A LITERATURE SURVEY ON SECURE JOINT DATA HIDING AND COMPRESSION SCHEME TO STORE HIGH CAPACITY DATA IN IMAGE

Karthiga Gurusamy, V.G.Karthiga[1], K.Maheswari[2], Dr.S.Kirubakaran[3]
[1]PG Student, INFO Institute of Engineering, Coimbatore
[2]Assistant Professor, SNS College of Technology, Coimbatore
[3]Assistant Professor, INFO Institute of Engineering, Coimbatore
karthigame2013@gmail.com

Abstract:- This survey propose a Novel Joint Data-Hiding and Compression Scheme (JDHC) for digital images using side match vector quantization (SMVQ) and image in painting. In this JDHC scheme image compression and data hiding scheme are combined into a single module. On the client side, the data should be hided and compressed in sub codebook such that remaining block except left and top most of the image. The data hiding and compression scheme follows raster scanning order i.e. block by block on row basis. Vector Quantization used with SMVQ and Image In painting for complex block to control distortion and error injection. The receiver side process is based on two methods. First method divide the received image into series of blocks the receiver achieve hided data and original image according to the index value in the segmented block. Second method use edge based harmonic in painting is used to get original image if any loss in the image.

I. INTRODUCTION

A. *Cryptography*

In traditional cryptographic methods [10] [11] encryption process are used to convert the plaintext into cipher text using the encryption algorithm. On the other side decryption process are used to convert the Cipher text into plain text. Cipher text implies meaningless random data. Even though cryptographic methods are providing good security, there may be chance of finding plain text by the attacker. To solve this problem steganography techniques are developed in both academia and industry. The goal of cryptography is to make text/information unreadable by a third party or attacker, whereas the goal of steganography is to hide the data from a third party or attacker.

B. *Steganography*

Steganography[12][13] is the art of hiding information in other information. Many different carrier file formats like text/image/audio/video are used but digital images are most popular because of their usage in the internet. Different application use different requirements of the Steganography techniques. Some application requires invisibility of the text into the carrier image. Some application requires less visibility. The combined cryptography and steganography scheme provide high level security to the information. In recent IT industries facilitates cryptography, stenography and security issues effectively.

C. *Compression*

While transferring larger images through standard internet connection create various scrambling problem. Compression techniques are incorporated to reduce the image's file size. Image compression techniques reduce redundancy and irrelevance of the image pixels in order to be able to store or transmit information in an efficient form. Compression techniques use mathematical calculation to analyze pixel and reduce pixel resulting in smallest image file size.

Types of Compression:-

Two types of compression techniques are followed for images.

- Lossy Compression
- Lossless Compression.

Both methods save storage space of the image but they use different procedures.

a. Lossy Compression

Lossy compression techniques creates smaller image by discarding excess image pixel from the original image. It discards details that are too small for the human eye to differentiate resulting in close approximations of the original image. An example of an image format that uses this compression technique is JPEG (Joint Photographic Experts Group). Lossy methods are works well for natural images such as photographs where minor/sometimes imperceptible loss of pixel is acceptable to achieve a substantial reduction in bit rate. The lossy compression that creates imperceptible differences may be called visually lossless.

b. Lossless Compression

Lossless compression, never removes any pixel from the original image, but instead data should be represented in mathematical formulas. In lossless compression the original image's integrity is maintained and the compressed image output is bit-by-bit identical to the original image input. An example of an image format that uses this compression technique is GIF (Graphical Interchange Format). Lossless compression technique is useful for archival purposes like medical images, technical drawings, clip arts, or comics.

D. *Joint Data Hiding And Compression Scheme (JDHC)*

Due to the affect of digital image on the internet, compressing images and hide the secret data into the compressed images efficiently deserves in-depth study. The motivation behind this project is secure image and data by Novel Joint Data Hiding and Compression to solve issues in the efficient and effective transmission and storage of multimedia data. The objective of the proposed scheme is to hide secret data or images into the host image while preserving the good image quality of the image. In an open network environment is we need to transmit secret or private data securely. Obviously, the goal of data hiding is to design schemes with high hiding capacity but low embedding distortion.

