2021 24th International Conference on Computer and Information Technology (ICCIT), 18-20 December, 2021

Image Steganography System based on Hybrid Edge Detector

Habiba Sultana

Department of Computer Science & Engineering,
Jatiya Kabi Kazi Nazrul Islam University,
Trishal, Mymensingh, Bangladesh.
E-mail: srity.cse@gmail.com.

A H M Kamal

Department of Computer Science & Engineering,
Jatiya Kabi Kazi Nazrul Islam University,
Trishal, Mymensingh, Bangladesh.
E-mail: kamal@jkkniu.edu.bd.

2021 24th International Conference on Computer and Information Technology (ICCIT) | 978-1-6654-9435-9/21/$31.00 ©2021 IEEE | DOI: 10.1109/ICCIT54785.2021.9689777

***Abstract*—In the field of image steganography, edge detection based implantation methods play vital rules in providing stronger security of hided data. In this arena, researcher applies a suitable edge detection method to detect edge pixels in an image. Those detected pixels then conceive secret message bits. A very recent trend is to employ multiple edge detection methods to increase edge pixels in an image and thus to enhance the embedding capacity. The uses of multiple edge detectors additionally boost up the data security. Like as the demand for embedding capacity, many applications need to have the modified image, i.e., stego image, with good quality. Indeed, when the message payload is low, it will not be a better idea to finds more local pixels for embedding that small payload. Rather, the image quality will look better, visually and statistically, if we could choose a part but sufficient pixels to implant bits. In this article, we propose an algorithm that uses multiple edge detection algorithms to find edge pixels separately and then selects pixels which are common to all edges. This way, the proposed method decreases the number of embeddable pixels and thus, increases the image quality. The experimental results provide promising output.**

Keywords—steganography; edge detector; LSB method; cover media; stego media.

I. INTRODUCTION

The word steganography comes from a Greek word that has two parts, i.e. 'steganos' means covered or concealed and 'graphy' means writing, and together it means covered writing or secret writing. It is an approach of hiding information in a media, known as cover media. As a cover media, steganographic algorithms use text, audio, video, image, etc. Steganographic methods implant secret message into a target media for ensuring security of implanted message. To retrieve the same from the used media at later on, an extraction algorithm essentially works. Thus, the embedding and extraction methods are two separate algorithms those work to hide and extract data, respectively, and these two methods comprise the whole steganographic process.

Various fields, such as medical safety, terrorism, hacking, intellectual property offenses, corporate espionage, indexing of video mail, military application, automatic monitoring of radio advertisements, protection against malware, etc., use steganographic processes,[1]. It is a flexible but secured way of communicating information. For clandestine steganographic communication, the sender sends a secret message implanting it into a cover media using an embedding technique. The media with implanted secret is called stego media. Sometime, the embedding algorithm associates a secret key to improve the security of the implanted data. That secret key is called stego key. The receiver performs a reverse task to extract the secret from the stego media.

To find the existence of stego contents in a media steganalyses are applied. However, steganography resists attack by its complex nature. In steganography, attackers cannot easily retrieve the secret message due to its length in a cover media, embedding or extracting technique, unknown stego key, pre and post processed of data and media, additional information, etc. The evaluation parameters of steganography system are the amount of maintaining virginity of cover media, payload or capacity of implanted data, robustness and security of hidden data, and some computational complexity. Virginity of cover media is measured by peak-signal-to-noise-ratio (PSNR)or structural similarity index matrix(SSIM). These are also known as visual quality measuring parameters when the media is visible, e.g., image. Payload states the number of bits that the system implants in the media and capacity says the statistic of how many bits are implanted per media contents. Nevertheless, commonly used performance measuring parameters are payload and visual quality of cover media.

When the steganographic methods use images as their carrier of secrets, it is called image steganography; and classified as spatial domain and frequency or transform domain. This research focused on image steganography in the spatial domain.

