RGB Image Steganography using Zigzag Pixel Indicator and Scan Techniques

T. Anvesh Gandhi, G. Naga Raju , Dr. P.V.Rama Raju
SRKR ENGINEERING COLLEGE, Bhimavaram

***Abstract*—** Information security is one of the main issues in communication to ensure that unauthorized user can't get unintended information. Cryptography and Steganography are such techniques to provide information security. Steganography is a data hiding technique that hides image, audio and video in image content. Steganography is advantageous than cryptography which is another data hiding technique that in steganography data hiding is invisible and undetectable in this paper we propose a steganography technique using pixel indicator method in the proposed model various data embedding is performed by using various patterns to increase the complexity.

***Keywords*—** Steganography, Zigzag method, LSB substation method, Pixel indicator algorithm, RGB bitmaps.

I. INTRODUCTION

Currently computers and its applications has became part of real time life. Information security has become important issue with advancement in computer applications and networks. There are so many techniques which are proposed to provide secure data transmission. Cryptography and Steganography are such techniques to facilitate information security. In Cryptography data like image, audio and video are converted to unrecognized form to achieve information security. Data is converted to hidden form by using various algorithms which are known as scanning techniques . C Scan, Z scan, spiral scan are some of important Cryptographic algorithms. Sometimes secret key can be associated with Cryptography to provide extra security.

Steganography is a data hiding technique in which secret data can be hidden in a cover media such that unintended user can not know the existence of secret data [1]. Secret message can be text, image, audio or video files whereas cover media can also be taken any one of the available digital file formats. Image and sound files are generally chosen for carrier media because of redundancy in the data. The images that are taken for data embedding are known as carrier image or cover image. After the data hiding or data embedding the resultant image is known as stego image. Changes that are made in carrier image after the message data embedding are unobservable so carrier image and stego image are almost visually similar.

Cryptography and Steganography are the popular data hiding techniques but Steganography is preferred to Cryptography [2]. The differentiating feature of Steganography from Cryptography is the secret message invisibility. In Cryptography data is converted to unreadable form so there is a chance to suspect the existence of data hiding. Whereas in Steganography hidden data is invisible and unsuspectable. In steganography, quality of cover image conveys the efficiency of steganography. Steganography techniques are of two types spatial and frequency domain techniques.

In spatial technique, data is embedded into image pixels directly while in frequency domain techniques data insertion is performed in transformed domain like Fourier transform, DCT and Wavelet transform. Simple LSB is one of the popular spatial domain techniques. In this technique data embedding is performed by altering the LSB of cover image. The LSBs of image pixels are replaced by MSBs of image data.

Proposed Steganography technique is comes under the category of spatial techniques it is similar to simple LSB with some modifications to provide better security. In this model pixel indicator method is used to denote the existence of the data in the pixel. In this model, we use one of three channels of RGB carrier image to denote the data existence. Data is embedded into image segments and move from one segment to other in a zigzag fashion. In each segment data embedded in a way such that using any one of the scanning techniques like C scan, Z scan, normal scan and spiral scan.

The rest of the paper is organized into following sections. In section II, we explain in detail about proposed Steganography model. In section III, we describe the experimental results and analysis. Finally Section IV, we conclude the paper.

II. PROPOSED STEGANOGRAPHY MODEL

In our proposed steganography model [3], message data is embedded into the cover image segments using simple LSB along pixel indicator method and different data embedding patterns to provide high security.

A. Algorithm for proposed model

In the proposed steganography model, steganography is performed by using the following sequential steps.

a. Divide the cover image into four sub images
b. Data embedding is taken place between the sub images in a zigzag fashion and different data embedding patters are used
c. Data embedding is taken place by using simple LSB and pixel indicator method
d. After data is embedded four segments of image is combined and transmitted

