International Journal of Electronics Communication and Computer Engineering
Volume 4, Issue 2, ISSN (Online): 2249–071X, ISSN (Print): 2278–4209

Pixel Swap Method to Shroud Information

Reena M. Patel
EC department, LDRP-Institute of technology and research, Gandhinagar, Gujarat

D. J. Shah
Principal, S P Collage of Engineering, Visnagar, Gujarat

Abstract **- Steganography is an art of secret communications. Its main purpose is to hide the occurrence of communication over a public channel. Steganalysis is the art and science of detecting a secret communication. Data hiding methods, there have been a number of steganography embedding techniques proposed over the past few years. In turn the developments of these techniques have led to an increased interest in steganalysis techniques. Steganalysis techniques have become more attractive since they work independently of the embedding technique. In my paper I go to discuss about pixel sweep method based on DCT in transform domain which use in stegnography. In this paper, authors' goal is to compare result with of available algorithm with modified algorithm and discuss about their capacity, delectability (perceptibility), robustness to attacks, PSNR and their Histogram.**

Keywords **- DCT, Histogram, Pixel Swap, Steganography.**

I. INTRODUCTION

There could be some important data that need to be secured (hide) during transmission. Therefore, how to hide the secret messages during transmission becomes an important research issue. Steganography [1] provides a kind of data hiding method that conceals the existence of the secret messages in the media. Today Steganography are mostly used for hiding a data. An image is selected as the media to hide the secret message (text) in it. Steganography techniques have led to an increased interest in Steganalysis techniques. Steganalysis techniques are nothing but investigation of hidden information.

Steganography is the art and science of secret communication, aiming to hide the existence of the Secret data (message) from a third party. The word steganography comes from the Greek word "stegano" meaning covered (or secret) and "graphy" meaning writing (or drawing). So, steganography literally means covered writing as described by Dr. Mohammed et al [2]. Steganography simply takes one piece of information and hides it within another. Among these methods are invisible inks, microdots, digital signatures, covert channels and spread-spectrum communications. Today, thanks to modern technology, steganography is used on text, images, sound, signals, and more. The advantage of steganography is that it can be used to secretly transmit messages without the fact of the transmission being discovered.

Steganalysis is Detection of steganography by a third party. As per Michael [3] Steganalysis will analyze whether a given content, contains any secret message hidden into it, or we can say that "The Investigation of Hidden Information". Steganalysis is an extremely difficult science, as it relies on insecure steganography. If steganography is to be successful, it should leave no indication that a secret message exists. Thus, if the model has been created successfully, it should be a difficult task for any third party to spot that alteration has occurred.

In terms of development, Steganography is comprised of two algorithms, one for embedding and one for extracting. The embedding process is concerned with hiding a secret message within a cover work, and is the most carefully constructed process of the two. A great deal of attention is paid to ensuring that the secret message goes unnoticed if a third party were to intercept the cover work. The extracting process is traditionally a much simpler process as it is simply an inverse of the embedding process, where the secret message is revealed at the end. The entire process of steganography for images can be presented graphically as two inputs are required for the embedding process. Fig 1 shows the data hiding model at sender.