The implantation technique embeds each secret message unit into pixel values of a cover image. least significant bit (LSB) substitution [2-5], pixel value differencing (PVD) [6-10], histogram shifting [11-13], texture based method, pixel intensity-based method, random pixel embedding method, pixel values [15-16], transformed coefficients of pixel values [17], neighbor pixel differences [6-8], and prediction errors [13] and edge-based data embedding method [2-8,14,18-19] are renown embedding techniques.

Based on the implantation techniques, steganography can be classified as reversible and irreversible. In reversible steganography, the receiver can recover both the secret message and cover media from stego media [13, 15-16, 20-26]. On the other hand, irreversible steganography does not concentrate to recover the cover media. Only, data extraction is their concerning issue [2-4, 27-28]. These techniques achieve higher embedding capacity with minimum computation time.

Many edge detection based embedding algorithms embed fewer secret message bits into smoothed area and more bits into sharp or edge area of the cover image to

manage better visual quality of stego image [2-4]. The LSB based methods are famous because these degrade lower amount of visual quality and implant more bits into pixels. As the edge pixels carry more bits, if edge detection algorithm can detect more edges and pixels in the edges, the embedding capacity will increase. Barring the concept, recent research [4, 18-19] applies multiple edge detection algorithms in the same cover image to detect edges and then edge pixels separately. The output of every algorithm is a matrices of same size of cover image with values 0 or 1 only where each 0 stands for a non-edge pixel and a 1 indicates an edge pixel. The matrices are called edge matrices. The research next combines the results of matrices by doing OR operation among the position wised contents of these matrices. Finally, OR results are used to label each pixel as edge or non-edge pixels. Though the method improves embedding capacity, it degrades the stego image quality. Moreover, when the requirement of data embedment is small, searching for more edge pixels will not be a smart approach. Then the scheme will implant all secrets in a small area of the image which may lead to a visual degradation. Hence, applying OR operation without analyzing the requirement could not be a good attempt. Additionally, many applications, e.g., embedding at national digital ID card, forensic applications, medical applications, may nottolerate high level of image degradations. Considering the demand of such applications, we propose to apply AND operation instead of OR at edge matrics. This proposal will act as a novel one when the requirement of embedding capacity is not too high and the secrets are embeddable to a cover image through our proposal. Also, one can check whether the secret is embeddable by our proposal or not by applying the steganographic process upto AND operation and counting the edge and non-edge pixels.The method will then distribute the secrets throughout the image, rather than in a portion of it.We also apply chaotic method to encrypt the bits of secrets. Thus, the scheme differs from its base method and enhance its data security.

Contribution of this article:

1. We encrypt secret message bits by a chaotic method.
2. We first apply AND operations among the contents of edge matrics to detect the real edge pixels. Thus, the AND result removes all false likely edge pixels. Therefore, from the perspective of edge-detection based embedding technique, the proposed method is more coherent.
3. If the proposed scheme cannot implant all bits of secret due to its larger size, we suggest to apply OR operation as it was in [19].The technique of embedding data applying OR operation is explained in [19]. We leave that discussion for the reader to read in the stated article.
4. The proposed method enhances the visual quality of stego images in our experiment.

The rest of the paper is organized as follows. Section II provides the details of edge detectors including Sobel, Canny, and hybrid edge detector with related works. Section III narrates our proposed scheme. Section IV presents some experimental results. Finally, section V concludes the article.

II. RELATED WORKS

Vanmathi.C and Prabu.S [2] use a modified fuzzy edge detector to as a policy of their data embedment process. The modified fuzzy edge detector helps in detecting edge pixels. They embed their secret message bits using Least Significant Bit (LSB) substitution to those edge pixels. Additionally, a chaotic method is used to encrypt the desired message at their pre-embedment stage. The scheme degrades the visual quality of image with the uses of more LSBs. However, large degradation increases the threatening factor of implanted secrets.

