www.ijecs.in

International Journal Of Engineering And Computer Science ISSN: 2319-7242
Volume 6 Issue 1 Jan. 2017, Page No. 19994-19998
Index Copernicus Value (2015): 58.10, DOI: 10.18535/ijecs/v6i1.27

Optimizing Information Rate in Polynomial Based Image Secret Sharing Scheme Using Huffman Coding

Nehal Markandeya, Prof.Dr.Sonali Patil
Department of Computer Engineering
Pimpri Chinchwad College of Engineering
Pune-44
Email: markandeya.nehal@gmail.com
Department of Computer Engineering
Pimpri Chinchwad College of Engineering
Pune-44
Email: sonalimpatil@gmail.com

***Abstract*— Image secret sharing is a technique to share a secret image among the group of participants. These individual shares are useless on their own, but when specified numbers of shares are combined together it gives the original secret image. These image shares has size greater than or equal to size of original image, it require high bandwidth while transmission. Because of the excessive bandwidth requirements of image there is need to reduce the bandwidth of images. To reduce the size of image, Huffman compression coding techniques are used. The purpose of this paper is to reduce the image share size in Thien and Lin's secret sharing scheme using Huffman coding technique. The experimental result's with high PSNR value of shows good image quality. Up to 40% reduction is achieved using compression technique, which results in reducing storage space and saving time while transmission images over network.**

***Keywords*— Image compression, Huffman coding, Image secret sharing.**

I. INTRODUCTION

Now a day's secret sharing schemes are widely used in missile launching, biometric authentication system etc. Where the maintaining the secrecy of missile details and person's personal data is important. In secret sharing a secret is divided into parts, giving each participant its own unique part, where some of the parts or all of them are needed in order to reconstruct the secret.

Image Secret sharing is the technique of distribution of secret image among the participants or group members within a group, each of the participants holds only a share of the secret and individual shares are of no use in order to reconstruct the original secret. The original secret can be reconstructed only when a definite number of shares are combined together and individual shares does not indicate the original secret. The process of the secret sharing scheme can be made easy and efficient by using image compression techniques.

II. LITERATURE SURVEY

In the paper [1], Sujit kumar Das, Bihas Chandra Dhara proposed that A (t,n) secret image sharing scheme where the secret image is first encoded by block based lossy compression technique and define t sub-images. The image compression technique gives a good quality image. To enhance the security level, the sub-images are scrambled by Arnold transform and then shares are generated. Finally, image hiding (i.e., steganography) concept is adopted to hide the shares within cover images. The proposed method gives good quality of the stego images[1].

In the paper [2], Christian L. F. Corniaux, Hossein Ghodosi proposed that In a ***k***-threshold secret sharing scheme, a dealer who holds a secret ***s*** distributes parts of this secret (the *shares*) to ***n*** players; If ***k*** or more of these players pool their shares, they are able to determine ***s***, but if less than ***k*** of them pool their shares, they cannot infer any information on ***s***. In 1979, Shamir introduced such a scheme, based on polynomial interpolation in a finite field. This scheme is widely used in other cryptographic protocols, because it is simple, elegant and above all information theoretically secure. There are a few proofs of the scheme's security, but to our knowledge, none of them is entirely based on the information-theoretical entropy function introduced by Shannon in 1948. We propose such a demonstration [2].

In the paper [3], Rachit Patel, Virendra kumar, vaibhav tyagi, vishal asthana proposed that Image Compression using Huffman coding technique is simpler & easiest compression technique. Compression of image is an important task as its implementation is easy and obtains less memory. The purpose of this paper is to analyse Huffman coding technique which is basically used to remove the redundant bits in data by analysing different characteristics or specification like Peak Signal to Noise Ratio (PSNR), Mean Square Error (MSE) Bits Per Pixel (BPP) and Compression Ratio (CR) for the various input image of different size and the new method of splitting an input image into equal rows & columns and at final stage sum of all individual compressed images which not only provide better result but also the information content will be kept secure. An image compression technique has various advantages in the field of image analysis and also for the security purpose for the image[3].

