ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 7, Issue 3, March 2018

An Implementation of Steganography Technique to Provide better Security in Workgroup Communication

Girjashankar M. Thakur [1], Pratima Sonwane [2], Roshni Bhalawi [3], Mohd. Jabeed Rihaz [4]

U.G. Student, Department of Information Technology, KITS Ramtek, Nagpur, Maharashtra, India[1, 2, 3]

Assistant Professor, Department of Information Technology, KITS Ramtek, Nagpur, Maharashtra, India[4]

ABSTRACT: Now days Internet is basic need, almost all work is being done on internet, the security for data transmission and online transactions is demanding. Security measures are handled by encryption/decryption, password protection etc. But it is not enough sufficient for communication because as technology increases threats, violation's also increases. Here is an idea is, 'why would not we choose a way that will make actual communication unknown to others', that is Steganography. Steganography is an art of hiding the secret data in an innocent medium so that nobody can notice it except entitled users. Here in this we propose a workgroup communication system that uses Encryption technique, LSB method of Steganography and password protection to make communication secure between the sender and receiver. If receiver enters password 3 times wrong system will notify it to admin as guilty user then admin will take necessary care of it. Workgroup may be an organization, security agency, group of people from community, government agencies etc. In an organization slave users will also remain sometime unknown to the actual message, because potential data will be maintained at admin site, users need to request file and send the receivers id to admin. Admin will take care of security by applying the encoding and received message is decoded by receiver using password sent on his mail. In this either communication can be a normal or any cover medium that contains secret message while in transit.

KEYWORDS: Data transmission, Online transaction, Encryption/Decryption, Technology, Threats, violation, Communication, Steganography, Secret Data, LSB, Decoding, Cover medium, Transit, Admin.

I. INTRODUCTION

A. Steganography

Steganography is robust technique to make our communication secret. Steganography is a technique which is capable to embed secret data bits by manipulating existing data bits of cover medium with negligible bad effect on quality of cover medium. In steganography cover medium could be from audio, video, image, communication etc. Steganography is not only being applicable in digital age and steganography is not a new thing it has been used from as far back as ancient time. Ancient methods are like invisible ink and layered painting were used by them to hide secret message in plain sight it is common to use steganography in defence for hidden communication along with cryptography. Generally in war cryptography were used as an example "*This is charley, Tango come in. I repeat, this is charley, Tango comes in*". In given example secret message is transmitted in coded form, who knows the code can decode it, there may be probabilities that enemy can note it and may be successfully decode it, in this situation we need a hidden way to communicate and precisely can be done with steganography with greater accuracy. Cryptography is for encoding secret message and steganography is as shell that protects encoded data. Now in growing digital age we have many steganography techniques such as *Audio steganography*, *Video steganography*, *Image steganography* and *Voice over Internet Protocol (VoIP).* Each steganography technique is related to its cover medium. Cover media is nothing but the medium which carries secret message. In Image steganography, image is a cover medium i which the secret

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 7, Issue 3, March 2018

message is embedded. Similarly video steganography will use video, audio steganography will use audio and VoIP is new concept. VoIP steganography allows transferring secret data bits while voice calling or video calling over Internet. Each steganography techniques having their own algorithms to encode secret data. Here we are using Image steganography in this LSB algorithm is used to form an encoding system. LSB algorithm works by manipulating the least significant bits.

Following terminologies are used very useful in steganography.

- Secret data - Data which is confidential to be hidden in medium.
- Cover file – It is the file where secret data is to be hide and sent to the recipient.
- Stego temp - It is the file discovered after applying the steganography algorithm to cover file.
- Stego key – it is extra level security key is applied over a Stego temp file to lock/unlock.

