© 2015 IJSRSET | Volume 1 | Issue 2 | Print ISSN : 2395-1990 | Online ISSN : 2394-4099
Themed Section: Engineering and Technology

Security Enhancement Using Image Inpainting

A.Rahul, M. Shankar Ganesh, T.R.B Shaman Raj, M. Veluchamy
Dhanalakshmi College of Engineering, Chennai, Tamilnadu, India

ABSTRACT

Data Hiding and Compression of digital images have always been considered as separate modules. Thus, we propose a joint data-hiding and compression scheme for digital images using Side Match Vector Quantization (SMVQ) and Image Inpainting. Data Hiding and Image Compression can be integrated into a Single Module. On the user side, the blocks in the leftmost and topmost of the image, each of the other residual blocks in raster-scanning order by hiding the data through embedded and compressed simultaneously. The receiver can achieve the extraction of secret bits and image decompression successfully according to the index values in the segmented sections.

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. 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, the meaningless random data of the cipher text may also provoke the suspicion from the attacker. To solve this issue, 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. This method ensures that a secret message is embedded into digital images and also does not arouse suspicion that the image consists of a secret data. 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 vector quantization (VQ). VQ is widely used for digital image compression due to its simplicity and cost effectiveness in implementation.

II. METHODS AND MATERIAL

Standard Technique

We had two separate modules data hiding and image compression. Data hiding is always conducted after image compression, which means the image compression process and the data hiding process are two independent modules for the users as shown in the Figure 1

The standard SMVQ method has the exactly same compression ratio scheme. However, the standard SMVQ method cannot carry secret information within its compressed codes.

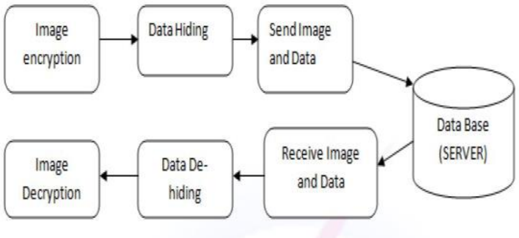

Figure 1: Data hiding process are two independent modules for the users

The decentralized CMS, each time it receives clients' requests for multimedia service tasks, the resource manager of the centralized CMS stores the global service task load information collected from server clusters and to client cluster.

The main issue in these open network environment, we can't able to transmit secret or private data securely. Traditional cryptographic methods failed to encrypt the plaintext into the cipher text. Thus here we send the encrypted data successful but compression is done separately.

Proposed Techniques

A joint data-hiding and compression scheme by using SMVQ and PDE-based image inpainting. The blocks, except for those in the leftmost and topmost of the image, can be embedded with secret data and compressed. 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. Hiding capacity, compression ratio, and decompression quality will be high.

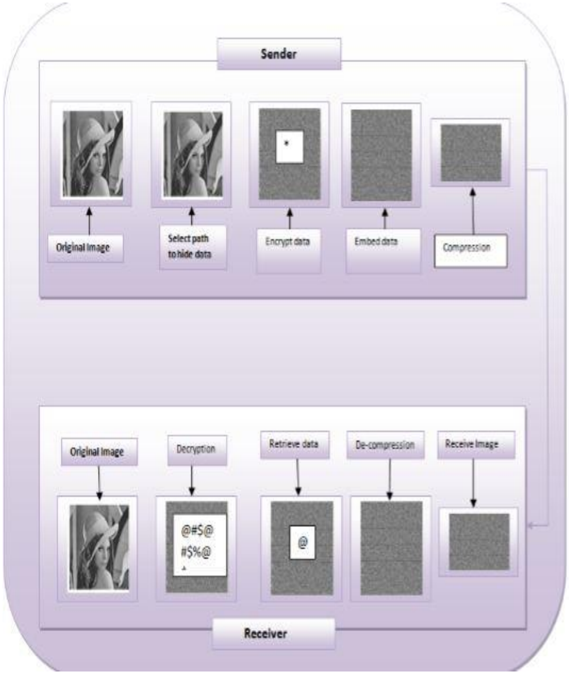

Figure 2: Two modules of hiding and compression can be combined.