In the paper [4], Doaa Mohammed, Fatma Abou-Chadi proposed that the present work investigates image compression using block truncation coding. Two algorithms were selected namely, the original block truncation coding (BTC) and Absolute Moment block truncation coding (AMBTC) and a comparative study was performed. Both of two techniques rely on applying divided image into non overlapping blocks. They differ in the way of selecting the quantization level in order to remove redundancy. Objectives measures were used to evaluate the image quality such as: Peak Signal to Noise Ratio (PSNR),Weighted Peak Signal to Noise Ratio (WPSNR), Bit Rate (BR) and Structural Similarity Index (SSIM).The results have shown that the ATBTC algorithm outperforms the BTC. It has been show that the image compression using AMBTC provides better image quality than image compression using BTC at the same bit rate. Moreover, the AMBTC is quite faster compared to BTC[4] .

III. ALGORITHM OF BLOCK TRUNCATION CODING

Block truncation coding is a type of lossy compression technique for images having gray scale. In BTC the effort required for computation is less as compare to the other compression techniques and also it reduces the channel error. Quantization process in BTC preserves the moment for block pixels, which makes the quality of image acceptable and also it reduces the demand for the storage space.

Step1: The image is split into rectangle shape regions which don't overlap with each other. To make it simple, blocks were made in square region with size n*n

Step 2: Each Pixel in block is represented by two values i.e mean $\bar{y}$ and standard deviation σ. These values are called as luminance value. Luminance values are selected for two level quantizer.

$$\bar{y} = \frac{1}{\mathrm{m}} \sum_{\mathrm{j=1}}^{\mathrm{m}} y_j \qquad (1)$$

$$\sigma = \frac{\sqrt{1}}{\sqrt{\mathrm{m}}} \sum_{\mathrm{j=1}}^{\mathrm{m}} (y_j - \bar{y}_j)^2 \qquad (2)$$

y $_{j =}$ jth Pixel value of the image block.

m= total number of the pixels in that block.

Step3: The Luminance value i.e mean and standard deviation are quantizers of BTC. To form two level bit plane, each pixel value y_j compared with the mean $\bar{y}$ which is used as threshold value. If the pixel's gray level value is greater than or equal to ȳ then it can be represented as 1 and If the pixel's gray level value is less than to ȳ then it can be represented as 0.

$$\mathrm{D} = \begin{cases} 1 & y_j \geq \bar{y} \\ 0 & y_j < \bar{y} \end{cases} \qquad (3)$$

D = binary block

Step 4: In this step the 1's in the bit plane are replaced with HV and '0's in the bit plane are replaced with LV

$$HV = \bar{y} + \sigma \frac{\sqrt{\mathrm{s}}}{\sqrt{\mathrm{t}}} \qquad (4)$$

$$LV = \bar{y} - \sigma \frac{\sqrt{\mathrm{s}}}{\sqrt{\mathrm{t}}} \qquad (5)$$

s = number of '0's in compressed bit plane

t = number of '1's in compressed bit plane

IV. ALGORITHM OF ABSOLUTE MOMENT BLOCK TRUNCATION CODING

Step 1: The image is split into blocks, these blocks are non-overlap blocks.The size of a block could be (4 x 4) or (8 x 8), etc.

Step 2: Calculate the average gray level of the block (4x4) as shown in equation (6)

Step3: In this step Pixel are classified in such a way that there will be two ranges of values i.e upper range values and lower range values. Pixel whose value is greater than $\bar{y}$ are the upper range values and pixel whose value is less than $\bar{y}$ are lower range, then mean of higher range values y_{HV} and lower range values y_{LV} are calculated.

$$y_{HV} = \frac{1}{\mathrm{K}} \sum_{y_j > \bar{y}_j}^{\mathrm{m}} y_j \qquad (6)$$

$$y_{LV} = \frac{1}{16 - \mathrm{K}} \sum_{y_j < \bar{y}_j}^{\mathrm{m}} y_j \qquad (7)$$

