Hiding Encrypted Messages in Medical Images using Dwt Technique

Manjula G, Mohan H.S.

Abstract: *Today, with the invent of modern technological applications, it requires a greater security measure to transmit confidential data over various unsecure networks particularly in the fields of military, medical Infrastructure and so on. It can be sent through various communication channels that includes multimedia media like audio/video, electronic signals etc. To transmit information securely, different methods like steganography or cryptography can be used. The term steganography has its derivative from the Greek words "steganos" meaning hidden or covert and graphia meaning writing.Steganography can be defined as a way of hiding a confidential file, text information, or any other multimedia content (image, video or audio)into any other multimedia carrier file. In this work, steganography based on Discrete Wavelet Transform (DWT) method is proposed where in the secret data is inserted in the modified coefficients of the cover image. The proposed steganography method is implemented in the frequency domain. This approach caters to the needs of users based on the capacity and quality of inclusion data to be transmitted using medical images. To attain this, the recommended algorithm comprises of converting the message into encrypted text using the modified AES algorithm with 8x8 state matrix and incorporating information of encrypted text into medical images. Contrasting to the spatial domain methods, the encrypted confidential messages will be are assimilated into the high frequency coefficients which are obtained by applying discrete Wavelet transformation. Experimental results reveal that embedding encrypted data using DWT technique gives good PSNR values to attain high quality stego images.*

Keywords : Cryptography, DWT, MSE, PSNR, RGB color planes, Steganography, Stego image

I. INTRODUCTION

Access to digital data has been enhanced by the rapid increase in the utilization of modern information expertise and the progression of digital technologies to hide information through various multimedia files. The reliability of the technology allows data processing, data storage, recovery, control, transfer, information protection and protection efficiency and accuracy. The handling of communications through digital formats like text files, images, audio and video requires to be reinvented by innovative technologies and faster applications so that it should not be easier for the attackers and adversaries to obtain illegal access to the original information.

However, the interchange or flow of data through the network (LAN or Internet) is easy to access from anywhere, which opens the door to many security threats. Therefore, considering for a long time to protect the confidentiality of the anticipated message, individuals began towards looking for new techniques to protect the informations. Two of the most ideal techniques for hiding sensitive and critical data is Cryptography and Steganography [1,2,3].Much attention has been received in the distributed system for the protection of intellectual property rights and the security of the digital data across various communication medium. Therefore, it presents new challenges for researchers. The general idea behind steganography is to hide information in digital format. By doing so it creates an invisible communication channel on the network. The information that has to be secured is embedded into a visually seen image or any other multimedia carrier and is usually hidden from the adversaries. Digital watermarking is yet another specific way of concealing information into images. The digital watermarking can be defined as a of process where sensitive information or message is inserted into digital carrier files and subsequently permits extraction or detection of the embedded data for a variety of purposes such as copyright protection and data access control. The digital watermark has become a vigorous and significant study in research field of Information security. In watermarking uses, such as copy right security and validation, there are aggressive partners trying to eliminate, disable or falsify watermarks. With the concealment of information, there would be no aggressive attackers as the information would be hidden into a different file. Nevertheless, this way of information concealment expertise must be robust and complex against inadvertent distortion. Unlike the concealment of information and the watermark, the core aim of steganography is to transfer the information securely in a entirely impossible manner to track. Steganography extension technology shares the important goal of maximizing stego channel capacity, making it robust and imperceptible. Steganography techniques can be classified into following techniques based on processing of pixels or image coefficients:

- Spatial domain: In this technique, the processing is straight away applied to the pixel values of the image or when changing pixel values. (Bit plane, LSB, pallet centred methods)

Revised Manuscript Received on January 30, 2020.
***** Correspondence Author

Manjula G*, Research Scholar, VTU, Bangalore, India.
Dr .Mohan H.S., Prof & Head, Dept. of ISE, SJBIT, Bangalore, India.

- Frequency Domain: The basic step is to make use of mathematical tools to convert the image data into frequency domain coefficients.
  Subsequently, then the data is inserted in frequency domain coefficients according to various data physiognomies spawned by these transformations.

