International Journal of Engineering Research and General Science Volume 3, Issue 3, May-June, 2015
ISSN 2091-2730

A REAL TIME APPROACH FOR SECURE TRANSMISSION USING IMAGE PROCESSING

Saranyarani.R
PG Student
Department Of Computer Science & Engineering
Dhanalakshmi Srinivasan Engineering College
Perambalur, Tamilnadu, India-621212
Mail id:senthilsaran16@gmail.com

Geetha.T
Assistant Professor
Department Of Computer Science & Engineering
Dhanalakshmi Srinivasan Engineering College
Perambalur, Tamilnadu, India-621212
Mail id:Geethut14@gmail.com

ABSTRACT- A novel joint data-hiding and compression scheme for digital images using side match vector quantization (SMVQ) and image in painting. The two functions of data hiding and image compression can be integrated into on single module seamlessly. On the sender side, except for the blocks in the leftmost and topmost of the image, each of the other residual blocks in raster-scanning order can be embedded with secret data and compressed simultaneously by SMVQ or image in painting adaptively according to the current embedding bit. Vector quantization is also utilized for some complex blocks to control the visual distortion and error diffusion caused by the progressive compression. 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 the segmented sections. Experimental results demonstrate the effectiveness of the proposed scheme.

KEYWORDS: Data hiding ,image compression,
Side match vector quantization(SMVQ), image inpainting

I INTRODUCTION

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 network bandwidth, compression techniques can be implemented on digital content to reduce redundancy, and the quality of the decompressed versions should also be preserved. 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 images on the Internet, how to compress images and hide 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, and vector quantization (VQ). 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 code words 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. In 2003, Du and Hsu proposed an adaptive data hiding method for VQ compressed images [18], 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 code books, and the best match in one of the sub code books 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.

II RELATED WORK

A) VECTOR QUANTIZATION

Vector quantization (VQ) has been widely used for image and speech compression in recent years, since it provides two attractive features optimal rate-distortion performance and quite simple decoder. VQ can be roughly classified into two categories: memory less VQ and memory VQ. The basic memory less VQ system is shown in Fig.1. An input image is divided into several non-overlapping blocks of pixels. A block of pixels with size $m \times m$ is called a vector with dimension $K = m \times m$. VQ is defined as a mapping Q that assigns each input vector a closest reproduction vector $\mathbf{y}=Q(\mathbf{x})$, drawn from a finite subset, $Y=\{\mathbf{y}i\ ,i=1,2,\ \ldots,C\ \}$. The subset Y is called a codebook. An element in Y is referred to as a codeword (code vector). The number of code words in the codebook, C, is the codebook size. Only index i is sent to the decoder. Consequently, the bit rate BR is $(1/K)\ C\ 2$ log bit/pixel . The decoder has a codebook identical to the encoder, and decoding can be implemented by a simple table look-up operation. In the conventional basic memory less VQ, the image blocks are processed independently.

An encryption method is presented with the novel property that publicly revealing an encryption key does not thereby reveal the corresponding decryption key. This has two important consequences Couriers or other secure means are not needed to transmit keys, since a message can be enciphered using an encryption key publicly revealed by the intended recipient. Only he can decipher the message, since only he knows the corresponding decryption key. A message can be \signed" using a privately held decryption key. Anyone can verify this signature using the corresponding publicly revealed encryption key. Signatures cannot be forged, and a signer cannot later deny the validity of his signature. This has obvious applications in electronic mail and electronic funds transfer “systems.

A message is encrypted by representing it as a number M, raising M to a publicly species power e, and then taking the remainder when the result is divided by the publicly species product, n, of two large secret prime numbers p and q. Decryption is similar; only a die rent, secret, power d is used, where The security of the system rests in part on the docility of factoring the published divisor, n. Key Words and Phrases: digital signatures, public-key cryptosystems, privacy,authentication,security, factorization, prime number, electronic mail, message-passing, electronic funds transfer, cryptography.

Digital images are the most common cover files used for steganography. In this paper, a new steganography method called JMQT based on modified quantization table is proposed. This steganography method is compared with steganography method PEG-JSteg. Theperformance parameters namely capacity and stego size has been compared. As a result capacity increases and stego size increases. So JMQT provides better capacity and JPEGJSteg provides better stego-size. Joint photographic expert group (JPEG) is a famous file for images. It applies the discrete cosine transformer (DCT) to image content transformation. DCT is a widely used tool for frequency transformation. If we apply JPEG images to data hiding, the stego-image will not easily draw attention of suspect. There is a JPEG hiding-tool Jpeg-Jsteg. In the Jpeg-Jsteg embedding method, secret messages are embedded in the least signification bits (LSB) of the quantized DCT coeficients whose values are not 0, 1, or) 1. The main drawback of Jpeg-Jsteg is less message capacity. This is because, after the DCT transformation and quantization of JPEG, the coeficients are almost all zero and cannot hide messages according to the definition of Jpeg- Jsteg. To improve the message capacity of Jpeg-Jsteg, a new data hiding method based on JPEG and quantization table modification is proposed.

