Journal of Harbin Engineering University Vol 44 No. 8
ISSN: 1006-7043 August 2023

Image Steganography based on Enhanced Payload Capacity using Hybrid Edge Detection and Least Significant Bit Steganography

Pooja Belagali[1], Dr. V. R. Udupi[2]

[1]Research Scholar, Gogte Institute of Technology and Visvesveraya Technological University ,Belagavi- 590018, Karnataka, India
[2]Professor, Gogte Institute of Technologyand Visvesveraya Technological University ,Belagavi- 590018, Karnataka, India

Abstract

Gigantic growth in technology leads to widespread usage of multimedia data over different social media platforms, internet, and internet of things. It is crucial to maintain the privacy and security of the data. Image steganography is process of hiding text, image, or audio inside cover image. This paper presents the image hiding technique using Least Significant Bit (LSB) steganography based on hybrid edge detection that maximized the data embedding capacity of the cover image. The performance of the system is evaluated for hybrid edge detection using pair of various edge detection techniques such as Canny, Sobel, Prewitt, and Roberts. The results of proposed steganography approach is estimated for different payload capacity based on Mean Square Error (MSE), Peak Signal to Noise Ratio (PSNR), Structural Similarity Index Metrics (SSIM), Cross-correlation (XCORR), and Universal Image Quality Index (UQI). It is examined that proposed approach performs better than existing state of arts for image steganography.

Keywords: Data security, Least Significant Bit, Steganography, Payload Capacity, Image Hiding

I. Introduction

Security is the important aspect while sending multimedia data using digital communication over the internet. In the public internet system confidentiality is not guaranteed. Digital data security can be obtained using data hiding and data encryption approaches. In data hiding, the content of secrete message or data are hidden in cover or container media [1]. The cover media can be image, video, text, and audio [2][3]. Data encryption can be performed by encoding and scrambling the data that looks like striking version of data to trick the attacker. In data encryption, the input data form is changed to different form which can be easily detected by attacker [4][5].Data hiding is categorized into watermarking and steganography [6]. The watermarking based data hiding intends to keep the image covercopyright so the watermark or hidden data must not be easilydamaged or deleted when manipulation occurs on the media cover, while the steganography technique aims to protectand secure messages embedded in the cover media so that itcannot be detected directly.

With the LSB method as the baseline, a number of related methods have been proposed. For example, a slight variation in converting the secret message into binary codes is undertaken in [7]. A Huffman encoding method is used to encode the secret message into the binary bits. The encoded bits are then embedded in the cover image using the LSB method. In [8], another version of the LSB method is used for RGB images. The cover image is in 3 channels and they are bit sliced. The secret message is embedded in all the three planes in the 2:2:4 ratio for R, G and B planes. Not only spatial domain, quantum images are also used [9] and [10]. The frequency domain is exploited in quantum image domain and the pixels which are considered to be affecting the color are used to hide the secret bits. A combination of cryptography and steganography is utilized where the LSB of the cover image is replaced with the most significant bits of the secret image [11]. The pseudo random number generator is used to

select the pixels and the key is encrypted using rotation every time. A k-LSB method is proposed where the k least bits are replaced with the secret message [12]. For steganalysis, an entropy filter is used to detect and uncover the secret image [12]. The LSB methods are used in hiding the secret information inside videos also. Videos are sequences of images called the video frames. Each video is dissected into image frames and the binary bits of the secret information are hidden in the LSB of the image frames of the video. A basic form of LSB substitution method [13] and a combination of the huffman encoding and LSB substitution methods is used on videos [14]. Another interesting approach is where along with the image frames of the video, audio is also used to enhance the hiding [15]. Besides the LSB methods, [15], has proposed a combination of Discrete Cosine Transformation (DCT) and Discrete Wavelet Transformation (DWT) for hiding the secret message inside a cover video. To find the regions of interest, the multiple object tracking (MOT) method is used. The secret data is encoded first and then converted to binary bits before embedding it in the cover video.

