|---|---|
| Cipher text | Z | Y | X | W |

One of the disadvantage of this method is by trail and error method any one can easily decrypt the original message. To overcome this lacuna second approach is available i.e. Transposition, in which elements in the Original text are rearranged using some well known phrase. The fundamental requirement is that no Information is lost.

### *B. Suggestive approach for number of keys used.*

There are two approaches, Symmetric &asymmetric cryptography. In symmetric key, Cryptography a single key is shared by sender and receiver. In asymmetric cryptography, public and private keys are used by sender and receiver. In this method sender can encrypt the data using public key of receiver and receiver can decrypt using his private key. In the case of the RSA encryption algorithm, it uses very large prime numbers to generate the public key and the private key. Although it would be possible to factor out the public key to get the private key (a trivial matter once the 2 prime factors are known), the numbers are so large as to make it very impractical to do so. The encryption algorithm itself is ALSO very slow, which makes it impractical to use RSA to encrypt large data sets. What PGP does (and most other RSA-based encryption schemes do) is encrypt a symmetrical key using the public key, then the remainder of the data is encrypted with a faster algorithm using the symmetrical key. The symmetrical itself key is randomly generated, so that the only way to get it would be by using the private key to decrypt the RSA-encrypted symmetrical key.

### *C. Methodology for processing plain text.*

A block cipher processes the input one Block of elements at a time, producing an output block for each input block. A Stream cipher processes the input Elements continuously, producing output one element at a time, as it goes along. The proposed algorithm uses a substitution cipher method. It is a symmetric key algorithm using the technique of stream cipher

## III. STAGENOGRAPHY

Steganography derived from Greek word literally means covered writing. It includes vast array of secret communication method that conceals message very existence. Computer based steganography allows us to implant message in different available what are known as digital carriers such as images or sounds. Digital images, videos, sound files, and other computer files that contain perceptually irrelevant or redundant information can be used as “covers” or carriers to hide secret messages. After implanting a secret message into the cover-image, a so called stego-image is obtained [3].

The basic model of steganography consists of Carrier, Message, and Embedding algorithm and Stego key. The model for steganography is shown in Figure1. Digital Carrier is used as a cover-object, which embeds the message and serves to hide its presence. The suitable carriers that can be used as cover object are Network Protocols such as TCP, IP and UDP, Audio that use digital audio formats such as wav, midi, avi, mpeg, mpi and voc, File and Disk that can hide and append files by using the slack space, Textiles such as html and java, Image files such as bmp, gif and jpg, where they can be both color and gray-scale [5]. Message is the data that the sender wishes to remain it confidential. It can be plain text, cipher text, other image, or anything that can be embedded in a hit stream such as a copyright mark, a covert communication, or a serial number. Password is known as a stego-key, which ensures that only the recipient who knows the message from a cover-object. The cover-object with the secretly implanted message is then called the Stego-object. This stego object is then transferred to other end, there we have detector algorithm which extract the message from cover object [3].

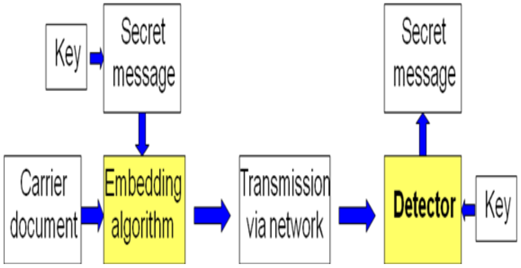


Fig. 1 Model of steganography

There are three different aspects in Information-hiding systems contend with Each other: capacity, security and robustness. Capacity refers to the amount of information that can be hidden in the cover medium, security to an secrete listener’s inability to detect hidden information and robustness to the amount of modification the stego medium can withstand before an adversary can destroy the hidden information.

## IV. PROPOSED MODEL

Data security is a big challenge for computer users. To provide security data hiding technique have been widely used. This proposed system have the software for data encryption and the implanted the cipher text in an image with help of stego key .This algorithm combine the essence of these two methods t enhance the security of the data. The system proposed two algorithms one for encrypting the data with crypto algorithm and second algorithm for implanting the encrypted text in an image file. This algorithm improves the security of the data implanting the encrypted text and not the plaintext in an image.

