International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 10 Issue: 9
DOI: https://doi.org/10.17762/ijritcc.v10i9.5709
***Article Received**: 02 July 2022 **Revised**: 09 August 2022 **Accepted**: 18 August 2022 **Publication**: 30 September 2022*

A High Secured Steganalysis Using QVDHC Model

[A]Praveena Akki
School of Computing, SRM Institute of Science and Technology, Kattankulathur, Chennai, 603203, Tamil Nādu, India
Email: praveena2@srmist.edu.in

[b]Dr. Gitanjali J
Dept of Information Technology and Engineering
Vellore Institute of Technology, Tamil Nādu, India
Email: Gitanjalij@vit.ac.in

[c]Dr. Celestine Iwendi
School of Creative Technology, University of Bolton, UK
c.iwendi@bolton.ac.uk

[d]Dr. Sumathy. S
School of Information Technology & Engineering
Vellore Institute of Technology, Tamil Nādu, India
ssumathy@vit.ac.in

[E]Amtul Waheed
Department of Computer Science,
Prince Sattam bin Abdul Aziz University, Saudi Arabia
w.amtul@gmail.com

Abstract— Data compression plays a vital role in data security as it saves memory, transfer speed is high, easy to handle and secure. Mainly the compression techniques are categorized into two types. They are lossless, lossy data compression. The data format will be an audio, image, text or video. The main objective is to save memory of using these techniques is to save memory and to preserve data confidentiality, integrity. In this paper, a hybrid approach was proposed which combines Quotient Value Difference (QVD) with Huffman coding. These two methods are more efficient, simple to implement and provides better security to the data. The secret message is encoded using Huffman coding, while the cover image is compressed using QVD. Then the encoded data is embedded into cover image and transferred over the network to receiver. At the receiver end, the data is decompressed to obtain original message. The proposed method shows high level performance when compared to other existing methods with better quality and minimum error.

Keywords- *Steganography, data-hiding, CR, PSNR, MSE, image compression, Huffman coding*

1. INTRODUCTION

At present, the secret messages have been sent from sender to receiver by hiding message in an image or a text so that only sender, receiver can view the message. Due to the advancement in technology and internet services, security has got greater attention. To conceal activity, data hiding is preferred. In data hiding, a secret message will be embedded into some media files like text files, audio and video. The technology of hiding secret message with media files is called steganography. Image which is used to hide data is called cover image and it is referred to as stegno-image after hiding the data. These data hiding techniques are mainly categorized into two types. They are:

1. Reversible data hiding
2. Non reversible data hiding.

In reversible data hiding it is possible to recover original cover media after extracting secret message. But the embedding capacity is limited to low level.

Non reversible data hiding is further categorized into three types.

1. LSB substitution
2. Pixel Value Differencing (PVD)
3. Reference Matrix (RM)

In LSB data hiding technique, it is very difficult and unstable to identify the data hidden in the media file. It is a spatial domain technique. It is very common and popular technique. PVD method improves quality by embedding data, by reducing or increasing the cover pixel pair. Pixel value difference histogram is analyzed to detect data. PVD of higher bit plane is named as Quotient Value Differencing (QVD).

Another application of steganography is healthcare. Due to the advancement of technology the diagnosis and treatment of many critical diseases has made east and fastened such as CT scan, MRI scan. These images will be processed or stored locally and also transmitted to respective healthcare professionals. To transmit these images through

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 10 Issue: 9
DOI: https://doi.org/10.17762/ijritcc.v10i9.5709
Article Received: 02 July 2022 Revised: 09 August 2022 Accepted: 18 August 2022 Publication: 30 September 2022

internet, it requires large amount of space or bandwidth. So, there is a requirement to reduce the size of an image. So, the image should be compressed to minimize image size. It improves the medical data transmission efficiency through internet particularly for tele-pathology, tele-radiology. Hence high compression with good quality images should be transmitted over internet. Another reason to compress image is to protect data from hackers. An attacker can hack medical images which are transmitted over internet and can corrupt the data like tampering, changing the data, damaging image quality. Hence the image needs to be compressed to enhance security.

The main objective of the proposed work is to provide security for the data with good quality and minimum error, noise. Many works have been proposed to provide security but they have some limitations such as poor signal to noise ratio, quality of compressed image. In the proposed work these limitations are addressed and provided better security with good performance metrics.

