International Journal of Applied Engineering Research ISSN 0973-4562 Volume 10, Number 24 (2015) pp 44241-44245

Block Based Multi Level Continuous Reversible Character Encoding Scheme For Improved Data Hiding Using Color Values

Prof. B. Chitradevi,

Assistant Professor, Department of Computer Science, Thanthai Hans Roever College, Elambalur, Perambalur-621212

Dr. S. Manikandan,

Professor & Head, Department of Computer Science and Engineering, Sriram Engineering College, Perumalpattu, Chennai-602024.

ABSTRACT:
The problem of data hiding has been well studied in several methods and the application of steganography has been well known. To perform data hiding using steganography method has been used in number of situations and there are some issues of distortion and irreversible data as well as image. To overcome the issues of earlier methods, the block based continuous reversible character encoding scheme is proposed in this paper. The method starts with encoding the meta data in the first block of the image, where the size of block is decided based on the size of data to be encoded. First the method computes the size of data to be encoded in bit and computes number of blocks to be used. Then the method choose the first block with size 3×3, and each row of the pixels are used to encode different information. The first row is to store the size of data has been encoded and the next row is used to encode number of blocks being used. The third row is used to specify whether multi level encoding has been used or not. The method then splits the input data into number of characters and based on the value of multi level being used, the method encodes the data using averaging scheme.

Index Terms:
Data Hiding, Block based encoding, Multi Level Reversible Encoding, Steganography

1. INTRODUCTION:

The growth of information technology has opened the gate for the internet users to perform their most activities through the internet. So in order to perform the information exchange in efficient manner, the data has to be transferred in a secure manner. In earlier days the data has been transferred using some encryption methods, where the data has been encrypted using some public key based methods. For example, the RSA based method uses the public key for encryption. The same key has been used to decrypt the information. What happens in the middle is, if there exist any middle men then the malicious user can perform guessing attacks to detect the original data. The malicious user tries to decrypt the data by using any key which is selected in random manner. In most cases the malicious user could do the work successfully and get the original information from the encoded data. Such activities spoils the communication performed in many commercial transactions and spoils the entire communication to fail. So in order to improve the performance of communication security and to improve the tampering of communication protocols the concept of steganograpy has been introduced. Steganography is the process of hiding the data in the image pixels in some form and sends the image from the source to the destination. In the other side of communication, the user extracts the information hidden in the image being received. The data hiding is the process of hiding information to be sent to the remote place into the image and sends the image to the remote location where the data added in the image could be extracted in efficient manner.

The problem of data hiding is about how efficient the data hidden in the image could be retrieved in efficient manner. There are many algorithms has been used in earlier days and the methods has used various measures and strategies to encode the data into the image. The block based methods has use, each block to encode the data and in some of the methods other form of approaches has been used. The problem of block based approach is to decide how many blocks are necessary to encode the data and how much amount could be encoded in the image. Also the destination user does not knew about how much amount of data has been encoded in the image and how it has to be extracted from the image without failure.

Multi level reversible encoding is the process of hiding large information in the image in different manner. The method splits the image into number of blocks and according to the size of data to be hidden the method extracts the data from each block of the image. If the number of blocks is less then the image will be encoded in single level and the method use multi level encoding when the size of data is higher. And also the method could differentiate the block number when it has to use multi level decoding and when it has to use single level decoding.

2. RELATED WORKS:

There are number of data hiding mechanisms has been discussed earlier and we discuss some of the methods here in this section.

Reversible Data Hiding in Encrypted Images by Reserving Room Before Encryption [1], propose a novel method by reserving room before encryption with a traditional RDH algorithm, and thus it is easy for the data hider to reversibly embed data in the encrypted image. The proposed method can achieve real reversibility, that is, data extraction and image recovery are free of any error. Experiments show that this novel method can embed more than 10 times as large payloads for the same image quality as the previous methods, such as for PSNR=40 dB.

