INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH & DEVELOPMENT

ISSN 2278 – 0211 (Online)

A Novel Data Hiding and Compression Scheme

A. Madhuri
M.Tech (DSCE), S.V. College of Engineering Tirupati, India
N. Suguna
Assistant Professor, Department of ECE, S.V. College of Engineering Tirupati, India

Abstract:
In order to guarantee communication efficiency and save network bandwidth, compression techniques can be implemented on digital content to reduce redundancy, and the quality of the decompressed versions should also be preserved. The two functions of data hiding and image compression can be integrated into one single module, which can avoid the risk of the attack from interceptors and increase the implementation efficiency. On the sender side, the blocks in the leftmost and topmost of the image are compressed by main codebook, each of the other residual blocks in raster-scanning order can be embedded with secret data and compressed simultaneously by SMVQ according to the current embedding bit. SMVQ is develop to alleviate the block artifact of the decompressed image and increase compression ratio, because the correlation of the neighboring block is consider and the indices of the sub codebooks are stored. After segmenting the image compressed codes into a series of sections by the indicator bits, the receiver can achieve the extraction of secret bits and image decompression successfully according to the index values in then segmented sections. On the receiver side image edge based harmonic inpainting is used for reconstructing lost or deteriorated parts of images. The proposed scheme shows the performances for hiding capacity, compression ratio and decompression quality.

Keywords*: Data hiding, image compression, image inpainting, side match vector quantization.*

1. Introduction

With the rapid development of internet technology, people can transmit and share digital content with each other conveniently. In order to guarantee communication efficiency and save the network bandwidth, compression technique can be implemented on digital content to reduce redundancy, and the quality of the decompressed versions should also be preserved. Nowadays, most digital content, especially digital images and videos are converted into the compressed forms for transmission. Another important issue in an open network environment is how to transmit secret or private data securely.

Even though traditional cryptographic methods can encrypt the plaintext into the cipher text [1-2], the meaningless random data of the cipher text may also arouse the suspicion from the attacker. To solve this problem, information hiding techniques have been widely developed in both academia and industry, which can embed secret data into the cover data imperceptibly. Due to the prevalence of digital image on the internet, how to compress images and hide the secret data into the compressed images efficiently deserves in depth study.

Recently, many data-hiding schemes for the compressed codes have been reported, which can be applied to various compression techniques of digital images, such as JPEG, JPEG2000 [3-4], and vector quantization (VQ) [6-9]. As one of the most popular lossy data compression algorithms, VQ is widely used for digital image compression due to its simplicity and cost effectiveness in implementation. During the VQ compression process, the Euclidean distance is utilized to evaluate the similarity between each image block and the codeword's in the codebook. The index of the codeword with the smallest distance is recorded to represent the block. Thus, an index table consisting of the index values for all the blocks is generated as the VQ compression codes.

Instead of pixel values, only the index values are stored, therefore, the compression is achieved effectively. The VQ decompression process can be implemented easily and efficiently because

only a simple table lookup operation is required for each received index. In this work, we mainly focus on the data embedding in VQ-related image compressed codes.

An adaptive data hiding method for VQ compressed images, which can vary the embedding process according to the amount of hidden data. In this method, the VQ codebook was partitioned into two or more sub codebooks, and the best match in one of the sub

codebooks was found to hide secret data. In order to increase the embedding capacity, a VQ-based data-hiding scheme by a codeword clustering technique was proposed. The secret data were embedded into the index table by codeword-order-cycle permutation. By the cycle technique, more possibilities and flexibility can be offered to improve the performance of this scheme. Adjusted the pre-determined distance threshold according to the required hiding capacity and arranged a number of similar codeword's in one group to embed the secret sub message. The search-order coding (SOC)[6] algorithm was proposed which can be utilized to further compress the VQ index table and achieve better performance of the bit rate through searching nearby identical image blocks following a spiral path. Some steganographic schemes were also proposed to embed secret data into SOC compressed codes.
Side match vector quantization was designed as an improved version of VQ, in which both the codebook and sub codebooks are used to generate the index values, excluding the blocks in the leftmost column and the topmost row. Recently many researchers have studied on embedding secret message by VQ. The weighted squared Euclidean distance (WSED) was utilized to increase the probability of VQ for a high embedding rate. In the following, we will briefly introduce the SMVQ based coding system.

