RESEARCH ARTICLE OPEN ACCESS

# A Novel Secured RGB LSB Steganography with Enhanced Stego-Image Quality

Koyi Lakshmi Prasad*, Dr. T.Ch.Malleswara Rao**
* (Assistant Professor, Department of Computer Science and Engineering, QIS College of Engg & Technology)
** (Professor, School of Electronics, Sreenidhi Institute of Technology, Hyderabad, India)

**ABSTRACT**
Steganography is the science of writing hidden messages in such a way that no one apart from the intended recipient knows of the existence of the messages. Steganography is a greek origin word which is pronounced as Stehg-uh-nah-grunf-ee where steganous means secret or covered and graphie means writing. In this paper a new steganography technique is presented, implemented and analyzed. The proposed RGB LSB method hides the secret message based on the comparison and searching about the identical bits between the secret messages and image pixel values. The proposed method is compared with LSB benchmarking method and achieved a efficient image with enhanced stego-image quality.
***Keywords:*** Identical bits, LSB, LSB benchmarking, RGB, Steganography, Stego-image.

## I. INTRODUCTION

Steganography is the science of writing hidden messages in such a way that no one apart from the intended recipient knows of the existence of the messages. Steganography is a greek origin word which is pronounced as Stehg-uh-nah-grunf-ee where steganous means secret or covered and graphie means writing. The message can be a text, an image or it can be an audio file [1, 6, 9].

Steganography methods were started in ancient Greece at 400 BC. In ancient Greece, text was written on wax covered tablets. One of the most popular story is that "Demeratus" wanted to promulgate Sparta that xerxes intended to invade Greece. So to convey that message to Spartans he scraped wax out of tablets and wrote a message on the underlying wooden blanks. He covered the tablets with wax again. The tablets appeared to be unused, so when the material is checked by sentries no one can identify them and allowed to move [6, 9].

Greeks used to shave the head of their slaves and tattoo a secret message on their heads. Until the hair was completely grown the slaves were not allowed to move. When hair was grown they were sent to various places to deliver the message to their agents. As well as invisible inks these inks came into focus when there usage gave success in the Second World War. An innocent letter may contain a very different message written between the lines. Early in World War II steganographic technology consisted almost exclusively of invisible inks. Common source to prepare these type of ink was milk, fruit juices etc. these get darken when they are heated.

Null cipher is another method used for steganography where the real message is "camouflaged" in an innocent sounding message. Due to the "sound" of many open coded messages, the suspect communications were detected by mail filters. The Germans developed microdot technology which FBI Director J. Edgar Hoover referred to as "the enemy's masterpiece of espionage." Microdots are photographs the size of a printed period having the clarity of standard-sized typewritten pages. The first microdots were discovered masquerading as a period on a typed envelope carried by a German agent in 1941 [5].

Masking and filtering is another technique where information is hidden inside of a image using digital watermarks that include information such as copyright, ownership, or licenses. The purpose is different from traditional steganography since it is adding an attribute to the cover image thus extending the amount of information presented. Algorithms and Transformations techniques are used to hide data in mathematical functions that are often used in compression algorithms. The idea of this method is to hide the secret message in the data bits in the least significant coefficients.

The main motivation behind the development of image steganography methods is its way to use in various organizations to communicate between its members. It can be also used to communicate between military, intelligence and secret agents. The main aim of image steganography is to avoid attention of the hackers when transmitting hidden information [6, 9].

The main attributes of the Steganography are: cover message, secret message, and secret key and embedding algorithm. The cover message is used to cover the encoded text in itself; it acts like a medium to hide things inside it. Secret message is the message which we want to transmit. The secret key is the key which is known by us to encode the secret message. The embedding algorithm is used to embed the text inside the cover message.

In the Steganography system the entire scenario is that first we have to opt for the best cover message as it may be like any of the media elements (image, video, audio). We have to encode the secret message using an appropriate key. Then we have use and embedding algorithm to embed the secret text in the cover message. When the stego-image is ready, we can send to the desired person by any mode of communication.

