ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 4, Issue 8, August 2015

Implementation of Watermarking Technique for Secured Transmission

Ms. Nidhi Bux[1], Prof. K. J. Satao[2]

M.Tech Scholar, Computer Science and Engineering, Rungta College of Engineering & Technology,

Kohka - Kurud Road, Bhilai, Chhattisgarh, India[1]

Professor, Computer Science and Engineering, Head, Department of Information Technology,

Rungta College of Engineering & Technology, Kohka - Kurud Road, Bhilai, Chhattisgarh, India[2]

Abstract: In this paper we proposed an approach which is a combination of Steganography technique and Watermarking. Steganography technologies play an important role of security and privacy, through which the sense of security for hiding information into another information becomes more influential. Watermarking technology is also very useful due to its importance in detection and prosecution of software pirates and digital thieves and also for copyright protection of images.The basic idea of this approach is that it will transfer an image by hiding it into another image with the help of watermarking technique and we are also using spatial domain LSB technique for security purpose.

Keywords: Steganography, Watermarking, LSB.

I. INTRODUCTION

In this paper we proposed an approach in which an image is being transferred and secured by the technique of steganography and watermarking so as to protect the data more easily. A combination of steganography and watermarking provides us a better security for transmission. This approach will limit the distortion which might occur in an image while processing. Another advantage of this approach is that we are embedding a text watermark in our original image and that text watermark is converted in the form of an image for making our original image secure.

II. STEGANOGRAPHY

Steganography is data hidden within data. It is an art and science of communicating in such a way which hides the existence of communication [1], [6].The main methodologies used in steganography system are the cover image, a secret message, a secret key and an embedding algorithm. In the steganography scenario sender has to select a carrier media for sending message like an image file, audio file, video or any text file [14]. The cover image which is used as a carrier can be image, an audio, video file in which the secret message is hidden; the secret key is usually used to transfer the secret message according to the hidden technique or the algorithm. The algorithm which is used for embedding the secret message or image is the way we want to embed it in the cover image and how efficiently that embedding algorithm will hide the secret message in cover image.

TYPES OF STEGANOGRAPHY:

1. Text

2. Image

3. Audio

4. Video

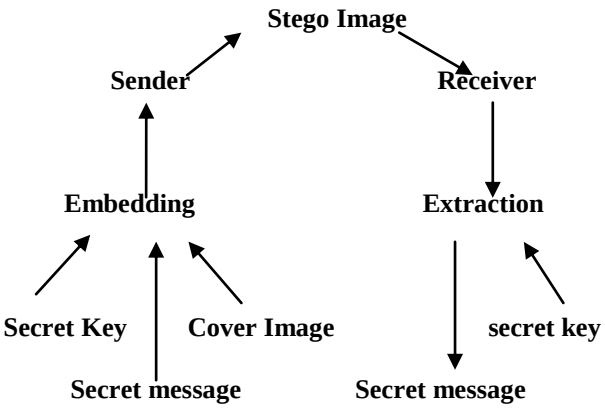

Figure 1.Basic Steganography Scenario

These four categories of file format are used in steganography for hiding purpose; the most popular hiding technique is image format because hiding information in an image with a secret message can easily be posted over the Internet [8]. There are many different methods to hide information inside an image by encoding each bit of information and embed the message in a noisy area for drawing less attention.

III.DIGITAL WATERMARKING

Digital watermarking is a process of embedding information in the digital media and hides it in such a way that it is invisible from its users [13]. We can hide it into a multimedia object so that watermark cannot be detected or extracted from that object [8].

Watermarking is a very popular technique which is used in steganography. In this approach we mainly focus on watermarking technique for applying a text as a watermark which is converted into an image and embed it to the secret image after which we apply a gaussian noise

ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 4, Issue 8, August 2015

to it for security purpose and then it is ready to transmit it to the receiver end [16]. There are two types of watermark:-

1. Visible Watermark
2. Invisible Watermark

1. Visible Watermark:-In visible watermark data is visible in the image or video, it is usually used as a company logo which means that the information in a company logo represents the owner of the media [16]. Most of the television channels have their own logo which means information on a specified channel is safe and no one can use their logo without the channel permission.

2. Invisible Watermark :- In invisible watermarking information is embedded into a digital media object in the form of image, video, audio and text format & that object is known as **invisible watermark.** Its appearance is same as the original image nobody can identify that anything is hidden in that image [8]. The most important advantage of "invisible watermark" is copyright protection.

