



HIGH CAPACITY REVERSIBLE DATA HIDING IN ENCRYPTED IMAGES

Dr. K.Murugesan¹, Y.Karthikeyan²
¹Professor, ²M.E Student

^{1,2}Department of Electronics & Communication Engineering
^{1,2}Easwari Engineering College, India

ABSTRACT

Reversible Data Hiding in Encrypted Images (RDHEI) is an effective technique to embed data in the encrypted domain.. In this work, we propose a new reversible method based on MSB (most significant bit) prediction with a very high capacity. We present two approaches, these are: High Capacity Reversible Data Hiding approach with Correction of Prediction Errors (CPE-HCRDH) and High Capacity Reversible Data Hiding approach with Embedded Prediction Errors (EPE-HCRDH).
Keywords: RDHEI, MSB, LSB, CPE-HCRDH, EPE-HCRDH

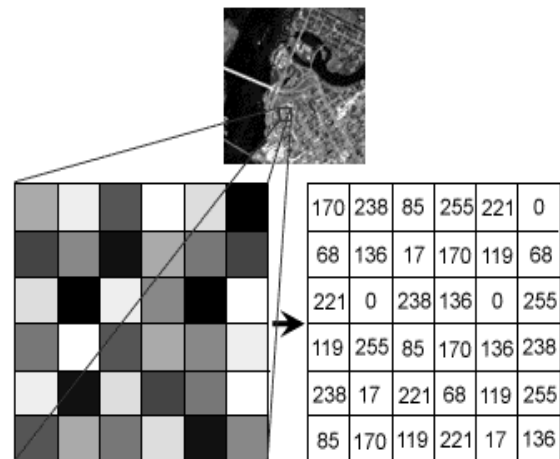
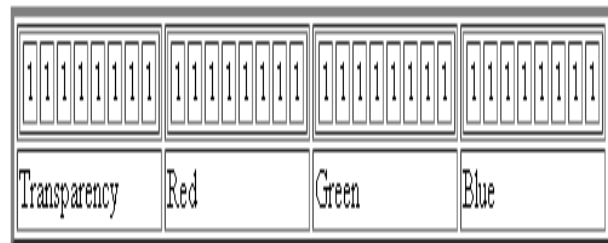


Fig 1.1 Pixel Measurement

Table 1.1 Pixel Colour Table



I. INTRODUCTION:

1.1 IMAGE

An image is a two-dimensional picture, which has a similar appearance to some subject usually a physical object or a person such as a photograph, as well as a three-dimensional, such as a statue. They may be captured by optical devices—such as cameras, mirrors, lenses, telescopes, microscopes, etc. and In this wider sense, images can also be rendered manually, such as by drawing, painting, carving, rendered automatically by printing or computer graphics technology, or developed by a combination of methods, especially in a pseudo-photograph which is shown in figure 1.1

1.1.1 Image File Size:

Image file size is expressed as the number of bytes that increases with the number of pixels. An image, and the colour depth of the pixels colours, the latter known as true colour.

1.2 Raster Formats:

These formats store images as bitmaps (also known as pixel map). In computer graphics, the raster graphics or bitmap image is a dot matrix data structure that represents a generally rectangular grid of pixels (points of colour),viewable via a monitor,paper, or other display medium. Raster images are stored in image files with varying formats. This is studied from [2].

1.3 VECTOR FORMATS

As opposed to the raster image formats above (where the data describes the characteristics of each individual pixel), vector image formats contain a geometric description which can be rendered smoothly at any desired display size.

This is studied from [2] However, vector images can be displayed with analog CRT technology such as that used in some electronic test equipment, medical monitors, radar displays, laser shows and early video games. Plotters are printers that use vector data rather than pixel data to draw graphics.

1.4 IMAGE PROCESSING:

Digital Image Processing, the manipulation of images by computer, is relatively recent development in terms of man's ancient fascination with visual Digital Image Processing like other glamour fields, suffers from myths, dis-connect ions, dis-understandings and dis-information.

. It is truly multidisciplinary endeavour ploughed with imprecise jargon. This is studied from [5].

