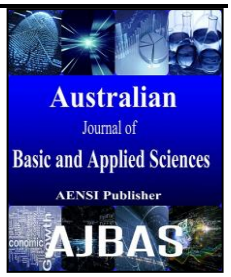
ISSN:1991-8178

Australian Journal of Basic and Applied Sciences

Journal home page: www.ajbasweb.com



Improved Image Steganography using Huffman encoding and LSB

[1]Rajesh G.R. and [2]Dr.Shajin Nargunam A.

[1] *Research Scholar, Noorul Islam University, Thuckalay, Tamil Nadu, India*
[2] *Professor, CSE, Noorul Islam University, Thuckalay, Tamil Nadu, India,*

ARTICLE INFO

Article history:
Received 20 January 2015
Accepted 02 April 2015
Published 20 May 2015

Keywords:
Steganography cryptography
Huffman encoding data hiding
LSB PSNR

ABSTRACT

In the present world information transmission and sharing has increased tremendously the same time unauthorized access and interception are also increased by same amount. Cryptography and Steganography are two major techniques for transfer of information in a secure, indiscernible, robust and in more protected form. In this paper a novel algorithm is introduced by changing the secret image into compressed codes using Huffman encoding and these codes are embedded into the LSB part of the cover image in a random manner. By using these two techniques the security of secret data is enhanced by two tiers and a stego image of high quality is obtained. Experimental results establish that the proposed method leads a considerable improvement in PSNR and the secret image is retrieved without any loss of information.

To Cite This Article: Rajesh G.R. and Dr.Shajin Nargunam A.., Improved Image Steganography using Huffman encoding and LSB. ***Aust. J. Basic & Appl. Sci.,*** *9(16): 62-66, 2015*

INTRODUCTION

People are very much anxious about the confidentiality of their information exchange. The growing use of digital media has made the security of digital media files highly critical against those users with malicious intentions, especially on the Internet. However, distributing digital data over public networks such as Internet is not reliable because of factors like copyright violation, counterfeiting, fraud etc. In order to protect digital media files, researchers proposed and improved many data-hiding algorithms, such as steganographic algorithms, cryptographic algorithms, watermarking algorithms and other data-embedding algorithms.

Steganography is derived from the Greek word steganos which means “covered” and graphia which means “writing”. As such Steganography means “covered writing”. It is the art and science of embedding secret messages in such a way that no one, other than the sender and intended recipient, suspects the occurrence of the hidden data. For embedding the secret information, multimedia carriers such us video, audio, image files are used and the hidden data may not be exposed to the intruders. The hidden data is a normal binary data which cannot be used unless one knows the embedding algorithm otherwise it is a junk of information. This data may be either the actual data about the secret information or encoded information using some algorithm. The combination of the carrier and the secret information forms the stego file. This stego file is transmitted through the open channel. An intruder may attack the stego file if there is any chance for retrieving the hidden data. So an unrevealed stego-image quality should be maintained.

In cryptography secret message is scrambled to form a cipher text and this is transmitted. The eavesdropper may get an idea that some insightful information is available in the bit stream and will try to decode the data by using some algorithm. Thus, it is important to enforce security to ensure authorized access to sensitive data. There are a number of encryption algorithms available such as DES, AES, IDEA and RSA. These traditional encryption algorithms have some drawbacks and they are not considered ideal for image transactions, because of low level of efficiency when dealing with large and redundant blocks of image data. Moreover, these algorithms require more than the usual expected processing time and resources while performing image encryption.

The concept of cryptography and steganography are combined to improve the strength, security and capacity of the information. Using the Huffman encoding technique the image data is converted to different format. These codes are embedded into a cover image without much distortion.

Related Works:

Image steganographic algorithms may be classified into two types, viz those embedding in the spatial domain and in the transform domain.

Corresponding Author: Rajesh G.R., Research Scholar, Department of Computer science and engineering, Noorul Islam University, Tamilnadu, India.
E-mail: grrajesh175@gmail.com

Algorithms used in spatial domain are Least Significant Bit (LSB) method and Pixel Value Differencing (PVD) method.

In the LSB method the least significant bits of the cover image are embedded into the information bits of secret image. The secret information bits are embedded in a uniform technique without affecting the visual effect of the cover image to the observer.