EMBEDDING & DETECTING PROCESS OF WATERMARKING

In embedding watermark in an image it needs a watermark or a logo, a cover object and a secret key. The secret key is of two types first a Symmetric Key in which sender and receiver both are having the same key and second an Asymmetric Key in which the sender is having a different key and the receiver is having a different key, we can use any one of the keys for security purpose and during transmission nobody knows that anything is hidden in that image because it will appear like the original image [3]. The figure below shows the embedding process.

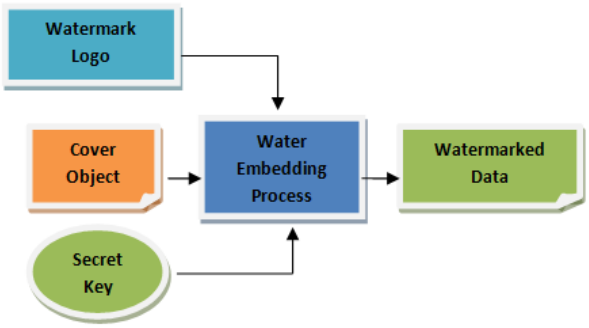

Figure 2.Watermark Embedding Process

The figure below shows the detecting process:-

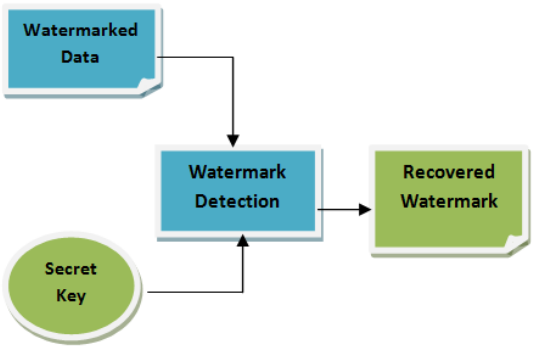

Figure 3.Watermark Detection Process

IV.LEAST SIGNIFICANT BIT (LSB)

Least Significant Bit substitution is the most popular and simple technique for steganography and is an easy approach for changing bits in image an [2].There are many algorithms available for digital watermarking but the simplest algorithm is Least Significant Bit insertion method. The primary concept of LSB is to conceal few or all bits inside an image that are replaced with bits of secret message [8].

V.SPATIAL DOMAIN TECHNIQUE

In our proposed methodology we are using Spatial Domain Technique because it deals with the image pixels values which are manipulated to achieve enhancement [3], [17]. Spatial Domain Technique is based on direct manipulation of the image pixels and are useful for embedding each pixel of gray level values of an image [9].The degradation of the original image is not easy and hiding capacity is more i.e. more information can be stored in an image because spatial domain refer to the image plane itself and are based on direct manipulation of pixels in an image [3].

Spatial domain process is denoted by the expressions:-

$$g(x,y) = T[f(x,y)] \quad \text{.....(1)}$$

where f(x, y) is input image, g(x, y) is processed image and T is a gray level transformation function of the form

$$s = T(r) \quad \text{..... (2)}$$

where r and s denote the gray level of f(x, y) an g(x, y) at any point (x, y) as shown in the figure below:-

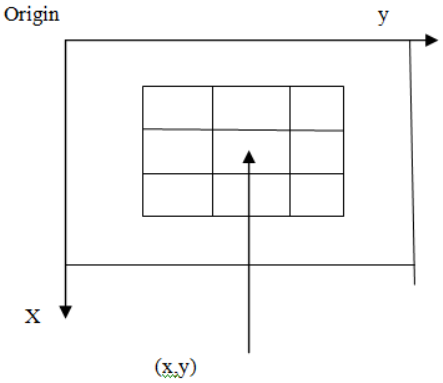

Figure 4. 3 X 3 neighborhood about a point (x,y) in an image

VI.PROPOSED METHODOLOGY

The proposed methodology works on steganography, watermarking, and LSB technique to encrypt secret image or message. Following steps show how our methodology works.

