

# Application of Steganography in Image Processing Framework

Arpitha K Shetty 1, Dr. Usha Desai 2, Ganesh Shetty 3, Pratheksha Rai N 4

1,2,3,4 Electronics and Communication Engineering Department, 1,2,3,4 Visvesvaraya Technological University

Address

1 [shettyarpitha6@gmail.com](mailto:shettyarpitha6@gmail.com)

Assistant Professor

A.J Institute Of Engineering & Technology. Mangaluru, Karnataka, India

2 [usha.nmamit@nitte.edu.in](mailto:usha.nmamit@nitte.edu.in)

Associate Professor

NMAMIT, Nitte, Udupi, Karnataka, India

3 [ganeshshetty27@gmail.com](mailto:ganeshshetty27@gmail.com)

Assistant Professor

Shri Madhwa Vadiraja Institute of Technology and Management, Udupi, Karnataka, India

4 [pratheerai@gmail.com](mailto:pratheerai@gmail.com)

Assistant Professor

A.J Institute Of Engineering & Technology. Mangaluru, Karnataka, India

**Abstract**— Steganography is the art of hiding the fact that communication is taking place, by hiding information in other information. Different applications have different requirements of the steganography techniques applied. For example, some applications may require absolute invisibility of the secret information, while others require a larger secret message to be hidden. This paper intends to give an overview of image steganography, its uses and techniques. It also attempts to identify the requirements of a good stenographic algorithm and briefly reflects on which stenographic techniques are more suitable for which applications.

**Keywords**— Steganography, PSNR, DWT, Transform domain, Palette based images

## I. INTRODUCTION

Steganography is an emerging area which is used for secured data transmission over any public media. Since the increased application of Internet, in the field of information technology and communication has been the security of information. It is sometimes not enough to keep the contents of a message secret, it may also be necessary to keep the existence of the message secret. The technique used to implement this, is called steganography. Steganography is a process that involves hiding a message in an appropriate

carrier like image or audio. Many different carrier file formats can be used, but digital images are the most popular because of their frequency on the Internet. For hiding secret information in images, there exists a large variety of stenographic techniques, which are more complex than others and all of them have respective strong and weak points.

## II. DIFFERENT KINDS OF STEGANOGRAPHY

Almost all digital file formats can be used for steganography, but the formats that are more suitable are those with a high degree of redundancy. Image and audio files especially comply with this requirement, while research has also uncovered other file formats that can be used for information hiding. Different file formats for steganography are based on the text, images, audio, video and protocol applications.

A. Image steganography is further classified into image domain and transform domain techniques.

- 1) *Image Domain*: In which the Least Significant Bit (LSB) will be in the Bit Map (BMP) file format. In which, LSB insertion is a common, simple approach for embedding the information in a cover image. The LSB of some or all of the bytes inside an image is changed to a bit of the secret message. Using a 24-bit image, a bit of each of the red, green and



Principal

SHRI MADHWA VADIRAJA  
INSTITUTE OF TECHNOLOGY & MANAGEMENT  
Vishwothama Nagar, Udupi Dist.  
BANTAKAL - 574 115

blue colour components can be used, since they are each represented by a byte. In other words, one can store 3 bits in each pixel. Since there are 256 possible intensities of each primary colour, changing the LSB of a pixel results in small changes in the intensity of the colours. These changes cannot be perceived by the human eye - thus the message is successfully hidden. *LSB and Palette Based Images*, for example *Graphics Interchange Format (GIF)* images, are another popular image file format commonly used on the Internet. GIF images are indexed images where the colours used in the image are stored in a palette, sometimes referred to as a colour lookup table. Each pixel is represented as a single byte and the pixel data is an index to the colour palette. The colours of the palette are typically ordered from the most used colour to the least used colours to reduce lookup time.

