NOVATEUR PUBLICATIONS
International Journal of Research Publications in Engineering and Technology [IJRPET]
ISSN: 2454-7875
VOLUME 3, ISSUE 4, April-2017

COMPRESSION AND DATA HIDING SYSTEM BASED ON SMVQ

MISS SAPATNEKAR APARNA A.
Department of Electronics and Telecommunication,V.V.P Institute of Engg & Technology, Solapur
University, Solapur, Ms, India. sapatnekaraparna@gmail.com

PROF MANTRI D. B.
Department of Electronics and Telecommunication,V.V.P Institute of Engg & Technology, Solapur
University, Solapur, Ms, India. dbmantri@yahoo.co.in

ABSTRACT:

There are many digital multimedia transmissions on the network. Therefore to protect the secret messages during transmission is an important issue. For assurance of communication efficiency and save network bandwidth compression techniques can be implemented to reduce redundancy and the quality of the decompressed versions should also be preserved. Here a novel system is shown for compression and data hiding using side match vector quantization (SMVQ). 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.

KEYWORDS: Data hiding, Image compression, Side match vector quantization.

I .INTRODUCTION:

With the fastest development of internet technology people can easily transmit and share the information with each other conveniently. Compression techniques can be implemented on digital content to reduce redundancy and the quality of the decompressed versions should also be preserved. 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 ciphertext the meaningless random data of the ciphertext 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 images on the Internet, how to compress images and hide secret data into the compressed images efficiently deserves in-depth study.

On the sender side we have to perform the image compression and data hiding process separately this may give attacker on opportunity to intercept the compressed image so this two independent modules may cause lower efficiency in applications. In this system focus is on the high hiding capacity and recovery quality and also establishes joint data hiding and compression into single module. This can avoid the risk of the attack from interceptors and increase the implementation efficiency.

W. C. Du Ni et.al. Proposed a reversible data hiding based on adaptive compresses method. In this method the VQ codebook was separated into two or three sub codebooks and the best one of the sub codebooks was found out to conceal the bits. This method increased the hiding capacity. Major drawback of this method was more distortion of extraction stage and recovered image. To overcome this problem side match vector quantization (SMVQ) is used in the proposed system.

II. METHODOLOGY:

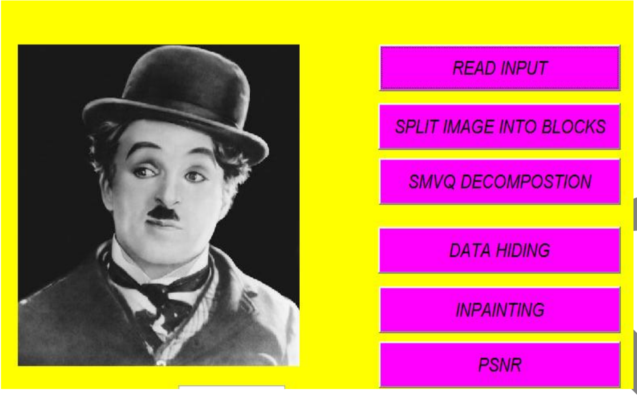
First the image gets divided into 4x4 blocks, where the top most and left most columns are compulsorily compressed using vector quantization. The left over blocks are compressed using SMVQ and image inpainting according to the mean square error (MSE) value. If the compression is done using SMVQ or inpainting then watermark bits are added to the block. For all the residual blocks, except those top most rows and leftmost column a mean square error (MSE) value or distortion value is calculated and this value is compared with threshold value. If MSE is greater than the threshold value then block is directly compressed using vector quantization index and if MSE is less than or equal to the threshold value, then embedded watermark bit is checked. If the embedded watermark bit is 0 then it is clear that block is compressed using SMVQ index and if the embedded watermark bit is 1 then it can be said that image inpainting is used for compression. Thus blocks in the image are compressed by adaptively using vector quantization, side match vector quantization or image inpainting.