In the layout of our methodology there are six different parts of modules which are designed and coded in MATLAB.
The first three modules will work for sender side modules and last three will work for receiver sides modules which are as follows:-

ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 4, Issue 8, August 2015

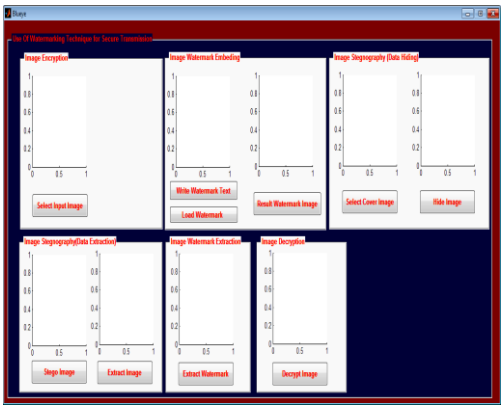

Figure 5. Layout of Proposed Methodology

A. **Sender Side Modules**
1. Image Encryption.
2. Image Watermark Embedding.
3. Image Steganography (Data Hiding).

B**. Receiver Side Modules**
1. Image Steganography (Data Extraction).
2. Image Watermark Extraction.
3. Image Decryption.

A.SENDER SIDE

1. IMAGE ENCRYPTION

In Image Encryption module first we select an input image or an original image which we are going to transmit to the receiver side. This input image can be in any format like .jpeg, .bmp or .png image as shown in the layout below:-

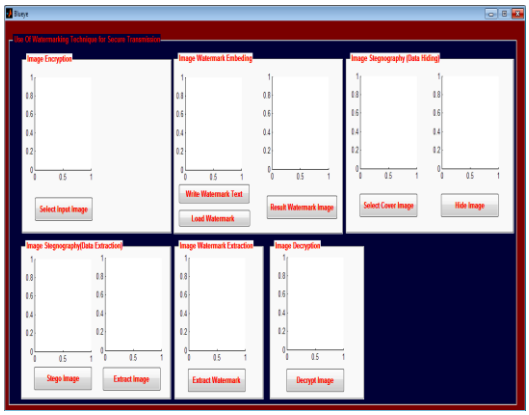

Figure 6.Select input image

Select input image by clicking on **select input image button.**

Figure7. Select a .jpg image

It will appear like this when we select our secret image; it is a .jpg image of Bill Gates.

Figure 8.Input image is selected

2. IMAGE WATERMARK EMBEDDING

Image Watermark Embedding is that module which comes after image encryption module or after selecting an input image. In this module we embed watermark into it, which is an invisible watermark or a text or we can say that it is our secret message or watermark text by selecting "write watermark text" button as shown in the figure above:-

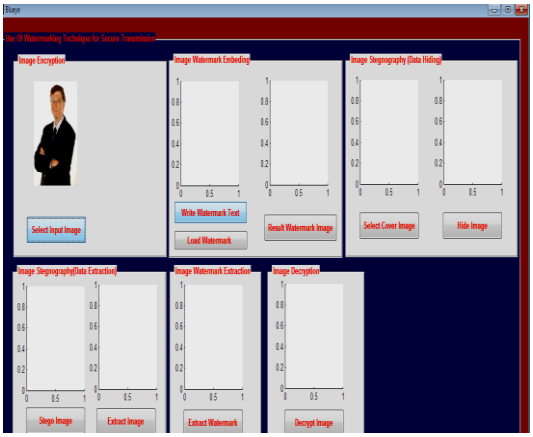

Figure 9.Select Write Watermark Text button

As we click on the **write watermark text** button a box will appear named as **Text to Image conversion** in which we have to write our secret message or watermark text as shown in the figure below:-

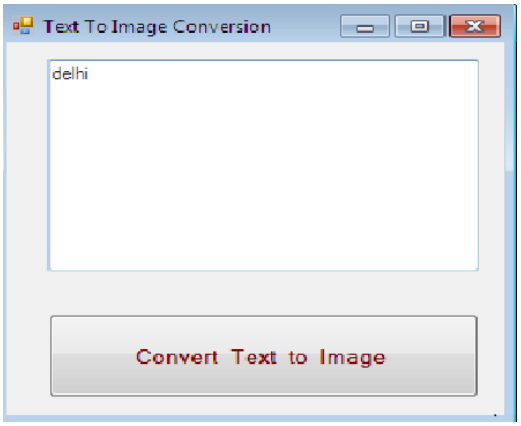

Figure 10.Text to Image Conversion

ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 4, Issue 8, August 2015

Then click on **Convert Text to Image button.** It will convert the text into an image, so no one inspect the existence of any type of message. After writing secret message or watermark text we click on **Load watermark button** with the help of this the text which is converted into image is loaded into the input image and at that time we apply LSB technique to it for more security purpose.

