ISSN:0975-9646

Venkata Giriprasad Ronanki et al, / (IJCSIT) International Journal of Computer Science and Information Technologies, Vol. 6 (5) , 2015, 4299-4303

A Novel 4X4 LSB Pixel Substitution Approach for Image Steganography

Venkata Giriprasad Ronanki[1], K Kavitha[2]

[1#]M.tech information Technology,[2]Sr.Assistant Professor Information Technology

Aitam ,Tekkali,Andhra Pradesh,India

***Abstract*— Steganography is the knowledge and art of hiding secret data into information which is a great extent utilized as a part of data security frameworks. Steganography typically manages the methods for concealing the presence of the conveyed information in a manner that it stays secret. It keeps up mystery between two conveying gatherings. In image steganography, mystery is accomplished by embedding information into a cover image and creating a stego image. Different techniques have been proposed in which in which most of them are not capable of both preventing visual degradation and providing a large embedding capacity. In this, we spotlights on the property of human vision structure that offer help to manufacture the measure of data concealing in the bitmap (.bmp) and JPEG (.JPG) pictures in every way that really matters. In this paper, we proposed a tunable visual picture quality and information lossless system in spatial domain based on a genetic algorithm. The essential thought about the proposed framework is showing the steganography issue as a hunt and advancement issue. Experimental results demonstrate that the proposed approach performs high embedding point of confinement and in addition overhauls the PSNR and MSE of the stego image.**

Keywords—**coverimage,stegoimage,stegangraphy, mse,psnr,capacity**

INTRODUCTION

Steganography is the art and science to conceal information in a spread media, for example, text, Audio, image, video, and so forth. (Cheddad et al.) [8] In other words, steganography is the procedure of concealing a mystery message inside of a bigger one in a manner that somebody can't know the vicinity or substance of the shrouded message.

The term Steganography is forked from the Greek words"stegos" signifying "cover" and "grafia" signifying "writing" characterizing it as " covered writing ". In this paper, steganography in pictures is subjected. For the most part there are various steganographic tecniques that cover mystery message in a digital image . As indicated by the technique for information hiding, two prominent sorts of concealing techniques ie: (i) spatial domain embedding and (ii) transform domain embedding. The most ordinarily utilized spatial domain method is Least Significant Bit (LSB) substitution. The most generally transform domain methods are: Discrete Cosine Transform (DCT), Discrete Wavelet Transform(DWT),and Fast Fourier Transform (FFT).[2][12]

Steganography is a procedure where secret information is implanted inside of a image that has been generally concentrated in the most recent decade because of the expense diminishing of picture stockpiling and correspondence furthermore the shortcomings of the human visual system(HVS). It ought to be specified that the cover or host image is referred as the original image without the embedded secret data, while the image that is acquired by inserting secret message into cover image without destroying the cover image is termed as stego image. The term capacity is used to depict the size of the secret message that can be embedded in a cover image.

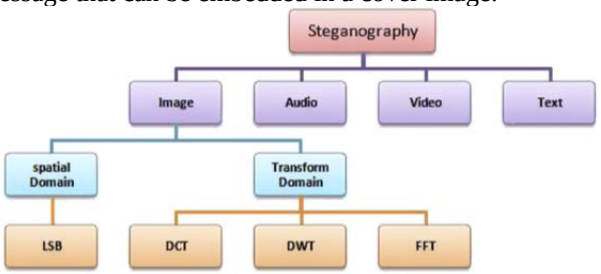


Fig-1: Different Types of Stegenographic Techniques

2. LITERATURE SURVEY

There are diverse steganography methodologies including spatial domain and frequency domain. Abbas Cheddad et al [8] proposed and investigated on distinctive Steganography approaches that includes hiding secret information in a fitting media transporter, e.g., image, audio, video and other multimedia carriers .It goes under the presumption that if the component is unmistakable, the purpose of assault is clear, in this manner the objective here is dependably to cover the very presence of the implanted information. Steganography has different valuable applications. On the other hand, similar to some other science it can be utilized for sick expectations. It has been pushed to the cutting edge of current security procedures by the striking development in computational force, the increment in security mindfulness by, e.g., people, bunches, offices, government and through scholarly interest.

