Hindawi
Wireless Communications and Mobile Computing
Volume 2022, Article ID 1505133, 11 pages
https://doi.org/10.1155/2022/1505133

Research Article

Histogram Shifting-Based Quick Response Steganography Method for Secure Communication

Geno Peter,[1] **Anli Sherine**,[2] **Yuvaraja Teekaraman**,[3] **Ramya Kuppusamy**,[4] **and Arun Radhakrishnan**[5]

[1]*CRISD, School of Engineering and Technology, University of Technology Sarawak, Malaysia*
[2]*School of Computing and Creative Media, University of Technology Sarawak, Malaysia*
[3]*Mobility, Logistics, and Automotive Technology Research Centre, Faculty of Engineering, Vrije Universiteit Brussel, Brussels 1050, Belgium*
[4]*Department of Electrical and Electronics Engineering, Sri Sairam College of Engineering, 562 106, Bangalore City, India*
[5]*Faculty of Electrical & Computer Engineering, Jimma Institute of Technology, Jimma University, Ethiopia*

Correspondence should be addressed to Arun Radhakrishnan; arun.radhakriahnan@ju.edu.et

Received 23 October 2021; Accepted 22 December 2021; Published 12 March 2022

Academic Editor: Shalli Rani

Steganography is a tool which allows the data for transmission by concealing secret information in a tremendously growing network. In this paper, a novel technique quick response method (QRM) is proposed for the purpose of encryption and decryption. Existing system uses side match vector quantization (SMVQ) technique which has some challenges such as security issues and performance issues. To handle the security and performance issues, the proposed system uses two methods, namely, quick response method and shifting method. In the proposed system, encoding part calculates the performance for capacity, PSNR (peak signal-to-noise ratio), MSE (mean square error), and SSIM (structural similarity index method), and the decoding part calculates the performance of MSE (mean square error) and PSNR (peak signal-to-noise ratio). The shifting method is used to increase the data hiding capacity. In this system, the encryption part embeds the secret image using steganography and the decryption part extracts the original image. By analyzing and comparing the proposed system with the existing system, it is proved that the system proposed was much better than the existing systems.

1. Introduction

For the security purpose, data hiding process is used to embed the data into digital media. It delivers large volume for secret information hiding which results into stego image imperceptible to human vision. Data hiding such as image and text that permits the cover image to be improved after the embedded message is mined from the marked image. Data hiding is broadly used to hide the secret information into a cover information like a video file, an audio file, and an image [1]. For efficient storage and transmission, embed data into an image and link with compression. Medical images are transferred from one hospital to another hospital for review by physicians across the globe. Such medical image data has to be stored in the database for future reference of patients. Normally, these medical images are compressed and stored before being transmitted over the Internet. Similarly, the patient data is also embedded within the medical images. The hidden and the host image data can be recovered from the embedded image without any data loss [2]. In RDH (reversible data hiding), the data to be covered up is embedded in the cover image. Data hiding technique and image compression technique can be integrated as one single module [3]. Reversible data hiding can embed the message data in a host image without any loss of the host image. If watermarked image is used for image authentication, with the improved histogram-based reversible data hiding scheme which is based on prediction and sorting, the original image can be reverted before the embedding

process. This histogram-based embedding increases the capacity of the embedding process [4]. The steganography method is aimed at secretly hiding the data in a multimedia medium between two sides to conceal the occurrence of the message. It is based on two important factors such as embedding payload and efficiency. It gives the result that creates it suitable to transfer data without being censored and the data interrupted. Data security is broadly based on encryption and for few cases based on an extra layer of security [5]. A high embedding performance is offered by transform domain JPEG image steganography method [6]. Histogram shifting technique in integer wavelet transform area converts information into higher frequency wavelet coefficients subbands. The histogram modification approach is useful to avoid overflow and underflow. It reallocates a fraction of the larger frequency wavelet subband histogram and consequently inserts data with the help of generated histogram zero-point.

The proposed method performance with data embedding payload is compared with the performance of existing methods in integer cosine transform domain, spatial domain, and integer wavelet transform domain. The maximum embedding payload in the same visual quality is computer by PSNR or has a higher PSNR in the same payload. At the time of shifting operation performed high-frequency integer wavelet subbands, the overflow (e.g., for an 8-bit image, the value of pixel grayscale exceeds 255) and/or underflow (e.g., for an 8-bit image, the pixel grayscale value below 0) could take place, hence preventing the lossless need consecutively to overcome overflow and/or underflow [7]. Image decompression is based on side match vector quantization (SMVQ). At the sender side, vector quantization is applied to composite blocks, to manage visual deformation and error flow. Image is segmented into nonoverlapping blocks. The leftmost and upmost blocks are compressed using vector quantization. Remaining blocks are compressed by side match vector quantization (SMVQ). At the receiver side, reconstruction of image takes place. Extraction phase consists of exactly reverse process, i.e., decompression side match vector quantization (DSMVQ) [8].

2. Related Work

A high-capacity modified steganography technique using wavelet transform was reported by Ali et al. In this technique, the original cover image was preadjusted such that the reconstructed pixels from the embedded coefficients would not exceed its threshold value. The drawback of the proposed method is the computational overhead. This technique obtained the PSNR value of 40.98%. Acharya et al. have proposed a method to hide multiple secret images and keys in color cover image using integer wavelet transform (IWT) using image steganography technique. The average PSNR value obtained is 44.7%. Sathish et al. suggested a high-capacity and optimized image steganography technique based on ant colony optimization algorithm. This technique achieved the PSNR value of 40.83. Ahmed et al. used nonlinear properties of quantum walks to design a novel technique for constructing S-boxes and applied those S-boxes to design a new steganography technique. The proposed method obtained the PSNR value which is 44.26%. Nadish et al. embedded the data in the edge pixel of carrier image using an improved image steganography. The PSNR value for this technique obtained is 45.33%. The organization of the paper is categorized as follows. Section 1 explains the introductory part of data hiding and steganography. Section 2 illustrates the related work based on the steganography. Section 3 describes the proposed quick response technique-based steganography. Section 4 elaborates the results and discussion. Finally, Section 5 gives the conclusion of the paper.

3. Proposed Quick Response-Based Steganography

The proposed quick response technique is developed such that the capacity for encoding process is increased. With the help of ZXing (open source library) and MATLAB, it can be retrieved. The algorithms are applied to process the QR codes which include some geometric properties like area, centroid, bounding box for finding and varying the color of "finder patterns," and its conditions for each code with several colors in MATLAB thus maximizing into three dimensions. To create three-dimensional quick response code encoding process, three processed codes are added for three separate messages. The reverse operation was performed for decoding process such that encoded code was initially delayered by splitting the red, green, and blue channels and subsequently thresholder to go again the originally encoded quick response codes. The improved patterns include the most important in covert applications. Histogram shifting method prevents overflow and underflow issues which enhances the visual quality of image and data hiding capacity. Quick response code technique is used to encrypt the cover image and later decrypt the original information with high quality.