1) Algorithm for message data embedding

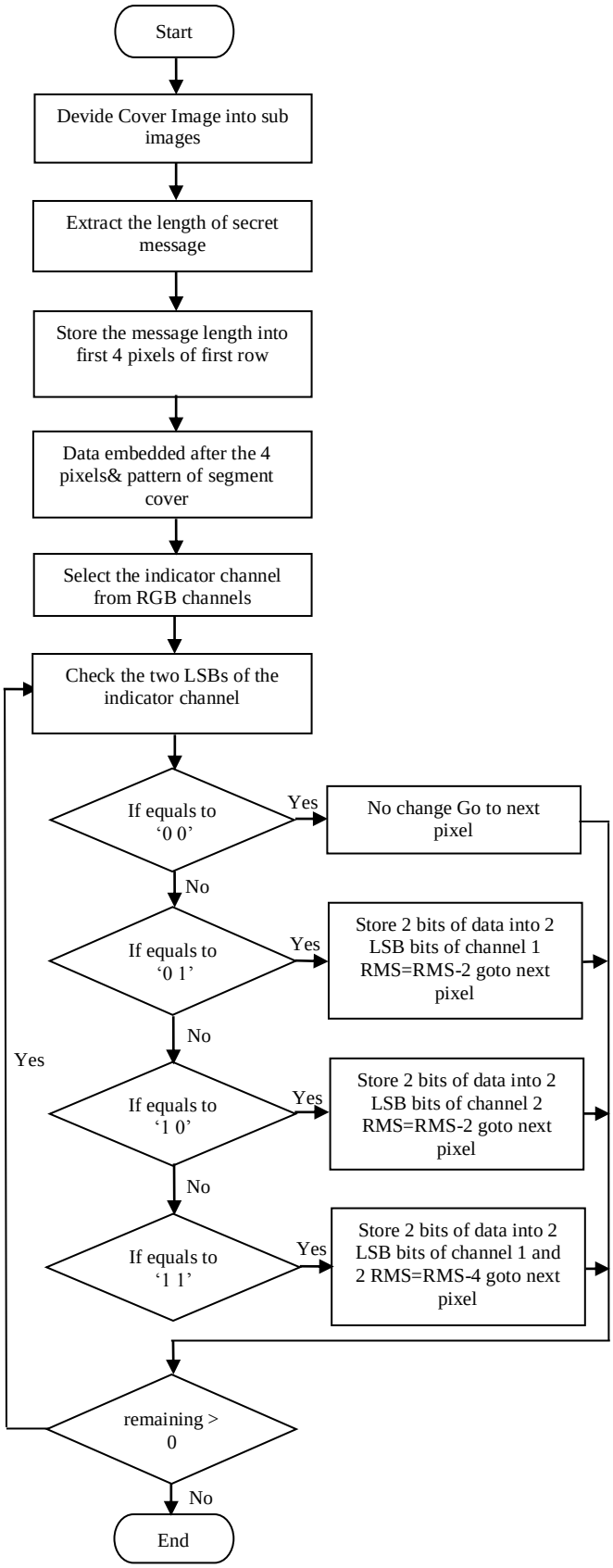


Fig.1: Flowchart for data embedding

2) Algorithm for message extraction

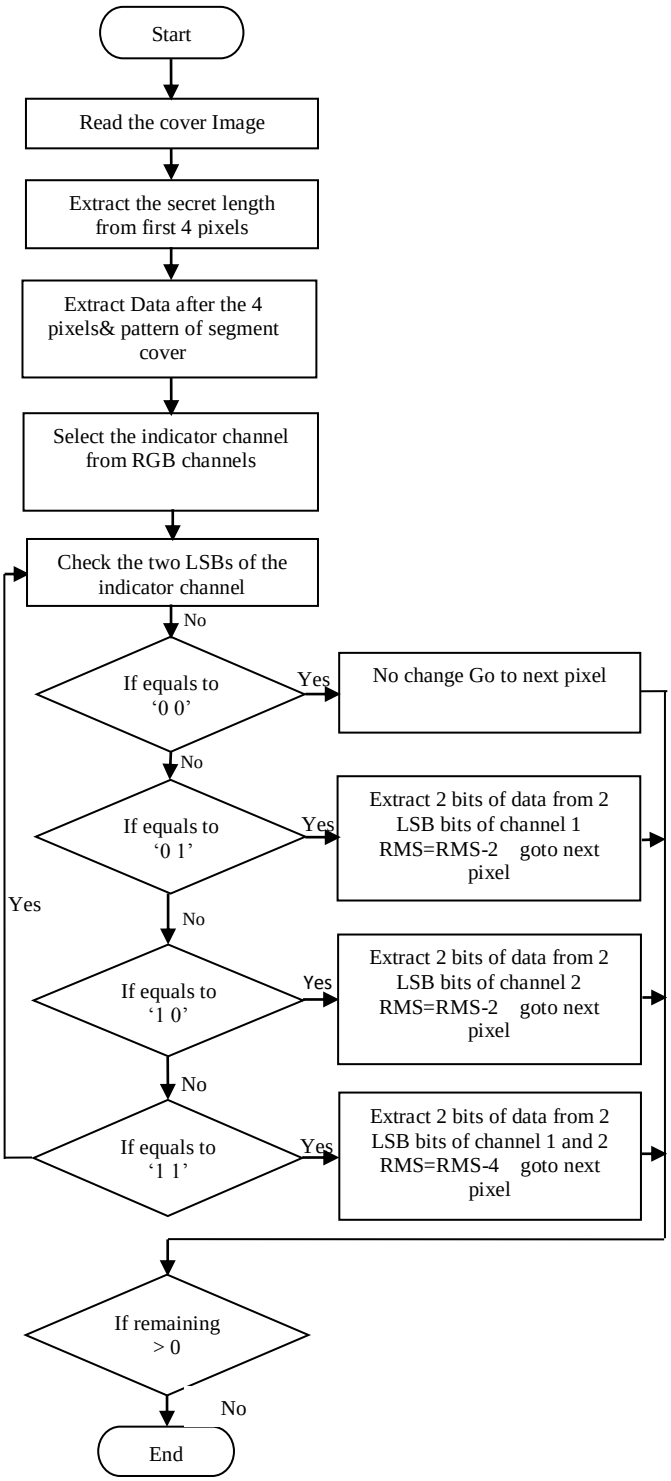


Fig.2: Flowchart for data extraction

B. Methodology

1) LSB substitution method:

In LSB substitution method, secret message data is embedded into the least significant bits of all pixels of cover image to make message is invisible to others [4]. It is commonly used steganography technique because it is simple. The basic idea behind LSB substitution is that altering the LSBs of cover image doesn't affect the cover image quality significantly. It can also be used for carrier media of other file formats.

2) Pixel indicator method

In pixel indicator technique any one of three channel Red, Green and Blue channels of cover image is used indicate the existence of message data in the remaining two channels which are intended to hide message bits. The below table shows the relationship between the indicators and the other two information hiding channels.2LSBs of the indicator channel is used to indicate the existence of message data in remaining two channels respectively. If indicator value for particular channel is 0 means data is not existed otherwise data is existed.

TABLE 1: PIXEL INDICATOR TECHNIQUE

2 LSB's of Red	2 LSB's of Green	2 LSB's of Blue
00	No data	No data
01	No data	Contains data
10	Contains data	No data
11	Contains data	Contains data

There are two types of pixel indicators. They are

i.Default

ii.User defined

In the *Default pixel indicator*, Red is assigned as a default indicator. It is denoted as channel one. The two least significant bits of the red channel will be used as a indication to the existence of hidden information in green channel and blue channel. Green is denoted as channel two and blue is denoted as channel three.

In *User defined Pixel indicator* method, among the three channels (R, G, B) any one is used as a indicator channel. Based on the chosen indicator's last two least significant bits the secret data is embedded in to the other two channels. If Red is the indicator, while Green is channel one and Blue is the channel two. If Green is the indicator, while Red is channel one and Blue is channel two. If Blue is the indicator, while Red is channel one and Green is channel two.