The scheme in [18-19] similarly applies edge detection method at their embedding phase to enhance the security level of the implanted secrets. The scheme hides edge information along with the secret in the cover image. As a consequence, the embedding capacity decreases notably. To increase the embedding space, Bai [3] proposes a novel steganography scheme that uses edge detection method as well. They overcome the problem of storing edge information. The method first clears 5 LSBs from the every of cover pixels. Thereafter, they apply multiple edge detectors like Sobel, canny, and fuzzy separately to find the edge images. They make a final edge image combining these edge images by exclusive-OR(XOR) operation. Based on that edge image, the cover image is divided into the edge and non-edge area. The scheme implants x bits and y bits into these edge and non-edge pixels using the LSB method.

Another research, conducted by Setiadi [4], propose a steganography system that applies dilated hybrid edge detection. This method clears 5 bits of LSBs from every pixel of the copied cover image. Next, the scheme individually applies sobel and canny edge detector and then combines these two edge images by XOR operator. To increase the number of edge pixels, a dilated operator with mask of 3 x 3 structure is used. Like then previous one, the scheme divides the pixels into edge and non-edge group. At the same time, the scheme converts the secret message of texts into ASCII and thereafter ASCII to binary. The method embeds x and y bits of secrets into edge and non-edge pixel of the cover image, respectively. The scheme significantly destroys the visual quality of image.

III. PROPOSED WORK

The main idea of this research is to yield better stego image quality. Mainly, it works well when the length of secret is very small or the embedding system works with small messages only, e.g., hiding personal information to his/her national digital ID card, implanting account balance to one's debit card. To decrease the cracking probability, secret data is encrypted by chaotic method. As the previous scheme, implants more bits to edge pixels than non-edge pixels, it is obviously a desired condition to increase the number of edge pixels to meet the demand for high payload. The inverse is true when the demanded embedding payload is small. That is, if the demanded payload is small, that would be better to minimize the number of edge pixels. That

then will distribute the implanted secret bits over the cover image. To achieve that, we apply multiple edge detectors to the cover image at the pre-embedding stage. Each detector produces an edge image separately. We compute the AND values of the contents of these edge images. The resultant edge image is used to classify edge and non-edge pixels of cover image. The rest, i.e., the embedding method, is the same of [3] and [4]. A pictorial view of the proposed embedding process is shown in Fig. 1, while the secret extraction process is shown in Fig. 2. The embedding process consists of three steps, as shown in following:

Step 1:

i. Create a text file where secret messages are stored.
ii. Generate a key using a chaotic method and encrypt the secret message with this key.
iii. Convert the secret message into binary.

Step 2:

i. Read a cover image and then take a copy of it.
ii. Clear 5-bits LSB of each pixel of the copied cover image.
iii. Apply, separately, multiple different edge detection methods. Each of them will produce an edge image. Apply AND operation among the edge images. The ANDed result will generate a single edge image.
iv. Based on resultant edge image, original cover image pixels are classified into edge and non-edge pixels.

Step 3:

i. Embed the number of x bits of secrets in edge pixels and y bits of secrets in non-edge pixels.
ii. The conceived image is called stego image.