Initially, the image data is partitioned into two main blocks. In the processing step, the histogram is created for every block. The quantity of data which can be embedded within image blocks is more by comparing the embedding within a single image. The proposed block schematic for encoding and decoding process is shown in Figures 1 and 2.

3.1. Image Acquisition. The input image was color which may be in the file format of (jpg, png, bmp, and tiff) and compressed or uncompressed formats. Then, the image is transformed into a color space. The different color spaces are RGB, HSV, YIQ, LAB, and YCbCr. Image enhancement is to increase the quality of images using spatial, frequency, and watermark transform domain.

3.2. Filter Image. The filtering takes both spatial and intensity domain information in calculating the edge-preserving smoothing output for an input image. It replaces the intensity of each pixel with intensity values from nearby pixels.

3.3. Histogram Shifting. Monotonic mapping between a test and reference image of histograms is computed by histogram shifting. Test and reference images can be any of the

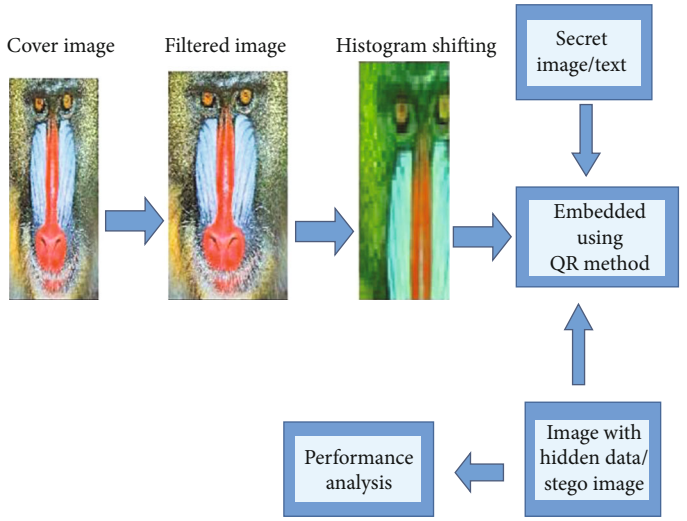

Figure 1: Block diagram proposed quick response encoding process.

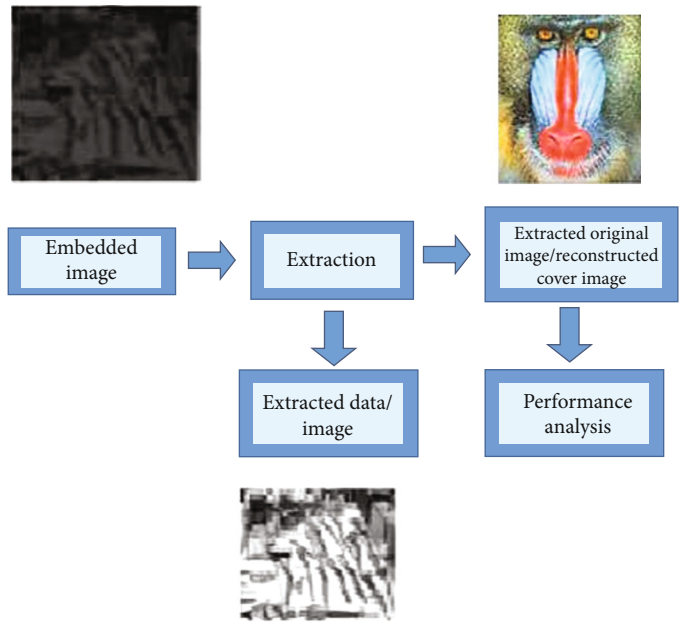

Figure 2: Block diagram proposed quick response decoding process.

permissible data types and need not be equal in size. This shifting technique increases the contract based on similarity between test and reference image.

3.4. QR Method. QR code is two-dimensional barcode which is categorized in matrix barcode that can store large alpha-numeric information. Barcode consists of black modules arranged in white background. Data can be restored even if the symbol is partially dirty or damaged. *EF* of a given image *D* in the form of a matrix is defined as

$$D = E \times F, \tag{1}$$

where E is an orthonormal matrix and F is an upper triangular matrix. D and E are denoted as $D = [d_1, d_2, d_3, \cdots, d_n]$ and $E = [e_1, e_2, \cdots, e_n]$, respectively.

Embedding algorithm:

(i) Read a test image

(ii) Make QR decomposition with a watermark image

(iii) Apply discrete wavelet transform (DWT) on both test and QR decomposition images

(iv) Insert the QR decomposition image into test image

(v) Reconstruction of test image to apply inverse of DWT

(vi) Finally, we get embedded image

Extraction algorithm:

(i) Read the embedded image and test image

(ii) Apply DWT on both test and embedded images

(iii) Subtract embedded image with the test image and get the QR decomposition image

(iv) By using QR decomposition reader extract watermark image from the QR decomposition image

Cover: the data or image which is masked inside the secret message. Embedding and extraction processes: in this process, the secret data was enveloped inside the cover and the hidden data can be recovered. Encryption: this is an embedding process where the secret data is coded [9]. Stego information: the information obtained at the end of the embedding process is known as stego information. Decoding process: the extraction phase can be followed by a suitable decoding phase depending upon whether encryption was used or not during embedding [10]. Steganography: steganography based on text, audio, video, or image is used as the cover medium. Digital image stenographic concepts are very famous mediums applied worldwide for data transfer in addition to data hiding [11]. Steganography mapping for a digital image using embedding and extraction process is given by

$$\begin{aligned} M_1 &= \{C_1 \times K_1 \times T_1\} \longrightarrow C_1', \\ X_1 &: \left\{C_1' \times (K_1)\right\} \longrightarrow C_1, \end{aligned} \tag{2}$$

where M_1 is the embedding function, X_1 the extraction function, C_1 the cover image, $C_1{}'$ the stego image, K_1 the set of keys, and T_1 the set of secret messages.