II. LITERATURE SURVEY

In the paper titled "PROTECTION AND RETRIEVAL OF ENCRYPTED MULTIMEDIA CONTENT", in the year (2007) by Zekeriya erkin

In each domain, state-of-the-art algorithms are described. Finally, the study discusses the challenges and open issues in the field of secure signal processing.

In another paper by (Ashwin Swaminathan) "ENABLING SEARCH OVER ENCRYPTED MULTIMEDIA DATABASES", in the year (2009)

Here, the authors have discussed regarding performance information retrieval tasks while preserving data confidentiality is a desirable capability when a database is stored on a server maintained by a third-party service provider. This paper addresses the problem of enabling content-based retrieval over encrypted multimedia databases. Search indexes, along with multimedia documents, are first encrypted by the content owner and then stored onto the server. Through jointly applying cryptographic techniques, such as order preserving encryption and randomized hash functions, with image

processing and information retrieval techniques, secure indexing schemes are designed to provide both privacy protection and rank-ordered search capability.

In the paper titled "USER-FRIENDLY RANDOM-GRID-BASED VISUAL SECRET SHARING", by (Kai-Hsiang Tsao) in the year (2011)

Recently, the Visual Secret Sharing (VSS) technique is based on a Random-Grid algorithm (RGVSS), proposed by Kafri and Keren, has drawn attention in academia again. However, Kafri and Keren's scheme is not participant-friendly; that is to say, the generated shared images are meaningless, so users feel that this huge amount of data is hard to manage. Those friendly VCVSS schemes are not directly suitable for RGVSS. Instead, a new friendly RGVSS must be designed. Most friendly VCVSS schemes worsen the pixel expansion problem, in which the size of shared images is larger than that of the original secret image, to achieve the goal of generic meaningful shares. As a result, in this paper we have focused on proposing a novel RGVSS scheme by skillfully designing a procedure of distinguishing different light transmissions on shared images based on the pixel values of the logo image with two primary advantages: no pixel expansion, and being user-friendly. In order to illustrate the correctness, the formal analysis is demonstrated while the experimental results show the proposed schemes do work.

III. METHODOLOGY

3.1 EXISTING METHOD

The encryption and decryption using DWT (Discrete Wavelet Transform) and RGB (Red, Green, Blue) pixel shuffling with steganography by using Hash-Least Significant Bit (HLSB) that make use of hash function to develop significant way to insert data bits in LSB bits of RGB pixels of cover image. Cryptography recently includes using advanced mathematical procedures in encryption and decryption techniques. Cipher algorithms are becoming more complex daily. Asymmetric key encryption algorithms the keys used for encryption and decryption must be different.

3.1.1 DISADVANTAGES:

The disadvantages of the existing methods are,

1. More complex.

2. Less accuracy.
3. Low PSNR and MSE.
4. Less secure
5. False sense of security
6. Computation difficulty

3.2 PROPOSED METHOD:

Image encryption algorithms and hiding algorithms should be designed to enhance the effectiveness of transmission and keep safety from attacks by the intruders. The proposed method can achieve the highest level of data integrity, confidentiality and security. The confidentiality of grey scale image that makes uses of pixel shuffling and DWT stream cipher for cryptography and Hash-LSB for steganography are verified. The main function of the pixel shuffling is that it involves no modification in the bit values and no expansion of pixels in the end of the encryption and the decryption procedure. The pixel values are redesigned and combined moving from their particular positions and then the values are swapped to give the cipher image which becomes recognizable.

3.2.1 Advantages

The advantages of proposed system are:

1. The proposed method can achieve the highest level of data integrity, confidentiality and security.
2. More accurate compared to existing method
3. High PSNR and MS than previous existing method

3.3 ALGORITHM DESCRIPTION:

3.3.1 DWT Algorithm

- A discrete wavelet transform (DWT) is any wavelet transform for which the wavelets are discretely sampled.
- As with other wavelet transforms, a key advantage it has over Fourier transforms is temporal resolution
- It captures both frequency and location information (location in time).
- Wavelets are often used to denote noise two dimensional signals, such as images
- Wavelets, by contrast, have both frequency and location. Rather than differing in frequency, they differ in location — the third is nonzero over the first two elements, and the fourth is nonzero over the second two elements.

