COMPRESSION OF VC SHARES

M. Mary Shanthi Rani[1] and G. Germine Mary[2]

[1]Department of Computer Science and Application, Gandhigram Rural Institute-Deemed University, Gandhigram-624302, Tamil Nadu, India
[2]Department of Computer Science, Fatima College,Madurai – 625016, Tamil Nadu, India.

ABSTRACT

Visual Cryptography (VC) schemes conceal the secret image into two or more images which are called shares. The secret image can be recovered simply by stacking the shares together.In VC the reconstructed image after decryption process encounter a major problem of Pixel expansion. This is overcome in this proposed method by minimizing the memory size using lossless image compression techniques. The shares are compressed using Vector Quantization followed by Run Length Encoding methods and are converted to few bits. Decompression is done by applying decoding procedure and the shares are overlapped to view the secret image.

KEYWORDS

Secret Image Sharing, Visual Cryptography, Image Compression, Vector Quantization, Run Length Encoding.

1.INTRODUCTION

In recent years, along with the prevalent advancements in image processing, secret image sharing also has been in active research. Secret Image Sharing refers to a method for distributing a secret image amongst a group of participants, each of whom is allocated a share of the secret. The secret can be reconstructed only when a sufficient number of shares are combined together; individual shares are of no use on their own. A special type of Secret Sharing Scheme known as Visual Cryptography was proposed in 1994 by Naor and Shamir [1]. The most important feature of this scheme is that the secret image can be decrypted simply by the human visual system (HVS) without having to resort to any complex computation.

VC schemes conceal the secret image into two or more images which are called shares. The secret image can be recovered simply by stacking the shares together. The shares are very safe because separately they reveal nothing about the secret image. Each of the shares looks like a group of random pixels and of course looks meaningless by itself [2]. Naturally, any single share, before being stacked up with the others, reveals nothing about the secret image. This way, the security level of the secret image when transmitted via the Internet can be efficiently increased. Suppose that we want to encode the secret S into n shares ($S_1, S_2,\ldots,S_n$) and we wish that the secret data S cannot be revealed without k or more shares. In Shamir secret sharing scheme the partition of the secret is done by the following polynomial:

$F(x_i) = y + m_1x_i + m_2x_i^2 + \ldots + m_{(k-1)}x_i^{(k-1)} \bmod(p)$ --(1) where $i = 1,2,\ldots,n$

DOI : 10.5121/ijcsity.2016.4106

where y is the share, S_1, p is a prime number and the coefficients of the K-1 degree polynomial m_1 are chosen randomly and then the shares are evaluated as $S_1 = F(1)$, $S_2 = F(2)$,…, S_n=F(n). In this scheme the size of the shared images is much bigger than the original image and hence it is compressed before it is shared.

Image Compression is the process of reducing the number of bits required to represent an image. Compression has traditionally been done with little regard for image processing operations that may precede or follow the compression steps. In this proposed scheme compression follows VC as it results in pixel expansion. Data compression is the mapping of a data set into a bit stream to decrease the number of bits required to represent data set. With data compression one can store more information in a given storage space and transmit information faster over communication channels. Strategies for Compression are reducing redundancies and exploiting the characteristics of human vision. The two types of data compression are lossless and lossy. Lossless compression has an advantage that the original information can be recovered exactly form the compressed data. The proposed system uses lossless compression techniques of vector quantization and RLE.

Vector quantization (VQ) is a popular image compression algorithm for reducing the transmission bit rate or storage, which maps the pixel intensity vectors into binary vectors and indexing a limited number of possible reproductions VQ is a block-coding technique that quantizes blocks of data instead of single sample.

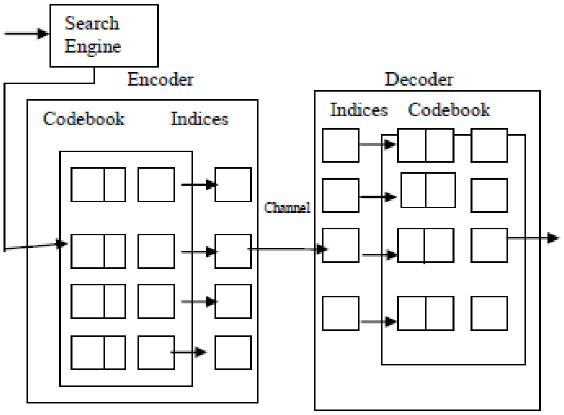


Figure 1. Vector Quantiztion Scheme

VQ exploits the correlation between neighboring signal samples by quantizing them together [3-5]. VQ Compression contains two components: VQ encoder and decoder as shown in Fig.1.
At the encoder, the input image is partitioned into a set of non-overlapping image blocks. The closest code word in the code book is then found for each image block. Next, the corresponding index for each searched closest code word is transmitted to the decoder. Compression is achieved because the indices of the closest code words in the code book are sent to the decoder instead of the image blocks themselves.