In the PVD method, the image is divided into blocks and the distance between the adjacent pixels are determined. The pixel difference will be higher at the edges and may be approaching zero at the flat regions. If the difference between the adjacent pixels is more, then number of bits required to embed into the cover image will be high. This method can accomplish better results when compared with LSB method for the same embedding capacity.

Many algorithms have been presented using LSB by directly embedding the secret image in the cover. (Wang *et al*., 2001) proposed a technique to improve the quality of the stego image by genetic algorithm of optimal LSB substitution. Then (Chan *et al*., 2004) proposed optimal pixel adjustment and (Wu *et al*., 2005) presented a combination of PVD and LSB with the same objective.(Rig Das *et al*., 2012) combined the lossless encoding on secret image and LSB to improve the quality of stego image and security.

We propose a new embedding technique to provide a better stego image quality and security with the Huffman codes generated from the secret image. The codes and the overhead bits required for retrieving the secret image are embedded in the border of the cover image. This will improve the security and the visual effect of the cover will not be affected.

huffman encoding:

An image is a two dimensional function f(x,y), where x and y are spatial coordinates and the amplitude of f at any pair of coordinates is called the intensity of the image at that point. An image f(x,y) is sampled so that the resulting image has M rows and N columns and the values of the coordinates are discrete.

Firstly, order the probabilities of the symbols and combining the lowest probability symbols into a single symbol that replaces them in the next source reduction. The initial set of source symbols and their probabilities are ordered from top to bottom in terms of decreasing probability values.

To form the first source reduction the bottom two probabilities are combined to form a compound symbol. This compound symbol and its associated probability are placed in the first source reduction column so that the probabilities of the reduced source are also ordered from the most to the least probable. The process is repeated until a reduced source with two symbols is reached.

Number of symbols in the information is N. Let the probability of i^{th} symbol is

$$\sum_{i=1}^{N} P(i) = 1 \quad (1)$$

Let the length of the code be L (i) then the average length is

$$L_{av} = \sum_{i=1}^{N} L(i)P(i) \quad (2)$$

No two symbols will have identical codes and no delimiters are required for codes.

It may be assumed that the probabilities of the symbols are arranged such that

$$P(1) \geq P(2) \geq P(3) \ldots \geq P(N-1) \geq P(N) \quad (3)$$

For the code to be optimum following conditions are to be satisfied.

$$L(1) \leq L(2) \leq L(3) \ldots \leq L(N-1) \leq L(N) \quad (4)$$

Huffman codes contain the smallest possible number of code symbols per source symbol.

Lsb algorithum:

Each pixel position of the image is represented by an 8 bit binary number. Least significant bit position of the cover image may be embedded with some secret information. If more bit positions of the cover image are used then more secret bits can be hidden in the cover image by sacrificing the image quality of the cover. So a compromise has to be made in taking the bit position to be used in the cover. If more number of LSB bit of the cover image is utilized then PSNR of the secret image will be increased and vice versa. To obtain the optimum result compromise should be made in selection of bits to be used for hiding the secret image.

Table 1: Psnr Of Cover And Secret Image For Varying Lsb Bits.

No of Bits	*MSE of cover Image*	*PSNR Cover image(db)*	*MSE of Secret Image*	*PSNR Secret image (db)*
1	0.5004	51.1714	2.9247e+003	13.5040
2	2.0280	45.0941	1.2633e+003	17.1498
3	9.0994	38.574	286.537	23.59
4	37.17	32.46	82.15	29.01
5	148.42	26.44	17.30	35.78
6	554.03	20.72	3.4478	42.78
7	2.0046e+003	15.14	0.4974	51.1977
8	5.2351e+003	10.9756	0	99

Table gives the PSNR of the cover and secret image of size 256x256 pixels for different bit utilization. An optimized number of LSB bits are selected based on the bits to be hidden in the cover mage. In this experiment we have selected two bits in the cover.

Estimation is done based on the number of bits required to be hidden. Based on that, the pixels are grouped to form a cell. In that cell, the information will be replaced in the least significant part of the pixel in the cell. To improve security, regions may be selected such that information in the consecutive pixel positions may be avoided using the algorithm for selecting cell blocks.

Alteration in the least significant part of the pixel does not give much distortion to the carrier image. Using the decoding algorithm information available will be retrieved.