We have change last 1 bit of the input image by reading the cover image and secret image that is a RGB image into 256 gray scale values. After that we generate watermark into it, by setting LSB value of input image by the MSB value of the cover image and also calculating the height and weight of both the input image or the cover image ,so that the values that are changing can be settle down according to the size of the images.

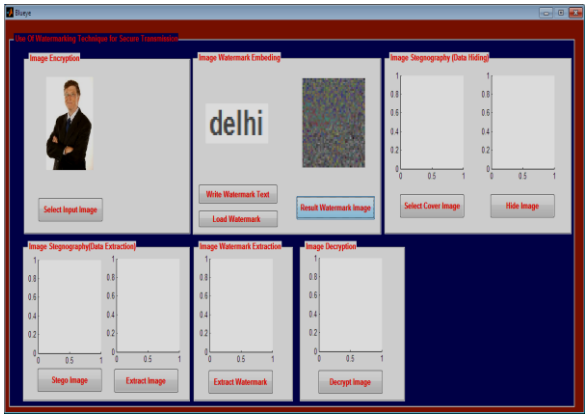

Figure 11.LSB substitution Technique

After we get the resultant watermarked image then in that image we apply noise to it, to make more secure, we are applying gaussion noise to it.

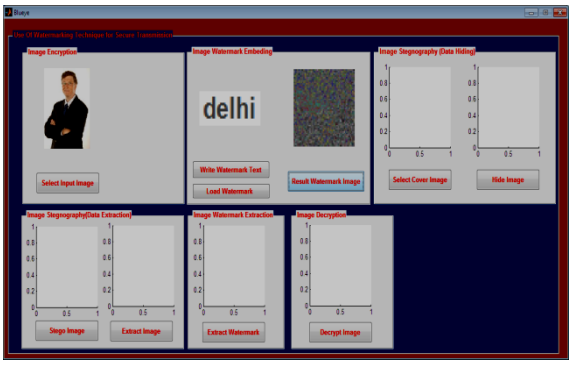

Figure 12.Resultant Watermarked image with noise

3 .IMAGE STEGANOGRAPHY (Data Hiding)

Steganography is a technique to hide information from the observer to establish invisible communication. In steganography system it consists of a cover image which helps the secret message to hide into it from its existence. Image steganography is one of its type in which we can hide our secret messages and transmit it to the Internet or to the receiver side.

In this module of Image Steganography or Data Hiding we have to choose a cover image, it can be any image of any format like .jpg, .png or .bmp type because we have to hide our secret image or resultant watermarked image into the cover image. It can be done by clicking the "**select cover image button**". In this methodology we have taken a .png image because png image is safer than any other image format.