Po-Yueh Chen and Hung-Ju Lin[11], proposed in their steganography procedure which embedded the mystery messages in frequency domain. As indicated by diverse clients' requests on the implanting capacity and image quality, the proposed calculation is isolated into two modes and 5 cases. Unlike the space domain approaches,, secret data is embedded in the high frequency coefficients resulted from Discrete Wavelet Transform. Coefficients in the low recurrence sub-band are protected unaltered to enhance the image quality. Some fundamental scientific

operations are performed on the mystery messages before hiding. These operations and an all around planned mapping table keep the messages far from stealing, destroying from unintended users on the web and consequently provide satisfactory security.

Masoud Nosrati and Ronak Karimi [7], proposed the use of Genetic Algorithms in steganography. Steganography media which is subjected regards image files. In this way, some of recent studies that present the steganography strategies are recorded and described. As it is seen, robustness and capacity are two imperative factors that are considered in all steganography techniques. Additionally, distinctive systems utilize one or both of stego-phases. Some of them have regards about embedding, and some of them modify the stego-image. and some of them alter the stego-image.

Shahzad Alam et al [6], in their work ,Steganography is the the idea of hiding private, confidential,sensitive data or information within something that appears to be nothing out of the normal. They improve the work of LSB and attempt to turn out with a superior result for both picture quality and the measure of information can be covered up inside it. They turn out with two methodologies; initial one is the 3-3-2 methodology with no confinements on the kind of image being utilized and can reach up to 33.3% of size of covered information, and the second one is the 4-4-4 methodology which expand the sum up to half of concealed information from the measure of picture however with specific constraints on the sort of images picked.

Chi-Kwong Chan and L.M. Cheng [12] proposed in their work an information hiding scheme by simple LSB substitution is proposed. By applying an optimal pixel adjustment process to the stego-picture obtained by the basic LSB substitution technique, the nature of the stego-image can be extraordinarily enhanced with low additional computational complexity.. The most pessimistic scenario mean square error(MSE) between the stego image and the cover image is indistinguishable from the original cover-image. The obtained results also show a significant improvement with respect to past work.

Wen-Jan Chen et al [9] in their work Steganography is the art and science of concealing information into data. The secret message is covered up in a manner that nobody can separated from the sender or the proposed beneficiary. Tseng et al. [10] proposed a steganography technique in based on Optimal Pixel Adjustment Process (OPAP) and GA. This strategy adjusts secret bits for accomplishing more similarity with host image.

The least significant bit(LSB) substitution instrument is the most well-known steganographic procedure for concealing a secret message in a image with high capacity, while the human visual system (HVS) would be unable to see the concealed message in the cover image. In this paper, besides employing the LSB substitution strategy as a central stage, the exploratory results demonstrate that the proposed plan accomplishes high embedding capacity as well as enhance the quality of the stego image from the HVS by an edge discovery system. Moreover, based on that the secret message is replaced with different LSBs, our scheme can effectively resist the image steganalysis.

3. METHODOLOGY

The proposed scheme is made up of image compression, data embedding and data extraction phases.

3.1 Image compression:

Run length encoding is an information compression technique that helps us encode extensive runs of repeating things by just sending one thing from the run and a counter demonstrating how often this thing is rehashed. Unfortunately this procedure is not so good when attempting to compress natural language texts, because of the fact that they don't have long runs of rehashing components. In the other hand RLE is helpful regarding the matter of image compression, in fact that pictures have long runs pixels with identical colors.

