# HIDING THE CONFIDENTIAL MESSAGE INTO THE IMAGE USING BIT PLANE METHOD

**Pooja R*, Santhiya M*, Ms Indra Priyatharshini****
Final Year Students*,Assistant Professor**,
Department of Electronics & Communication Engineering,
Prince Shri Venkateshwara Padmavathy Engineering College ,Chennai 127

## ABSTRACT

Text encryption is process of hiding the text into the image in order to prevent unauthorized persons to gain access to confidential message. In the existing, Reversible Data Hiding in Encrypted Image method (RDHEI), there occurs blurring of images, watermarking, production of errors. In order to avoid these problems, we proposed bit plane method. In this method a image is selected, text is encrypted in a selected bit plane and sent to the receiver. The receiver can decrypt the text only with the help of the secret key. Without knowing the encryption key the text will not be retrieved. Thus there will be no blurring of images, and a clear image with text hidden in it can be retrieved with high speed and security. Fast evaluation of digital data exchange occurs in recent years. Due to that security of information is much important in data storage and transmission process. Security of internet banking account passwords, email accounts password etc. requires text protection in digital media. In the same way image transmission and storage during industrial and research processes requires image protection. This method allows high capacity of data to be hidden inside the grayscale images. The clear image with text hidden in it can be retrieved with high speed and security.

*Keywords*- Reversible Data Hiding in Encrypted Image method (RDHEI), bit plane method, no blurring.

## 1. INTRODUCTION

The term digital image refers to processing of a two dimensional picture by a digital computer. In a broader context, it implies digital processing of any two dimensional data. A digital image is an array of real or complex numbers represented by a finite number of bits. An image given in the form of a transparency, slide, photograph or an X-ray is first digitized and stored as a matrix of binary digits in computer memory. This digitized image can then be processed and/or displayed on a high-resolution television monitor. T Text encryption is process of hiding the text into the image in order to prevent unauthorized persons to gain access to confidential message. In the existing, Reversible Data Hiding in Encrypted Image method (RDHEI), there occurs blurring of images, watermarking, production of errors. In order to avoid these problems, we proposed bit plane method. In this method a image is selected, text is encrypted in a selected bit plane and sent to the receiver. The receiver can decrypt the text only with the help of the secret key. Without knowing the encryption key the text will not be retrieved. Thus there will be no blurring of images, and a clear image with text hidden in it can be retrieved with high speed and security. Fast evaluation of digital data exchange occurs in recent years. Due to that security of information is much important in data storage and transmission process. Security of internet banking account passwords, email accounts password etc. requires text protection in digital media. In the same way image transmission and storage during industrial and research processes requires image protection. This method allows high capacity of data to be hidden inside the grayscale images. The clear image with text hidden in it can be retrieved with high speed and security.

*Keywords*- Reversible Data Hiding in Encrypted Image method (RDHEI), bit plane method, no blurring.

## 1. INTRODUCTION

The term digital image refers to processing of a two dimensional picture by a digital computer. In a broader context, it implies digital processing of any two dimensional data. A digital image is an array of real or complex numbers represented by a finite number of bits. An image given in the form of a transparency, slide, photograph or an X-ray is first digitized and stored as a matrix of binary digits in computer memory. This digitized image can then be processed and/or displayed on a high-resolution television monitor. For display, the image is stored in a rapid-access buffer memory, which refreshes the monitor at a rate of 25 frames per second to produce a visually continuous display.