The expected transformation domain of steganographic schemes is to improve the balance of robustness, security and fidelity over spatial domain schemes.

A wavelet can be defined as a mathematical function wherein a given continual time signal data is divided into various frequency components. A wavelet can be defined as a indigenous change in a one-dimensional acoustic signal, or a local change in the details of a two-dimensional image. By using steganographic methods we can embed the secret data into regions that are not noticeable by human eyes and this can be achieved by hiding data into detailed sub bands of HL and LH coefficients.

The Discrete Wavelet Transform [4] is a technique where the secret data can be effectively embedded in the recognized portions of the cover image. In DWT technique, the information is separated into it's high and low frequency constituents. The edge information of the signal is stored in High frequency component whereas peak signal information is kept in the low frequency component. The information in low frequency component is again fragmented into high and low frequency fragments. To implement DWT in two dimensional applications, every level of decomposition requires DWT to be accomplished in the vertical way and then followed by horizontal direction.

II. LITERATURE SURVEY

Chan, C.K et.al [5] have proposed frequently used steganographic technique known as Least Significant Bit Substitution (LSB) technique. In this LSB method the secret data is inserted into least significant bits which have minimum weighting and are unable to be noticed by naked human eye. In the paper proposed by Chang, C.C et.al [6], a novel method in spatial domain is proposed where the correlation between adjoining pixels of the images are exploited to define the bit number that is used to embed the secret data.

I. Khalil et al. [7] presented a novel wavelet-based steganographic system that combined both encryption and data scrambling method to secure patient's sensitive information. In this method patient's critical data such as blood pressure, temperature, glucose reading and other biomedical data would be encrypted hidden in the patient's ECG signal. This signal is then directed to the server at the hospital through Internet. Only Authorized person will be able to decode the concealed data thus patient's transmitted ECG signal is used as a carrier file to transmit the hidden data.

Athani et al. [8] recommended a new method of hiding the data securely inside the non-overlapping blocks of pixels in the colour image by making use of sparse representation. In this method the sub images of the two dimensional wavelet transform for a given color image is used to conceal data without For a given colour image the sub-images of the two-dimensional wavelet transform of two colour bands are utilized for data hiding without disturbing the image quality .

Sharma V.K et. al. [9] have proposed a combined method of steganography and cryptography. This method makes use of two stages: i) Using encryption the secret data is first encrypted ,which is the followed by generating a secret image from this encrypted message.ii) Next, hide this encrypted data, into a cover image by making use of Daubechies Discrete Wavelet Transform procedure trailed by collaborating operation. Subsequently, performing the Daubechies inverse discrete wavelet transform (IDWT) process on the cover image, we acquire the stego image. This increases the image visual quality of the stego image.

Dave and H.J. Patel [10] have proposed a new variation of image steganography which is based on LSB. In this method both the communicating parties must approve on a series of host images and a assured number of factors. First, the source selects a image file among the given set of images and uses LSB technique to hide the secret message to spawn the stego image. At the receiving end, the designated receiver will be capable to remove the hidden message from the LSB bits of the stego image with the help of the constraints that was chosen during transmission. The probability of predicting the parameters is very low. Hence, abstraction of the data without these parameters is very challenging.

Hamad A. A. et al [11] have presented a high capability and effective steganography method, in which binary images, colour images, and huge text files can all be covered inside a single distinct cover image simultaneously using Haar Wavelet transform.

Stuti Goel et.al 12] have discussed the performance of DCT,LSB and DWT techniques and their performance is evaluated based on metrics such as MSE, PSNR, capacity and robustness. From the results generated DWT provides high robustness where the hidden data is extracted in a secure manner without degrading the image quality.

