# An Enhanced Comparative Techniques for Improving Reversible Data Hidden Images with SMVQ

**Paparao Nalajala**
*Department of Electronics and Communication Engineering, Institute of Aeronautical Engineering, Hyderabad, India, nprece@gmail.com*

**Bhavana Godavarthi**
*Department of Electronics and Communication Engineering, Institute of Aeronautical Engineering, Hyderabad, India, bhavana.bhanu402@gmail.com*

**Dr. M. Sivakoti Reddy**
*Department of Management Studies, Vignan's Foundation for Science, Technology and Research, Guntur, shiva.manukonda@gmail.com*

**Abstract**

Sharing private information has gotten difficult over the last few years as data security has increased. In a number of industries, including the military, the medical profession, networks, and others, exchanging data involves not only concealing signals in multimedia, but also receiving the data without any distortion at the recipient end. In order to protect against intruders, data hiding is thus established, whereby the sender conceals the crucial data into the media. The content owner encrypts an original image using Reversible data hiding in encrypted images (RDHEI), embeds the hidden image using Arnold transform and Side Match Vector Quantization, and transfers it to the recipient. Using the Inverse Arnold Transform and painting, the recipient obtains the cover picture containing the secret image. To obtain the optimum performance, the key goal is to further enhance the PSNR and better data concealing. With this, prediction errors are compared and further improved, and the two metrics PSNR (dB) and compression ratio can be enhanced in comparison to other state-of-the-art systems.

**Keywords:** *Reversible data hiding, side match vector quantization (SMVQ), Arnold transform, Image in painting.*

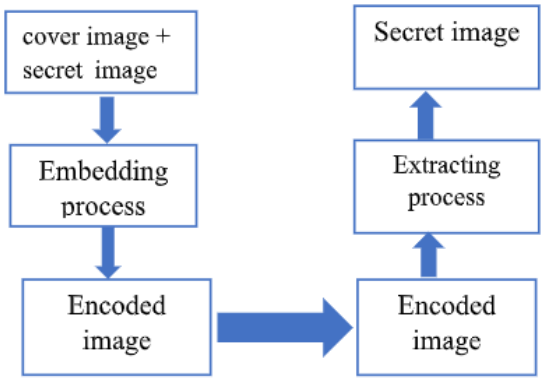
## 1. INTRODUCTION

Regarding security, there are several applications, including military and medical. The primary consideration for both the sender and the receiver is the protection of the information being exchanged. When sending confidential information, the information shouldn't be lost until it reaches the intended recipient. Data concealing is one of the techniques that is most frequently used. This data concealing can be employed in military applications when a secret message or image needs to be sent to the appropriate destination [1]. The secret message which has to be transmitted might be of bits of data or audio or image. In case a secret image is one that needs to be transferred then it can be embedded or encoded in another image which is generally a cover image[2].After embedding the embedded image will be same as the cover image so that during transmission any unauthorized user cannot access the secret information. It almost

preserve the same appearance which is imperceptible [3,4]to any hacker who tries to get the secret information.

In the recent years, many algorithms for embedding the secret data have been proposed. In several data hiding techniques reversible data hiding is one which is mostly suitable for this kind of applications. Using reversible data hiding not only the secret image is hided but also it can extracted successfully at the receiver without any distortions. Many reversible data hiding schemes came into existence over the past years[6].Like the prediction error expansion (PEE),PVO, difference expansion ,histogram shifting and soon. As for the embedded methods there are different methods such as time domain, spatial domain, transform domain method. If it is done in transform method then some image scrambling needs to be performed such that in pixel position or values arranged randomly so the image will be visually unreadable. Before transmitting any image or information in order to store it should be compressed before sending. Now as for the compression there different methods such as lossy and lossless. If lossy compressing is decided to use then JPEG [20], JPEG 2000,vector quantization[7] can be used. As for the lossless compression Huffman coding, arithmetic coding, etc can be used.

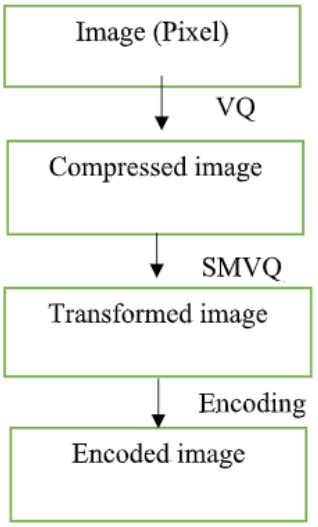
**Fig.1 Process of data hiding**




## 2. Existing methods

In many algorithms the image after embedding the image compression is done doing so causes loss of data occurs. So compression before embedding the secret data can more secure the only limitation is that there will be introduce of noise. VQ(vector quantization) is a common lossy compression technique that is frequently used for digital image compression due to its ease of implementation. In VQ after diving the image into blocks the Euclidian distance is utilized [8].But by using VQ the boundary of block after compression is visible so the improved version of VQ which is SMVQ(side match vector quantization) is developed.