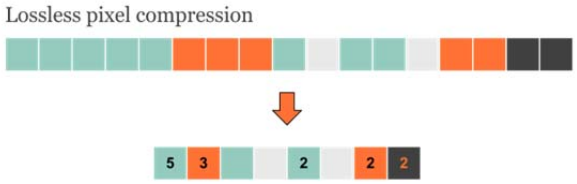
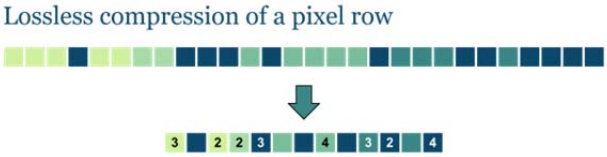


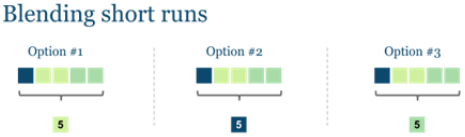
Fig-2: Lossless pixel compression

Although lossless RLE can be truly effective for image compression, it is still not the best approach. For this situation we can spare counters for pixels that are rehashed more than once. Such the data stream "aaaabbaba" will be packed as "[4]a[2]baba". There are few ways of run-length encoding that can be utilized for image compression. A conceivable method for compression of a image can be either row by row or column by column. Clearly run-length encoding is a decent approach when compacting images, however when we discuss enormous images with a large number of pixels, it's by one means or another common to accompany some lossy compression.



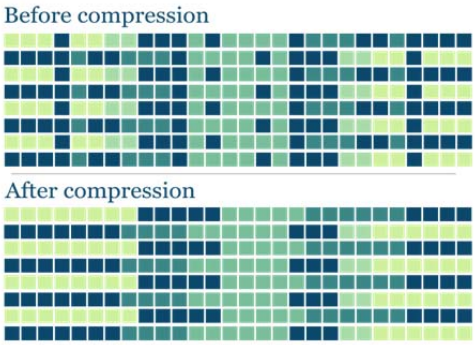
Fig(5): Lossless pixel row compression

One thing is the manner by which to consolidation short runs. For example the accompanying three runs must be mixed into one shading run.



Fig(6): Blending short runs

We must pick how to mix short runs! We can pick the center shading (alternative #1) or not, but rather this will dependably rely on upon the photo and it will be compelling at times and insufficient in other.



Steps to compress cover image:

With a specific end goal to actualize the image compression calculation, we separated the procedure into different steps:

Step1: calculate the sums and differences of every row of the image

Step2: calculate the sums and differences of every column of the resulting matrix

Step3: repeat this process until we get down to squares of 16x16

Step4: quantize the final matrix using different bit allocation schemes

Step5:write the quantized matrix out to a binary file

The initial two stages are proficient utilizing simple loops in Matlab. In particular, we composed two distinct functions - rowthing for caluclating sums and contrasts of individual rows and colthing for computing sums and differences of individual coulmns.

The third step includes rehashing the past two stages until we get down to a sufficiently little last picture. The function squisher() achieves this task. This function performs the sums and differences of rows and coulmns, in substituting order, until the last entireties of totals picture is of size 16x16.

With a specific end goal to keep the energy of the picture the same, we multiplied each sum and difference by a factor of 1/sqrt(2). Performing these two operations once will bring about a picture that is part into four sections, with the upper left hand quadrant being the sums of sums region.

The quantization function called quant(), is also called squisher(). Our quantization plot just relegates different quantities of bits to distinctive regions, using masks (for instance, [b16, b32, b64, b128, b256], where b16 is the quantization level for the upper left 16x16 network, b32 is for the following 32x32 lattice encompassing the first, and so on.). We utilized various diverse bit allotment masks keeping in mind the end goal to figure out which plan is better. The quantization function takes in as arguments not only the input matrix, but also the mask, as well as the cover, i.e. the quantity of bits to be utilized to speak to every area in the compression plan. This permits us to adjust and test out distinction bit allotment calculations effectively.

When we have produced the the compressed matrix,, we are ready to exchange it to a binary file for storage capacity (and, all the while, quantize it). We utilize the fwrite Matlab command, determining the quantity of bits with which to quantize. When the record is saved, we can utilize the file size data to assess the accomplishment of the compression process.

3.2. LSB (Least Significant bit embedding)[12]:

LSB method is actualized in spatial domain. The strategy alters image into shaded Gray Scale picture. This image will be act as reference image to cover the content. By utilizing this gray scale reference image any content can be hide. Single character of a content can be represented in 8-bit. On the off chance that the reference picture and the information are transmitted through system independently, we can accomplish the impact of Steganography. Here the image is not at all distorted because of the fact that said image is utilized for referencing. Any huge amount of text material can be hide using a very small image.

