Asian Journal of Information Technology 16 (6): 399-409, 2017
ISSN: 1682-3915

VQ, SMVQ Based Efficient Reversible Image Data Hiding with EICA Method

[1]K.R. Prabha and [2]M. Jagadeeswari
[1]Department of Electronics and Communication Engineering,
[2]Department of Electronics and Communication Engineering (PG-VLSI Design),
Sri Ramakrishna Engineering College, 641022 Coimbatore, Tamil Nadu, India

Abstract: A novel reversible data hiding and compression scheme to embed high capacity of secret bits into a Vector Quantization (VQ) and Side Match Vector Quantization (SMVQ) based compressed image and recover cover image after data extraction is proposed. This study, uses Enhanced Imperialist Competitive Algorithm (EICA) that uses contrast sensitivity as the fitness function to determine threshold value to signify embedding rate for each region of the cover image based on the size of the secret message for optimal embedding capacity and to achieve exact recovery of cover image. The output size of code stream is preserved hiding two secret bits into a single index value during data hiding. For complete recovery of the cover image after the secret extraction and to achieve a high compression ratio Discrete Cosine Transform (DCT) transform and Burrows Wheeler Transform (BWT) transform is used before the quantization. DCT provides excellent energy compaction and lossless BWT reorders the symbols according to their following context. Thus, the proposed method embeds secret bits and compresses the image with secret data and gives the output as code streams with preserved size. Experimental results show that the proposed scheme achieves high embedding capacity and compression rate.

Key words: Data compression, discrete cosine, transforms, image retrieval, image reconstruction, vector quantization

INTRODUCTION

The digital data communication helps in efficient and faster communication and also provides higher protection from the malicious transmissions. With the increased growth of digital communication, the security threats have also grown considerably proving to be a greater threat for efficient communication. The security threat not means the illegal retrieval of data but also includes the blockage of data, data corruption and loss of data due to fake traffic. In order to avoid these security issues, many techniques have been developed and still the research is carried out for the betterment. Data hiding is one of the basic technique incorporated for secure transformation and privacy. It has various fields of application such as steganography, cryptography and watermarking. Each of this has its unique identity and usage.

Wu *et al*. (2003a, b) presented the problems and the problems on data hiding in the images are presented. Of all the above data security problems, the most prominent issue is the illegal data retrieval to trace the confidential details of a person or an organization for the beneficial of trackers. This problem has become pivotal in the confidential communication process especially in the defense fields. The problem also creates privacy breach. Hence, an efficient technique called data hiding has been introduced to provide protected data and communication of confidential information.

Data hiding is implemented with various method of implementation. Evolution of data hiding is very vast. The basic data hiding and their issues were considered. Data can be hidden inside another data or an image, video/audio file as per the necessity. Data hiding in images has been regarded as the simplest technique other than data hiding in messages. Many concepts of data hiding based on LSB stenography (Yang *et al*., 2009; Tyagi, 2012), diamond encoding (Chao *et al*., 2009) and lossless compression (Ni *et al*., 2004; Kumar and Garg, 2012) and retrieval have been utilized.

Image data hiding has many techniques like stenography, cryptography and watermarking. The techniques are used for a long time and been efficient to a greater level. There have been many other techniques from time-to-time but were not sufficiently effective (Sanyal *et al*., 2015; Lin *et al*., 2015). Watermarking is a copyright marking technique in which the secret data is

Corresponding Author: K.R. Prabha, Department of Electronics and Communication Engineering,
Sri Ramakrishna Engineering College, 641022 Coimbatore, Tamil Nadu, India

embedded into the cipher text of a cover media. Cryptography is a technique that hides data in the presence of third party and converts the data into an unreadable form.

Literature review: Wang *et al*. (2010) proposed reversible image data hiding scheme primarily based on VQ compressed pix. Embedding of secret bits into the VQ index table with the aid of modifying the index fee in step with the distinction of neighboring indices is executed. The proposed scheme is compared with the scheme proposed by Wang and Lu in both data hiding capacity and bit rate. The main disadvantage in this technique is that reduced code stream and increased embedding capacity era not gained simultaneously.

Goswami and Tamrakar (2013) presented a data hiding technique based on the neural networks to enable efficient retrieval encrypted media. The technique uses Multilayer Perceptron (MLP) algorithm of Artificial Neural Networks to improve security in data hiding. The synaptic link structure helps in propagating. The MLP algorithm estimates the synaptic weight of the neurons connected in the input stage and uses back propagation learning model to retrieve the cover media, i.e., image, video or audio files.

Eleni Varsaki presented a singular statistics hiding technique based on histogram modification. The technique has large embedding capacity that enables better peak signal-to-noise ratio. The technique has the ability to retrieve the cover image without any damage. The technique has major applications. However, the drawback with the machine is that it's miles taken into consideration to be the weakest embedding approaches that has much less security.

Zhang *et al*. (2014) introduced an improved data hiding with efficient reversibility of the cover image. In this approach, before embedding the data, some of the pixels are estimated before encryption. This increases the additional data to be embedded in the estimating errors. The encryption errors are estimated using a special encryption scheme while a benchmark algorithm is used to analyze the rest of the pixels. The approach is highly applicable and has better PSNR value to embed additional data. The extraction and estimation are natural processes that improve the data hiding capacity with less errors and hence high security.