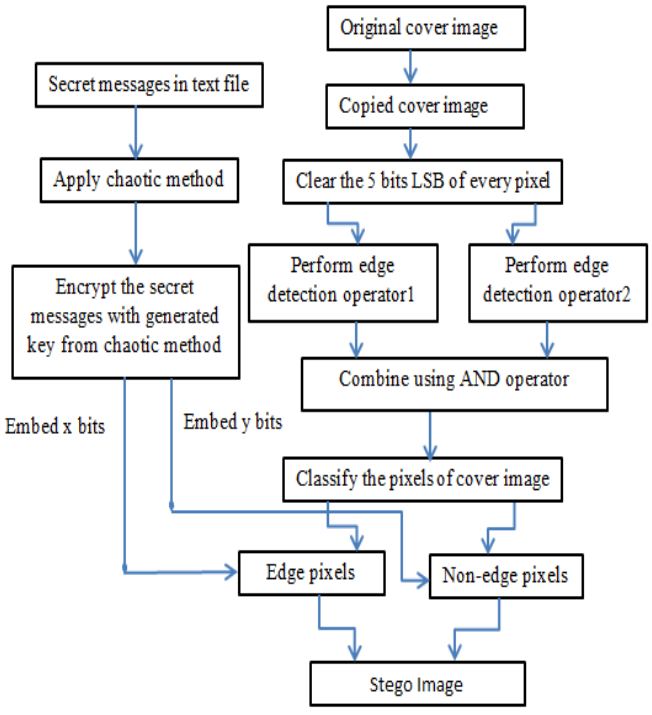


Fig. 1. Embedding procedure of proposed method

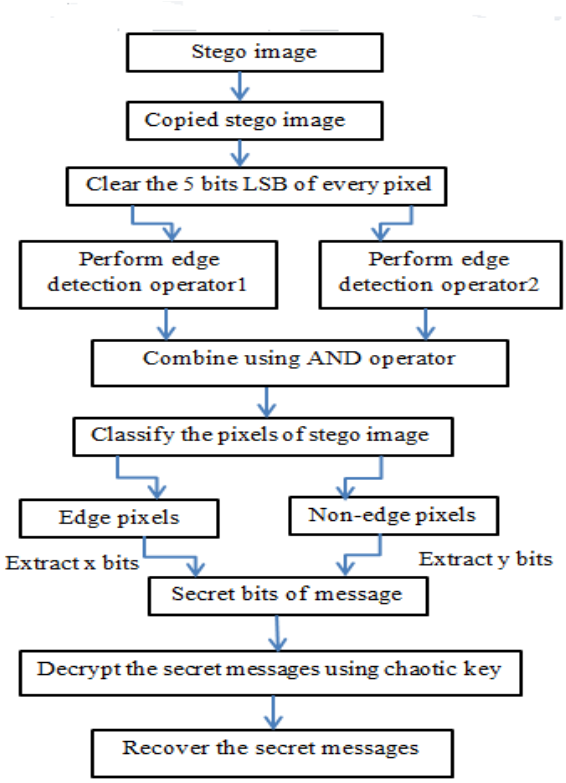


Fig. 2. Extracting procedure of proposed method

Fig. 2 depicts the data extraction procedure of the proposed scheme. Data extraction procedure is described briefly in the following:

1. Read the stego image and make a copy of it.
2. Clear 5 bit LSBs of all pixel values in the copied stego image.
3. Separately apply two different edge detection algorithms. The edge detection algorithms will generate similar edge images as of embedding phase. Apply AND operation among the values of edge images. The ANDed image is the resultant edge image.
4. That edge image is used to identify the edge and non-edge pixels in the stego imaged.
5. Extract x bit and y bit of LSBs from the edge and non-edge related stego pixels, respectively.
6. These extracted LSBs are the secret message bits. Now decrypt those using the chaotic method to retrieve the original message.

IV. Experimental Results and Discussion

The results of the proposed scheme are simulated in MATLAB 2017 on WINDOWS 7. The experimented images are taken from BOSS image dataset. Moreover, some popular sample cover images which are frequently used in researches are also tested. Sample images are shown in figure 3.

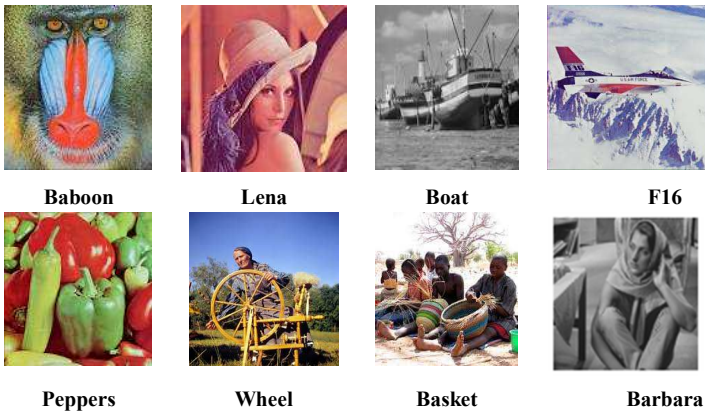


Fig. 3. Test images

In our experiment, we apply renowned Canny and Sobel edge detection method to detect the edge pixels in the 5-bits cleared image. The results are shown in Figure 4 as edge images. These are, indeed, binary images. Each pixel with value 1 in edge image indicates an edge pixel, while the 0 represents a non-edge pixel.