III. DWT (DISCRETE WAVELET TRANSFORM)

This is another frequency domain where steganography can be implemented. To implement lossless image compression DWT is used in signal and image processing. DWT is applied on a image using Haar Wavelet method where in low frequency components are produced by taking the average of two pixel values and simultaneously calculating the high frequency components by taking half the difference of the same two pixel values. DCT is designed by calculating on chunks of independent pixels, and this coding might trigger a incoherence between blocks causing an aggravating obstructive artifact. This shortcoming of DCT is eradicated using DWT. DWT is applied on complete image and gives improved compaction rate. DWT splits the obtained frequency components into various sub bands as defined below:

LL – Horizontally and vertically low pass

LH – Horizontally low pass and vertically high pass

HL - Horizontally high pass and vertically low pass

HH – Horizontally and vertically high pass

The confidential message can be concealed in the LH, HL, HH frequency bands as these contain insignificant data.

The LL sub band is not altered since it is the low frequency sub band and is clearly very sensitive to naked human eye vision. Hiding secret data in high frequency bands will not degrade the quality of the stego image.

IV. PROPOSED METHODOLOGY

In this paper, the proposed method presents a innovative method to embed confidential data in the mask, which uses certain areas rather than embedding data anywhere in the image. Before hiding the data , skin color detection method is accomplished on the input cover image by using the Hue, Saturation and Brightness (HSV) color space. The skin area of the cover image is cropped to improve security of the message. This cropped area works like a key on the decoding side. The embedding can be done in the G or B plane, but it cannot be done strictly in the R plane because the influence of the R plane in flesh color is greater than the G or B plane.
Therefore, if the value of Pixel of the R plane, the detection of skin on the decoder side provides a different mask than the encoder side, so the decoder side will not get any data. When leaving the R plane, one of the two planes for the cover image is converted to the frequency domain by applying Haar-DWT. Lastly, the confidential data is embedded in one of the high frequency sub bands, by tracking the mask pixels of that band. With this method the embedding operation affects only a specific region of interest (ROI), not the entire image. Therefore, it is advantageous to use objects in the image. The figure 1 shows the proposed methodology.

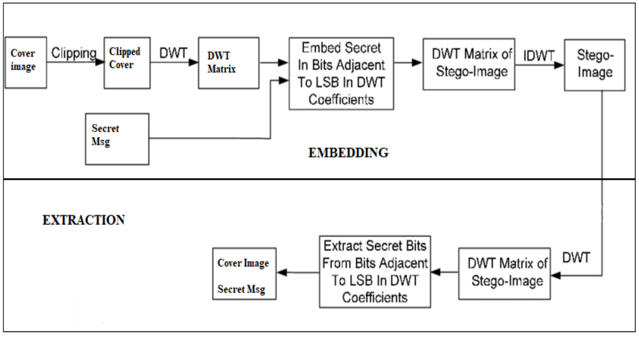
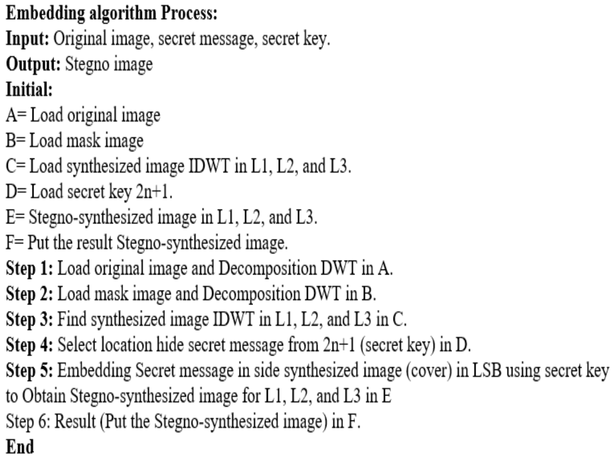

Cover image
Clipping
Clipped Cover
DWT
DWT Matrix
Embed Secret In Bits Adjacent To LSB In DWT Coefficients
DWT Matrix of Stego-Image
IDWT
Stego-Image
Secret Msg
EMBEDDING
EXTRACTION
Cover Image
Secret Msg
Extract Secret Bits From Bits Adjacent To LSB In DWT Coefficients
DWT Matrix of Stego-Image
DWT

