AN EFFICIENT JOINT DATA HIDING AND COMPRESSION TECHNIQUE

Athira Mohan,Ms.Nasseena N
College of Engineering chengannur,athirapolayil@gmail.com,9400820559

Abstract — In this paper an improved joint data-hiding and compression scheme for digital images is proposed. This technique use vector quantization and side match. In both techniques data hiding and image compression, can be performed in a single module. In this method VQ or side match is used for compression. Indicator bits are used for segmenting the image compressed codes into a series of sections. The receiver can achieve the mining of secret bits and image decompression productively according to the index values in the segmented sections. Experimental results reveal the efficiency of the proposed schemes.

Keywords— Data hiding, image compression, vector quantization (VQ), side match vector quantization (SMVQ), image inpainting, side match and hiding capacity.

INTRODUCTION

Nowadays people transmit and share digital contents conveniently due to the advancement in the information and internet technology. To ensure communication efficiency and save network bandwidth in such scenarios, compression techniques can be implemented on digital content. In many applications digital images and videos are converted into the compressed forms for transmission. Large numbers of privacy related issues are there in an open network environment regarding how to transmit secret or private data securely. Information hiding techniques contributes many exceptional solutions for this problem which embeds secret data into the cover image indiscernibly.

Researches conducted in the field of data hiding for digital images [2]-[5] where data hiding and image compression process are performed as two independent modules on the sender side. Under this condition, there may have many likelihood for an attacker to tear down or take advantage of the compressed image without the watermark information embedded. Performing data hiding and image compression independently may direct to lower efficiency in the applications.

The proposed work focuses on improving the high hiding capacity and compression ratio and integrates the data hiding and the image compression into a single module seamlessly. It evades the risk of the attack from interceptors and increases the implementation efficiency. The image compression in these schemes is based largely on the VQ and horizontal and vertical side match. Huffman encoding is performed among the resulting compressed code streams.

RELATED WORKS

Researches are being made in the field of data hiding and compression for digital images which conceal secret facts into the compression code of the image. VQ is one of the mainly accepted and extensively used compression techniques for digital images owing to its simplicity, i.e. simple encoding and decoding, and cost effectiveness in execution. The Euclidean distance is utilized as a measure to assess the match between each image block and the codewords in the VQ codebook during the vector quantization compression procedure. The index of the codeword with the minimum distance is used include a mention to symbolize the block. Thus, VQ encoding process consequences in a VQ index table. As an alternative of pixel values, index values are stored, therefore, the compression is achieved successfully. The VQ decompression method can be implemented easily and efficiently since each received index can be recovered by effortless table lookup procedure.

Numerous vector quantization based data hiding methods have been proposed to date. As an enhanced version of VQ, SMVQ has been introduced which create use of original VQ codebook and a sub-codebook to carry out compression of digital images. Lately, several researchers have studied on embedding secret information by SMVQ [3]-[5], [7]. In 2006 Chin-Chen Chang et.al planned a reversible data hiding based on side match vector quantization [3]. During this effort each block in the SMVQ compressed cover image was represented by fitting codeword in the sub-codebook.

In the majority of these schemes data hiding and image compression are conducted as two separate modules which imply the two processes, image compression and the data hidings are two free modules on the sender side. This will direct to some security harms and make it effortless for an attacker to compromise the compressed image devoid of the watermark data embedded. Moreover performing these two functions separately leads to incompetence in applications. To explain this problem Chuan Qin et.al proposed joint data hiding and compression scheme based on SMVQ and image inpainting [1] which incorporate the two process, data hiding and image compression, into a single module impeccably.

In [1] all image block apart from for the non residual blocks (blocks in the leftmost and topmost of the image), each of the further residual blocks in raster-scanning order can be used for embedding secret data and compressed concurrently by SMVQ or image inpainting. The compression methods vary adaptively according to the recent embedding bit. To manage the visual misrepresentation and error diffusion caused by the progressive compression of several residual blocks, vector quantization was used. The receiver can attain the extraction of secret bits and image decompression productively after segmenting the image compressed codes into a sequence of sections by the indicator bits, according to the index values in the segmented sections. The trouble with this system is that, it was a threshold depended approach. i.e. the amount of SMVQ blocks and inpainting blocks increases with T. The secret bits are simply embedded in the SMVQ and inpainting blocks. Hence, the hiding capacity of the future scheme is equal to the total number of SMVQ and inpainting blocks.

PROPOSED METHOD

The improved data hiding and compression scheme can be primarily divided into two phases. First phase is the image compression and secret data embedding and the second phase is the image decompression and secret data extraction.

