A Reversible Data Hiding Technique Using Histogram Modification and SMVQ for Very Large Payloads

S. Arockiaraj, S. Sundara Mahalingam, B.V. Manikandan and V.P. Gowtham Kumar

Abstract--- Reversible data hiding (RDH) is the process of embedding secret information into a cover image. The prime essence of the concept is that, the recovered secret information as well as the cover image should be recovered without any damage or with imperceptible error in the pixel values. In this paper, we propose an RDH technique based on simple histogram modification and SMVQ. The proposed histogram modification technique attains high PSNR values with impressive payload capacities. The SMVQ technique further increases the payload capacity by four folds. The damage in the extracted secret message is imperceptible and the recovered cover image is either exactly same or has a very high PSNR value. The algorithm has been well tested and compared with various other techniques.

Keywords--- RDH, PSNR, SMVQ, PAYLOADS.

I. INTRODUCTION

In computer vision, data hiding is the rule of isolation of the configuration choices in a PC program that are destined to change, in this manner shielding different parts of the project from broad alteration if the outline choice is changed. The insurance includes giving a steady interface which shields the rest of the project from the execution (the points of interest that are well on the way to change). Composed another way, data hiding is the capacity to keep certain parts of a class or programming segment from being open to its customers, utilizing either programming dialect highlights (like private variables) or an unequivocal sending out approach. The term encapsulation is regularly utilized conversely with data hiding. Not all concede to the refinements between the two however; one may consider data hiding away similar to the standard and embodiment being the strategy. A product module conceals data by embodying the data into a module or other develop which shows an interface.

A typical utilization of data concealing is to shroud the physical storage design for information so that on the off chance that it is changed, the change is limited to a little subset of the aggregate project. For instance, if a three-dimensional point (x,y,z) is spoken to in a project with three coasting point scalar variables and later, the representation is changed to a solitary cluster variable of size three, a module planned in view of data stowing away would shield the rest of the system from such a change. In OOP (object oriented programming), data hiding (by method for settling of sorts) lessens programming improvement hazard by moving the code's reliance on an unverifiable usage (plan choice) onto a very much characterized interface. Customers of the interface perform operations absolutely through it so if the usage changes, the customers don't need to change.

Information hiding is a procedure that subtly implants the mystery message in spread media, for example, pictures, recordings, sounds or messages. The spread medium is somewhat adjusted subsequent to inserting and is alluded to as the stego medium. An objective of information concealing is to guarantee that nobody can recognize a spread medium and a stego medium. At that point the stego medium can be distributed or transmitted. Whenever, the mystery message can be separated if necessary. On the other hand, in a few applications, for example, military pictures or therapeutic pictures, metadata will be inserted in the picture and any contortion made by information covering up is not worthy. In light of this issue, much writing about reversible (lossless) information stowing away has been published.1–16 Reversible information stowing away is a system that indistinctly implants the mystery message in spread media and the first cover media can be recuperated in the wake of separating the concealed mystery message from the stego media.

II. LITERATURE

Data compression: Fridrich [1],[2] compacted the slightest critical piece plane to empty space for inserting the mystery message. Be that as it may, the inserting limit is not vast because of the low proficient pressure on the minimum critical piece plane. Celik [3] presented a high-limit and low-mutilation reversible watermarking calculation in 2003. The pixels of the first picture are quantised and the buildups are packed utilizing a lossless picture pressure calculation keeping in mind the end goal to make limit for the payload information.

Difference expansion: Tian [4] proposed a distinction development strategy that inserts the mystery message by extending the contrast between two nearby pixels. Alattar [5] proposed an enhanced variant of Tian's system to improve the installing limit and the picture quality. Alattar utilized a summed up distinction extension technique to conceal a few bits in the distinction development of vectors of adjoining pixels. Later, more contrast develoment
based reversible information concealing methods [7]–[11] are proposed.

Revised Version Manuscript Received on 22 February, 2019

S. Arockiaraj, Mepco Schlenk Engineering College, Sivakasi.Tamil Nadu. India (e-mail:arockiarocks@gmail.com)

S. Sundara Mahalingam, Mepco Schlenk Engineering College, Sivakasi. Tamil Nadu, India.

B.V. Manikandan, Mepco Schlenk Engineering College, Sivakasi.