Huang *et al*. (2013) provided reversible records hiding schemes based on SMVQ to increase both the image first-class and the embedding ability where multiple secret bits are embedded into a block. Other reversible facts hiding scheme which has a natural VQ index table as output is proposed. The weighted bipartite graph is used to version the scheme and the matching method is used to find out the high-quality answer. Mahajam *et al*. (2014) presented a technique with the similar approach of introducing a reserved room concept before encryption. Unlike other reserving approaches, the approach reserves the room of pixels by utilizing only the emptied out rooms without removing the current data. Hence, the reservation improves data hiding.

Kumar ana Grag (2012) offered a unique approach of integrating information hiding and lossless image compression. The approach was based on SMVQ and image in-portray. The method adaptively uses image compression function. Initially, the data are embedded into the cover image using SMVQ technique and then the cover image along with secret data is compressed by SMVQ index. The data and the image can be retrieved at the decryption process without any quality loss.

Ni *et al*. (2004) also presented a lossless data hiding approach that mainly reduces the loss creating salt-pepper noise. The method uses robust static quantity as a parameter to improve the retrieval capacity in the robust JPEG image compression. The technique of bit embedding improves the data embedding pixels and difference approach retrieves the cover media effectively with no loss.

Chiou *et al*. (2011) discussed the drawbacks of using distorted data hiding techniques and came up with a new technique of data hiding by the use of quad-tree segmentation and histogram shifting. The technique uses the local distribution of pixel intensities to maximum advantage by considering multiple local histograms for hierarchical partitioning. The cover image is partitioned into multiple blocks of pixels and are arranged in an in tree format. Secret data and the partition tree details are embedded into the image blocks. This partitioning improves the hiding capacity and helps in efficient decryption of cover media with the secret data with no errors/loss.

MATERIALS AND METHODS

Proposed work: Though the mentioned techniques in the existing papers are efficient, it lacks certain improvement for the capacity of embedding the message and also in maintaining the size of the code stream. Hence, the proposed work incorporates both the challenges and provides us better results that extend the use of this technique. The process is initialized by applying DCT to the subdivided blocks of the cover image. Then BWT is introduced to enhance the compression rate. After the blocks are transformed vector quantization and side matching quantization is implemented by selecting the threshold value by ICA technique. And by incorporating a special path to data embedding where 2 bits of secret data is embedded into the index value gives us reduced length of the code stream. The following study explains the proposed system in a detailed manner and gives the performance comparisons of each process based on the quality measurement metrics.

The proposed work consists of flow of processes; initially a cover image is taken and divided into blocks. DCT and BWT are applied on it to transform it into compressible form. The method of embedding the secret bits is modified in proposed path in order to reduce the length of the code circulate of the encoded output. Embedding technique is finished based on the brink fee that divides it into VQ or SMVQ technique. The choicest threshold price is chosen the usage of the EICA scheme that promises better compression fee and excessive embedding potential.

Data hiding and compression phase: The proposed scheme as opposed to two separate modules, most effective a single module is used to realize the 2 procedures specifically, image compression and secret data embedding, simultaneously. The whole technique is described below with the Pseudo code. Pseudo code for data-hiding and compression:

- The cover image is transformed into blocks of pixels that represent a matrix
- Then, it undergoes discrete cosine transform to pre-process the image block
- Then, the cover image block of pixels are under BWT technique
- The converted image pixel of the cover image is ready for simultaneous compression and embedding
- The image I is divided into n×n blocks. The blocks inside the leftmost and topmost part of the image I are encoded by using VQ
- The residual blocks are encoded using VQ or SMVQ technique based on the threshold value. This process is done progressively with relation to secret bits and correlation between their neighboring blocks
- The encoding process is completed and the code stream is given as output

Initially, a cover image is taken and divided into blocks. DCT and BWT are applied on it to transform it into compressible form. The method of embedding the secret bits is modified in proposed path in order to reduce the length of the code stream of the encoded output. Embedding process is finished based on the threshold value that divides it into VQ or SMVQ technique. The proposed block includes a single module that is used to realize the 2 techniques namely, image compression and secret data embedding, concurrently.

Pre-processing using discrete cosine transform: The idea of DCT (Van, 2009) is to de correlate the image data by converting the image into elementary frequency components. By using DCT-based coding, the digitized image needs to be split into blocks of pixels, typically 8×8 blocks. The DCT scheme is lossless. A quantization step where the process will produce a lot of zero coefficients for better compression ratio could be applied here but there is some loss of information during this step. The forward discrete cosine transform of a 2-dimensional 8×8 block image is given as follows:

$$F(u,v)=\frac{1}{4}\left\{\begin{matrix}C(u)C(v)\sum f(x,y)\cos\left(\left(2i+1\right)u\Pi\right)/ \\ 16\cos\left(\left(2j+1\right)v\Pi\right)/16\end{matrix}\right\} \quad (1)$$

The forward discrete cosine transform concentrates the energy on low frequency elements which are placed in the top-left corner of the sub image.

F(u, v) is the transformed DCT coefficient and f(x, y) is the value of the pixel of the unique sample of the block. When the images is considered, f(x,y) is the 8×8 matrix of the original image. The Pseudo code for the DCT is as follows:

- The image of 256×256 pixels is considered and it is represented as an 8×8 blocks of pixels and represented in matrix denoted by f(x, y)
- Shift the pixels of f(x, y) matrix by -128 levels to yield pixel values between (-128, 127)
- Then DCT is applied using equation F(u, v) is obtained as a matrix where large values also called as lower frequencies are in top-left and higher frequencies are in the lower-right corner

Lossless Burrow-Wheeler transform: The Burrows-Wheeler transform is based on the block-sorting lossless data compression algorithms which are used in many practical applications, especially in data compression. The BWT transforms a block of data into a form which is easier to compress. In this research, DCT is applied before using the BWT to achieve the better compression rate of the image. BWT is an efficient algorithm used in the compression stage of image as it has the advantage of efficient reversible property. BWT (Van, 2009) uses the image as blocks of pixels and compresses the blocks without the loss of finer details. At the decryption stage, the Inverse Burrows-Wheeler Transform (IBWT) is applied to reconstruct the original image blocks with the concealed data.