In image compression and secret data embedding phase or at sender side, the original uncompressed input image I, is divided into the non-overlapping n×n blocks. The blocks in the leftmost and topmost of the input image I called as non residual blocks. These non-residual blocks are encoded by standard VQ method and these VQ encoded blocks are not used to embed secret bits. When the encoding process is complete, each non-residual blocks is simply represented by the index of the codeword with smallest distance.

A. Image Compression and Secret Data Encryption

Vector quantization (VQ) has widely been used for signal processing due to its excellent compression performance. Data hiding techniques in the VQ-compressed domain can relish advantages of both data hiding and compression for a multimedia distribution, achieving a secure channel and bandwidth/space saving for data transmission/storage. In this scheme, along with VQ, redundancy between current encoding block and neighboring block is utilized for better compression performance. This method is known as horizontal and vertical side match.

In this work, the sender performs image compression with the help of VQ code book containing codewords of length n^2.Denote the original uncompressed input image I of size M×N. The image I is divided into the non-overlapping blocks of size n×n. In this scheme, it is assumed that M and N can be divided by n with no remainder. Denote all k divided blocks in raster scanning order as $X_{(i,j)}$, where k= M×N/n^2, i= 1, 2. . . M/n, and j = 1, 2. . . N/n. The blocks in the leftmost and topmost of the image I called non-residual blocks, i.e.,$X_{(i,1)}$ (i = 1, 2,.....,M/n) and $X_{(1,j)}$ (j = 2, 3,......,N/n), are encoded by direct VQ method and these VQ encoded blocks are not used to embed secret bits. Euclidean distance used to measure the similarity between a block, X= (X_1, $X_{2,}$............,X_k) and a codeword, C_{tk}(C_{t1}, C_{t2},..........,C_{tk}) is defined as Eq (1), where C_t denotes the codeword in the codebook.

$$D_{(X,C_t)} = \sqrt{\sum_{i=1}^{k}(X_i - C_{(t,i)})^2} \qquad (1)$$

At the end of the encoding process, each image block X is represented by the index of the codeword having smallest distance i.e. index of the neighboring codeword in the codebook. In the decoder process, with the same codebook as that used in the encoder, the original image is restored from the indices using a table-lookup operation.

The residual blocks are encoded sequentially in raster scanning order i.e. from left to right and top to bottom. The encoding methods of these residual blocks are related to the whether current block has any similarity between its top or left block or not. Figure 1 shows the compression and secret data embedding in the residual block.

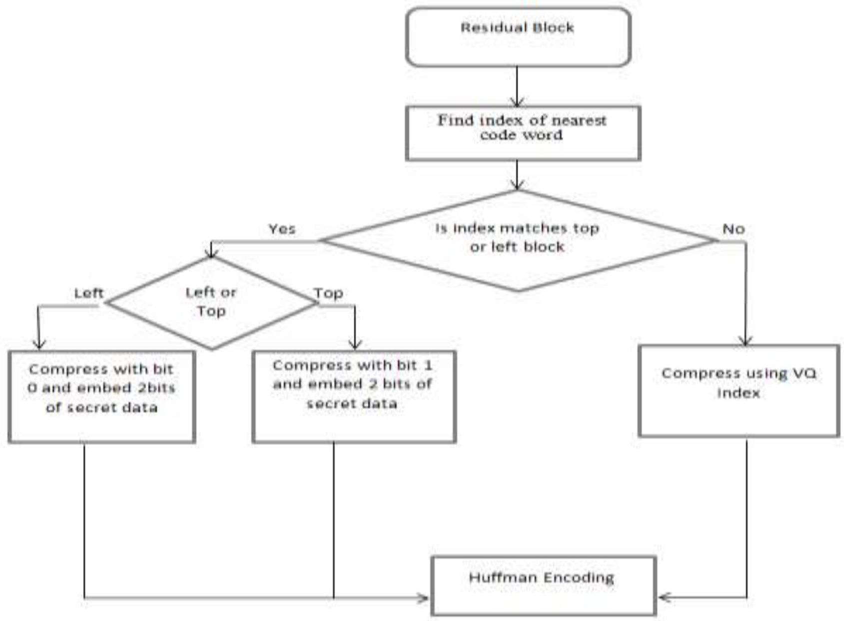


Figure.1. Flow Chart of the Compression and Secret Data Embedding in the Residual Block.

