International Journal of Science and Research (IJSR)
ISSN (Online): 2319-7064
Index Copernicus Value (2013): 6.14 | Impact Factor (2013): 4.438

Separable Reversible Data Hiding In Encrypted Image Using Modified Least Significant Bit and Virtual Embedding

Shreya M. S.[1], Sandeep Kumar S[2]

[1]M.Tech Student, Department of Computer Science & Engineering, Mangalore Institute of Technology and Engineering, Mangalore, Karnataka, India

[2]Assistant Professor, Dept.of Computer Science & Engineering, Mangalore Institute of Technology and Engineering Mangalore, Karnataka, India

Abstract: ***Nowadays digital communication has become an essential part of our daily activities. A lot of applications are internet-based and it is important that communication be made secret especially if it involves exchange of confidential information. As a result, the security of information passed over an open channel has become a fundamental issue and therefore, the confidentiality and data integrity are required to protect against unauthorized access and use. This has led to an unstable growth in the field of information hiding. Cryptography and steganography are the two popular methods available to provide security. Using cryptography, the data is transformed into some other gibberish form and then the encrypted data is transmitted. In steganography, the data is embedded in an image without affecting the quality of the image and that image will be transmitted. This paper proposes a new method for embedding the data inside the image using ordinal virtual embedding technique and also modification of data.***

Keywords: Cryptography, Feedback shift, MLSB, Ordinal Virtual Embedding, Reversible Data Hiding, Steganography, Separable Reversible Data Hiding

1. Introduction

Computer and the internet are major communication media that connect different parts of the world as one global virtual world in this modern era. As a result, people can exchange information easily and distance is no longer a barrier to communication. Perhaps, the safety and security of long-distance communication will be an issue. This is indeed important in the case of confidential data. The solution for this problem has led to the development of steganography schemes. Steganography is a very powerful security tool that provides a higher level of security, in particular when it is combined with encryption. Cryptography and Steganography are well known and widely used techniques that manipulate information in order to cipher or hide their existence respectively. Cryptography scrambles a message so that it cannot be understood; steganography hides the message so it cannot be seen. Even though both the techniques provide security, a research is made to combine both cryptography and steganography methods into one system for better confidentiality and security.

1.1 Cryptography and Steganography

Cryptography is a method of storing and transmitting data in a particular form so that only those for whom it is intended can read and process it. Cryptography systems can be broadly classified into symmetric-key systems that use a single key that both the sender and the receiver have, whereas public-key systems that use two keys, a public key which will be known to everyone and a private key that only the recipient of messages uses [1]. Commonly used terminologies in cryptography are:
1) Plain text
2) Cipher text
3) Encryption
4) Decryption
5) Key.

The word steganography comes from the Greek Steganos, which mean secret or covered and graphy means writing or drawing. Hence, steganography means, covered writing. The aim of steganography is to communicate securely in a completely undetectable manner and to avoid drawing suspicion to the transmission of a hidden data. There exist two types of materials in steganography they are message and the carrier. Message will be the secret data that will be hidden and the carrier will be the material that will take the message in it.

Watermarking and fingerprinting related to steganography are typically used for protection of the intellectual property. A digital watermark is a type of marker covertly embedded in a noise-tolerant signal such as audio or image data. It is normally used to identify ownership of the copyright of such signal. The embedded information in a watermarked object is a signature that refers the ownership of the data in order to ensure copyright protection. In fingerprinting technique, different and specific marks are embedded in the copies of the work that different customers are supposed to get. In this case, it will be easy for the property owner to find out such customers who give themselves the right to violate their licensing agreement when they illegally transmit the property to other groups [2].

1.2 Reversible Data Hiding

Reversible Data Hiding is a technique that hides data in

digital images for secret communication. It is a technique used for hiding additional message into cover media with a reversible manner so that the original cover content can be perfectly restored after extraction of the hidden message. Traditionally, the data hiding technique is used for secret communication of data. In some applications, the embedded carriers are further encrypted to prevent the carrier from being analyzed to reveal the presence of the embedment of data. Other applications could be for when the owner of the carrier might not want the other person, including the data hider, to know the content of the carrier before data hiding is actually performed, such as confidential medical images or military images. Here, the content owner has to encrypt the content before passing to the data hider for data hiding. The receiver can extract the embedded message and recover the original image which was used as cover image. Many reversible data hiding methods have been proposed recently.

Encryption is an effective and popular means for providing privacy. In order to securely share a secret image with other person, a content owner will encrypt the image before transmission. It may be also expected that the original content can be recovered without any error after decryption and retrieve of additional message at receiver side. Hence a reversible data hiding scheme for encrypted image is desirable.