The reconstructed image will be of the same original quality and size indicating that the approach provides lossless data hiding. Then, the decryption retrieves the secret message and the cover image efficiently. BWT is applied to the block of data of the cover image. It transforms the block values such that the image can be compressed later. The scanning path for data embedding is selected and path of the pixels are transformed using BWT.

Image compression and secret data embedding: The proposed block includes a single module this is used to recognize the two approaches particularly, compression and embedding, simultaneously. This process is based particularly on VQ and SMVQ method to compress the cover image and embed the secret data into the compressed codes (Qin *et al*., 2014). Blocks of the first column and the first row are not embedded with the secret bit. Then, from left to right and from top to down each block X is processed by the VQ or side-match VQ which is determined by the optimal value of the threshold.

To preserve the size of the output code stream: The cover image block is set for encoding process. The blocks are scanned using a path in which the two secret bits are embedded into the cover image to hold the scale of the code stream.

Two secret data bits are being hidden in each block and the output M-sequence bits are twice as large as the number of blocks in the cover image in order to maintain that almost each block can be distributed with two bits data from the M-sequence. The algorithm for the selection of path that produces the shorter output code stream is illustrated by Wang *et al.* (2011). This also adds on another feather to the cap of the advantages of the proposed scheme.

Selection of scanning path for preserving code stream size: Two secret data bits are being hidden in each block and the output M-sequence bits are twice as large as the number of blocks in the cover image in order to maintain that almost each block can be distributed with two bits data from the M-sequence. The algorithm for the selection of path that produces the shorter output code stream is illustrated by Wang *et al.* (2010). This also adds on another feather to the cap of the advantages of the proposed scheme.

Selection of threshold value by Enhanced Imperialist Competitive Algorithm (EICA): Blocks of the first column and the first row are not embedded with the secret bit. Then, from left to right and from top to down, each block X is processed by the VQ or side-match VQ which is determined by the surest value of the threshold. To decide the threshold value to suggest embedding rate for each region of the cover image EICA technique is proposed. EICA uses contrast sensitivity as the fitness function to locate optimal threshold value of the cover image.

Imperialist Competitive Algorithm (ICA) (Lin *et al*., 2012) in the evolutionary computation field is based on human's socio-political evolution. The algorithm initiates with the random population called countries. Best countries in the population are selected as the imperialists and the rest shapes as the colonies of these imperialists. Country = [p1, p2... pN]. The cost of the country is found by evaluating the function f at the variables p1, p2... pN. Among them countries with minimum cost is chosen as imperialists. Then, a normalised cost and normalised power is calculated to divide the colonies among the imperialists:

- Initialize the empires and their colonies positions randomly
- Colonies move towards the imperialist's position
- Compute the total price of all empires the use of the electricity of both the imperialist and its colonies
- Choose the weakest colony from the weakest empire and supply it to the empire that is maximum effective and do away with the powerless empires
- If there's just one empire, then prevent else do
- Check the termination conditions

The proposed algorithm of enhanced ICA technique involves the introduction of fitness function as Contrast Sensitive Function (CSF). CSF (Qin *et al*., 2014) describes the observing trend of humans to the visibility of sine gratings. The logical and eminent form of CSF is:

$$\text{CSF}(f) = \alpha f e^{-bf} \sqrt{1+ee^{bf}} \quad (2)$$

Where:

f = The frequency in cycle per degree
c = 0.06
L = The luminance of the pattern of the image

$$b = 0.3\left(1+\frac{100}{L}\right)0.15 \quad (3)$$

$$\alpha = \frac{540\left(1+\frac{0.7}{L}\right)^{-0.2}}{1+\frac{12}{w}\left(1+\frac{f}{3}\right)^{-2}} \quad (4)$$

The enhanced ICA method involves the introduction of artificial imperialist. The process begins with the listing of all the imperialists in the ascending order based on the fitness function CSF. An artificial imperialist is constructed as weighted sum of all imperialists.

The process begins with the listing of all the imperialists in the ascending order based on the fitness function CSF. An artificial imperialist is constructed as weighted sum of all imperialists:

$$P\alpha = \sum_{i=1}^{m} w_i p^i \quad (5)$$

$$W_i = \frac{(0.9)^i}{\sum_{j-1}^{m}(0.9)^j} \quad (6)$$

Where:
i = The n umber of empires and
j = The imperialist number

The weights of these imperialists shape a geometric series with ratio 0.9. An efficient imperialist has the very best weight. The artificial imperialist combines the area of interest of all imperialists and allows exploring all global surest correctly. If the artificial imperialist p^a is better than the weakest imperialist p^m, then p^a becomes the brand new imperialist of empire m and p^m is clearly discarded. The algorithm is explained as:

- All imperialists are sorted in ascending order of their fitness function as p^1, p^2, Y, p^m
- Assemble artificial imperialist p^a using Eq. 5:

$$P\alpha = \sum_{i=1}^{m} w_i p^i$$

And:

$$W_i = \frac{(0.9)^i}{\sum_{j-1}^{m}(0.9)^j}$$

- If $f(p^a)>f(p^m)$ then
- p^a replaces p^m as the imperialist of empire m
- End if