3.5. Peak Signal-to-Noise Ratio and Mean Square Error Computation. The PSNR calculates the peak signal-to-noise ratio, among the two different images expressed in terms of decibels. This relation is frequently used as an excellence measurement between the original and a compressed image. For better quality measurement, the value of PSNR should be high; thus, it produces a high-quality image even if it is a compressed or reconstructed image [12]. The mean square error (MSE) and the peak signal-to-noise ratio (PSNR) are the two most important terms for the accurate image quality determination. When the value of MSE is lower, the error obtained is also reduced [13].

PSNR can be calculated using equations (3) and (4).

$$\mathrm{MSE} = \sum_{M_1, N_1} \frac{[I_1(m_1, n_1) - I_2(m_2, n_2)]^2}{M_1 \times N_1}, \tag{3}$$

where M_1 is the number of rows and N_1 is the number of columns in the input image. After that, the block calculates the PSNR using the given equation:

$$\mathrm{PSNR} = 10 \log_{10}\left(\frac{r^2}{\mathrm{MSE}}\right), \tag{4}$$

where r can be varied based on the input image data type.

3.6. Structural Similarity Index Method. The structural similarity index method (SSIM) is a method for determining the stego image quality. SSIM is used for computing the similarity of two images. This measures the image quality based on an uncompressed or distortion-free image. SSIM is simulated to develop on the latest techniques such as peak signal-to-noise ratio (PSNR) and mean squared error (MSE) [14]. SSIM is measured from the host image and the dense image. It is calculated based on the important metrics, namely, contrast and luminance [15].

The SSIM index is measured based on various images. The measure between two images a and b of common size $B \times B$ is

$$\mathrm{SSIM}\,(a, b) = \frac{(2\mu 1_a \mu 1_b + C_2)(2\sigma 1_{ab} + C1_2)}{\left(\mu 1_a^2 + \mu 1_b^2 + C_1\right)\left(\sigma 1_a^{12} + \sigma 1_b^2 + C1_2\right)}, \tag{5}$$

where $\mu 1_a$ is the average of a_i, $\mu 1_b$ is the average of b_i, $\sigma 1_a^2$ is the average of a_i, $\sigma 1_b^2$ is the average of b_i, and $\sigma 1_{ab}$ is the covariance of a and b.

$C_{1=}(N_1 L)^2, C_{2=}(N_2 L)^2 C_1, C_2$ provides a weak denominator to stabilize. L is the pixel dynamic range value, $N_1 = 0.01$ and $N_2 = 0.03$ by default. The symmetry condition for SSIM index is $\mathrm{SSIM}\,(a, b) = \mathrm{SSIM}\,(b, a)$ using this formula:

$$\begin{aligned} (a, b) &= \frac{2\mu_a \mu_b + C_1}{\mu_a^2 + \mu_b^2 + C_1} \mathrm{lu} \\ \mathrm{co}(a, b) &= \frac{2\sigma_a \sigma_b + C_2}{\sigma_a^2 + \sigma_b^2 + C_2} \mathrm{co}(a, b) = \frac{2\sigma_a \sigma_b + C_2}{\sigma_a^2 + \sigma_b^2 + C_2}, \end{aligned} \tag{6}$$

$$\mathrm{st}(a, b) = \frac{\sigma_{ab} + C_3}{\sigma_a \sigma_b + C_3} \mathrm{st}(a, b) = \frac{\sigma_{ab} + C_3}{\sigma_a \sigma_b + C_3}. \tag{7}$$

With, in addition to the above definition,

$$C_3 = \frac{C_2}{2} C_3 = \frac{C_2}{2}. \tag{8}$$

SSIM is the a weighted combination of those comparative measures

$$\begin{aligned} \mathrm{SSIM}(a, b) &= \left[d(a, b)^\alpha \cdot c(a, b)^\beta \cdot s(a, b)^\gamma\right] \mathrm{SSIM}(a, b) \\ &= \left[d(a, b)^\alpha \cdot c(a, b)^\beta \cdot s(a, b)^\gamma\right], \\ &\text{Setting the weights } \alpha, \beta, \gamma \text{ to } 1. \end{aligned} \tag{9}$$

Generally, SSIM expression is based on three measurements between the test images of a and b: luminance (lu), contrast (co), and structure (st). The entity comparison approach evaluates the image quality [16].

4. Results and Discussion

The proposed technique was evaluated for the security efficiency on both the gray level and color images. The

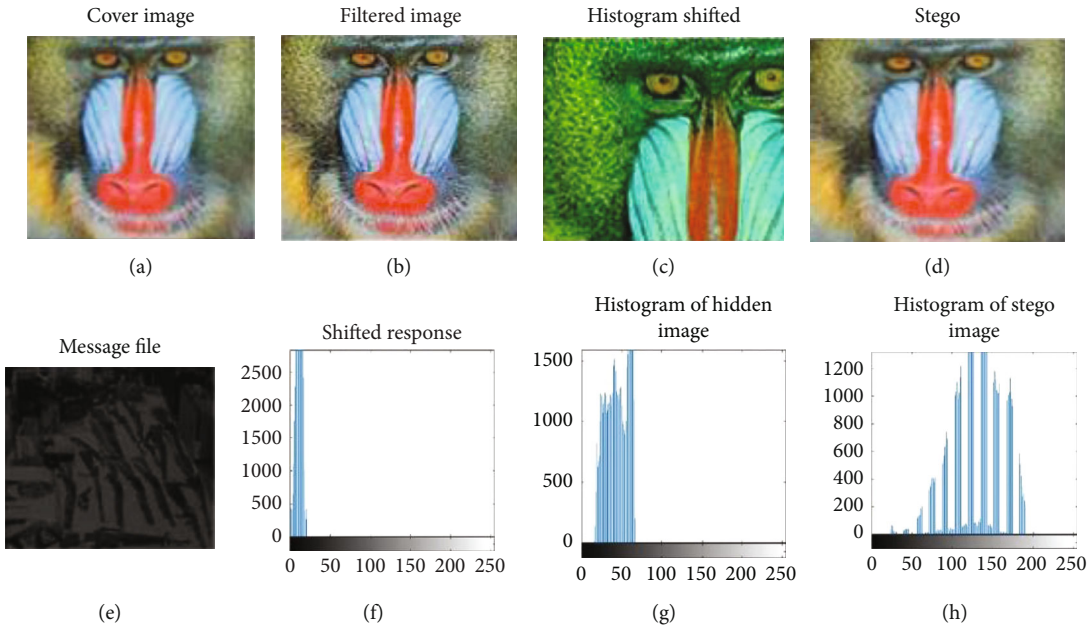

Figure 3: (a) Cover image; (b) filtered image; (c) histogram shifted image; (d) stego; (e) message file; (f) shifted response; (g) histogram of hidden image; (h) histogram of stego image.