**Fig.2 Flowchart for Image encoding**

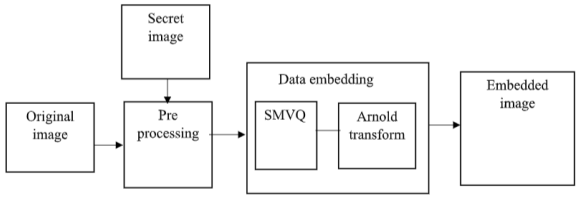



The image is first separated into blocks in the prediction error and block selection [9], after which each block is forecasted using block modulation, and the prediction values are then obtained. The blocks are separated into usable and non-usable blocks using block modulation. Using Huffman coding [10], the prediction errors in the useable blocks are compressed. And the ineffective blocks are not included. It makes space for the data to be incorporated after encoding so that the data can benefit from the auxiliary information and be included in the encoded image.

Considering these methods ,the side match vector quantization (SMVQ) is well known for the compression before encoding and as for the embedding algorithm to be in transfer domain we will be using the Arnold transform which arbitrary the pixel position instead of using two modules separately for different schemes we will be combining these methods as a single module so that the original image is first compressed using the SMVQ technique and then using the Arnold transform determining the pixel position the secret image will be embedded into the original image. And same SMVQ technique is used to recover the image at the receiver followed by inverse Arnold transform.

## 3. Proposed method

The first part of the suggested procedure, data embedding, is carried out at the sender's end. The second step is data extraction, which is carried out at the receiver's end to obtain the hidden message or image. The original image is first compressed using the SMVQ approach on the sender's end, and then the secret image is inserted into the original image using the Arnold transform, yielding the embedded encrypted image. The original image is successfully retrieved at this point from the receiver side utilising the secret image's extraction using the Inverse Arnold transform. Here is a block diagram that is suggested for the sender and recipient sides.




### 3.1 Pre processing

To prepare the images for further processing, pre processing is carried out. It requires a number of actions, including picture conversion and scaling. Think about an original image that is size MXM and a hidden image that is size NXN. The secret image's proportions shouldn't be different from the original image's. Consider creating m blocks with a block size of m from the image.

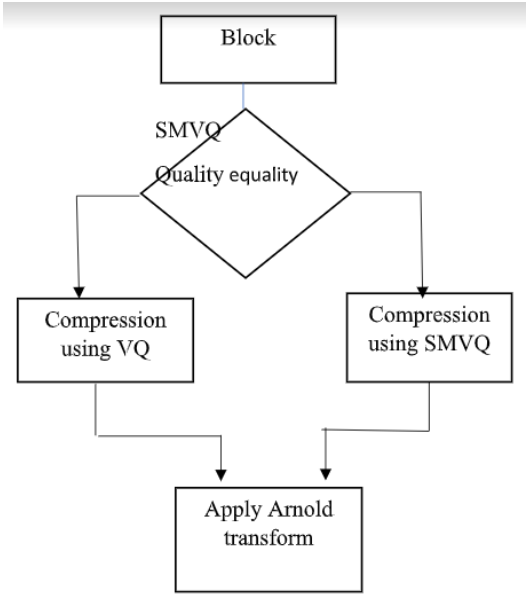
### 3.2 Data embedding phase

In the data embedding phase, the secret picture is first embedded into the original image using side match vector quantization and Arnold transform after the original image, which is separated into m blocks, has first been compressed.

#### 3.2.1Side match vector quantization (SMVQ)

A codebook is need to be generated to encode the blocks. With the same of the original image blocks a codebook is generated which consist of indexed image blocks. Instead of transferring the actual image the cookbook is sent and the closest match block index is transmitted.