After finding the most excellent threshold price with the aid of EICA the residual blocks are encoded. The simultaneous compression and embedding segment of the residual block is explained inside the following study. The residual blocks are encoded steadily using raster scanning order and their encoded techniques are associated to the name of the secret bits for embedding and the correlation among their neighboring blocks. The Pseudocode of the embedding manner (Qin *et al*., 2014) in residual block is given under:

- Denote the processing block as Bx,y and its left and top blocks are Bx, y-1 and Bx-1, y, respectively
- cp, 1 ($1 \le p \le n$) and c1, q ($2 \le q \le n$)represent the 2n-1 pixels in the left and upper borders of the current processing block
- The n pixels in the right side of $B_{x,y-1}$ and the n pixels in below the $B_{x-1,y}$ are denoted as $l_{p,n}$ ($1 \le p \le n$) and $u_{n,q}$ ($1 \le q \le n$), respectively
- This 2n-1 pixel in the left and upper borders of current block are predicted by neighboring pixels in $B_{x, y-1}$ and $B_{x-1, y}$
- This 2n-1 expected pixels are used to look in the codebook. After reworking all code phrases within the codebook into n×n matrices, the mean square error is calculated between the 2n-1 pixels and corresponding values of each codeword
- R code words with the smallest MSE are filtered to generate one sub code book for the current processing block
- Assume if there exists a code word listed with has the smallest MSE (E^r) then if E^r > Threshold (T) which determined the use of EICA, then it is clear that the current residual block is in a complex area and it has very low correlation with its neighbouring blocks
- Consequently, VQ with codebook log2 W is used to compress the block $B_{x, y}$ and no secret bits are embedded in this case
- Otherwise, if $Er \le T$, it implies that the residual block Bx, y locates in a notably clean vicinity and it has higher correlation with its neighboring blocks. As a consequence on this condition, SMVQ is used to encode
- Before the process of embedding the adoption of the proposed work to preserve the code stream length is taken into account. Thus, the scan path preferred embeds two secret bits into the cover image block

Beware that, if VQ is followed, an indicator bit 0, need to be introduced before the compressed code of the VQ index for $B_{x, y}$. If no longer, the indicator bit, 1 is added as the prefix of the compressed code for $B_{x, y}$. As for the present block if its Er is not greater than the Threshold T and the current secret bit s for embedding is 0, SMVQ is applied to conduct compression which implies that the index price λ that occupies [log2 R] bits is substituted in the compressed code. This procedure of image compression and secret data embedding continues until all residual blocks are processed. Then, the compressed codes of all image blocks of embedded image are concatenated and transmitted to the receiver side.

Image de-compression and data extraction: After receiving the compressed codes, the receiver decompresses the image to attain the decoded image that looks as visually similar to the authentic uncompressed picture and the embedded secret bits may be extracted (Qin *et al*., 2014). Pseudocode for decompression and extraction of secret records is as follows:

- Partition the compressed code stream Cw into section segments
- Find whether the indicator bit of the current section is 0 or 1
- If indicator bit is 0, then read index value with log2W bits and decompression is done using VQ technique.
- If indicator bit is 1, then read index value with log2 (R+1) bits and decompression is done using SMVQ technique
- Finally the secret data and corresponding block data of cover image are extracted
- The values of the recovered blocks that represent the cover image are applied for inverse BWT for decompression
- The output of the inverse BWT is processed for inverse DCT to obtain the decompressed image as original cover image
- Thus data and cover image are extracted without any loss (Fig. 1)

Hence, the secret data and the code stream of cover image are extracted. Therefore, besides 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. Thus, the secret data is recovered and the cover image is sent for retrieval through inverse BWT and inverse DCT (Fig. 2).

The inverse Burrows-Wheeler transform: The matrix of the cover image is sent as an input to the inverse BWT. As BWT is a reversible transformation which can recover the original sequence from the BWT output sequence,