2. LITERATURE REVIEW

Structural obfuscation-based security has been performed On JPEG CODEC hardware in [1]. The proposed method in [1] was based on tree height transformation (THT), however it did not include hardware steganography. Even though this strategy provides a countermeasure against RE, it could not be to detect pirated JPEG processors. Furthermore, a potential attacker may be able to de-obfuscate the obfuscated JPEG design. The JPEG design can be altered with once it has been de-obfuscated. To address this issue, the proposed technology incorporates hardware steganography as a protection mechanism into the obfuscated JPEG processor, making counterfeiting/cloning detection easier.

Proposed a four-category classification of steganographic algorithms in [2]: 1) permutation domain, 2) two-state domain, 3) LSB domain, and 4) transform domain. Categorized steganalysis algorithms into two types: 1) universal steganalysis and 2) customized steganalysis. The current technological level was discussed in the paper for each category.

An Adaptive payload distribution was formulated in multiple picture steganography which was based on image texture attributes and theoretical security analysis was discussed in [3] from the Steganalyst's perspective. 2 payload distribution algorithms are developed and described, one based on image texture complexity and the other on distortion distribution. These state-of-the-art single image steganographic algorithms can be used in conjunction with the described techniques. The security performance is compared to that of the modern universal pooled steganalysis.

Proposed secure steganography algorithms in [4], such as Secure Base LSB, Neural Networks, and Fuzzy logic, and evaluate them using PSNR and MSE data. That information was gathered via video broadcasts. And the results were better than other offered solutions in terms of more formats, security, output quality, and PSNR and MSE accuracy values.

The use of encryption and steganography was proposed in [5] to hide information based on two things: the encrypted object's size and the degree of security. The signature image information is hidden in the cover picture using the sender and receiver's private keys, and the information is extracted from the stego image using a public key. By using this method, non-repudiation, message integrity, Message authentication can be achieved.

Proposed three ways for generalizing SPC to lengths in [6]. The ability of SPC to decrease arbitrary distortion has been shown in experiments. When compared to STC, SPC has better overall coding performance and lower embedding complexity. This study establishes the use of polar codes in the practical design of steganographic codes, as well as a methodology for designing enhanced steganographic codes based on polar coding/decoding advancements.

For sequence generation, a novel mapping rule based on filtered robust object labels was proposed in [7]. As a result of multi-object recognition, an image can yield a stable binary sequence. Because the sent image is not altered during transmission, our solution can withstand attacker's suspicions and steganalysis tools. Furthermore, the proposed method's capacity and concealment rate are also good. Under geometric attacks, evaluations reveal a 3.1-fold gain in robustness over the other five coverless steganography methods. Furthermore, evaluation under 10 different noise attacks revealed that the suggested technique is very resilient, with an average robustness of 83 percent.

An embedding method is proposed in [8] that takes all of the correlations into consideration. It has four sub-lattices and each sub-lattice has 64 lattices. The modification probabilities of each DCT coefficient are calculated using the conditional probabilities inferred from a multivariate Gaussian distribution using the Cholesky decomposition of the covariance matrix. This approach is also used to calculate each image's embedding capacity.

In [9], proposed a unique linguistic steganographic model which is based on generative adversarial network and an adaptive probability distribution and a achieves the goal of hiding secret messages in generated text while retaining excellent security. To effectively combat exposure bias, the

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 10 Issue: 9
DOI: https://doi.org/10.17762/ijritcc.v10i9.5709
***Article Received**: 02 July 2022 **Revised**: 09 August 2022 **Accepted**: 18 August 2022 **Publication**: 30 September 2022*

steganographic generator is first trained using a generative adversarial network, and the candidate pool is then obtained using a probability similarity function at each time step, which reduces embedding deviation by dynamically maintaining probability distribution diversity. Third, a unique technique for information embedding during model training is proposed to further increase security.

Proposed an approach in [10], which is based on the abstract concept of picture components and can be used to create cover images in JPEG, Bitmap, TIFF, and PNG. The suggested approach is, to our knowledge, the first Steganography algorithm that can work with numerous cover picture formats. Furthermore, we used ideas such as capacity pre-estimation, adaptive partition methods, and data spreading to embed secret data with increased security. The suggested technique is robustly evaluated against Steganalysis, with positive findings. Furthermore, comparison findings for the suggested technique for three alternative cover image formats are quite encouraging.