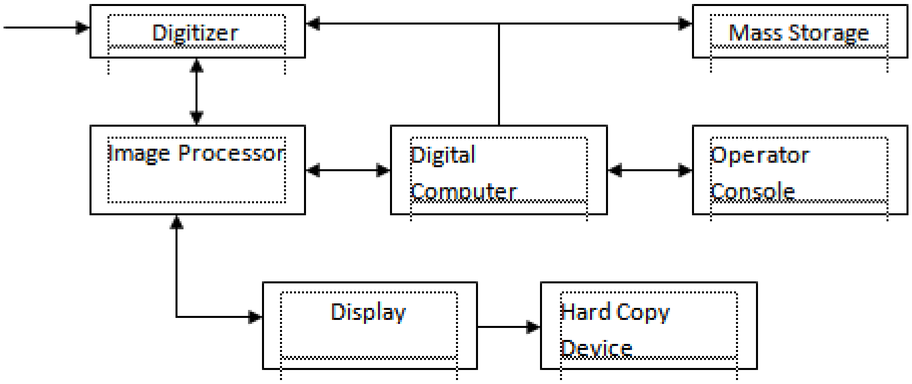

**Figure 1** Block diagram of image processing system

An image processor does the functions of image acquisition, storage, preprocessing, segmentation, representation, recognition and interpretation and finally displays or records the resulting image as in figure 1.1. Image enhancement operations improve the qualities of an image like improving the image's contrast and brightness characteristics, reducing its noise content, or sharpen the details. This just enhances the image and reveals the same information in more understandable image. It does not add any information to it.

Image restoration like enhancement improves the qualities of image but all the operations are mainly based on known, measured, or degradations of the original image. Image restorations are used to restore images with problems such as geometric distortion, improper focus, repetitive noise, and camera motion.

## 2. LITERATURE REVIEW

This system is based on an approach which combines a substitutive watermarking algorithm, the quantization index modulation, with an encryption algorithm: a stream cipher algorithm (e.g., the RC4) or a block cipher algorithm (e.g., the AES in cipher block chaining (CBC) mode of operation) [2]. A systematic development of watermarking schemes is desirable, but at present, their development is usually informal, ad hoc, and omits the complete realization of application scenarios. This practice not only hinders the choice and use of a suitable scheme for a watermarking application, but also leads to debate about the s tate-of-the-art for different watermarking applications. With a view to the systematic development of watermarking schemes, we present a formal generic model for digital image watermarking [3].

Then, a data-hider may compress the least significant bits of an encrypted image using a data-hiding key to create a sparse space to accommodate some additional data. With an encrypted image containing an additional data, if a receiver has a data-hiding key, he can extract the additional data though he does not know the image content. If the receiver has an encryption key, he can decrypt the received data to obtain an image similar to the original one, but cannot extract the additional data. If the receiver has both the data-hiding key and the encryption key, he can extract the additional data and recover the original content without any error by exploiting the spatial correlation in natural image and the amount of additional is not too large [4].

Our work utilized the correlation between image pixels better to solve the inherent contradiction between payload and distortion rate in the state-of-the-art data hiding algorithms[5]. At the sender side the data/message is embedded in the image to hide the data. Then at the receiving end, the extraction of the data is performed from the image and the original image is restored. neighbouring pixels are strongly correlated and the difference is expected to be very close to zero for most of the pixels. This can cause a prominent maximum in the histogram of the difference image, which can ultimately result in high data embedding capacity[7].

A permutation process utilized two affine modular maps to get two index order sequences for the shuffling of image pixel positions, while a diffusion process employed another two affine modular maps to produce two pseudo-random gray value sequences for a two-way diffusion of gray values. Liu and Tian [6] proposed algorithm to encrypt images using color map and spatial chaos at the bit level flipping (SBLP). First, the algorithm used the logistic chaos sequence to shuffle the positions of image pixels and then to convert them into a binary matrix component including red, green and blue at one time, rather than the order of the matrix as well as at the level prior to appointment of scrambling bit that has been created by SBLP. Second, the logistics rearranged the chaotic sequence for [1].

The image is stored in a rapid-access buffer memory, which refreshes the monitor at a rate of 25 frames per second to produce a visually continuous display.

