ISSN(Online) : 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 5, Issue 5, May 2016

Analysis of Information Concealing Utilizing Advanced Picture

Asif Pasha[1], Divyashree B A[2]

P.G. Student, Department of Computer Science & Engineering, BNMIT, Bengaluru, India[1]

Professor, Department of Computer Science & Engineering, BNMIT, Bengaluru, India[2]

ABSTRACT: Information concealing procedure installs information into computerized media with the end goal of security. Advanced picture is one of the best media to store information. It gives vast ability to concealing mystery data which results into stego-picture subtle to human vision, a novel steganographic approach taking into account such as, pixel value differencing. This technique gives both high installing limit and remarkable vagueness for the stego-picture. Pixel Value Differencing based systems is done to deliver changed information concealing strategy. In versatile strategy picture is separated into pieces and after that information will be covered up.Another technique such as discrete cosine transformations ,produces cosine transformations on 8*8 piece of picture and then embedding is done followed by on the other hand IDCT is utilized to go along with all the squares into single picture, for example, stego-picture. Target of the implementation work is to expand the stego – picture quality and in addition expand limit of mystery information.

KEYWORDS: Pixel value differencing (PVD), Discrete cosine transformations(DCT), Inverse discrete cosine transformations(IDCT),TIFF ,JPEG images and secret data.

I. INTRODUCTION

In today's reality everybody can't have faith in what you see is the thing that you get (WYSIWYG). The straightforward purpose for this is all the pictures including sight and sound conveys information, pictures. Taking a gander at the picture our human visual framework (HVS) couldn't perceive whether picture conveys any data or not. Over the couple of decades individuals have created numerous Steganographic strategies to conceal information inside advanced picture what's more, that ought not be vague by HVS. On the opposite there are high odds of information spillage when open media is utilized for correspondence. Consequently it is a test to send an information furtively up to the destination. In long time past days cryptography was utilized to defeat this issue. With the increment being used of Internet mystery correspondence utilizing open correspondence has turned into an imperative field of research. High security has been come to with the current cryptographic procedures. Still programmers can decode the encoded information in view of appearance of mystery information spoken to as figure content. To occupy the consideration of programmers the transmission of mystery information ought to be utilizing some other interchange strategy. Steganography is the field that gives a significant method for secure information being transmitted through an open channel without the consideration of busybodies.

Frequency domain

In frequency domain, images are first transformed and then the message is embedded in the image [1][2][3]. When the data is embedded in frequency domain, the hidden data resides in more robust areas, spread across the entire image, and provides better resistance against statistical attacks. There are many techniques used to transform image from spatial domain to frequency domain. The most common frequency domain method usually used in image processing is the 2D discrete cosine transform [4][5] where the image is divide into 8*8 blocks and then DCT transformations is done followed by quantization is done to DCT coefficients to achive quantized block where the data is embedded [7].

ISSN(Online) : 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 5, Issue 5, May 2016

II. RELATED WORK

Pixel value differencing using color image

A. LSB swap for 24-bit shading pictures by applying condition on MSB Kekre proposed PVD for gray scale pictures where two successive pixel sets are framed and implanting limit is chosen in view of contrast in their qualities like unique PVD [6]. Creator likewise proposed adjusted calculation which stretched out PVD to 24-bit shading pictures furthermore another enhanced rendition of LSB technique is connected on 24-bit shading pictures.

In the inserting process a distinction quality is figured from each RED, GREEN and BLUE (R, G, B) segment of non-covering square of two continuous pixels of a given spread picture. The method for dividing the spread picture into two-pixel squares goes through all the lines of the picture. The first Kekre's technique made utilization of up to four LSB's for installing data. Chosen number of LSB's relies on upon pixel worth to control the mistake. Creator altered this to incorporate fifth LSB coordinating to increment limit further.

Before inserting the information, 8-bit mystery key(S) and message (M) is XOR'ed. Also, Message is recuperated by XOR operation of the same 8-bit key.

S XOR M= E'

E' XOR S=M

Each pixel value in this picture is broke down and the checking procedure is utilized on MSB bits.

Condition 1: If the value of the pixel gi is in the reach between 240 to255, then check for the message bit to be implanted (m).

• If m=1 then use the fifth piece of the pixel esteem.

• If m=1 then implant 4-bits of mystery information into the 4 LSB's of the pixel. • This should be possible by watching the initial 4 MSB's. On the off chance that they are all 1's then the remaining 4 LSB's can be utilized for installing information.