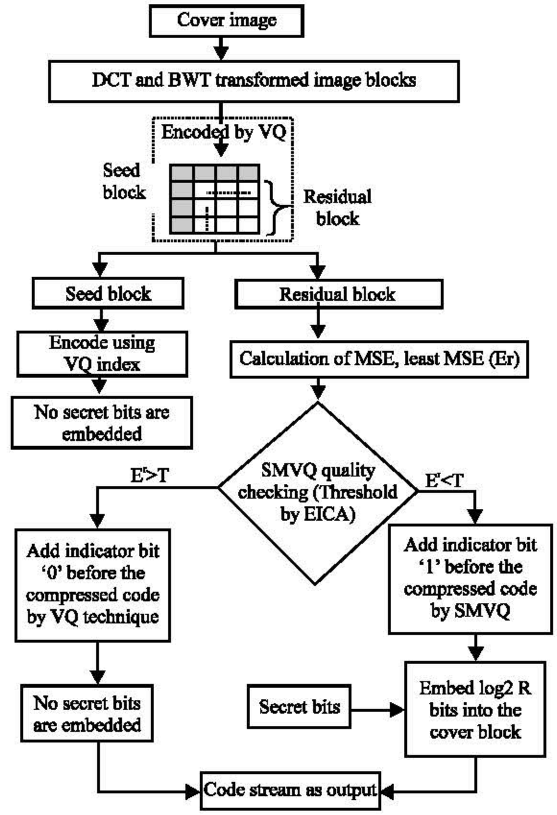

Fig. 1: Block diagram for data hiding and compression

128	136	142	137	126	125
132	138	133	137	131	137
110	135	137	168	119	123

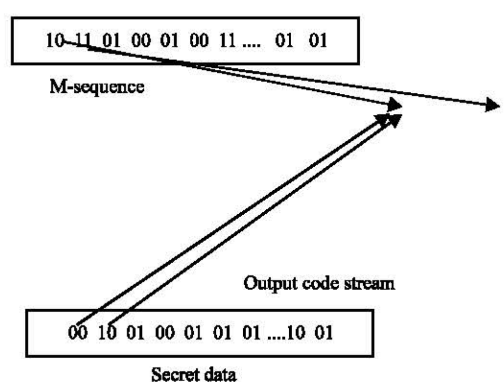

Fig. 2: Path for encoding

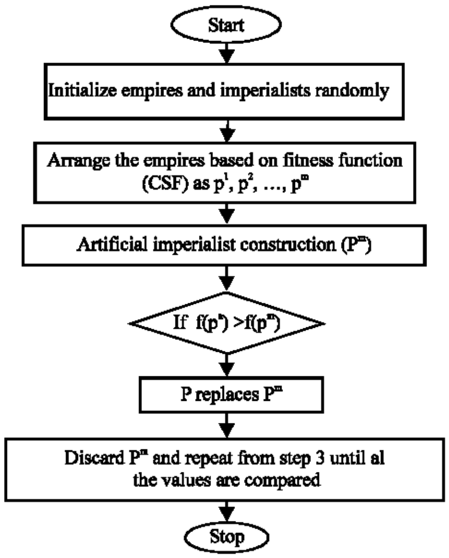

Fig. 3: Flow chart of imperialist competitive algorithm

only the BWT output sequence and index value are needed for reconstructing the original sequence. To solve the reverse BWT (Van, 2009) using output of the BWT and index, the steps are:

- For I = 1.... n-1
- Step (3i-2): place column n in front of column 1.... i-1
- Step (3i-1): order the resulting length i strings lexicographically
- Step 3i: place the ordered list in the first I columns of table
- The flowchart of the Imperialist Competitive algorithm is shown in Fig. 3

The inverse discrete cosine transform: The matrix obtained after reverse BWT undergoes inverse DCT (Van, 2009). Following equation is Inverse Cosine Transform (IDCT) using for decoding the compressed image (Fig. 4):

$$f(x,y)=\frac{1}{4}\sum_{u=0}^{7}\sum_{v=0}^{7}C(u)C(v)F(u,v)\cos\frac{(2i+1)u\pi}{16}\cos\frac{(2j+1)u\pi}{16} \quad (7)$$

Where:

$$C(u)C(v)=\begin{cases}\frac{1}{\sqrt{2}} & u,v=0\\ 1 & \text{otherwise}\end{cases} \quad (8)$$

Where:

F(u, v) = The transformed DCT coefficient
f(x, y) = The value of the pixel of the original sample of the block

Thus, the proposed work not only retrieves the secret data but also able to get the cover image without any loss.

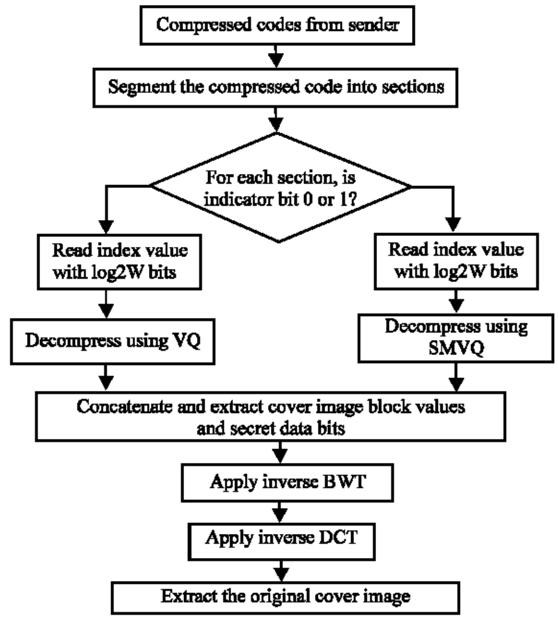

Fig. 4: Flow chart for image decompression and extraction

RESULTS AND DISCUSSION

In this study, the lossless reversible data hiding using DCT-BWT-VQ-SMVQ-EICA method is compared with data hiding using simple VQ-SMVQ, DCT-VQ-SMVQ and DCT-BWT-VQ-SMVQ and the results are tabulated. Evaluation is done using a set of parameters that defines the performance of the system. The parameters are Peak Signal-to-Noise Ratio (PSNR), error rate, compression ratio, structural similarity, bit rate, embedding capacity. By comparing the evaluation parameters of the methods, their performance of the proposed technique outstands from other existing techniques.

The image results of the lossless reversible data hiding using DCT-BWT-VQ-SMVQ-EICA method is compared with data hiding using simple VQ-SMVQ, DCT-VQ-SMVQ and DCT-BWT-VQ-SMVQ and the results are shown in Fig. 5.

From the comparison result shown above, it is clear that the proposed scheme gives you the best result in the extraction of the cover image. Evaluation is done using a set of parameters that defines the performance of the system. The parameters are Peak Signal-to-Noise Ratio (PSNR), error rate, compression ratio, structural similarity, bit rate, embedding capacity.