In a gray scale image every pixel is spoken to in 8 bits. The last bit in a pixel is called as Least Significant bit as its worth will influence the pixel value just by "1". Along these lines, this property is utilized to conceal the information in the image. Here we have considered last two bits as LSB bits as they will influence the pixel value by "3". This helps in putting away additional information. The Least Significant Bit (LSB) steganography is one such procedure in which least significant bit of the image is substituted with information bit. As this technique is vulnerable against stegano analysis to make it more secure we encode the raw data before embedding it in the image. Despite the fact that the encryption procedure builds the time complexity, yet in the meantime gives higher security. This methodology is exceptionally simple. In this strategy the least significant bits of some or the majority of the bytes inside a image is embedded with a bits of the secret message. The LSB implanting methodology has turned into the premise of numerous procedures that conceal messages inside of mixed media bearer information. LSB implanting may even be connected specifically information areas - for instance, inserting a concealed message into the shading estimations of RGB bitmap information, or into the frequency coefficients of a JPEG image. LSB installing can likewise be connected to a mixed bag of information organizations and sorts. In this manner, LSB embedding approach is one of the most important steganography strategies being used today. From one of our reference paper we found that in LSB steganography, to hide the message the minimum huge bits of the spread media's advanced information are utilized. The valuable element of the LSB steganography methods is LSB substitution that makes LSB stegnography as basic. To extract the message it should be hidden, LSB substitution steganography flips the last bit of each of the information values. Consider a 8-bit gray scale bitmap image where every pixel is put away as a byte. Furthermore, it additionally represented in a gray scale value. Suppose the initial eight pixels of the first picture have the accompanying gray scale values: 11010010 01001010 10010111 10001100 00010101 01010111 00100110 01000011

The letter C whose binary value is 1000001. To conceal this binary value, substitute the LSBs of these pixels to have the accompanying new grayscale values:

11010011 01001010 0010110 10001100 00010100 01010110 00100111 01000011

On a normal, just a large portion of the LSBs should be changed. The contrast between the covered (i.e. unique) image and the stego picture is hard to see by human eye. The major limitation of LSB is small size of data which can be hide in such sort of images utilizing just LSB. The LSB is extremely vulnerable to attacks.

Proposed LSB Approach:

In this novel approach 4 pixel substitution takes place, which is implemented to .bmp images or jpeg picture. In this the secret message can be changed over to binary format, in this binary information the two least significant bits substituted in the LSB of 8X8 bit pixel values, the two most significant bits are substituted in MSB of 8X8 bit pixel value. Consider a 8-bit gray scale bitmap picture where every pixel is put away as a byte. Assume the initial eight pixels of the first picture have the accompanying dark scale values: Suppose the first eight pixels of the original image have the following gray scale values: 11010010 01001010 10010111 10001100 00010101 01010111 00100110 01000011

The letter C whose binary value is 01000001. To conceal this binary value in a gray scale image pixels it can supplant the LSBs,MSBs of these pixels to have the accompanying new gray scale values: 01010001 00001000 10010111 1000110 00010101 01010111 00100110 01000011

Steps to embedding the secret message:-

Step 1: Read the cover image and the text message which is to be hidden in the cover image.

Step 2: Convert the text message in binary format.

Step 3: Calculate the two LSB of each pixel of the cover image.

Step 4: Replace the cover image of the LSB with two bit of secret message in last two bit position.

Step 5: Write stego image

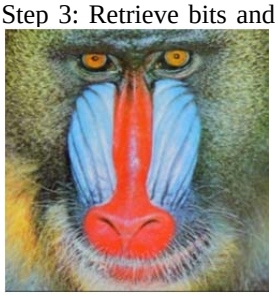
Step 6: Calculate the Mean square Error (MSE) and the Peak signal to noise ratio (PSNR) and capacity and co relation of the stego image.