In this paper, we present image steganography based on dilated hybrid edge detection algorithm and LSB steganography to improve the payload capacity of the cover image. The proposed approach uses hybrid edge detection algorithm based on ORing of two edge detection algorithms among Canny, Sobel, Roberts and Prewitt to improve the payload capacity of the cover image. Extensive experiments are performed of various types of images based on different image quality measures.

The rest of the paper is organized as follow: Section II describes the proposed methodology in detail. Section III provides brief discussions on experimental results. Section IV gives the concise conclusion and provides the future direction for improvement of proposed method in future.

II. Proposed Methodology

The proposed methodology is divided in two major phases such as secrete image embedding in cover image and image extraction from stego image. The proposed method uses combination of two edge detection algorithms for the hybrid edge detection.

A. Secrete Image Embedding Phase

In this phase, the secrete image data having dimension m×nis hide into edge and non-edge pixels of the cover image without damaging the visual quality of the cover image having dimension M×N. The dimensions of cover image must be larger than dimensions of secrete image to avoid the loss of data. The image embedding phase is shown Fig. 1. The process of secrete image embedding into cover image can be given as:

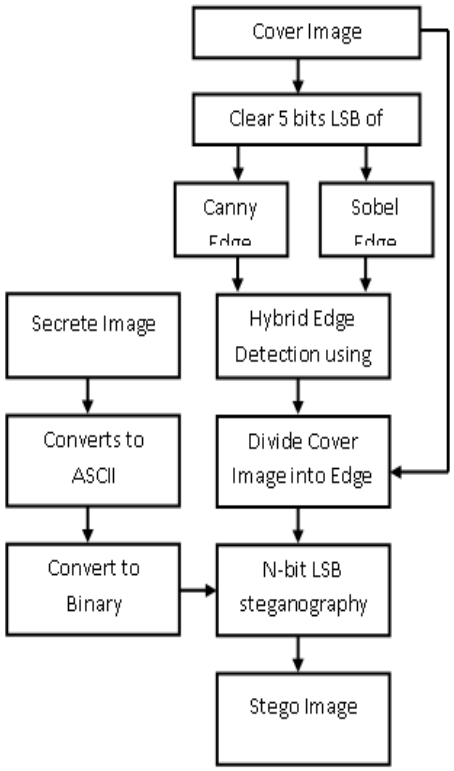

Fig. 1 Proposed Steganography: Data Embedding Phase

1. ***Read Cover Image:*** In this step, cover image (X1) is read and converted to gray scale image. The cover image is then copied to another variable (X2).

2. ***Clear 5 bit LSB:*** Clear the 5 bits LSB of all pixels of cover image (X2). The first to fifth LSB are set to 0 and then whole pixel value is again converted to integer. Because of setting 5 bit LSB to the 0, the individual pixel value may reduce by 0 to 32.
3. ***Edge Detection:*** Perform the Canny edge detectionon X2 and save the results to E_c. Also, perform the Sobel edge detection on X2 and store the result in E_s.
4. ***Hybrid Edge Detection:*** The hybrid edges (E_h) are obtained by taking the OR operation of E_c and E_s . Further, morphological dilation is applied to minimize the noise in hybrid edges and enhance the edges.
5. ***Edge and Non-Edge pixel Decision:*** The pixels of cover image (X1) are divided into edge pixels and non-edge pixels based on hybrid edges.
6. ***Read Secrete Image:*** On the other hand, read the secrete image and convert it to ASCII equivalent.
7. ***ASCII to Binary Conversion:*** Convert the ASCII value of secrete image into binary equivalent (Xb) for LSB steganography.
8. ***Data Embedding:*** Embed the x bits of the Xb to LSB of X1 if the pixel is edge pixel otherwise embed the y bits of Xb to LSB of X1. The x and y value should not exceed 5 bits because current approach can only accommodate 5 bits per pixel. Again, the value of x must be greater than y because the edge area provides the better tolerance.
9. ***Stego Image (S1):***Stego image (S1) can be obtained by embedding all the bits of Xb to X1.