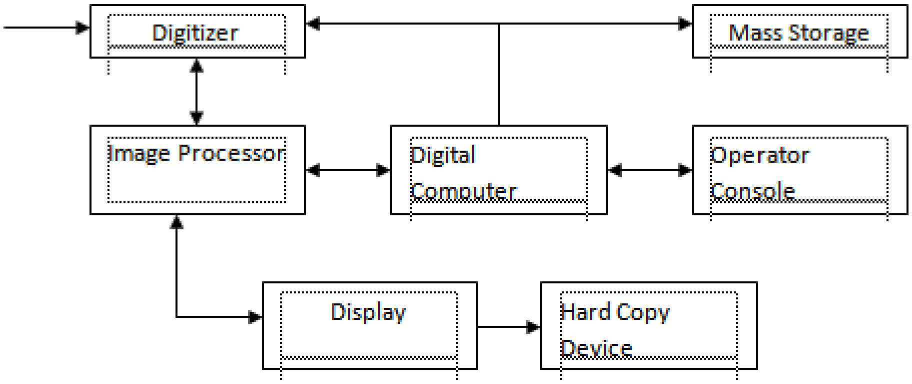

**Figure 1** Block diagram of image processing system

An image processor does the functions of image acquisition, storage, preprocessing, segmentation, representation, recognition and interpretation and finally displays or records the resulting image as in figure 1.1. Image enhancement operations improve the qualities of an image like improving the image's contrast and brightness characteristics, reducing its noise content, or sharpen the details. This just enhances the image and reveals the same information in more understandable image. It does not add any information to it.

Image restoration like enhancement improves the qualities of image but all the operations are mainly based on known, measured, or degradations of the original image. Image restorations are used to restore images with problems such as geometric distortion, improper focus, repetitive noise, and camera motion.

## 2. LITERATURE REVIEW

This system is based on an approach which combines a substitutive watermarking algorithm, the quantization index modulation, with an encryption algorithm: a stream cipher algorithm (e.g., the RC4) or a block cipher algorithm (e.g., the AES in cipher block chaining (CBC) mode of operation) [2]. A systematic development of watermarking schemes is desirable, but at present, their development is usually informal, ad hoc, and omits the complete realization of application scenarios. This practice not only hinders the choice and use of a suitable scheme for a watermarking application, but also leads to debate about the state-of-the-art for different watermarking applications. With a view to the systematic development of watermarking schemes, we present a formal generic model for digital image watermarking [3].

Then, a data-hider may compress the least significant bits of an encrypted image using a data-hiding key to create a sparse space to accommodate some additional data. With an encrypted image containing an additional data, if a receiver has a data-hiding key, he can extract the additional data though he does not know the image content. If the receiver has an encryption key, he can decrypt the received data to obtain an image similar to the original one, but cannot extract the additional data. If the receiver has both the data-hiding key and the encryption key, he can extract the additional data and recover the original content without any error by exploiting the spatial correlation in natural image and the amount of additional is not too large [4].

Our work utilized the correlation between image pixels better to solve the inherent contradiction between payload and distortion rate in the state-of-the-art data hiding algorithms[5]. At the sender side the data/message is embedded in the image to hide the data. Then at the receiving end, the extraction of the data is performed from the image and the original image is restored. neighbouring pixels are strongly correlated and the difference is expected to be very close to zero for most of the pixels. This can cause a prominent maximum in the histogram of the difference image, which can ultimately result in high data embedding capacity[7].

A permutation process utilized two affine modular maps to get two index order sequences for the shuffling of image pixel positions, while a diffusion process employed another two affine modular maps to produce two pseudo-random gray value sequences for a two-way diffusion of gray values. Liu and Tian [6] proposed algorithm to encrypt images using color map and spatial chaos at the bit level flipping (SBLP). First, the algorithm used the logistic chaos sequence to shuffle the positions of image pixels and then to convert them into a binary matrix component including red, green and blue at one time, rather than the order of the matrix as well as at the level prior to appointment of scrambling bit that has been created by SBLP. Second, the logistics rearranged the chaotic sequence for [1].

## 3. DATA HIDING USING BIT PLANE METHOD

Steganography can be classified into four types. They are 1. Text 2.Image 3. Audio 4. Video.

- Text Steganography: In this type of steganography a very small amount of redundant data, therefore they are most commonly used.
- Audio/Video steganography: They are very complex in use.
- Image steganography**:** It is popularly used steganography for hiding data since it provides a secure and simple way to send the information over the internet. Images are routinely used in diverse areas such as medical, military, science, engineering, advertising, education as well as training. With the increasing use of digital techniques for transmitting and storing images, the fundamental issue of protecting the confidentiality, integrity as well as the authenticity of images has become a major concern.