The comparison of the proposed work is done with various existing works that incorporate VQ based reversible data hiding (Wang *et al*., 2010), SMVQ with classification codebooks (Lee *et al*., 2010) and VQ, SMVQ image in-painting (Qin *et al*., 2014). The results are

Table 1: Parameter comparison results based on parameters

Parameters	Lena: Wang *et al.* (2010)	Lena: Lee *et al.* (2010)	Lena: Qin *et al.* (2014)	Lena: DCT-BWT-VQ-SMVQ-EICA method	Barbara: Wang *et al.* (2010)	Barbara: Lee *et al.* (2010)	Barbara: Qin *et al.* (2014)	Barbara: DCT-BWT-VQ-SMVQ-EICA method	Vegetables: Wang *et al.* (2010)	Vegetables: Lee *et al.* (2010)	Vegetables: Qin *et al.* (2014)	Vegetables: DCT-BWT-VQ-SMVQ-EICAmethod
Compression ratio (%)	27.00	31.00	36.50	39.00	22.00	25.00	27.60	30.50	24.00	26.90	35.80	31.20
PSNR(db)	28.00	32.00	34.80	38.30	26.00	29.00	32.00	35.80	29.00	33.50	36.90	39.80
Structural similarity	0.89	0.70	0.91	0.93	0.87	0.88	0.90	0.91	0.81	0.83	0.89	0.91
Bit rate (kb/s)	11.00	9.50	8.60	5.00	10.00	9.20	8.50	6.20	12.00	10.60	8.10	5.00
Embedding capacity (kb sec)	1.32	1.44	1.47	1.49	1.25	1.33	1.37	1.45	1.36	1.49	1.52	1.57
Error rate (%)	0.23	0.20	0.18	0.15	0.25	0.21	0.19	0.17	0.28	0.24	0.23	0.18

Fig. 5: Images results of DCT-BWT-VQ-SMVQ-EICA method: a, c, e) Original image and b, d, f) Reconstructedimage,DCT-BWT-VQ-SMVQ-EICA method

projected as a bar chart for parameters and the comparison is summarised in Table 1 for all the four methods.

Peak Signal-to-Noise Ratio (PSNR): Peak Signal-to-Noise Ratio (PSNR) is used to represent the index of media quality evaluation and substitutes the common MSE of frames or pixels in the PSNR computing equation to obtain the PSNR of the media segment, expressed as:

$$PSNR_{(s)} = -10\times\log_{10}\sum_{i=1}^{N}\left(\left(MSE_i\right)/MAX^2\right)/N \quad (9)$$

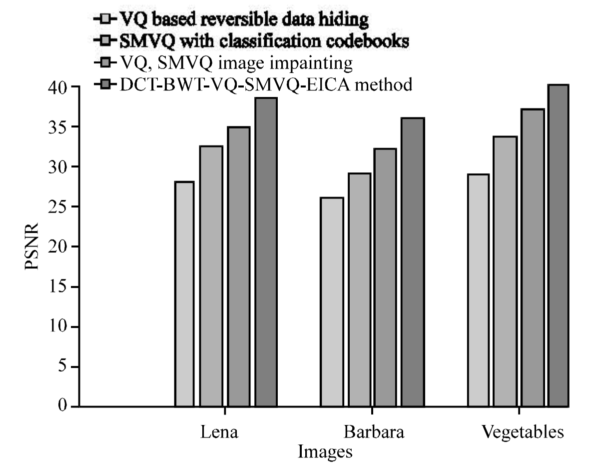

Fig. 6: Comparison result of the PSNR value

Figure 6 shows the comparison of all the four methods in terms of PSNR value for the 3 images tested. This shows that the proposed DCT-BWT-VQ-SMVQ-EICA method is the better technique in terms of PSNR.

Error rate: Error rate is the ratio of number accurately retrieved pixels in an image to the number of corrupted or lost pixels. Figure 7 shows the comparison of all the four methods in terms of error rate with respective to three images. This shows that the proposed DCT-BWT-VQ-SMVQ-EICA is the better technique in terms of error rate.

Compression ratio: The compression ratio is used to measure the potential of data compression by means of comparing the dimensions of the image being compressed to the size of the original image. The more the compression ratio, the higher the wavelet features.

Figure 8 indicates the evaluation of all the four methods in terms of compression ratio respective

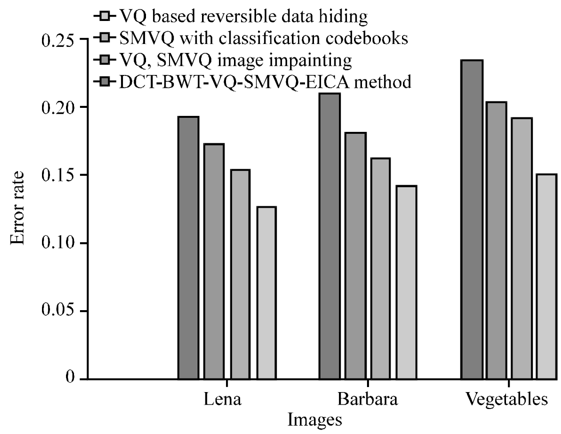

Fig. 7: Comparison result of the error rate

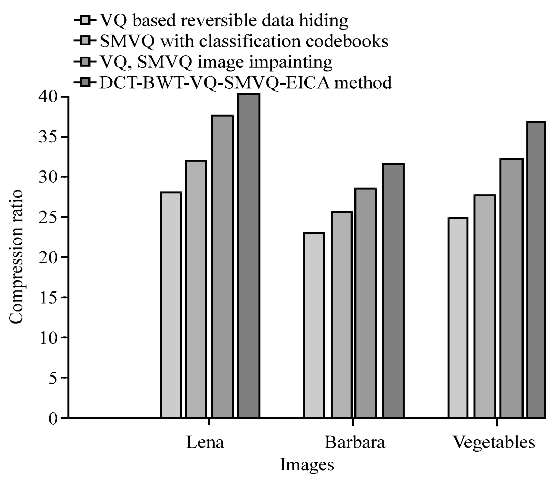

Fig. 8: Comparison result of the compression ratio

to 3 images. This indicates that the proposed DCT-BWT-VQ-SMVQ-EICA is the higher method in phrases of ratio of compression.