Reversible Data Hiding in Encrypted Image [2], proposes a novel reversible data hiding scheme for encrypted image. After encrypting the entire data of an uncompressed image by a stream cipher, the additional data can be embedded into the image by modifying a small proportion of encrypted data. With an encrypted image containing additional data, one may firstly decrypt it using the encryption key, and the decrypted version is similar to the original image. According to the data-hiding key, with the aid of spatial correlation in natural image, the embedded data can be successfully extracted and the original image can be perfectly recovered.

A Reversible Data Hiding Method for Encrypted Images [4], original work partitions an encrypted image into blocks, and each block carries one bit by flipping three LSBs of a set of pre-defined pixels. The data extraction and image recovery can be achieved by examining theblock smoothness. Zhang's work did not fully exploit the pixels in calculating the smoothness of each blockand did not consider the pixel correlations in the border of neighboring blocks. These two issues could reduce the correctness of data extraction. This letter adopts a better scheme for measuring the smoothness of blocks, and uses the side-match scheme to further decrease the error rate of extracted-bits.

Secure and Authenticated Reversible Data Hiding in Encrypted Images [6], proposes a Secure and authenticated discrete reversible data hiding in cipher images deals with security and authentication. In the first phase, a content owner encrypts the original uncompressed image using an encryption key. Then, a data hider may compress the least significant bits of the encrypted image using a data hiding key to create a sparse space to accommodate some additional data. With an encrypted image containing additional data, if a receiver has the data hiding key, receiver can extract the additional data though receiver does not know the image content. If the receiver has the encryption key, can decrypt the received data to obtain an image similar to the original one, but cannot extract the additional data. If the receiver has both the data hiding key and the encryption key, can extract the additional data and recover the original content without any error by exploiting the spatial correlation in natural image when the amount of additional data is not too large. It is also a drawback because if the receiver has any one key as known, and then he can take any one information from the encrypted data. In order to achieve authentication SHA-1 algorithm is being used.

Joint reversible data hiding and image encryption [7], Image encryption process is jointed with reversible data hiding in this paper, where the data to be hided are modulated by different secret keys selected for encryption. To extract the hided data from the cipher-text, the different tentative decrypted results are tested against typical random distribution in both spatial and frequency domain and the goodnessof-fit degrees are compared to extract one hided bit. The encryption based data hiding process is inherently reversible. Experiments demonstrate the proposed scheme's effectiveness on natural and textural images, both in gray-level and binary forms.

Adaptive reversible data hiding scheme based on integer transform [10], present a new reversible data hiding algorithm based on integer transform and adaptive embedding. According to the image block type determined by the pre-estimated distortion, the parameter in integer transform is adaptively selected in different blocks. This allows embedding more data bits into smooth blocks while avoiding large distortion generated by noisy ones, and thus enables very high capacity with good image quality. For instance, by the proposed method, we can embed as high as 2.17 bits per pixel into Lena image with a reasonable PSNR of 20.71 dB.

A Novel Approach Towards LSB Substituted Data Hiding In Images [12], will embed the message bits in the deeper layers of samples and alter a bit near the substitute bit to decrease the error and if not possible then ignore them and improved security, reliability, and efficiency. So, using the proposed method, message bits could be embedded into vague and deeper layer depending on the environment of the host sample robustness. Our future work will cover against all kinds of intentional and unintentional attacks to increase the robustness of the image steganography. Our experimental results have shown that the proposed method provides good image quality and large message capacity as well as increase in the system immunity. It is very sensitive to any kind of filtering or manipulation of the stego-image. Scaling, rotation, cropping, addition of noise, or lossy compression to the stego-image will destroy the message.

All the above discussed methods has the problem of performing data hiding in efficient manner with higher rate of data hiding and lossless recovery.