K = number of pixels whose gray level value is greater than $\bar{y}$

Step 4: If the pixel's gray level value is greater than or equal to ȳ then it can be represented as 1 and If the pixel's gray level value is less than to ȳ then it can be represented as 0.In encoding process y_{HV} , y_{LV} are written.

$$\mathrm{D} = \begin{cases} 1 & y_j \geq \bar{y} \\ 0 & y_j < \bar{y} \end{cases} \qquad (8)$$

D = binary block

Step 5: The 1's in the bit plane are replaced with y_{HV} and '0's in the bit plane are replaced with y_{LV} to reconstruct the image block. AMBTC and BTC both requires 16 bits to code bit plane. Computation required by AMBTC is less than BTC.

$$y = \begin{cases} y_{LV} & D = 0 \\ y_{HV} & D = 1 \end{cases} \qquad (9)$$

V. Algorithm of Huffman Coding

The image compression techniques are categorized into two main classifications namely Lossy compression techniques and Lossless compression techniques.

1] Lossless compression:

A technique in which the compressed image is reconstructed without any loss of data is called lossless compression. Lossless compression ratio gives good quality of compressed images, but yields only less compression.

2] Lossy compression:

A technique in which the compressed image is reconstructed with loss of data is called lossy compression. The lossy compression techniques lead to loss of data with higher compression ratio.

Huffman coding is loss less technique with more attractive features in various application such as medical survey and analysis, technical drawing etc. Huffman coding has better characteristics of image compression. As we know that huffman coding algorithm is a step by step process and involves the variable length codes to input characters & it is helpful in finding the entropy and probability of the state[3]. It is very easy to calculate quality parameter in Huffman algorithm. Original image can be reconstructed with the help of digital image restoration[3].

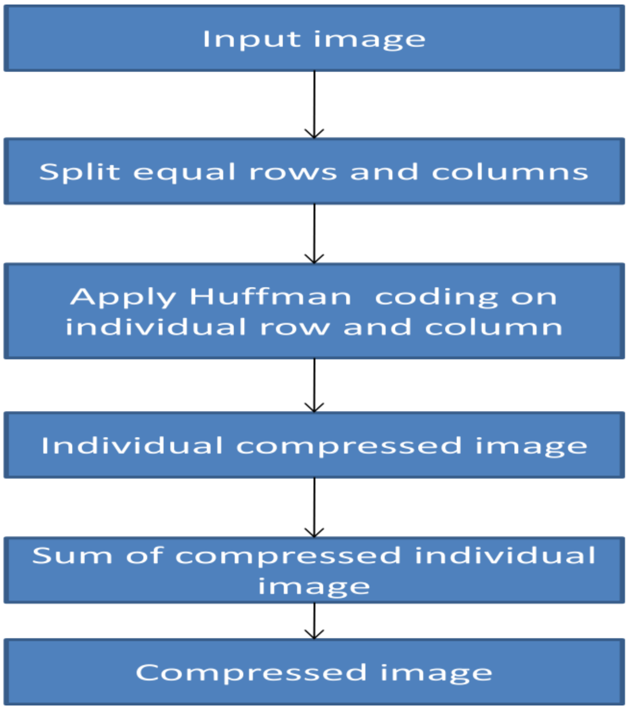
Input image
Split equal rows and columns
Apply Huffman coding on individual row and column
Individual compressed image
Sum of compressed individual image
Compressed image

Fig. 1 Block diagram of Huffman compression

- Analysis of Huffman coding algorithm

This matrix represent digital image N x N. These matrix arrays given in matrix are the elements of image.

$$f(x,y) = \begin{matrix} b_{0,0} & b_{0,1} \dots \dots & b_{0,M-1} \\ b_{1,0} & b_{1,1} \dots \dots & b_{1,M-1} \\ b_{M-1,0} & b_{M-1,1} \dots \dots & b_{M-1,M-1} \end{matrix}$$

This digital image f(x, y) is break into a set of non-overlapping four sub images i.e two row and two column this can be represented as

f(x, y) which is a digital image is divided into four small images. These small images is also called as non-overlapping sub images.

$$f(x,y) = \begin{bmatrix} f_1(x,y) & f_2(x,y) \\ f_3(x,y) & f_4(x,y) \end{bmatrix}$$

