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

A NOVEL JOINT DATA-HIDING AND COMPRESSION SCHEME BASED ON SMVQ AND IMAGE INPAINTING

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:
The internet and multimedia are the fastest development technology, the problem of protecting transmitted information become an important issue. To save the network bandwidth and to reduce redundancy and to improve the decompressed quality compression techniques can be implemented .The system shown a joint data hiding and image compression using side match vector quantization and image inpainting, the system helps to increase the implementation efficiency and avoid the risk of attack. Here system use both codebook and subcodebooks to generate the index values and it also including the topmost row and the left most column of the image with each other residual block in raster scanning order and it can be embed with secret data and it will compressed simultaneously by side match vector quantization (SMVQ) or image inpainting.
KEYWORDS: Data hiding, Image compression, Side match vector quantization, Image inpainting.

I.INTRODUCTION:

The rapid development in the internet technology, people can share and transmit information or digital content with each other very easily .Therefore the problem is to protect transmitted media has become more important. In order to enhance the safety of information transmissions, secret information can be protected by traditional cryptographic method can encrypt the plaintext into the ciphertext. The problem is 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.

Data hiding has an essential role to play in information security. Secret information is hidden into cover digital content, i.e images, audio, videos, or texts, before such digital content is transmitted on the public channels like the Internet. Using a data hiding technique ensures that cover media has been distorted minimally even though it does contain secret information. That technique can prevent the transmitted content from arousing the attraction of malicious attackers. As a result, the privacy of the secret information is maintained.

In this paper the joint data hiding and compression is based on SMVQ and image inpainting. Vector quantization is also used for some complex residual blocks to control the visual distortion and error diffusion .The sender side, except for the block in the topmost and leftmost of the image each of the other residual block in raster scanning order can be embedded with secret data and it compressed by side match vector quantization or image inpainting.

Image inpainting is the recovery of the missing or corrupted part of an image, so that the reconstructed image looks natural. Image inpainting also know as image completion or disocclusion. There are three classes of image inpainting methods; partial differential equation (PDE) based method, interpolation based method and patch based method.

II.METHODOLOGY:

Rather than two separate modules, only a single module is used to realize the two function i.e secret data embedding and image compression simultaneously. According to the secret bits for embedding, the image compression based on SMVQ is adjusted adaptively by incorporating the image inpainting technique. After receiving the secret embedded and compressed codes of the image, one can extract the embedded secret bits successfully during the image decompression.

The sender and receiver both have same codebook Ψ with W code words and each codeword length is n2. The original uncompressed image size is M × N as I, and it is divided into the non-overlapping n × n blocks. We assume that M and N can be divided by n with no remainder. Denote all k divided blocks in raster scanning order as Bi, j, where k = M × N/ n2, i = 1,2, . . . , M/n, and j = 1, 2, . . . , N/n. Before being embedded, the secret bits scrambled by a secret key to ensure security. The blocks in the leftmost and topmost of the image I, i.e., Bi, 1(i = 1, 2, . . . , M/n) and B1, j (j = 2, 3, . . . , N/n),

are encoded by VQ directly and are not used to embed secret bits. The residual blocks are encoded progressively in raster scanning order and their encoded methods are related to the secret bits for embedding and the correlation between their neighboring blocks.

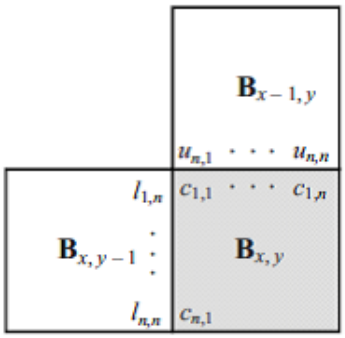


Illustration of the prediction based on left and up neighboring pixels.

$$E^{w} = \sum_{p=1}^{n} (c_{p,1} - c_{p,1}^{w})^2 + \sum_{q=2}^{n} (c_{1,q} - c_{1,q}^{w})^2$$

The calculation of mean square error (MSE) E^w is between the 2n-1 predicted pixels in $B_{x,y}$ with corresponding values of each transformed codeword C^w of sized nxn.