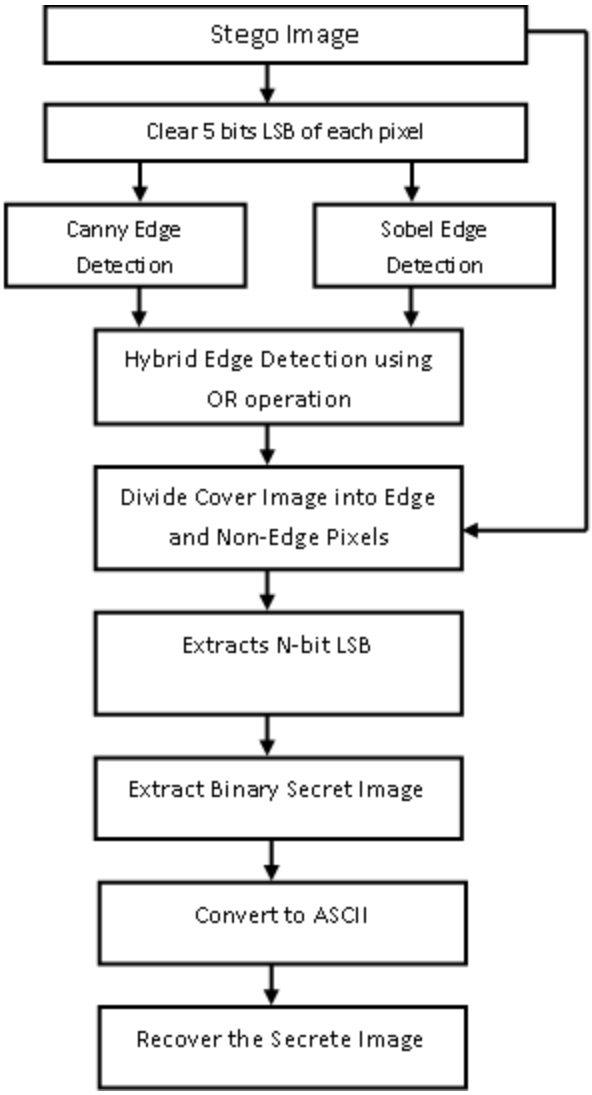

Fig. 2 Proposed Steganography: Data Extraction Phase

B. Secrete Image Extraction Phase

In this phase, the secrete image from the stego image is retrieved without loss of secrete image information. The secrete image extraction phase is shown Fig. 2. The process of secrete image extraction from stego image can be given as:

1. ***Read Stego Image:*** In this step, stego image (S1) is read. The stego image is then copied to another variable (S2).
2. ***Clear 5 bit LSB:*** Clear the 5 bits LSB of all pixels of stego image (S2). The first to

fifth LSB are set to 0 and then whole pixel value is again converted to integer.

3. ***Edge Detection:*** Perform the Canny edge detectionon S2 and save the results to E_c. Also, perform the Sobel edge detection on S2 and store the result in E_s.
4. ***Hybrid Edge Detection:*** The hybrid edges (E_h) are obtained by taking the OR operation of E_c and E_s . Further, morphological dilation is applied to minimize the noise in hybrid edges and enhance the edges.
5. ***Edge and Non-Edge pixel Decision:*** The pixels of stego image (S1) are divided into edge pixels and non-edge pixels based on hybrid edges.
6. ***Extraction of LSB:*** Extract x bits LSB from edge pixel area and y bits LSB from non-edge pixels area of stego image.
7. ***ASCII to Binary Conversion:*** Group the every 8 bits of extracted bits converts it to ASCII value.
8. ***Secrete Image Extraction:*** Finally, the secrete image is extracted by resizing the ASCII values to M×N dimensions.

III. Experimental Results and Discussion

The proposed system is simulated using MATLAB software on Windows platform using personal computer having core i3 processor and 8 GB RAM. We have selected four cover images and four message images for the performance evaluation of the proposed system as shown in Fig.3. We have selected the medical image, satellite image, natural image, portrait image as sample images for cover image and secrete image. The dimensions of cover image are set to 256×256.