Figure 4: Cover image segmentation.

following subsections describe the encoding and decoding process and their performance analysis of the proposed system [17]. The encoding process of the proposed system consists of the following subprocesses: (i) input image, (ii) filtered image, (iii) histogram shifting, (iv) embedding, and (v) stego image. The decoding process of the proposed technique consists of the following subprocesses: (i) embedded image and (ii) extraction.

4.1. Encoding Process. The following section describes the encoding process of the proposed system. Initially, the cover image is taken as an input image [18]. Then, the input image is filtered using trilateral filter and the filtered image is given to the histogram shifting to increase the data hiding capacity of the proposed system. The resultant image is embedded with secret. Image/text using embedding technique is called the quick response method. The stego image is obtained from the embedded image, and the evaluation of the performance provides better results than the other existing systems.

Input image is given by the user. Figure 3(a) shows the user given over image. The filtered image is obtained from the given input image using trilateral filter as shown in Figure 3(b). Histogram shifting is a technique which is done on each block of the image. Figure 3(c) shows the histogram shifted image and its histogram [19]. Embedding is the process of inserting text/image behind the original image. This process is carried out using the quick response method. This

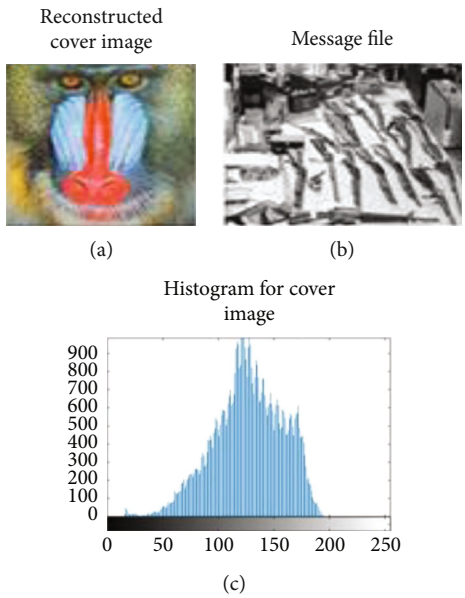

Figure 5: (a) Reconstructed cover image; (b) message file; (c) histogram for cover image.

method improves the data hiding capacity of the proposed system. Figure 3(d) shows the message file and histogram of hided image. At first, cover image segmentation is done

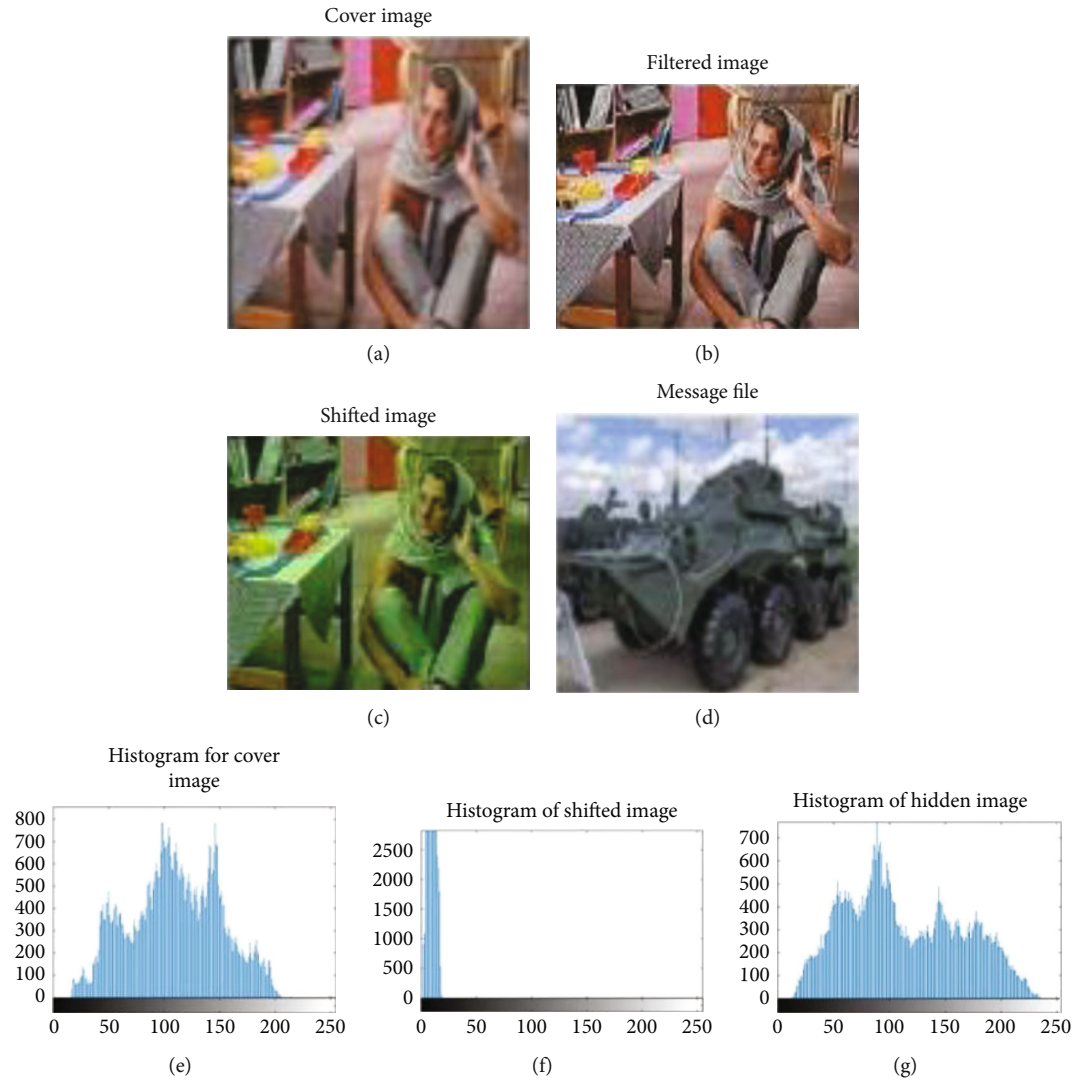

Figure 6: (a) Cover image; (b) histogram for cover image; (c) filtered image; (d) histogram of shifted image; (e) shifted image; (f) message file; (g) histogram of hidden image.

