BIT LENGTH REPLACEMENT
STEGANOGRAPHY BASED ON DCT
COEFFICIENTS

K B Shiva Kumar¹, K B Raja², R K Chhotaray³, Sabyasachi Pattanaik⁴

¹Department of Telecommunication, Sri Siddhartha Institute of Technology, Tumkur, Karnataka, India.
²Department of Electronics and Communication, University Visvesvaraya College of Engineering Bangalore University, Bangalore, India.
³Department of Computer Science and Engineering, Seemanta College of Engineering, Mayurbhanj Balasore, Orissa, India
⁴Department of Computer Science and Engineering, Fakir Mohan University Balasore, Orissa, India

Abstract:
Steganography is a means of establishing secret communication through public channel in an artistic manner. In this paper, we propose Bit Length Replacement Steganography Based on DCT Coefficients (BLSDCT). The cover image is segmented into 8x8 blocks and DCT is applied on each block. The numbers of payload MSB bits are embedded into DCT coefficients of the cover image based on the values of DCT coefficients. It is observed that the proposed algorithm has better PSNR, Security and capacity compared to the existing algorithm.

Keywords: Steganography, Cover Image, Payload, Stego Image, Discrete Cosine Transform (DCT), Bit length.

1. INTRODUCTION

In the present electronic communication scenario, data security is one of the major challenges. After the World War II, the need for a secure and robust communication between the communicating entities has increased due to the fear of terrorism. The publishers of digital audio and video are worried of their works being corrupted by illegal copying or redistribution, hence it is of primary importance to protect information. Cryptography is the method to hide secret data by scrambling so that it is unreadable, however it does not assure security and robustness as the hacker can obviously guess that there is a confidential message passing on from the source to the destination. Steganography is concealed writing and is the scientific approach of inserting the secret data within a cover media such that the unauthorized viewers do not get an idea of any information hidden in it. Steganography is an alternative to cryptography in which the secrete data is embedded into the carrier in such way that only carrier is visible which is sent from transmitter to receiver without scrambling. The combination of cryptography and steganography provide high level security to the secrete information. Cover image is known as carrier image and is the original image in which the secret data ie., the payload is embedded. The unified image obtained after embedding the payload into the cover image is called the stego image. The recent boom in IT industry facilitates embedding data and security issues effectively.

Image Steganography includes several techniques of hiding the payload within the cover image. The most popular hiding techniques are Spatial Domain based Steganographic Techniques and Transform Domain based Steganographic Techniques. Spatial domain based steganography includes the Least Significant Bit (LSB) technique, and Bit Plane Complexity Steganographic (BPCS) technique. The LSB technique [1] is the most significant example of spatial domain embedding wherein the LSBs of the cover image is replaced by the MSBs of the payload. BPCS steganography hides secret data by means of block replacing. Each image plane is segmented into the same size pixel-blocks (a typical size of 8x8) which are classified into informative and noise like blocks. The noise like blocks is replaced by the secret blocks. In transform domain the cover image or the payload is transformed into frequency domain viz., Fast Fourier Transform, DCT, Discrete Wavelet Transform (DWT) and Integer Wavelet Transform. The DCT is used in common image compression format MPEG or JPEG, wherein, the LSBs of the DCT coefficients of the cover image are replaced by the MSBs of the payload. The Discrete Wavelet
Transform [2] is used for hiding the secret message into the higher frequency coefficient of the wavelet transform while leaving the lower frequency coefficient sub band unaltered. The various ways of using transform domain techniques in steganography are (i)The cover image is transformed into frequency domain and LSBs of transformed domain are replaced by the spatial domain payload bit stream. (ii)The payload is converted into frequency domain and the coefficients are embedded into the spatial domain LSBs of cover image. (iii) Both the cover and payload are transformed into frequency domain for embedding process. In contrary, steganalysis is a process of detecting the secret communication, against Steganography. Steganalysis is achieved by detecting any alteration in the carriers or the presence of some unusual signatures or any form of degradations. A hidden message can be attacked in different phases like stego-only attack, known cover attack, known message attack, known chosen cover or chosen message and known stego attack.

**Contribution** In this paper we proposed a Bit Length Replacement Steganography Based on DCT Coefficients, where the number of payload bits $L$ is embedded into the DCT coefficient of cover image based on the DCT coefficient of cover image in order to maximize the hiding capacity.