IV. RESULT AND DISCUSSIONS

The input image is the secret image in the fig 4.1. This image is hidden using the cover image. In this graph both the X-axis and Y-axis are pixels. This input image is encrypted using cover image. The extracted image is called payload. Now the secret image and extracted image is compared the extracted image has less loss of pixels compared to input image which is very less which can be ignored.

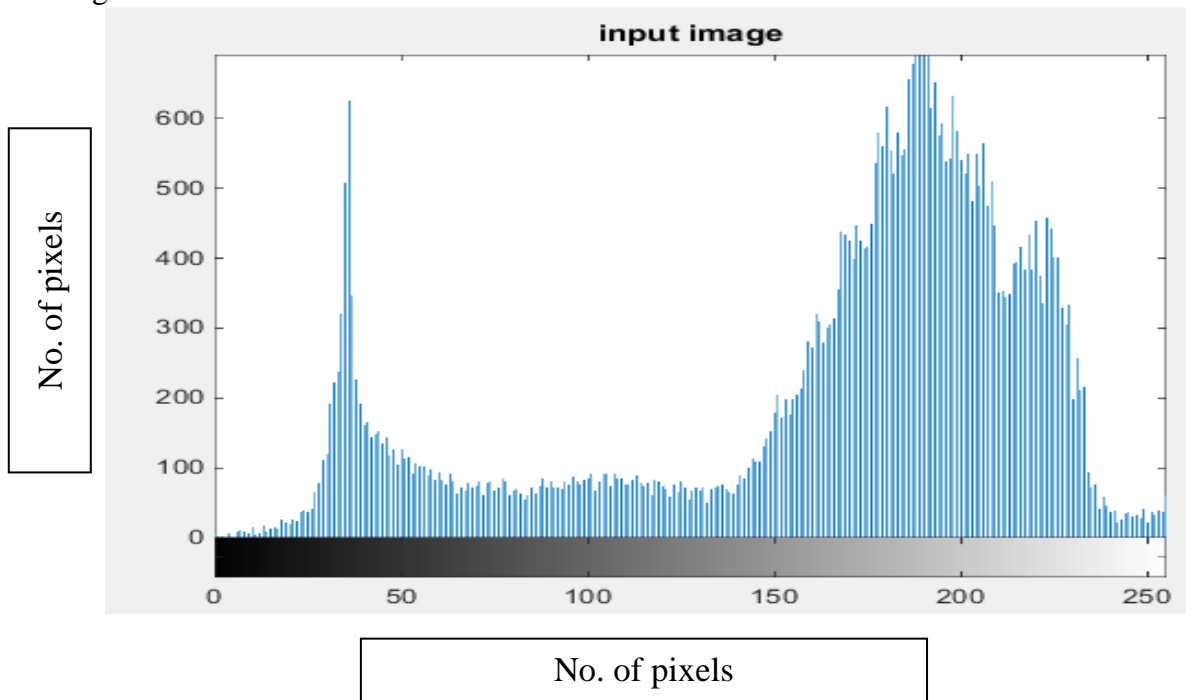


Fig 4.1

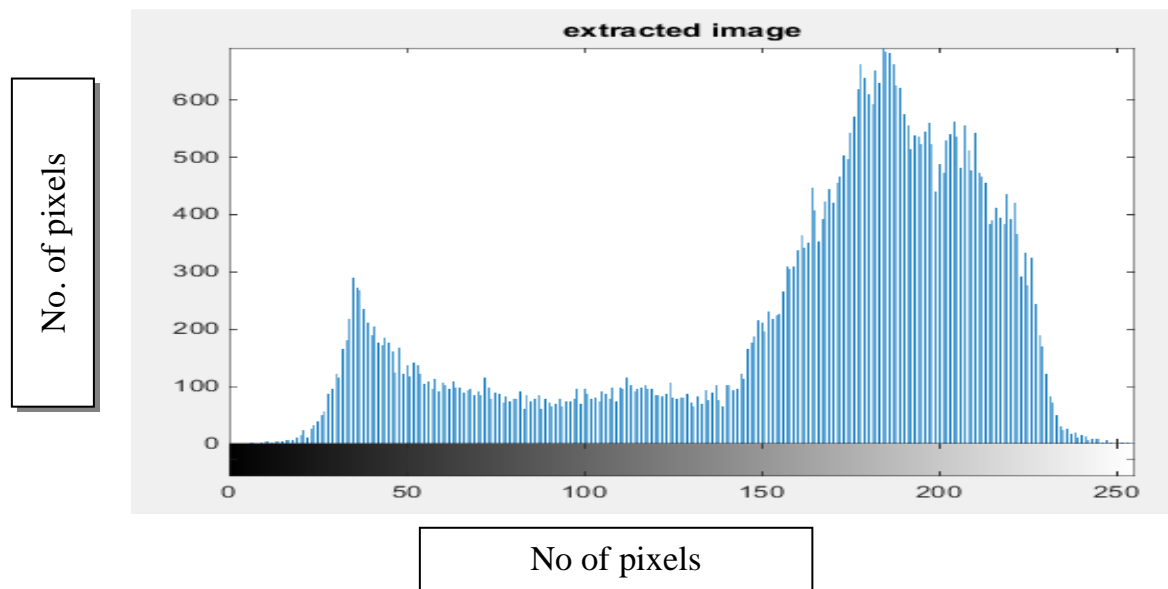


Fig 4.2

The extracted image is reversed image which is shown in fig 4.2 The extracted image when compared with input image the pixel loss is there it is very less compare to the input. The extracted image is also called payload which is 1bit per pixel is achieved in this work.

V.CONCLUSION:

The usage of secret image serves the purpose of encryption, and DWT, watermarking, LSB and MSB algorithm help in improving the hiding capacity. The advantage of using DWT over other transforms, is that it offers a temporal resolution. This algorithm is also stronger and robust as well as secure compared to other algorithms. No visual defects can be observed from the corresponding stego images. It can also be referred to devise new algorithms on ways to send different language secret texts or images in audio as well as video files with more dynamicity.

REFERENCES:

- [1] S. Li, G. Chen, and X. Mou, "On the dynamical degradation of digital piecewise linear chaotic maps," *International Journal of Bifurcation and Chaos*, vol. 15, no. 10, pp. 3119–3151, 2005.