Data hiding is referred as a process to hide data (representing some information) into cover media.The data hiding process links two types of data, one a set of the embedded data and another set of the cover media data. In several cases of data hiding, the cover media will be distorted due to data hiding and cannot be inverted back to the original media. Means, cover media has permanent distortion even after the hidden data have been removed. In some applications, like medical diagnosis and law enforcement it is desired that the original cover media can be recovered efficiently with no loss. The techniques satisfying this requirement will be referred to as lossless, reversible, invertible, distortion-free or data hiding techniques [3].

1.3 Separable Reversible Data Hiding

As the name indicates that it is the reversible data hiding technique but which is separable. The separable means that the information hidden can be separated using suitable criteria. The activities that can be separated are extraction of original cover image and extraction of original data which was embedded. This separation exists based on the keys available. At the receiver side, three different cases are encountered viz., if encryption key is available, get the original image, if data extraction key is available, get the original data and if both the keys are available, get both data and the image. Hence it is called as Separable Reversible Data hiding.

2. Literature Survey

A. Vivek Jain, Lokesh Kumar, Madhur Mohan Sharma, Mohd Sadiq, Kshitiz Rastogi,[4]

This paper proposed a technique to implement steganography and cryptography to hide the data inside the image. Here the original data will be encrypted by the stego key which is generated and shared by using Diffie Hellman key exchange protocol. Using the same stego key, some pixels are selected for hiding the encrypted data. From the selected pixel its LSB is taken for hiding the data. At the receiver side the shared stego key will be used to select the pixels where the data is embedded. Then extract the data which is encrypted using the key. Here based on the key shared the pixels will be selected. So if any intruder gets the stego image without the key will not know which pixel will be selected for data embedding. Thus it will ensure more security to the embedded data.

B. Divyani UdayKumar Singh, Kasturi Mohan Padwal, Madhura Pundlik Jadhav [5]

In this the authors proposed a new method for embedding the data into the image. Here sender will encrypt the data using AES algorithm, hides encrypted data in the image using LSB technique and then the system will auto generate the hide key. Sender will send the file with the help of mailing system. Receiver can retrieve the data based on the keys available. If he has only data hiding key then he can get only the original image. If he has the data hiding key and decryption key then he can get original data. All operation is done by proper login process. The system will generate fake data when unauthorized user tries to login. This proposed system will provide high security by providing access to only authenticated users and generating a fake data for the unauthorized users.

C. Guorong Xuan, Chengyun Yang, Y. Q. Shi, Yizhan Zheng, Zhicheng Ni [6]

This paper presents a reversible data hiding method based on wavelet spread spectrum and histogram modification. Using the spread spectrum scheme, the data is embedded in the coefficients of integer wavelet transform in high frequency sub-bands. Here pseudo bits are also embedded which will enhance data hiding efficiency. To prevent overflow and underflow an efficient histogram modification method is developed and it is used. Performance in terms of data embedding capacity and visual quality of marked image was high when compared to existing method.

D. C.Anuradha, S.Lavanya [7]

This paper presented a new secure and authenticated discrete reversible data hiding in cipher images deals with security and authentication. Here the content owner will encrypt the image with encryption key. The data hider may compress the LSB of the encrypted image for creating a space for embedding the data. The data hider can then embed the data in the allocated space by using the data hiding key. At the receiver based on the keys available he can get the data or the image. Here only the intended user with particular key can get the particular information. Here both image and data will be useful information. So the security of both image and data will be maintained.

E. Chaithu V Kumar [8]

In this paper the author proposed a novel secure Reversible Data Hiding for encrypted image by conforming space before encryption for embedding the data. In existing system, the

data is embedded by reversibly vacating room after the encryption of the cover image, which may make some error in data extraction and/or the restored image. Here the room for data hiding is reserved before encryption and the data is reversibly embedded in the encrypted image. Hence the image recovery and data extraction can be performed without error. In the proposed method the data is also encrypted using data encryption key and during data embedding another key will be used that is data embedding. Here it provides the separation of data extraction from image decryption thus improves the quality of marked image.

F. Mazen Abu Zaher [9]
In this paper the author proposed a new method for representing the data that will be embedded inside the cover image. Generally, characters of the data will be represented using 8 bits, but the MLSB technique will represent the characters of the data using 5 bits and then the 5 bits can be embedded in to the image using LSB method. Control symbols will be used to indicate the small, capital, number and space. By doing this a large amount of data can be embedded inside the cover image.

3. Problem Statement

In existing system reversible data hiding technique the image will be encrypted by using the encryption key and the data hider will compress the least significant bit (LSB) of the image to allocate space for hiding the data in it by using the data hiding key. At the receiver side, based on the keys available particular type of data can be obtained. But for embedding the data into an image, the image's LSB's will be compressed which will lead for the modification of the LSB value of the image. In the traditional system the data hiding key was needed for embedding the data into the image. So a technique is needed for data embedding which will not modify the image content.