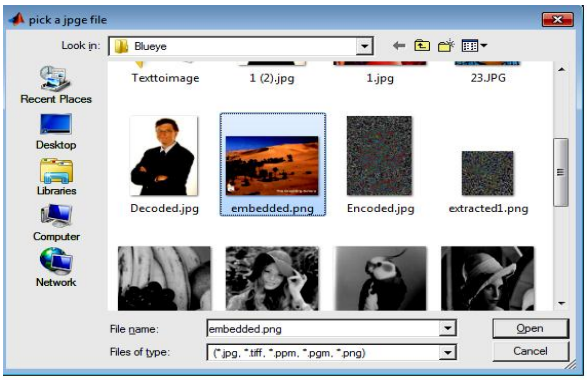

Figure 13.Selecting a cover image for hiding

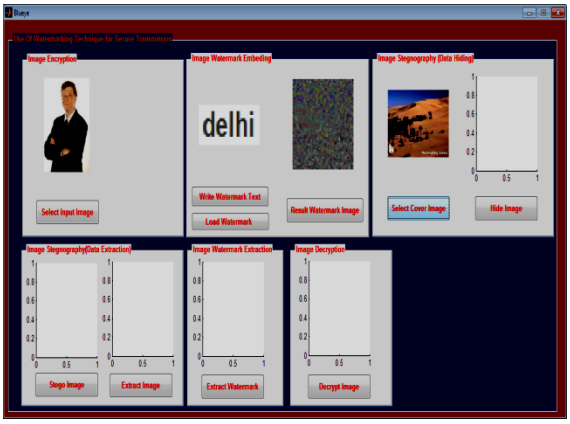

Figure 14.Cover image for hiding

Now comes the main part that is hiding part which plays an important role in our methodology, in this part we hide the "resultant watermark image" into the cover image which we have chosen yet and it can be done by clicking the **"Hide Image Button",** the function of this button "hide image" is that it will first read the message image or cover image and then open both the message image or cover image after that it will embed some bits of message image into cover image then only the bits that are embedded in the cover image must shift from LSBs to MSBs and lastly embed zero bits to the cover image to make it a **"stego image"** and save this file as "stego image".

Stego image is that image in steganography in which we can hide our secret messages or image into another image i.e. cover image when both the image are combine together or hide into one another with the help of some coding then the resultant image is known as "stego image".

This "Stego image" is now transmit to the receiver side which looks like the cover image only, because the purpose of using this cover image is that its appearance which does not represent or existence any message into it.

It will appear like this;-

ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 4, Issue 8, August 2015

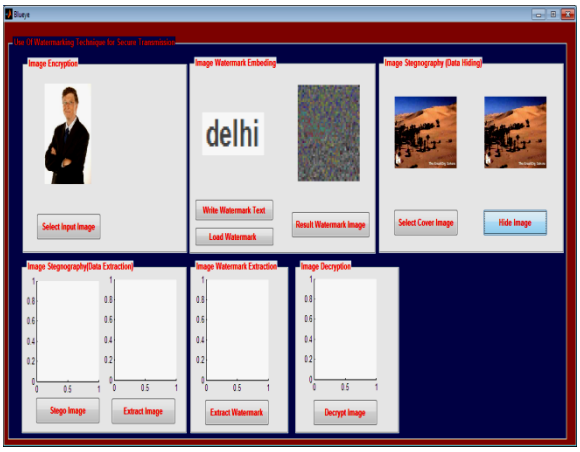

Figure 15.Hidden Image

Now the sender part or module is finished lastly it will only transmit the hidden image to the receiver side.

B.RECEIVER SIDE

1. IMAGE STEGANOGRAPHY (Data Extraction)

In this section of Image Steganography or Data Extraction part we are going to extract the hidden data which is covered under a cover image and which is send or transmitted by the sender side and it is known as **"stego image".** We can get this stego image by clicking on **"Stego image"** button which will appear like this:-

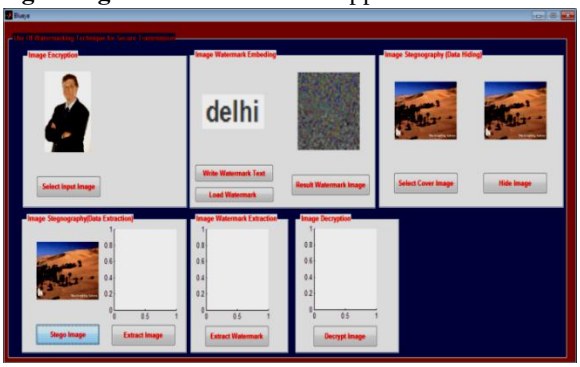

Figure16. Image Steganography (Data Extraction)

After receiving the stego image from the sender side now we have to extract the hidden data or secret message or image from it by clicking the **"Extract Image button"** from this with the help of coding we are able to extract secret data from the cover image and we get our watermarked image. Through this code we can get extract our watermarked image from stego image.

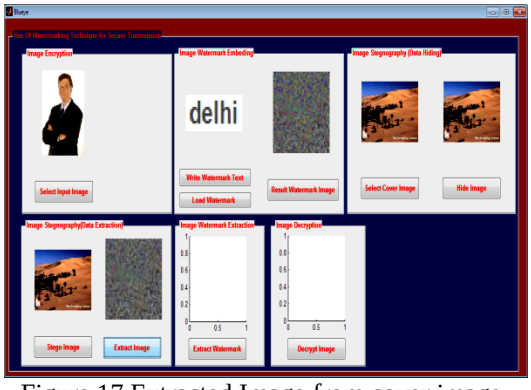

Figure 17.Extracted Image from cover image.

2. IMAGE WATERMARK EXTRACTION

In this part of image watermark extraction we extract the watermark which is embedded in the form of a text and that text which is then converted into image, but firstly we have to remove the gaussion noise and then watermark after that only we can get our original image by clicking on **"Extract Watermark** "button.