Similarity: The Structural Similarity (SSIM) was utilized to assess the visual quality of the decompressed image. The degree of SSIM become advanced based totally at the characteristics of the Human Visual machine (HVS) which incorporated the statistics of shape, luminance and evaluation synthetically for the photograph satisfactory evaluation. The value of SSIM is decimal value; it becomes 1 if both are identical.

Figure 9 shows the comparison of all the four methods in terms of structural similarity with respect to three images. This shows that the proposed DCT-BWT-VQ-SMVQ-EICA is the better technique in terms of ratio of compression.

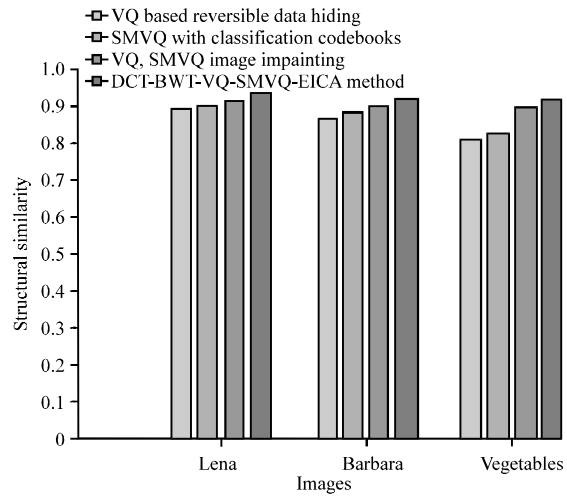

Fig. 9: Comparison result of the structural similarity

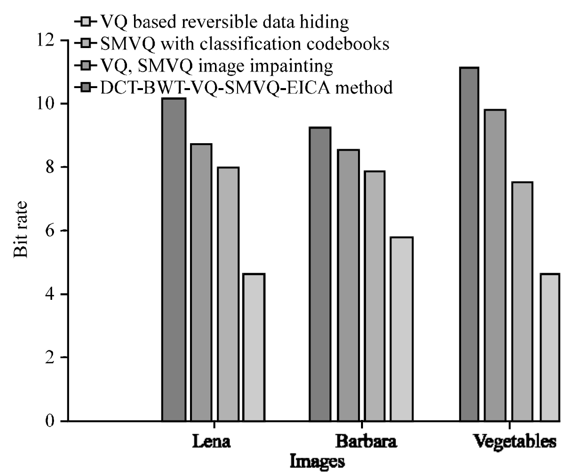

Fig. 10: Comparison result of the bit rate (kb/sec)

Bit rate: Bit rate as the name implies, describes the rate at which bits are transferred from one location to another. In other words, it measures how much data is transmitted in a given amount of time. Bit rate is commonly measured in bits per second, kilobits per second or megabits per second.

Figure 10 shows the comparison of all the four methods in terms of bit rate with respective to three images. This shows that the proposed DCT-BWT-VQ-SMVQ-EICA is the better technique in terms of bit rate.

Embedding capacity: Embedding capacity is defined as the capacity or the number of secret bits that can be embedded inside the blocks of the cover image. The embedding capacity should be greater for an efficient embedding scheme.

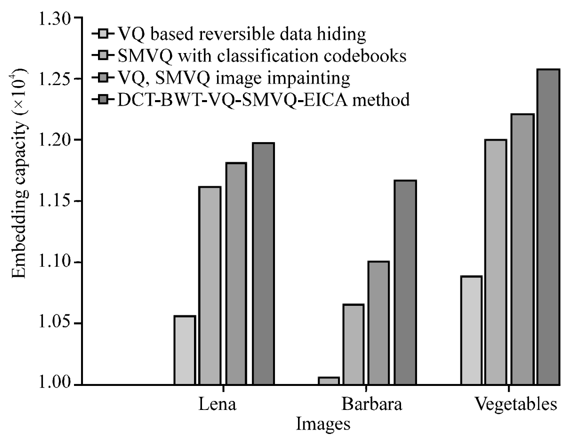

Fig. 11: Comparison result of the embedding capacity

Figure 11 shows the comparison of all the four methods in terms of embedding capacity with respect to three images. This shows that the proposed DCT-BWT-VQ-SMVQ-EICA method is the better technique in terms of embedding capacity.

The graphs were presented in the above study which consist of parameter values comparison such as PSNR, error rate, compression ratio, structural similarity, bit rate and embedding capacity.

Comparison of the experimental results were done in terms of images and as well as using parameters. The proposed DCT-BWT-VQ-SMVQ-EICA method is considered to be the efficient when comparing with all other techniques used.

Comparison of the experimental results were done in terms of images and as well as using parameters. The proposed DCT-BWT-VQ-SMVQ-EICA method is considered to be the efficient when comparing with all other techniques used.