The growing demand for quick and robust wireless transmission has caused standardization units to enhance WLAN standards due to the increased interest in networks built on the IEEE 802.11 standards family. The security considerations and available throughput of the prior technologies have some limitations. In typical IEEE 802.11n networks, this study tries [14] to provide a novel information-hiding technique based on OFDM modulation. This strategy is used because steganographic channels based on fast networks allow for more secure and reliable secret communications than more antiquated and insecure ones.

The paper [15] introduces a new Huffman Encoding-based method for image steganography. As the cover image and secret image, two 8-bit grey level images with dimensions of M x N and P x Q are employed, respectively. Before embedding, the secret image or message is subjected to Huffman encoding. Each bit of the secret image or message is then embedded inside the cover image by changing the least significant bit (LSB) of each pixel's intensity. The Stego-Image is presented to the recipient as standalone information by including the size of the Huffman-encoded bit stream and the Huffman Table[16] inside the cover image.

3. QUOTIENT VALUE DIFFERENCING (QVD)

3.1 Data hiding procedure:

The image is accessed in roster-scan order and distinct pixel blocks with 3*3 size are formed as shown in Fig.1.QVD approach is applied on pixels Ac, A2, A4, A6, A8.

Step1: Two sets of values i.e., quotients and remainders are calculated.

$$P_c = A_c \bmod 4 \quad (1)$$
$$P_i = A_i \bmod 4 \quad (2)$$
$$R_c = A_c \operatorname{div} 4 \quad (3)$$
$$R_i = A_i \operatorname{div} 4 \quad (4)$$

From eq (1 - 4),

$$P_2 = A_2 \bmod 4$$
$$P_4 = A_4 \bmod 4$$
$$P_6 = A_6 \bmod 4$$
$$P_8 = A_8 \bmod 4$$

From eq (4)

$$R_2 = A_2 \operatorname{div} 4$$
$$R_4 = A_4 \operatorname{div} 4$$
$$R_6 = A_6 \operatorname{div} 4$$
$$R_8 = A_8 \operatorname{div} 4$$

Where “Mod” represents remainder and “Div” represents quotient division.

Step2: From secret binary bit stream, one bit will be taken and will be appended to the left of indicator bit1. These two bits will be converted to decimal digit and considered as stego-value of Pc. The next two bits will be converted to decimal and represented as P2. Next two bits will be represented as P4.Similarlyf orP6,P8.

Step3: From eq(3) four quotient value differences will be calculated.

$$B_i = (R_i - R_c) \quad (5)$$

$$B_i = (R_i - R_c)$$

here i=2,4,6,8

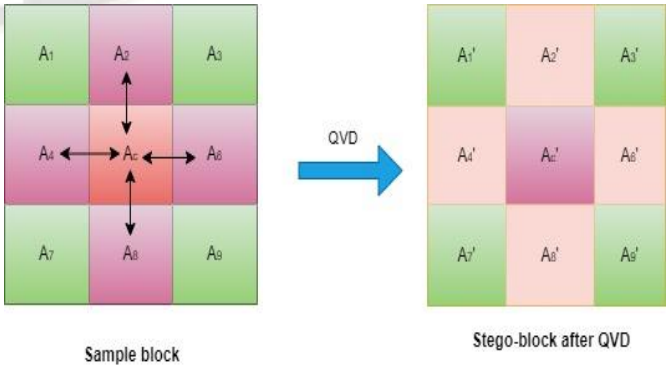

Fig.1. Quotient Value Differencing (QVD)

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 10 Issue: 9
DOI: https://doi.org/10.17762/ijritcc.v10i9.5709
Article Received: 02 July 2022 Revised: 09 August 2022 Accepted: 18 August 2022 Publication: 30 September 2022

$B_i = (R_i - R_c)$ where i=2,4,6,8
Where, b2 = (R2 - Rc)
b2 = (R2 - Rc)
b4 = (R4-Rc)
b6 = (R6 -Rc)
b8 = (R8 -Rc)

Step4: For i, next take n_i secret message bits and those bits will be converted to decimal value d_i. Then calculate b_i' from eq (4),

$$B_i' = L_i + d_i, \quad \text{if } b_i >= 0$$
$$-L_i - d_i \quad \text{if } b_i < 0 \qquad (6)$$

$$M_i = b_i' - b_i \qquad (7)$$

Step5: Now by using eq (6) embed quotient pairs (R_c, R_i).