3. MULTI LEVEL REVERSIBLE CHARACTER ENCODING SCHEME:

The multi level reversible character encoding scheme computes the size of data to be hidden and compute the number of blocks necessary to hide the data. Based on the size and number of blocks the method assigns the level of coding should be used. The method encodes the size of data to be hidden in the first row of the block and the second layer is used to specify the number of blocks and then the third layer is used to specify the number of layers to be used. The entire process has been split into number of stages namely, Metadata Coding, Multi Level Reversible Character Encoding, Multi Level Decoding and Remainder-Averaging scheme. In this section, we discuss about each section in detail.

The Figure 1, shows the architecture of the proposed multi level reversible encoding scheme and shows the functional components in detail.

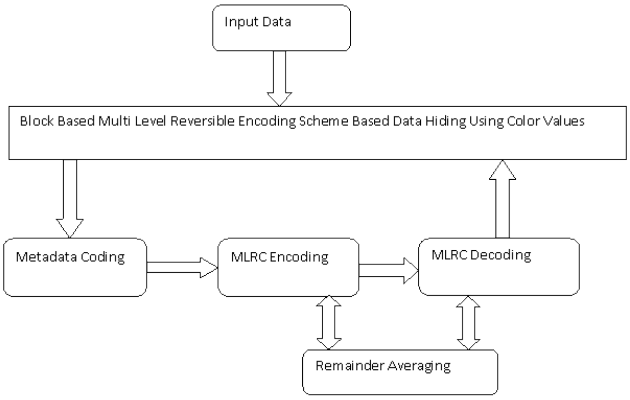


Figure 1: Architecture of proposed system

3. 1 Meta Data Coding:

The method first computes the size of data to be hidden in bits, for each character the method takes one bit. Then the method computes the size of image and identifies the number of blocks can be generated. Using both the values the method computes the amount of data to be hidden in each block and decides the number of layers to be used for data hiding. If the number of bits to be hidden is within the range of number of blocks then the method uses single level and if it is greater then it uses two or three layer to perform data encoding. The decided values are stored in the first block of the image by splitting the entire image into number of fixed size blocks.

Algorithm:
Input: Data D, Image Img
Output: Meta Encoded image MED.
Start
Initialize Box Filter to the size 3.
Generate Integral Image Img set.
Imgs = $\int_{i=1}^{size(Img)} \sum Img(Bs)$
Compute Number of bits of D.
Nb = size(D)×1024.
Compute number of blocks of image.
Nbimg = size(Imgs).
Compute Number of layers Nl = $\frac{Nbimg}{Nb}$
MED(1,1) = $\int \frac{\sum_{i=1}^{3} Img(1,1,i)}{3} == Nb$
MED(1,2) = $\int \frac{\sum_{i=1}^{3} Img(1,1,i)}{3} == size(Nbimg)$
MED(1,3) = $\int \frac{\sum_{i=1}^{3} Img(1,1,i)}{3} == NI$
Stop.

The above described meta data coding scheme encodes the meta information of data hiding and gives the details about number of bits, blocks and layers has been used.

3.2 Multi Level Reversible Character Encoding (MLRC):

In this stage, the method reads each bit of input information and number of bits to be encoded and the number of layer prescribed. For each layer or row of the block, the method computes the averaging scheme. The averaging scheme returns the row and the method replaces the block row with the averaging result produced. This will be iterated for each of the bit of the information and if the number of layer is higher than one , then the method uses the second and third layer, which is continued till the number of bits to be encoded is finished.

Algorithm:
Input: Blocks Nb, Bits Bs, Eimg, Layer L.
Output: Encoded image Enimg.
Start
For each bit Bi from Bs
Read the block Bl
Bl = Perform Remainder Averaging.
If L==2 || L==3 then
Use same Block
End
End
Stop

The above described algorithm performs the multi level encoding using the averaging scheme and the averaging method replace the layer bits according to the input value of the bit.