In the modern scenario many cover messages can be used such as image, video, audio. The image file is the most popularly used cover message because it is easy to transmit messages from sender to receiver. The images are basically divided into three categories they are: binary images, Gray scale images and RGB images. In binary images every one bit value for pixel represents 0 for black and 1 for white. In Gray scale images every pixel has 8-bit value where 00000000 represents black and 11111111 represents white. In RGB (RED-GREEN-BLUE) images every pixel has 24-bit value where (00000000 - 00000000 - 00000000) represents black and (11111111-11111111-11111111) represents white. We use the RGB images because a slight change in the RGB images doesn't make any change in the image resolution so ultimately which will not affect the quality of the image and the data will be highly secure.

## II. BACKGROUND THEORY

In the last few years the theoretical foundations of information hiding has advanced very rapidly. Modeling the information hiding process as one of the communication security produced improved information hiding algorithms as well as accurate models of the channel capacity and error rates. At the same time, steganography security, i.e. the ability of information hiding to serve in a scenario where the presence of an enemy explicitly aiming at nullifying the hidden information goals, whatever they are, has been recognized as one of the main open issues steganographic techniques face with.

As explained in reference [8, 10], for all the steganographic systems, most vital and elementary requirement is the un-detectability. The hidden message should not be detected by any other people. Moreover, the cover message with hidden message i.e. stego-media are indistinguishable from the original ones i.e. Cover media. The cover media and stego-media should appear identical under all possible statistical attacks and the embedding process should not degrade the media fidelity [8] presents several attacks on cover media. The difference between stego-media and the cover-media should be imperceptible for visual attacks.

Steganography uses two types of protocols: secret-key and public- key steganography. In secret-key steganographic model, both sender and receiver share a secret-key before conveying messages. The input message may be in any digital form and be treated as a bit stream. Public-key cryptography requires the use of two keys, one private and one public key. The public-key is used in the embedding process where as the private key is used to extract the hidden message.

Even though a considerable number of steganography techniques were in use, study of this subject in the scientific literature goes back to Simmons [3, 5, 11], who in 1983 formulated it as the "prisoners' problem". A detailed review on steganographic techniques is discussed by the author in her previous paper Ref. [2].

### 2.1 Digital Steganography Methods

The steganography applications range from those that actually hide data, often encrypted, with in the file, to those that simply attach hidden information to the end of a file such as Camouflage. As explained in Ref. [7], the community is concerned with a number of digital technologies, namely, text files, images, movies and audio. One of the main methods typically used for steganography involves the process of hiding a message in image pixels. Digital images are the most wide spread carrier medium used [9]. NeilF.Johnson[6] explains different methods of hiding data in digital images.

### 2.2 Image-based Steganography

Many steganographic tools in the internet are available for varied image formats. The fact that image scan be usefully subjected to lossy compression methods has suggested that extra information could be concealed in them .Properties of image scan be manipulated including luminescence, contrast and colors. A24-bit color image has three components corresponding to Red, Green and Blue. The three components are normally quantized using 8 bits. An image made of these components is described as a 24-bit color image. Each byte can have a value from 0 to255representing the intensity of the color. The darkest color value is 0 and the brightest is 255. Transparency is controlled by the addition of information to each element of the pixel data. A24-bit pixel value can be stored in 32bits. The extra 8 bits is for specifying transparency. This is sometime scaled the alpha channel. An ideal 8-bit alpha channel can support transparency levels from 0(completely transparent) to255 (completely opaque). It can be stored as part of the pixel data. Structure of digital images is discussed in the "An evaluation of Image Based Steganography Methods" by Kevin Curran of Internet Technologies Research Group [9].

Current techniques for embedding of messages into image carriers fall into three categories [4][7]:

- Least-Significant Bit embedding (or simple embedding).
- Advanced Least-Significant Bit embedding.

## III. EXISTING METHODS

### 3.1 Least Significant Bit Embedding

Least significant bit embedding technique is the most popular steganography technique. Depending upon the binary coding of the secret message it hides the message in the binary coded image. The below figure (a) depicts the knowledge of pixel values and secret messages. LSB makes changes in the image which are very easy to recognize and the stego images are easy to attack.