**Organization:** The paper is organized into following sections. Section 2 is an overview of related work. The steganography model is described in section 3. Section 4 discusses the algorithms used for embedding and extracting process. Performance analysis is discussed in section 5 and Conclusion is given in section 6.

## 2. LITERATURE SURVEY

Weiqi Luo et al., [3] proposed LSB matching revisited image steganography and edge adaptive scheme which can select the embedding regions according to the size of secret message and the difference between two consecutive pixels in the cover image. For lower embedding rates, only sharper edge regions are used while keeping the other smoother regions as they are. When the embedding rate increases, more edge regions are released adaptively for data hiding by adjusting just a few parameters. Safy et al., [4] proposed an adaptive steganographic technique in which the bits of the payload are hidden in the integer wavelet coefficients of the cover image adaptively along with optimum pixel adjustment algorithm. Hassan Mathkour et al., [5] compared the strengths and weaknesses of the existing techniques of steganography and implemented a new steganographic wizard based tool, which have been examined against several other tools like F5, S-Tools etc., for more robust and secure steganography. Vijayalakshmi et al.,[6] proposed modulo based image steganography algorithm. The method combines samples of LSB bits using addition modulo to get the value which is compared to the part of the payload. If these two values are equal, no change is made in sample otherwise add the difference of these two values to the sample. Wein Hong et al., [7] proposed a lossless steganography technique wherein the secret information is hidden inside the compressed Absolute Moment Block Truncation Coding image. Naji et al., [8] analysed different steganographic techniques and weaknesses in the respective techniques. Hassan Shirali-Shahreza and Mohammad Shirali-Shahreza [9] proposed a synonym text steganographic technique in which the words in American English are substituted by the words having different terms in British English and vice-versa. Vladimir Banoci et al., [10] presented Code Division Multiple Access Technique, where the embedding process is carried out by hiding secret image in each block of quantized DCT coefficients. Chen Ming et al., [11] discussed different steganography tool algorithms and classified the tools into spatial domain, transform domain, document based, file structure based and other categories such as spread spectrum technique and video compressing encoding. Mankun Xu et al., [12] proposed a technique to estimate the embedding rates of secret information in the Model Based steganography based on least square method.

Abbas Cheddad et al., [13] enhanced steganography in digital images by proposing a color image steganography which performs better than S-Tools and F5. The secret message is embedded in specific areas of the cover image where the payload is safer. Aos et al., [14] implemented a means of hiding the secret information in the Executable (.EXE) file, such that it is unrevealed to any anti-virus software, since anti-virus software secretly read the furtive data embedded inside the cover file. Daniela Stanescu et al., [15] proposed a technique in which steganographic algorithm is implemented on embedded devices and also suggests on using microcontrollers or microprocessors for executing steganographic algorithms instead of using Field Programmable Gate Arrays. Jin-Suk Kang et al., [16] described steganography using block-based adaptive threshold. Initially the bit-plane blocks of the cover image and the payload are compared and if the blocks are similar, then those blocks of the payload are embedded in the cover image. Mci-Ching Chen et al., [17] introduced an extension to the existing steganography to improve the capacity. At the receiver, template matching techniques are used to find the location of the object file. Neha Agarwal and Marios Savvids [18] proposed a steganographic method to hide biometric data in DCT coefficients of the cover.
image in a more robust way. Nan Wu and Min-Shiang Hwang [19] developed steganographic techniques for gray scale images and introduced schemes such as high hiding capacity schemes and high stego-image degradation imperceptibility schemes. Bo-Luen Lai and Long-Wen Chang [20] proposed a transform domain based adaptive data hiding method using Haar discrete wavelet transform. Most of the data was hidden in the edge region as it is insensitive to the human eye. Po-Yueh Chen and Hung-Ju Lin [21] developed a frequency domain based steganographic technique. The secret data is embedded in the high frequency coefficients/sub-bands of DWT and the low frequency sub-bands are not altered. Kang Leng Cheiew and Josef Pieprzyk [22] proposed a scheme to estimate the length of hidden message through histogram quotient in Binary image embedded by using Boundary pixels Steganography technique. Mahdi Ramezani and Shahrokh Ghaemmaghami [23] presented an Adaptive Steganography method with respect to image contrast thereby improving the embedding capacity of stego image contrast by selecting valid blocks for embedding based on average difference between the gray level values of the pixels in 2*2 blocks of non-overlapping spatially and their mean gray level. Saed Sarreshtedari and Shahrokh Ghaemmaghami [24] proposed a high capacity image steganography in Discrete Wavelet Transform (DWT) domain. Hongmei Tang et al., [25] suggested a scheme for image encryption and steganography by encrypting the message with a combination of gray value substitution operation and position permutation and then it is hidden in the cover image.