V.P. Gowtham Kumar, Mepco Schlenk Engineering College, Sivakasi. Tamil Nadu, India.

Histogram moving: Ni et al. [6] proposed a histogram-based strategy that moves the histogram of a picture to empty space for inserting the mystery message. The top point is characterized as the canister of greatest number of pixels in a histogram. The zero point is characterized as the canister of zero number of pixels in a histogram. At that point the pixels between the crest point and the zero point are moved and a vacant canister alongside the crest point container is created. The top point container and the unfilled canister are utilized to insert the mystery bits 0 and 1, separately. The implanting limit of the strategy measures up to the most extreme number of pixels in a histogram. Some reversible information concealing techniques in light of histogram moving had been proposed along these lines. Fallahpour and Sedaaghi [12] enhanced Ni et al's. work and infer better execution. Lin and Hsueh [13] implanted the data into a spread picture utilizing the two contrasts as a part of a 3pixel piece. Lin [14] utilized a multilevel concealing methodology to accomplish extensive concealing limit and keep contortion low. Tsai [15] connected prescient coding and histogram moving particularly for restorative pictures. Tai [16] misused a parallel tree structure to convey various crest point sets and the pixel contrasts are utilized to accomplish expansive concealing limit.

III. PROPOSED METHOD

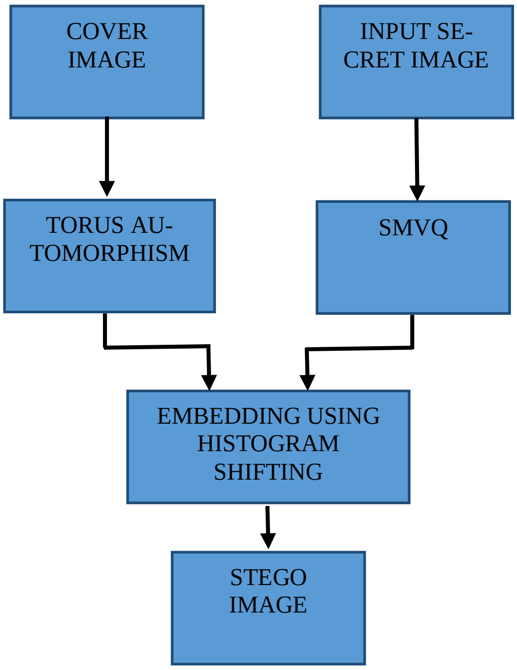


Figure 1: The proposed RDH embedding block diagram.

The novel algorithm proposed in this paper is as follows. First the input secret image is compressed using SMVQ. Then the using bit decomposition the binary form of the message is obtained. Then torus automorphism selects the pixel locations to be embedded. The binary secret data is embedded using histogram modification, thus producing the stego image. The detailed explanation is given in the following sections.

IV. TORUS AUTOMORPHISM

In geometry, a torus (plural tori) is a surface of transformation created by spinning a circle in three-dimensional space around a hub coplanar with the circle. On the off chance that the hub of upset does not touch the circle, the surface has a ring shape and is known as a torus of transformation.

In topology, a ring torus is homeomorphic to the Cartesian result of two circles: S1 × S1, and the last is taken to be the definition in that connection. It is a reduced 2-complex of sort 1. The ring torus is one approach to install this space into three-dimensional Euclidean space, yet another approach to do this is the Cartesian result of the implanting of S1 in the plane. This produces a geometric article called the Clifford torus, a surface in 4-space.

The homeomorphism bunch (or the subgroup of diffeomorphisms) of the torus is examined in geometric topology. Its mapping class amass (the gathering of associated segments) is isomorphic to the gathering GL(n, Z) of invertible whole number frameworks, and can be acknowledged as straight maps on the all-inclusive covering space Rn that save the standard grid Zn (this relates to whole number coefficients) and along these lines drop to the remainder.