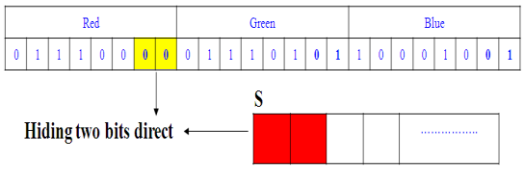


Fig 1: Least Significant Bit Hiding Technique

#### 3.1.1 Algorithm for LSB Method

- Steps to Hide the Message Using the LSB Method.
- Choose the proper image for the cover medium.
- Scan the image row by row and encode it in to binary form.
- Encode the secret message into binary notation.
- Calculate the sizes of the image and secret message.
- Consider one pixel of the image.
- Segment the image into three parts (Red, Green and Blue parts)
- Hide two by two bits of the secret message in each position of the pixel at the last two significant positions.
- Set the image with the newly considered values.
- Set the image and save it.

### 3.2 Advanced LSB Embedding

The LSB method hides the secret text at the least two significant bits of the image pixels. Hence a change in the value of image pixels affects the image resolution, which ultimately leads to the reduction of image quality and make the image easy to attack. This LSB method is already attacked and broken. So in advanced LSB we are hiding the secret message based on searching about the identical values between the image pixels and secret messages. The image shown below gives a clear idea of arrangements of bits in the image pixel.

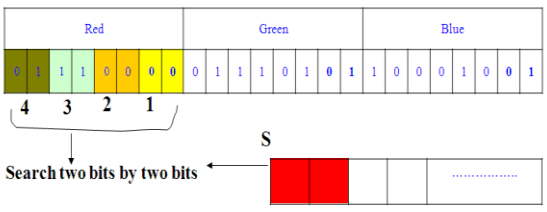


Fig 2: Advanced Least Significant Bit Hiding Technique

#### 3.2.1 Algorithm for Advanced LSB Method

- Steps to Hide the Message Using the LSB Method.
- Choose the proper image for the cover medium.
- Scan the image row by row and encode it in to binary form.
- Encode the secret message into binary notation.
- Calculate the sizes of the image and secret message.
- Consider one pixel of the image.
- Segment the image into three parts (Red, Green and Blue parts)
- Hide two by two bits of the secret message in each position of the pixel by searching the identical.
- If the search is unsuccessful then hide two by two bits of the secret message in the least significant position of pixel image.
- Store the positions of the hiding bits in a binary table.
- Set the image with the newly considered values.
- Set the image and save it.

## IV. PROPOSED METHOD

when we consider all the existing techniques for steganography we come across with the facts that we are replacing the least significant bits of the pixel images with the bits of the secret message hence which ultimately leads to the downfall of the quality of the image .in the proposed method we are considering the RGB image and converting that image into binary form. While considering the secret message each character is represented with 8 bits. We will segment these 8 bits into 3 parts (3bits+3bits+2 bits). We will select an image pixel randomly using a random function and compare the equivalence of the message bits with the pixel image bits. When the case is identical we replace the bits with those identical. If the case is non- identical we will simply replace the bits with the least significant bits of the image pixel. So when we are selecting the pixel image randomly and hiding the total 8 bits in one single pixel image, we are providing a better image resolution as compared to existing models.

### 4.1 Algorithm for Proposed Method

- Steps to Hide the Message Using the RGB LSB Method:
- Choose the proper image for the cover medium.
- Scan the image row by row and encode it in to binary form.
- Encode the secret message into binary notation.
- Calculate the sizes of the image and secret message.
- Consider one pixel of the image randomly.

- Segment the image into three parts (Red, Green and Blue parts).
- Segment the secret message into three parts (3bits, 3bits and 2bits).
- Hide the bits of the secret message in each position of the pixel by searching the identical.
- If the search is unsuccessful then hide the bits of the secret message in the least significant position of pixel image.
- Store the positions of the hiding bits in a binary table.
- Set the image with the newly considered values.
- Set the image and save it.

## V. EXPERIMENTAL ANALYSIS

The traditional LSB methods do not provide high capacity and flexibility to hide a whole character in a single pixel. Usually steganography is applied to normal images; by the segmentation technique we can provide higher level security to the secret message against steganalysis. Compared to the steganography used to hide the normal text, this proposed method provides rather better security with the use of cipher text. In total the analysis shows that the performance of the proposed method is much better than the existing methodologies.