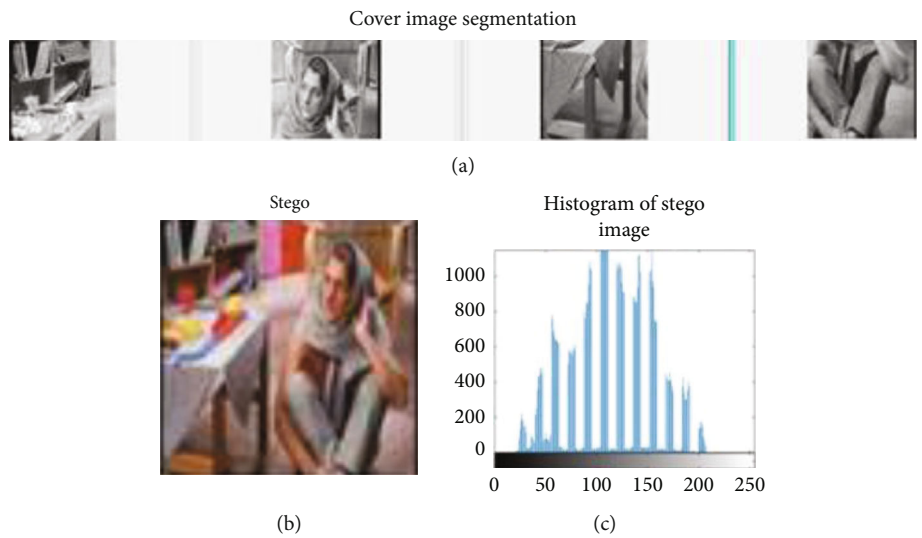

Figure 7: (a) Cover image segmentation; (b) stego; (c) histogram of stego image.

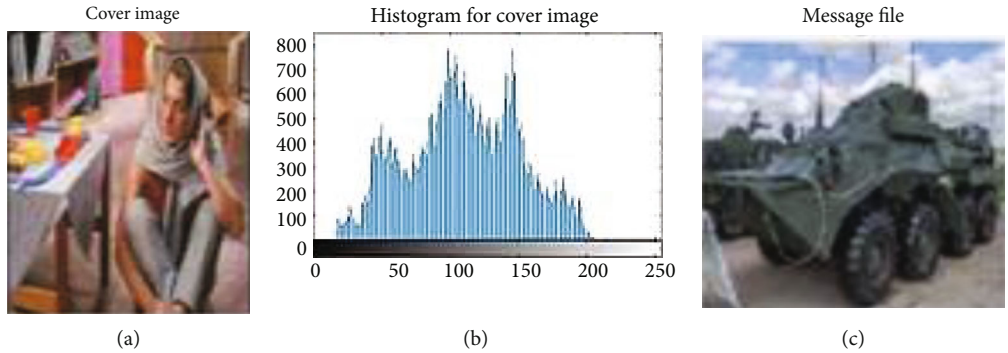

Figure 8: (a) Cover image; (b) histogram for cover image; (c) message file.

Table 1: Performance analysis of the proposed QR-based steganography.

Test images	Secret image	Capacity	Encoding			Decoding	
			SSIM	MSE	PSNR	MSE	PSNR
Barbara	Data	71061	0.9291	4.6266	52.5359	0.23	78.80
	Image		0.9340	5.0853	52.0185	0.234	78.80
Helen	Data	71076	0.9872	4.6688	52.4915	0.25	81.79
	Image		0.9961	5.1484	51.9526	0.207	81.90
Lenna	Data	70965	0.9645	4.6285	52.5335	0.26	78.87
	Image		0.9760	5.0780	52.0264	0.269	78.81
Lighthouse	Data	70919	0.9907	4.6542	52.5029	0.21	78.74
	Image		0.9834	5.0899	52.0136	0.251	78.63
Mandrill	Data	71169	0.9623	4.5675	52.6072	0.19	78.56
	Image		0.9669	5.0186	52.0901	0.180	78.51
Owl	Data	71281	0.9825	4.8155	52.3153	0.18	79.45
	Image		0.9522	5.2936	51.8026	0.148	78.51
Penguin	Data	70850	0.9591	4.4858	52.7078	0.18	77.02
	Image		0.9695	4.9354	52.1810	0.189	76.99
Pepper	Data	70868	0.9926	3.0433	55.02	0.24	76.58
	Image		0.9909	3.3089	54.4968	0.234	76.56
Taj Mahal	Data	71064	0.9810	4.8616	52.2632	0.18	77.46
	Image		0.8349	5.300	51.7961	0.154	77.41

on the embedded image and it is the process of dividing the images using discrete wavelet transform. Figure 4 shows the representation of cover image segmentation.

Steganography is a process of communicating secretly where the text/image is hidden in another image. It increases the data hiding capacity of the proposed system. The figure shows the stego image and its histogram.

4.2. Decoding Process. The following section explains the decoding process of the proposed system. Initially, the reconstructed cover image is taken as an input image. The hidden text/image is extracted from the reconstructed cover image or embedded image using inverse quick response method [20]. Finally, the performance evaluation is done on the reconstructed cover image and it provides better results than the other existing systems. Figures 5(a)–5(c) show the reconstructed cover image, the hidden text/image extracted from the reconstructed cover image, and its histogram.

4.3. For Color Image. Similarly, the encoding and decoding process of the proposed system was carried out for the color images. Figures 6(a) and 6(b) show the cover image and its histogram. Figure 6(c) shows the filtered image which is done with the help of trilateral filter for color images. The histogram shifted image and its shifted histogram are shown in Figures 6(d) and 6(e). The filtered color image is given as an input for histogram shifting technique [21]. The histogram shifted image is embedded with message file using quick response method as shown in Figures 6(d) and 6(e). Figures 6(f) and 6(g) show the message file and its histogram.

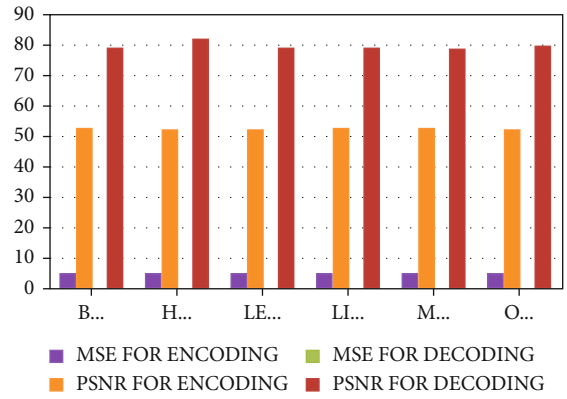

Figure 9: MSE and PSNR graph for encoding and decoding.