At the level of homotopy and homology, the mapping class gathering can be distinguished as the activity on the first homology (or proportionately, first cohomology, or on the basic gathering, as these are all normally isomorphic; additionally the first cohomology bunch produces the cohomology polynomial math):

As the torus is an Eilenberg–MacLane interplanetary K(G, 1), its homotopy correspondences, up to homotopy, can be related to automorphisms of the key gathering); this concurs with the mapping class bunch mirrors that all homotopy equivalences can be acknowledged by homeomorphisms – each homotopy proportionality is homotopic to a homeomorphism – and that homotopic homeomorphisms are truth be told isotopic (associated through homeomorphisms, not simply through homotopy equivalences). All the more concisely, the guide Homeo(Tn) → SHE(Tn) is 1-joined (isomorphic on way segments, onto major gathering). This is a "homeomorphism lessens to homotopy decreases to variable based math"

V. VECTOR QUANTIZATION

Vector quantization depends on the aggressive learning worldview, so it is firmly identified with the self-arranging map model and to inadequate coding models utilized as a part of profound learning calculations.

Side Match Vector Quantization

As an augmentation of VQ, SMVQ was produced to ease the square antique of the decompressed picture and build the pressure proportion, in light of the fact that the relationship of neighboring pieces is considered and the files of the subcodebooks are put away. In our plan, the standard calculation of SMVQ is altered to advance accomplish better decompression quality and to make it suitable for installing mystery bits. The itemized methodology is depicted as takes after.

Published By:
Blue Eyes Intelligence Engineering
& Sciences Publication

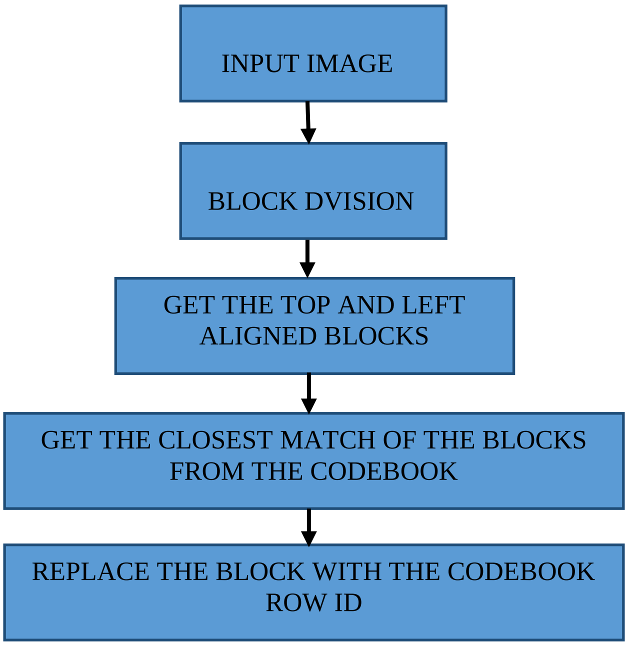


Figure 2: The proposed Vector Quantization Algorithm

In our plan, the sender and the beneficiary both have the same codebook with W code words, and each codeword length is n2. Mean the first uncompressed picture measured M × N as I, and it is separated into the non-covering n × n pieces. For effortlessness, we accept that M and N can be partitioned by n with no leftover portion. Indicate all k separated pieces in raster scanning request as Bi,j , where k = M × N/n2, i = 1, 2,..., M/n, and j = 1,2,..., N/n. Before being implanted, the mystery bits are mixed by a mystery key to guarantee security. The pieces in the furthest left and highest of the picture I, i.e., Bi,1(i = 1,2,..., M/n) and B1,j(j = 2,3,..., N/n), are encoded by VQ specifically and are not used to implant mystery bits. The leftover squares are encoded dynamically in raster scanning request, and their encoded strategies are identified with the mystery bits for implanting and the relationship between's their neighboring piece.

Histogram Modification

In our proposed method, the histogram is modified according to the data bit that is to be embedded. The torus automorphism decides the pixel bit to be embedded. We tested two different ways of data hiding techniques using histogram modification.

Pre processing stage

Change the image pixel values in the following manner:

- The even positioned pixel should have even value.
- The even positioned pixel should have even value.