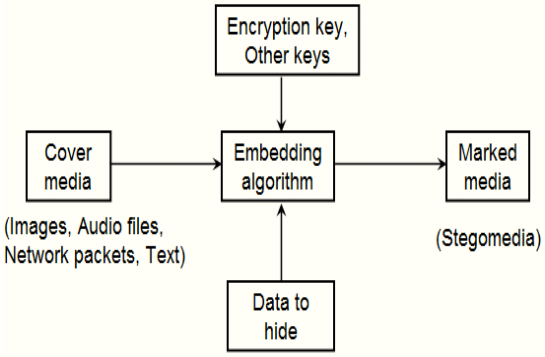


Fig.1. Data Hiding Model

The next step is to pass the inputs through the Stego-system Encoder, which will be carefully engineered to embed the message within an exact copy of the cover work, such that minimum distortion is made; the lower the distortion, the better the chances of undetectability. The stego-system encoder will usually require a key to operate, and this key would also be used at the extraction phase. This is a security measure designed to protect the secret message. Without a key, it would be possible for someone to correctly extract the message if they managed to get hold of the embedding or extracting algorithms. However, by using a key, it is possible to randomize the way the stego-system encoder operates, and the same key will need to be used when extracting the message so that the stego-system decoder knows which process to use. This means that if the algorithm falls into enemy hands, this extremely unlikely that they will be able to extract the message successfully. The resulting output from the stego-system encoder is the stegogramme, which is designed to be as close to the cover work as possible, except it will contain the secret message. This stegogramme is then sent over some communications channel along with the key that was used to embed the message. Both the stegogramme and the key are then fed into the stego-system decoder where an

International Journal of Electronics Communication and Computer Engineering
Volume 4, Issue 2, ISSN (Online): 2249–071X, ISSN (Print): 2278–4209

estimate of the secret message is extracted. Fig 2 show extracted model for stegogramme at the receiver side.

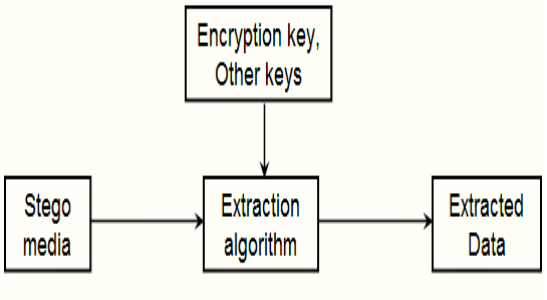


Fig.2. Data Extraction model

II. CONCEPT

In order to understand more about how a steganographic algorithm is created, it is necessary to consider the concepts of steganography like perceptibility, capacity & robustness [4].

1. Perceptibility: The stegogramme that is produced after embedding a secret message should not be altered such that it is visually obvious that information has been embedded. In fact, the resulting image should be so similar to the original that if you compare both side by side, you should not be able to see any difference at all between the two.

2. Capacity: The amount of information that is embedded should be as small as possible. Logic suggests that the longer the message, the more the image has to be altered to compensate for this. Obviously, the more a work is modified, the easier it is for the steganalyst to discover changes within an image. Therefore, the usual practise for embedding is to make the message as short as possible so that the image is altered as little as possible.

3. Robustness: This refers to the degree of difficulty required by a steganalyst to determine whether or not the image contains a hidden message or not. A good implementation of steganography would be one where the image can be subjected to many attacks that each proves inconclusive.

If a steganographic algorithm can fulfill these three principles, then the resulting image will highly likely reach its recipient undetected, meaning a successful implementation of steganography has been developed.

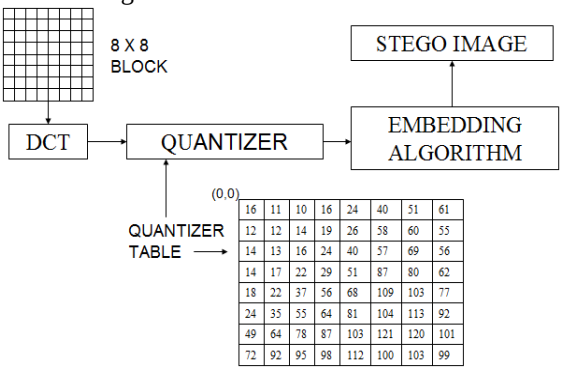
III. TRANSFORM DOMAIN TECHNIQUES

This technique hides data in mathematical functions that are often used in algorithms. These techniques try to encode message bits in the transform domain coefficients of the image [5]. Data embedding performed in the transform domain is widely used for robust data hiding. Similar techniques can also realize large-capacity embedding for steganography [6]. Candidate transforms include discrete cosine Transform (DCT), discrete wavelet transform (DWT), and discrete Fourier transform (DFT). By being embedded in the transform domain, the hidden data resides in more robust areas, spread across the entire image, and provides better resistance against signal processing. For example, we can perform a block DCT and, depending on payload and robustness requirements, choose one or more components in each block to form a new data group which is pseudo randomly scrambled and undergoes into a second layer transformation. Modification is then carried out on the double transform domain coefficients using various schemes. These techniques have high embedding and extraction complexity. Because of the robustness properties of transform domain embedding, these techniques are generally more applicable to aspect of data hiding.