The working of this proposed algorithm is as follows:

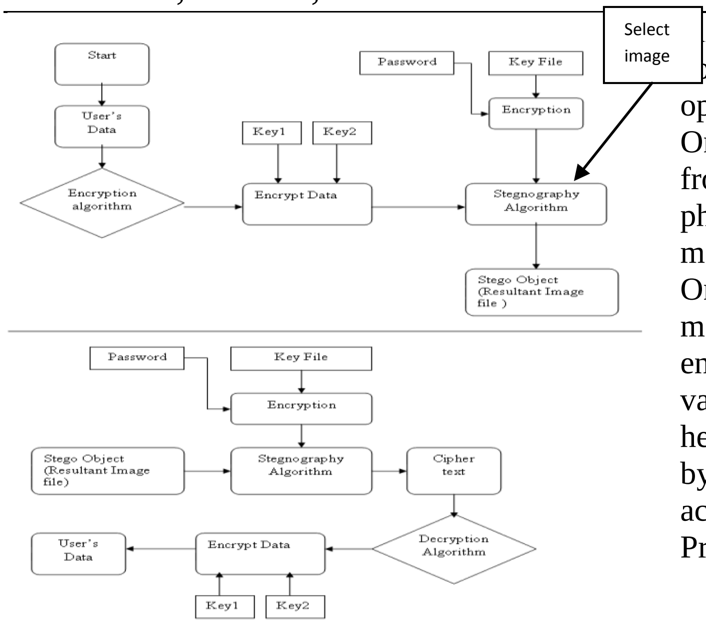


Fig. 2 Procedure for Hiding and Extraction

### *A. Encryption algorithm*

The encryption algorithm built in is a shared key stream cipher algorithm which requires a secure exchange of a shared key that is outside the specification. The algorithm is used identically for encryption and decryption as the data stream is simply XORed with the generated key sequence. The algorithm is serial as is requires successive exchanges of state entries based on the key sequence. The algorithm features are to generate cipher text a variable length key from 1 to 256 bytes is used. The state table is used for subsequent generation of pseudo- random bytes and then to generate a pseudo-random stream which is XORed with the plaintext to give the cipher text. Plaintext to give the cipher text. The algorithm works in two phases, key setup and ciphering. Key setup is the first and most difficult phase of this algorithm. During a N-bit key setup (N being your key length), the encryption key is used to generate an encrypting variable using two arrays, state and key, and N-number of mixing operations. These mixing operations consist of swapping bytes, modulo operations, and other formulas.

Once the encrypting variable is produced from the key setup, it enters the ciphering phase, where it is XORed with the plain text message to create an encrypted message. Once the receiver gets the encrypted message, he decrypts it by XORing the encrypted message with the same encrypting variable. The four symmetric algorithms here using are DES, AES, RC2 and 3DES, by using this algorithms we can encrypt the actual secret data.

Procedure for encryption is as follows:

1. Select the secret data file which we want to hide or simply type the text information.
2. Select two password pass1 and pass2 which generate strong password by combining Two passwords.
3. Select the key for the selected algorithms from the strong password and also select Encryption algorithm.
4. Encrypt the secret data by using the selected key.

Decryption process also requires the same pass1 and pass2 and same algorithm for decrypting the chipper text.

### *B. Hiding data in an image*

To a computer, an image is an array of numbers that represent light intensities at various points, or pixels. In digital, images are represented with the numerical values of each pixel where the value represents the color and intensity of the pixel. These pixels make up the image's raster data. Digital images are typically stored in either 24-bit or 8-bit per pixel files. 24-bit images are known as true color images. Obviously, a 24- bit image provides more space for hiding information as compared to 8 bit image.

*1.) Least significant bit insertion:*

The least significant bit insertion method is probably the most well known image steganographic technique. In 24 bit image we can embed 3 bits in each pixel while in 8-bit we can embed only 1 bit in each pixel. To hide an image in the LSBs of each byte of the 24- bit image, one can store 3 bits in each pixel. A 1024 X768 image has the potential to hide a total of 2,359,296 bits of information for e.g., the letter A can be hidden in three pixels. The binary value of A is 10000011. The original raster data of 3 pixels may be.

(00100111 11101001 11001000)
(00100111 11001000 11101001)
(11001000 00100111 11101001)
After inserting the binary value for A.
(00100111 11101000 11001000)
(00100110 11001000 11101000)
(11001000 00100111 11101001)

The underlined bits are the only three actually changed in the 8 bytes of data. One can hide data in the least and second least significant bits and still the human eye would not be able to discern it. In this proposed algorithm we generate random number initialized with a stego- key and its output is combined with the input data, and this is implanted to a cover image. The usage of a stego-key is important, because the security of a protection system should not be based on the secrecy of the algorithm itself, instead of the choice of a secret key.