Run Length Encoding (RLE) is a simple and popular data compression algorithm. It is based on the idea to replace a long sequence of the same symbol by a shorter sequence. The RLE algorithm performs a lossless compression of input data based on sequence of identical values (runs).In this algorithm is represents explicitly by a pair (e, r) where e is the value of the element and r is the run length of the value e [6]. For example, consider a screen containing plain black text on a solid white background. A hypothetical scan line, with B representing a black pixel and W representing white, might read as follows:

WWWWWWWWWWWWBWWWWWWWWWWWWBBBWWWWWWWWWWWWWW
WWWWWWWWWWBWWWWWWWWWWWWWW

With a RLE data compression algorithm applied to the above hypothetical scan line; it can be rendered as follows: 12W1B12W3B24W1B14W. This can be interpreted as a sequence of twelve Ws, one B, twelve Ws, three Bs, etc. The run-length code represents the original 67 characters in only 18 characters.

In this paper, a novel method is proposed to enhance the process of image compression by using RLE algorithm to the Vector Index Table created by VQ. This reduces the size of VC shares significantly. The paper is organized as follows; Chapter 2 describes the proposed method in detail. Chapter 3 discusses the results of the proposed method based on standard metrics. Chapter 4 gives a summary and future direction of research in this area.

2.PROPOSED METHOD

Cryptography is most commonly used techniques used for data security. Visual Cryptography is a secured and easy way of sharing secret images/information, which is devoid of any cumbersome decryption algorithm.

The main objectives of this proposed method is to formulate a secret sharing system which has the following characteristics.

- Exploit the advantage of VC to create meaningless shares to hide secret
- Minimizing the drawback of VC, that is image expansion, by applying multistage Image Compression.

The proposed system consists of three phases. In the first phase general VC scheme is applied to create 2 shares of secret image. The size of the shares will be 4 times the size of the original secret image as each pixel is replaced by a 2X2 block of pixel as illustrated in Fig.2. Shares generated in the first phase are compressed using VQ followed by RLE method and the images are converted to few bits in the second phase. Decompression is done in the third phase and the shares are overlapped to view the secret image.

2.1.Phase I: Creation of VC Shares

The secret image sharing scheme proposed by Naor and Shamir is used in the first phase, in which a secret monochrome image is encrypted into two shares. Monochrome pixels have only two values either black or white. If the pixel is white, one of the above two rows (Fig. 2(b)) is chosen to generate two shares. Similarly if the pixel is black, one of the below two rows is chosen to generate the two shares. Fig. 2(b) shows the possible values of pixels in each of the two generated shares. The reconstruction of the secret image is simply done by stacking the pixels again as shown in Fig. 2(b). There is expansion of pixels in the shares and the expansion factor is 4, which is the block size used to replace a single pixel. This drawback is overcome by reducing the share size using Phase II.

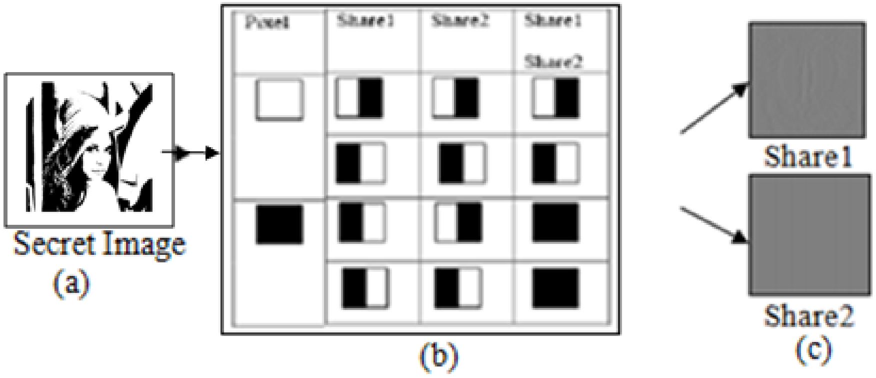


Figure 2. Phase I – Creation of VC Shares

2.2.Phase II: Image Compression (Encoding)

VQ technique is applied to the shares generated in phase I. The basic idea in this technique is to develop a dictionary of fixed-size vectors, called code vectors (Code Book). A vector is usually a block of pixel values. A given image is then partitioned into non-overlapping blocks (vectors) called image vectors of size 4. Then each image vector is compared with the code vectors in the dictionary and its index in the dictionary is determined which is used to encode the original image vector. Thus, each image is represented by a sequence of indices and is stored in a Vector Index Table (VIT) as shown in Fig. 3.