II. CRYPTOGRAPHY

Cryptography is another important security measure used widely in the digital world that makes commonly readable text to unreadable text. Now day's security means cryptography because this maintains integrity, authentication and confidentiality of message. This technique is used everywhere, that could be weather online transaction, database transactions, social messaging, message in transit, data transfer etc so that only entitled user can read it. Cryptography involves encryption and decryption process. Encryption process converts from plain text to cipher text. Decryption process is opposite to encryption. Encryption is done by sender by some sort of key(s) and receiver will use same key or its private key to decrypt the data. Here in cryptography key length of key(s) varies from algorithm to algorithm, for example DES algorithm uses 56 bit one key for encryption and decryption. Cryptography comes with two types of keys first is symmetric key encryption/decryption and second is Asymmetric key encryption/decryption. Symmetric key encryption/decryption algorithm uses only one key for both encryption and decryption process (ex. DES, Triple DES, AES). Asymmetric key algorithms use 2 keys, one for encryption called public key and another for decryption called private key only known to receiver itself. In asymmetric key encryption algorithms authentication and confidentiality is rescued, these algorithms are more secure, robust , varies in key length, process data in 512 bit blocks, provides substitutions and permutations for confusion and diffusion examples of such algorithms are RSA, IDEA, Diffie-Hellman, Digital Signature Standard and more. Here in our proposed system we used RSA algorithm for encryption/decryption of secret message.

Some terminologies related to Cryptography

- Plain text – The normal text which can be read by anyone.
- Cipher text – The text which is in unreadable format.
- Key – key can be alphanumeric words used for converting message into cipher and retain it back into plain text.
- Key length – key size in bits.

Following figure as fig 1.Symmetric Cryptography, depict the symmetric encryption process where only single key is used for both encryption and decryption. Plaintext is supplied to encryption module that makes use of key to convert easily readable text form to unreadable form at the sender side. The Outcome as Cipher text is transferred through some sort of network and reaches to the receiver, on this side receiver uses same key to get back the original data (Plain text).

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 7, Issue 3, March 2018

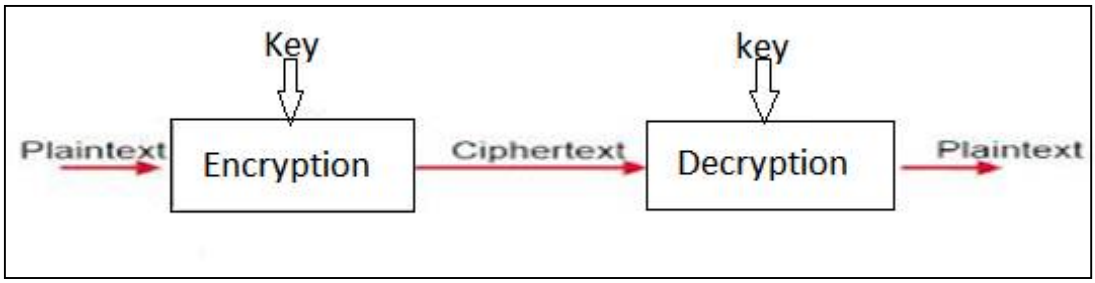


Fig1. Symmetric Cryptography

Following figure as fig2. Asymmetric Cryptography, this is more secure than symmetric cryptography because it deals with the 2 keys, one is for encryption called public key of receiver and another is for decryption as private key of receiver. When any plain text is encrypted using public key can be only decrypted by receiver's private key. Here public key is like User ID (ex. gmail id) known to any one and private key is like password. Asymmetric key cryptography maintains the authentication of message.