$$(R_{ci}', R_i') = (R_c - \text{floor}(\tfrac{Mi}{2}), R_i + \text{ceiling}(\tfrac{Mi}{2})) \text{ if } b_i \text{ is even}$$
$$(R_c - \text{ceiling}(\tfrac{Mi}{2}), R_i + \text{floor}(\tfrac{Mi}{2})) \text{ if } b_i \text{ is odd} \qquad (8)$$

Step6: From Rm'Rc2', Rc4', Rc6', Rc8' the stego value of Rc i.e., Rc' is calculate using equation (9)

$$R_m' = \frac{(Rc2' + Rc4' + Rc6' + Rc8'')}{4} \qquad (9)$$

Mean Square Error (MSE) can be calculated by,

$$MSE = \left[\frac{((Rc' - Rc)2 + (R2' - R2)2 + (R4' - R4)2 + (R6' - R6)2 + (R8' - R8)2)}{2}\right] \qquad (10)$$

Step7: Stego value of Ac i.e., Ac' is calculated as

$$A_c' = R_c' * 4 + P_c',$$
$$A_i' = R_i' * 4 + P_i' \qquad (11)$$

Step8: If at least one of the four quotient values, R_2', R_4', R_8', R_c' falls out of boundary, steps 1-7 should be undone.

3.2 Huffman coding

It has many advantages compared to other lossless data compression techniques. It is cheap and also very effective. In Huffman coding produce Huffman tree, which will be used for restoring the data to form original data after compression. It was designed primarily to reduce code duplication and retain the reconstructed image's quality. This can be understood with an example[17].

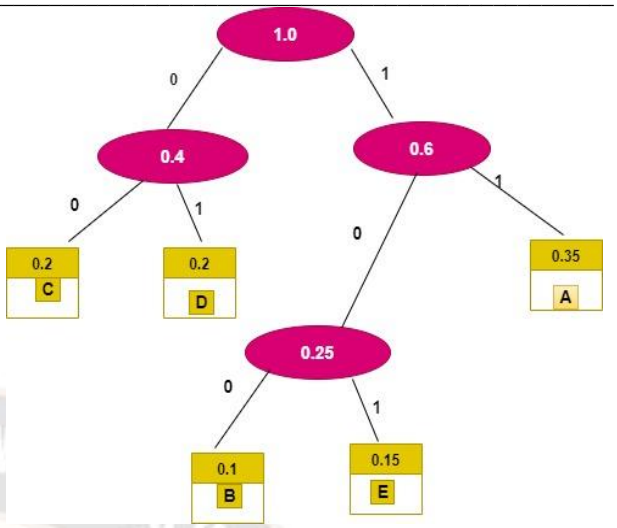

Fig.2. Huffman Tree

Let us consider there are 7 source codes for a digital image shown in Fig. 2. (A, B, C, D, E) with probabilities (0.35, 0.1, 0.2, 0.2, 0.15). The probability which is equal to sum of last 2 numbers. Thus, the process continues.

1. For each unique character, create a leaf node.
2. Extract two nodes from min heap whose frequency is minimum.
3. Now create an internal node whose frequency is equal to sum of 2 nodes frequency shown in Table 1. and Table 2.

Table 1. Symbols with frequencies

Symbol	5r4e432
A	0.35
B	0.1
C	0.2
D	0.2
E	0.15

Table 2. Encoded symbols

Symbol	Codeword
A	11
B	100
C	00
D	01
E	101

4. First node will be placed as left child and other node as right child.
5. Repeat steps 2,3 until there is only one node left in min heap. Now the tree

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 10 Issue: 9
DOI: https://doi.org/10.17762/ijritcc.v10i9.5709
Article Received: 02 July 2022 Revised: 09 August 2022 Accepted: 18 August 2022 Publication: 30 September 2022

is complete.
Total length,
$N = q(gi) * p(gi)$ (10)
Q(gi) is the number of bits in gray level
P (gi) is the value of probability.

4. QVDHC (Quotient Value Differencing with Humming Code)

The proposed algorithm (QVDHC) combines QVD and Huffman coding. A good image has some important aspects. First one is capacity i.e., how much data can be stored in the cover image[18], second one is quality of image and third one is robustness. When the size of the data increases the quality of the image will be reduced. So, image steganography will not generate good results. QVD compress image block with low mean, high mean and bitmap matrix. Hence produce good image quality with minimum noise error.