3. MODEL

Steganography is used for covert communication. The secret image which is communicated to the destination is embedded into the cover image to derive the stego image. In this section evaluation parameters and proposed embedding and retrieval techniques are discussed.

3.1 Evaluation Parameters

3.1.1 Mean Square Error (MSE):

It is defined as the square of error between cover image and stegoimage. The distortion in the image can be measured using MSE and is calculated using Equation 1.

$$MSE = \left[ \frac{1}{N \times N} \sum_{i=1}^{N} \sum_{j=1}^{N} (X_{ij} - \bar{X}_{ij})^2 \right]$$  \hspace{1cm} (1)

Where:

- $X_{ij}$: The intensity value of the pixel in the cover image.
- $\bar{X}_{ij}$: The intensity value of the pixel in the stego image.
- N: Size of an Image.

3.1.2 Peak Signal to Noise Ratio (PSNR):

It is the measure of quality of the image by comparing the cover image with the stegoimage, i.e., it measures the statistical difference between the cover and stegoimage, is calculated using Equation 2.

$$PSNR = 10 \log_{10} \frac{255^2}{MSE} \text{db}$$  \hspace{1cm} (2)

3.1.3 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 the Maximum Hiding Capacity (MHC) in terms of percentage.
3.2 Proposed BSLDCT Embedding Technique

The payload is embedded into the cover image by segmentation, DCT and coherent bit length $L$ is shown in the Figure1.

![Block Diagram of BSLDCT Embedding Technique](image)

3.2.1 Cover Image:

The cover image is color or gray scale of any size and format. If the cover image is color then convert into gray scale image and corresponding pixel intensity values.

3.2.2 Pixel Management:

The gray scale cover image pixel intensity vary from zero to 255. During the payload embedding process the intensity values of cover image may exceed lower and higher level limits which results in difficulty to retrieve the payload at the destination. Hence the cover image pixel intensity values are limited to lower 15 and upper 240 instead of zero and 255.

3.2.3 Segmentation:

The cover image is segmented into 8x8 matrices. The DCT is applied on each 8x8 block to get DCT coefficients which are used to hide the payload Most Significant Bit (MSB) based on the DCT coefficient values of the cover image.

3.2.4 2D-DCT:

Transform each 8x8 matrix into frequency domain using 2D-DCT. Using DCT on 8*8 sub blocks has an advantage of less computation time for embedding as well as security to payload increases compared to applying DCT to whole cover image.
3.2.5 Coherent bit length L:

The length $L$, which determines the number of LSBs of each DCT coefficients ($C_0$) of cover image that can be used to hide the payload MSB bits and is calculated according to the conditions given below:

- If $C_0 \geq 2^5$; \quad L=5
- If $2^4 \leq C_0 \leq 2^5$; \quad L=4
- If $2^3 \leq C_0 \leq 2^4$; \quad L=3
- Else \quad L=2

The conditions to determine $L$ also serves as secret key to retrieve the payload at the destination.

3.2.6 Embedding:

The spatial domain payload bits are embedded into the DCT coefficients of the cover image coherently based on the values coefficients. Four MSBs of each spatial domain payload pixel are embedded into the cover image DCT coefficients in a continuous manner depends on the value of $L$ to derive the stegoimage in DCT domain.

3.2.7 IDCT:

The stegoimage in the transform domain is converted to the spatial domain by applying IDCT. The stegoimage obtained is similar to the cover image and the difference is not perceptible by the human eye. This image is transmitted to the destination over the open channel.

3.3 BSLDCT Retrieval Technique

The payload is retrieved from the stegoimage by adapting reverse process of embedding technique is as shown in Figure 2

3.3.1 Stegoimage:

The image received at the destination over the open channel is the stegoimage. Any intruder interfering in the transmission process will only be able to read the stegoimage and cannot extract the secret image embedded in it as the payload bits are embedded coherently.