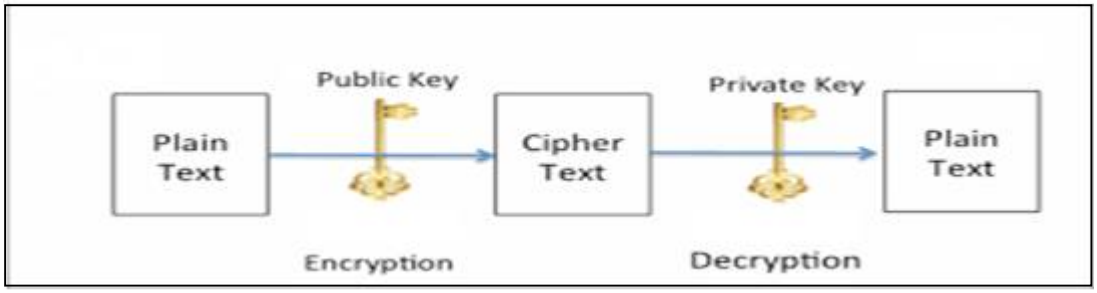


Fig2. Asymmetric Cryptography

III. RELATED WORK

Our workgroup steganography system consists of encoding/decoding, password protection and detection of guilty user. Encoding of secret message is nothing but the applying RSA Asymmetric cryptography to convert it into cipher text and it has some advantages first, hiding of encrypted message having almost negligible bad effect on quality of Image. Second, in case from cover medium secret message is been extracted by third party, but he/she won't come to know that what was the message because of receiver's private key. After that the encrypted message has to gone through hiding process to be embedded in cover file. Hiding process is done by LSB algorithm of Image Steganography technique. Then the entire message is surrounded by password, so the locked file is only unlocked by entitled receiver if receiver fails to unlock file more than 3 attempts then he/she will be recognised as guilty user and notified to administrator. Unlocked message is tend to extract message from cover medium and then decrypted to get secret message, this was about decoding. So the data is 3 times secure from being attacked and tempered.

1. LSB Algorithm

The LSB technique belongs to the spatial domain technique of steganography manipulates cover image pixel value by embedding directly the secret message to pixel value. The LSB is one of the main technique in spatial domain image steganography. A digital image is a 2 dimensional matrix of color intestine at each grid point (pixel). Typically grey image makes use of 8 bits, at another side colored image uses 24 bits to implement color model, such as RGB model.

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

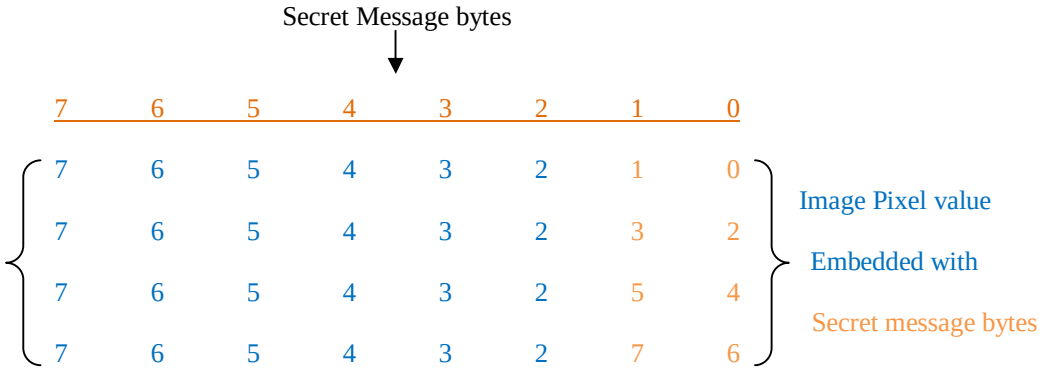
(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 7, Issue 3, March 2018

The secret data bits are merged directly to the image bytes. Spatial domain techniques are simple to implement and in that LSB is popular.

Consider the following example-



Some Outputs:

- Following an image represents the hexadecimal data of original cover image, as well as it shows the intensity of each and every pixel that may be manipulated by the secret message bits so the pixels may slightly change their original color intensity.