**Fig.4 Flowchart of SMVQ compression**

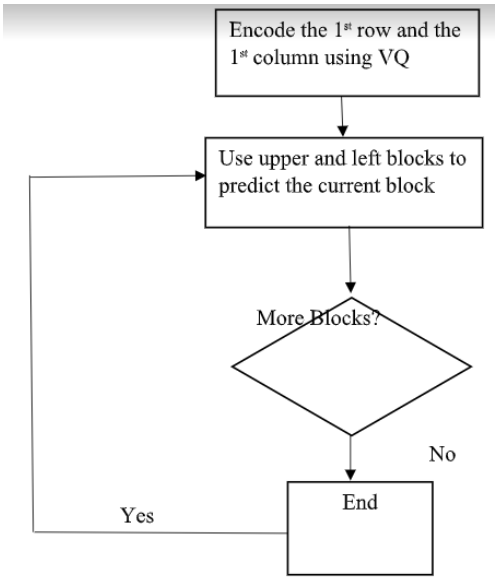



The first row and column of blocks must be encoded with a major codebook, while the remaining blocks must be encoded with a sub codebook. There is a significant association between the right column in the left block and the top row in the upper block as well as the

first column in the current block. Figure 4 depicts the SMVQ compression flowchart. The previously encoded upper and left blocks are utilised in the sub codebook generation process to create the sub code book for the present block.

The sub code book is picked from the main codebook with the least side-match distortion, and it has N code words in contrast to the grey areas. The VQ compress method and a size N sub code book are used to encrypt the current block. Each block of the original image is subjected to this process until all of the blocks have been encoded. The sub code book is significantly smaller than the main code book because only the code words in the sub code book must be searched rather than all of the code words in the main code book.

**Fig.5 Flowchart of SMVQ**




3.2.2 Arnold transform

As the digital image is in two dimensional matrix form and if the size of the image is N then there will be NXN number of elements. Where the sub script x,y gives the position of the pixel. For each value of the pair (x,y) after Arnold scrambling it becomes(x',y'). Like wise it travels all the points or pixels of the image. Based on the periodicity of the Arnold scrambling the image can be retrieved.

[]=[]mod N

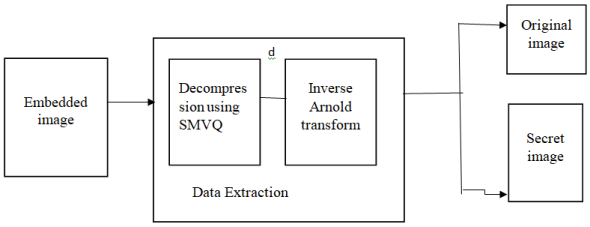
Where N is the order of the digital image matrix for values of x,y∈ {0,1,2,3⋯.,N-1}.

The secret message is first jumbled using transform at various levels during the embedding process to make it more resistant to unauthorised extraction. The embedded image is created by embedding this jumbled message into the cover image. The embedded image is then transferred, and the concealed secret message is recovered at the receiving end by continuing the extraction and decryption process in reverse order. The values are kept secret and only known by authorised users during this approach, and extraction without the keys results in sounds, making the procedure secure. Image in painting can also be used to restore the missing data.

3.3 Data extraction phase

In this phase, the original image and the secret image is separated which is done at the receiver side. The extraction of secret image from original image involves reverse process which is applied at the data embedding phase. The embedded image is divided into m blocks and then it is decompressed and secret image is retrieved using SMVQ and inverse Arnold transform. The below shown is the block diagram of proposed method at the receiver side.Fig.7 shows how an embedded image is decompressed and the secret image extraction and the recovery of original image which is basically need to be done at the receiver.

**Fig.6 Data extraction at receiver side**




3.3.1 Inverse Arnold Transform

The hidden image is retrieved using the inverse Arnold transform once the embedded image has been decompressed. The decompressed image is transformed using the inverse Arnold transform.

[]=[]mod N

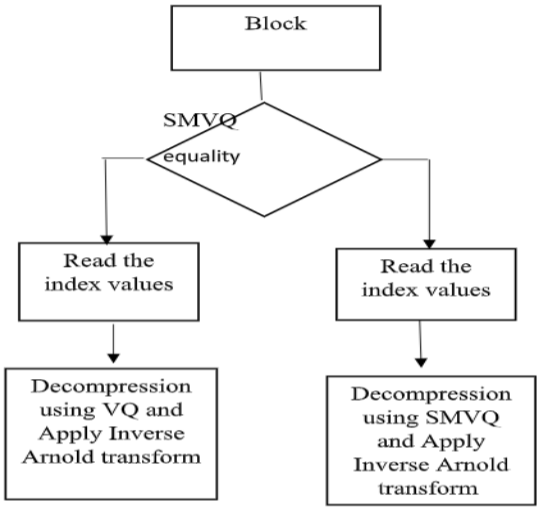
Where the pixels position changes from transformed position to its original position i.e (x',y') changes to (x,y) . N is the order of the image matrix.

$$\begin{bmatrix} X' \\ Y' \end{bmatrix} = \begin{bmatrix} 2 & -1 \\ -1 & -2 \end{bmatrix} \begin{matrix} X \\ Y \end{matrix} \; mod\ N \qquad \text{----------(2)}$$

3.3.2 Decompression using SMVQ

The data extraction step at the receiver will use the same procedure used to compress the image during the embedding phase using SMVQ.