3) Embedding patterns

In the proposed steganography model, different embedding patterns are used among different sub images of cover image to improve the security.The embedding patterns of the proposed methods are spiral, c, normal and zigzag. The following table shows the indications to represent the embedding patters.

TABLE 2: SCAN PATTERNS

Indicator	Embedding pattern
00	Normal
01	Zigzag
10	C
11	spiral

III. RESULTS

The proposed steganography model was implemented using matlab in i3 processor using 2GB RAM. Results are obtained as follows.

Cover image:

Fig.3: Input image 512X512.png

Text Message:

Steganography is derived from the Greek for covered writing and essentially means "to hide in plain sight". Steganography is the art and science of communicating in such a way that the presence of a message cannot be detected. Simple steganographic techniques have been in use for hundreds of years, but with the increasing use of files in an electronic format new techniques for information hiding have become possible. This document will examine some early examples of steganography and the general principles behind its usage. We will then look at why it has become such an important issue in recent years. There will then be a discussion of some specific techniques for hiding information in a variety of files and the attacks that may be used to bypass steganography. Figure shows a common taxonomy of steganography techniques. Technical steganography uses scientific methods to hide a message, such as the use of invisible ink or microdots and other size-reduction methods. Linguistic steganography hides the message in the carrier in some nonobvious ways and is further categorized as semagrams or open codes. Semagrams hide information by the use of symbols or signs. A visual semagram uses innocent-looking or everyday physical objects to convey a message, such as doodles or the positioning of items on a desk or Website. A text semagram hides a message by modifying the appearance of the carrier text, such