Fig 1: Recommended Methodology for hiding data in Image using DWT technique

Assume C is the cover 24-bit colour cover image of M×N Size. It is represented as:

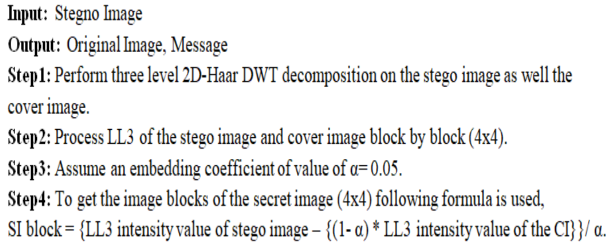
$$C= \{xij, yij, zij \mid 1 \leq i \leq M, 1 \leq j \leq N, xij, yij, zij \in \{0, 1 \dots 255\}\}$$

Let the representation of the size of cropped image be denoted as Mc×Nc where Mc ≤M and Nc ≤N and Mc=Nc. This makes the cropped portion of the image to be in the shape of a square, Since we have to apply DWT again on this portion.
Different stages in implanting the confidential data within the cover image is defined as follows:
Step 1: First apply skin tone detection method on the cover image before loading the image. By using this operation a different mask image is produced that contains skin and non-skin pixels.
Step 2: The next operation is to clip the mask image ($M_c \times N_c$). After clipping is done on the original image we get an exact square area. The clipped region should contain skin areas such as face, hand etc. since we will hide secret data in skin pixels in one of the high frequency components of DWT. DWT is applied only on the cropped part of the original image and this will not be detected by the eavesdroppers.
Step 3: On the clipped area ($M_c \times N_c$) of the image apply DWT and not on the whole image. The output of this process generates four sub bands which are denoted by LL, LH,HH, HL. The capacity of the image to store the hidden data is determined by the number of skin pixels associated in the high frequency sub bands.
Step 4: Now, the process of embedding the secret data is done in any one of the 3 high frequency sub bands. Here high frequency HH band is chosen to embed the secret data. The LL band is not chosen because it contains significant information about the image and any variations in this band affects the eminence of the stego image and can be visualized by naked human eye. Further to improve the security DWT process is applied only to the skin pixels of the clipped image.
Step 5: Next, to merge the 4 sub bands apply the Inverse DWT (IDWT) and a stego image is ready with similar size of the original image for further evaluation of the quality.



```
Embedding algorithm Process:
Input: Original image, secret message, secret key.
Output: Stegno image
Initial:
A= Load original image
B= Load mask image
C= Load synthesized image IDWT in L1, L2, and L3.
D= Load secret key 2n+1.
E= Stegno-synthesized image in L1, L2, and L3.
F= Put the result Stegno-synthesized image.
Step 1: Load original image and Decomposition DWT in A.
Step 2: Load mask image and Decomposition DWT in B.
Step 3: Find synthesized image IDWT in L1, L2, and L3 in C.
Step 4: Select location hide secret message from 2n+1 (secret key) in D.
Step 5: Embedding Secret message in side synthesized image (cover) in LSB using secret key
to Obtain Stegno-synthesized image for L1, L2, and L3 in E
Step 6: Result (Put the Stegno-synthesized image) in F.
End
```

Algorithm for Embedding Process



```
Input: Stegno Image
Output: Original Image, Message
Step1: Perform three level 2D-Haar DWT decomposition on the stego image as well the
cover image.
Step2: Process LL3 of the stego image and cover image block by block (4x4).
Step3: Assume an embedding coefficient of value of α= 0.05.
Step4: To get the image blocks of the secret image (4x4) following formula is used,
SI block = {LL3 intensity value of stego image – {(1- α) * LL3 intensity value of the CI}}/ α.
```

Algorithm for Extraction Process

V. PERFORMANCE METRICS

The quality of any stego image is evaluated based the PSNR and MSE. These two are considered as the performance metrics for any steganographic technique. Peak Signal to Noise Ratio PSNR (in dB) is defined in the following equation:

$$PSNR = 10\log_{10}\frac{255^2}{MSE}$$

The cumulative squared error between the compressed and the original image is defined by MSE and is denoted by the following equation.

$$MSE = \frac{\sum_{M,N} [I_1(m,n) - I_2(m,n)]^2}{M * N}$$

where M and N represents the number of rows and columns of the image respectively.