A stegosystem encoder can be represented by using the following relation

$$I' = f\ (I, m, k)$$

- where *I' is the stego-object*
- *I is the cover-object*
- *m is the message*
- *k is the stego-file.*

Recovering message from a *stego-object requires the cover-object itself and a corresponding decoding key if a stego-key was used during the encoding process.*

*2). Multi-level securities proposed in the algorithm: To hide a text into the image:*

Step 1**:** Apply encryption algorithm on the text with a strong stream cipher mechanism the stego key is used in encryption of data.
Step 2**:** The cipher text file is implanted into the stego medium.
Step 3**:** The password or stego-key is also encrypted and embedded in image file.
Step 4**:** The key file and password is used to select random pixels for embedding data. The key file is used not only to facilitate random selection of bytes for hiding message file bits but also is used to encrypt the message. The encryption method is based on XORing the message bytes with random numbers generated by a pseudo-random number generator whose seed is derived from the key file and password.

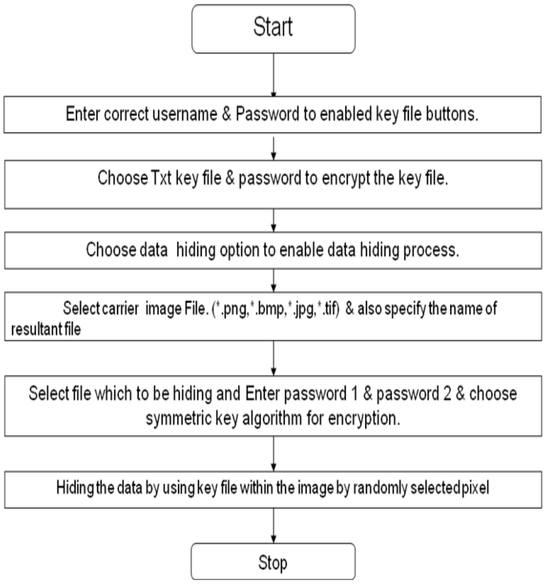

Start
Enter correct username & Password to enabled key file buttons.
Choose Txt key file & password to encrypt the key file.
Choose data hiding option to enable data hiding process.
Select carrier image File. (*.png,*.bmp,*.jpg,*.tif) & also specify the name of resultant file
Select file which to be hiding and Enter password 1 & password 2 & choose symmetric key algorithm for encryption.
Hiding the data by using key file within the image by randomly selected pixel
Stop

Fig.3 Procedure for hiding process

*3.) To retrieve a text from the image:*

Step 1**:** The key file and password is required to extract the message.

Step 2**:** By extracting the LSBs from the stego image, a file containing cipher text is obtained.
Step 3: This file is decrypted using encryption algorithm to get the original file

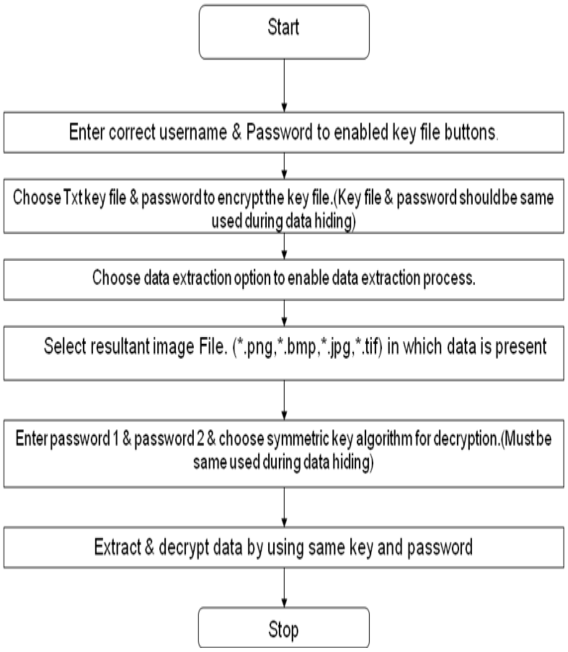
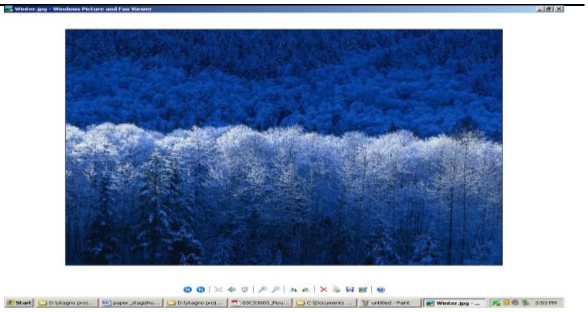