The main objective is to reduce number of information bit in steganography. There are 2 stages in the proposed algorithm.

1. Embedding the secret message with cover image.
2. Extracting the secret message.

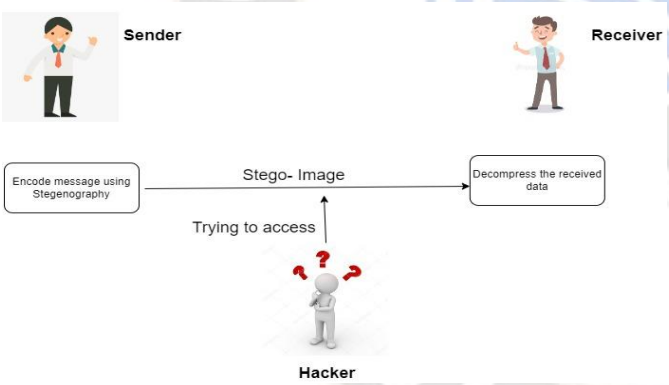

Fig.3. Basic Communication

Fig.3. Presents data transfer between sender and receiver. The secret message will be encoded and embedded with cover image. The stego-image will be transferred to the receiver over the network. Receiver will decompress the cover image and decode the secret message[20]. Hacker when trying to get access over the data cannot be able to decode the secret message because it appears to be a simple image. The Fig.3. Presents the general communication procedure. The encoding and decoding process is presented in the Fig. 4. and Fig.5.

4.1 Embedding secret message

1. The secret message is processed by using Huffman coding.
2. A Huffman tree is constructed with internal node and leaf nodes by extracting internal node and leaf nodes by extracting first 2 nodes with minimum frequencies.
3. The code word is calculated for all symbols given in the secret message[19].
4. The encoded secret message is then embedded with one cover image.
5. The cover image is compressed by using QVD technique.
6. Finally, the encoded stego-image is sent to the receiver.
7. Last step is to calculate Compression Ratio (CR), Compression Density
(CD), PSNR, MSE, SP %.

The input message is ADA BCE CDA. It will be encoded using Huffman coding. After encoding the data will be 110111 10000101 000111.

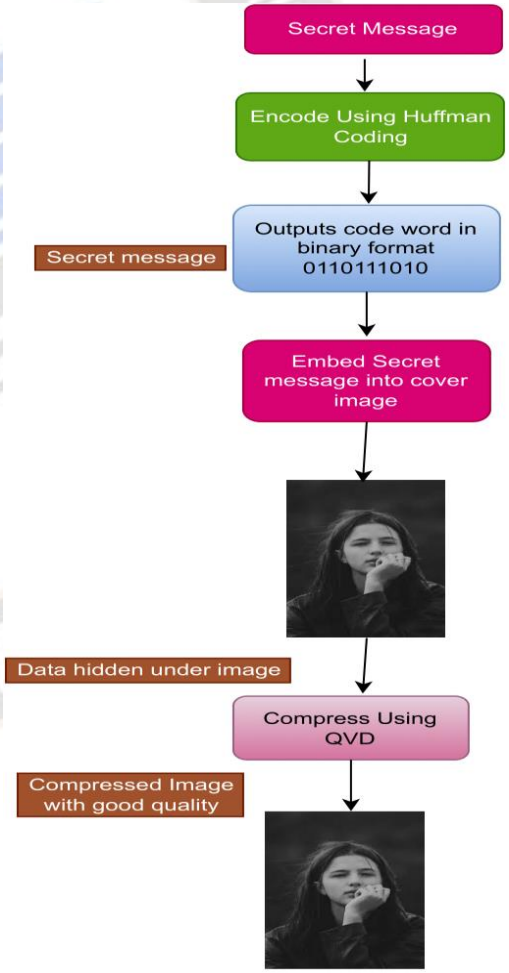

Fig.4. Encoding Process at Sender's end

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 10 Issue: 9
DOI: https://doi.org/10.17762/ijritcc.v10i9.5709
***Article Received**: 02 July 2022 **Revised**: 09 August 2022 **Accepted**: 18 August 2022 **Publication**: 30 September 2022*