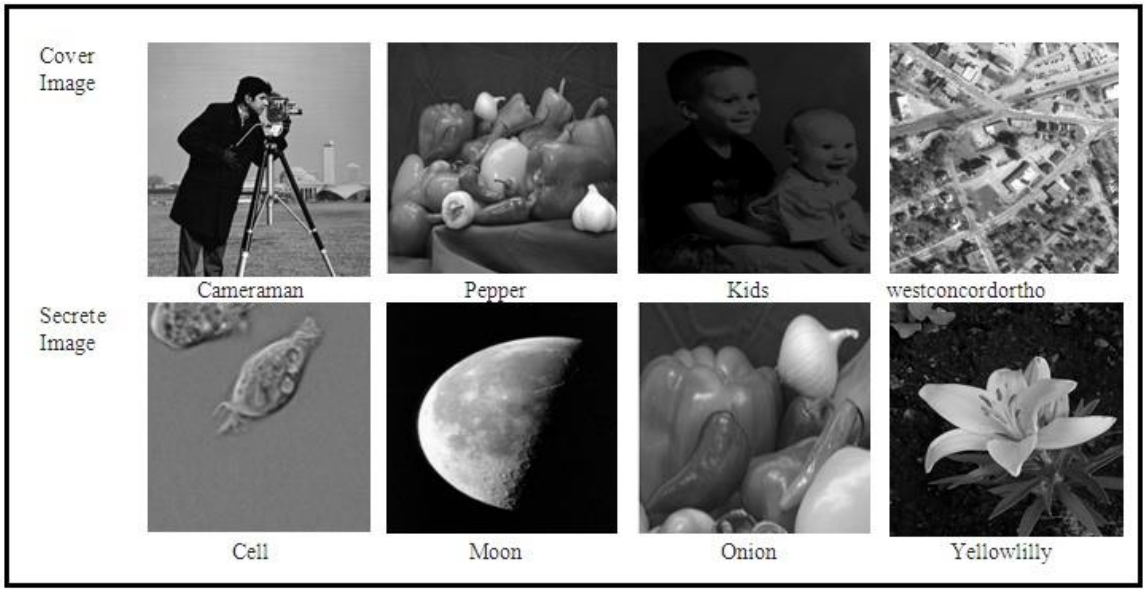

Fig. 3 Sample cover and secrete images

We have evaluated the effectiveness of the proposed system for different payload capacities based on Mean Square Error (MSE), Peak Signal to Noise Ratio (PSNR), Structural Similarity Index Metrics (SSIM), Cross-correlation (XCORR), and Universal Image Quality Index (UQI).

MSE and PSNR is used to measure the overall quality of the cover image after steganography which can be given using Eq. 1 and Eq. 2.

$$MSE = \frac{1}{mn}\sum_{i=0}^{m-1}\sum_{j=0}^{n-1}[I(i,j) - N(i,j)]^2 \quad (1)$$

$$PSNR = 10.log_{10}\left(\frac{2^B - 1}{MSE}\right) \quad (2)$$

Where, $I(i,j)$ *and* $N(i,j)$ are cover image and stego image, *m*and *n*stands for rows and columns of images, and *B*is number of bits per sample.

The SSIM provides the information about structural content of the stego image and cover image which can be given using Eq. 3.

$$SSIM(x,y) = \frac{(2\mu_x\mu_y + c_1)(2\sigma_{xy} + c_2)}{(\mu_x^2 + \mu_y^2 + c_1)(\sigma_x^2 + \sigma_y^2 + c_2)} \quad (3)$$

Where, μ_x , μ_y stands for average of cover image and stegoimage, μ_x^2 , μ_y^2 stands for variance of cover image and stegoimage, σ_{xy} is covariance of cover and stegoimage, $c_1 = (k_1 L)^2$ and $c_2 = (k_2 L)^2$ weak denominator stabilizer, L is dynamic range of cover image pixels (up to 255 for 8 bit image), $k_1 = 0.01$ and $k2 = 0.03$. SSIM value lies in between 0 and 1. Higher value of SSIM shows superior quality of cover image after data hiding. SSIM is calculated over the window size (x,y) of 5×5 pixels.

Fig. 4 Dilated hybrid images for different cover images

The various dilated hybrid edges are shown in Fig. 4 that shows the noteworthy improvement in the edge pixel area after dilation process. The hybrid edges combines the edges obtained from Sobel and Prewitt edge detector. Dilation process increases the thickness of the edge and hence helps to improve the payload capacity of the image.