II. EXISTING SYSTEM

Various compression techniques of digital images are JPEG, JPEG2000, and vector quantization (VQ), SOC with VQ**.** In all of these schemes, data hiding is always conducted after the image compression such that image compression process and the data hiding process are two separate modules on the sender/client side. Under this circumstance, the attacker may have the opportunity to know the compressed image/data.

A. JPEG

JPEG technique controls the level of embedding rate by using a capacity factor. This method achieves high embedding capacity of maximum 20% of the compressed image size [1].

B. JPEG 2000

Rate of hiding is very important for efficient and secure communications. A high-capacity rate steganography scheme is proposed for the JPEG2000 baseline system by using bit-plane encoding procedure twice [2].

A steganographic scheme is used to reliably embed high-volume data into the JPEG2000 bit stream. The upcoming still image coding standard is an JPEG2000. This new standard overcomes JPEG by providing several important features such as resolution/quality progressive image transmission, better hardness to bit-errors, and Region of Interest (ROI) coding and so on. So JPEG2000 and its rich features will be used in many emerging applications [8].

C. Vector Quantization (VQ)

One of the most popular Lossy data compression algorithms is Vector Quantization(Vector Quantization) .This process can vary the embedding process according to the amount of hidden data. In this method, the VQ codebook such that Left and Top of the image was compressed and remaining parts are divided into two or more sub code books, and codebook/sub code books was found to hide secret data. VQ is widely used for digital image compression due to its simple use and cost reducing factor in implementation [5].

To improve security in communication Hamming codes are applied for increasing the embedding efficiency (the number of bits embedded per embedding change). This scheme provides increasing steganographic security and good image quality compared with existing schemes based on VQ compressed images [9].

D. SOC with VQ

The proposed SOC with VQ scheme, the embedding process induces no extra coding distortion and adjust the bit rate according to the size of secret data. It yields a good and acceptable compression ratio of the image. In next step, the receiver can efficiently receive both the compressed image and the embedded data almost at the same time. The search-order coding (SOC) algorithm was utilized to further compress the VQ index table and achieve better performance by searching nearby identical image blocks following a spiral path[4][5].

E. PROBLEM STATEMENT

- In JPEG method little degradation in image quality should occur[2].
- JPEG2000 compression standard limited redundancy and bit stream truncation makes it difficult to hide information. To overcome these two problems redundancy evaluation need to use [3].
- Embedding messages into VQ compression codes may greatly reduce the resolution of image because compression done at left and top of the image (Codebook) [5].
- In Vector quantization method Text boundaries are clear visible between input block.
- The two independent modules data hiding and compression used in SOC with VQ may cause a lower efficiency while using in applications [5].
- However, in all of the above mentioned schemes (JPEG, JPEG 2000, VQ, and SOC WITH VQ) data hiding could be done after image compression such that the image compression process and the data hiding process are two independent modules. So the attacker may know either image/data [5].
- Security features is not considered in JPEG 2000[8].

III. PROPOSED SYSTEM

The JDHC scheme not only focuses on the high hiding capacity and recovery quality, also integrates the data hiding and the image compression into a single module. The survey of JDHC scheme is based on SMVQ and image in painting [14][15]. The Side match vector quantization (SMVQ) was implemented as an advanced version of VQ in which sub codebooks are used to data hiding and compression [Fig 1.2].

Codebook refers to leftmost column and topmost row blocks. Sub Codebook refers to blocks excluding leftmost column and the topmost row. To increase the embedding rate in SMVQ Weighted Square Euclidean Distance is used. VQ is also utilized for some complex blocks to control the visual distortion and error diffusion. Additionally, in decompression process, the receiver can obtain the hided data/image bits at any time if he or she preserves the compressed codes. Edge based harmonic in painting [14][15] are used to construct lost part of image on receiver side.