- Embed secret message in a transform space (e.g. frequency domain) of cover
- Example: Steganography in the Discrete Cosine Transform (DCT) domain as described by Neil et al [7]
  - Split the cover image into 8×8 blocks. Each block is used to encode one message bit
  - Blocks are chosen in a pseudorandom manner
  - The relative size of two pre-defined DCT coefficients is modulated using the message bit
  - The two coefficients are chosen from middle frequencies (trade off between robustness and imperceptibility)

DCT based algorithm

The classic and still most popular domain for image processing is that of the Discrete Cosine Transform. The DCT allows an image to be broken up into different frequency bands, making it much easier to embed watermarking information into the middle frequency bands of an image.



16	11	10	16	24	40	51	61
12	12	14	19	26	58	60	55
14	13	16	24	40	57	69	56
14	17	22	29	51	87	80	62
18	22	37	56	68	109	103	77
24	35	55	64	81	104	113	92
49	64	78	87	103	121	120	101
72	92	95	98	112	100	103	99

Fig.3. Basic step of DCT base algorithm

As shown in Fig 3, the basic steps of DCT base algorithm are as follow:

- Each color plane is partitioned into 8x8 blocks
- Apply DCT to each block
- Values are quantized by dividing with preset quantization values (in a table)
- Values are then rounded to nearest integer

IV. PIXEL SWAP TECHNIQUE

The main motivation the steganographic algorithm proposed in this section is to embed data such that the histogram of the image does not get modified. Such a requirement entails an embedding procedure which does not modify the pixel values such that the corresponding bin value in the histogram is changed. We propose a

International Journal of Electronics Communication and Computer Engineering
Volume 4, Issue 2, ISSN (Online): 2249–071X, ISSN (Print): 2278–4209

simple yet effective algorithm called "Pixel Swap Embedding" [8][9] which embeds message bits into the cover image without making any modifications to the image histogram. The main idea is to consider a pair of pixels such that their difference is within a fixed threshold value. To embed a value of 0 check that if the first pixel is greater than the second pixel or not. Otherwise swap these two gray level values. Similarly pixel value of 1 can be embedded by making the value of first pixel lesser than the second pixel. The algorithm is discussed formally in the next subsection.

The basic algorithm is described in as splitting the image into 8x8 blocks and calculating the DCT of the block. Then two middle-frequency (so that they are not to altered by the quantization/compression which will take place in JPEG) are chosen and agreed upon by both send and receive parties.

A block encodes a 1 if DCT (a,b) > DCT(c,d) otherwise it encodes a 0 as shown in Fig 4 [6]. In the encoding step the coefficients are swapped if their relative size does not match with the bit to be encoded. Since the JPEG compression can affect the relative size of the coefficients the algorithm ensures that **abs(DCT(a,b) - DCT(c,d)) > x** where x is a value which represents the tradeoffs between image quality and robustness.

for $i = 1, \ldots, \ell(M)$ do
  choose one cover-block b_i
  $B_i = \mathcal{D}\{b_i\}$
  if $m_i = 0$ then
    if $B_i(u_1, v_1) > B_i(u_2, v_2)$ then
      swap $B_i(u_1, v_1)$ and $B_i(u_2, v_2)$
    end if
  else
    if $B_i(u_1, v_1) < B_i(u_2, v_2)$ then
      swap $B_i(u_1, v_1)$ and $B_i(u_2, v_2)$
    end if
  end if
  adjust both values so that $|B_i(u_1, v_1) - B_i(u_2, v_2)| > x$
  $b'_i = \mathcal{D}^{-1}\{B_i\}$
end for
create stego-image out of all b'_i

Fig.4. Pixel swap method: encoding process

Pixel Swap - Modification

- Proposed algorithm works fine when value of *(u1,v1)* and *(u2,v2)* are not same.
- Algorithm don't specify what to do when *(u1,v1)* and *(u2,v2)* having same value.
- We modified it by changing values of *(u1,v1)* and *(u2,v2)* according to input message bit and threshold value.