2. Data Hiding and Compression Scheme

The goal of the proposed scheme is to hide secret data or images into the host image while preserving the good image quality of the stego image. To achieve the goal, the SMVQ scheme is used to compress the secret data before they are embedded into the host image. According to the secret bits for embedding, the image compression based on SMVQ is adjusted adaptively by incorporating the image in-painting technique. After receiving the stego-image, one can extract the embedded secret bits successfully during the image compression.

2.1. Encryption

Image compression and secret data embedding is performing in the encryption process. As an extension of VQ, SMVQ is develop to alleviate the block artifact of the decompress image and increases the compression ratio, because the correlation of neighboring blocks is consider and indices of the sub codebooks are stored. In this scheme, the standard algorithm of VQ is modified to further achieve better decompression quality and to make it suitable for embedding secret bits. The detailed procedure is described as follows. In this scheme, the sender and the receiver both have the same codebook Ψ with W codewords, and each codeword length is n2. Denote the original uncompressed image sized M × N as I, and it is divided into the non-overlapping n × n blocks. For simplicity, we assume that M and N can be divided by n with no remainder. Denote all k divided blocks in raster-scanning order as Bi, j, where k = M × N / n2, i = 1, 2, …, M / n, and j = 1, 2, …, N / n.
The blocks in the leftmost and topmost of the image I, i.e., $B_{i,1}$ (i = 1, 2, …, M / n) and $B_{1,j}$ (j = 2, 3,…, N / n), are encoded by VQ directly and are not used to embed secret bits. Denote the current processing block as $B_{x,y}$ ($2 \le x \le M / n$, $2 \le y \le N / n$), and its left and up blocks are $B_{x, y-1}$ and $B_{x-1, y,}$ respectively. $c_{p,1}$ ($1 \le p \le n$) and $c_{1,q}$ ($2 \le q \le n$) represent the 2n − 1 pixels in the left and upper borders of $B_{x, y}$. The n pixels in the right border of $B_{x, y-1}$ and the n pixels in the bottom border of B_{x-1}, y are denoted as $l_{p,n}$ ($1 \le p \le n$) and $u_{n,q}$ ($1 \le q \le n$), respectively. Similar with SMVQ, the 2n − 1 pixels in the left and upper borders of Bx, y are predicted by the neighboring pixels in $B_{x, y-1}$ and B_{x-1}, y: $c_{1,1} = (l_{1,n} + u_{n,1}) / 2$, $c_{p,1} = l_{p,n}$ ($2 \le p \le n$), and $c_{1,q} = u_{n,q}$ ($2 \le q \le n$). Instead of all n^2 pixels in $B_{x, y}$, only these 2n − 1 predicted pixels are used to search the codebook Ψ. After transforming all W codewords in the codebook Ψ into the n î n matrices, the mean square error (MSE) E^w is calculated between the 2n − 1 predicted pixels in $B_{x,y}$ with the corresponding values of each transformed codeword C^w sized n × n. where $c_{p,qw}$ are the elements of each codeword C^w in codebook Ψ. The R codewords with the smallest MSEs, i.e., E^w, are selected to generate one subcodebook Θx, y for the block $B_{x,y}$ (R < W). Suppose that, among the R codewords in $\Theta_{x, y}$, the codeword indexed λ has the smallest MSE, i.e., Er ,with all n^2 pixels in $B_{x, y}$ ($0 \le \lambda \le R - 1$). The residual blocks are encoded progressively in raster -scanning order, and their encoded methods are related to the secret bits for embedding and the correlation between their neighboring blocks. SMVQ is utilized to conduct compression, which means that the index value λ occupying log2 R bits is used to represent the block Bx,y in the compressed code. Because the codeword number R in subcodebook Θx,y is less than the codeword number W of the original codebook Ψ, the length of the compressed code for Bx,y using SMVQ must be shorter than using VQ. The used image inpainting technique is described in the next subsection detailed. Then, the compressed codes of all image blocks are concatenated and transmitted to the receiver side.