Many steganographic schemes have been developed for hiding data in vector-quantisation (VQ) compressed colour images (also called palette images) . Although there are variations among them, a common feature of these methods is that they partition the codebook into a number of groups or clusters and then embed the secret message by replacing the code word indices of the compressed image with those of the same group/cluster selected according to the corresponding secret data bits. For example with a cluster of 8 (= 23) code words, each code word can embed 3 bits of the secret message. If the binary secret data bits is 0102, (or 1102), the second (or sixth) code word is used to replace the original codeword. The receiving end of the stego-image needs to have the same clustering of the same codebook. we can see that the greater the cluster, the greater the embedding capacity of each codeword of the cluster . The size of a cluster is determined by the distance between each codewordandthe cluster's centroid. The greater the distance is allowed, the larger the cluster becomes, meaning the average embedding distortion is greater because the possibility that a codeword gets replaced with a more distant codeword is higher. The feasibility resides in the optimality of the codebook clustering algorithm .Because of the indexing characteristic of this type of schemes, algorithm treats the secret message as a clustering parameter.

Vector quantization (VQ) has been widely used for image and speech compression in recent years, since it provides two attractive features: optimal rate-distortion performance and quite simple decoder.VQ can be roughly classified into two categories: memory less VQ and memory VQ. In memory less VQ, the input image vectors (blocks) are encoded independently, whereas the memory VQ exploits the correlation among neighboring blocks to further reduce the bit rate. The basic memory less VQ system. An input image is divided into severalnonoverlapping blocks of pixels. A block of pixels with size $m \times m$ is called a vector with dimension $K = m \times m$. VQ is defined as a mapping Q that assigns each input vector a closest reproduction vector$\mathbf{y}=Q(\mathbf{x})$, drawn from a finite subset$=\{\mathbf{y}i\ ,i=1,2,\ \ldots,C\ \}$. The subset Y is called codebook. An element in Y is referred to as a code word(code vector). The number of codewordsin the codebook, C, is the codebook size. Only index i is sent to the decoder. Consequently, the bit rate BR is $(1/K)\ C\ 2$ log bit/pixel (bpp). The decoder has codebook identical to the encoder, and decoding can be implemented by a simple table look-up operation. In the conventional
basic memory less VQ, the image blocks are processed independently. The bit rate can be further reduced if the interlocks correlation is appropriately exploited

IV PROPOSED SYSTEM DESIGN

This chapter describes about image compression and secret data embedding A novel joint data-hiding and compression scheme for digital images using side match vector quantization (SMVQ) and image in painting. We not only focus on the high hiding capacity and recovery quality, but also establish a joint data-hiding and compression concept and integrate the data hiding and the image compression into a single module seamlessly. On the sender side, except for the blocks in the leftmost and topmost of the image, each of the other residual blocks in raster-scanning order can be embedded with secret data and compressed simultaneously by SMVQ or image in painting adaptively according to the current embedding bit.

A) SECRET DATA EMBEDDING

In this module scheme, rather than two separate modules, only a single module is used to realize the two functions, i.e., image compression and secret data embedding, simultaneously. The image compression in our JDHC scheme is based mainly on the SMVQ mechanism. According to the secret bits for embedding.

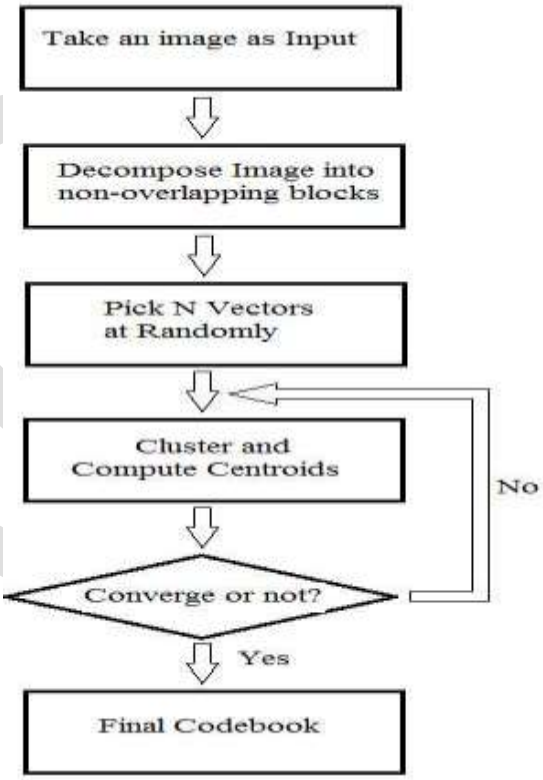
B) SECRET DATA EXTRACTION

After receiving the compressed codes, the receiver conducts the decompression process to obtain the decoded image that is visually similar to the original uncompressed image, and the embedded secret bits can be extracted either before or during the decompression.

