IJCSE International Journal of Computer Sciences and Engineering Open Access
Survey Paper Vol.6, Special Issue.11, Dec 2018 E-ISSN: 2347-2693

# Data-Hiding and Compression Schema Based on Image Inpainting

**P.S.S. Akilashri[1*], B. M .Kannan[2]**

[1]Department of Computer Science,National College, Tiruchirappalli, India
[2]RKV Matric Hr Sec School Jedarpalayam, Tamil Nadu, India

**Available online at: www.ijcseonline.org**

***Abstract***— Digital images and videos are converted into the compressed forms for transmission. The compression and hiding the secret data in images is done because of a wide range of hackers. In order to overcome this, the messages are sent with the help of images. Many data hiding schemes have been found in the recent times with various compression techniques in digital images. Vector Quantization method help in error distortion and error diffusion which are a cause of progressive diffusion. The new idea is that one can side match vector quantization (SMVQ) and image inpainting. Data hiding and image compression can be integrated into a single module to sent the message. The receiver then finds the secret message using the image decompression technique through the index values in the segmented sections.

***Keywords***— Image Compression, Side Match Vector Quantization (SMVQ), Data Hiding, Image In Painting.

## I. INTRODUCTION

The rapid development of Internet technology that in development, people can transmit the data and share digital (images, video) content with each other conveniently and it is rapidly used. In order to guarantee communication (that is internet) efficiency and save the network bandwidth, efficiency, compression techniques can be implemented in digital components to reduce redundancy, noise and the quality of the decompressed should also be preserved. Most digital content, digital images and videos are converted into the compressed form of transmission. Another important issue in a network environment is how to transmit the secret or private data securely through the internet. In the traditional cryptographic methods, the encryption process is used to convert the plaintext into cipher text using the encryption algorithm; the meaningless random data of the ciphertext may also arouse the suspicion from the attacker. On the other side decryption process are used to convert the Ciphertext into plain text. Ciphertext implies meaningless random data. Even though cryptographic methods are providing better security, there may be a chance of finding a plain text by the attacker. To solve this problem in steganography technique is developed in academia, industry and more. 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. Due to the rapid use of digital images on the Internet, how to compress the images and hide the secret data into the compressed form of images efficiently deserves in depth study. There many data hiding schemes for compressed codes that it is applied to hide the data, i.e. stenography etc. which apply to various different compression techniques of images, that may be JPEG200, JPEG, vector quantization (VQ). But digital images are most popular because of their usage on the internet. Different application uses different Steganography techniques on their requirements Lossy data compression techniques that create smaller image by discarding excess image pixel from the original image. VQ is used due to its simplicity and cost effectiveness for digital image compression. The Euclidean distance is taken to evaluate the similarity between the code words in the codebook and image block for the VQ compression process. The block is represented, that is recorded which is having the index of the codeword with smallest distance. The index values containing in the table for all blocks are generated as code of VQ compression. And only index values are stored instead of pixel values. And through lookup table for each received index, that is a VQ decompression process. The side match vector quantization (SMVQ) is an improved version of VQ. Both the sub codebooks and codebook are used to generate index value.

## II. LITERATURE SURVEY

1. THE JPEG STILL IMAGE DATA COMPRESSION STANDARD (1993)Authors name: w. b. penne baker and j.

l. Mitchell.

ADVANTAGES: This method is applicable to practically any kind of continuous tone digital source image (i.e. for most practical purposes not be restricted to images of certain dimensions, color spaces, pixel aspect ratios, etc.) and not be limited to classes of imagery with restrictions on scene content, such as complexity, range of colors, or statistical properties. As diverse imaging applications become increasingly implemented on open networked computing systems.

DISADVANTAGE: At the time of its selection, the DCT based method was only partially defined for some of the modes of operation.

2. VECTOR QUANTIZATION AND SIGNAL COMPRESSION. NORWELL, MA, USA: KLUWER, 1992. Authors name: a.gersho and r. m. gray**.**

ADVANTAGE: To improve the embedding capacity as well as to have minimum distortion to carrier media our method proves good.

DISADVANTAGE: The proposed method cannot handle the large secrete data to be hiding.

3. A METHOD FOR OBTAINING DIGITAL SIGNATURES AND PUBLIC-KEY CRYPTOSYSTEMS (1978).Authors name: r. l. rivest, a. Shamir, and l. Adelman.

ADVANTAGES: This method useful for secure communications to be established without the use of couriers to carry keys, and it also permits one to \sign" digitized documents. Signatures cannot be forged, and a signer cannot later deny the validity of his signature.

DISADVANTAGE: It may be possible to prove that any general method of breaking our scheme yields an efficient factoring algorithm

## III. PROBLEM STATEMENT

For improved system efficiency and for secure transmission of the data which has to be kept private, the two different modules viz. data hiding and data compression are combined into one module.