$$E^w = \sum_{p=1}^{n} (c_{p,1} - c_{p,1}^w)^2 + \sum_{q=2}^{n} (c_{1,q} - c_{1,q}^w)^2 .$$

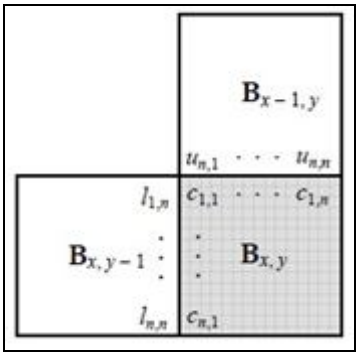


Figure 1: Illustration of the prediction based on left and up neighboring pixels

2.2. Decryption

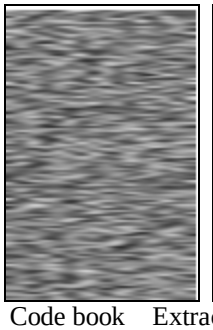
Image decompression and secret data extraction is performed in the decryption process. After receiving the decompressed codes, the receiver conducts the decompression process to obtain the decode image that is visually similar to the original uncompressed image, and the embedded secret bits can be extracted either before or during the decompression process. Because the (M + N − n) / n blocks in the leftmost and topmost of the image need to be used in the decompression for other residual blocks, they should be first decompressed by their SMVQ indices retrieved from the image compressed codes. Each SMVQ index of these pre-decompressed blocks occupies log2 W bits. Then, the k - (M + N − n) / n residual blocks are processed block by block in raster-scanning order and secret bit extraction for each residual block. To conduct the decompression and secret bit extraction of each residual block, the compressed codes are segmented into a series of sections adaptively according to the indicator bits. If the current indicator bit is 1, this indicator bit and the following log2 (R + 1) bits are then segmented as a section, which means this section corresponds to an SMVQ compressed block. After extracting a secret data, image edge based harmonic in-painting technique is used for reconstructing lost or deteriorated parts of the images Therefore, besides the image compression, the proposed scheme Image decompression and secret data extraction is performed in the decryption process. After receiving the decompressed codes, the receiver conducts the decompression process to obtain the decode image that is visually similar to the original uncompressed image, and the embedded secret bits can be extracted either before or during the decompression process. Because the (M + N − n) / n blocks in the leftmost and topmost of the image need to be used in the decompression for other residual blocks, they should be first decompressed by their SMVQ indices retrieved from the image compressed codes. Each SMVQ index of these pre-decompressed blocks occupies log2 W bits. Then, the k - (M + N − n) / n residual blocks are processed block by block in raster-scanning order and secret bit extraction for each residual block. To conduct the decompression and secret bit extraction of each residual block, the compressed codes are segmented into a series of sections adaptively according to the indicator bits. If the current indicator bit is 1, this indicator bit and the following log2 (R + 1) bits are then segmented as a section, which means this section corresponds to an SMVQ compressed block. After extracting a secret data, image edge based harmonic in-painting technique is used for reconstructing lost or deteriorated parts of the images Therefore, besides the image compression, the proposed scheme can achieve the function of data hiding that can be used for covert communication of secret data. The sender can transmit the secret data securely through the image compressed codes, and the receiver can extract the hidden secret data effectively from the received compressed codes to complete the process of covert communication. Additionally, because the secret data extraction in our scheme can be conducted independently with the decompression process, the receiver can obtain the secret bits at any time if he or she preserves the compressed codes. The proposed scheme can also be used for the integrity authentication of the images, in which the secret bits for embedding can be regarded as the hash of the image principle contents. The receiver can calculate the hash of the principle contents for the decompressed image, and then compare this calculated hash with the extracted secret bits.