4. Methodology

The proposed method will have 4 stages. They are image encryption, data modification, data embedding, image recovery and data extraction. The content owner will encrypt the cover image using the encryption key. The data hider will use the encrypted image for embedding the information (image or text). The encryption key is securely obtained by the receiver by using an appropriate key exchange protocol based on RSA algorithm. Virtual embedding of the information is done by the data hider by extracting the indexes of pixels that match with the bits of the data and will generate the data extraction key. This extraction key will be encrypted using public key generated by RSA and is sent to the receiver. If the receiver has data extraction key then the original data can be recovered. If receiver has encryption key then original image can be retrieved. If the receiver has both the keys then both data and the image can be obtained. The block diagram for sender and receiver side is shown in Fig 1 and Fig 2 respectively.

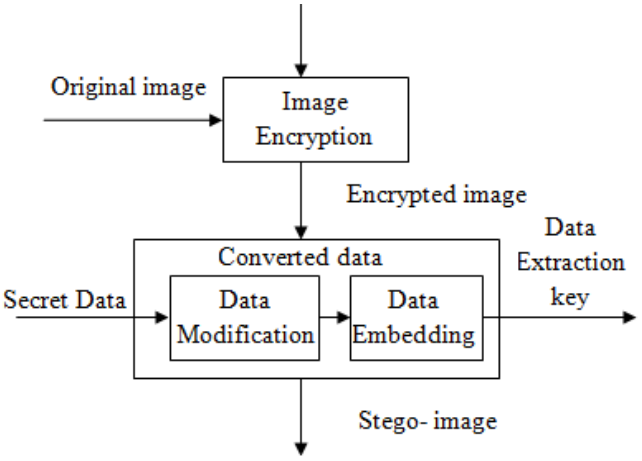

Figure 1: Architectural Diagram of the sender side

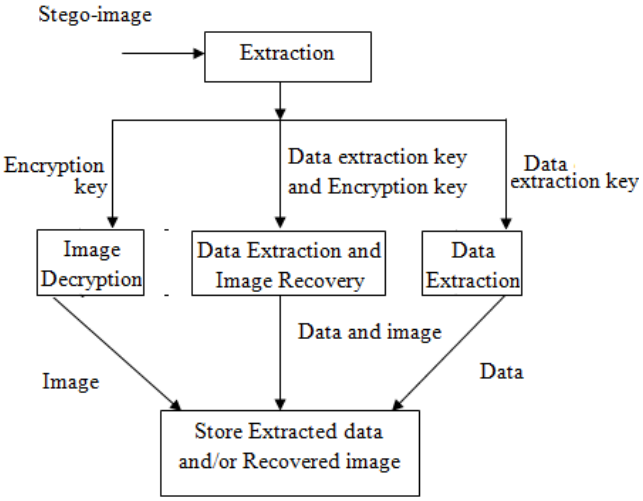

Figure 2: Architectural Diagram of the receiver side

5. Implementation Modules

5.1 Image Encryption

Encryption means applying special mathematical algorithms along with the help of the key and converting data to cipher code before transmitting it and decryption means performing the reverse operation of encryption to get back the original data from the cipher code. In this paper the cover image will be encrypted using modular additive encryption technique. The key sequence for the encryption will be generated using Feedback Shift Register (FSR). FSR generator generates the key sequence using an initial key called the seed value / initial value (IV). This generated seed value will be shared between the sender and the receiver. Every pixel of the image is encrypted using additive mod 256 to generate cipher text. At the receiver side, decryption algorithm is used for which the key sequence is generated by FSR as mentioned before. The decryption method will take this key sequence as additive inverse key to obtain back the original image.

Suppose we consider the colored image of size M*N. Each pixel will have Red, Green and Blue component with its value ranging from [0-256]. Each color component is made up of 8 bits that means each pixel is made up of 24 bits. Consider the initial seed value as $S_1\ S_2\ S_3 \ldots S_n$. The length can be varied up to 8 to 12 digits. Initially left most value of the seed value is a taken for encryption and then new S_{value} is

calculated. Then it is placed to the right by shifting the values to the left.