After the current block $X_{(i,j)}$ is processed, the above same procedure is repeated for the remaining residual blocks until the last residual block is processed. Then, the compressed codes of all image blocks (residual and non-residual) are concatenated. For improving the compression performance the concatenated compressed code are again decoded with Huffman coding, which will further reduce the size of transmitting data thereby saving space for data transmission/storage.

B. Image Decompression and Secret Data Extraction

The decompression and secret bit extraction of each residual block is performed at the receiver side. For that the received compressed codes are first decompressed using Huffman decoding. Huffman decoding is accomplished by a simple table look up operation.

Figure 2 shows the decompression and secret bit extraction for residual blocks. Then in order to recover the cover image and extracting secret bits, compression code stream, which is the result of Huffman decoding, are divided into a number of sections according to the indicator bits.

If the current indicator bit in the compressed codes is 0, this indicator bit and the following $\log_2 T$ bits are partitioned as a section and this section corresponds to a VQ compressed block with no embedded secret bit. The decimal value of the last $\log_2 T$ bits in this section is exactly the VQ index and the block is recovered with respect to this decimal value. Otherwise, if the current indicator bit is 1, this indicator bit and the following $\log_2(2n)$ bits are then segmented as a section, which means this section corresponds to horizontal or vertical side match. If the indicator bit is 1 then read next bit in this section. If next indicator bit is 1 then this block similar to its upper block and is replaced with the VQ index of up block index that can be used directly to recover the block. If next indicator bit is 0 then this block similar to its left block and is replaced with the VQ index of left block index that can be used directly to recover the block. In both this case remaining bits in the section represent secret bits. The original secret message can be extracted by performing decryption on the received secret bits by the security key.

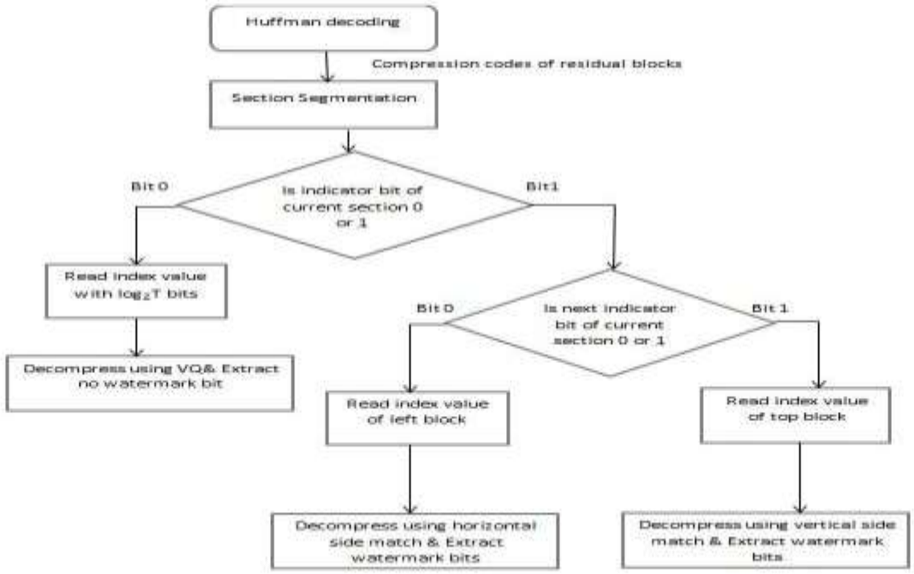
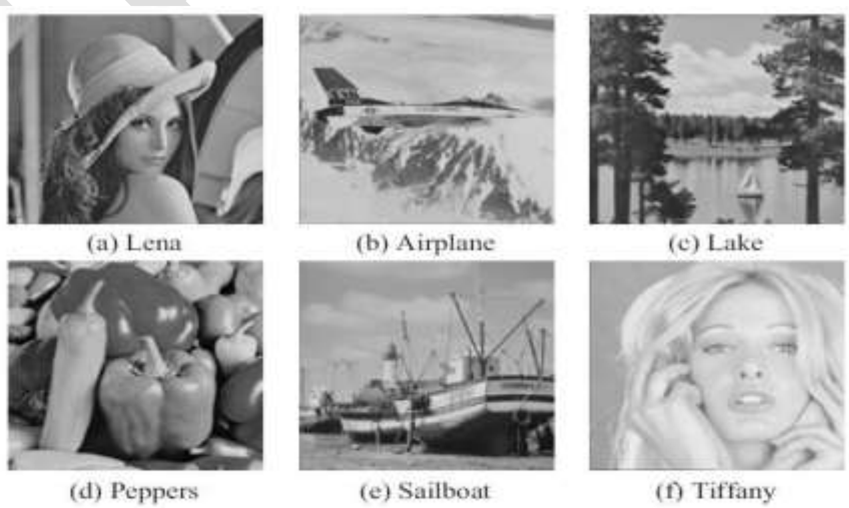


Figure. 2. Flow Chart of the Decompression and Secret Data Extraction in the Residual Block

This method is repeated for each segmented section until all sections are processed. After all the segmented sections in the compressed codes complete the above described procedure, the embedded secret bits can be extracted correctly, and the decompressed image can be obtained successfully. The final decompressed image does not contain the embedded secret bits any longer.