Information hiding techniques have been widely developed. Both academia and industry, which can embed secret data into the cover data imperceptibly.
The Figure 1.2 explains how these two modules of hiding and compression can be combined.

Technique Used
Vector Quantization

Vector quantization (VQ) is a classical quantization technique from signal processing which allows the modeling of probability density functions by the distribution of prototype vectors. It was originally used for data compression. The density matching property of vector quantization is powerful, especially for identifying the density of large and high-dimensioned data. Since data points are represented by the index of their closest centroid, commonly occurring data have low error, and rare data high error. This is why VQ is suitable for lossy data compression. It can also be used for lossy data correction and density estimation.

Vector quantization, also called "block quantization" or "pattern matching quantization" is often used in lossy data compression. It works by encoding values from a multidimensional vector space into a finite set of values from a discrete subspace of lower dimension. A lower-space vector requires less storage space, so the data is compressed. Due to the density matching property of vector quantization, the compressed data has errors that are inversely proportional to density.

Side Match Vector Quantization (SMVQ)

Side match vector quantization (SMVQ) was designed as an improved version of VQ, in which both the codebook and the sub code books 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 SMVQ. An SMVQ-based secret-hiding scheme using adaptive technique.
Implementation

The two functions of data hiding and image compression can be integrated into one 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 VQ or image inpainting.

The implementation of project is initiated with a registration process, where the user can get their username and password. Using these credentials the user can log in to the system and then start uploading their images. The simple implementation is shown in the Figure 3.

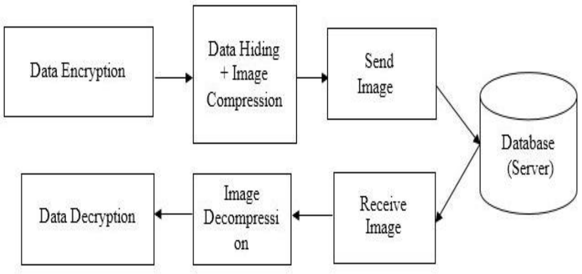

Figure 3: Implementation of System

The next step is image encryption and data hiding. Then the image with hidden encrypted data is compresses and then the image is sent. These images are stored in the database. The appropriate receiver logs in the system and then receives the file from the database. The image is decompressed and then image decryption is done. The hidden data is then extracted from the image and the receiver can read the original data that was hidden by the sender.

III. CONCLUSION

We proposed a joint data-hiding and compression scheme by using SMVQ and PDE-based image inpainting. 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. The experimental results show that our scheme has the satisfactory performances for hiding capacity, compression ratio, and decompression quality.

In future we include the proposal of a mathematical formulation of the CMS-dynMLB problem but also a theoretical analysis for the algorithm convergence

IV. REFERENCES

[1] 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.

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

[3] 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.

[4] 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.

[5] 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.

[6] 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.

[7] W. Tseng and C. C. Chang, “High capacity data hiding in JPEGcompressed images,” Informatica, vol. 15, no. 1, pp. 127–142, 2004.

[8] P. C. Su and C. C. Kuo, “Steganography in JPEG2000 compressed images,” IEEE Trans. Consum. Electron., vol. 49, no. 4, pp. 824–832,

Nov. 2003.

[9] W. J. Wang, C. T. Huang, and S. J. Wang, “VQ applications in steganographic data hiding upon multimedia images,” IEEE Syst. J.,vol. 5, no. 4, pp. 528–537, Dec. 2011.

[10] Y. C. Hu, “High-capacity image hiding scheme based on vector quantization,” Pattern Recognit., vol. 39, no. 9, pp. 1715–1724, 2006.

[11] Y. P. Hsieh, C. C. Chang, and L. J. Liu, “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, 2008.