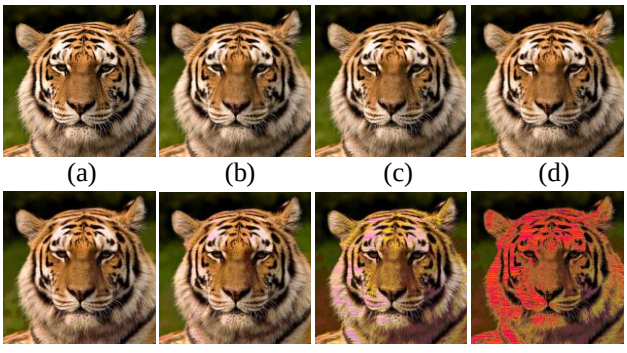
Stego Image: 1 bit LSB

Fig.4: stego image 512x512 (.png)

Extracted Text:

Steganography is derived from the Greek for covered writing and essentially means "to hide in plain sight". Steganography is the art and science of communicating in such a way that the presence of a message cannot be detected. Simple steganographic techniques have been in use for hundreds of years, but with the increasing use of files in an electronic format new techniques for information hiding have become possible. This document will examine some early examples of steganography and the general principles behind its usage. We will then look at why it has become such an important issue in recent years. There will then be a discussion of some specific techniques for hiding information in a variety of files and the attacks that may be used to bypass steganography. Figure shows a common taxonomy of steganography techniques. Technical steganography uses scientific methods to hide a message, such as the use of invisible ink or microdots and other size-reduction methods. Linguistic steganography hides the message in the carrier in some nonobvious ways and is further categorized as semagrams or open

We can analyze the results by varying the number of least significant bits (LSB) used for data embedding.



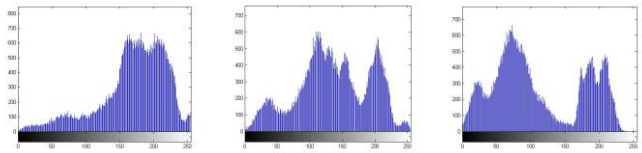
(a) (b) (c) (d)

(e) (f) (g) (h)

Fig.5: Stego images for (a)1 bit (b)2 bit (c)3 bit (d)4 bit (e)5 bit (f)6 bit (g)7 bit (h)8 bit

From the results it is observed that the visual quality of the cover image didn't degraded up to 5LSBs. The following figures shows the histograms of three channels cover image and stego images.

Histogram for input image (Figure 3) RED, GREEN, and BLUE are show in figure 4



(Red) (Green) (Blue)