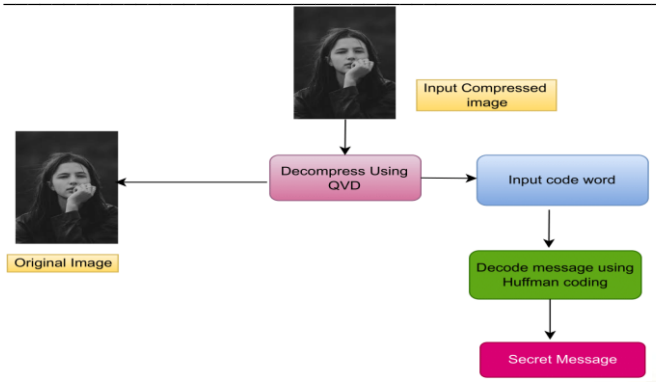

Fig.5. Decoding process at Receiver's end

4.2 Extracting secret message

At the receiver end, the secret message is decoded.

1. Read compressed stego-image.
2. Decompress image by QVD.
3. Decode secret message after decompressing cover image.
4. Apply Huffman coding to decompress the secret message.
5. Construct the Huffman tree generate symbols from code word.
6. Finally, the secret message is extracted.
7. Calculate performance metrics such as CR, CD, PSNR, MSE, SP%.

5 . PERFORMANCE METRICS

The following parameters are used for compressed and compressed image. When an image is compressed, it is necessary to check the quality of image. The quality should be good without loss in the data. Hence, the compressed ratio, mean square error, signals to noise ratio and error should be considered[21].

5.1 Compressed Ratio (CR)

It's the ratio between the original and compressed image sizes. The image quality improves as the compression ratio is increased.

$$CR = \frac{Original\ image\ size}{Compressed\ image\ size} \qquad (12)$$

5.2 Saving Percentage (SP)

It is the ratio of difference between original and compressed image size to original image size.

5.3 Mean Square Error (MSE)

It is used to assess the quality of an image. If the value is 0, the image has been compressed, and the original image has been retained. This is a lossless image compression technique.

$$MSE = \frac{1}{x+y} + \sum_{i=1}^{x} \quad \sum_{j=1}^{y} \quad (f(i,j) - f'(i,j))2 \qquad (13)$$

f (i, j) - original input image.
f (i, j) - compressed image.
x, y – dimensions of the images.

5.4 Peak Signal to Noise Ratio (PSNR)

This is the proportion of signal strength to noise in the signals. It is dependent on the quality of the image. The image quality is high if the PSNR is high.

$$PSNR = 10log10\left(\frac{MAX2}{MSE}\right) \qquad (14)$$

MAX is the maximum intensity of pixels in ideal image. The steganography quality is trusted using PSNR.

6. EXPERIMENTAL EVALUATIONS

The proposed work is simulated in MATLAB 2018A software. It is used on Windows10 platform. MATLAB supports to do many numerical computations, visualization capabilities, data analysis and also used to develop applications. It also helps user to process encryption, decryption efficiently by using the functions. An image was taken as input with size 256*256. And a secret message. Then by applying QVD method the cover image was compressed. This process is repeated with another cover image "camera.tiff" shown in Fig. 6 - 9. Next the secret message is encoded using Huffman coding. The Huffman tree is generated and code word of different lengths was derived from the tree. The encoded data is embedded with compressed cover image.

Table 3. Performance Metrics for Image 'Woman'

Threshold	Message Size (Bytes)	Compressed Message size (Bytes)	CR	CD	Saving Percentage (%)	MSE	PSNR
20	52428	41568	74.328	0.2569	20.7	1.802	25.61
30	52428	36261	82.785	0.1721	30.83	1.9	38.433
40	52428	27608	86.294	0.1371	47.34	2.01	42.3
50	52428	15428	88.528	0.1147	70.57	2.33	48.25

Table 4. Performance Metrics for Image 'Camera'

Threshold	Message Size (Byte	Compressed Message size	CR	CD	Saving Percentage (%)	MSE	PSNR

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 10 Issue: 9
DOI: https://doi.org/10.17762/ijritcc.v10i9.5709
Article Received: 02 July 2022 Revised: 09 August 2022 Accepted: 18 August 2022 Publication: 30 September 2022

	s)	(Bytes)					
20	20740	16608	72.655	0.278	19.92	1.67	28.3
30	20740	14568	78.94	0.2105	29.75	1.734	31.04
40	20740	11700	83.16	0.1681	43.58	2.011	35.04
50	20740	8160	85.89	0.1410	60.65	2.51	38.18