The resultant images are visually intact and the change is imperceptible. The PSNR values and the output images are displayed in figure 5 and table 2.

Embedding stage

The embedding stage is as follows.

- If the data bit is 1, the pixel value is altered by 1.
- If the data bit to be embedded is 0, the pixel value remains intact.

Experimental Analysis

The following images have been taken from MATLAB image processing tool box.

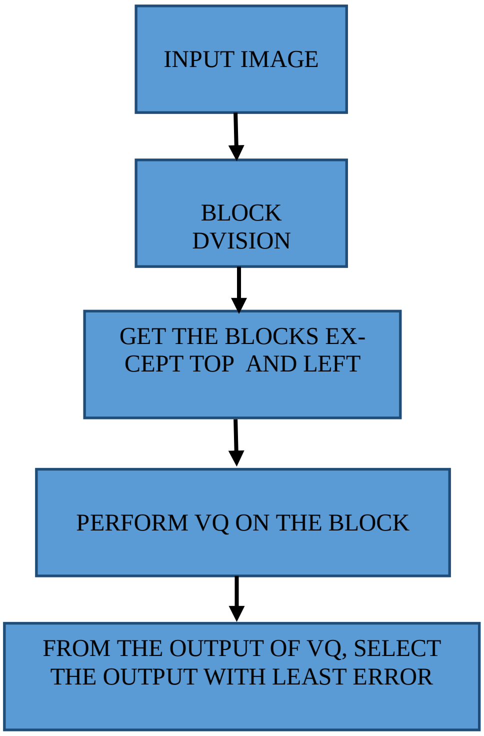
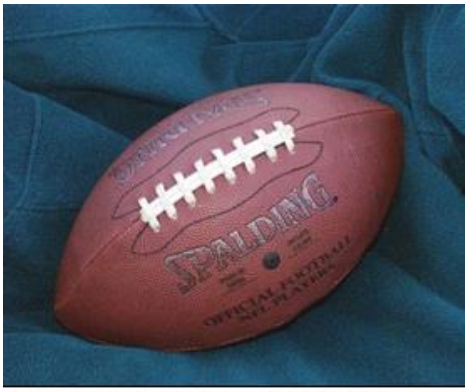


Figure 3: Vector Quantization with least error

(a). tape.png (512 X 384)

(b). Peppers.png (512 X 384)

Published By:
Blue Eyes Intelligence Engineering
& Sciences Publication



(c). football.jpg (320 X 256)

(d). fabric.png (640 X 480)

(f). greens.jpg (500 X 300)

(g). gantrycrane.png (400 X 264)

(h). concordaerial.png (3060 X 2036)

Figure 4: The figures (a) – (h) are the input cover images used to test the proposed algorithm

Table 1: Payload in Procedure 1

S. No	Image name	Payload (bits)
1.	tape.png	5,89,824
2.	Peppers	5,89,824
3.	Football	2,45,760
4.	Fabric	9,21,600
5.	greens	4,50,000
6.	gantrycrane	3,16,800
7.	concordaerial	1,86,90,480

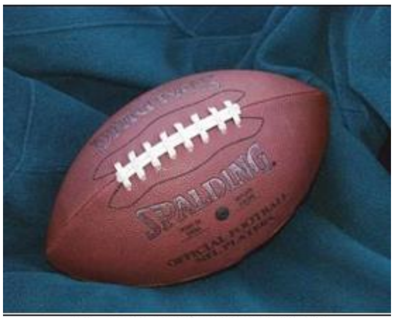
Table 2: Pre-processed Images

S. No	Image name	PSNR
1.	tape.png	51.1832
2.	Peppers	51.2765
3.	Football	51.1943
4.	Fabric	51.2342
5.	greens	51.1730
6.	gantrycrane	51.1896
7.	concordaerial	51.1802

SMVQ based compression – the original image “pears.png” was resized to 256 x 256 x 3 and given as an input to SMVQ. The resultant image was of size 64 x 64 x 3. The no of bits to be embedded was 98304, which can be accommodated by an image of size 128 x 256 x 3.