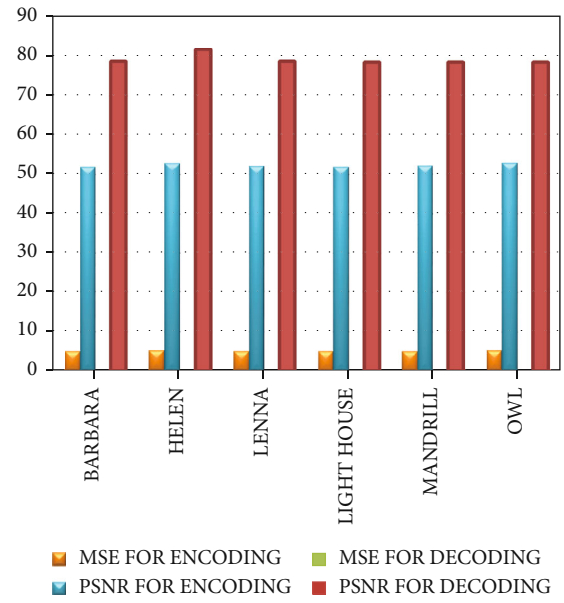

Figure 10: MSE and PSNR graph for secret image.

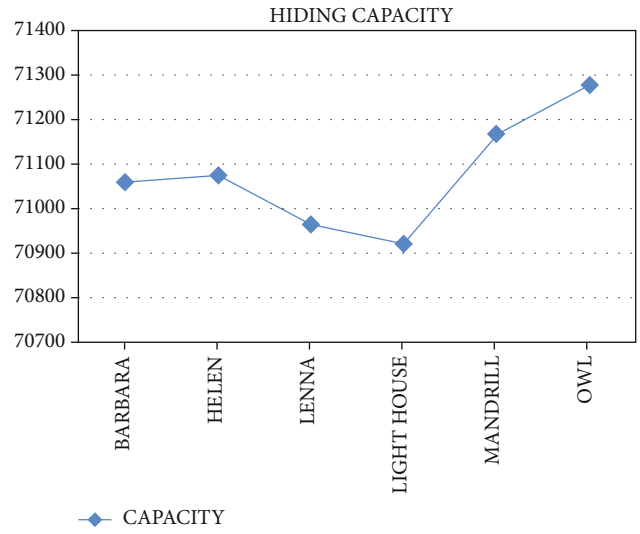

Figure 11: Hiding capacity for test images.

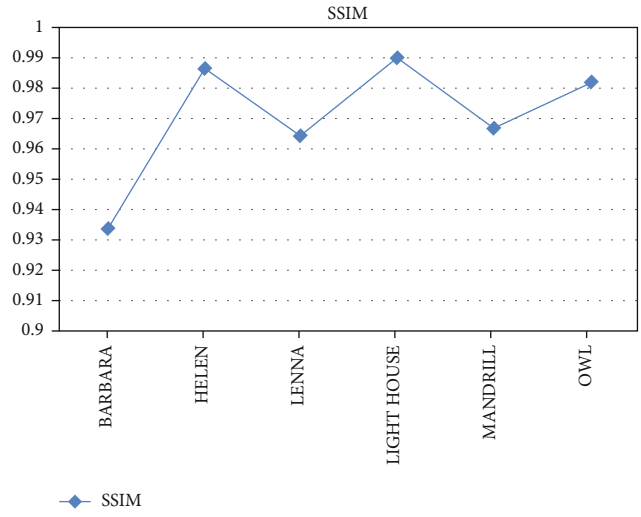

Figure 12: SSIM graph for test images.

The cover image segmentation for color image is carried out using discrete wavelet transforms as shown in Figure 7(a) [22]. The stego image is obtained from the resultant embedded image. Figures 7(b) and 7(c) show the stego image and its histogram. Finally, the hidden data/image is extracted from the cover image. Figures 8(a)–8(c) show the cover image, message file, and histogram for the cover image.

Table 1 shows the performance analysis of both encoding and decoding process of the proposed system using quick response-based steganography technique. The table illustrates the simulation results including the following parameters: test images, secret image, capacity, and encoding and decoding parameters (Mishra, 2016). The encoding parameters are SSIM, MSE, and PSNR. The decoding parameters are MSE and PSNR.QR-based steganography technique with various message sizes on various grayscale images is determined. Moreover, the mean square error and average PSNR values are explained.

Mean square error and PSNR values for secret data are clearly illustrated for the test images such as Barbara, Helen, Lenna, Lighthouse, Mandrill, and Owl as shown in Figure 9. The MSE for encoding process, MSE for decoding process, PSNR value for encoding process, and PSNR value for decoding process are described in this graph.

The result of simulation shows the mean square error and PSNR values for secret images are clearly illustrated for the test images such as Barbara, Helen, Lenna, Lighthouse, Mandrill, and Owl as shown in Figure 10. The MSE for encoding process, MSE for decoding process, PSNR value for encoding process, and PSNR value for decoding process are described in this graph. Figure 10 depicts the graphical representation of obtained hiding capacity values for the test images. The test image Owl has higher capacity compared to other test images. From the graph, the test image light images have the lower hiding capacity value. The results of steganography capacity denote the most significant view of any stenographic method.

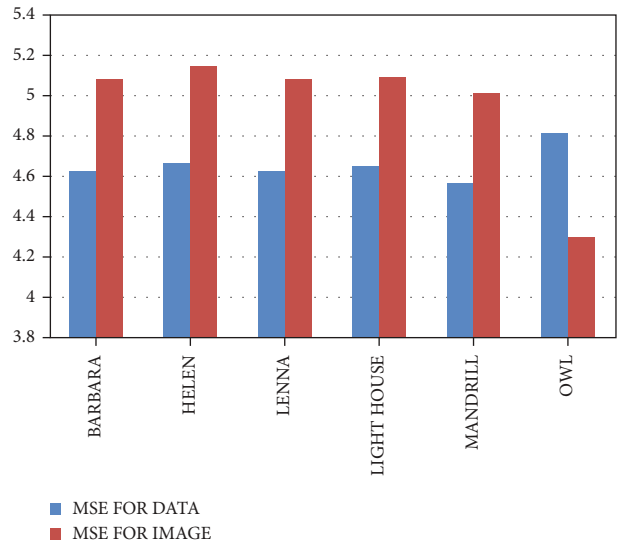

Figure 13: Graphical representation of MSE difference between the secret image and data.