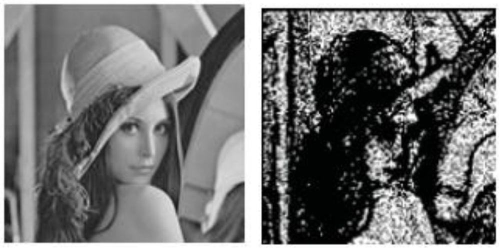
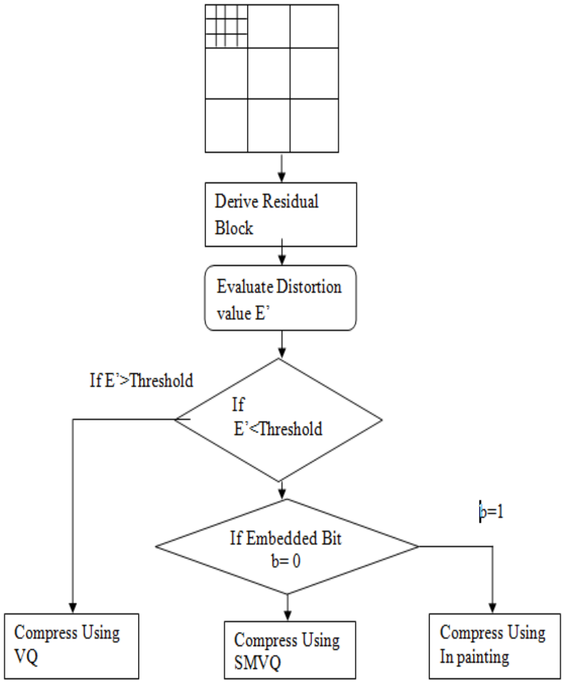


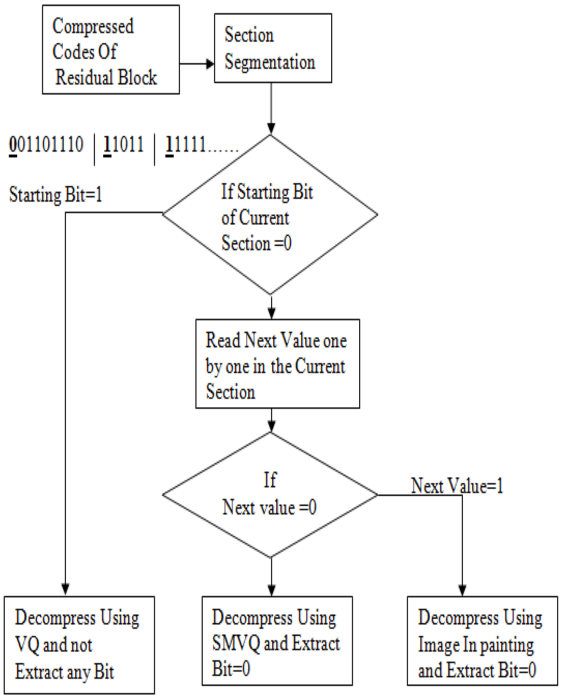
Figure. 1.1. Figure. 1.2.

Figure.1.1 Shows Original Image, Figure 1.2 shows output image get by JDHC Scheme. The Output is based on combined VQ+SMVQ+Image In painting.

Architecture of Encryption
(Compression + Data Hiding)



Architecture of Decryption
(Decompression + Data Extraction)


Compressed Codes Of Residual Block
Section Segmentation
001101110 | 11011 | 11111......
Starting Bit=1
If Starting Bit of Current Section =0
Read Next Value one by one in the Current Section
If Next value =0
Next Value=1
Decompress Using VQ and not Extract any Bit
Decompress Using SMVQ and Extract Bit=0
Decompress Using Image In painting and Extract Bit=0

Advantages:-

- For guaranteed communication efficiency and to save network bandwidth, compression techniques can be implemented on digital content to reduce redundancy.
- The quality of the decompressed image should be preserved.
- The data hiding and image compression can be integrated into one single module; it should avoid risk of attack from attackers.
- The combined module increase implementation efficiency.
- SMVQ is developed to alleviate the block artifact of the decompressed image.
- Increase compression ratio due to the correlation of the neighboring block is consider and the indices of the sub codebooks are stored.
- JDHC scheme also be used for the integrity authentication of the images.