VI. RESULT AND DISCUSSION

All the results are simulated in matlab software 2014.This paper discusses the methodology for hiding data in Image DWT technique.

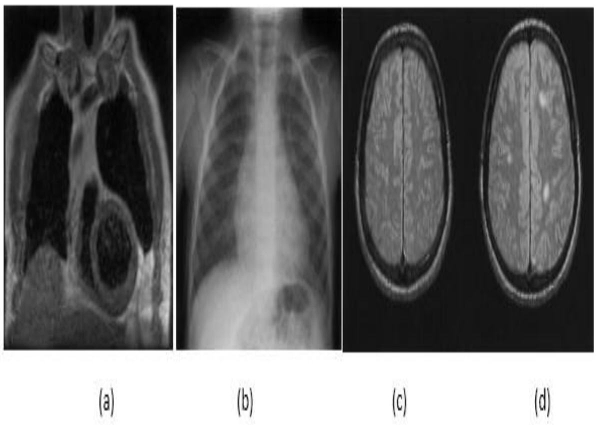
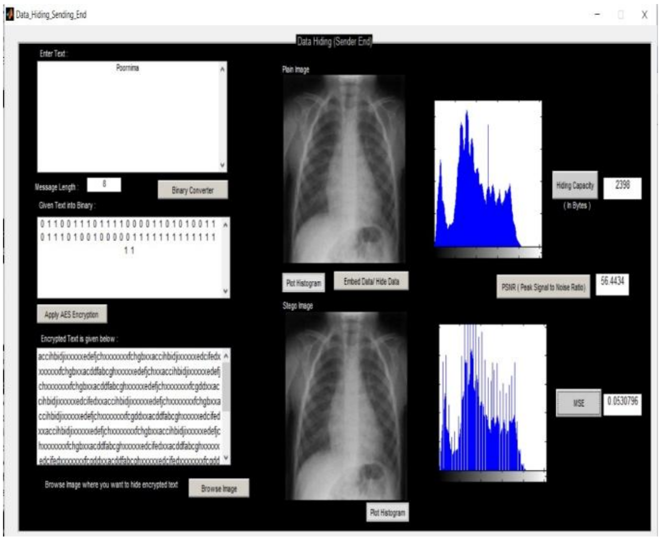


Fig 3: a)Lung1 b) Lung2 c) Brain

Table 1. PSNR and MSE values of different cover images

Image Name	PNSR before DWT	PNSR after DWT	Image Size	MSE after DWT
Lung1	22.197	56.444	800x752	0.053
Lung2	21.538	56.45	800x739	0.052
Brain	21.574	56.75	800x490	0.054
Brain1	21.344	56.09	225x225	0.127



Enter Text : Poornima

Message Length : 8

Given Text into Binary :

0 1 1 0 0 1 1 1 0 1 1 1 1 0 0 0 0 1 1 0 1 0 1 0 0 1 1
0 1 1 1 0 1 0 0 1 0 0 0 0 0 1 1 1 1 1 1 1 1 1 1 1 1 1
1 1

Encrypted Text is given below :

accihbidjixxxxxedefjchxxxxxxxfchgbxxaccihbidjixxxxxedcifedx
xxxxxxfchgbxxacddfabcghxxxxxedefjchxxaccihbidjixxxxxedefj
chxxxxxxxfchgbxxacddfabcghxxxxxedefjchxxxxxxxfcgddxxac
cihbidjixxxxxedcifedxxaccihbidjixxxxxedefjchxxxxxxxfchgbxxa
ccihbidjixxxxxedefjchxxxxxxxfcgddxxacddfabcghxxxxxedcifed
xxaccihbidjixxxxxedefjchxxxxxxxfchgbxxaccihbidjixxxxxedefjc
hxxxxxxxfchgbxxacddfabcghxxxxxedcifedxxacddfabcghxxxxx
edcifedxxxxxxxfcgddxxacddfabcghxxxxxedcifedxxxxxxxfcgdd