Table 1-4 provides the experimental results of image steganography by considering different pair of cover and secrete image for variable payload capacity. It is observed that hybrid edge detection algorithm based on Sobel-Prewitt gives better performance compared to hybrid edge detection based on Canny-Sobel, Canny-Roberts, Canny-Prewitt, Sobel-Robert, and Robert-Prewitt.

Table 1: Performance of proposed approach (Cover Image: Cameraman, Secrete Image: Cell)

Payload Capacity	Edge Detector 1	Edge Detector 2	No of Edge Pixels	MSE	PSNR	SSIM	XCORR	UQI
1024	Canny	Sobel	22550	0.055527	60.7198	0.34498	0.99998	1
	Canny	Robert	22233	0.053986	60.842	0.3452	0.99998	0.99998
	Canny	Prewitt	22543	0.055756	60.7019	0.34526	0.99998	1

	Sobel	Robert	9511	0.05394	60.8457	0.35256	0.99998	1
	Sobel	Prewitt	8596	0.05368	60.8666	0.36605	0.99995	1
	Robert	Prewitt	9520	0.056015	60.6818	0.354	0.99995	0.99987
4096	Canny	Sobel	22550	0.2261	54.6217	0.35419	0.9999	0.9999
	Canny	Robert	22233	0.22621	54.6197	0.35109	0.99991	0.99967
	Canny	Prewitt	22543	0.22017	54.7372	0.37821	0.99991	1
	Sobel	Robert	9511	0.13528	56.8523	0.35496	0.99991	0.99934
	Sobel	Prewitt	8596	0.12038	57.3594	0.38033	0.99993	0.99987
	Robert	Prewitt	9520	0.13284	56.9314	0.36254	0.99991	0.99988
16384	Canny	Sobel	22550	0.31744	53.1481	0.34876	0.99989	0.99955
	Canny	Robert	22233	0.31479	53.1846	0.36624	0.9999	0.99976
	Canny	Prewitt	22543	0.31421	53.1926	0.35325	0.99989	0.99985
	Sobel	Robert	9511	0.1255	57.1782	0.36472	0.99991	0.99978
	Sobel	Prewitt	8596	0.11316	57.6279	0.3719	0.99993	0.99994
	Robert	Prewitt	9520	0.12781	57.0992	0.36813	0.99991	0.9997

Table 2: Performance of proposed approach (Cover Image:Pepper, Secrete Image: Moon)

Payload Capacity	**Edge Detector 1**	**Edge Detector 2**	**No of Edge Pixels**	**MSE**	**PSNR**	**SSIM**	**XCORR**	**UQI**
1024	Canny	Sobel	22101	0.13641	56.8162	0.45653	1	1
	Canny	Robert	21712	0.13744	56.7838	0.45692	1	1
	Canny	Prewitt	22061	0.13574	56.8377	0.45635	1	1
	Sobel	Robert	8445	0.13416	56.8887	0.45722	1	1
	Sobel	Prewitt	7954	0.13538	56.8494	0.45784	1	1
	Robert	Prewitt	8434	0.13599	56.8298	0.45867	1	1
4096	Canny	Sobel	22101	0.53134	50.9111	0.44279	1	0.99999
	Canny	Robert	21712	0.5262	50.9533	0.44307	1	0.99999
	Canny	Prewitt	22061	0.53154	50.9094	0.44369	1	0.99999
	Sobel	Robert	8445	0.25879	54.0353	0.45664	1	1
	Sobel	Prewitt	7954	0.24867	54.2085	0.45734	1	1
	Robert	Prewitt	8434	0.26237	53.9756	0.45676	1	1
16384	Canny	Sobel	22101	0.73627	49.4944	0.42994	1	0.99999
	Canny	Robert	21712	0.72011	49.5908	0.43056	1	0.99998
	Canny	Prewitt	22061	0.7319	49.5203	0.42993	1	0.99999
	Sobel	Robert	8445	0.33339	52.9353	0.45537	1	0.99999
	Sobel	Prewitt	7954	0.31638	53.1628	0.45633	1	0.99999
	Robert	Prewitt	8434	0.33424	52.9242	0.45626	1	0.99999