The size of VIT is further reduced by applying RLE algorithm. This is a very simple compression method used for sequential repetitive data. This technique replaces sequences of identical symbols (index value in our case), called runs in a separate vector. The Index in VIT has just two values 0 or 1 to represent the index of code vector. This is passed as an input to RLE algorithm. RLE creates two vectors, one to represent the arrangement of element and the other to represent the runs of the element. These two vectors and the code vector is the final output sent to the receiver. The phase II – encoding process is shown in Fig. 3.

2.3.Phase III: Image Decompression (Decoding)

The advantage of Image Compression and VC is taken into account to reveal the Secret Image in phase III. Using the two vectors, elements and run vectors VIT is recreated using the reverse algorithm. Similarly using VIT and Code Vectors the Image Vectors (blocks) are formed which are combined together and the shares are created. By simply overlapping the shares Secret Image can be seen using our HVS. The Phase III decoding process is illustrated in Fig. 4.

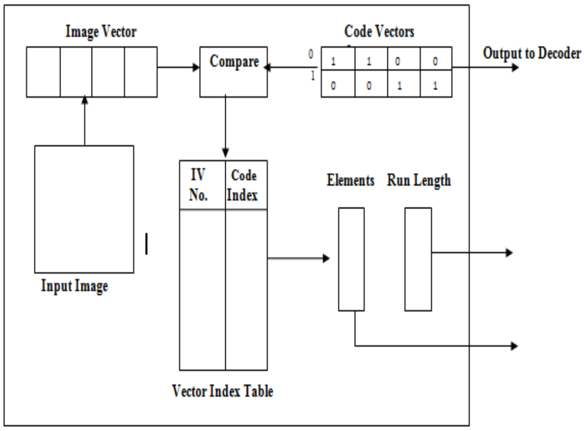


Figure 3. Phase II - Encoding

The proposed algorithm is outlined below.

Phase I: VC share creation

Step 1: Read a binary Image
Step 2: Extract pixels from the image and replace it with a 2x2 block as shown in fig.1.
Step 3: Combine all the blocks to create 2 images share1 and share2

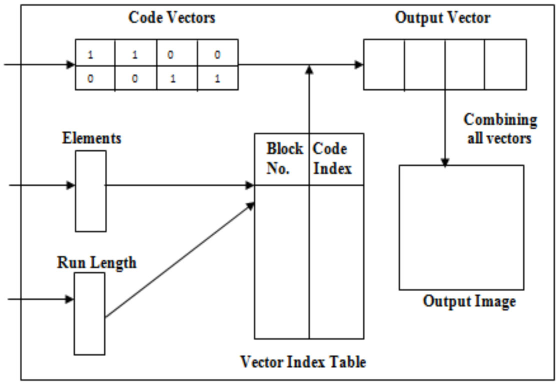


Figure 4. Phase III - Decoding

Phase II: Image Compression (Encoding)

Step 1: Read the shares and perform the following steps for both the shares
Step 2: Convert the image into blocks of size 2X2 and then to a vector of size 4.
Step 3: Compare each vector with the predefined vector used for creating shares. The Code book has 2
vectors (1,0,1,0) and (0,1,0,1)

Step 4: Create Vector Index Table (VIT) which contains block number and code book index
Step 5: Index in VIT has a sequence of two values 0 or 1 to represent the index of code book. This is
passed as a input to RLE algorithm

Step 6: RLE creates two vectors, one to represent the arrangement of element and the other to
represent the length of the element. These two vectors and the code book is the final output
sent to the receiver

Phase III: Decompression (Decoding) and Revealing Secret Image

Step 1: From the two vectors (element and length) VIT is recreated using the reverse algorithm
Step 2: Using VIT and Code book the blocks and then the shares are created.
Step 3: By simply overlapping the shares Secret Image can be seen using our HVS

3.RESULTS AND DISCUSSION

Using the above proposed method experiments are conducted on several binary test images of size 512 x 512 pixels and 2 x 2 pixel block size using Pentium Dual-Core processor at 2.5 GHz with 2GB RAM. The performance of the proposed method is evaluated using standard compression metrics like peak signal-to-noise ratio (PSNR), compression and decompression time, bit rate in bits per pixel (BPP), compression ratio and structured quality index (Q) to measure the quality of the reconstructed image. Table 1 shows the performance of the proposed method for different images.