- 2) *Transform Domain*: It is also known as *JPEG steganography*, which is the JPEG compression, in which the colour data is down sampled to reduce the size of the file. The colour components (U and V color space) are halved in horizontal and vertical directions, thus decreasing the file size by a factor of 2. For JPEG, the Discrete Cosine Transform (DCT) or Discrete Fourier Transform (DFT) is used. These mathematical transforms convert the pixels in such a way as to give the effect of "spreading" the location of the pixel values over part of the image. The DCT transforms a signal form of an image representation into a frequency representation, by grouping the pixels into  $8 \times 8$  pixel blocks and transforming the pixel blocks into 64 DCT coefficients each. A modification of a single DCT coefficient will affect all 64 image pixels in that block. The next step is the quantization phase of the compression. JPEG divides all the values in a block by a quantization coefficient. The results are rounded to integer values and the coefficients are encoded using Huffman coding to further reduce the size.

### III. RELATED WORK

Alam and Islam [1] in 2013 proposed SDS (Sieve Division Shuffle) and Medical Imaging techniques to compare the accuracy of the transmitted data and efficiently authenticate the sender SDS. The observation was that Peak Signal to Noise Ratio performance is not very much good and not effective for standard datasets.

Geetha, et al [7] in 2013 implemented Edge Detection Method using Gaussian filter, dimensional convolution filter, Multiple Error Replacement, Variable Embedding Ratio. This work provides good visual qualities and highest embedding capacity with high security.

Jose and Abraham [7] applied Image Encryption, Chaotic sequence, and pseudorandom number steganographic techniques to provide higher data hiding capacity.

Kadam, et al., [6] in 2013 employed AES(Advanced Encryption Standard) 128 bit key, 32-bit words, 128-bit cipher key to prevent transformation of secret file from third party access. The paper also showed the increased data security level where keys of decryption process is protected from the hackers. The limitation of the work was that memory required for implementation should be as small as possible.

Mahato, et al., [6] in 2013 used HTML attributes and Stegno-crypto techniques. It was found that steganography is achieved easily by HTML as HTML is rich in code and there is very less chance to check its source code and can be easily communicated through internet. The limitation of the work was increase in the complexity of the algorithm and also the secret message could not be extracted.

Ramaiya, et al., [4] applied employed different steganographic methods to provide high level of and showed that variation in two LSB of each pixel will not affect the cover image quality.

Samidha and Agrawal [8] in their paper used LSB, Raster Scan, Random Scan, Layout Management and Spatial Domain techniques to show that Pixels can be used to hide data. The paper also proved that this technique can be extended at any place in image using any dimension of any shape.

Thenmozhi and Chandrasekaran [3] in 2013 employed 2-D DWT,  $M \times N$  size cover image, and Henon Map to ensure high capacity and good invisibility of the hidden data. The secret message could not be extracted and also removes the outlines of the encrypted images completely.

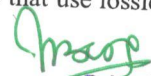
There are various research conducted [9] - [17] to study transformation techniques. This paper gives framework for using steganography in image processing applications.

## IV METHODOLOGY

### A Image Compression

In order to display an image in a reasonable amount of time, techniques must be incorporated to reduce the image's file size. These techniques make use of mathematical formulas to analyse and condense image data, resulting in smaller file sizes. This process is called compression. Lossy compression creates smaller files by discarding excess image data from the original image. It removes details that are too small for the human eye to differentiate, resulting in close approximations of the original image, although not an exact duplicate. An example of an image format that uses this compression technique is JPEG (Joint Photographic Experts Group).

Lossless compression represents data in mathematical formulas. The original image's integrity is maintained and the decompressed image output is bit-by-bit identical to the original image input. The most popular image formats that use lossless compression is GIF (Graphical

  
Principal

SHRI MADHWA VADIRAJA  
INSTITUTE OF TECHNOLOGY & MANAGEMENT  
Vishwothama Nagar, Udipi Dist.  
BANTAKAL - 574 115



Interchange Format) and 8-bit BMP (a Microsoft Windows bitmap file).