(a). tape

(b). Peppers



(c). football.jpg (320 X 256)

Published By:
Blue Eyes Intelligence Engineering
& Sciences Publication

(f). greens.jpg (500 X 300)

(g). gantrycrane.png (400 X 264)

(h). concordaerial.png (3060 X 2036)

Figure 5: The above figures (a) – (h) are the output of pre processing stage

Figure 6. Input secret image for data hiding

Figure 6: Input secret image for data hinding

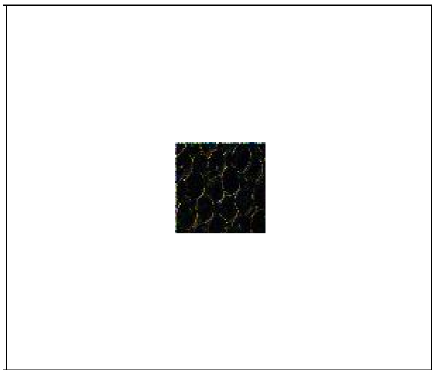


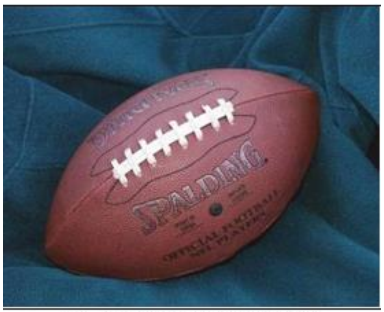
Figure 7. SMVQ output

Figure 7: SMVQ output

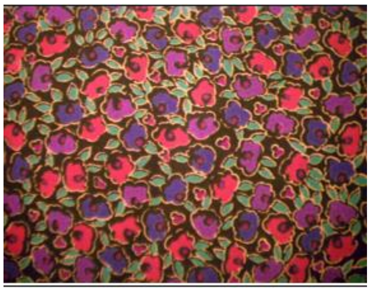
The output of SMVQ is embedded into the cover images shown in figure __. The resulting images are shown below.

(a). tape

(b). Peppers



(c). football.jpg (320 X 256)



(d). fabric.png (640 X 480)

(f). greens.jpg (500 X 300)

Published By:
Blue Eyes Intelligence Engineering
& Sciences Publication

(g). gantrycrane.png (400 X 264)

(h). concordaerial.png (3060 X 2036)

Figure 8: The figures (a)-(h) represent the output stego image with secret data hiding

Table 3: PSNR values of proposed ststem steg images

S. No	Image name	PSNR
1.	tape.png	57.5025
2.	Peppers	57.5025
3.	Football	53.7003
4.	Fabric	59.4409
5.	greens	56.3564
6.	gantrycrane	54.8476
7.	concordaerial	72.5114

The extracted secret image and the recovered cover images are shown below.

Figure 8. Extracted secret image (256x256)

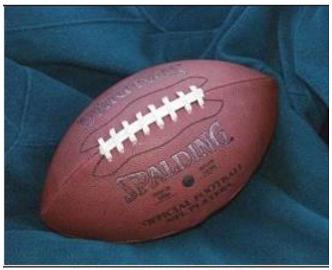
Figure 8: Extracted secret image

Figure9. Extracted secret image (1024x1024)

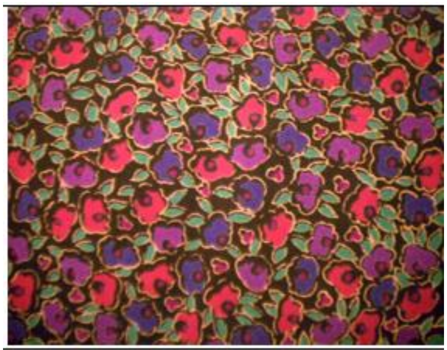
Figure 9: Extracted secret image (1024x1024)

(a). tape

(b). Peppers



(c). football.jpg (320 X 256)



(d). fabric.png (640 X 480)

(f). greens.jpg (500 X 300)

(g). gantrycrane.png (400 X 264)

(h). concordaerial.png (3060 X 2036)