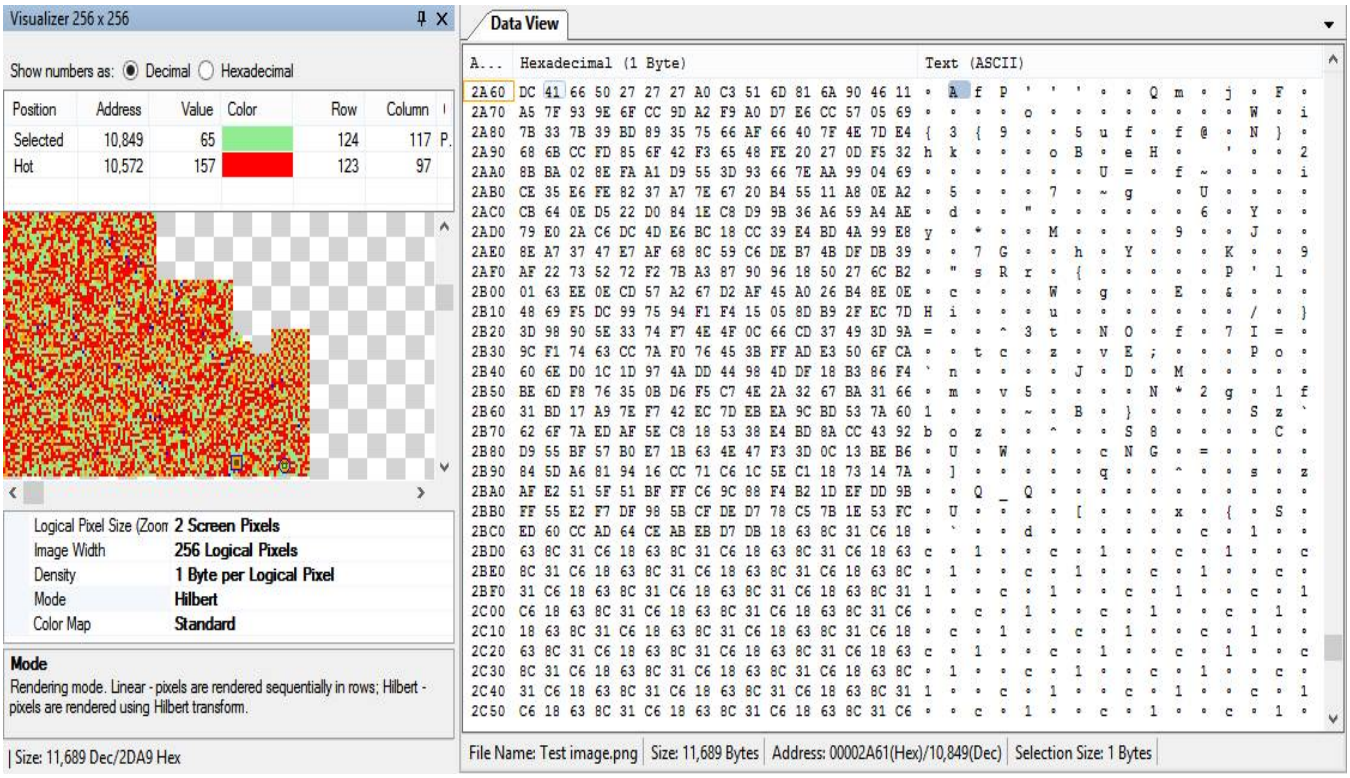


Fig. 3- Original Image pixel values

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 7, Issue 3, March 2018

Following an image carries the secret data, if we analyse the both the images we come to figure out some variance between them. Here yellow color pixel's is secret data embedded to the cover image via LSB technique and if you can see then there is some change in hexadecimal data presentation comparing to the previous.