There are two phases in the system. Compression and secret data embedding following are the algorithm steps:

Encryption

Step1: First read the input image

Step2: After reading the image take the luminance component of the image

Step3: Split the image into 4x4 blocks

Step4: After splitting the image the top most row and left most column compressed by VQ and embedding 0

Step5: Calculate E^w (Mean Square Error) and set the threshold for all residual blocks

Step6: If E^w > T then block is compressed by VQ

Step7: If E^w < T embedded secret bit is 0 the block is compressed by SMVQ and if embedded secret bit is 1 the block is compressed by image inpainting

Step8: Got stego image

Decryption

Setp1: In this step split the stego image into 4x4 block

Step2: After splitting the stego image segmentation is done

Step3: If indicator bit is 0 the decompress the image by VQ

Step4: If indicator bit is 1 then read index value if it is less than R (codeword in subcodebook) block is decompressed by SMVQ and secret bit 0 is extracted

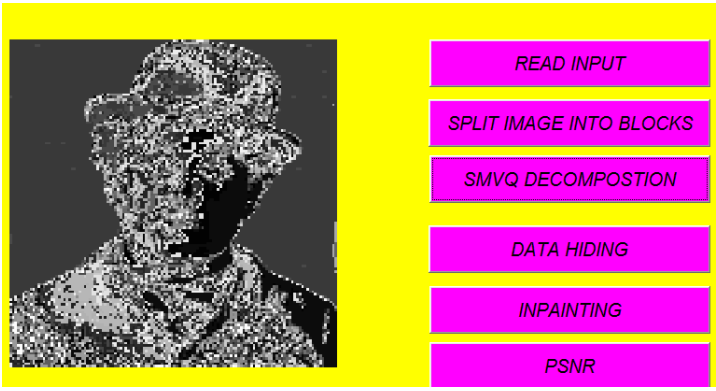
Step5: If index value is equal to R then block is decompressed by image inpainting and secret bit 1is extracted

III.EXPERIMENTAL RESULTS

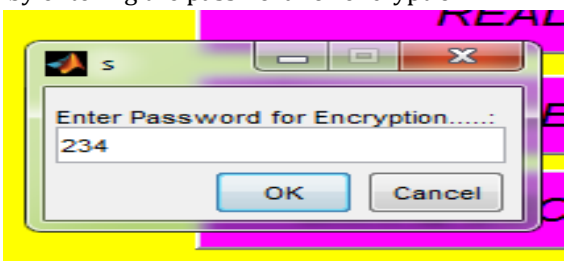
1. First read the input image

2. Split image into 4x4 block

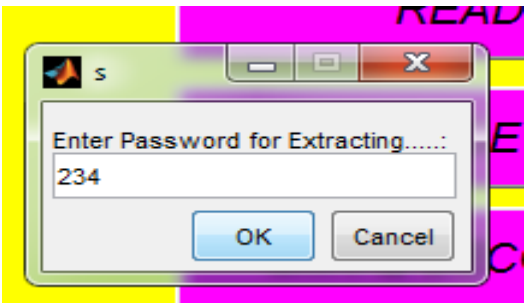
3. Perform SMVQ and decompose the image



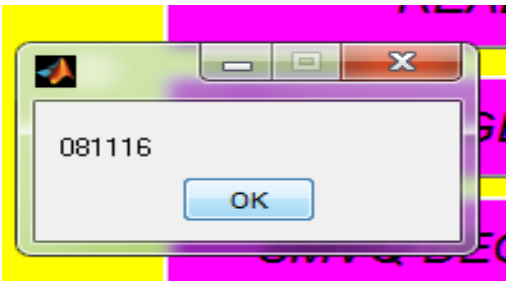
4. After decomposing the image to hide the data into image by entering the password for encryption



After entering password for encryption it show the same message for entering password for extracting the hide data

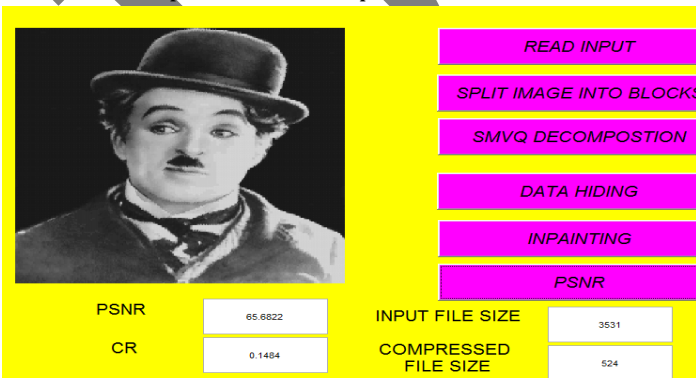


5. After performing data hiding, 081116 this hidden data is extracted



6. After performing inpainting got original image

7. In the last step it calculate value of PSNR, CR and also calculate the input file size, compressed file size



IV.CONCLUSION

Here a novel system is described which integrate the two function of data hiding and compression in to single module and it is based on SMVQ and image inpainting according to embedding bits. For some complex blocks VQ is used. On the receiver side the compressed code are segmented by using indicator bits into series of section, so whatever secret data is embedded can be easily extracted by index value and the decompression of the image can be done by SMVQ , VQ and image inpainting.

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.