Steps to Extract text message:-

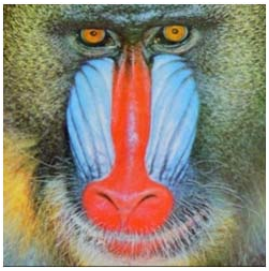
Step 1: Read the Stego image.

Step 2: Calculate the last two LSB positions of each pixels of stego image.

Step 3: Retrieve bits and convert each 8 bit into character



Fig(8): cover image



Fig(9): stego image

EXPERIMENTAL RESULTS:

This area displays the execution of the proposed methodology against other existing calculations. To assess the adequacy of the proposed steganography technique, the stego picture quality is considered from two perspectives. To begin with, , we utilized the peak-signal-to-noise ratio (PSNR) metric between the stego image and the host image which is defined as follows. Second, we look at the quality of the stego image to that of the host picture as seen by the human visual system (HVS). PSNR is most effortlessly characterized through the Mean Square Error (MSE). Given a noise free m×n monochrome image I and its noise estimate K,

(i)Mean Square Error:

$$MSE = \frac{1}{mn}\sum_{i=0}^{m-1}\sum_{j=0}^{n-1}[I(i,j) - K(i,j)]^2$$

(ii) Peak Signal to Noise Ratio (PSNR): It is the measure of quality of the stego image by comparing with the cover image in terms of signal and noise.

PSNR is calculated using Equation

PSNR = $10\log_{10}(255^2/\text{MSE})$ dB

(iii) Capacity: It is the size of the data in a cover image that can be modified without deteriorating the integrity of the cover image. The steganographic embedding operation needs to

preserve the statistical properties of the cover image in addition to its perceptual quality. Capacity is represented by bits per pixel (bpp) and is computed using Equation .

$$\text{Capacity} = \frac{\textit{number of bits of payload embedded}}{\textit{total number of bits in the cover image}}$$

(iv) Entropy: Entropy is a measure of security for a steganography system. A system is perfectly secure when the Relative Entropy (RE) tends to zero.

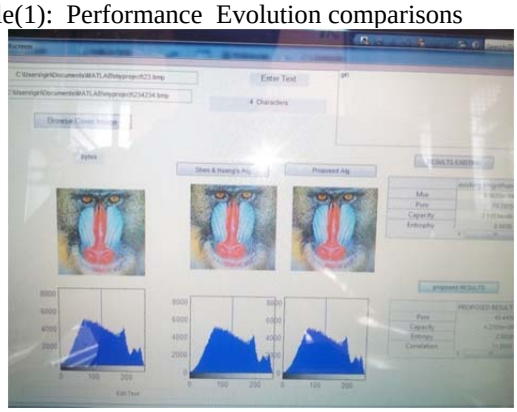
(v) Correlation: If we have a series of n measurements of *X* and *Y* written as *xi* and *yi* where *i = 1,2… n*, then the sample correlation coefficient can be used to estimate the population Pearson correlation r between *X* and *Y*. The sample correlation coefficient is written as

$$r_{xy} = \frac{\sum_{i=0}^{n}(x_i - \bar{x})(y_i - \bar{y})}{\sqrt{\sum_{i=1}^{n}(x_i - \bar{x})^2 (y_i - \bar{y})^2}}$$

Where *sx* and *sy* are the sample standard deviations of X andY

Performance evolution	EXISTING results	PROPOSED RESULTS
MSE	6.955e-04	1.8056e-04
PSNR	79.705	40.443
CAPACITY	2.115e+06	4.2305e+06
ENTROPY	0.0030	2.5030
CORELATION	1.000	11.000

Table(1): Performance Evolution comparisons



Fig(10): Proposed system Result

CONCLUSION

In this paper, a novel high data embedding capacity and data lossless spatial domain image steganography approach is proposed. The presented calculation, steganography is demonstrated as search problem. The used approach avoids the exhausting searching and allows us to find the best place in host image for embedding modified secret data. Thus, the proposed system can accomplish high embedding capacity, furthermore it enhances the stego image quality (i.e. PSNR). The procedure of inserting is expert in two primary steps, first to change secret message to bits and second embedded it into host image. The algorithm has been assessed and contrasted with prevalent existing methodologies from the perspective of from the viewpoint of secret hiding effectiveness and stegoimage quality. It is exceptionally reassuring finding that the proposed methodology performs reliably better than the analyzed benchmark approaches. Experimental results have additionally shown that, notwithstanding when the capacity of embedded secret image is expanded, the stegoimage visually indistinguishable from its corresponding host image.