Figure 10: Recovered cover images

Table 4: PSNR values of recovered cover images

S. No	Image name	PSNR (w.r.t original Image)	PSNR (w.r.t processed Image)
1.	tape.png	51.1832	inf
2.	Peppers	51.2765	inf
3.	Football	51.1943	inf
4.	Fabric	51.2342	inf
5.	greens	51.1730	inf
6.	gantrycrane	51.1896	inf
7.	concordaerial	51.1802	inf

VI. CONCLUSION

In this research, we proposed an RDH technique based on simple histogram modification and SMVQ for larger payloads. The proposed histogram modification technique attains high PSNR values with impressive payload capacities. The SMVQ technique further increases the payload capacity by four folds. The damage in the extracted secret message is imperceptible and the recovered cover image is either exactly same or has a very high PSNR value.

REFERENCES

1. Chuan Qin, Chin-Chen Chang, Yi-Ping Chiu, “A Novel Joint Data-Hiding and Compression Scheme Based on SMVQ and Image Inpainting”, IEEE Transactions Image Processing,Vol. 23, Issue 3, pp. 969 – 978, Jan 2014.
2. Z. Ni, Y. Q. Shi, N. Ansari, and W. Su, “Reversible data hiding,” IEEE Trans. Circuits Syst. Video Technol., vol. 16, no. 3, pp. 354 – 362, Mar. 2006.
3. Fridrich, J., Goljan, M. and Du, R. Lossless data embedding — new paradigm in digital watermarking. EURASIP J. Appl. Signal Process., 2002, 2002, 185–196.
4. Fridrich, J., Goljan, M. and Du, R. Lossless data embedding for all image formats. Proc. SPIE, 4675, 572–583.
5. Celik, M. U., Sharma, G., Tekalp, A. M. and Saber, E. Reversible data hiding, Proc. IEEE Int. Conf. on Image processing: ICIP 2002, Rochester, NY, USA, September 2002, IEEE, Vol. II, pp. 157–160.
6. Tian, J. Reversible data embedding using a difference expansion. IEEE Trans. Circuits Syst. Video Technol., 2003, 13, 890–896.
7. Alattar, A. M. Reversible watermark using the difference expansion of a generalized integer transform. IEEE Trans. Image Process., 2004, 13, 1147–1156.
8. Ni, Z., Shi, Y. Q., Ansari, N. and Su, W. Reversible data hiding. IEEE Trans. Circuits Syst. Video Technol., 2006, 16, 354–362.
9. Chang, C. C. and Lu, T. C. A difference expansion oriented data hiding scheme for restoring the original host images. J. Syst. Software, 2006, 79, 1754–1766.
10. Weng, S., Zhao, Y. and Pan, J. S. A novel reversible data hiding scheme. Int. J. Innov. Comput. Inf. Control, 2008, 4, 351–358.
11. Tseng, H. W. and Chang, C. C. An extended difference expansion algorithm for reversible watermarking. Image Vision Comput., 2008, 26, 1148–1153.
12. Thodi, D. M. and Rodriquez, J. J. Expansion embedding techniques for reversible watermarking. IEEE Trans. Image Process., 2007, 16, 721–730.
13. Tseng, H. W. and Hsieh, C. P. Prediction-based reversible data hiding. Inf. Sci, 2009, 179, 2460–2469.
14. Fallahpour, M. and Sedaaghi, M. H. High capacity lossless data hiding based on histogram modification. IEICE Electron. Express, 2007, 4, 205–210.
15. Lin, C. C. and Hsueh, N. L. A lossless data hiding scheme based on three-pixel block differences. Patt. Recogn., 2008, 41, 1415–1425.
16. Lin, C. C., Tai, W. L. and Chang, C. C. Multilevel reversible data hiding based on histogram modification of difference images. Patt. Recogn., 2008, 41, 3582– 3591.
17. Tsai, P., Hu, Y. C. and Yeh, H. L. Reversible image hiding scheme using predictive coding and histogram shifting. Signal Process., 2009, 89, 1129–1143.
18. Tai, W. L., Yeh, C. M. and Chang, C. C. Reversible data hiding based on histogram modification of pixel differences. IEEE Trans. Circuits Syst. Video Technol., 2009, 19, 906–910.

Published By:
Blue Eyes Intelligence Engineering
& Sciences Publication