for *i* = 1, ..., *l(M)* **do**
  get cover-block *bi* associated with bit *i*
$B_i = D\{b_i\}$
if $Bi(u_1,v_1)<Bi(u_2,v_2)$ **then**
  $m_i=0$
  else
  $m_i=1$
end if
end for

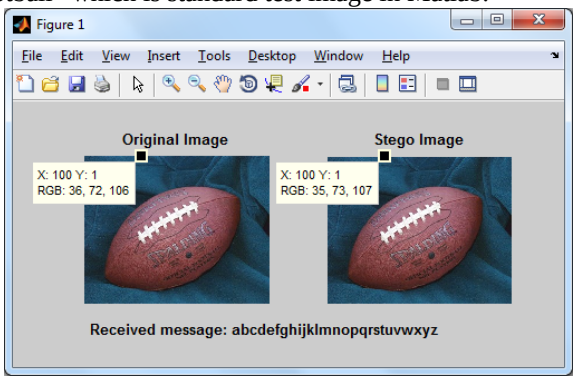
Fig.5. Pixel swap method: decoding process

As shown in Fig 5, decoding is straightforward in that all available blocks are DCT-transformed and by comparing the coefficients of each block the information is restored.

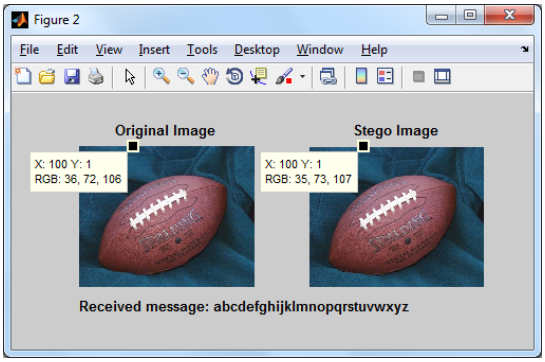
V. Result & Conclusion

We have tested the original & modified pixel swap algorithm by taking different cove images. We have passed input message "abcdefghijklmnopqrstuvwxyz" to both the algorithm in Matlab. Stego image is the image after embedding message (using some algorithm) into cover or original image. We get received message by passing stegoimage as input into decoding algorithm.

Fig 5 shows actual Matlab results for cover image "football" which is standard test image in Matlab.



(a) Original algorithm



(b) Modified algorithm

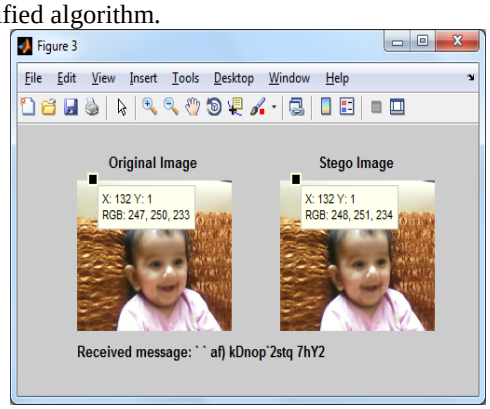
Fig.5. Result for cover image "football"

Fig 5(a) shows result for original algorithm while (b) shows for modified algorithm. As shown at bottom side in Fig 5(a) & (b), we get same received message in both algorithms. We have also shown RGB value for pixel at location x=100, y=1. RGB values for the original image are (36, 72, 106) while for stego image its (35,73,107). We have tested both algorithms for different images & kept same input message.

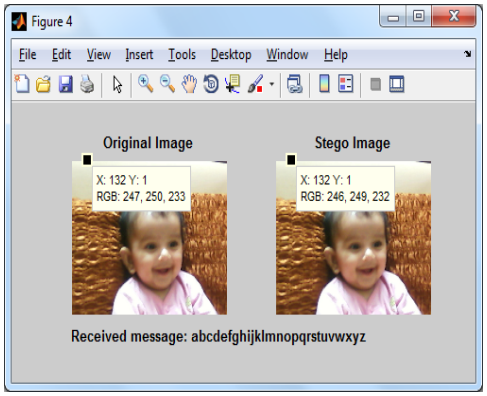
Fig 6 shows Matlab results for cover image "akshat" which is taken from camera. As shown at bottom side in Fig 6(a), the received message is different compare to input message.Fig 6(a) shows result of original algorithm, according to it the RGB values for the original image are (247, 250, 233) while for stego image it's (248, 251, 234) at location x=132, y=1.Fig 6(b) shows result of modified algorithm, according to it the RGB values for the original