Proposed method:

Let us consider two still images of size PX Q and MXN as carrier and secret image respectively. In the secret image minimum pixel value is subtracted from all the pixel values. On this flat encrypted image, minimum redundancy coding based on Huffman coding is made on the secret image. The symbol which is occurring more frequently will be having less number of bits and vice versa. In the codes, the number of bits required to represent a data is obtained and this information is embedded as overhead in the cover. These codes will be coded from top to bottom and left to right in the blocks selected. Pixel values are replaced by respective codes. Depends on the redundancy the length of the symbol code will vary and total number of bytes required to represent the secret image will be less. Total number of bits required to represent the image will be reduced considerably. Tables are created with symbol code and histograms. Table information and overheads required to decode the symbol were encoded on the least significant bit of cover image blocks to form a stego image. Entire information has to be encoded in the cover image to recover the exact image.

From the received stego image encoded bits and the payloads are extracted. Huffman table is reconstructed using the decryption algorithm. The secret image is recovered from the Huffman table.

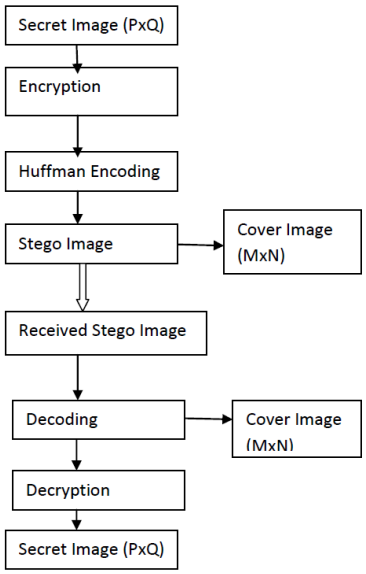


Fig. 1: Block Diagram of the proposed algorithm.

Experimental Result And Analysis:

Experimental results reveal much better performance over the present algorithms. The cover images selected for analysis are 1024X1024, 512X512 and the secret images of size 512X512, 256X256, 128X128. The experimental setup was implemented using Matlab and C++.

Peak signal to Noise ratio (PSNR) was used to measure the performance.

$$PSNR = 10 \log_{10} \frac{255^2}{MSE} \quad (5)$$

$$MSE = \frac{1}{PXQ} \sum_{m=1}^{p-1} \sum_{n=1}^{q-1} (A_{m,n} - B_{m,n})^2 \quad (6)$$

PXQ is the dimension of the cover image.

$A_{m, n}$ is the pixel position of the cover image and

$B_{m, n}$ is the pixel position of the stego image.

In this work, we are presenting a novel steganographic work that is capable of embedding large information without degrading the visual effect. For high values of PSNR, the distortion of the cover image will be less which gives much better visibility to human vision. The embedding capacity of the cover image is calculated based on the total bits of

secret information to be hidden. Total available pixel quantities in the cover image are estimated. From the information of number of secret bits to be hidden, number of bits to be used from each pixel of the cover image can be estimated. Least significant bits of cover image are selected and the secret information must be replaced. In this experiment, we have selected two bits of each pixel of the cover image and total number of data to be embedded is encoded in the initial block of pixels. Since only the least significant bits of the cover image are used for hiding there will be a small distortion in the cover image. There is a probability that the data to be embedded and the pixel value be the same. In such condition there would not be any distortion in the cover image pixel. Since the information is stored in random manner it is very difficult for the intruder to retrieve the secret information. One more level of security is added over the cover using Huffman codes. The hidden image is decoded from the Huffman codes only if exact data is collected. A loss or change of one bit of information will give a distorted image even though the intruder detects that some information is hidden.

Fig. 2: Cover image is Barbara.bmp (512x512) a)stego image with 256x256 cameraman embedded b)stego image with 256x256 lena embedded.

Table 2: Results For 512x512 Cover.

Secret Image	Immunity of cover image to distortion		Quality of extracted image
	MSE	PSNR	MSE
Cameraman.tif 256X256	2.296	50.574	0
lena_gray_256.tif 256X256	2.50	50.19	0

We have conducted experiments on some of the standard images which give better results than the existing algorithms.

Experimental results, for cover image of size 1024 x1024 and the secret image of size 256x256, shows much improved performance over the existing algorithms. The secret image is camaraman.tif of size 256x256. Results obtained by [1] and [2] is compared with the proposed algorithm.