Table 5. Comparison of Proposed method with Existing Methods

Method	CR	SP (%)	MSE	PSNR
QVDHC	82.97	42.30	1.321	39.473
[11]	82.97	19.175	9.155	38.175
[12]	82.97	15.325	2.685	25.331
[13]	82.97	16.833	1.981	37.781

Table 1., shows the size of original message and size of compressed image. It also presents performance metrics such as CR, CD, SP (%), MSE, PSNR. The cover image is compressed with different threshold values. From the Table 3. – Table 6., it is observed that for cover image 'woman', after compression with threshold 20, the size of image is 41568 bytes, CR is 74.306, CD is 0.2569, saving percentage is 20.7 and MSE is 1.802, PSNR 25.61. This is repeated with threshold values 30, 40 and 50. It is observed that for threshold 50, the compressed image size is 15,428 bytes, PSNR 48.25. Hence it can be concluded that for threshold 50, the image size is reduced but still maintaining good quality with 48.25 PSNR value. In Table 5., With compressed ratio 82.97 different values are produced by different methods. Is is observed from the table that the proposed method is generating good results compared to existing methods [11][12][13].

Fig.6. Image of Woman before compression

Fig.7. Image of a Woman after compression with PSNR 48.25

Fig. 8. Image of a camera before compression

Fig.9. Image of a camera after compression with PSNR 38.18

The secret message of length 300 bits was encoded with Huffman coding. The length of secret message has been reduced to 198 bits after encoding. Next the message is embedded with high quality cover image.

7. CONCLUSION

Image compression reduces the size of the image and helps in saving memory space. Transferring of encoded data over the network is also easy and fast, very efficient. QVD gives efficient output. In the proposed method the Huffman

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 10 Issue: 9
DOI: https://doi.org/10.17762/ijritcc.v10i9.5709
***Article Received**: 02 July 2022 **Revised**: 09 August 2022 **Accepted**: 18 August 2022 **Publication**: 30 September 2022*

coding and QVD are integrated to provide better security. The performance metrics were also calculated. By using hybrid approach a better-quality lossless image with high PSNR value was generated and the data size has also been reduced after encoding with Huffman code. The image quality plays an important role when the size of the data increases. By applying QVD the quality can be maintained, robustness and capacity will also be good. The proposed method has given minimum error of 1.321 compared to other existing methods and high PSNR value of 39.473 % compared to other existing methods. Hence it can be concluded that the proposed method gives good quality lossless image with reduced size, fast transfer and also saves memory space. The work can be continued by developing a method which gives more robustness, best image quality and security.

REFERENCES

[1]. Sengupta, A., Roy, D., Mohanty, S.P. and Corcoran, P., 2018. Low-cost obfuscated JPEG CODEC IP core for secure CE hardware. IEEE Transactions on Consumer Electronics, 64(3), pp.365-374.

[2]. Zhou, H., Zhang, W., Chen, K., Li, W. and Yu, N., 2021. Three-dimensional mesh steganography and steganalysis: A review. IEEE Transactions on Visualization and Computer Graphics.

[3]. Liao, X., Yin, J., Chen, M. and Qin, Z., 2020. Adaptive payload distribution in multiple images steganography based on image texture features. IEEE Transactions on Dependable and Secure Computing.

[4]. Manohar, N. and Kumar, P.V., 2020, May. Data encryption decryption using steganography. In 2020 4th International Conference on Intelligent Computing and Control Systems (ICICCS) (pp. 697-702). IEEE.

[5]. Pramanik, S., Bandyopadhyay, S.K. and Ghosh, R., 2020, March. Signature image hiding in color image using steganography and cryptography based on digital signature concepts. In 2020 2nd International Conference on Innovative Mechanisms for Industry Applications (ICIMIA) (pp.665-669). IEEE.

[6]. Li, W., Zhang, W., Li, L., Zhou, H. and Yu, N., 2020. Designing near-optimal steganographic codes in practice based on polar codes. IEEE Transactions on Communications, 68(7), pp.3948-3962.

[7]. Luo, Y., Qin, J., Xiang, X. and Tan, Y., 2020. Coverless image steganography based on multi-object recognition. IEEE Transactions on Circuits and Systems for Video Technology, 31(7), pp.2779-2791.