International Journal of Electronics Communication and Computer Engineering
Volume 4, Issue 2, ISSN (Online): 2249–071X, ISSN (Print): 2278–4209

image are (247, 250, 233) while for stego image values are (246, 249, 232) at location x=132, y=1. Also the received message in Fig 6(b) is also same as input message in case of modified algorithm.



(a) Original algorithm



(b) Modified algorithm

Fig.6. Result for cover image "akshat"

Histogram Attack

Histogram of an image is a plot of number of pixels verses pixel intensity or value. In case of pixel swap algorithm we are changing DCT coefficients so we need histogram of DCT coefficients.

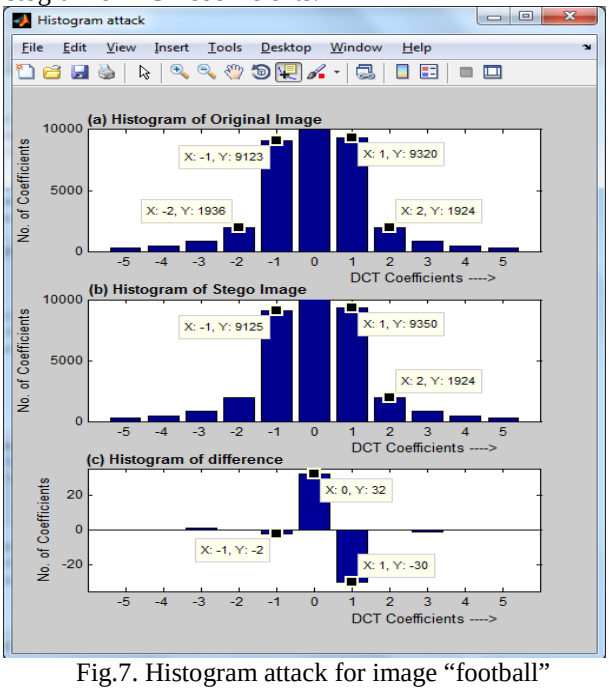


Fig.7. Histogram attack for image "football"

Fig 7 shows result of histogram attack for original image "football" & text "abcedfghijklmnopqrstuvwxyz" as input message. Histogram of DCT coefficients for original image and for stego image is shown in Fig 7(a) & (b) respectively (inside Fig 7). We have zoomed in these to show the values of "No. of Coefficients" (Y axis) for different intensity of "DCTCoefficients" (X axis). If we don't do it then we can't see it properly since for DCTCoefficients = 0 (X axis), we have No. of Coefficients = 215424 (Y axis) for original image. Histogramdifference of Fig 7(a) and (b) is plotted in Fig 7(c) for checking histogram attack. As shown in Fig 7(c), symmetry or asymmetry is not there i.e. at X= -1 we have Y= -2 while at X= 1 we have Y= -30. This kind of problems occur in various other DCT domain steganography algorithms but in case of pixel swap algorithm we don't have to worry about histogram attack.

PSNR & Capacity:

PSNR (Peak signal-to-noise ratio) is a standard measurement used in steganography technique in order to test the quality of the stego images. The higher the value of PSNR, the more quality the stego image will have. Let original image and stego image has size of M × N. The PSNR is calculated as follows:

$$PSNR = 10 \log_{10} \left(\frac{R^2}{MSE} \right)$$

$$MSE = \frac{\sum_{M,N} \left[I_1(m,n) - I_2(m,n) \right]^2}{M * N}$$

Note that R is the maximum possible pixel value of the images. For example, if the pixels are represented using 8 bits per sample, then the R value is 255. If the stego image has a higher PSNR value, then the stego image has more quality image.