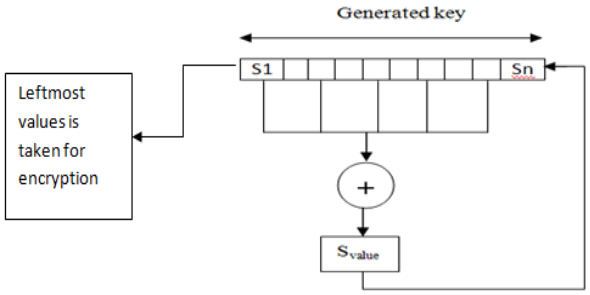

Figure 3: Key usage for encryption

5.2 Data Modification

In this technique the amount of data that can be hidden in the cover image can be increased. In addition, to increase data protection this technique has a built in encryption technique. 24 bit color image will be used as the cover image where 8 bit each will represent three basic colors Red Green and Blue. The embedding operation will be done on the basis of bit wise message embedding technique. Every characters of the message will be treated with their 8-bits ASCII codes, and then the codes will be converted to 5-bits code using MLSB technique [8]. Then the 5bit code will be embedded in the LSB of the image using LSB method. When we look for ASCII representation we can note that, small letter character representation (hexadecimal)will be in the range from 61h to 7Ah, capital letter character will be in the range from 41h to 5Ah and the number ranges from 30h to 30h.

In the case of small letter if the binary representation of it is considered of last four bits, it will be "0110" or "0111". For capital letter the last four bits will be "0100" or "0101". As we can see the last three bits are identical so we can discard them. For numbers last 4 bits will be same so it can be represented using a single bit. So the last 3 bits can be discarded. In this way each character can be represented using 5 bits.
In order to distinguish between small letter, capital letter, numbers and special character a control symbol can be used that defines the state of next character. To perform that we use control symbol that can define the state of next character. The control symbols will also be 5-bits. In 5 bit representation if fifth bit of the character is 1, then the first four bits of that character will lie in the range from 10h to 1Fh. 1Bh to 1Fh will not be used for any character representation. Hence these unused characters will be used to represent the control symbols. Control symbols will be small letter, capital letter, space, numbers and end of text which will be represented using 1Bh, 1Ch, 1Dh, 1Eh and 1Fh respectively. Then the binary representation of these hex values will be stored in the LSB of the image.

The following steps are carried out by the receiver to retrieve the data or the image. This retrieval will be based on the key available with the receiver. If the receiver has the data extraction key, he or she can obtain only the data that is embedded inside the image. If the receiver has only the encryption key, he or she can retrieve only the image. If receiver has both the keys, he or she can retrieve both data as well as the image.

5.3 Data Modification

The original image is encrypted using the encryption key. The encrypted data will be used for data embedding. In Ordinal Virtual Embedding actual embedding will not be carried out. Here ordinal indicates the location of the pixels where there will be a match with the data. At each pixel the data will be virtually embedded based on the bit values of the data and the LSB bit of the pixel. If the LSB bit of the pixel and the bit value of the data match, it is indicated that the embedding of the data is done in that pixel of the encrypt image. The indication of the ordinal value of the pixel where data is virtually embedded will be noted in a separate location and that will be considered as the key for retrieving the data at the receiver. For the security purpose it can even be encrypted and then sent to the receiver. If there is a mismatch, go for the next pixel for virtual embedding. Repeat the same until the end of the file is reached. At the end a Stego image will be produced and it will be sent to the receiver.
In the example the original data considered is "Hai". Its representation after data modification is shown below.

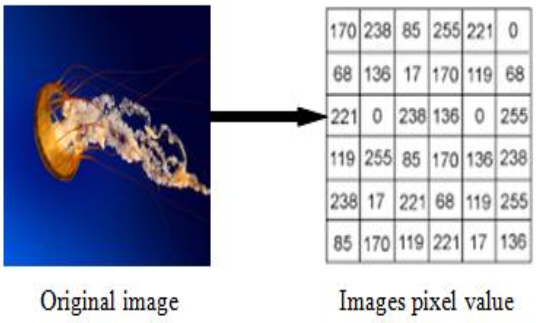

Figure 4: The original data and its pixel value

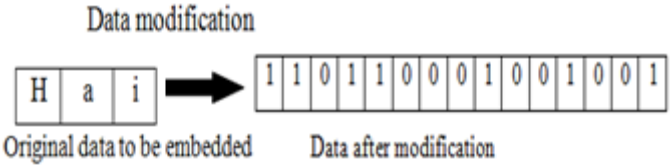

Figure 5: Data after modification

Algorithm
1. Read the input image and input from data modification stage.
2. Read the RGB values of the each pixel of the image.
3. Compare the LSB bit of the pixels with the bit value of the data.
4. If matched read the location where it is matched which will be the data extraction key
Else
Try to find the match of data bits with the LSB bits of the pixels
5. Finally obtain data extraction key which will be locations of the pixel where the data bits are present.

5.4 Image Recovery

At the receiver side, if encryption key is available, the original image can be decrypted using the encryption key.