### B Discrete Wavelet Transform

DWT decomposes images into four sub bands: LL, HL, LH and HH. LL part contains the most significant features. So if the information is hidden in LL part the stego image can withstand compression or other manipulations. But sometimes distortion may be produced in the stego image and then other sub bands can be used. The decomposition of Lena image by 2 levels of 2D - DWT is shown in Fig. 1.

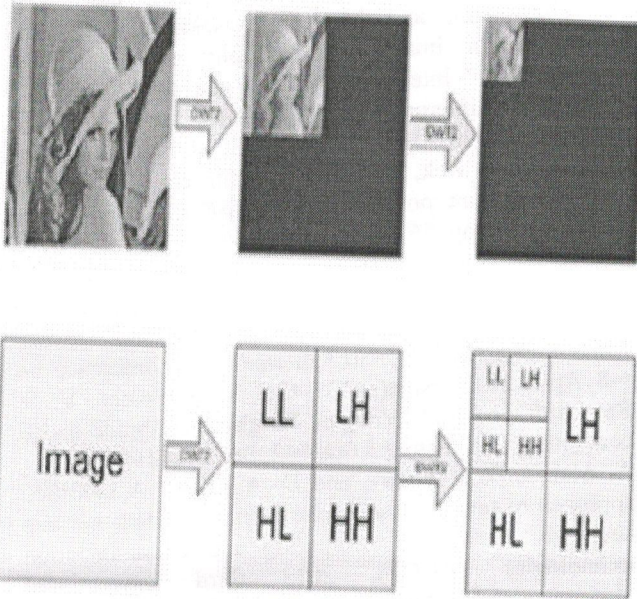


Fig 1: Levels of decomposition using 2D-DWT

### C Integer Wavelet Transform

IWT is a more efficient approach to lossless compression. The coefficients in this transform are represented by finite precision numbers which allows for lossless encoding. This wavelet transform maps integers to integers and output can be completely characterized with integers. The LL sub-band in the case of IWT appears to be a close copy with smaller scale of the original image while in the case of DWT the resulting LL sub-band is distorted slightly, as shown in Fig. 2.

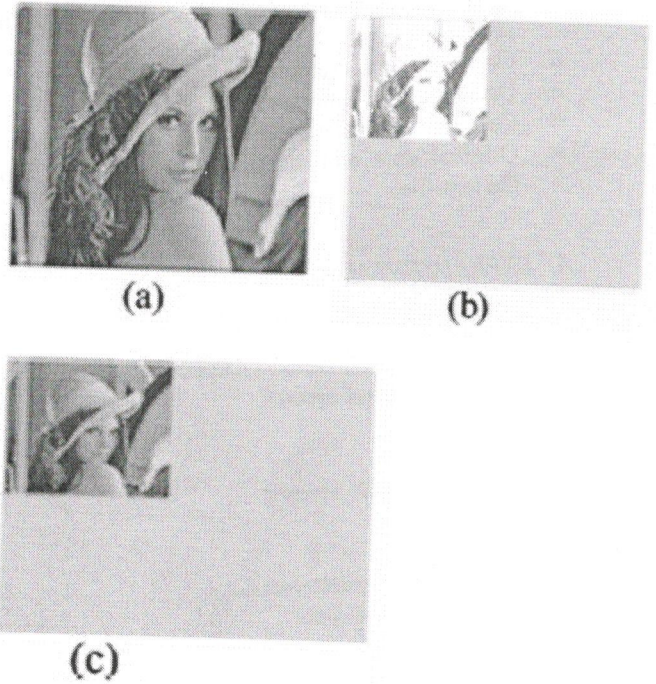


Fig 2: (a) Original image (b) One level DWT in sub band LL (c) One level IWT in sub-band LL.


### V PROPOSED WORK

A message is embedded in a digital image (cover image) through an embedding algorithm, with the help of a secret key. The resulting stego image is transmitted over a channel to the receiver where it is processed by the extraction algorithm using the same key. During transmission the stego image, it can be monitored by unauthenticated viewers who will only notice the transmission of an image without discovering the existence of the hidden message. The LSB insertion embeds the message in the least significant bit of some selected pixels of the cover image.