Table I: PSNR and Capacity of Pixel swap algorithm for cover image "football.jpg" (320 x 256)

Capacity in 'bits'	Message length		PSNR (dB)
	in 'bits'	% of capacity	
3840	182	4.74 %	57.72
	959	24.97 %	52.48
	1918	49.95 %	47.68
	2877	74.92 %	45.41
	3836	99.89 %	44.98

Table I shows the PSNR values for different message length. Football.jpg has size of 320 x 256 & it is 24 bits image i.e. 3 planes (R, G, B). In pixel swap we are embedding 1 bit in 8 x 8 block i.e. in 64 pixels. So total capacity = (320 * 256 *3) / 64 = 3840 bits. Different size of messages is taken for checking PSNR. We are converting each character into ASCII format 7 bits. So message length will be always multiple of 7. As shown in Table I we have PSNR = 57.72 dB for text message "abcedfghijklmnopqrstuvwxyz". 44.98 dB is the minimum value of PSNR for message length around full capacity of image.

It can be clearly observed that Pixel Swapping is highly robust technique but at the same time its data hiding capacity is less compare to other techniques. Many

steganographic algorithms offer a high capacity for hidden messages (like LSB), but are weak against visual and statistical attacks (Histogram attacks).

REFERENCES

[1] Steganography - Wikipedia, the free encyclopedia files [Online]: http://en.wikipedia.org/wiki/Steganography

[2] Dr. Mohammed Al-Mualla and Prof. Hussain Al-Ahmad, "Information Hiding: Steganography and Watermarking", [Online].Available: http://www.emirates.org/ieee/information_hiding.pdf

[3] Michael T. Raggo, CISSP Principal Security Consultant VeriSign "Steganography, Steganalysis, & Cryptanalysis". "Steganography, Steganalysis, & Cryptanalysis", Michael T. Raggo, CISSP Principal Security Consultant , VeriSign

[4] Mehdi Kharrazi, Husrev T. Sencar, and Nasir Memon "Image Steganography: Concepts and Practice" WSPC/Lecture Notes Series: 9in x 6in, Institute of mathematical sciences, Singapore April 22,2004

[5] Westfeld, A. and Pfitzmann, A.: Attacks on Steganographic Systems. In: Pfitzmann A.(eds.): 3rd International Workshop. Lecture Notes in Computer Science, Vol.1768. Springer-Verlag, Berlin Heidelberg New York (2000) 61−75

[6] Vikram Vijayaraghavan and Prof.Wandell, Course project for Applied Vision & Image Systems (Winter2005): Transfer Domain Techniques [Online]. Available: http://scien.stanford.edu/pages/labsite/2005/psych221/projects/05/vvikram/stegotransfer.htm

[7] N. Provos, and P. Honeyman, Hide and Seek: An Introduction to Steganography, IEEE Security & Privacy, 1(3), 2003: 32-44

[8] Sur, P. Goel, and J. Mukhopadhyay, "A SDS based Steganographic scheme for reducing Embedding Noise", 15th International Conference on Advanced Computing and Communication, (ADCOM-2007), Guwahati, India, 18-21 Dec., pp. 771-775.

[9] D.C. Wu, and W.H. Tsai, "A Steganographic method for images by pixel-value differencing", Pattern Recognition Letters, vol. 24, Jan. 2003, pp. 1613–1626.

AUTHOR'S PROFILE

Reena M. Patel

received M.E. degree in communication system engineering from L.D. collage of engineering, Ahmedabad, India in 2009 and she is a research scholar at KSV University, Gandhinagar, Gujarat. Currently she is assistant professor in the department of electronics and communication Engineering at LDRP Institute of Technology and Research, Gandhinagar, Gujarat, India. She has presented & published numbers of research articles in national & International conferences & journals.

Dr. D. J. Shah

has completed his graduation from L.D.C.E, Ahmedabad India in 1992 and his M.E. from Indian Institute of Science, Banglore, India in 2001. He received PhD degree in Microcontroller from M.S. University, Baroda, India in 2008.

He served IT industry and academics for more than 21 years in various positions. Currently he is principal at S.P. Collage of engineering, Visnagar, Gujarat. He has presented and published many papers in national & international conferences & journals.

.