C) ANALYSIS OF DATA

Finally we are analysis the data using MSE and PSNR method .The experimental result show that satisfactory performance for hiding capacity, compression ratio, and decompression quality.

C)SYSTEM ARCHITECTURE



GeneralizedLloydAlgorithm(GLA)called,Linde-Buzo-Gray (LBG)Algorithm. They used a mapping function to partition training vectors into N clusters. The mapping function is defined as: R→CB Let X = (x, x12…xk) be a training vector and d(X; Y) be the Euclidean Distance between any two vectors. The iteration of GLA for a codebook generation is given as follows: Step 1: Randomly generate an initial codebook CB0. Step 2: i = 0. Step 3: Perform the following process for each training vector. Compute the Euclidean distances between the training vector and the code words in CB. The Euclidean distance is defined as d(X; C) = (v∑k t=1(xt- ct) 2)…….. (1) Search the nearest code word among CBi.Step 4:Partition the codebook into N cells. Step 5**:** Compute the centroid of each cell to obtain the new codebook CB. Step 6**:** Compute the average distortion for CBi+1i+1i. If it is changed by a small enough amount since the last iteration, the codebook may converge and the procedure stops. Otherwise, i = i + 1 and go to Step 3.

V CONCLUSION

A joint data-hiding and compression scheme by using SMVQ and PDE-based image 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 switches between SMVQ and image inpainting adaptively according to the embedding bits. VQ is also utilized for some complex blocks to control the visual distortion and error diffusion. On the 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 values in the segmented sections, and the decompression for all blocks can also be achieved successfully by VQ, SMVQ, and image inpainting. The experimental results show that our scheme has the satisfactory performances for hiding capacity, compression ratio, and decompression quality. Furthermore, the proposed scheme can integrate the two functions of data hiding and image compression into a single module seamlessly

REFERENCES:

1.Chang .C. C., G. M. Chen, and M. H. Lin,(2004), "Information hiding based on search-order coding for VQ indices," *Pattern Recognit. Lett.*, vol. 25,no. 11, pp. 1253–1261.

2. Chang .C, and W. C. Wu,(2006) "Hiding secret data adaptively in vector quantization index tables," *IEE Proc. Vis., Image Signal Process.*, vol. 153, no. 5, pp. 589–597.

3. Du. W. C, and W. J. Hsu(2003) "Adaptive data hiding based on VQ compressed images," *IEEE Proc. Vis., Image Signal Process.*, vol. 150, no. 4, pp. 233–238.

4. Gersho. A, and R. M. Gray, *Vector Quantization and Signal Compression*. Norwell, MA, USA: Kluwer, (1992).

5.Hu. Y. C,(2006), "High-capacity image hiding scheme based on vector quantization," *Pattern Recognit.*, vol. 39, no. 9, pp. 1715–1724.

6. Hsieh. Y. P., C. C. Chang, and L. J. Liu(2008), "A two-codebook combination and three-phase block matching based image-hiding scheme with high embedding capacity," *Pattern Recognit.*, vol. 41, no. 10, pp. 3104–3113.

7. Hsieh .C. H, and J. C. Tsai(1996), "Lossless compression of VQ index with search-order coding," *IEEE Trans. Image Process.*, vol. 5, no. 11, pp. 1579–1582.

8. T. Kim. T (1992) , "Side match and overlap match vector quantizers for images," *IEEE Trans. Image Process.*, vol. 1, no. 2, pp. 170–185.

9. Lin. C. C, S. C. Chen, and N. L. Hsueh, "Adaptive embedding techniques for VQ-compressed images," *Inf. Sci.*, vol. 179, no. 3, pp. 140–149, 2009.

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

11. Petitcolas F. A. P., R. J. Anderson, and M. G. Kuhn(1999), "Information hiding a survey," *Proc. IEEE*, vol. 87, no. 7, pp. 1062–1078.

12. Pennebaker W. B. 16nd J. L. Mitchell (1993), *The JPEG Still Image Data Compression Standard*. New York, NY, USA: Reinhold.

13. Rivest R. L., A. Shamir, and L. Adleman1(1978),A method for obtaining digital signatures and public-key cryptosystems," *Commun. ACM*, vol. 21, no. 2, pp. 120–126.

14. Su P. C. and C. C. Kuo (2003),"Steganography in JPEG2000 compressed images," *IEEE Trans. Consum. Electron.*, vol. 49, no. 4, pp. 824–832.

15. Shie S. C and S. D. Lin [2009], "Data hiding based on compressed VQ indices of images," *Comput. Standards Inter.*, vol. 31, no. 6, pp. 1143–1149, 2009