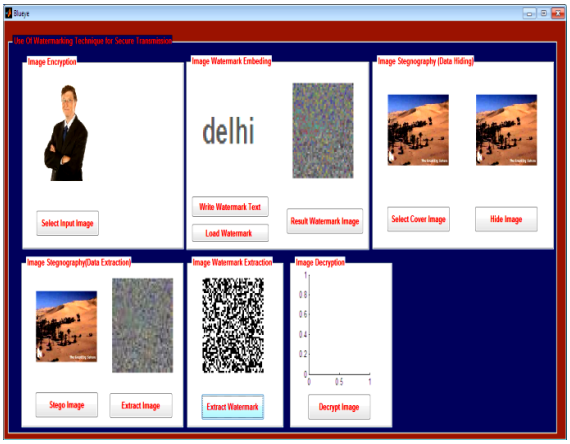

Figure 18.Extracted Watermark and noise from image.

3. IMAGE DECRYPTION

Image decryption is the reverse part of Image Encryption. Decryption is the process of transforming data that has been rendered unreadable through encryption back to its unencrypted form. In decryption technique it extract and convert the distorted data and transform it to texts and images that are easily understandable by the receiver, it can be accomplished by using a set of keys and password, manually and automatically. This is our original image which the sender transfers it to the receiver side.

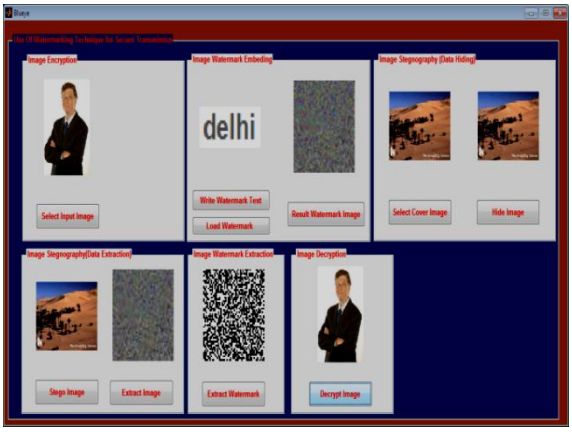

Figure 19.Decrypt Original image.

VII. CONCLUSION

The Experimental result shows that the proposed methodology is a combination of Steganography and Watermarking which gives highly secured method for data communication. This effective method is used to hide information inside an image and it is not that easy to inspect by any unauthorized user to identify the changes or existence of any type of message inside that image. In this approach we use secret key of symmetric key type for both sender side and receiver side that help us to hide our

ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 4, Issue 8, August 2015

information from others and the spatial domain method LSB technique with watermarking that will provides a new dimension to image steganography.

In our methodology we apply watermarking technique or invisible watermark in an image which is a text that is loaded and converted into an image, after that we apply a noise to it to make our methodology more secure and gives better quality of image after decoding. In future our aim is divide the image into blocks in matrix form and in each block we can hide our secret message and apply embedding algorithm can change its pixel value.

REFERENCES

[1] Krati vyas, B.L.Pal**,** "A PROPOSED METHOD IN IMAGE STEGANOGRAPHY TO IMPROVE IMAGE QUALITY WITH LSB TECHNIQUE", International Journal of Advanced Research in Computer and Communication Engineering Vol. 3, Issue 1, January 2014.

[2] Salony Pandey,Vinay Harsora, "Enhanced LSB algorithm for Color Image", *(IJAERD) Volume 1,Issue 5,May 2014, e-ISSN: 2348 – 4470.*

[3]*Ramadhan Mstafa1, Christian Bach2, "*Information Hiding in Images Using Steganography Technique *2013 ASEE Northeast Section Conference*s".

[4] Aayushi Verma, Rajshree Nolkha, Aishwarya Singh and Garima Jaiswal, "Implementation of Image Steganography Using 2-Level DWT Technique" IJCSBI.ORG ISSN: 1694-2108 | Vol. 1, No. 1. MAY 2013.