3.3 Remainder Averaging Scheme:

The remainder averaging scheme plays the vital role in the proposed method and will be accessed at the all level of encoding process. The method will be given with the data and the layer where the data has to be hidden. Based on the input values and their details, the method performs iterative process on computing values for each column by which the remainder could obtain the original value to be encoded. For example, the value to be encoded is 32 then the method places different values at three indexes of the layer, summing them and remainder which yield the value 32. In such way, the method is accessed by all the stage.

Algorithm:
Input: Layer l, Block B, Data D
Output: Encoded Block B.
Start
Identify the layer L.
Ascii = Compute ascii value of character D.
While $Mod(\frac{\sum L(i)}{3})$!=Ascii
B(L(1)) = $\int_{i=1}^{Max} Pi(L(1))$
B(L(2)) = $\int_{i=1}^{Max} Pi(L(2))$
B(L(3)) = $\int_{i=1}^{Max} Pi(L(3))$
End
Return B
Stop.

The above discussed algorithm computes the remainder averaging scheme for given layer and block to encode the data given.

3.4 MLRC Decoding:

The decoding process is performed as an reverse operation to the encoding phase. By receiving the encoded image,the method generates the number of small scale images and fro m the first image,the method computes the number of data bits, number of layers and blocks has been used in the encoding phase using the averaging scheme. The same remainder averaging scheme is iterated for each of the block being generated and the original information is obtained.

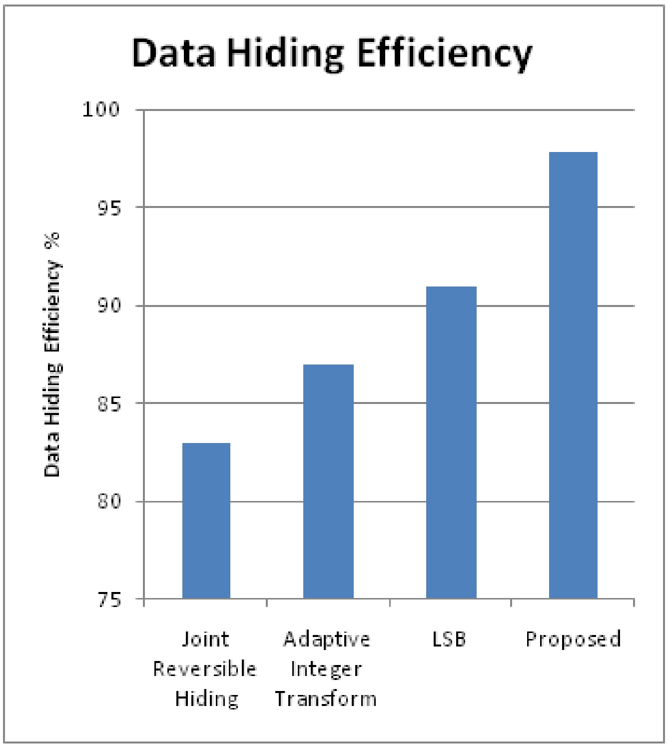
Algorithm:
Input: Encoded Image Eimg
Output: Decoded Data D.
Start
Initialize Box Filter to the size 3.
Generate Integral Image Img set.
Imgs = $\int_{i=1}^{size(EImg)} \sum EImg(Bs)$

Read First sectional image Si = Imgs(1).
Compute Number of bits Nb = $Mod(\frac{\sum Si(1,\{1.2.3\})}{3})$
Compute Number of blocks Nbl= $Mod(\frac{\sum Si(2,\{1.2.3\})}{3})$
Compute Number of layers Nl = $Mod(\frac{\sum Si(3,\{1.2.3\})}{3})$
For each block Bi from Imgs
Compute data d= $Mod(\frac{\sum Si(x,\{1.2.3\})}{3})$
Add to decode data D
End
Stop
.