**Fig.7 SMVQ Flow chart for decompression**




## 4. Results and Analysis

To Evaluate the performance of our proposed scheme experiments are conducted on different standard grey level images. The four test images are taken from different schemes for analysing the performance of the proposed methodology. The statistical parameter metrics are calculated for different images. The PSNR(peak signal to noise ratio) ,Compression ratio, Mean square error(MSE) are obtained by using the suggested method. The visual quality difference between the secret image and the decrypted image is estimated by PSNR. Equations listed below are used to determine PSNR.

$$MSE = \frac{1}{MXN} \sum_{i=1}^{M} \sum_{j=1}^{N} (Oi,j - Si,j)^2 \qquad \text{----------(3)}$$

Where Oi, jis the Original image pixel values andSi, jis the Recovered image pixel values

PSNR = 10 log10 $(255)^2$ (db)

MSE ----------(4)

Compression ratio = 8XMXN

Lb ----------(5)

Where M,N are length and width of the images ,Lb is the length of the compressed or code book.

4.1 Output images of embedding and extraction of different images

**Fig.8 (a) original image (b) secret image (c ) Embedded image (d) Recovered original image (e)Extracted secret image**


a b

c d


e

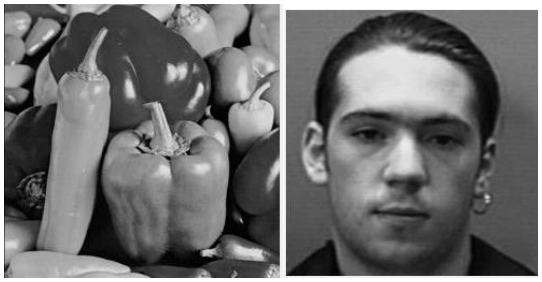
**Fig.9 (a) original image (b) secret image (c ) Embedded image (d) Recovered original image (e)Extracted secret image**

a b

c d

e

**Fig.10 (a) original image (b) secret image (c ) Embedded image (d) Recovered original image (e)Extracted secret image**



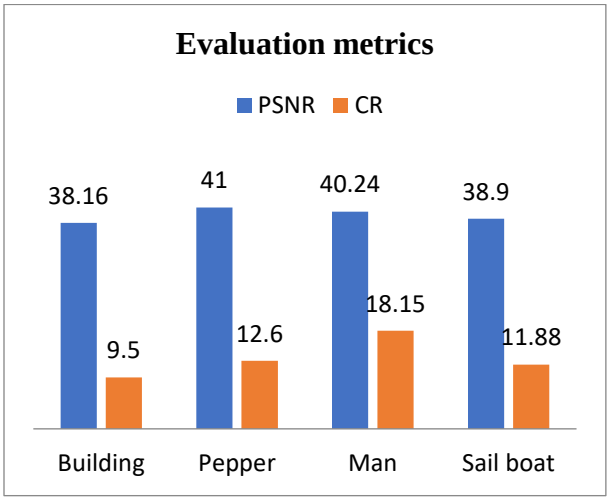
a b

c d

e

## 5. Evaluation Metrics

**Figure.11. Evaluation metrics**




As shown the above figure 11 has evaluation metrics for PSNR and CR values

## 6. Conclusion

The recommended way to enhance reversible data concealing in photos embeds the original image inside a hidden image utilising a compression methodology. With the exception of the blocks at the top and bottom of the image, all of the blocks can be modified using SMVQ and Arnold. Also, the blocks are capable of being correctly compressed and secret data implanted. The encoded secret bits are simply recovered from the compressed codes on the decoding side in accordance with the index values in the segmented sections, and the decoding for all blocks can also be effectively accomplished by VQ, SMVQ, and Arnold transform. The test results demonstrate that our system has acceptable decompression quality and compression relationship capabilities. Additionally, the suggested technique can reliably combine the two tasks of data hiding and image compression into a single module.

## References

Z.Ni,Y.-Q. Shi, N. Ansari, and W. Su, "Reversible datahiding," IEEE Transactions on Circuits and Systems for VideoTechnology, vol. 16, no. 3, pp. 354–362, 2006.