Sender sends the encryption key to the receiver. The key will be used as the input seed value for feedback shift register. This seed value is used to generate a pseudorandom number which is then added with the pixel value of the image and then perform the modulus operation with 256. The value generated will be the new pixel value. The same procedure will be followed for all the pixels of the cover image. Thus the image gets decrypted. The pseudo-random number is generated by performing the subtraction operations on any combination of the numbers in the seed value. The result is placed at the end of the seed value by shifting the seed value to the left.

5.5 Data Extraction

Data extraction will be the reverse process of data embedding. Initially the key which contains the location where the data is present in the encrypted image will be located and the LSB's from that location will be taken. Group the LSB bits into 5 bits. Then check the 5bits with the control symbols i.e. 1B, 1C, 1D and 1E and based on these control symbols reconstruct each character by adding appropriate character values. Finally the original data will be obtained.

6. Results and Analysis

A colored image of dimension 1600x1195 is considered as the cover image for the analysis is as shown in Fig 6(a). After the encryption the image will be as shown in Fig 6(b). Data which has to be embedded will be taken from the file and will be embedded into the encrypted image and a stego image will be produced shown in Fig 6(c). After decryption of the image is done from the stego image the original image will be obtained is shown in Fig 6(d).

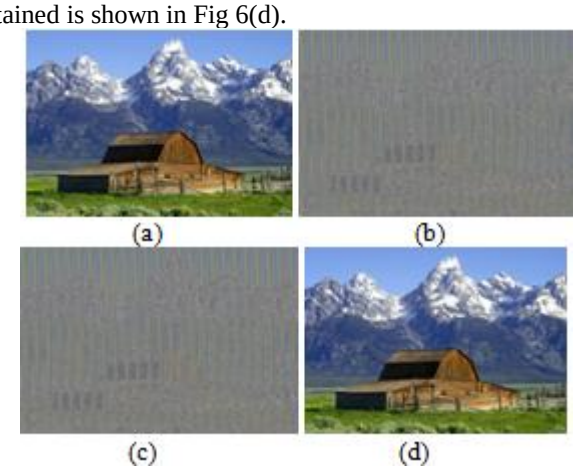

Figure 6: (a)Cover image (b) Encrypted image (c) Stego image (d) Original image

a. Histogram Comparison

The histogram of all the images is shown in the Fig 7

The histogram of the image before encryption and after decryption will be the same which means that the same image will be obtained after decryption and there will be no distortion which will be added. This is shown in Fig 7(a) and (b).