Table 1:-Comparative Study on Existing vs. Proposed System

Methods	**Existing System**	**Proposed System**
Technique	**VQ** (Vector Quantization) [4].	**VQ** (Vector Quantization) +**SMVQ**(Side Match Vector Quantization) +**IMAGE INPAINTING**
Compression	Done at Codebook (blocks in Left column and Top most row [5].	Done at Sub code book (blocks Except Left Column and Top Row)
Compression Name	Lossy Compression[4]	Lossless Compression
Data Embedding Rate	Based on Euclidean distance[4]	The Weighted Squared Euclidean distance (WSED)
Encryption	First Image compression could be done then Data is to be hided as a separate module [5].	Compression and Data Hiding is a Single Module
Decryption	First Data should be extracted then Image should be decompressed [5].	Embedded secret bits can be extracted either before or during the decompression process

IV. CONCLUSION

The survey shows that the JDHC scheme based on high capacity data hiding. On sender side the adopted compression method switches between SMVQ and image in painting. VQ is also utilized for some complex blocks to control the visual distortion and error diffusion. On the receiver side, decompression for all blocks can also be achieved successfully by VQ, SMVQ, and image in painting. In JDHC scheme adjust capacity factor to balance between the image quality and the embedding capacity. Furthermore, the proposed method is securer than most of its predecessors. The survey shows that JDHC scheme has the satisfactory performances for data hiding rate, compression ratio, and decompression quality. Furthermore, the JDHC scheme can integrate the two functions of data hiding and image compression into a single module seamlessly.

REFERENCES

[1] H. W. Tseng and C. C. Chang, “High capacity data hiding in JPEG compressed images,” Informatics, vol. 15, no. 1, pp. 127–142, 2004.

[2] P.RamakrishnaRao”ASteganography method for JPEG2000 Baseline System” Vol. 1 No. 3 229-239 2009.

[3] ArjunNichal, Dr.ShraddhaDeshpande” A High Capacity Data Hiding Method for JPEG2000 Compression System” Vol.2, Issue4,June-July 2012,pp.751-755

[4] W. J. Wang, C. T. Huang, and S. J. Wang,“VQapplication in steganographic data hiding upon multimedia images,” IEEE Syst. J.,vol. 5, no. 4, , Dec. 2011.

[5] Chuan Qin, Chin-Chen Chang, Fellow, IEEE, and Yi-Ping Chiu” A Novel Joint Data-Hiding and Compression Scheme Based on SMVQ and Image In painting”.

[6] K.Maheswari, S.Kirubakaran, S.Karthik “Optimization techniques in heterogeneous Mobile wireless network for fast Disaster response and recovery” Research Journal of Computer Systems Engineering, Vol 04; Special Issue; PP:485-493,June 2013.

[7] V.Madhumitha, Dr.S.Kirubakaran, “A Survey on Anonymous Routing Protocols in Mobile Ad hoc Networks”, International Journal of Computer Science Trends and Technology, Volume1 Issue2, PP:34-38,Nov-Dec 2013.

[8] Po-Chyi Su and C.-C. Jay Kuo, Fellow, IEEE” Steganography in JPEG2000 Compressed Images” IEEE Transactions on Consumer Electronics, Vol. 49, No. 4, NOVEMBER 2003.

[9] Wei-Liang Tai1 And Chin-Chen Chang “Data Hiding Based On VQ Compressed Images Using Hamming Codes And De clustering” International Journal Of Innovative Computing, Information And Control Volume 5, Number 7, July 2009.

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

[11] 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.

[12] 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.

[13] 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.

[14] M. Bertalmio, G. Sapiro, V. Caselles, and C. Ballester, “Image inpainting,”in Proc. 27th Int. Conf. Comput. Graph.

[15] C. Qin, F. Cao, and X. Zhang, “Efficient image inpainting using adaptive edge-preserving propagation,” *Imag. Sci. J.*, vol. 59, no. 4, pp. 211–218,2011.