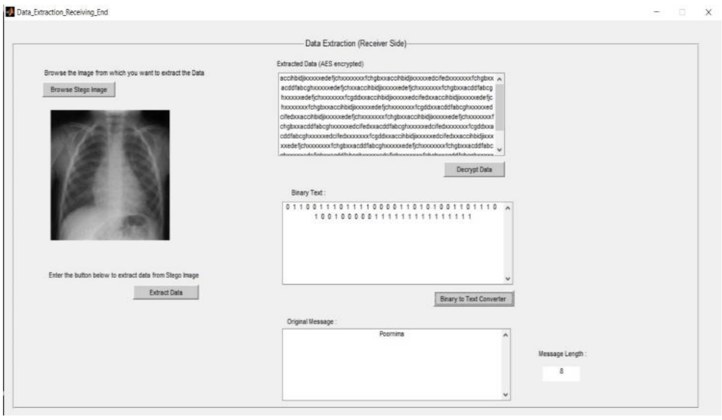
Browse Image where you want to hide encrypted text

Hiding Capacity (In Bytes): 2398

PSNR (Peak Signal to Noise Ratio): 56.4434

MSE: 0.0530796

Fig 4 : Data Embedding



Browse the Image from which you want to extract the Data

Extracted Data (AES encrypted)

accihbidjixxxxxedefjchxxxxxxxfchgbxxaccihbidjixxxxxedcifedxxxxxxxfchgbxx
acddfabcghxxxxxedefjchxxaccihbidjixxxxxedefjchxxxxxxxfchgbxxacddfabcg
hxxxxxedefjchxxxxxxxfcgddxxaccihbidjixxxxxedcifedxxaccihbidjixxxxxedefjc
hxxxxxxxfchgbxxaccihbidjixxxxxedefjchxxxxxxxfcgddxxacddfabcghxxxxxed
cifedxxaccihbidjixxxxxedefjchxxxxxxxfchgbxxaccihbidjixxxxxedefjchxxxxxxxf
chgbxxacddfabcghxxxxxedcifedxxacddfabcghxxxxxedcifedxxxxxxxfcgddxxa
cddfabcghxxxxxedcifedxxxxxxxfcgddxxaccihbidjixxxxxedcifedxxaccihbidjixxx
xxedefjchxxxxxxxfchgbxxacddfabcghxxxxxedefjchxxxxxxxfchgbxxacddfabc

Binary Text :

0 1 1 0 0 1 1 1 0 1 1 1 1 0 0 0 0 1 1 0 1 0 1 0 0 1 1 0 1 1 1 0
1 0 0 1 0 0 0 0 0 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1

Enter the button below to extract data from Stego Image

Original Message : Poornima

Message Length : 8

Fig 5: Data Extraction

VII. CONCLUSION

Steganography is used as one of the secure transmission technique to hide the secrets into different multimedia carriers and to conceal the presence of any private data in it. This paper proposes a new technique where both cryptography with enhanced AES algorithm and steganography with DWT is combined to give more security for transmission of data. The experimental work has accomplished DWT to exhibit robustness and effectiveness against any attacks. The proposed method adopts skin detection method to hide the confidential data into images making it perceptually invisible. Performance metrics such as PSNR and MSE are evaluated and tabulated to show the quality of the stego images. Different formats and size of images are to be explored by DWT technique.

ACKNOWLEDGMENT

This research is supported by Visvesvaraya Technological University Jnana Sangama ,Belagavi -590018 for grant of financial assistance.