Start
Enter correct username & Password to enabled key file buttons.
Choose Txt key file & password to encrypt the key file.(Key file & password should be same used during data hiding)
Choose data extraction option to enable data extraction process.
Select resultant image File. (*.png,*.bmp,*.jpg,*.tif) in which data is present
Enter password 1 & password 2 & choose symmetric key algorithm for decryption.(Must be same used during data hiding)
Extract & decrypt data by using same key and password
Stop

Fig.4 Procedure for Extraction process

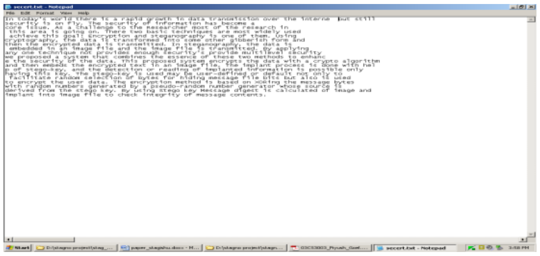
Introducer's must know the following to hack the data:
1. Algorithm to extract the message from the image. (Stego algorithm)
2. Encryption algorithm.
3. Correct password for algorithm.
With these increased levels of protection using encryption algorithm, the proposed system for steganography is stronger from attacks than any other existing system

## V. SIMULATION AND RESULT

Following images were taken and processed by the application of Digital Steganography and the results are as following:

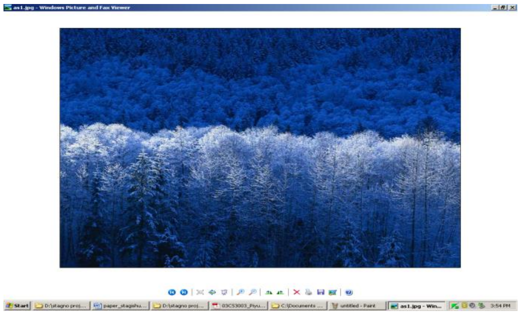


Carrier Image before hiding



```
In today's world there is a rapid growth in data transmission over the interne but still
security is on fly. The security of information has become a
core issue. As a challenge to the Researcher most of the research in
 this area is going on. There two basic techniques are most widely used
 achieve this goal: Encryption and steganography is one of them. Using
cryptography, the data is transformed into some other gibberish form and
then the encrypted data is transmitted. In steganography, the data is
 embedded in an image file and the image file is transmitted. By applying
any one technique not provides enough security's provide multilevel security
we proposed a system that combines the essence of these two methods to enhanc
e the security of the data. This proposed system encrypts the data with a crypto algorithm
and then embeds the encrypted text in an image file. The implant process is done with hel
p of stego-key, and the detection or reading of implanted information is possible only
having this key. The stego-key is used may be user-defined or default not only to
 facilitate random selection of bytes for hiding message file bits but also is used
to encrypt the user data. The encryption method is based on XORing the message bytes
with random numbers generated by a pseudo-random number generator whose source is
derived from the stego key. By using Stego key Message digest is calculated of image and
implant into image file to check integrity of message contents.
```