3.3.2 Segmentation:

The stegoimage is segmented into 8x8 blocks to ensure proper retrieval of payload.

---

**Fig. 2 Block Diagram of BSLDCT Retrieval Technique**

ISSN: 0975-5462

3565
3.3.3 2D-DCT:

The 8x8 sub blocks of stegoimage are transformed into frequency domain to generate DCT coefficients using 2D-DCT.

3.3.4 Bit length L:

At the receiver $L$ is determined based on the DCT coefficient values similar to the conditions of embedding technique. A spar matrix is initially taken as payload output matrix. The payload bits are extracted into this output matrix based on the value of $L$ to get back the payload.

4. ALGORITHMS

Problem definition:

The cover image and the payload are given. The objectives are

(i) Embed the payload into the cover image to derive the stegoimage for secure .
(ii) Improve PSNR between cover image and stegoimage.

4.1 Embedding algorithm:

The embedding BSLDCT algorithm is given in Table 1, the payload is embedded into the cover image using segmentation, DCT and coherent length. The cover image is segmented into smaller blocks of size 8x8 matrices to increase the embedding capacity. The payload is embedded into the DCT coefficients of cover image based on coherent length $L$ determined by the coefficient values to enhance the security to the secrete message.

**Table 1: Embedding algorithm of BSLDCT**

<table>
<thead>
<tr>
<th>Inputs: Cover image and Payload</th>
</tr>
</thead>
<tbody>
<tr>
<td>Output: Stego image</td>
</tr>
</tbody>
</table>

1. A cover image of any size and format is considered and is converted to gray scale.
2. Apply pixel management to the cover image, to avoid overflow and underflow.
3. Segmentation of cover image into 8*8 blocks and are transformed into DCT domain.
4. The number of bits $L$ of each DCT coefficient of cover image to be replaced by the payload MSB bits using coherent bit length.
5. The stego image obtained in the DCT domain is converted into the spatial domain using IDCT.

4.2 Retrieving AI Algorithm:

The payload is retrieved from the stego image by the adaptive reverse procedure of embedding and is given in the Table 2.
Input: Stego image  
Output: Retrieved Payload  
1. The stego image is segmented into 8*8 blocks.  
2. The 8*8 blocks are transformed into frequency domain using DCT.  
3. The payload length $L$ for each DCT coefficient is calculated similar to the procedure adapted in the embedding technique.  
4. Extract $L$ bits from each DCT coefficients.  
5. The payload is constructed using $L$ number of bits.

Table 2: Retrieving Algorithm

5. PERFORMANCE ANALYSIS

For performance analysis, Cover Image (CI) and Payload (PL) of any size and formats are considered. The payload Barbara image is embedded into the cover Lena image to derive the stego image and the payload is retrieved from stego image using reverse embedding process at the destination is as shown in the Figure 3. The cover Baboon image is considered into which the payload Cameraman (CM) image is hidden to generate stego image. At the recipient end, the payload is extracted from the stego image is shown in the Figure 4.

![Fig. 3: (a) CI: Lena (b) PL: Barbara (c) Stego Image (d) Retrieved PL](image1)

![Fig. 4: (a) CI: Baboon (b) PL: Cameraman (c) Stego Image (d) Retrieved PL](image2)

The Maximum Hiding Capacity (MHC) in terms of bits and percentage as well as the PSNR between the cover image and stegoimage is tabulated for existing algorithm [4] Adaptive Steganography Based on Integer Wavelet Transform (ASIWT) and the proposed algorithm CSSDCT is given in the Table 3. It is observed that the PSNR is improved around 25% in the proposed algorithm compared to the existing algorithm for the same MHC.
The graph shown in Figure 5 gives the corresponding PSNR for different embedding capacity values for two sets of images. In the first set Lena is used as cover image and Barbara as the payload and in the second set, Baboon is taken as the cover image and Cameraman as payload. The graph depicts that the quality of the stego image which is determined by PSNR not only depends on the algorithm but also on the images used. The Lena as cover image gives higher PSNR compared to the cover image Babbon.