These $f_1(x,y)$, $f_2(x,y)$, $f_3(x,y)$, $f_4(x,y)$ are the sub-matrix of original image after applying Huffman coding on these sub-matrix they gives

f_1` (x, y) $f_2$`(x, y) f_3`(x, y), $f_4$`(x, y) respectively the compressed image can be obtain by adding these matrixes**.**

VI. Proposed Model

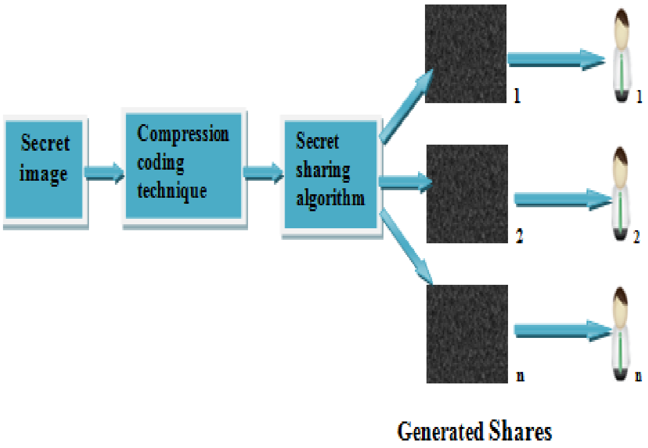

Fig 2: Share distribution phase

DOI: 10.18535/ijecs/v6i1.27

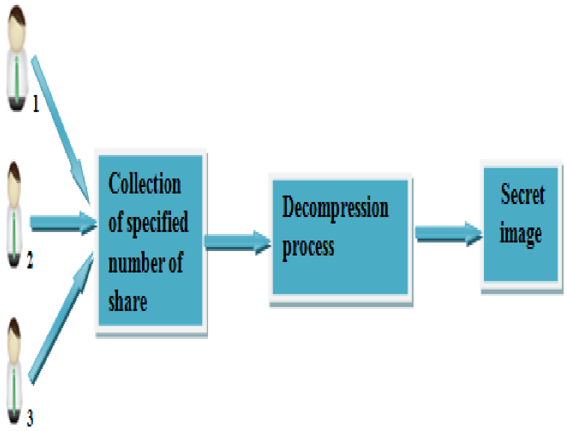

Fig 3: Reconstruction phase

Image secret sharing is a technique to share a secret image among the group of participants. These individual shares are useless on their own, but when specified numbers of shares are combined together it gives the original secret image. These image shares has size greater than or equal to size of original image, it require high bandwidth while transmission. Because of the excessive bandwidth requirements of image there is need to reduce the bandwidth of images. To reduce the size of image, Huffman compression coding techniques are used.

In proposed model secret image is taken as input. Before applying the secret sharing algorithm, compress the secret image using compression coding technique. When secret sharing algorithm is applied the shares are created and that shares are distributed to participants. According to (k,n) secret sharing when specified number of shares are collected we get the original secret image. The purpose of this project is to reduce the image share size in Thien and Lin's secret sharing scheme using Huffman coding technique. The experimental result's with high PSNR value of shows good image quality. Up to 40% reduction is achieved using compression technique, which results in reducing storage space and saving time while transmission images over network.

VII. IMAGE QUALITY PARAMETER

There are four major important parameters measure between uncompressed image and compressed image [3], these are following-

A. Compression ratio (CR)

Compression ratio is used to measure the compression efficiency. Compression ratio is the ratio of original image and compressed image. As compression ratio increases the image quality increases.

CR=Size of original image/Size of compressed image.

B. Bit Rate:

It is information (bits) stored per pixel of an image. This is ratio of number of bits in the compressed image to total number of pixel in original image.

Number of bits per pixel required by the compressed image.

BR= (b/CR)

b= No. of bits per pixel.

When bit rate is large it means large memory required to store an image. High bit rate indicate that image acquire more colours so bit rate should be less.