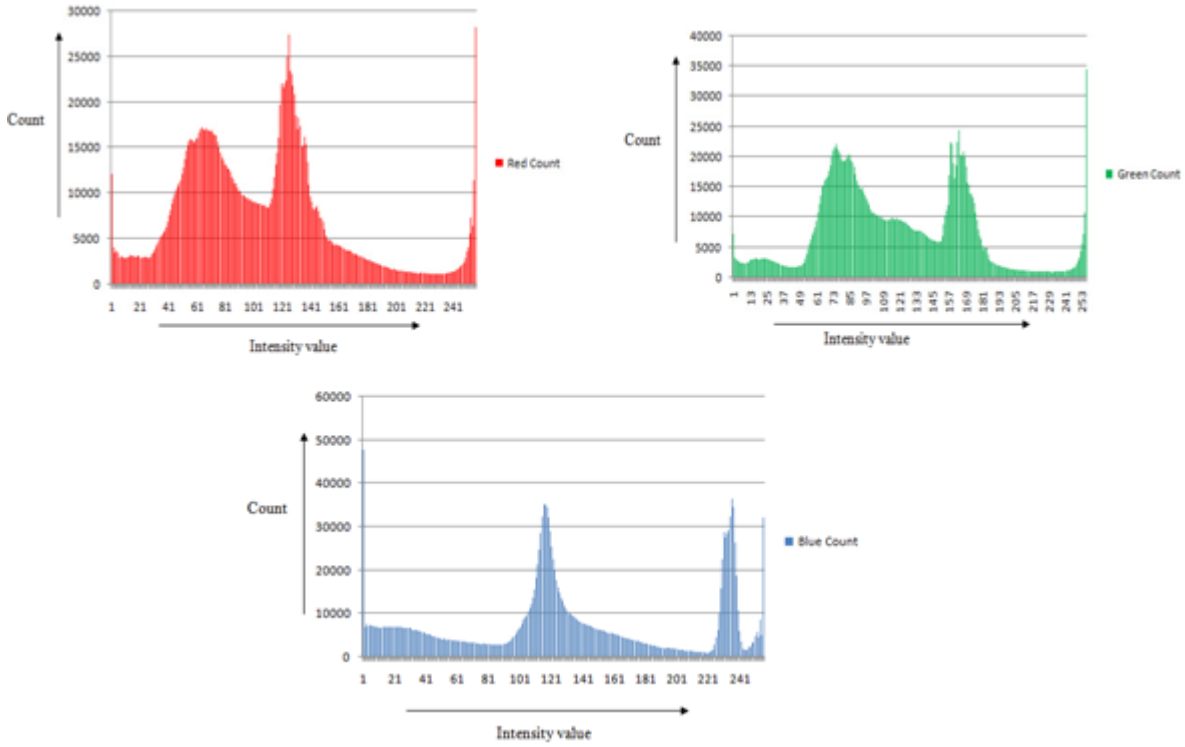

Figure 7(a): Histogram of the RGB component of image

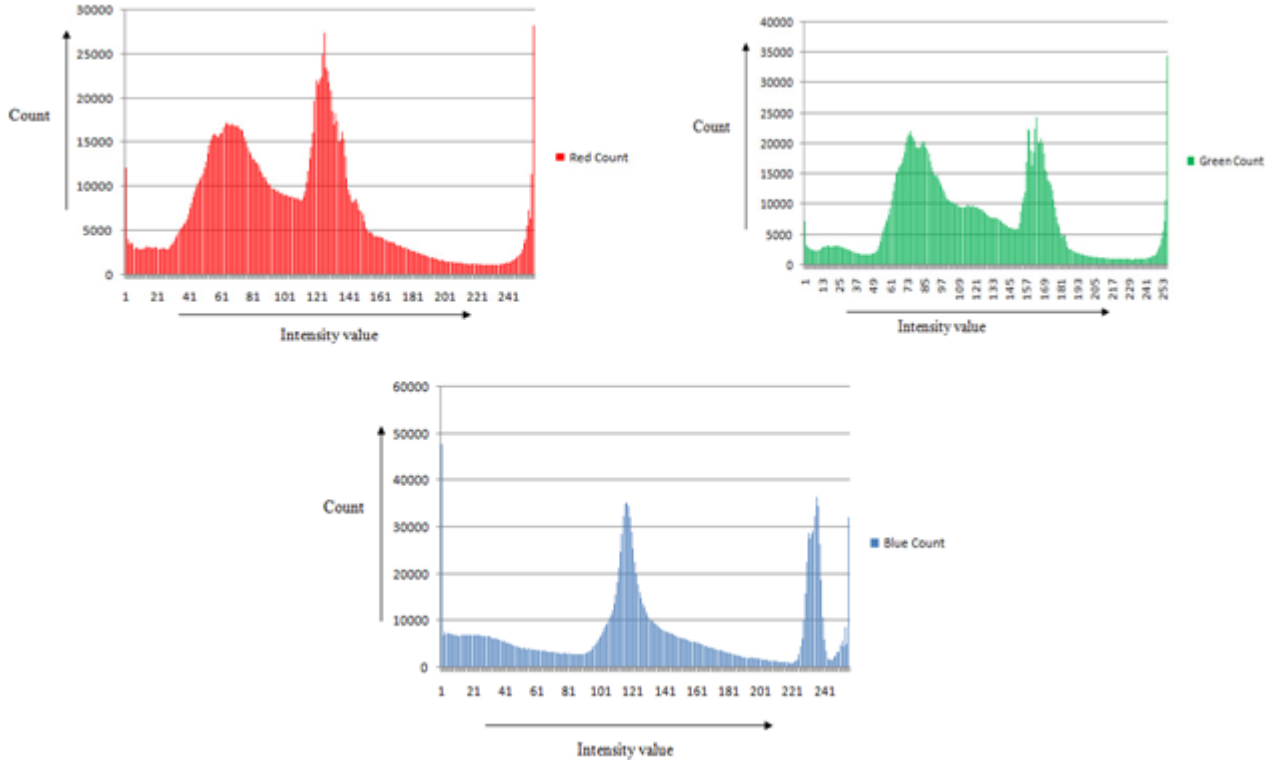

Figure 7(b): Histogram of the RGB component of image after decryption

The histogram of the encrypted and the stego image will be same which indicates that there will be no changes done to the encrypted image after embedded. This will be because virtual embedding. Here we cannot make out that the data is embedded in to the image at all. This is shown in Fig 7(c) and (d).