Table 1: Comparative Results

| S.No | Original | Regular LSB | Proposed RGB LSB |
|---|---|---|---|
| 1 | 71.2131 | 71.2107 | 71.2133 |
| 2 | 91.4541 | 91.4515 | 91.454 |
| 3 | 116.8887 | 116.8766 | 116.8881 |
| 4 | 82.7183 | 82.7076 | 82.7182 |
| 5 | 131.8025 | 131.799 | 131.8025 |
| 6 | 101.9898 | 101.9865 | 101.9898 |
| 7 | 105.4361 | 105.4215 | 105.4353 |
| 8 | 91.9313 | 91.9226 | 91.9305 |
| 9 | 18.9911 | 18.9803 | 18.9914 |


Fig 3: Original Images and its Histograms


Fig 4: Regular LSB Embedded Images and its Histograms


Fig 5: Proposed COLOR LSB embedded Images and its Histograms

The above results point up that the mean of proposed method values increased than original and regular LSB methods. When message is embedding in the image by using regular LSB method, message bits stored in pixels eight bit plane. Thus, the pixel value does not change well. Then mean value of image also not changed much and the value is relative to original image mean. When message is embedding in the image by using proposed RGB LSB method, Message bits of single character stored in single RGB pixel. So, pixel value changes a tiny than other embedding methods. Even though mean value of proposed method increases integrity of message and sturdiness of message security is enhanced.

In total the analysis shows that the performance of the proposed method is much better than the current methodologies.

## VI. CONCLUSION

In this paper a new steganography technique presented, analyzed and implemented. The proposed method hides the secret message based on comparing and searching the least significant bits of RGB image in an order of(3bits to R- component-3bits to G-component-2bits to B- component)by which we can hide a single character in one pixel image, so that only appropriate number of pixel images are required to hide the secret message. While we are selecting a pixel image randomly, image will not get affected in the issues of resolution and clarity. The proposed method was compared with the LSB and advanced LSB methods which hide the data in least significant bits and identical bits.

The proposed and LSB methods were used to implement stego image for the secret message on number of different images. The results of the proposed and LSB hiding methods were analyzed based on the mean of original image and embedded image. This paper conclude that that the proposed stegonography method is highly efficient, ace and accurate than the LSB methods which were proposed, it starts comparing and searching the identical bits in the pixel image and hides the data in it so that the resolution and quality of the images are never affected and keeps the message more secure. The experimental results also depict that the efficiency rate of the proposed method is relatively high when compared to the existing methods.

## REFERENCES

[1] A Discussion of Covert Channels and Steganography by Mark Owens, March19, 2002.

[2] Review on current Steganography technologies by S.G.K.D. N.Samaratunge, 7th International Information Technology Conference, 2005, SriLanka.

[3] An efficient color re-indexing scheme for palette based compression by Wenjun Zeng, JinLiand Shawmin Lei, Sharp Laboratories of America.

[4] A Review of Data Hiding in Digital Images by Eugene T.Lin and Edward J.Delp, Video and Image Processing Laboratory (VIPER), School of Electrical and Computer Engineering, Purdue University, Indiana.

[5] On the limits of Steganography by Ross J.Anderson, FabienA. P. Petitcolas, IEEE Journal of selected areas in Communications, 16(4):474-481, May 1998. Special issue on Copyright & Privacy protection. ISSN0733-8716.

[6] Exploring Steganography: Seeing the Unseen by Neil F.Johnson, Sushil Jajodia, George Mason University.

[7] Steganography and the Art of hiding information by Vish Krishnan, Overland Park, K.S.

[8] Information hiding–a survey by Fabien A.P.Petitcolas, Ross J.Anderson & Markus G.Kuhn (Proceedings of the IEEE– special issue on protection of multimedia content, 87(7):1062-1078, July1999).

[9] An evaluation of Image Based Steganography Methods by Kevin Curran, Internet Technologies Research Group, University of Ulster Karen Bailey, Institute of Technology, Letter kenny, Ireland (International Journal of Digital Evidence).

[10] Secure Error-Free Steganography for JPEG Images by Yeuan-Kuen Lee, Ling-Hwei Chen, Department of Computer and Information Science, National Chiao Tung University,1001 Taiwan, R.O.C. Second international Conference on Industrial and Information Systems, ICIIS2007, 8–11August, 2007, SriLanka339.

[11] New Steganography Technique for Palette Based Images by S.G.K.D.N.Samaratunge, University of Colombo School of Computing (UCSC), University of Colombo, Second International Conference on Industrial and Information Systems, ICIIS 2007, 8 – 11 August 2007, SriLanka.