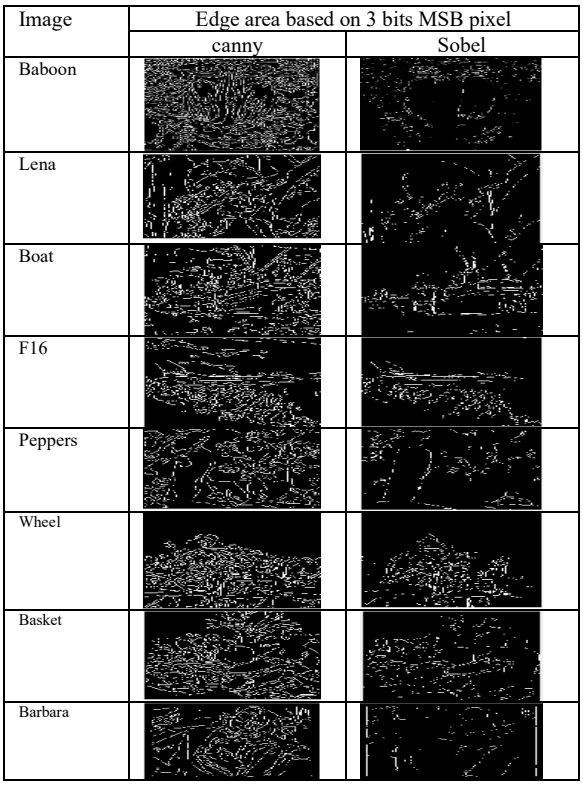


Fig. 4. Edge area generated by canny and sobel detector in modified cover image.

Based on that edge image, we implanted x-number of bits in edge pixel and y-number of bits in non-edge pixels. Thus, (x,y)=(2,1) means that 2-bits are implanted in each edge pixel and 1-bit is embedded in each non-edge pixel by LSB substitution method. In fact, we experimented for (x,y)= {(2,1), (3,1), (3,2), (4,1),(4,2),(4,3)}. However, for the convenient, we have shown the results only for (2,1) and (3,1). Measured payloads are tabulated in Table 1. The table shows that Setiadi, i.e., [4] gives highest payload. It is obvious, because, that method increases the number of edge pixels by dilation operation. Though Bai [3] does not uses dilation operation, they use OR operation among edge images. Consequently, they produce more number of edge pixels than the proposed method, however, less than Setiadi. Thus, Bai is the second one that embeds more bits. The proposed method embeds the lowest bits in the same images. As our objective is to propose a good algorithm for producing better visual quality of stego image while implanting small sized message, the embedding payload is not very concerning issue to our research. Moreover, the proposed scheme implants 66840 or more bits in an image of size 255 x255, which is enough to comprise a small sized image.

We, therefore, concentrate on image quality. Very two famous method measuring image quality is to measure peak-signal-to-noise-ratio (PSNR) and structural similarity index measurement (SSIM).

The PSNR is measured by the following equation (1).

$$PSNR = 10log10(\frac{255^2}{MSE}) \qquad (1)$$

Where MSE, i.e., mean square error, is defined by

$$MSE = \sum_{i=1}^{W\times H} \frac{(St - A)^2}{W \times H}$$

In the MSE equation, St and A stand for stego and cover images, respectively.

Similarly, SSIM values are computed by equation (2).