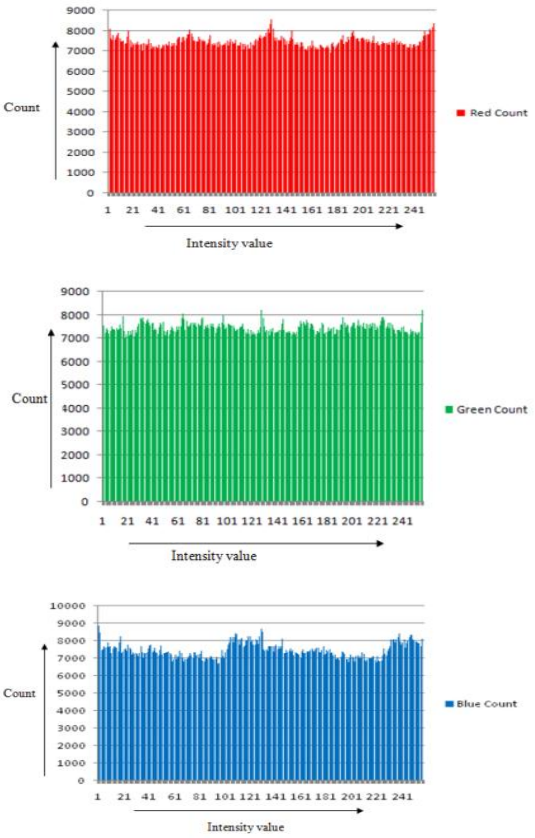

Figure 7(c): Histogram of the RGB component of Encrypted image

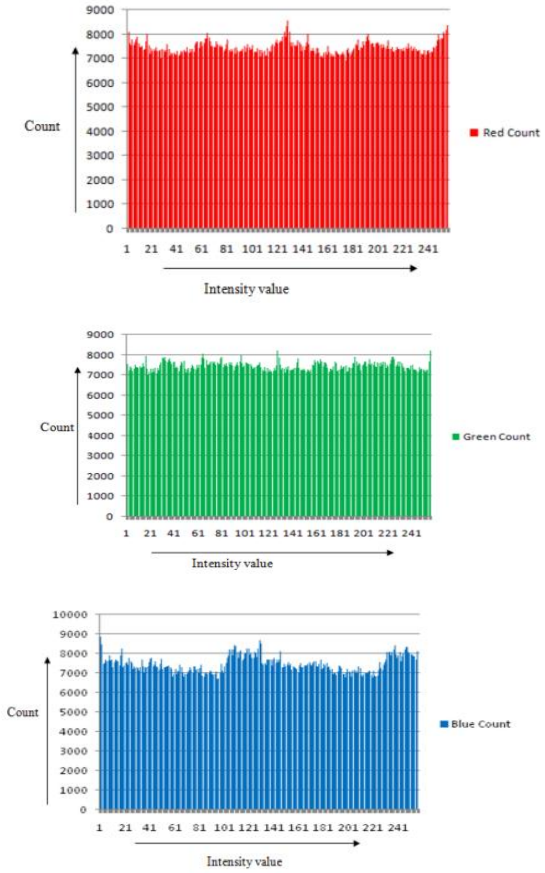

Figure 7(d): Histogram of the RGB component of Stego image

b. Amount of data embedded

Amount of data embedded is calculated by number of bits that is embedded. In the existing method all the 8 bits of each character in the data was used for embedding but, in the

proposed system only the 5 bits of 8 bits will be used for embedding. So there will be the reduction in the number of bits getting embedded. The Fig 8 shows the comparison of the existing and the proposed method for the amount of data getting embedded. In the proposed method there will be best case, average case and the worst case. The best case scenario will be when the data will contain only one type of characters. The average case scenario will be when the data will contain the normal text format. The worst case scenario will be when there will be alternative changes between the characters in the data.