Table 3: Performance of proposed approach (Cover Image: Kids, Secrete Image: Onion)

Payload Capacity	Edge Detector 1	Edge Detector 2	No of Edge Pixels	MSE	PSNR	SSIM	XCORR	UQI
1024	Canny	Sobel	15168	0.30751	53.2862	0.59141	0.99989	0.99971
	Canny	Robert	15419	0.31233	53.2186	0.59099	0.99988	0.99946
	Canny	Prewitt	14472	0.3028	53.3533	0.59422	0.9999	1.0003
	Sobel	Robert	12172	0.26491	53.9339	0.5952	0.99992	0.99975
	Sobel	Prewitt	7954	0.24867	54.2085	0.45734	1	1
	Robert	Prewitt	15168	0.31973	53.1169	0.59167	0.99989	1.0065
4096	Canny	Sobel	15453	0.31303	53.2089	0.58978	0.99988	1.0009
	Canny	Robert	15168	0.30751	53.2862	0.59141	0.99989	0.99971
	Canny	Prewitt	15419	0.31233	53.2186	0.59099	0.99988	0.99946
	Sobel	Robert	14472	0.2997	53.398	0.59281	0.99989	0.99996
	Sobel	Prewitt	12172	0.25526	54.0949	0.59706	0.99993	0.99971
	Robert	Prewitt	14496	0.29572	53.4561	0.59381	0.99989	0.99955
16384	Canny	Sobel	15453	0.32259	53.0783	0.59242	0.99988	1.0013
	Canny	Robert	15168	0.31973	53.1169	0.59167	0.99989	1.0065
	Canny	Prewitt	15419	0.32317	53.0705	0.59256	0.99988	0.99968
	Sobel	Robert	14472	0.3028	53.3533	0.59422	0.9999	1.0003
	Sobel	Prewitt	12172	0.26491	53.9339	0.5952	0.99992	0.99975
	Robert	Prewitt	14496	0.3107	53.2414	0.59245	0.99989	1

Table 4: Performance of proposed approach (Cover Image: Westconcordortho , Secrete Image: Yellolilly)

Payload Capacity	Edge Detector 1	Edge Detector 2	No of Edge Pixels	MSE	PSNR	SSIM	XCORR	UQI
1024	Canny	Sobel	39115	0.10767	57.844	0.0066495	1	1
	Canny	Robert	38384	0.10683	57.878	0.006921	1	1
	Canny	Prewitt	38963	0.10616	57.9054	0.0066499	1	1
	Sobel	Robert	14117	0.10365	58.009	0.0070103	1	1
	Sobel	Prewitt	13712	0.10362	58.0103	0.0070222	1	1
	Robert	Prewitt	13285	0.10393	57.9975	0.0070026	1	1
4096	Canny	Sobel	39115	0.41228	52.0129	0.0066531	1	1
	Canny	Robert	38384	0.41553	51.9788	0.0065634	1	1
	Canny	Prewitt	38963	0.41298	52.0055	0.0064982	1	1
	Sobel	Robert	14117	0.3571	52.6369	0.0068089	1	1
	Sobel	Prewitt	13285	0.33514	52.9125	0.0068164	1	1
	Robert	Prewitt	13712	0.3441	52.7979	0.0067693	1	1
16384	Canny	Sobel	39115	1.0273	48.0476	0.0058119	1	0.99999

	Canny	Robert	38384	1.0176	48.0889	0.006031	1	1
	Canny	Prewitt	38963	1.0303	48.0351	0.005966	1	0.99999
	Sobel	Robert	14117	0.40865	52.0513	0.0067331	1	1
	Sobel	Prewitt	13285	0.38803	52.2761	0.006863	1	1
	Robert	Prewitt	13712	0.39476	52.2015	0.0069407	1	1

IV. Conclusions and Future Scope

Thus, this paper present image hiding based on improved steganography based on dilated hybrid edge detection and LSB steganography technique. The proposed hybrid edge detection based on Sobel-Prewitt provides better results for payload capacity of 1024. It has shown significant improvement in the different evaluation metrics such as MSE, PSNR, SSIM, XCORR and UQI for higher payload capacity. In future, the performance of the proposed image steganography approach can be evaluated for the various noisy conditions and for higher payload capacity. The colorimage steganography is challenging and time consuming approach, in future the existing approach can be extended for color image steganography.