[8]. Gupta, D. J. . (2022). A Study on Various Cloud Computing Technologies, Implementation Process, Categories and Application Use in Organisation. International Journal on Future Revolution in Computer Science &Amp; Communication Engineering, 8(1), 09–12. https://doi.org/10.17762/ijfrcsce.v8i1.2064

[9]. Taburet, T., Bas, P., Sawaya, W. and Fridrich, J., 2020. Natural steganography in JPEG domain with a linear development pipeline. IEEE Transactions on Information Forensics and Security, 16, pp.173-186.

[10]. Zhou, X., Peng, W., Yang, B., Wen, J., Xue, Y. and Zhong, P., 2021. Linguistic steganography based on adaptive probability distribution. IEEE Transactions on Dependable and Secure Computing.

[11]. Ansari, A.S., Mohammadi, M.S. and Parvez, M.T., 2020. A multiple-format steganography algorithm for color images. IEEE Access, 8, pp.83926-83939.

[12]. N. Sharma and U. Batra, Jul. 2018, "Performance analysis of compression algorithms for information security: A review," ICST Trans. Scalable Inf. Syst., vol. 7, no. 27, Art. no. 163503.

[13]. A. Jeromel and B. ˇZalik, Jan. 2020, "An efficient lossy cartoon image compression method," Multimedia Tools Appl., vol. 79, nos. 1–2, pp. 433–451.

[14]. M. Dehshiri, S. G. Sabouri, and A. Khorsandi, 2021, "Structural similarity assessment of an optical coherence tomographic image enhanced using the wavelet transform technique," J. Opt. Soc. Amer. A, Opt. Image Sci., vol. 38, no. 1, pp. 1–9.

[15]. Das, R. and Tuithung, T., 2012, March. A novel steganography method for image based on Huffman Encoding. In *2012 3rd National Conference on Emerging Trends and Applications in Computer Science* , pp. 14-18.

[16]. Grabski, S. and Szczypiorski, K., 2013, May. Steganography in OFDM symbols of fast IEEE 802.11 n networks. In *2013 IEEE security and privacy workshops* pp. 158-164.

[17]. Samunnisa, K., Lakshmi, M.S., & Kumar, D.S. (2015). Design of an adaptive JPEG Steganalysis with UED., International Journal Of Computer Engineering In Research Trends,2(8),pp.497-504.

[18]. Gunjan, Er. Madan Lal (2016), Investigation of Various Image Steganography Techniques in Spatial Domain , International Journal Of Computer Engineering In Research Trends,3(6),pp.347-351.

[19]. Saraireh, J., & Joudeh, H. (2022). An Efficient Authentication Scheme for Internet of Things. International Journal of Communication Networks and Information Security (IJCNIS), 13(3).

[20]. Viswanathan, P., & Krishna, P. V. (2009, October). Text fusion watermarking in medical image with semi-reversible for secure transfer and authentication. In 2009 International Conference on Advances in Recent Technologies in Communication and Computing (pp. 585-589). IEEE.

[21]. Linda R. Musser. (2020). Older Engineering Books are Open Educational Resources. Journal of Online Engineering Education, 11(2), 08–10. Retrieved from http://onlineengineeringeducation.com/index.php/joee/article/view/41

[22]. Viswanathan, P., & VenkataKrishna, P. (2011). Fusion of cryptographic watermarking medical image system with

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 10 Issue: 9
DOI: https://doi.org/10.17762/ijritcc.v10i9.5709
***Article Received**: 02 July 2022 **Revised**: 09 August 2022 **Accepted**: 18 August 2022 **Publication**: 30 September 2022*

reversible property. Computer Networks and Intelligent Computing, 533-540.

[23]. Yasar, A. (2021). Data Classification of Early-Stage Diabetes Risk Prediction Datasets and Analysis of Algorithm Performance Using Feature Extraction Methods and Machine Learning Techniques. International Journal of Intelligent Systems and Applications in Engineering, 9(4), 273–281. https://doi.org/10.18201/ijisae.2021473767

[24]. Ajin P Thomas , Sruthi P.S , Jerry Rachel Jacob , Vandana V Nair , Reeba R (2017), Secret Data Transmission Using Combination of Cryptography &Steganography. 4(5),pp.171-175.

[25]. Lakshmi, T. Naga, S. Jyothi, and M. Rudra Kumar. "Image Encryption Algorithms Using Machine Learning and Deep Learning Techniques—A Survey." Modern Approaches in Machine Learning and Cognitive Science: A Walkthrough. Springer, Cham, 2021. 507-515.