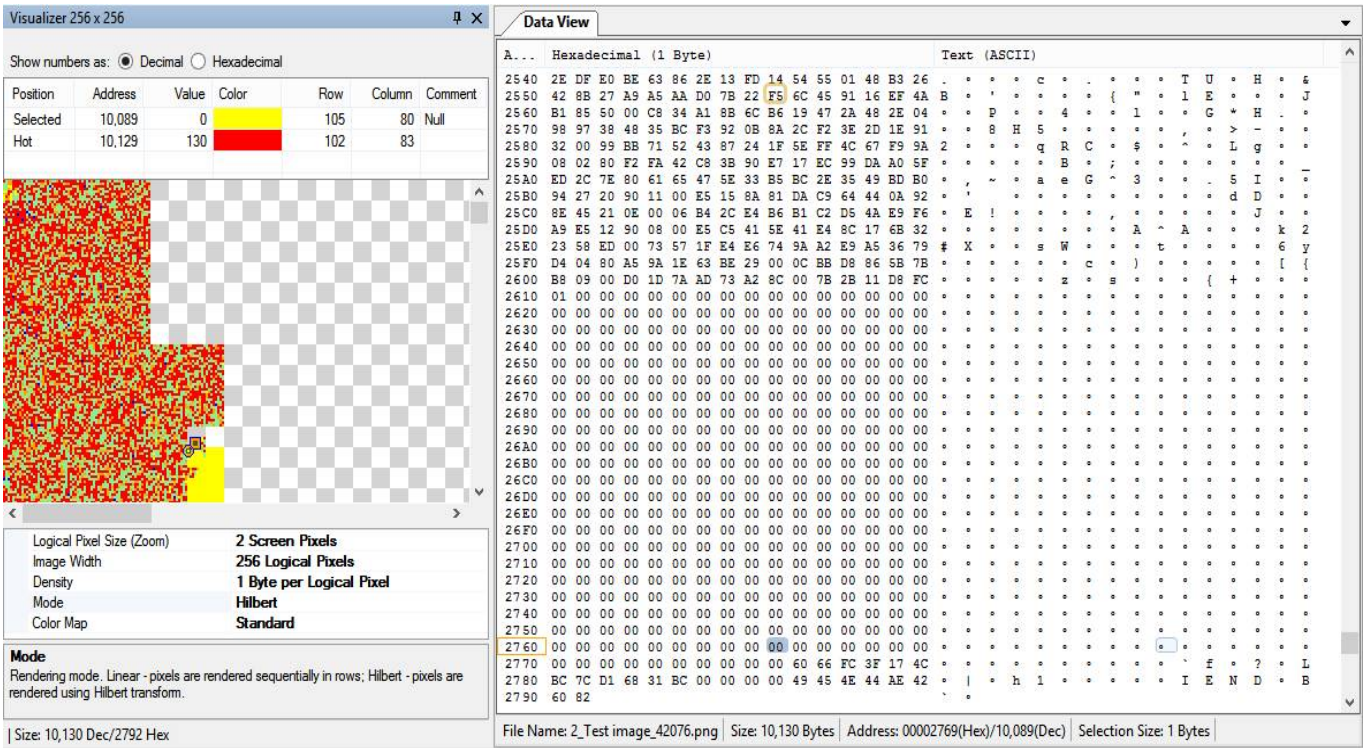


Fig. 4 – Manipulated pixel values with secret data.

2. RSA Algorithm

RSA is an asymmetric key cryptography algorithm; it uses public key to encrypt the text and private key for decryption. It was introduced by Ron Rivest, Adi Shamir, and Leonard Adleman In 1978 to replace National Bureau of Standards (NBS) algorithm because of less security. RSA were implemented two concepts first is public key encryption and second is digital signature. Digital signature used to ensure message is from authenticated user or not and public key encryption is used for confidentiality of message.

Public key cryptosystem – Encryption and Decryption is done by each user, let's take encryption as E and decryption as D. The process E & D involves keys are public key (senders key), private key (receivers key) and of course text will be there.

- Decryption - D(E(M)) = M
- Encryption - E(D(M)) = M
- The publicity of E does not compromise the secrecy of D, meaning you cannot easily figure out D from E.

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 7, Issue 3, March 2018

Signatures – Digital signature completely ensures that the message is from entitled user, if third party grabs the message and try to replay to receiver couldn't be succeed because of false signature. False signature can be found out by comparing the digital signature in message and sender's signature if are equal then it is considered as message is not tempted.

Consider the example – BOB wants to send message to ALICE. We decrypt the message by BOB's key, the cipher text is treated as the message.

$$DB(M) = S$$

Encryption will be by ALICE's encryption key,

$$E_A(S) = E_A(D_B(M))$$

When we get the signature by $D_A(E_A(D_B(M)) = S$. Now ALICE knows the message came from Bob. Since ALICE decryption key can compute signature correctly. Now let's say an intruder try to prove that this message is from public file, this is not the problem with the RSA because of the signature is used

Algorithm - working of RSA is explained below.

Encryption - $C = M^e \bmod n$

Decryption - $M = C^d \bmod n$

Step1. Select large prime number (p, q).

Step2. Calculate n. (n = p*q).

Step3. Calculate Ø (n) = (p-1) * (q-1)

Step4. Select public key e = gcd (Ø(n), e) = 1

$d = e^{-1} \bmod n$
$ed = 1 \bmod n$

Where,

C – Cipher text
M – Message
d – Private key
e – Public key
Ø (n) – Euler function
p ,q – Prime no

From above algorithm we conclude the following steps to find the keys.