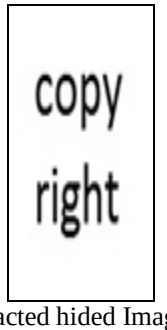
3. Results

Comparison based on threshold is done by using different code book sizes. Experiments were conducted on a group of gray-level images to verify the effectiveness of the proposed scheme. In the experiment, the sizes of the divided non-overlapping image blocks were 4x4, i.e., n=4. Accordingly, the length of each codeword in the used SMVQ codebook was 16. The parameter R was set to 15. Six standards, 512 x 512 test images, i.e., Lena, Peppers, Lake, Airplane, Sailboat, Tiffany are shown in fig2. Besides these six standard images, the uncompressed color image database that contains 1338 various color images with sizes of 512 x 384 was also adopted. The performances of the compression ratio, e-compression quality, and hiding capacity for the proposed scheme were evaluated. Because the threshold T used in the procedure of the image compression and secret data embedding is closely related to the compression method for each residual block and also influences on the performance of the proposed scheme, testing for different values of T was conducted in the compression and secret embedding procedure. The Results are shown in below figure.


Input Image


SMVQ Compressed Image


Code book



Extracted hided Image

Hide data Image


Decompressed Image

Figure 2: Experimental Results

4. Conclusion

In this paper, we proposed a joint data-hiding and compression scheme by using SMVQ and image edge based harmonic in-painting. The blocks, except for those in the leftmost and topmost of the image, can be embedded with secret data and compressed simultaneously, and the adopted compression method SMVQ according to the embedding bits. VQ is also utilized for some complex blocks to control the visual distortion and error diffusion. On receiver side, after segmenting the compressed codes into a series of sections by the indicator bits, the embedded secret bits can be easily extracted according to the index value in the segmented sections, and the decompression for all blocks can be achieved successfully by VQ, SMVQ and image in-painting. The experimental results show that our scheme has the satisfactory performances for hiding capacity, compression ratio, and decompression quality.

5. References

1. National Institute of Standards & Technology, ―Announcing the Advanced Encryption Standard (AES),‖ Federal Information Processing Standards Publication, vol. 197, no. l, 2001.
2. R. L. Rivest, A. Shamir and L. Adleman, ―A Method for Obtaining Digital Signatures and Public-Key Cryptosystems,‖ Communications of the ACM, vol. 21, no. 2, pp. 120-126, 1978.
3. P. C. Su and C. C. Kuo, ―Steganography in JPEG2000 Compressed Images,‖ IEEE Transactions on Consumer Electronics, vol. 49, no. 4, pp. 824-832, 2003.
4. H. W. Tseng and C. C. Chang, ―High Capacity Data Hiding in JPEG- Compressed Images,‖ Informatics, vol. 15, no. 1, pp. 127-142,2004.
5. 5.Y. C. Hu, ―High-Capacity Image Hiding Scheme Based on Vector Quantization,‖ Pattern Recognition, vol. 39, no. 9, pp. 1715-1724, 2006
6. C. C. Lee, W. H. Ku and S. Y. Huang, ―A New Steganographic Scheme Based on Vector Quantization and Search- Order Coding,‖ IET Image Processing, vol. 3, no. 4, pp. 243-248, 2009.
7. C. C. Chen and C. C. Chang, ―High Capacity SMVQ Based Hiding Scheme Using Adaptive Index,‖ Signal Processing, vol. 90, no. 7, pp.2141-2149, 2010.

8. L. S. Chen and J. C. Lin, ―Steganography Scheme Based on Side Match Vector Quantization,‖ Optical Engineering, vol. 49, no. 3, pp.0370081-0370087, 2010.
9. W. J.Wang, C. T. Huang and S. J. Wang, ―VQ Applications in Steganographic Data Hiding Upon Multimedia Images,‖ IEEE Systems Journal, vol. 5, no. 4, pp. 528-537, 2011