Secret information which has to be hiding



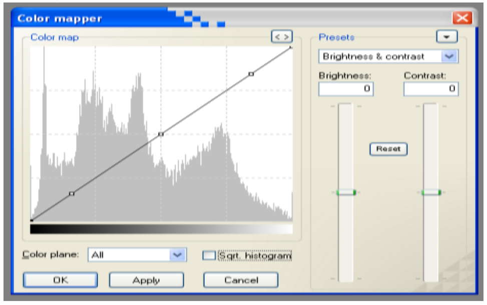
Resultant Image after hiding data

1. Pixel Information before and after stenography process

Consider a pixel with RGB color value

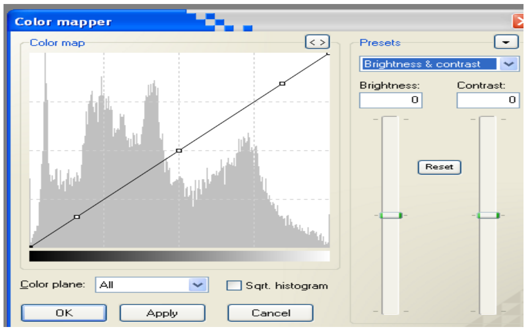
| Sr.No | Pixel Information | Decimal Value | After replacement of LSB bit | Decimal Value After embedding data | Quantization error |
|---|---|---|---|---|---|
| 1 | 10101000 (R) | 168 | 10101001 | 169 | +1 |
| 2 | 10101001 (G) | 169 | 10101000 | 168 | -1 |
| 3 | 10101010 (B) | 170 | 10101001 | 171 | +1 |

2. Histograms of original and resultant image



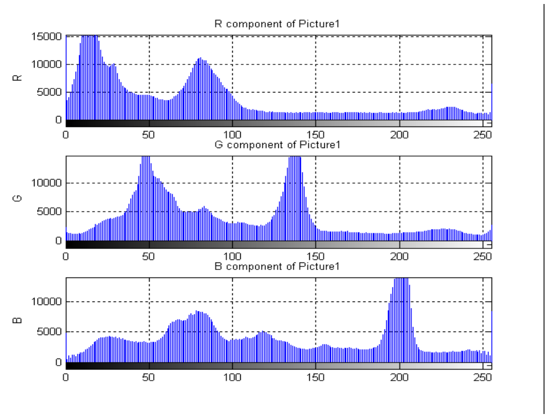
Brightness & contrast
Brightness: 0
Contrast: 0
Color plane: All

Original Image Histograms



Brightness & contrast
Brightness: 0
Contrast: 0
Color plane: All

Resultant Image histograms



RGB component of the resultant Image

## VI. CONCLUSION

Steganography provides many different mechanisms to hide the data. This paper presents an image steganography algorithm which uses LSB insertion technique, random number generation algorithm, region of interest selection. These techniques are used for providing better security for efficient data transmission Randomization adds more security to the algorithm. Higher Security is achieved through the use of strong keys during encryption. Higher capacity than any other data hiding method. Simple to use as well as simple way to hide data.

## VII. REFERENCES

[1] Stinsown,D.“Cryptography:Theory and practice”

[2] Z. Hrytskiv, S. Voloshynovskiy & Y. Rytsar “Cryptography of Video InformationIn Modem communica-tion”, Electronics And Energefics,vol. 11, pp. 115-125, 1998

[3] Neil F. Johnson, Zoran uric,Sushil. Steganography and Watermarking –Attacks and Countermeasures”,Kluwer Academic Press, Norwrll,MA,New York, 2000

[4]C. Cachin, “An Information -theoretic Model for steganography”,in proceeding 2nd Information Hiding Workshop, vol.1525, pp.306-318,1998

[5] J. Zollner, H. Federrath, H. Klimant, et al.,“Modeling the Security of Systems”, Steganographic in 2nd Workshop on Informafion Hiding,Portland, April 1998, pp. 345-355.proceeding of IEEE, pp. 1062-1078,July1999.

[6] R A Isbell, “Steganography: Hidden Menace or Hidden Saviour”,steganography White Paper,IO May 2002

[7] M. M Amin, M. Salleh, S. Ibrahim, M .R. Katmin, and M. Z. I. Shamsuddin,“ Information Hiding using Steganography”, IEEE 0-7803-7773-March 7,2003

[8] Comprehensive Analysis and Enhancement of Steganographic Strategies for Multimedia Data Hiding and Authentication Ali Javed, Asim Shahzad,

Romana shahzadi, Fahad Khan (IJCNS) International Journal of Computer and Network Security, Vol. 2, No. 3, March 2010 .

[9] A New Image Stegano graphy Based On First Component alteration Technique Amanpreet Kaur1, Renu Dhir2, and Geeta Sikka3 (IJCSIS) International Journal of Computer Science and Information Security Vol. 6, No. 3, 2009

[10] A Novel Technique for Embedding Data inSpatial Domain , V.madhuViswanatham, Jeswanth Manikonda , (IJCSE) International Journal on Computer Science and Engineering ,,Vol. 02, No. 02, 2010, 233-236