The steps for embedding data inside the image are as follows:

- i. obtain the username and password for the user of the system
- ii. Retrieve the cover image, secret message and secret key for steganography.
- iii. Convert the message to text file
- iv. Convert the resulting file into digital code format
- v. Convert the key into digital code format
- vi. Encode the message into binary code
- vii. Pre-define the bits per unit for encoding.
- viii. The resultant image is a stenographic image.

The steps for extracting data from stego image are as

  
 Principal  
 SHRI MADHWA VADIRAJA  
 INSTITUTE OF TECHNOLOGY & MANAGEMENT  
 Vishwothama Nagar, Udupi Dist.  
 BANTAKAL - 574 115



follows:

- i. Read the input steganographic image and the secret key
- ii. Compare the secret key for verification
- iii. Decode all the binary codes obtained.
- iv. Convert the binary code to a zipped text file
- v. Original data embedded can be obtained from the text file.

#### A. EXPERIMENTAL RESULTS OBTAINED

```
Command Window
New to MATLAB? Watch this Video, see Demos, or read Getting Started.
data that can be embedded(in bytes)=
9
data that can be embedded(in bytes)=
9
Displaying the contourlet coefficients...
[256x256 double] (1x2 cell)
encoded msg as:
hi hellos
Displaying the reconstructed image...
It should be a perfect reconstruction
Decoded msg is:
hi hellos
snr
-92.4477
>>
```

PSNR is a standard measurement used in steganography technique in order to test the quality of the stego images. The higher the value of PSNR, the more quality the stego image will have.

The image file format used in proposed algorithm is focused on bitmap (BMP) format. The BMP file format handles graphics files within the Microsoft Windows OS. Typically, BMP files are uncompressed, hence they are large. The advantage of using BMP files is the simplicity and wide acceptance of BMP files in Windows programs. Since BMP image has a relatively larger size, the pixels in image are relatively larger as well. Thus, it provides more space for binary codes to be encoded within it.

#### VI. CONCLUSION

This paper proposed a new steganography algorithm with 2 layers of security. A system named SIS (Steganography Imaging System) has been developed using the proposed algorithm. Thus for an agent to decide on which steganographic algorithm to use, he would have to decide on the type of application he want to use the algorithm for and if he is willing to compromise on some features to ensure the security of others. SIS can be used by various

users who want to hide the data inside the image without revealing the data to other parties. SIS maintains privacy, confidentiality and accuracy of the data.

#### ACKNOWLEDGMENT

We thank the Principal and Management of AJ Institute of Engineering and Technology for support.

#### REFERENCES

- [1] F. I Alam, and M. M Islam, "An investigation into image hiding steganography with digital signature framework," Informatics, Electronics & Vision (ICIEV), 2013 international conference on 17-18 May 2013, page(s):1-6.
- [2] S. Thenmozhi, and M. Chandrasekaran, "A novel technique for image steganography using nonlinear chaotic map," Intelligent systems and control (ISCO), 2013 7th international conference on 4-5 Jan. 2013, page(s):307-311. S. Zhang, C. Zhu, J. K. O. Sin, and P. K. T. Mok, "A novel ultrathin elevated channel low-temperature poly-Si TFT," *IEEE Electron Device Lett.*, vol. 20, pp. 569-571, Nov. 1999.
- [3] M. K Ramaiya, N. Hemrajani, and A. K Saxena, "Improvisation of security aspect in steganography applying DES," Communication systems and network technologies (CSNT), 2013 international conference on 6-8 April 2013, page(s):431-436. R. E. Sorace, V. S. Reinhardt, and S. A. Vaughn, "High-speed digital-to-RF converter," U.S. Patent 5 668 842, Sept. 16, 1997.
- [4] S. Mahato, D. K Yadav, and D. A Khan, "A modified approach to text steganography using hypertext markup language," Advanced computing and communication technologies (ACCT), 2013 third international conference on 6-7 April 2013, page(s):40-44.
- [5] R. Jose, and G. Abraham, "A separable reversible data hiding in encrypted image with improved performance," Emerging research areas and 2013 international conference on microelectronics, communications and renewable energy (AICERA/ICMiCR), 2013 annual international conference on 4-6 June 2013, page(s):1-5.
- [6] P. Kadam, A. Kandhare, M. Nawale, and M. Patil, "Separable reversible encrypted data hiding in encrypted image using AES algorithm and lossy technique," Pattern recognition, Informatics and medical engineering (PRIME), 2013 international conference on 21-22 Feb. 2013, page(s):312-316. A. Karnik, "Performance of TCP congestion control with rate feedback: TCP/ABR and rate adaptive TCP/IP," M. Eng. thesis, Indian Institute of Science, Bangalore, India, Jan. 1999.
- [7] C.R. Geetha, S. Basavaraju, and Dr. C. Puttamadappa, "Variable load image steganography using multiple edge detection and minimum error replacement method," Information & communication technologies (ICT), 2013 IEEE conference on 11-12 April 2013, page(s):53-58. *Wireless LAN Medium Access*