REFERENCES

1. N.F. Johnson and S. Katzenbeisser, “A survey of steganography techniques,” in S. Katzenbeisser and F. Peticolas (Eds): Information Hiding, pp.43-78, Artech House, Norwood, MA, 2000
2. MAB. Younes, A. Jantan, “Image Encryption using Block-Based Transformation Algorithm,” International Journal of Computer Science, vol. 35, issue 1, pp.15-23, 2008.
3. M.M. Amin, M. Salleh, S. Ibrahim and M.Z.I. Shamsuddin, “Information hiding using Steganography,” National Conference on Telecommunication Technology, pp.21-25, 2003
4. Po-Yueh Chen, Hung-Ju Lin, A DWT Based Approach for Image Steganography, International Journal of Applied Science and Engineering, 2006. 4, 3: 275-290
5. Chan, C.K., Chang, L.M., “Hiding data in image by simple LSB substitution,” Pattern Recognition, vol 37, pp.469-471, 2003
6. Chang, C.C, Tseng, H.W., “A Steganographic method for digital images using side match,” Pattern Recognition, vol. 25, pp.1431-1437, 2004
7. I. Khalil, A. Ibaida “Wavelet Based ECG Steganography for Protecting Patient Confidential Information in Point-of-Care Systems”, IEEE Trans. Of Biomed. Eng., vol. 60, pp. 3322-3330, Dec. 2013.
8. S.Athani, S. Ghaemmaghami, “Colour Image Steganography Method Based on Sparse Representation”, IET Image Process, vol. 9, pp. 496-505, 2015.
9. Sharma V.K., Mathur P., Srivastava D.K. (2019) Highly Secure DWT Steganography Scheme for Encrypted Data Hiding. In: Satapathy S., Joshi A. (Eds) Information and Communication Technology for Intelligent Systems. Smart Innovation, Systems and Technologies, vol 106. Springer, Singapore.

Retrieval Number: C8730019320/2020©BEIESP
DOI: 10.35940/ijitee.C8730.019320
Journal Website: www.ijitee.org

Published By:
Blue Eyes Intelligence Engineering
& Sciences Publication

10. P. K. Dave and H. J. Patel, “Least Significant Bits Based Steganography Technique,” in Proc. IJECCE 2012, vol. 3, pp. 97- 103.
11. Hamad A. A, Ali A, Majid A. A, Waleed A, “High Capacity Image Steganography Based on Haar DWT for Hiding Miscellaneous Data”, IEEE Jordan Conf. on Applied Electrical Eng. and Comp. Tech., March 2015
12. Stuti Goel, Arun Rana, Manpreet Kaur,” A Review of Comparison Techniques of Image Steganography”. IOSR Journal of Electrical and Electronics Engineering (IOSR-JEEE) e-ISSN: 2278-1676, ISSN: 2320-3331, Volume 6, Issue 1 (May. - Jun. 2013), PP 41-48.
13. Anderson RJ, Petitcolas FAP (1998) On the limits of steganography. IEEE J Sel Areas Commun 16(4): 474-481.
14. J. Fridrich, Application of data hiding in digital images, Tutorial for the ISSPA’99, Brisbane, Australia, August 22-25 1999.
15. Bailey K, Curran K (2006)” An evaluation of image based steganography methods. Multimedia Tools Appl” 30(1):55–88.

AUTHORS PROFILE

MANJULA G. received her B.E degree in Computer Science & Engg from Bangalore University in 2001 and M. Tech degree in computer science from Visveswaraya Technological University, Belgaum, India in 2010 .She is currently pursuing Ph.D. in the Department of Information Science and Engineering of SJB Institute of Technology, Bangalore, India. Her professional membership includes ISTE and IAENG. She was working as Associate Professor in the Department of ISE in SJB Institute of Technology, Bangalore, India. Her area of interest are information security, DBMS, and Computer Networks.

Dr. MOHAN. H. S received the M.Tech degree in computer science from Visveswaraya Technological University, Belgaum, India in 2004 and Ph.D. degree from Dr. MGR University, Chennai, India in 2012. He is currently working as professor and head of department of ISE in SJB Institute of Technology, Bangalore, India. His professional membership includes CSI, ISTE, IEEE and IAENG. He is a reviewer for IJCSIS, IJSCAI, VLSICS and IJWSC intemational journals. His area of interests are Information and Network Security, and Applied Cryptography.