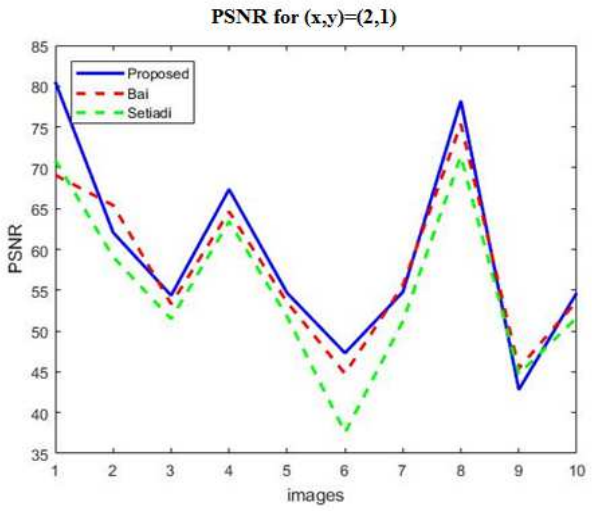
$$SSIM = \frac{(2\mu_c\mu_s + C_1)(2\sigma_{cs} + C_2)}{(\mu_c{}^2 + \mu_s{}^2 + C_1)(\sigma_c{}^2 + \sigma_s{}^2 + C_2)}$$

Where μ_c, μ_s and σ_c, σ_s are the mean pixel values and variance for the cover and stego image respectively. σ_{cs} is the covariance between the cover and stego image, C_1 and C_2 are the constants.

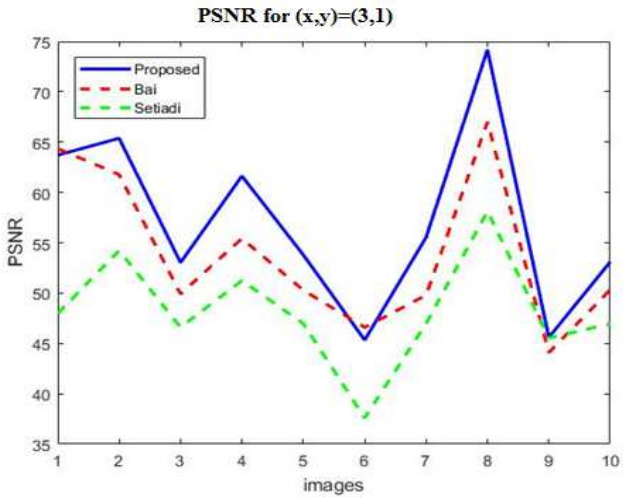
The PSNR values are demonstrated in Figure 5. Figure 5(a) depicts the PSNR values for (x,y)=(2,1) and the PSNRs for (x,y)=(3,1) in Figure 5(b). Both figure states that the proposed method shows dominating results in about all the images.

Table 1: Statistics of Payload

JPG Image	Methods					
	(x,y)=(2,1)			(x,y)=(3,1)		
	Proposed	Bai	Setiadi	Proposed	Bai	Setiadi
F16	67626	72630	85272	69716	79724	105008
babon	66840	78405	99521	68144	91274	133506
basket	67639	74063	88769	69742	82590	112002
boat	67183	74192	90120	68830	82848	114704
brbra	66872	72996	85821	68208	80456	106106
lena	66988	73341	86883	68440	81146	108230
livingroom	67176	75120	92921	68816	84704	120306
pepper	67023	72972	86175	68510	80408	106814
walkbridge	67180	77010	96658	68824	88484	127780
wheel	67802	73228	87249	70068	80920	108962



(a)



(b)

Fig. 5. PSNR values for (a) (x,y)=(2,1) and (b) (x,y)=(3,1)

Table 2: Statistics of SSIM

JPG Image	Methods					
	(x,y)=(2,1)			(x,y)=(3,1)		
	Proposed	Bai	Setiadi	Proposed	Bai	Setiadi
F16	0.9954	0.9951	0.9944	0.9955	0.9922	0.9886
Babon	0.9736	0.9723	0.9694	0.9736	0.9655	0.9560
Basket	0.9984	0.9982	0.9979	0.9983	0.9974	0.9955
Boat	0.9963	0.9953	0.9939	0.9961	0.9911	0.9836
Barbara	0.9973	0.9968	0.9958	0.9973	0.9944	0.9900
Lena	0.9936	0.9922	0.9873	0.9928	0.9877	0.9758
Livingroom	0.9979	0.9971	0.9962	0.9975	0.9949	0.9889
Pepper	0.9932	0.9925	0.9911	0.9931	0.9886	0.9823
Walkbridge	0.9984	0.9982	0.9974	0.9985	0.9963	0.9927
Wheel	0.9969	0.9968	0.9965	0.9968	0.9961	0.9947