EXPERIMENTAL RESULTS

The experiment was conducted on a set of gray-level images of size 512×512. Six standard test images, as shown in Figure 3, are used for evaluating the presentation of the proposed system. In addition to these six standard images, the uncompressed color image database (UCID) was also considered for evaluation process.



The execution of the system is done using MATLAB R2010a programming environment. In the evaluation process, the input images are divided into non-overlapping 4×4 blocks. With respect to the size of image blocks, the length of codewords containing in the codebook was 16. The VQ codebook size T used for evaluation was 256, and secret bits for embedding were generated by RC4 encryption algorithm. After dividing the images into non- overlapping blocks, the blocks in the topmost row and the leftmost column were compressed by VQ. The VQ encoded blocks are not used for embedding secret bit. These blocks are used as a reference for encoding residual blocks. The secret bits are only embedded in the vertical or horizontal side match encoded blocks. Thus, the hiding capacity of the proposed scheme is equal to the sum of the numbers of vertical or horizontal side match encoded blocks. Figure 4 shows the input image and output image after decompression by VQ and side match. Tables 1- 7 show the comparison results for six standard test images such as Lena, Airplane, Lake, Peppers, Sailboat, Tiffany and UCID data set.

Figure.4.(a) Original Uncompressed Input Image, (b) Decompression Result

Table 1: Comparison of performance measures for Lena

Schemes	CR	PSNR	SSIM	HC
JDHC	14.2523	29.2923	0.8347	33
Proposed	19.3316	29.2935	0.8349	5522

Table 2: Comparison of performance measures for Airplane

Schemes	CR	PSNR	SSIM	HC
JDHC	14.2554	27.6578	0.8644	397
Proposed	22.5069	27.6594	0.8647	7268

Table 3: Comparison of performance measures for Lake

Schemes	CR	PSNR	SSIM	HC
JDHC	14.2616	24.6629	0.8649	543
Proposed	19.6007	26.5247	0.8692	5742

Table 4: Comparison of performance measures for Sailboat

Schemes	CR	PSNR	SSIM	HC
JDHC	14.2616	28.7814	0.8625	594
Proposed	19.2824	29.3231	0.8645	5435

Table 5: Comparison of performance measures for Tiffany

Schemes	CR	PSNR	SSIM	HC
JDHC	14.2492	25.3505	0.7724	15
Proposed	19.3587	26.4376	0.7739	5449

Table 6: Comparison of performance measures for Peppers

Schemes	CR	PSNR	SSIM	HC
JDHC	14.2522	28.8759	0.7861	32
Proposed	20.355	28.783	0.7864	6287

PERFORMANCE EVALUATION

The performance of the proposed system is presented in terms of hiding capacity, compression ratio, PSNR and SSIM value. The hiding capacity of the proposed scheme was compared against the hiding capacity of Chuan Qin.et.al method [1]. In Chuan

Qin.et.al method [1] the secret data hiding was performed depending up on the threshold and distortion value. In this method the total hiding capacity is equal to the number of SMNQ and inpainted blocks.

Denote the length of the compressed codes for the image as L. The compression ratio CR [1] can be calculated according to eq. (2). Peak signal-to-noise ratio (PSNR) [1] was utilized to measure the visual quality of the decompressed images Id, see eq. (3).

$$CR = \frac{8 \times M \times N}{L} \qquad (2)$$

$$PSNR = 10 \times \log_{10} \frac{255^2 \times M \times N}{\sum_{x=1}^{M} \sum_{y=1}^{N} [I(x,y) - I_d(x,y)]^2} \qquad (3)$$

where M and N represent image size I(x, y) and $I_d(x, y)$ represent the pixel values at (x, y) of the uncompressed image I and the decompressed image I_d respectively. For image quality assessment both PSNR value and the structural similarity (SSIM) value was used.