[5] Ankit Chadha, Neha Satam, Rakshak Sood, Dattatray Bade, "An Efficient Method for Image and Audio Steganography using Least Significant Bit (LSB) Substitution", *International Journal of Computer Applications (0975 – 8887) Volume 77– No.13, September 2013.*

[6] Mamta Juneja, and Dr. Parvinder S. Sandhu, "An Improved LSB based Steganography Technique for RGB Color Images", 2nd International Conference on Latest Computational Technologies (ICLCT'2013) June 17-18, 2013 London (UK).

[7] Maryam Habibi , Ronak Karimi , Masoud Nosrati, "Using SFLA and LSB for Text Message Steganography in 24-Bit RGB Color Images", International Journal of Engineering Sciences, 2(3) March 2013.

[8] Sarita Poonia, Mamtesh Nokhwal, Ajay Shankar**,** "A Secure Image Based Steganography and Cryptography with Watermarking", (IJESE) ISSN: 2319–6378, Volume-1, Issue-8, June 2013.

[9] Shilpa Thakar, Monika Aggarwal, "A Review –Steganography", *2013, IJARCSSE.*

[10] Ankita Gangwar, Vishal shrivastava, "Improved RGB -LSB Steganography Using Secret Key", International Journal of Computer Trends and Technology- volume4Issue2- 2013.

[11] Mamta. Juneja, and Parvinder S. Sandhu,"An Analysis of LSB Image Steganography Techniques in Spatial Domain", (IJCSEE) Volume 1, Issue 2 (2013) ISSN 2320–401X.

[12] Vipul Sharma,Sunny Kumar, " A New Approach to Hide Text in Images Using Steganography", *2013, IJARCSSE.*

[13] Gurpreet Kaur, Kamaljeet Kaur, "Image Watermarking Using LSB (Least Significant Bit)", *2013, IJARCSSE.*

[14] Atallah M. Al-Shatnawi, "A New Method in Image Steganography with Improved Image Quality", Applied Mathematical Sciences, Vol. 6, 2012

[15] Nitin Jain, Sachin Meshram, Shikha Dubey, "Image Steganography Using LSB and Edge Detection Technique",(IJSCE) ISSN: 2231-2307, Volume-2, Issue-3, July 2012.

[16] Deepshikha Chopra, Preeti Gupta, Gaur Sanjay B.C., Anil Gupta, "Lsb Based Digital Image Watermarking For Gray Scale Image", *(IOSRJCE)ISSN: 2278-0661, ISBN: 2278-8727 Volume 6, Issue 1 Sep-Oct. 2012.*

[17] Snehal O.Mundhada, V. K.Shandilya, "Spatial and Transformation Domain Techniques for Image Enhancement", IJESIT Volume 1, Issue 2, November 2012.

[18] Shailender Gupta, Ankur Goyal, Bharat Bhushan, "Information Hiding Using Least Significant Bit Steganography and Cryptography",*I.J.Modern Education and Computer Science*, 2012.

[19] Parisa Gerami, Subariah Ibrahim, Morteza Bashardoost, "Least Significant Bit Image Steganography using Particle Swarm Optimization and Optical Pixel Adjustment", International Journal of Computer Applications (0975 – 8887) Volume 55– No.2, October 2012.

[20] G. Viji and J. Balamurugan, "LSB Steganography in Color and Grayscale Images without using the Transformation", International Journal of Advances in Image Processing, Vol. 1, Special Issue, December 2011.

[21] Jassim Mohmmed Ahmed† and Zulkarnain Md Ali, "Information Hiding using LSB technique", IJCSNS International 18 Journal of Computer Science and Network Security, VOL.11 No.4, April 2011.

[22] Mr. Vikas Tyagi, Mr. Atul kumar, "IMAGE STEGANOGRAPHY USING LEAST SIGNIFICANT BIT WITH CRYPTOGRAPHY", JGRCS 2010.

[23] Mohammad Tanvir Parvez and Adnan Abdul-Aziz Gutub, "RGB Intensity Based Variable-Bits Image Steganography", 2008 IEEE Asia-Pacific Services Computing Conference.

BIOGRAPHIES

Prof. Kashiram. Jayaram. Satao is Computer Science & Engineering and Head of Information Technology Department at Rungta College of Engineering & Technology, Bhilai (C.G.), India

Ms. Nidhi Bux (Correspondence Author) received the B.E. From Pt. Ravishankar Shukla University, Raipur (C.G.), India in Computer Science & Engineering in the year 2008. She is currently pursuing M.Tech. Degree in Computer Science & Engineering with specialization in CSVTU .