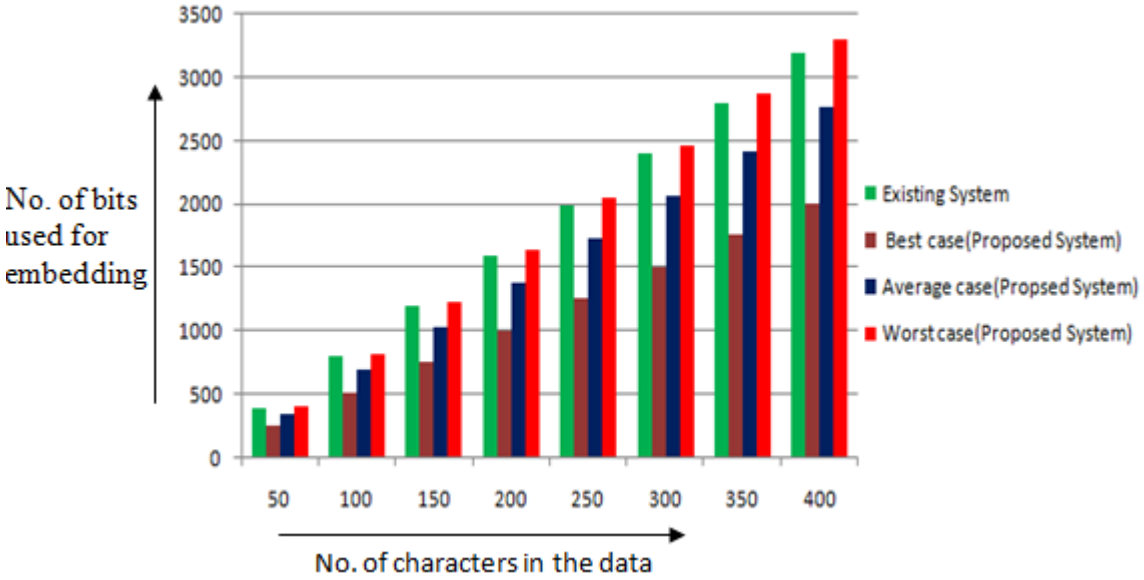

Figure 8: Comparison between the existing and the proposed method for the amount of data embedding

7. Conclusion And Future Scope

In this paper, a new method for Separable Reversible Data Hiding is proposed where virtual embedding will take place and the data bit is modified before embedding. In the first phase, the content owner will encrypt the cover image using the encryption key. Data hider will not know the content of the original image and he will use this encrypted image for embedding the data. Selected data is converted using MLSB technique. The converted data will be embedded into the image using virtual embedding technique. After embedding the data extraction key will be generated and it is encrypted and sent to receiver. At the receiver side if he has only encryption key and the stego image then he can retrieve only the original image. If he has only the data exaction key and the stego image then he can get only the original data from the stego image. If he has both data extraction and encryption key along with stego image then he can get both original image as well as the data. Thus there will be separation at the receiver side and based on the keys available receiver can obtain the information. In this paper only the LSB of the pixel is considered for virtual embedding. Future enhancement can consider LSB's of the RGB component for embedding the data virtually.

8. Acknowledgment

I am very thankful to my guide Mr. Sandeep Kumar S Assistant Professor, Department of Computer Science and Engineering, Mite for his cordial support, valuable information and guidance, to prepare this paper and also thankful to Prof. Dr. Nagesh H R, Head of the Department, Computer Science and Engineering, for his valuable and constructive suggestions during the planning and development of this work.

References

[1] E Thambiraja, G. Ramesh, Dr. R. Umarani," A Survey on Various Most Common Encryption Techniques", International Journal of Advanced Research in Computer Science and Software Engineering, Volume 2, Issue 7, July 2012 ISSN: 2277 128X.
[2] Kshetrimayum Jenita Devi, Dr. Sanjay Kumar Jena, "A Sesure Image Steganography Using LSB Technique and PseudoRandom Encoding Technique ", May 2013.
[3] Zhicheng Ni, Yun-Qing Shi, Nirwan Ansari, Wei Su, " Reversible Data Hiding", IEEE Transactions On Circuits And Systems For Video Technology, Vol. 16, No. 3, March 2006.
[4] Divyani UdayKumar Singh, Kasturi Mohan Padwal, Madhura Pundlik Jadhav," Separable Reversible Data Hiding in Image Using Advanced Encryption Standard with Fake Data Generation", International Journal of Computer Science and Information Technologies, Vol. 5 (3), 2014, 3469-3473.
[5] Divyani UdayKumar Singh, Kasturi Mohan Padwal, Madhura Pundlik Jadhav," Separable Reversible Data Hiding in Image Using Advanced Encryption Standard with Fake Data Generation", International Journal of Computer Science and Information Technologies, Vol. 5 (3), 2014, 3469-3473.
[6] G. Xuan, C. Yang, Y. Zheng, Y. Q. Shi and Z. Ni, "Reversible data hiding based on wavelet spread spectrum," IEEE nternational workshop on multimedia signal processing (MMSP2004), Sept. 2004, Siena, Italy.
[7] C.Anuradha, S.Lavanya,"Secure and Authenticated Reversible Data Hiding in Encrypted Image", International Journal of Advanced Research in Computer Science and Software Engineering, Volume 3, Issue 4, April 2013.

[8] Chaithu V Kumar," Secure RDH for Encrypted Images by Conforming Space before Encryption", International Journal of Research in Advent Technology, Vol.2, No.2, February 2014.
[9] Mazen Abu Zaher," Modified Least Significant Bit (MLSB)", Computer and Information Science, Vol. 4, No. 1; January 2011.

Authors Profile

Shreya M S completed the Bachelor's Degree in Computer Science & Engineering from Visvesvaraya technological University (VTU). Currently pursuing M.Tech degree in Computer Science & Engineering at Mangalore Institute of Technology, Karnataka, India.

Mr. Sandeep Kumar S received Master Degree in computer science and engineering from Canara Engineering College Mangalore. He is currently an Assistant professor in the department of Computer Science and Engineering, Mangalore institute of Technology and Engineering Mangalore, Karnataka India. His research interest area includes Image Processing, Network Security, information Security.