Condition 2: If the estimation of gi (First 3 MSB's are every one of the 1's), is in the extent between 224 to 239 then check for the message bit to be installed (m)

• If m=0 then use 5-bits of the pixel esteem.

• If m =0 then install 3-bits of mystery information into the 3 LSB's of the pixel.

Condition 3: If the estimation of gi (First 2 MSB's are every one of the 1's), is in the extent between 192 to 223 then install 2 bits of mystery information into the 2 LSB's of the pixel.

Condition 4: All different cases for the qualities in the extent 0 to 192 install 1 bit of mystery information into 1 LSB of the pixel. The installing process keeps up a network to keep a track of the pixels where 5 bits are used for installing process. This aides in the recovering the mystery message. The recovering procedure is exceptionally basic by watching the MSB and utilizing the network kept up. In PVD amid the implanting stage there is a plausibility that the dim estimations of the two-Pixel piece may tumble off the limit esteem which needs a checking procedure to be utilized in the inserting stage and incase of quality fall off the limit esteem the piece is ended for embeddings the mystery information. The same checking procedure is once more rehashed in the recovery stage. Because of this there can be certain squares which are not used for inserting mystery information. This checking procedure is dreary and takes additional time both for implanting and recovery of the message. In the adjusted Kekre's strategy there is no such checking process required making it quicker than PVD. This strategy moreover uses each pixel of the picture to install the mystery information. Subsequently, strategy is basic for execution contrasted with PVD technique and accomplishes a high implanting limit and great vagueness.

Discrete cosine transformation

The challenge in this work was to figure out how to cover a mystery message in a picture without recognizable debasing the picture quality and to give better resistance against steganalysis process. In this way, a mix of recurrence area by method for DCT and LSB system of spatial space steganography has been utilized to conceal information. Two dimensional DCT changes over the picture obstruct from spatial area to frequency space and after that information bits are implanted by modifying LSB of DCT coefficients[7].

ISSN(Online) : 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 5, Issue 5, May 2016

The image of size M×N is divided into 8×8 blocks and two dimensional (2-D) DCT is performed on each block. The DCT is calculated using equation 1:

$$F(u,v) = \frac{1}{4}C(u)(v)\sum_{x=0}^{7}\sum_{=0}^{7} f(x,y)\cos\left[\frac{\pi(2x+1)u}{16}\right]\cos\left[\frac{\pi(2y+1)v}{16}\right] \quad \text{.....(1)}$$

Where

$$c(k) = \{\frac{1}{\sqrt{2}}\ for\ k = 0\ else\ 1\ otherwise\}$$

In DCT block lower frequency cofficents are at upper left positions and high frequency coefficients are lower right positions. Low frequency coefficients are of larger value than high frequency coeffcients.

Quantization

The 8 x 8 block of DCT coefficients is compressed by quantization. A useful feature in this process is the image compression and quality is obtainable through selection of specific quantization table. The standard quantization matrix. Quantization is achieved by dividing each element in the DCT coefficient block by the corresponding value in the quantization matrix, and the result is rounded to the nearest integer. As eye is not able to discern the change high frequency components so these can be compressed to larger extent. Lower right side components of quantization matrix are of high value so that after quantization high frequency components become zero. The quantized DCT coefficients matrix P is computed by equation (2)

$$p(u,v) = \frac{F(u,v)}{q(u,v)} \quad \text{.....(2)}$$

III. PIXEL VALUE DIFFERENCING AND DISCRETE COSINE TRANSFORMATIONS

Proposed method

Every pixel in a colour image composed of three colours (channels) i.e. Red, Green and Blue. So, every pixel contains 24 bits (for 8-bit representation) where 8 bits for red component, 8 bits for green and 8 bits for blue component in a pixel. In the proposed technique, all the three components have been used for data embedding. First, separate each colour component from a pixel and get three separate M*N matrix, one for each component colour, where the original image size is M*N. Now, apply pixel value differencing method for data hiding in each matrix separately, but in a sequencing manner. First embed bits in 1st pixel block (two consecutive non-overlapping pixels) of the red component matrix, then in 1st block of green component matrix and lastly in blue component matrix, then again 2nd block of red matrix and so on. In this way secret data is embedded into the total image. Further embedd different number of bits for different component pixel blocks for increasing security as well as improving the visual quality of the stego-image[8].