This paper analyzed the security performance of an image text encryption scheme based on bit-plane extraction. Based on the identified security defects, we proposed efficient known-plaintext and chosen-plaintext attacks for recovering some information of the original plain image. Known- plain attack is an attack where the attacker has a access to both the plain text and its encrypted version. Chosen-plain text attack is an attack which presumes that the attacker can obtain the cipher text for arbitrary plain texts. The goal of the attack is to gain information that reduces the security of the encryption scheme. In general, 8-bit per pixel images are processed. We can slice an image into the 8 bit-planes. Zero is the least significant bit (LSB) and 7 is the most significant bit (MSB).

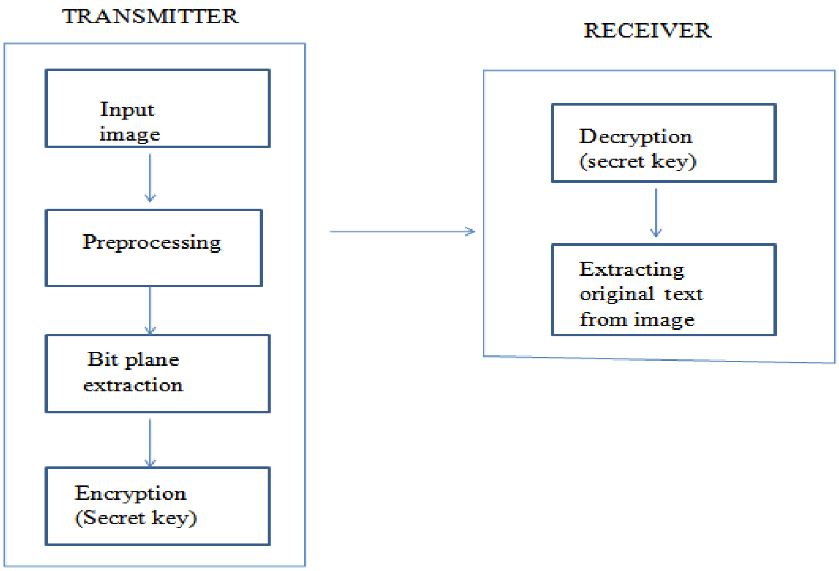

**Figure 1** Block diagram of the data hiding in an image using bit plane method

In figure 1, all the blocks such as input image, preprocessing, bit plane extraction, encryption, decryption and extraction of the original message from the image are explained in detail.

1) PREPROCESSING

Initially, the image is given as input and preprocessing is done. It is done in order to prepare the data for primary processing or for further analysis. Preprocessing is converting the raw data into an understandable format. Real-world data is often incomplete, inconsistent, lacking in certain behaviours or trends, and is likely to contain many errors. Data preprocessing is a proven method for resolving the above mentioned issues.

Let the user select from a list of all the demo images that ship with the Image Processing Toolbox. Image is basically combination of individual pixel (dots) information. When we write that image is of 620 X 480 sizes, it means that image has 620 pixels in horizontal direction and 480 pixels in vertical direction. So, altogether there are 620 X 480 pixels and each pixel contains some information about image.

The aim of pre-processing is an improvement of the image data that suppresses unwanted distortions. It enhances some image features important for further processing. Neighboring pixels corresponding to one object in real images have essentially the same or similar brightness value. Thus distorted pixel can often be restored as an average value of neighboring pixels.

2)BIT PLANE EXTRACTION

- Least Significant Bit-planes (LSBP)
- Most Significant Bit-planes (MSBP)

Then, bit plane extraction is performed. A bit plane of a digital discrete signal (image) is a set of bits corresponding to a given bit position in each of the binary numbers representing the signal. The input image is sliced into different bit planes which consists of 8 bits per pixels. Plane 1 contains the lowest order bit of all the pixels in the image. And plane 8 contains the highest order bit of all the pixels in the image. The secret data is hidden into any of the selected bit plane of the input image.

An 8-bit plain-image, which is denoted by I , can be extracted as eight binary bit-planes I1; I2;-----; I8, and each binary bit plane contains one bit information of the image. Binary matrixes I1, I2, I3, and I4 represent the least significant bits planes (LSBPs). In contrast, matrixes I5, I6, I7, and I8 represent the MSBPs . Every bit plane is different in terms of the amount of contained visual information.