We conclude that our proposed methodology can create an astounding stego image fulfilled the positive interest of the embedding capacity by users. Our plan is simple, and feasable for versatile steganographic applications.

REFERENCES:

[1]. Hamidreza Rashidy Kanan , Bahram Nazeri (2014) A novel image steganography scheme with high embedding capacity and tunable visual image quality based on a genetic algorithm. Expert Systems with Applications 41 (2014) 6123–6130 Elsiever sciencedirectory

[2]. Wafaa Mustafa Abduallah et al (2014) Mix column transform based on irreducible polynomial mathematics for color image steganography: A novel approach Computers and Electrical Engineering 40 (2014) 1390–1404 Elsiever sciencedirectory

[3]. Blanca E. Carvajal-Gámez et al(2013) Adjust of energy with compactly supported orthogonal wavelet for steganographic algorithms using the scaling function 1/sqrt (2^{j}) International Journal of Physical Sciences Vol. 8(4), pp. 157-166

[4]. Parul et al(2013) Optimized Image Steganography using Discrete Wavelet Transform (DWT) International Journal of Recent Development in Engineering and Technology (ISSN 2347 - 6435 (Online) Volume 2, Issue 2, February 2014)

[5] Mamta. Juneja, and Parvinder S. Sandhu (2013) An Analysis of LSB Image Steganography Techniques in Spatial Domain International Journal of Computer Science and Electronics Engineering (IJCSEE) Volume 1, Issue 2 ISSN 2320–401X (Print)

[6]. Shahzad Alam et al (2013)nalysis of Modified LSB Approaches of Hiding Information in Digital Images 2013 5th International Conference on Computational Intelligence and Communication Networks

[7]. Masoud Nosrati and Ronak Karimi(2012) A Survey on Usage of Genetic Algorithms in Recent Steganography Researches World Applied Programming, Vol (2), No (3), March 2012. 206-210ISSN: 2222-2510

[8]. Cheddad, A. et al. (2010). Digital image steganography: Survey and analysis of current methods. Signal Processing, 90(3), 727–752.

[9]. Wen-Jan Chen et al (2010) High payload steganography mechanism using hybrid edge detector Expert Systems with Applications 37 (2010) 3292–3301 Elsiever sciencedirectory

[10]. Tseng, L. -Y., & et al. (2008). Image hiding with an improved genetic algorithm and an optimal pixel adjustment process. In Eighth international conference on intelligent systems design and applications, 2008. ISDA'08 (Vol. 3). IEEE.

[11] Po-Yueh Chen and Hung-Ju Lin(2006) A DWT Based Approach for Image Steganography International Journal of Applied Science and Engineering 2006. 4, 3: 275-290

[12]. Chi-Kwong Chan and L.M. Cheng (2004) Hiding data in images by simple LSB substitution Pattern Recognition 37 469 – 474 11, 1997.

Venkata GiriPrasad Ronanki received B.Tech degree in Computer Science and Engineering from JNTU, Kakinada and pursuing M. Tech degree in Information Technology from an autonomous institute Aditya Institute of Technology and Management (AITAM), Tekkali, India, permanently affiliated to JNTU, Kakinada. His present areas of interests include Network Security and Image Processing.

K.Kavitha received B.Tech degree in Information Technology from JNTU, Hyderabad and M. Tech degree in Computer Science and Engineering from JNTU, Kakinada. She is a Sr.Assistant professor in the department of Information Technology from an autonomous institute Aditya Institute of Technology and Management (AITAM), Tekkali, India, permanently affiliated to JNTU, Kakinada. Her present areas of interests include Computer Organization and Architecture, Design Analysis of Algorithms, Multimedia, Network Security, and Image Processing.