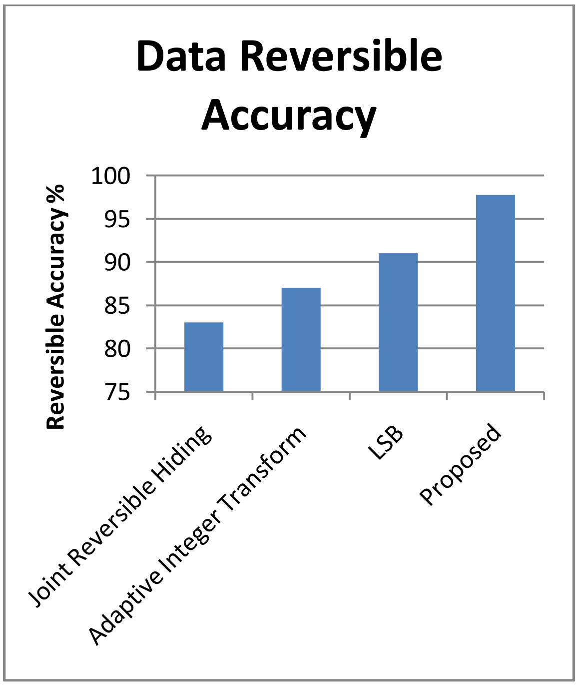
The above discussed algorithm computes the decoding process and extracts the data encoded in the image.

4. RESULTS AND DISCUSSION:

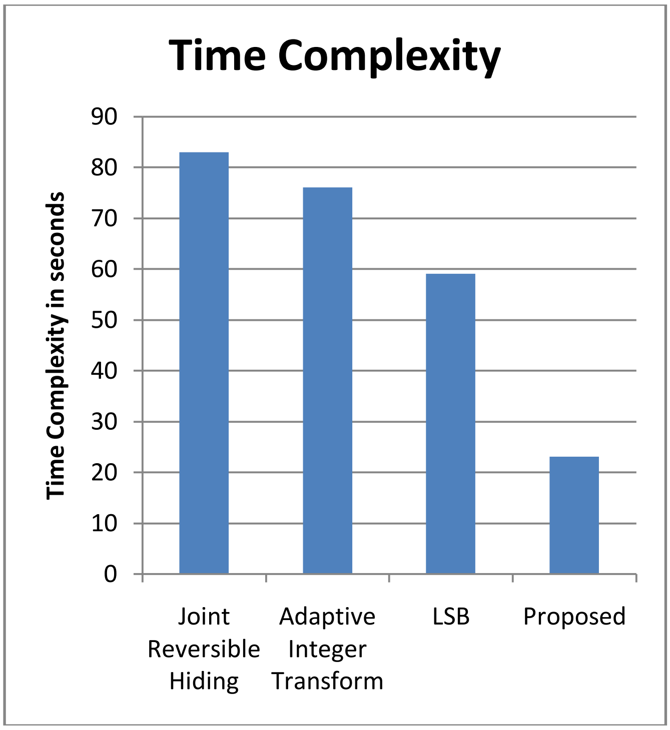
The proposed block based multi level continuous reversible encoding scheme has been developed and implemented in matlab. The performance of the method has been tested with various simulation setup and has been tested with various input pattern of data. The method has produced efficient results in data encoding and decoding phases. Also the method has produced efficient result in tamper resistance and has produced less time complexity.
The Graph 1, shows the comparison of data hiding efficiency produced by different methods and it shows clearly that the proposed method has produced more efficiency than other methods.
The Graph 2,shows the comparison result on data reversible accuracy of different methods and it shows clearly that the proposed method has produced more data reversible accuracy than other methods.
The Graph 3, shows the comparison of time complexity produced by different methods and it shows clearly that the proposed method has produced less time complexity than other methods.



Graph 1: Comparison of data hiding efficiency



Graph 2: Comparison of data reversible accuracy



Graph 3: Comparison of Time complexity

5. CONCLUSION:

We proposed a block based multi level reversible encoding scheme for efficient data encoding process. The method splits the input image into number of small scale images and computes the size, number of blocks, number of layer to be used to encode the data using the input data. The computed values are encoded in the first block of the image and the original data is encoded in each block of the image using the remainder averaging scheme which encodes the data by computing the averaging value and remainder value to encode the data. The same process is iterated for each of the data to produce the encoded image. On the other side, the method performs the same to identify the parameters and then computes the modulus value at each of the block to get the original value. The method has been implemented and tested for its efficiency. The method has produced efficient results in all the factors of data hiding and reduces the time complexity also.