Table 2 records the SSIM values of our experiments. That table states that proposed method gives better SSIM values. Thus, when the size of to be embedded message, e.g., less than 66800bits, is small, Fig. 5 and Table 2 suggest that the proposed method would be better to use in data hiding application to get better image quality.

V. CONCLUSION

In this research, we proposed an edge detection based image steganography where various edge detectors are used to create resultant edge image. The resultant image helps us in classifying edge and non-edge pixels in the cover image. We apply AND operation among the different edge images to produce the resultant edge image. The resultant edge image minimizes number of edge pixels in the cover image. As the proposed and competing schemes embeds more bits in edge pixels and less in non-edge pixels, the proposed one generate a stego image that is more close to cover image. The image quality thus remains better by the proposed scheme. Therefore, while embedding small sized secret, the proposed method will be a better choice to the data hiding applications.

In our future work, we would like to apply a predictor in the cover image. Next, we would apply edge detector to absolute valued prediction errors to enhance the embedding payload as well. We hope that then the scheme will overcome the limitation of small sized data embedment.

ACKNOWLEDGMENT

This research was financially supported by ICT division of Ministry of Post, Telecommunication and Information Technology of Bangladesh and was also supported by the Department of Computer Science & Engineering, Jatiya Kabi Kazi Nazrul Islam University.

REFERENCES

[1] H. Sultana, "A study on steganography and steganalysis", International Journal of Scientific & Engineering Research 9(12), ISSN 2229-5518, 2018.

[2] C.Vanmathi and S. Prabu, "Image Steganography Using Fuzzy Logic and Chaotic for Large Payload and High Imperceptibility", International Journal of Fuzzy Systems, 2017. https://doi.org/10.1007/s40815-017-0420-0 .

[3] J.Bai, C.-Chen Chang, T.-Son Nguyen, C. Zhu and Y.Liu, "A high payload steganographic algorithm based on edge detection" Displays, 46, 42-51, 2017. https://doi.org/10.1016/j.displa.2016.12.004 .

[4] D.R.I.M. Setiadi, "Improved payload capacity in LSB image steganography uses dilated hybrid edge detection", Journal of King Saud University- Computers and Information Sciences, 2019. https://doi.org/10.1016/j.jksuci.2019.12.007 .

[5] S.Sun, "A Novel edge based image steganography with 2^k correction and Huffman encoding", Information Processing Letters, 2015.https://doi.org/10.1016/j.ipl.2015.09.016 .

[6] G.Swain, "Adaptive pixel value differencing steganography using both vertical and horizontal edges", Multimedia Tools and Applications. 75, 13541-13556, 2015. https://doi.org/10.1007/s11042-015-2937-2.

[7] A.Prodhan, K.R. Sekhar and G.Swain, "Adaptive PVD Steganography Using Horizontal, Vertical and Diagonal Edges in Six-Pixel Blocks" Security and Communication Networks, 2017. https://doi.org/10.1155/2017/1924618 .

[8] S.Kumar, A.Singh and M. Kumar, "Information hiding with adaptive steganography based orn novel fuzzy edge identification", Defence Technology, 2018. https://doi.org/10.1016/j.dt.2018.08.003 .

[9] M.Tang, S.Zeng, X.Chen, J.Hu and Y.Du, "An adaptive image steganography using AMBTC compression and interpolation

technique", Optik. 127, 471-477, 2016. https://doi.org/10.1016/j.ijleo.2015.09.216 .

[10] W.Hong and T.-S.Chen, "A Novel Data Embedding Method Using Adaptive Pixel Pair Matching", IEEE Transactions on Information Forensics and Security, 2012. https://doi.org/10.1109/TIFS.2011.2155062 .