3) ENCRYPTION

Encryption, is a process that encodes a message or file so that it can be only be read by certain people. Encryption uses a algorithm to scramble, or encrypt data and then uses a key for the receiving party to unscramble, or decrypt the information.

## 4) DECRYPTION

The conversion of encrypted data into its original form is called decryption. It is generally a reverse process of encryption . It decodes the encrypted information so that an authorized user can only decrypt the data because decryption requires a secret key or password. Decryption is the process of taking encoded or encrypted text or other data and converting it back into text that you or the computer can read and understand.

## 4. RESULTS AND DISCUSSION

Initially a colour image is taken. It is converted into gray scale image. A gray scale image is simply one in which the only colours are shades of gray.The reason for differentiating such images from any other sort of colour image is that less information needs to be provided for each pixel. A gray scale image is chosen from the image processing tool box. Once the gray scale image is being selected, any text of our choice can be entered. Here the bit plane can be divided into eight different planes. The text can be hidden in any one of the plane from 1 to 8. The pixel value depends upon the size of the image. According to the pixel value of the image, the message can be hidden. That is, the text can be entered until the bit plane becomes full. Since pixel value of gray scale image lies between 0 -255, so its information is contained using 8 bit. So, we can divide that image into 8 planes (8 Binary Image). Binary image are those images whose pixel value can be either 0 or 1. So, our task is to extract each bit planes of original image to make 8 binary images. Hence the bit planes, from 1 to 8 can be entered in the appearing box.

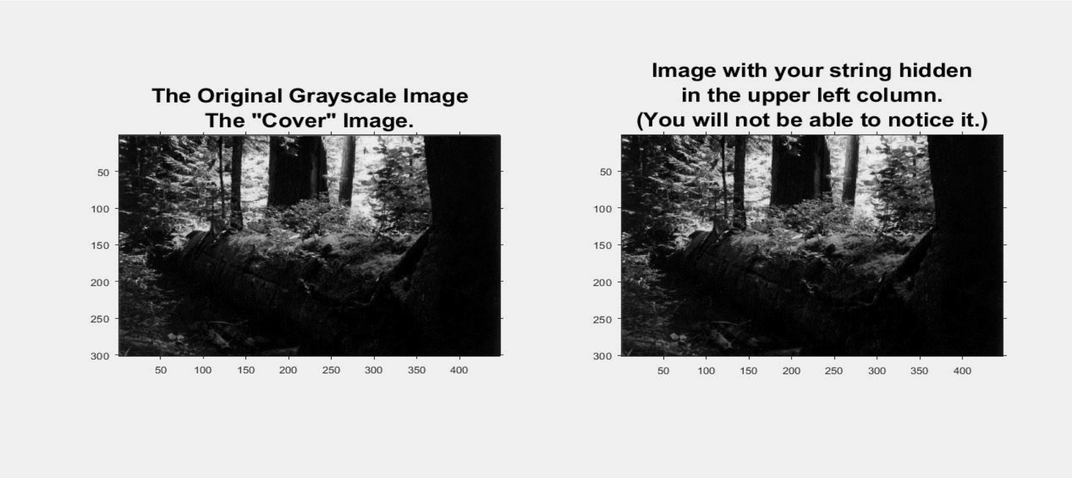
The Original Grayscale Image
The "Cover" Image.
Image with your string hidden
in the upper left column.
(You will not be able to notice it.)
50
100
150
200
250
300
50
100
150
200
250
300
350
400

**Figure 2** Text gets hidden into the image

In the figure 2, the secret message entered by the sender gets hidden into the image.

Now, the text which was being entered gets encrypted into the selected image. The encrypted image looks similar to the original image before encryption. There will be no blurring of image. A secret key is being set by the transmitter. The receiver can decrypt the text which is hidden into the image only with the help of the secret key. The secret keys which were set by the sender must be added and entered as the decryption key. This aids in safe and secure transmission of the message. Once the receiver enters the correct secret key, the original text can be retrieved from the image. If the receiver enters the wrong key, the text hidden into the image cannot be retrieved.