<table>
<thead>
<tr>
<th>Image</th>
<th>Technique</th>
<th>MHC</th>
<th>MHC</th>
<th>PSNR (db)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Lena</td>
<td>CSSDCT</td>
<td>986408</td>
<td>47</td>
<td>39.48</td>
</tr>
<tr>
<td>Barbara</td>
<td>ASIWT</td>
<td>986408</td>
<td>47</td>
<td>31.80</td>
</tr>
<tr>
<td>Baboon</td>
<td>CSSDCT</td>
<td>1008593</td>
<td>48</td>
<td>38.60</td>
</tr>
<tr>
<td>CM</td>
<td>ASIWT</td>
<td>1008593</td>
<td>48</td>
<td>30.89</td>
</tr>
</tbody>
</table>

6. CONCLUSION

The steganography is used in the covert communication to transport secrete information. In this paper Bit Length Replacement Steganography using Segmentation and DCT is proposed. The cover image is segmented into smaller matrix of size 8x8 and converted to DCT domain. The MSB bits of payload in spatial domain are embedded into each DCT coefficients of cover image based on the coherent length $L$ which is determined by the DCT coefficient values. The performance results in terms of PSNR for different kinds of images and dimensions are better in the proposed algorithm compared to the existing algorithm. In future the technique can be verified for robustness.
REFERENCES


ShivaKumar K B received the BE degree in Electronics & Communication Engineering, ME degree in Electronics, MBA from Bangalore University, Bangalore and MPhil from Dravidian University Kuppam. He is pursuing his Ph.D. in Information and Communication Technology of Fakir Mohan University, Balasore, Orissa under the guidance of Dr. K. B. Raja, Assistant Professor, Department of Electronics and Communication Engineering, University Visvesvaraya College of Engineering, Dr.Sabayasachi Pattanaik Reader & HOD, Department of Information and Communication Technology F M University, Balasore, Orissa R K Chhotaray, Principal, Seemantha Engineering College, Orissa. He is currently working as Professor, Dept. of Telecommunication Engineering, Sri Siddhartha Institute of Technology, Tumkur. His research interests include Signal processing, Multi rate systems and filter banks, and Steganography.
Dr. K B Raja is an Assistant Professor, Dept. of Electronics and Communication Engineering, University Visvesvaraya college of Engineering, Bangalore University, Bangalore. He obtained his BE and ME in Electronics and Communication Engineering from University Visvesvaraya College of Engineering, Bangalore. He has been awarded Ph.D. in Computer Science and Engineering from Bangalore University. He has 25 years of teaching experience and has over 45 research publications in refereed International Journals and Conference Proceedings. Currently he is guiding six Ph D scholars in the field of image processing. He has received Best Paper Award for the contributed paper in Fourteenth IEEE-ADCOM 2006. His research interests include Image Processing, Biometrics, VLSI Signal Processing and computer networks.

Dr. Sabyasachi Pattnaik has done his B.E in Computer Science, M Tech., from IIT Delhi. He has received his Ph D degree in Computer Science in the year 2003 & now working as Reader in the Department of Information and Communication Technology, in Fakir Mohan University, Vyasavigar, Balasore, and Orissa, India. He has got 20 years of teaching and research experience in the field of neural networks, soft computing techniques. He has got 42 publications in national & international journals and conferences. He has published three books in office automation, object oriented programming using C++ and artificial intelligence. At present he is involved in guiding eight Ph D scholars in the field of neural networks, cluster analysis, bio-informatics, computer vision & stock market applications. He has received the best paper award & gold medal from Orissa Engineering congress in 1992 and institution of Engineers in 2009.

Dr. R K Chhotaray received his B.Sc Engineering in Electrical Engineering and M.Sc Engineering in Electrical Engineering with specialization in Control Systems from Banaras Hindu University, and Ph D in Control Systems from Sambalpur University. He was Professor and Head of Department of Computer Science and Engineering, Regional Engineering College, Rourkela, from which he retired in 2003. Currently he is working as Principal of Seemanta Engineering College, Orissa. He has been associated with many Universities of India in the capacity of Chairman and member of various Boards of Studies, syllabus committee, and Regulation committee. He has about hundred publications in International and National journals of repute, and has received Best Technical Paper award in many occasions. His special fields of interest include Control of Infinite dimensional Hereditary Systems, Modeling and Simulation, Theoretical Computer science, signal and Image processing, and optimization.