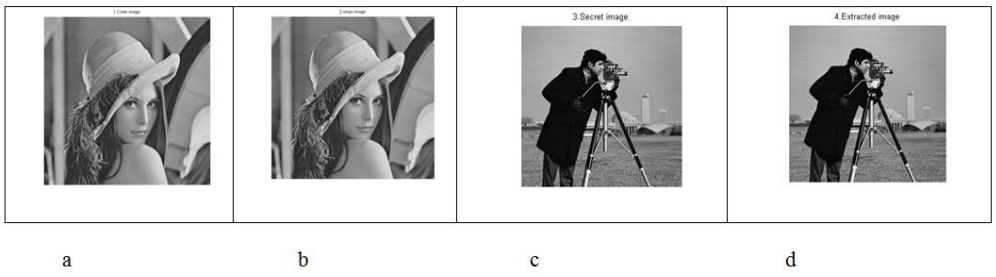


Fig. 3: Cover image of size 1024x1024 and the cameraman of size 256x256. (a) cover image (b) stego image (c) secret image (d) extracted image.

Table 3: Results For 1024x1024 Cover Image And 256x256 Secret Image.

Cover Image 1024X 1024	PSNR(dB) Between Cover image and Stego image		
	Steganography Based on Block-DCT and Huffman Encoding	Steganography Based on Huffman Encoding with Huffman	Proposed Algorithm
Lena	+50.48	+57.43	+62.590
Baboon	+50.28	+57.46	+62.256
Airplane	+50.91	+57.46	+62.391
Boat	+50.36	+57.46	+62.416

Conclusion:

The advantages and disadvantages of the technique proposed by us are discussed. Most of the real time images will have more redundant information. If the redundancy is high, number of bits required to code is less. In effect the number of pixels to be embedded in the cover image will be less and a good quality of cover image is maintained. We can encode the cover in any random manner so the intruder cannot easily know about the presence of secret message. The quality of the image produced is similar to the image used. Security against any attack can be improved. Disadvantages are if any noises are added in the stego images which in turn affect the information of the secret image. If the information is affected then the secret image cannot be retrieved.

As future work we are planning to improve the security by adding some more levels of encryption. By adding more encryption level the original image will be distorted and a junk data will be encoded using Huffman Algorithm.

REFERRENCES

Abbas Cheddad, Joan Condell, Kevin Curran, Paul Mc Kevitt, 2010. "Digital Image Steganography: Survey and Analysis of Current Methods". ELSEVIER Journal on Signal Processing, 90: 727-752.

Das, R., T. Tuithung, 2012. "A Novel Steganography Method for Image Based on Huffman Encoding",IEEE Digital library, Emerging Trends and Applications in Computer Science (NCETACS), 3rd National Conference

Nag, A., S. Biswas, D. Sarkar, P.P. Sarkar, 2010. "A Novel Technique for Image Steganography Based on Block-OCT and Huffman Encoding". International Journal of Computer Science and Information Technology, 2-3.

David, A., Huffman, Associate, Ire, "A Method for the Construction of Minimum-Redundancy Codes".

Gonzalez, R.C. and R.E. Woods, 2006. Digital Image Processing using MA TLAB, Pearson Education,Tndia.

Bin Li, Junhui He, Jiwu Huang, Yun Qing Shi, 2011. "A Survey on Image Steganography and Steganalysis". Journal of Information Hiding and Multimedia Signal Processing, 2-2.

Chung-Ming Wang, A., A. Nan-I Wu, B. Chwei-Shyong Tsai, Min-Shiang Hwang, 2008. "A high quality steganographic method with pixel-value differencing and modulus function", The Journal of Systems and Software, 81: 150–158.

Esra Satir, Hakan Isik, 2012."A compression based text steganography method", The journal of systems and software, 85: 2385-2394.

Zhensong Liao, Yan Huang and Chisong Li, 2007. Research on Data Hiding Capacity,, International Journal of Network Security, 5(2): 140–144.

Constantinos Patsakis, Nikolaos G. Aroukatos, 2014. "LSB and DCT Steganographic Detection Using Compressive Sensing", *Journal of Information Hiding and Multimedia Signal Processing* ©2014 ISSN 2073-4212 Ubiquitous International, 5-1.

Chan, C.K., L.M. Cheng, 2004. Hiding data in images by simple LSB substitution. Pattern Recognition 37 (March), 469–474.