Fig.4: Histogram of cover image

Histogram for various output images are shown in order with figure 5 in figure 6

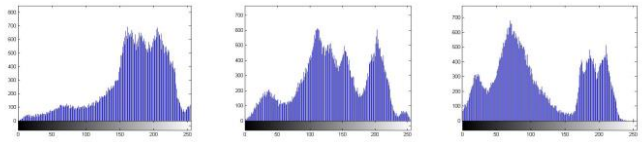


Figure 6.a (Red) **(Green)** **(Blue)**

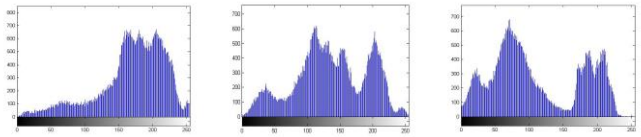


Figure 6.b (Red) **(Green)** **(Blue)**

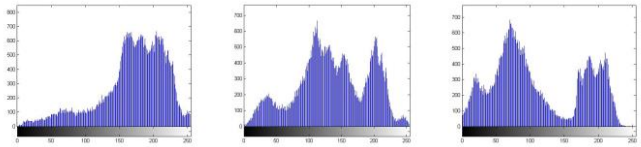


Figure 6.c (Red) **(Green)** **(Blue)**

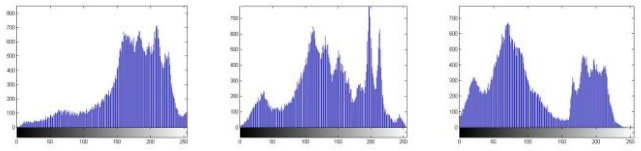


Figure 6.d (Red) **(Green)** **(Blue)**

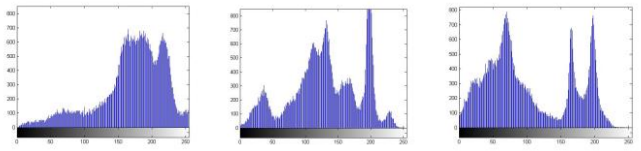


Figure 6.e (Red) **(Green)** **(Blue)**

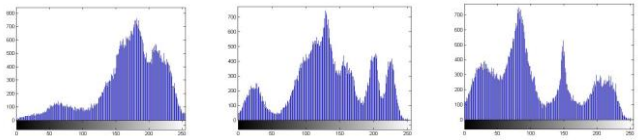


Figure 6.f (Red) **(Green)** **(Blue)**

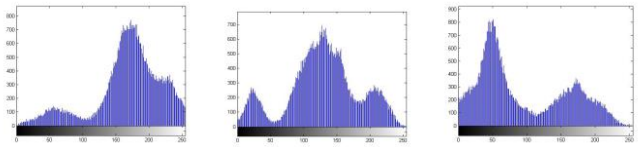


Figure 6.g (Red) **(Green)** **(Blue)**

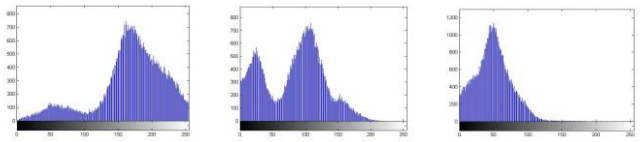


Figure 6.h (Red) **(Green)** **(Blue)**

IV. CONCLUSION

In this project secret message is inserted in to the image involves in image partition, Zig zag movement among the segments, different data embedding patterns and pixel indicator technique, which improves the security of the hidden data.

V. REFERENCES

[1] P.Mahimah, Mrs.R.Kurinji, "*Zigzag Pixel Indicator based Secret Data Hiding Method*",979-1-4799-1597-2/13,IEEE 2013.

[2] Wien Hong , "*Adaptive image data hiding in edges using patched reference table and pair-wise embedding technique*",0020-0255, 2012 Elsevier Inc..

[3] S. M. Masud Karim, Md. Saifur Rahman, "*A New Approach for LSB Based Image Steganography Using Secret Key*," Proceedings of 14th International Conference on Computer and Information Technology (ICCIT 201 I) 22-24 December, 2011 IEEE.

[4] J. AnitaChristaline1, D.Vaishali, "*Image steganographic techniques with improved embedding capacity and robustness*," 978-1-4577-0590-8/11, ICRTIT 2011 IEEE.

[5] Gandharba Swain and Saroj Kumar Lenka,"*A Novel approach to RGB channel Based Image Steganography Technique*," International Arab Journal of e-Technology, vol. 2, No. 4, June 2012.

[6] El-Sayed M. El-Alfy, Azzat A. Al-Sadi,"*Improved Pixel Value Differencing Steganography Using Logistic Chaotic Maps*," International Conference on Innovations in Information Technology (IIT) , 978-1-4673-1101-4/12,2012 IEEE.

[7] Chi-Kwong Chan, L.M. Cheng, "*Hiding data in images by simple LSB substitution*," 0031-3203, 2003 Pattern Recognition Society. Published by Elsevier Ltd2003.

[8] R. C. Gonzalez and R. E. Woods, *Digital Image Processing*, Pearson prentice Hall, 2005.

[9] G. Naga Raju, T V Hyma lakshmi,"*Image Encryption using Secret-Key images and SCAN Patterns*," National Conference of NCIPA_VVIT -2012

[10] P.V. Rama Raju, G. Naga Raju, R. Krishna Chaitanya, "*Image Encryption and Decryption using Encryption Algorithm*," International Journal on Discovery-2015

[11] G. Naga Raju, James Vijay, "*Secret-key based Separable Reversible Data-Hiding in Encrypted image*," National Conference on VLSI, Signal processing & Communications NCVSComs-2011.

T Anvesh Gandhi Currently pursuing M.E in Communication Systems from S.R.K.R Engineering College, A.P, India

Nagaraju G Presently working as assistant professor in Dept. of ECE, S.R.K.R. Engineering College, Bhimavaram, AP, India. He received B.Tech degree from S.R.K.R Engineering College, Bhimavaram in 2012, and M.Tech degree in Computer electronics specialization from Govt. College of Engg., Pune university in 2004. His current research interests include Image processing, digital security systems, Signal processing, Biomedical Signal processing, and VLSI Design.

Dr. P. V. RAMA RAJU Presently working as a Professor at the Department of Electronics and Communication Engineering, S.R.K.R. Engineering College, AP, India. His research interests include Biomedical-Signal Processing, Signal Processing, Image Processing, VLSI Design, Antennas and Microwave Anechoic Chambers Design. He is author of several research studies published in national and international journals and conference proceedings.