In the table 1, the correlation value of the Reversible data hiding in encrypted images and bit plane method are displayed.

| Correlation of Reversible data hiding in encrypted images method | Correlation of bit plane method |
|---|---|
| 0.1-0.2 | 0.8-0.99 |

**Table 1** Comparison of reversible data hiding in encrypted images and bit plane method

## 5. CONCLUSION

As the internet has become the medium for transferring the sensitive information, the security of the transferred message has become the utmost priority. In the existing, they used Reversible Data Hiding in Encrypted Image method, there occurs blurring of images, watermarking, production of errors. In order to avoid these problems, we proposed bit plane method. This method allows high capacity of data to be hidden inside the grayscale images. One of the major requirements of this method is to send the secret message, inside the image without creating much difference to the original image. Our technique fulfills this requirement to a higher extent. A particular grayscale image is selected and the text is encrypted in a selected bit plane and sent to the receiver. The receiver can decrypt it with the help of the secret key. Without knowing the encryption key the text will not be retrieved. The clear image with text hidden in it can be retrieved with high speed and security. So, there will be no blurring of image, and it will not be suspicious to hijackers. Our system has a correlation value which is 0.999 which is greater than the existing system. In future, we can enhance by using forthcoming algorithm for greater accuracy.

## REFERENCES

[1] Data hiding in virtual bit plane using efficient Lucas number sequences by Biswajita Datta, Koushik Datta, Sudipta Roy, May 2020.

[2] A Joint Encryption/Watermarking System for Verifying the Reliability of Medical Images Dalel Bouslimi, Member, IEEE, Gouenou Coatrieux, Member, IEEE, Michel Cozic, and Christian Roux, Fellow, IEEE.,VOL. 16, NO. 5, SEPTEMBER 2012.

[3] Secure and robust image steganography using reference image as key by Giridhar Maji, Sharmistha and Mandal, May 2019.

[4] Digital image watermarking: its formal model, fundamental properties and possible attacks Hussain Nyeem1*, Wageeh Boles2 and Colin Boyd2,3., Nyeem et al. EURASIP Journal on Advances in Signal Processing 2014, 2014:135.

[5] A new method of image steganography using 7 bit of a pixel as indicator by introducing the successive temporary pixel in a grayscale image, Kamaldeep Joshi, August 2019.

[6] K. Katzner, The Languages of the World. Evanston, IL, USA: Routledge, 2002. [7] Steganographic techniques classification according to image format by Khaldi Amine, June 2019.

[8] Prudently Secure Information Theoretic LSB Steganography for Digital Grayscale Images Khan Farhan Rafat Riphah Institute of Systems Engineering (RISE) Islamabad, Pakistan, 2020.

[9] H.-C. Lin, C.-N. Yang, C.-S. Laih, and H.-T. Lin, ``Natural language letter based visual cryptography scheme,'' J. Vis. Commun. Image Represent, May 2019.

[10] J. Nantel and E. Glaser, ``The impact of language and culture on per- ceived website usability,'' J. Eng. Technol. Manage., vol. 25, nos. 12, pp. 112122, 2008.

[11] Image encryption based on Independent Component Analysis and Arnold's Cat Map Nidaa AbdulMohsin Abbas University of Babylon,Iraq, May 2015.

[12] J. Ramya and B. Parvathavarthini, ``An extensive review on visual cryptog- raphy schemes,'' in Proc. Int. Conf. Control, Instrum., Commun. Comput. Technol., Kanyakumari, India, Jul. 2014, pp. 223228.

[13] S. A. Sattar, S. Haque, M. K. Pathan, and Q. Gee, "Implementation challenges for Nastaliq character recognition," in Proc. Int. Multi Topic Conf., Germany,2008.

[14] Hiding in encrypted images: a three tier security data hiding technique Shabir A. Parah1 · Javaid A. Sheikh1 · Umer I. Assad2 · Ghulam M. Bhat1., Received: 19 August 2014 / Revised: 13 August 2015 / Accepted: 27 August 2015.

[15] R. G. Sharma, ``Visual cryptographic techniques for secret image shar- ing: A review,'' Inf. Secur. J., Global Perspective, vol. 27, nos. 56, pp. 241259, Jan. 2019.