REFERENCES

1. Ma, K.; Weiming Zhang; Xianfeng Zhao; Nenghai Yu; Fenghua Li, "Reversible Data Hiding in Encrypted Images by Reserving Room Before Encryption" *IEEE Transactions onInformation Forensics and Security*, , vol.8, no.3, pp.553,562, March 2013.
2. Xinpeng Zhang, "Separable Reversible Data Hiding in Encrypted Image",*IEEE Transactions onInformation Forensics and Security*, vol.7, no.2, pp.826,832, April 2012.
3. Xinpeng Zhang, "Reversible Data Hiding in Encrypted Image," *IEEE Signal Processing Letters*, vol.18, no.4, pp.255-258, April 2011.
4. W. Puech, M. Chaumont and O. Strauss, "A Reversible Data Hiding Method for Encrypted Images", *SPIE Electronic Imaging, Security, Forensics, Steganography, and Watermarking of Multimedia Contents*, San Jose, CA, USA, July 2008.
5. Manikandan R, UmaM, and MahalakshmiPreethiS M, "Reversible Data Hiding for Encrypted Image" *Journal of Computer Applications*,Volume-5, Issue EICA2012-1, pp. 104-110, February 10, 2012.
6. V.Khanaa, and Krishna Mohanta, "Secure and Authenticated Reversible Data Hiding in Encrypted Images", *International Journal of Engineering and Computer Science*, Vol. 2, Issue 3, pp. 558-568, March 2013.
7. Bian Yang ; Christoph Busch ; Xiamu Niu; "Joint reversible data hiding and image encryption.", Proc. SPIE 7541, Media Forensics and Security II, 75410V (January 27, 2010).
8. Zhicheng Ni; Yun-Qing Shi; Ansari, N.; Wei Su, "Reversible data hiding," *IEEE Transactions onCircuits and Systems for Video Technology*, vol.16, no.3, pp.354,362, March 2006.
9. Wien Hong, Tung-Shou Chen, Chih-Wei Shiu , " Reversible data hiding for high quality images using modification of prediction errors", *Journal of Systems and Software*, Volume 82, Issue 11, Pages 1833-1842, November 2009.
10. Fei Peng, Xiaolong Li, Bin Yang, "Adaptive reversible data hiding scheme based on integer transform",*in Transactions of Signal Processing*, Volume 92, Issue 1, pp. 54-62,January 2012.
11. Amin, P.K.; Ning Liu; Subbalakshmi, K. P., "Statistically Secure Digital Image Data Hiding," *IEEE 7th Workshop onMultimedia Signal Processing, 2005* , pp.1,4, Nov 2005.
12. Ruchira Datta, "A Novel Approach Towards LSB Substituted Data Hiding In Images", *International Journal of Emerging Technology and Advanced Engineering*, Volume 3, Issue 3, pp. 50-60, March 2013
13. X. Zhang, "Lossy compression and iterative reconstruction for encrypted image," IEEE Trans. Inform. Forensics Security, vol. 6, no. 1, pp. 53-58, Feb. 2011.
14. T. Bianchi, A. Piva, and M. Barni, "On the implementation of the discrete Fourier transform in the encrypted domain," IEEE Trans. Inform. Forensics Security, vol. 4, no. 1, pp. 86-97, Feb. 2009.
15. T. Bianchi, A. Piva, and M. Barni, "Composite signal representation for fast and storage-efficient processing of encrypted signals," IEEE Trans. Inform. Forensics Security, vol. 5, no. 1, pp. 180-187, Feb. 2010