In addition, it is seen that pixel values in the stego image may exceed the range 0~255 on applying PVD which is not desirable as it may lead to improper visualisation of the stego image. In this section we introduce a technique to overcome this problem. In this proposed method the original PVD method to embeds secret data. If any pixel value exceeds the range (0 to 255), then check the bit-stream 't' to be hidden. If MSB(most significant bit) of the selected bit stream 't' is 1 then we embed one less number of bits, where MSB position is discarded from t; otherwise the bit number of hidden data depends on wi . For instance, if pixel value exceeds the range and selected bit-stream t=101, then set t=01 and embed it. If it is seen that the pixel value again exceeding range, then embed the value at one pixel, rather than both pixels(of the pixel block), which will not exceed the range after embedding; where the other pixel is kept unchanged. It will keep the pixel values within the range because both pixels of a block cannot exceed at the same time as per the PVD method by Wu and Tsai. Keep the information within each block, whether one less bit is embedded or not, as overhead.

Embedding Algorithm

Step 1: Separate the colour image into three component colour matrix and apply the following steps on each of them sequentially i.e. apply following steps on 1st pixel block of RED Three components of a colour pixel One true colour

ISSN(Online) : 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 5, Issue 5, May 2016

pixel matrix, then 1st block of GREEN matrix and finally on BLUE matrix, then started from 2nd block of each matrix and so on.
Step 2: Calculate the difference value di for each block of two consecutive non-overlapping pixels pi and pi+1 , is given by di=|pi-pi+1|.
Step 3: Find optimal range Ri for the di such that Ri =min(ui-di) , where ui_di .Then Ri ∈ [li , ui] is the optimum range where the difference lies.
Step 4: Compute the amount of secret data bits t from the width wi of the optimum range, can be defined as t= ⌊log2 wi⌋ .
Step 5: For RED matrix, if t <= 5 then execute the next steps; otherwise no embedding in the Block For GREEN matrix, if t <= 3 then execute the next steps; otherwise no embedding For Blue matrix execute the following steps.
Step 6: Read t bits and convert it into a decimal value b. Then calculate the new difference value by the formula di'=li+b .
Step 7: Now, calculate the pixel values after embedding t bits (pi' , pi+1')by original PVD method.
Step 8: Check the embedded pixel values whether it exceed the gray-level range or not . If it exceeds then check the embedded bit-stream t . Otherwise go to step 9.
Step 8.1: If the left most position of the bit-stream is 1 then select 't' by discarding one bit from its left most position. Convert 't' bits into its corresponding decimal value b and find new difference value as di'=li+b . Otherwise do not discard any bit from 't' and calculate di' .
Step 8.2: Calculate new pixel values (pi' , pi+1') using original PVD method and check again if it is in the gray range. If it is in the range then go to step 9.Otherwise do the following :

(pi' , pi+1')=(pi-m , pi+1), if pi+1 _ pi and pi+1 crossing the upper range(i.e 255) ;
(pi ', pi+1')=(pi , pi+1-m), if pi+1<pi and pi crossing the upper range(i.e 255) ;
(pi' , pi+1')=(pi , pi+1+m), if pi+1_pi and pi crossing the lower range(i.e 0);
(pi ', pi+1')=(pi+m , pi+1), if pi+1<pi and pi+1 crossing the lower range(i.e 0) . where m=|di'-di| .

Step 9: Now, the pixel block (pi , pi+1) is replaced by (pi' , pi+1').
Step 10: To keep the information whether 't' bits or 't-1' bits has been embedded, do the following for each modified block :
Step 10.1: If no bit has been discarded then do the following:

	LSB of P'i	LSB of P'i+1	then do
i)	0	0	P'i+1 +1
ii)	0	1	
a)	P'i+1 <255 and P'I _ 0		P'i+1 +1
b)	P'i >0 and P'i+1 =255		P'i-2 and P'i+1 -1
c)	P'i=0 , P'i+1=255		P'i +1
iii)	1	0	P'i -1
iv)	1	1	P'i -1

Step 10.2: One bit has been discarded

	LSB of P'I	LSB of P'i+1	then do
i)	0	0	P'i +1
ii)	0	1	P'i +1
iii)	1	0	
a)	P'i+1 >0 and P'i _ 255		P'i+1 -1
b)	P'i <255 and P'i+1 =0		P'i+2 and P'i+1+1
iv)	1	1	P'i+1 -1

Step 11: Now get the stego blocks and hence the stego image.

Extraction Algorithm
The steps used for extracting thehidden data are as follows :

ISSN(Online) : 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 5, Issue 5, May 2016

Step 1: Divide the stego image into three component matrix RED, GREEN and BLUE and execute the following steps for each pixel block, consist of two consecutive non-overlappingpixels, of RED, GREEN, BLUE respectively i.e. extract bits from one stego pixel at a time.