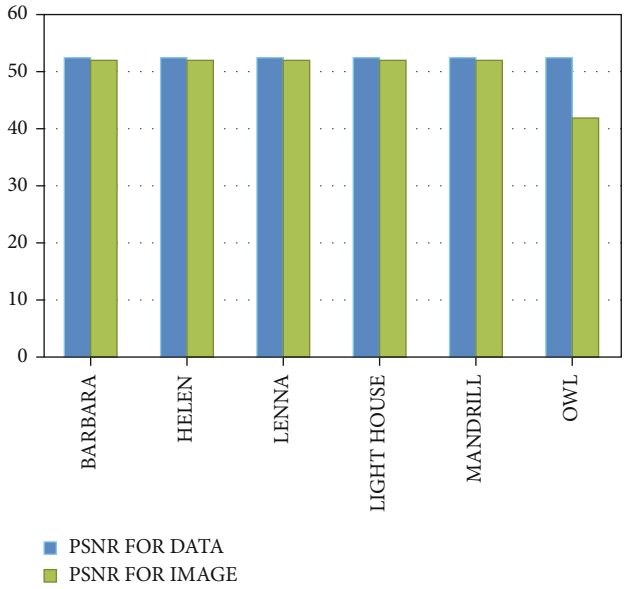

Figure 14: Graphical representation of PSNR difference between the image and data.

Figure 11 depicts the graphical representation of obtained hiding capacity values for the test images. The test image Owl has higher capacity compared to other test images. From the graph, the test image light images have the lower hiding capacity value. The results of steganography capacity denote the most significant view of any stenographic method. The capacity of all cover images to embed the secret image increases, and the QR method increases the security of the secret information.

The SSIM graphical representation for the test images is shown in Figure 12. By using the proposed technique, the obtained value for SSIM using different test images is clearly mentioned to evaluate the proposed method performance.

Table 2: Comparative study of various algorithm-obtained PSNR for steganography.

Author and year	Algorithm	Cover image	PSNR (dB)
Shabir et al., 2010	Pixel repetition method	Barbara	45.13
		Mandrill	45.16
		Lenna	45.14
		Pepper	45.21
Iyad et al., 2016	Reversible data hiding	Barbara	48.70
		Mandrill	48.71
		Lenna	48.70
		Pepper	48.71
Mehdi et al., 2017	Parity-bit pixel value difference and improved rightmost digit replacement	Barbara	36.90
		Mandrill	38.55
		Lenna	39.09
		Pepper	39.11
Ahmed et al., 2019	Quantum substitution boxes	Barbara	44.18
		Mandrill	44.19
		Lenna	44.13
		Pepper	44.11
Inas et al., 2020	Dual tree complex wavelet transform	Barbara	51.42
		Mandrill	51.02
		Lenna	51.37
		Pepper	51.19
Proposed	Quick response	**Barbara**	**52.53**
		Mandrill	**52.60**
		Lenna	**52.53**
		Pepper	**52.61**

Figure 13 shows the graph for MSE difference between the secret image and data.

Figure 14 shows the graph for PSNR difference between the digital image and data. From the graph, the PSNR value obtained for secret data is higher for all test images compared to the PSNR value for secret images. Secret messages should be protected not only in the cyber domain but also in the complex physical domain [23]. The results of Table 2 show that the proposed QR-based steganography method yields better results than all the existing techniques in almost all stenographic images. From this table, by using the proposed method, the PSNR value obtained for the test images Barbara, Mandrill, Lenna, and Pepper is 52.53 dB, 52.60 dB, 52.53 dB, and 52.61 dB, respectively. Steganography conceals the existence of a secret message while cryptography alters the message format itself [24].

Figure 15 clearly shows the comprehensive results of different algorithms as well as the proposed quick response algorithm. The proposed algorithm was considered to be the threshold value to calculate the PSNR percentage for all the existing algorithms.

From Figure 16, it is proved that the PSNR is much improved in the proposed quick response algorithm by

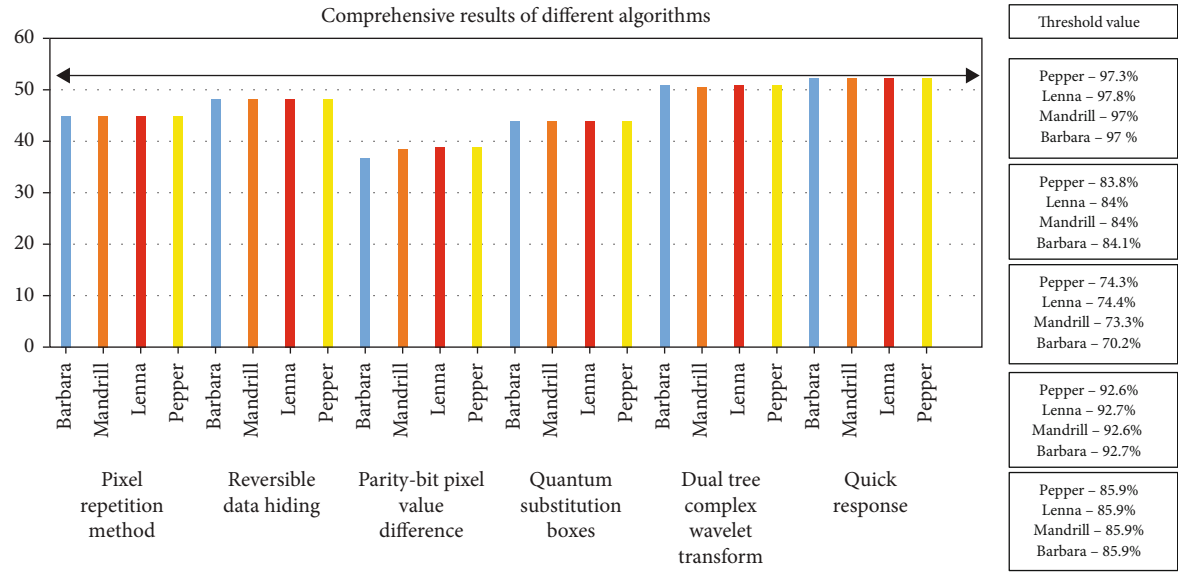

Figure 15: Comprehensive results of different algorithms.

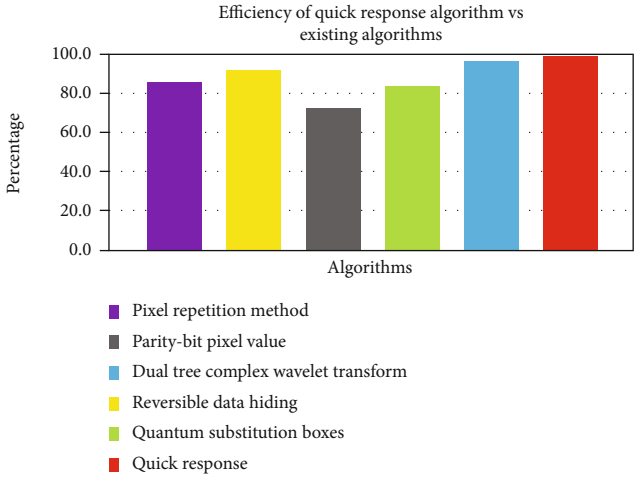

Figure 16: Efficiency of quick response algorithm vs. existing algorithms.