Phase I of this method generates two shares of size 1024 x 1024 from the secret image of size 512 x 512. Out of the two shares, first share of all the secret images is the same, having the same 2x2 block (1,0,1,0) repeated for all pixels irrespective of the color of the pixel as discussed in phase I. Thus share1 will be acting as a mask and share2 will vary for different images. When share1 is compressed it needs just 4 bits to represent the block which is used to replace the pixel. So a bit per pixel for share1 is 3.8 x $10^{-6.}$ The compression ratio of share1 is calculated to be 2,097,152. The PSNR of share1 is infinity and the image quality index Q is 1. In this chapter performance metrics of share2 for different secret images is discussed in detail.

3.1.PSNR

In statistics, the mean square error (MSE) of an estimator measures the average of the squares of the "errors", that is, the difference between the estimator (original image) and what is estimated (recovered image).

The peak signal-to-noise ratio (PSNR) in decibels is computed between two images. This ratio is often used as a quality measurement between the original and the reconstructed image [7]. The higher the PSNR value better is the quality of the reconstructed image. PSNR is most commonly used to measure the quality of reconstruction of lossy compression. The signal in this case is the original data, and the noise is the error introduced by compression.

PSNR is most easily defined via the MSE. Given a noise-free m×n monochrome image I and its noisy approximation K, MSE is defined as:

$$MSE = \frac{1}{m\,n}\sum_{i=0}^{m-1}\sum_{j=0}^{n-1}[I(i,j) - K(i,j)]^2$$

The PSNR (in dB) is defined as:

$$PSNR = 20log_{10}\left(\frac{Max|I|}{\sqrt{MSE}}\right)$$

The results table shows PSNR value as infinity for all images conforming the method used in this proposed method is a lossless compression.

3.2.Bit Rate

The compression efficiency is also measured by the bit rate, which is the average number of bits required to store a pixel and is computed as follows [4]. Bit Rate = $\frac{C}{N}$ (bits per pixel) where C is the number of bits in the compressed file and N is the number of pixels in the original image. The bit rate for Barbara image is 0.1886 (Table 1) which is high compared to other standard images.

The bit rate for a Rose image is just 0.0231, which shows the compression efficiency of the algorithm.

3.3.Compression Ratio

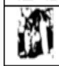
Data compression ratio is the ratio of the original file size to the compressed file size. This shows how much compression is achieved for a given image and it is evident that higher compression ratio results in drastic reduction in the size of the compressed file. Compression ratio of Barbara image is 42.412, where as that of rose is 344.84. Refer Table 1.

$$\text{Compression Ratio} = \frac{\textit{Uncompressed Size}}{\textit{Compressed Size}}$$

3.4.Compression Speed

It is the amount of time required to compress and decompress an image. This value depends on a number of factors such as the complexity of the algorithm, efficiency of Software/Hardware, implementation of the algorithm etc. Compression speed helps to rate the efficiency of the algorithm. The result table shows the efficiency of this algorithm. The proposed method, on an average takes 1.3 sec to compress and 0.65 sec to decompress the image.

Table 1. Performance Metrics – results of the proposed system.

Image		Performance Metrics					
Original	Share2	PSNR	Q	Bits per pixel	Compression Time (sec)	Decompression Time (sec)	Compression Ratio
		∞	1	0.1886	1.3602	0.6802	42.412
		∞	1	0.1618	1.3506	0.6763	49.45
		∞	1	0.0742	1.1257	0.6565	107.756
		∞	1	0.0561	1.1882	0.6770	142.488
		∞	1	0.0512	1.1064	0.6733	156.218
		∞	1	0.0363	1.2739	0.6578	220.561
		∞	1	0.0231	1.0323	0.6567	344.84

3.5.Structured Similarity Index (Q)

A quality assessment measure for images, called the Universal Image Quality Index, Q was proposed by Wang *et al.*[8] which is defined as

$$Q = \frac{4\sigma_{xy}\mu_x\mu_y}{(\sigma_x^2+\sigma_y^2)(\mu_x^2+\mu_y^2)}$$

where μ_x and μ_y, σ_x and σ_y represent the mean and standard deviation of the pixels in the original image (x) and the reconstructed image (y) respectively. σ_{xy} represents the correlation between the original and the reconstructed images. The dynamic range of Q is [-1, 1] [9]. The best value 1 is achieved for all our sample images as shown in Table 1, which shows the proposed method retains the exact original image after decompression.