Algorithm of compression and secret data embedding

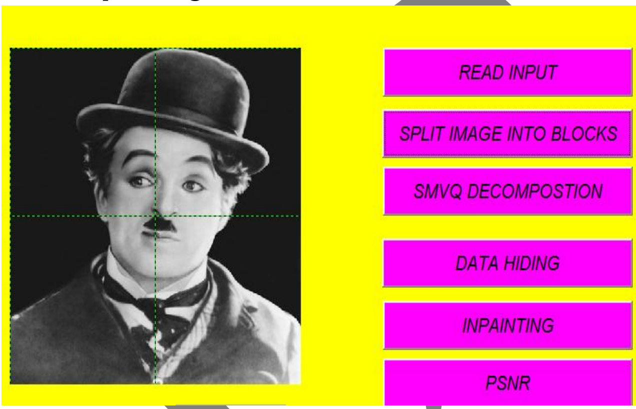
```
Step1: Read input image
Step2: Take luminance component of the image
Step3: Split the image into 4x4 blocks
Step4: Top most row and left most column compressed by VQ and embedding 0
Step5: For all residual blocks calculate $E^r$ (Mean Square Error) and set threshold
Step6: If $E^r > T$ then block is compressed by VQ
Step7: If $E^r \leq T$ embedded secret bit is 0 then block is compressed by SMVQ and if embedded secret bit is 1 block is compressed by image inpainting
Step8: Stego image
```

III.EXPERIMENTAL RESULT:

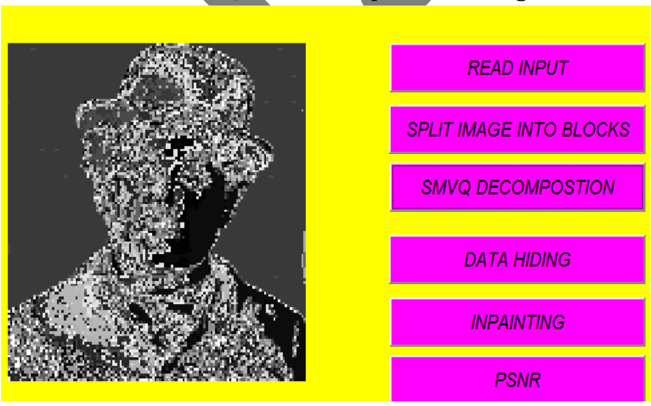
1. First read the input image



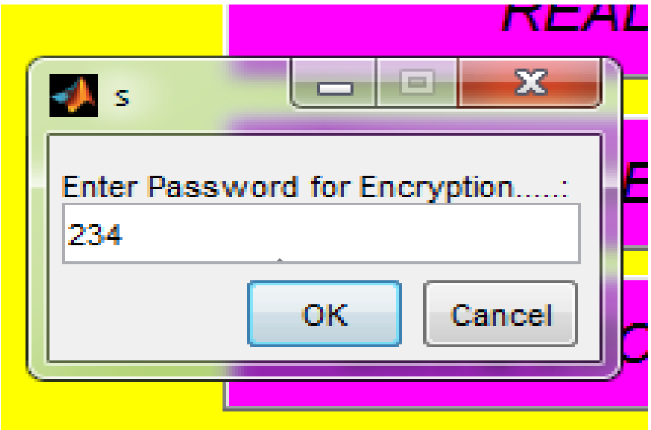
2. Split image into 4x4 block



3. Perform SMVQ and decompose the image



4. After decomposing the image to hide the data into image by entering the password



Enter Password for Encryption.....:
234

IV.CONCLUSION:

A joint data-hiding and compression (JDHC) concept can integrate the two functions of data hiding and image compression into a single module, which can avoid the risk of attack from interceptors and increase the implementation efficiency, recovery quality.

REFERENCES:

1) Xinmiao Zhang, Student Member, IEEE, and Keshab K. Parhi, Fellow, IEEE "*High-Speed VLSI Architectures for the AES Algorithm*" IEEE TRANSACTIONS, VOL. 12, NO. 9, SEPTEMBER 2004.

2) Tim Good, Student Member, IEEE, and Mohammed Benaissa, "*Very Small FPGA Application-Specific Instruction Processor for AES*" IEEE TRANSACTIONS ON CIRCUITS AND SYSTEMS, VOL. 53, NO. 7, JULY 2006.

3) Ashwini M. Deshpande, Mangesh S. Deshpande and Devendra N. Kayatanavar,*"FPGA Implementation of AES Encryption and Decryption"* International Conference on Control, Automation, Communication and Energy Conservation-2009, 4th-6th June 2009.

4) Chen-Hsing Wang, Chieh-Lin Chuang, and Cheng-Wen Wu *"An Efficient Multimode Multiplier Supporting AES and Fundamental Operations of Public-Key Cryptosystems"* IEEE TRANSACTIONS, VOL. 18 NO. 4, April 2010.

5) Issam Hammad, Student Member, IEEE, Kamal Sankary, Member *"High-Speed AES Encryptor with Efficient Merging Techniques"* IEEE EMBEDDED SYSTEMS LETTERS VOL. 2, NO. 3, SEPTEMBER 2010.