References

1. Singh, Laxmanika, Amit Kumar Singh, and Pradeep Kumar Singh. "Secure data hiding techniques: a survey." Multimedia Tools and Applications 79, no. 23 (2020): 15901-15921.
2. Bender, Walter, Daniel Gruhl, Norishige Morimoto, and Anthony Lu. "Techniques for data hiding." IBM systems journal 35, no. 3.4 (1996): 313-336.
3. Singh, AMIT KUMAR. "Data hiding: current trends, innovation and potential challenges." ACM Transactions on Multimedia Computing, Communications, and Applications (TOMM) 16, no. 3s (2020): 1-16.
4. Dixit, Pooja, Avadhesh Kumar Gupta, Munesh Chandra Trivedi, and Virendra Kumar Yadav. "Traditional and hybrid encryption techniques: a survey." In Networking communication and data knowledge engineering, pp. 239-248. Springer, Singapore, 2018.
5. Mota, Aquino Valentim, Sami Azam, BharanidharanShanmugam, Kheng Cher Yeo, and Krishnan Kannoorpatti. "Comparative analysis of different techniques of encryption for secured data transmission." In 2017 IEEE International Conference on Power, Control, Signals and Instrumentation Engineering (ICPCSI), pp. 231-237. IEEE, 2017.
6. Hussain, Mehdi, Ainuddin Wahid Abdul Wahab, Yamani Idna Bin Idris, Anthony TS Ho, and Ki-Hyun Jung. "Image steganography in spatial domain: A survey." Signal Processing: Image Communication 65 (2018): 46-66.
7. R. Das and T. Tuithung, ‘‘A novel steganography method for image based on Huffman encoding,’’ in Proc. 3rd Nat. Conf. Emerg. Trends Appl. Comput. Sci., Mar. 2012, pp. 14–18.
8. A. Singh and H. Singh, ‘‘An improved LSB based image steganography technique for RGB images,’’ in Proc. IEEE Int. Conf. Electr., Comput. Commun. Technol. (ICECCT), Mar. 2015, pp. 1–4.
9. Z. Qu, Z. Cheng, W. Liu, and X. Wang, ‘‘A novel quantum image steganography algorithm based on exploiting modification direction,’’ Multimedia Tools Appl., vol. 78, no. 7, pp. 7981–8001, Apr. 2019.
10. S. Wang, J. Sang, X. Song, and X. Niu, ‘‘Least significant qubit (LSQb) information hiding algorithm for quantum image,’’ Measurement, vol. 73, pp. 352–359, Sep. 2015.
11. N. Patel and S. Meena, ‘‘LSB based image steganography using dynamic key cryptography,’’ in Proc. Int. Conf. Emerg. Trends Commun. Technol. (ETCT), Nov. 2016, pp. 1–5.
12. O. Elharrouss, N. Almaadeed, and S. Al-Maadeed, ‘‘An image steganography approach based on k-least significant bits (k-LSB),’’ in

Proc. IEEE Int. Conf. Informat., IoT, Enabling Technol. (ICIoT), Feb. 2020, pp. 131–135.

13. M. V. S. Tarun, K. V. Rao, M. N. Mahesh, N. Srikanth, and M. Reddy, ‘‘Digital video steganography using LSB technique,’’ Red, vol. 100111, Apr. 2020, Art. no. 11001001.
14. S. S. M. Than, ‘‘Secure data transmission in video format based on LSB and Huffman coding,’’ Int. J. Image, Graph. Signal Process., vol. 12, no. 1, p. 10, 2020.
15. M. B. Tuieb, M. Z. Abdullah, and N. S. Abdul-Razaq, ‘‘An efficiency, secured and reversible video steganography approach based on lest significant,’’ J. Cellular Automata, vol. 16, no. 17, Apr. 2020.