Step 2: Check the LSB positions of Pi (first pixel of the block) for each block and do the following :

LSB of Pi	Convert it as
0	Pi +1
1	Pi -1

Step 3: Now calculate the difference value di of two consecutive pixels of each block by using the formula di=|pi-pi+1|
Step 4: Find the appropriate range Ri for the difference di.
Step 5: Calculate the number of bits hidden into each block by the formula t= ⌊log2 wi⌋ , wi is the width of the optimal range Ri .
Step 6: If operating on RED block and 't' _ 3 then execute following steps; otherwise no extractionIf operating on GREEN block and 't' _ 5 then execute following steps; otherwise noextractionIf operating on BLUE block and 't'<=7 then execute the following steps
Step 7: Extract 't' bits, by the extracting method of original PVD.
Step 8: Check the LSB of Pi . If it is 1, replace the MSB position of extracted 't' bits with '1'.Otherwise do nothing.

Discrete cosine transformations
Data embedding
Data bits are concealed by altering the LSB of elements of zigzag array.
a) If data bit is „0", then make the DCT coefficient even or,
b) If the data bit is „1", then make the DCT coefficient odd.

Dequantization and inverse DCT

After embedding data zigzag array is again converted into 8×8 block. These blocks are dequantized and inverse DCT is performed. The entire 8×8 blocks are combined to form the stego image which is then sent to receiver. Complete embedding algorithm is given as follow:
Input: An M×N size cover image and data to be concealed.
Output: Stego image.
Step 1: Divide the cover image into 8×8 blocks. Step 2: Perform 2-D DCT on each block.
Step 3: Perform quantization on each block.
Step 4: Perform zigzag scan to convert 8×8 block into one dimensional array.
Step 5: Replace the LSB of DCT coefficients with data bits. Step 6: Convert 1-D zigzag array back to 8×8 block.
Step 7: Perform Inverse DCT on each block.
Step 8: Combine all the blocks to form stego image.

Extraction of secret message
The stego-image is received in spatial domain. Now stego image is divided into 8×8 blocks and DCT is performed on each block. Then scan the DCT block in zigzag way and extract the embedded data. Extraction algorithm is given as follows:
Input: Stego image.
Output: Secret message.
Step 1: Divide the stego image into 8×8 blocks.
Step 2: Perform 2-D DCT on each block.
Step 3: Perform quantization on each block.
Step 4: Perform zigzag scan to convert 8×8 block into one dimensional array.
Step 5: Check the DCT coefficient.
a) If DCT coefficient is even then data bit is 0 or,
b) If DCT coefficient is odd then data bit is 1.

ISSN(Online) : 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 5, Issue 5, May 2016

Step 6: Concatenate the bits to obtain secret message and display it on screen.

IV. EXPERIMENTAL RESULTS

The performance of the proposed algorithms is evaluated by conducting experiments pixel value differencing for color image as shown in the figure where embedded image along with original image is shown with RGB planes.

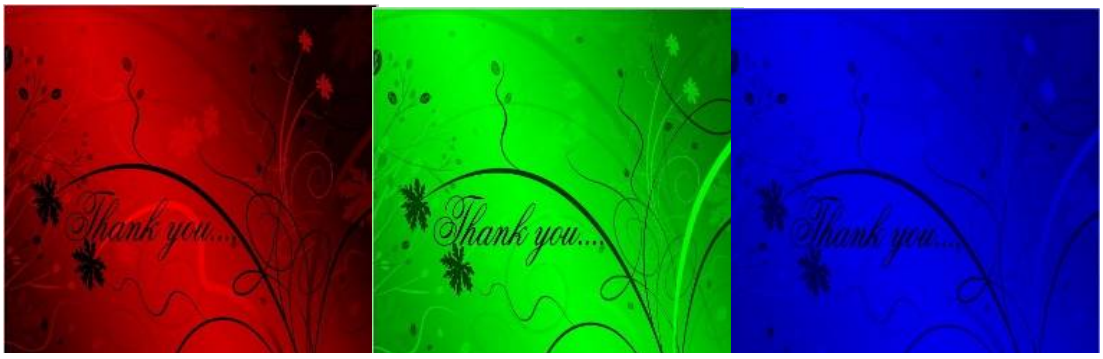

Fig: 1 Hello.bmp (a)Red plane (b)Green plane (c)Blue

As shown in figure 1 it represents the RGB planes separated where we get 8 bits for each pixel for data embedding purpose. Here pixel value differencing and discrete cosine transformations techniques are used for data embedding.

Fig:2 (a) Cover image (b) Stego image

As shown in the figure 2 cover image is input for hiding text data and stego image is generated after embedding of data which uses PVD and DCT.