C. The Mean Squared Error(MSE):

The difference between original image data and compressed image data is called mean square error (MSE). MSE is inversely proportional to PSNR, as MSE decreases the PSNR increases. PSNR indicate quality of image. Image compression is lossless when MSE is zero. Its better to have less MSE

D. Peak Signal to noise Ratio(PSNR):

PSNR is the ratio between maximum signal powers to noise appear in signal. PSNR is related to quality of image. For good quality of image the PSNR of image should be high. PSNR is depends upon the mean square error(MSE)of image. When the difference between the original image and compressed is less the PSNR is high so eventually the quality of image is also high.

$$\mathrm{PSNR} = 10\log\frac{MAX^2}{\mathrm{MSE}}$$

VIII. RESULTS

Original image Size	Image after applying Huffman coding on original image	Share size in Thien and lin secret sharing
256 x 256	102.4 x 102.4	51.2 x51.2
512 x 512	204.8 x 204.8	102.4 x 102.4
1024 x 1024	409.6 x 409.6	204.8 x 204.8

Table 1: Image size reduction

Sr. No	Compression technique	Bit rate
1	BTC	1.25
2	AMBTC	2.15
3	Huffman coding	0.95

Table 2: comparison of image compression technique

DOI: 10.18535/ijecs/v6i1.27

IX. CONCLUSION

Image compression plays vital role in saving memory storage space and saving time while transmission images over network. Compression technique increase storage capability and transmission speed.Using compression coding techniques the shares size in image secret sharing is reduced. Optimal information rate can be achieved using compression coding technique in secret sharing schemes. By using Huffman coding the image is compressed by 40%. And then the Thein and Lin algorithm is applied for secret sharing which again compress the image size by 80%. The properties of Huffman coding and Thien and lin helps to compress the image while districbuting the share to participant without losing the accuracy of original image.

REFERENCES

[1] SUJIT KUMAR DAS, BIHAS CHANDRA DHARA, "AN IMAGE SECRET SHARING TECHNIQUE WITH BLOCK BASED IMAGE CODING", IEEE, PP. 648-652, 2015.

[2]Christian L.F. corniaux, hossein ghodosi, "An Entropy-based Deme onstration of the Security of Shamir's Secret Sharing Scheme", IEEE, PP. 46-48, 2014.

[3]Rachit patel, virendra kumar, vaibhav tyagi, vishal asthana, "A Fast and Improved Image Compression Technique Using Huffman Coding", IEEE, PP. 2283-2286, 2016.

[4]Doaa mohammad, fatma abou-chadi, "Image Compression Using Block Truncation Coding", IEEE,PP. 9-13, 2011.

[5]Adi Shamir, "How to share a secret", Communication of the ACM, Volume. 22, No11, PP. 612-613, Nov 1979.

[6]Thien and 'Lin, "secret image sharing", Computer and graphics, Volume.26, No.5, PP. 765-770, 2002.

[7]Chin-chen chang, chin-yu sun, "Polynomial-based secret sharing scheme based on the absolute moment block truncation coding technique", 2014 Tenth International Conference on Intelligent Information Hiding and Multimedia Signal Processing, PP. 485-488, 2014.

[8] Yongge Wang, Yvo Desmedt,"Efficient Secret Sharing Schemes Achieving Optimal Information Rate", IEEE, 512-520, 2014.

[9] C. Lv, X. Jia, J. Lin, J. Jing, L. Tian, and M. Sun. Efficient secret sharing schemes. In Communications in Computer and Information Science,volume 186, pages 114–121. Springer Berlin Heidelberg, 2011.

[10]A. M. Eskicioglu and P.S. Fisher, "Image quality measures and their performance," IEEE Trans. Communications, vol. 34, pp. 2959-2965, Dec. 1995.

[11]Jagdish H. Pujar and Lohit M. K. Kadlaskar "A New Lossless Method of Image compression and decompression using Huffman coding technique" Journal of Theoretical and Applied Information Technology, 2010.

[12] Ran-Zan Wang and Chin-Hui Su. Secret image sharing with smaller shadow images. Pattern Recognition Letters, 27(6):551–555, 2006.