CONCLUSION

This work proposes an improved integrated data-hiding and compression scheme using VQ and side match. The blocks, except for non residual blocks (those in the leftmost and topmost of the image), can be embedded with secret data. Here compression and data hiding is performed simultaneously and the compression method switches between VQ and side match according to redundancy among the neighbouring blocks. If the current encoding residual block is same as its upper block then vertical side match is used. If the current encoding block is same as its left block then horizontal side match is used. Secret data is scrambled by secret key to ensure the security. These encrypted secret data is placed on the vertical and horizontal side match blocks. To further improve the compression performance Huffman encoding is applied on the secret embedded compression codes of the image. The receiver can extract the original secret data and obtain the input cover image successfully after segmenting the Huffman decoded code stream into various sections during the decompression phase.

Since the proposed method utilizes the redundancy between the blocks it is capable of embedding two bits of secret data with each side match encoded blocks. Also the proposed system follows a threshold independent procedure for integrated data hiding and compression. The experimental results show that this scheme has the better performances for hiding capacity, compression ratio, and decompression quality.

ACKNOWLEDGMENT

This project would never have been successful to this point if it weren't for the dedication put in by many minds selflessly. First, I thank GOD, THE ALMIGHTY for showering his abundant blessings upon me for the fulfillment of this project.

I express my deep sense of gratitude to Prof. Jyothi John, Principal, College of Engineering, Chengannur, for providing the necessary facilities and help from the management side to make this project.

I express my sincere thanks to Dr. Smitha Dharan, Head of the department, and Dr.Shyama Das, Associate Professor, Department of Computer Engineering, for giving me the insight which has resulted in proceeding successfully with the project. Their constant support and encouragement has been a motivation.

My special thanks to Ms.Nasseena N, project guide, for aiding me in my work and providing timely advice and valuable suggestions. I also thank all the teaching staff of College of Engineering, Chengannur, especially Computer Engineering Department. They have always been steady reflection of dedication and hard work. This humble endeavor wouldn't have become a success without the constant support, inspiration and blessings from my parents. I express my love and gratitude to all my well-wishers and friends without whose support and encouragement this work would have ever come into limelight.

REFERENCES:

[1] W. B. Pennebaker and J. L. Mitchell, The JPEG Still Image Data Compression Standard. New York, NY, USA: Reinhold, 1993.

[2] D. S. Taubman and M. W. Marcellin, JPEG2000: Image Compression Fundamentals Standards and Practice. Norwell, MA, USA: Kluwer,2002.

[3] A. Gersho and R. M. Gray, Vector Quantization and Signal Compression. Norwell, MA, USA: Kluwer, 1992.

[4] N. M. Nasrabadi and R. King, "Image coding using vector quantization:A review," IEEE Trans. Commun., vol. 36, no. 8, pp. 957–971,Aug. 1988.

[5] Announcing the Advanced Encryption Standard (AES), National Institute of Standards & Technology, Gaithersburg, MD, USA, Nov. 2001.

[6] R. L. Rivest, A. Shamir, and L. Adleman, "A method for obtaining digital signatures and public-key cryptosystems," Commun. ACM, vol. 21, no. 2, pp. 120 126, 1978.

[7] F. A. P. Petitcolas, R. J. Anderson, and M. G. Kuhn, "Information hiding survey," Proc. IEEE, vol. 87, no. 7, pp. 1062–1078, Jul. 1999.

[8] C. D. Vleeschouwer, J. F. Delaigle, and B Macq, "Invisibility and application functionalities in perceptual watermarking: An overview," Proc. IEEE, vol. 90, no. 1, pp. 64–77, Jan. 2002.

[9] C. C. Chang, T. S. Chen, and L. Z. Chung, "A steganographic method based upon JPEG and quantization table modification," Inf. Sci., vol. 141, no. 1, pp. 123–138, 2002.

[10] C. Qin, C. C Chang and Yi-Ping Chiu, "A novel joint data-hiding and compression scheme based on SMVQ and image inpainting," IEEE Trans. Image Process., vol. 23, no. 3, March. 2014.

[11]. C. C. Chang, W. L. Tai, and C. C. Lin, "A reversible data hiding scheme based on side match vector quantization," IEEE Trans. Circuits Syst. Video Technol., vol. 16, no. 10, pp. 1301-1308, Oct. 2006.

[12]. J. D. Lee, Y. H. Chiou, and J. M. Guo, "Reversible data hiding based on histogram modification of SMVQ indices," IEEE Trans. Informat. Forensics Security, vol. 5, no. 4, pp. 638-648, Dec. 2010.