Fig:3 (a)Cover image (b)Stego image

Next DCT Based steganography using transform where DCT transformations done to generate the DCT coefficeints and then this values are quantized using quantization table then embedding of data is done .

ISSN(Online) : 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 5, Issue 5, May 2016

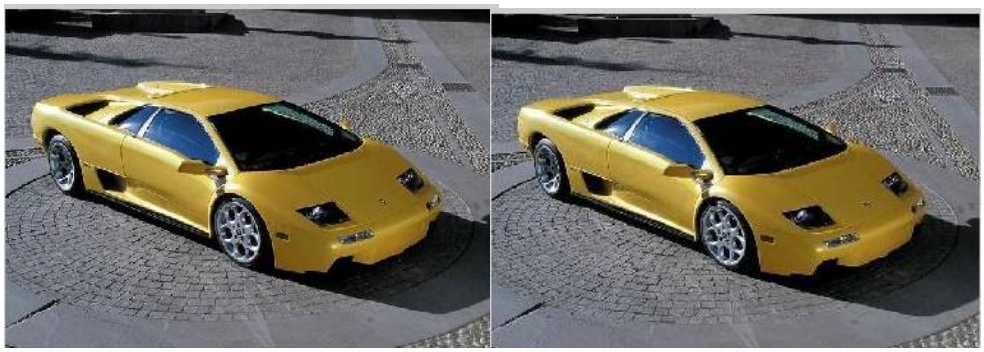

Fig. 4(a) Cover image (b)Stego image

As shown in the figure 4 diablo image which uses discrete cosine transformation technique for embedding of data and even extraction of data.

Cover image (512*512)	Proposed method 1 (Pixel value differencing) PSNR	Proposed method 2 (Discrete cosine transformations) PSNR
hello	44.44	53.33
Lena (color)	42.26	55.44
Diablo	41.41	55.32

Fig: 5 Comparision between two PVD and DCT

As shown in figure 5 both the pixel value differencing technique and discrete cosine trransformation techniques are compared using peak signal to noise ratio term.

V. CONCLUSION

In this paper,a steganographic method for data hiding by using pixel value differencing in colour images which also guarantees that no pixel value will exceed the range 0 to 255 in stego-image. In this Proposed scheme on colour images gives more security than the original PVD used in grey images and also provides better visual quality of stego-image. Furthermore, proposed method extracts the hidden secret message efficiently without using the original cover image.In addition to this a mixed approach that applies the spatial domain with the frequency domain of steganography techniques. The idea is to utilize a significant bit of the DCT coefficients of a cover image to hide encrypted message bits. Thereafter, the information and the variation of the coefficients, affected by the embedding process, are spread in the stego image by utilizing the inverse of the DCT process.After this both pixel value differencing and discrete cosine transformation techniques are compared for better image quality and roboustness.

REFERENCES

[1] Wenqiong Yu, “Blind Detection for JPEG Steganography”, International Conference on Networking and Information Technology , pp. 128-132, July 2010.
[2] AChung, K.L., Shen, C.H. and Chang, “A novel SVD- and VQ-based image hiding scheme”.Pattern Recognition Letters, 22, pp. 1051 – 1058, 2001.
[3] Iwata M., Miyake K., and Shiozaki, “Digital Steganography Utilizing Features of JPEG Images”, IEICE Transfusion Fundamentals, E87-A, 4, pp. 929 – 936, 2004.
[4] M. Kharrazi06, H. Sencar, and N. Memon, “Performance study of common image steganography and steganalysis techniques,” Communications of the SPIE and IS&T, 15, No.4, pp. 1017-9909, Oct- Dec., 2006.
[5] Nedal M.S. Kafari, Hani Y. Suleiman, “Bit-4 of Frequency Domain DCT Steganography Technique”, FIRST national conference on networked digital technologies, pp. 286-291, 2009.

ISSN(Online) : 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 5, Issue 5, May 2016

[6] H.B. Kekre, Archana Athawale, Pallavi N. Halarnkar, "Performance Evaluation of Pixel Value Differencing and Kekre's Modified Algorithm for Information Hiding in Images", International Conference on Advances in Computing, Communication and Control (ICAC3'09).
[7] Deepak Singla, Rupali Syal ,"Data Security Using LSB & DCT Steganography In Images",IEEE Trans, 2012.
[8] Sumedha Sirsikar, Jagruti Salunkhe,"Analysis of data hiding using Digital Image Signal Processing", International Conference on Electronic Systems, Signal Processing and Computing Technologies 2014.