2.5% compared to the best existing algorithm. The higher the PSNR, the better the quality of the compressed or reconstructed image.

5. Conclusion

The data hiding and stenographic capacity is the most significant aspect of the proposed system. A novel data hiding technique is proposed to improve the security of the proposed system. The histogram shifting method ensures the improvement in data hiding capacity, and the quick response method is helpful in extracting the hidden data or image from the original cover image. Several images were taken as test images, and the experiment was carried out on these test images. The resultant images proved that the proposed technique enhances the data hiding capacity by embedding the secret data/image in the cover image using the shifting method. The performance analysis of both encoding and decoding process provides better result than any other techniques used for data hiding.

Data Availability

The data used to support the findings of this study are available from the corresponding author upon request.

Conflicts of Interest

The authors declare that they have no conflicts of interest.

References

[1] O. F. AbdelWahab, A. I. Hussein, H. F. A. Hamed, H. M. Kelash, A. A. M. Khalaf, and H. M. Ali, "Hiding data in images using steganography techniques with compression algorithms," *Telkomnika*, vol. 17, no. 3, pp. 1168–1175, 2019.

[2] U. D. Acharya and P. R. Kamath, "A secure and high capacity image steganography technique," *International Journal*, vol. 4, no. 1, pp. 83–89, 2013.

[3] N. Ayub and A. Selwal, "An improved image steganography technique using edge based data hiding in DCT domain," *Journal of Interdisciplinary Mathematics*, vol. 23, no. 2, pp. 357–366, 2020.

[4] S. Bhavani and B. Raviteja, "Secure data transmission through RDH," *International Journal of Signal Processing, Image Processing and Pattern Recognition*, vol. 7, no. 6, pp. 261–272, 2014.

[5] Y. Zandi Mehran, M. Nafari, A. Nafari, and N. Zandi Mehran, "Histogram shifting as a data hiding technique: an overview of recent developments," *Communications in Computer and Information Science*, vol. 166, pp. 770–786, 2011.

[6] A. E. L.-L. AA, B. Abd-El-Atty, and S. E. Venegas-Andraca, "A novel image steganography technique based on quantum

substitution boxes," *Optics and Laser Technology*, vol. 116, pp. 92–102, 2019.

[7] L. Buzo and R. M. Gray, "An algorithm for vector quantizer design," *IEEE Transactions on Communications*, vol. 28, no. 1, pp. 84–95, 1980.

[8] A. Al-Ataby and F. Al-Naima, "A modified high capacity image steganography technique based on wavelet transform," *International Arab Journal of Information Technology*, vol. 7, pp. 358–364, 2010.

[9] C. Chang and W. C. Wu, "Fast planar-oriented ripple search algorithm for hyperspace VQ codebook," *IEEE Transactions on Image Processing*, vol. 16, no. 6, pp. 1538–1547, 2007.

[10] C. C. Chang, G. M. Chen, and M. H. Lin, "Information hiding based on search-order coding for VQ indices," *Pattern Recognition Letters*, vol. 25, no. 11, pp. 1253–1261, 2004.

[11] W. C. Du and W. J. Hsu, "Adaptive data hiding based on VQ compressed images," *IEE Proceedings-Vision, Image and Signal Processing*, vol. 150, no. 4, pp. 233–238, 2003.

[12] L. S. T. Chen and C. J. C. Lin, "Steganography scheme based on side match vector quantization," *Optical Engineering*, vol. 49, no. 3, article 037008, 2010.

[13] C. C. Chen and C. C. Chang, "High capacity SMVQ-based hiding scheme using adaptive index," *Signal Processing.*, vol. 90, no. 7, pp. 2141–2149, 2010.

[14] C. De Vleeschouwer, J. F. Delaigle, and B. Macq, "Invisibility and application functionalities in perceptual watermarking an overview," *Proceedings of the IEEE*, vol. 90, no. 1, pp. 64–77, 2002.

[15] M. Hussain, A. W. Abdul Wahab, A. T. S. Ho, N. Javed, and K. H. Jung, "A data hiding scheme using parity-bit pixel value differencing and improved rightmost digit replacement," *Signal Processing: Image Communication*, vol. 50, pp. 44–57, 2017.

[16] C. C. Lin, S. C. Chen, and N. L. Hsueh, "Adaptive embedding techniques for VQ-compressed images," *Information Sciences*, vol. 179, no. 1-2, pp. 140–149, 2009.

[17] M. Mishra and B. K. Mishra, "Secret communication through information camouflaging in the mimesis and the crypsis way," in *2016 International Conference on Electrical, Electronics, and Optimization Techniques (ICEEOT)*, pp. 3045–3050, Chennai, India, 2016.

[18] A. Priya, "High capacity and optimized image steganography technique based on ant colony optimization algorithm," *International Journal of Emerging Technology and Innovative Engineering*, vol. 4, no. 6, pp. 1989–1993, 2018.

[19] S. Parah, J. Sheikh, J. Akhoon, and N. Loan, "Electronic health record hiding in images for smart city applications: a computationally efficient and reversible information hiding technique for secure communication," *Future Generation Computer Systems*, vol. 108, 2018.

[20] M. M. Rani and L. Shanti, "An integrated method of data hiding and compression of medical images," *International Journal of Advanced Information Technology*, vol. 6, no. 1, pp. 43–51, 2016.

[21] R. Shamir and L. Adleman, "A method for obtaining digital signatures and public-key cryptosystems," *The Computer*, vol. 21, no. 2, pp. 120–126, 1978.

[22] W. J. Wang, C. T. Huang, and S. J. Wang, "VQ applications in steganographic data hiding upon multimedia images," *IEEE Systems Journal*, vol. 5, no. 4, pp. 528–537, 2011.

[23] Z. Luo, W. Xie, B. Wang, Y. Tang, and Q. Xing, "EasyStego: robust steganography based on quick-response barcodes for crossing domains," *Symmetry*, vol. 11, no. 2, p. 222, 2019.

[24] M. S. Taha, M. S. Rahim, S. A. Lafta, M. M. Hashim, and H. M. Alzuabidi, "Combination of steganography and cryptography: a short survey," *IOP Conference Series: Materials Science and Engineering*, vol. 518, no. 5, article 052003, 2019.