- [2] T.-H. Chen and K.-H. Tsao, "User-friendly random-grid-based visual secret sharing," *IEEE Transactions on Circuits and Systems for Video Technology*, vol. 21, no. 11, pp. 1693–1703, 2011.
- [3] X. Gao, L. An, Y. Yuan, D. Tao, and X. Li, "Lossless data embedding using generalized statistical quantity histogram," *IEEE Transactions on Circuits and Systems for Video Technology*, vol. 21, no. 8, pp. 1061–1070, 2011.
- [4] C.-Y. Hsu, C.-S. Lu, and S.-C. Pei, "Image feature extraction in encrypted domain with privacy-preserving SIFT," *IEEE Transactions on Image Processing*, vol. 21, no. 11, pp. 4593–4607, 2012.
- [5] W. Hong, T.-S. Chen, and H.-Y. Wu, "An improved reversible data hiding in encrypted images using side match," *IEEE Signal Processing Letters*, vol. 19, no. 4, pp. 199–202, 2012.
- [6] Q. Kester, "A Cryptographic Image Encryption Technique based on the RGB Pixel Shuffling," *International Journal of Advanced Research in Computer Engineering & Technology*, vol. 2, no.2, pp.848-854, 2013.
- [7] P. R. Deshmukh and B. Rahangdale, "Hash Based Least Significant Bit Technique for Video Steganography", *Int. Journal of Engineering Research and Applications*, vol. 4, no. 1, pp. 44–49, 2014.
- [8] P. Korshunov and T. Ebrahimi, "Scrambling-based tool for secure protection of JPEG images," in *Image Processing (ICIP), 2014 21th IEEE International Conference on*, 2014, pp. 3423–3425