4.CONCLUSION

A novel secret image sharing scheme with Image compression is proposed in this paper. The disadvantage of VC is overcome in this by repeated image compression using vector quantization followed by RLE. The results show that the technique used here is lossless compression. Hence the shares received by the receiver are exactly the same as the sender. The proposed scheme uses binary images and compression ratio and bits per pixel obtained shows the efficiency of this method. In future this work can be extended to include color images. The bits per pixel needed for color images is high and thus this method can reduce the number of bits needed to a great extent. Data security can be further enhanced by integrating Steganography with Visual Cryptography (VC) with the goal of improving security, reliability and efficiency.[10]

5.REFERENCES

[1] Naor, M and Shamir, A.,(1995). “Visual Cryptography”, Advances in Cryptology-EUROCRYPT’94, pp. 1-12.

[2] M.Mary Shanthi Rani and G.Germine Mary,(2014). “MSKS for Data Hiding and Retrieval using Visual Cryptography”, International Journal of Computer Applications, Volume 108-No 4,pp. 41-46.

[3] Mukesh Mittal and Ruchika Lamba (2013). “Image Compression Using Vector Quantization Algorithms: A Review“, International Journal of Advanced Research in Computer Science and Software Engineering, Volume 3, Issue 6,pp. 354-358.

[4] K.Somasundaram and M.Mary Shanthi Rani, (2011). “Novel K-means algorithm for compressing images”, International Journal of Computer Applications Vol.18-No.8, pp.9-13,2011

[5] K.Somasundaram and M.Mary Shanthi Rani, (2012). “Eigen Value Based K-means Clustering for Image Compression”, International Journal of Advanced Information Systems, Vol.3-No.7, pp.21-24..

[6] S. Sarika and S. Srilali , (2013). “Improved Run Length Encoding Scheme For Efficient Compression Data Rate”, Int. Journal of Engineering Research and Applications , Vol. 3, Issue 6, pp.2017-2020

[7] C. Sasi Varnan et al., (2011). “Image Quality Assessment Techniques pn Spatial Domain”, International Journal of Computer Science and Technology, Vol. 2, Issue 3, pp. 177- 184.

[8] Zhou Wang et al.,(2004). “Image Quality Assessment from error visibility to structural similarity”, IEEE transactions on Image Processing, Vol 13, No. 4, pp.600-602.

[9] Ravi Kumar and Munish Rattan, (2012). “Analysis Of Various Quality Metrics for Medical Image Processing”, International Journal of Advanced Research in Computer Science and Software Engineering, Volume 2, Issue 11, pp. 137-144.

[10] M. Mary Shanthi Rani. et.al., (2015). “Multilevel Multimedia Security by Integrating Visual Cryptography and Steganography Techniques”, Computational Intelligence, Cyber Security and Computational Models, Proceedings of ICC3 2015, Springer Publications, Volume 412 pp 403-412, On-line ISBN - 978-981-10-0251-.

Authors

Dr. Mary M. Shanthi Rani, a NET qualified Assistant Professor in the Department of Computer Science and Applications, Gandhigram Rural Institute (Deemed University), Gandhigram has twelve years of teaching and eight years of research experience as well. She has nearly twenty publications in International Journals and Conferences. Her research areas of interest are Image Compression, Information Security, Ontology, Biometrics and Computational Biology. She has authored a book titled “Novel Image Compression Methods Based on Vector Quantization”. She has also edited a volume on “New Horizons in Computational Intelligence and Information Systems” and is one of the editors of Conference Proceedings “Recent Advances in Computer Science and Applications”. She has also served as reviewer of Peer-reviewed International Journals and Conferences and is a Life member of Indian Society for Technical Education. She has the credit of being the Associate Project Director of UGC Indo-US 21st Knowledge Initiative Project.

Germine Mary.G, Associate Professor in Computer Science, Fatima College, Madurai, obtained her Post-Graduate Degree in Computer Applications (M.C.A) from St.Joseph’s College, Trichy, and M.Phil. in Computer Science from Mother Teresa Women’s University, Kodaikanal. She is currently pursuing the Ph.D degree in Computer Science at Gandhigram Rural Institute – Deemed University. She has 25 years teaching experience. Has great zeal for teaching. Her research interest includes Information Security, Visual Cryptography, Image Compression and Image segmentation. Has published seven papers in International Journals and Proceedings.