Comparison results for the three images lena, barbara, vegetables shown in Table 1. From Table 1, it is clear that the proposed DCT-BWT-VQ-SMVQ-EICA method is so far efficient than any other existing systems such as VQ based reversible Data hiding, SMVQ with classification codebooks (Lee *et al*., 2010) and VQ, SMVQ image in-painting (Qin *et al*., 2014). The proposed work stands out from the existing techniques in every stage of data hiding compression and extraction phases.

CONCLUSION

Image data hiding is an important technique in ensuring the security of data communication. The major problems in modern data hiding techniques are the image quality degradation after decryption and the lack of proper data visibility. In this study, a lossless reversible data hiding technique is introduced to provide progressed and efficient data hiding in images. The technique uses DCT-BWT-VQ-SMVQ-EICA to retrieve the cover image and improve the data embedding capacity. Also, the ICA technique is used to select an optimal value of threshold to improve the quality of secured data. Thus, the proposed method embeds the secret bits and compresses the image with secret data and gives the output as code streams with preserved size. The experimental results shows that the proposed work is achieved high embedding capacity and compression rate by comparing the work with all existing techniques. Thus, the method solves the problems in data hiding and provides high data security. The experimental results show that the presented technique has better performance also in terms of PSNR value, error rate, structural similarity, bit rate.

REFERENCES

Chao, R.M., H.C. Wu, C.C. Lee and Y.P. Chu, 2009. A novel image data hiding scheme with diamond encoding. EURASIP. J. Inf. Secur.ity, Vol. 2009, 10.1155/2009/658047.

Chiou, S.F. I.E. Liao and M.S. Hwang, 2011. A capacity-enhanced reversible data hiding scheme based on SMVQ. Imaging Sci. J., 59: 17-24.

Goswami, R.G. and S. Tamrakar, 2013. Evolution of data hiding by neural network and retrieval or encrypted image, text, audio and video files. Int. J. Emerging Technol. Adv. Eng., 3: 153-158.

Huang, C.T., W.J. Wang, C.H. Yang and S.J. Wang, 2013. A scheme of reversible information hiding based on SMVQ. Imaging Sci. J., 61: 195-203.

Kumar, S. and N. Garg, 2012. Integrated data hiding and lossless image compression based on SMVQ and image inpainting. Int. J. Sci. Res., 3: 2321-2323.

Lee, C.F., H.L. Chen and S.H. Lai, 2010. An adaptive data hiding scheme with high embedding capacity and visual image quality based on SMVQ prediction through classification codebooks. Image Vision Comput., 28: 1293-1302.

Lin, C.C., X.L. Liu and S.M. Yuan, 2015. Reversible data hiding for VQ-compressed images based on search-order coding and state-codebook mapping. Inf. Sci., 293: 314-326.

Lin, J.L., Y.H. Tsai, C.Y. Yu and M.S. Li, 2012. Interaction enhanced imperialist competitive algorithms. Algorithms, 5: 433-448.

Mahajan, N.M.S.P.P. and D.D. Ahire, 2014. A reserving room approach for reversible data hiding algorithm before encryption on encrypted digital images. Int. J. Innovative Res. Adv. Eng., 1: 372-377.

Ni, Z., Y.Q. Shi, N. Ansari, W. Su and Q. Sun *et al*., 2004. Robust lossless image data hiding. Proceeding of the 2004 IEEE International Conference on Multimedia and Expo, Vol. 3, June 27-30, 2004, IEEE, New Jersey, USA. isBN:0-7803-8603-5, pp: 2199-2202.

Qin, C., C.C. Chang and Y.P. Chiu, 2014. A novel joint data-hiding and compression scheme based on SMVQ and image inpainting. IEEE. Trans. Image Process., 23: 969-978.

Sanyal, N., A. Chatterjee and S. Munshi, 2015. Fuzzy VQ based image compression by bacterial foraging optimization algorithm with varying population. Proceeding of the 3rd International Conference on Computer, Communication, Control and Information Technology (C3IT), February 7-8, 2015, IEEE, New Delhi india isBN:978-1-4799-4445-3, pp: 1-6.

Tyagi, V., 2012. Data hiding in image using least significant bit with cryptography. Int. J. Adv. Res. Comput. Sci. Software Eng., 2: 120-123.

Van, V.S., 2009. Image compression using burrows-wheeler transform. P.hD Thesis, Helsinki University of Technology, Espoo, Finland. http://lib.tkk.fi/Dipl/2009/urn100116.pdf.

Wang, W.J., C.T. Huang and S.J. Wang, 2011. VQ applications in steganographic data hiding upon multimedia images. IEEE. Syst. J., 5: 528-537.

Wang, Z.H., C.C. Chang, K.N. Chen and M.C. Li, 2010. An encoding method for both image compression and data lossless information hiding. J. Syst. Software, 83: 2073-2082.

Wu, M. and B. Liu, 2003. Data hiding in image and video: Part I-fundamental issues and solutions. IEEE Trans. Image Process., 12: 685-695.

Wu, M., H. Yu and B. Liu, 2003. Data hiding in image and video. II. designs and applications. IEEE. Trans. Image Process., 12: 696-705.

Yang, H., X. Sun and G. Sun, 2009. A high-capacity image data hiding scheme using adaptive LSB substitution. Radioengineering, 18: 509-516.

Zhang, W., K. Ma and N. Yu, 2014. Reversibility improved data hiding in encrypted images. Signal Process., 94: 118-127.