## IV. PROPOSED SYSTEM

The proposed scheme is an improved method for joint reversible data-hiding and compression scheme for digital multiband images. The image compression techniques like Vector Quantization and Side Match Vector Quantization along with the image inpainting are used for data hiding and compression. In the proposed method, the multiband image is used to hide the secret data. On the sender side, the image is separated into individual bands. From the multiband image the user can select the bands to hide the secret data according to the size and nature of the data to be embedded. The bands are then compressed according to the ascending order of their band number. The bands used for hide secret data are sub divided into equal size blocks. The number of blocks and the correlation between neighboring blocks determines the hiding capacity. In the proposed method, 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 compression of bands is based mainly on the Side Match Vector Quantization (SMVQ) mechanism which is a modified form of VQ. Except for the blocks in the leftmost and topmost of the band, each of the other residual blocks will be embedded with secret data and compressed simultaneously by SMVQ or image inpainting adaptively according to the current secret bit. VQ is also used for some complex blocks and the blocks in the leftmost and topmost of the band to control the visual distortion and error diffusion caused by the progressive compression.

**Comparative Study on Existing vs. Proposed System**

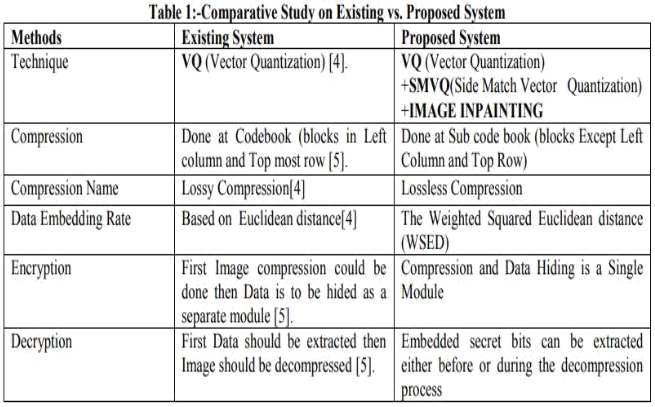


Table 1:-Comparative Study on Existing vs. Proposed System

| Methods | Existing System | Proposed System |
|---|---|---|
| Technique | **VQ** (Vector Quantization) [4]. | **VQ** (Vector Quantization)<br>+**SMVQ**(Side Match Vector Quantization)<br>+**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 |

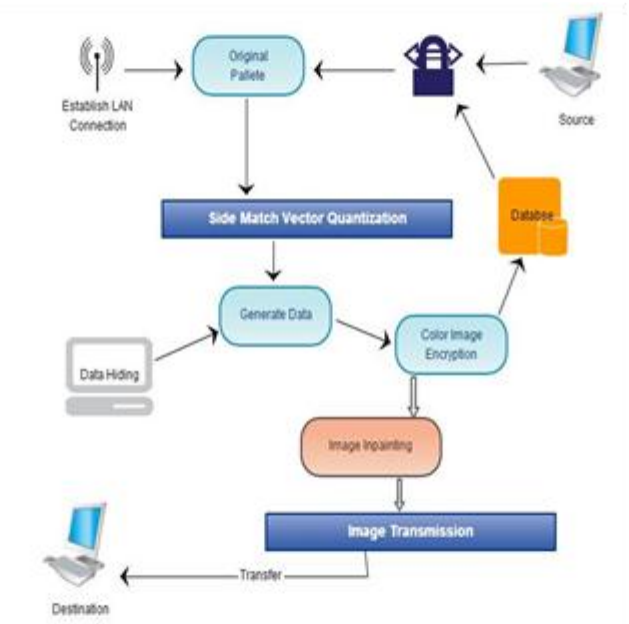
## V. IMPLEMENTATION

In the proposed 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, the image compression based on SMVQ is adjusted adaptively by incorporating the image inpainting technique. Embedding: Embedding is the process of combining the original and key image. The embedded image seems to be like the original image. Then the embedded image is sent. Extraction: Extraction is the process of separating the original and key image from the embedded image

## VI. ALGORITHM
## SMVQ (SIDE MATCH VECTOR QUANTIZATION)

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. We are using SMVQ in high capacity data hiding and color image encryption algorithm was developed to encrypt 64-bits of plaintext into 64-bits of cipher text efficiently and securely. The operations selected for the algorithm were table lookup, modulus, addition and bitwise exclusive or to minimize the time required to encrypt and decrypt data on 32-bit processors. A conscious attempt was made in designing the algorithm to keep the operations simple and easy to code while not compromising security. But during each round of Blowfish, the left and right 32-bits of data are modified unlike DES which only modifies the right 32-bits to become the next round's left 32-bits. This operation is different from the permutation function performed in DES. The first block is entered to the decryption function and the same encryption key is used to decrypt the image but the application of sub keys is reversed. The process of decryption is continued with other blocks of the image from top to bottom.

## SYSTEM MODEL



## VII. CONCLUSION AND FUTURE WORK

A joint data-hiding and compression scheme by using SMVQ and image edge based harmonic in-painting. Only the left most and the top most data blocks can be compressed simultaneously. The adopted compression method SMVQ is done according to the embedding bits. The compressed codes are then converted in to a series of indicator bits when it reaches the receiver side. Embedded bits are extracted through index value segmentation. The decompression for all blocks can be achieved successfully by VQ, SMVQ and image in-painting. The results prove that the system has hiding capacity, compression and decompression quality.

## REFERENCES

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

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