P. Tsai, Y.-C. Hu, and H.-L. Yeh, "Reversible image hiding scheme using predictive coding and histogram shifting," Signal Processing, vol. 89, no. 6, pp. 1129–1143, 2009.

X. Li, J. Li, B. Li, and B. Yang, "High-fidelity reversible data hiding scheme based on pixel-value-ordering and prediction error expansion," Signal Processing, vol. 93, no. 1, pp. 198–205, 2013

X.Zhang, "Reversible data hiding in encrypted image," IEEE Signal Processing Letters, vol. 18, no. 4, pp. 255–258, 2011.

W.Hong, T.-S. Chen, and H.-Y. Wu, "An improved reversible data hiding in encrypted images using side match," IEEE Signal Processing Letters, vol. 19, no. 4, pp. 199–202, 2012

X.Wang, C.-C. Chang, and C.-C. Lin, "Reversible data hidingin encrypted images with block-based adaptive MSBencoding," Information Sciences, vol. 567, pp. 375–394, 2021.

K.-M.Chen, "High capacity reversible data hiding based onthe compression of pixel differences," Mathematics, vol. 8,no. 9, p. 1435, 2020.

A Novel Joint Data-Hiding and Compression Scheme Based on SMVQ and Image Inpainting", Chuan Qin; Chin-Chen Chang; Yi-Ping Chiu, IEEE Transactions on Image Processing ( Volume: 23, Issue: 3, March 2014).

X. Wu and W. Sun, "High-capacity reversible data hiding in encrypted images by prediction error," Signal Processing, vol.

104, pp. 387–400, 2014.

Xu Wang, Li-Yao Li, Ching-Chun Chang, Chih-Cheng Chen, "High-Capacity Reversible Data Hiding in Encrypted Images Based on Prediction Error Compression and Block Selection", Security and Communication Networks, vol. 2021, Article ID 9606116, 12 pages, 2021.

Zhenfei Zhaoa,b, Hao Luoc, Zhe-Ming Luc, Jeng-Shyang Pan, "Reversible data hiding based on multilevel histogram medication and sequential recovery", International Journal on Electronic and communication, Z. Zhao et al. / Int. J. Electron. Commun.(AEÜ) 65 (2011) 814–826

C. Vinoth Kumar, V. Nataranjan and Deepika Bhogadi, "High capacity Reversible Data hiding based on histogram shifting for medical image", International Conference on Communication and Signal Processing, April 3-5 2013, India © IEEE 2013

Che-Lun Pan, Wien Hong, Tung-Shou Chen, Jeanne Chen and Chih-Wei Shiu, "Multilevel Reversible Data Hiding using Modification of Prediction Errors", ICIC Vol 7,No. 9, Sept 2011

Xiaolong Li, Bin Yang and Tieyong Zeng, "Efficient Reversible Watermarking Based on Adaptive Prediction-Error Expansion and Pixel Selection", IEEE Transaction on Image Processing, Vol, 20, No. 12, Dec 2011

Kuo-Ming Hung, Wen-Kai Su, Ting-Wen Chen, Li-Ming Chen, " Reversible Data Hiding Base on VQ and Halftoning Technique", International Conference on Microelectronics, Communication and Renewable Energy (ICMiCR-2013).

V Yu, Song Wei, "Study on Reversible Data Hiding Scheme for Digital Images", 2 nd International Asia Conference on Informatics in Control, Automation and Robotics,(CAR) 2012

Wei Qiao, Hongdong Huaqing Liang, "A kind of Visual Cryptography Scheme For color Images based on halftone technique", International Conference on Measuring Technology and Mechatronics automation © 2009 IEEE

Yi-Hui Chen, Ci-Wei lan and Chiao Chih Huang, " A verifiable Visual Cryptography Scheme", Fifth International Conference and Evolutionary Computing © IEEE 2011.

Rintu Jose, Gincy Abraham, "A Separable Reversible Data Hiding in Encrypted Image with Improved Performance", International Conference on Microelectronics, Communication and Renewable Energy, ICMiCR-2013

Bhavana Godavarthi, Anandbabu Gopatoti, Merajothu Chandra Naik, Paparao Nalajala," Image Processing For Sdr Applications To Recreate Lost Image Pixels/Packets", Journal of Fundamental and Applied Science, Vol. 10, Issue 6s, Pages 2826-2838

Bhavana Godavarthi, Paparao Nalajala, K Chiranjeevi, P Madhuri,"Implementation of RGB Based Face Detection Using Threshold Values and Morphological Processing", Journal of Engineering and Applied Sciences, Vol 12, Issue 12SI, PP. 9520-9527, 2017.