- Finding the large prime numbers.
- Finding d.
- Finding e form d and φ(n).

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 7, Issue 3, March 2018

Example:

p = 3, q = 11**, m = 5**, d = 7, e =? , n =? , Ø (n).

$C = M^e \bmod n \quad M = C^d \bmod n$

n = p*q = 3*11 = 33

Ø (n) = (p-1) (q-1) = (3-1) *(11-1) = 20

ed -1 = Ø (n)
e*7-1 = 20
e*7 = 21
e = 3

$C = 5^3 \bmod 33$
$= 125 \bmod 33$
$= 26$

$M = 26^7 \bmod 33$
$= 8031810176 \bmod 33$
M = 5

IV. CONCLUSION

In this paper we discussed about, how we can emerge the steganography and cryptography techniques in workgroup communication and it is essential to have strong security in communication because an organisation posses very potential data related to organisation should not be disclosed while in transit. Here we used LSB Image steganography algorithm for data hiding purpose and RSA algorithm in cryptography for encryption of secret data. RSA is more secure because it uses asymmetric keys, becomes difficult to beat the security because it ensures the confidentiality as well as authentication. LSB algorithm is good for hiding the data in image with negligible side effects which can't be seen by open eyes. Not only the Steganography and cryptography but also password protection is provided to entire encoded message. This makes the perfect combination for protecting data on transit because the data is encrypted, which is been sent secretly along with it is locked by password.

REFERENCES

1. Priyanka Tirkey, Dipika Kudiyam, Neha Dhruw, Deepshikha Markam, Miss Rumi Ghosh., "Image Steganography Using LSB Along With IDEA Algorithm", Department of CSE, New Government Engineering College Raipur, Chhattisgarh, India 492001.
2. Champakamala, B.S, Padmini.K, Radhika .D. K Asst Professors, "Least Significant Bit algorithm for image steganography", Department of TCE, Don Bosco Institute of Technology, Bangalore, India.
3. Evgeny Milanov, "The RSA Algorithm", 3 June 2009.
4. C.P.Sumathi, T.Santanam and G.Umamaheswari, "A Study of Various Steganographic Techniques Used for Information Hiding", Department of Computer Science, SDNB Vaishnav College for Women, Chennai, India.
5. Hanzhou Wu, Wei Wang, Jing Dong and Hongxia Wang, "A Simply Study to Steganography on Social Network", Institute of Automation, Chinese Academy of Sciences, Beijing 100190, China School of Inf. Science & Technology, Southwest Jiaotong University, Chengdu 611756, China
6. Jędrzej Bieniasz, Krzysztof Szczypiorski, "SocialStegDisc: Application of steganography in social networks to create a file system", Institute of Telecommunications Warsaw University of Technology Warsaw, Poland
7. Champakamala .B.S, Padmini .K, Radhika .D.K Asst Professors, "Least Significant Bit Algorithm for Image Steganography", Department of TCE, Don Bosco Institute of Technology, Bangalore, India.
8. Dr. Rajkumar L Biradar, Ambika Umashetty, "Survey Paper on Steganography Techniques", IJIRCCE vol. 4, Issue 1, January 2016.

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 7, Issue 3, March 2018

9. 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 University of Pretoria, 0002, Pretoria, South Africa.
10. Shailender Gupta, Ankur Goyal and Bharat Bhushan, "Information Hiding Using Least Significant Bit Steganography and Cryptography", Department of Electrical & Electronics Engineering, YMCAUST, Faridabad, India. I.J.Modern Education and Computer Science, 2012, 6, 27-34.
11. Shilpa Gupta, Geeta Gujral and Neha Aggarwal, "Enhanced Least Significant Bit algorithm For Image Steganography", IJCEM International Journal of Computational Engineering & Management, Vol. 15 Issue 4, July 2012.
12. Jawahar Thakur and Nagesh Kumar, "DES, AES and Blowfish: Symmetric Key Cryptography Algorithms Simulation Based Performance Analysis", ISSN 2250-2459, Volume 1, Issue 2, December 2011