[11] H.Sultana, A H M.Kamal and M.M.Islam, "Enhancing the robustness of visual degradation based HAM reversible data hiding", Journal of Computer Science,12(2), 88-97, 2016.

[12] S.Ong, K.Wong and K.Tanaka,"A Scalable Reversible Data Embedding Method with progressive quality degradation functionality", Signal Processing-Image Communication, 2013. https://doi.org/10.1016/j.image.2013.09.001.

[13] W.Hong, "Adaptive reversible data hiding method based on error energy control and histogram shifting", Optics Communications. 285, 101-108, 2011. https://doi.org/10.1016/j.optcom.2011.09.005 .

[14] H.Al-Dmour and A.Al-Ani, "A steganography embedding method based on edge identification and XOR coding", Expert Systems With Applications. 46, 293-306, 2016. https://doi.org/10.1016/j.eswa.2015.10.024 .

[15] H.Yao, C.Qin, Z.Tang and Y.Tian, "Improved dual-image reversible data hiding method using the selection strategy of shiftable pixels' coordinates with minimum distortion", Signal Processing. 135, 26-35, 2016. https://doi.org/10.1016/j.sigpro.2016.12.029 .

[16] S.Yi and Y.Zhou, "Binary – block embedding for reversible data hiding in encrypted images", Signal Processing, 133, 40-51, 2017. https://doi.org/10.1016/j.sigpro.2016.10.017 .

[17] P.W.Adi, F.Z.Rahmanti and N.A.Abu, "High Quality Image Steganography on Integer Haar Wavelet Transform Using Modulus Function", IEEE, 2015 International Conference on Science in Information Technology (ICSITech), 2015. https://doi.org/10.1109/ICSITech.2015.7407781 .

[18] W.-J.Chen, C.-C.Chang and T.H.N.Le, "High payload steganography mechanism using hybrid edge detector", Expert Syst. Appl. 37, 3292-3301, 2010. https://doi.org/10.1016/j.eswa.2009.09.050 .

[19] H.W.Tseng and H.S.Leng, "High-payload block-based data hiding scheme using hybrid edge detector with minimal distortion", IET Image Process. 8, 647-654, 2014.

[20] A. H. M. Kamal and M. M. Islam, "Enhancing embedding capacity and stego image quality by employing multi predictors", Journal of Information Security and Applications . 32, 59-74, 2017.

[21] A. H. M. Kamal and M. M. Islam, "Boosting up the data hiding rate through multi cycle embedment process" Journal of Visual Communication and Image Representation. 40, 574-588, 2016.

[22] A. H. M. Kamal and M. M. Islam, "Capacity improvement of reversible data hiding scheme through better prediction and double cycle embedding process" 2015 IEEE International Conference on Advanced Networks and Telecommuncations Systems (ANTS). IEEE, 2015.

[23] A. H. M. Kamal and M. M. Islam, "An image distortion-based enhanced embedding scheme" Iran Journal of Computer Science. 1.3 175-186, 2018.

[24] A. H. M. Kamal and M. M. Islam, "A prediction error based histogram association and mapping technique for data embedment" Journal of Information Security and Applications . 48, 102368, 2019.

[25] A. H. M. Kamal, M. M. Islam, and Zehadul Islam, "An embedding technique for smartcard-supported e-healthcare services", Iran Journal of Computer Science. 3.4 , 195-205, 2020.

[26] A. H. M. Kamal and M. M. Islam, "Enhancing the embedding payload by handling the affair of association and mapping of block pixels through prediction errors histogram", 2016 International Conference on Networking Systems and Security (NSysS). IEEE, 2016.

[27] A. H. M. Kamal and M. M. Islam, "Enhancing the performance of the data embedment process through encoding errors", Electronics. 5.4, 79, 2016.

[28] A. H. M. Kamal and M. M. Islam, "Facilitating and securing offline e-medicine service through image steganography", Healthcare technology letters. 1.2, 74-79, 2014.