Principal  
SHRI MADHWA VADIRAJA  
INSTITUTE OF TECHNOLOGY & MANAGEMENT  
Vishwathama Nagar, Udipi Dist.  
BANTAKAL - 574 115

*Control (MAC) and Physical Layer (PHY) Specification*,  
IEEE Std. 802.11, 1997.

- [8] Dr. D. Samidha, and D. Agrawal, "Random image steganography in spatial domain," Emerging trends in VLSI, embedded system, nano electronics and telecommunication system (ICEVENT), 2013 international conference on 7-9 Jan. 2013, page(s):1-3.
- [9] Desai, Usha, et al. "Diagnosis of multiclass tachycardia beats using recurrence quantification analysis and ensemble classifiers." *Journal of Mechanics in Medicine and Biology* 16.01 (2016): 1640005.
- [10] Desai, Usha, et al. "Machine intelligent diagnosis of ECG for arrhythmia classification using DWT, ICA and SVM techniques." *2015 Annual IEEE India Conference (INDICON)*. IEEE, 2015.
- [11] Desai, Usha, et al. "Decision support system for arrhythmia beats using ECG signals with DCT, DWT and EMD methods: a comparative study." *Journal of Mechanics in Medicine and Biology* 16.01 (2016): 1640012.
- [12] Desai, Usha, C. Gurudas Nayak, and G. Seshikala. "Application of ensemble classifiers in accurate diagnosis of myocardial ischemia conditions." *Progress in Artificial Intelligence* 6.3 (2017): 245-253.
- [13] Gurupur, Varadraj P., et al. "Analysing the power of deep learning techniques over the traditional methods using medicare utilisation and provider data." *Journal of Experimental & Theoretical Artificial Intelligence* 31.1 (2019): 99-115.
- [14] Gurupur, Varadraj P., et al. "Analysing the power of deep learning techniques over the traditional methods using medicare utilisation and provider data." *Journal of Experimental & Theoretical Artificial Intelligence* 31.1 (2019): 99-115.
- [15] Desai, Usha, C. Gurudas Nayak, and G. Seshikala. "An application of EMD technique in detection of tachycardia beats." *2016 International Conference on Communication and Signal Processing (ICCSP)*. IEEE, 2016.
- [16] Desai, Usha, C. Gurudas Nayak, and G. Seshikala. "An efficient technique for automated diagnosis of cardiac rhythms using electrocardiogram." *2016 IEEE International Conference on Recent Trends in Electronics, Information & Communication Technology (RTEICT)*. IEEE, 2016.
- [17] Desai, Usha. "Automated detection of cardiac health condition using linear techniques." *2017 2nd IEEE International Conference on Recent Trends in Electronics, Information & Communication Technology (RTEICT)*. IEEE, 2017.



Principal

SHRI MADHVA VADIRAJA  
INSTITUTE OF TECHNOLOGY & MANAGEMENT  
Vishwothama Nagar, Udupi Dist.  
BANTAKAL - 574 115