An Edge Detection Based Reversible Data Hiding Scheme

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.

***Abstract*— Edge detection based embedding techniques are famous for data security and image quality preservation. These techniques use diverse edge detectors to classify edge and non-edge pixels in an image and then implant secrets in one or both of these classes. Image with conceived data is called stego image. It is noticeable that none of such researches tries to reform the original image from the stego one. Rather, they devote their concentration to extract the hidden message only. This research presents a solution to the raised reversibility problem. Like the others, our research, first, applies an edge detector e.g., canny, in a cover image. The scheme next collects *n*-LSBs of each of edge pixels and finally, concatenates them with encrypted message stream. This method applies a lossless compression algorithm to that processed stream. Compression factor is taken such a way that the length of compressed stream does not exceed the length of collected LSBs. The compressed message stream is then implanted only in the edge pixels by *n*-LSB substitution method. As the scheme does not destroy the originality of non- edge pixels, it presents better stego quality. By incorporation the mechanisms of encryption, concatenation, compression and *n*- LSB, the method has enriched the security of implanted data. The research shows its effectiveness while implanting a small sized message.**

***Index Terms*— information hiding; reversible steganography; edge detection; LSB method; SSIM.**

I. INTRODUCTION

ThisIn modern communication world, exchanging of digital information is getting popularity due to its fast-going access. For a secured communication, it is urgent to protect digital information from security intimidation. Among different tech- niques, information hiding and cryptography are the two main procedures for invulnerable communication [1].

Cryptography is a technique of transforming or encrypting the plain text or secret message into an unreadable format called cipher text [2]. Though encryption method destroys the meaning of plain text, these modified texts create curiosity to intruders to look for secrets and break the security [1-2].

The perception of information hiding is to camouflage an important clandestine message in a cover media. The conceived media is then called a stego media. Generally, that stego media is transmitted over a network [1, 3] to a destination end for communicating implanted secrets. Screening the existence of secret information is the main amenities of information hiding techniques over cryptography.

Information hiding can be classified into several research areas such as watermarking, fingerprinting, and steganography [4-7]. Watermarking and fingerprinting both are applied for the purpose of validation and authentication but cannot prevent unauthorized distribution [3].

On the other hand, steganography is able to protect the secret message from illicit access. Steganography is a process of information hiding where the sender implants the secret message in a cover media and thus, forms a stego media. The receiver extracts the secret message from that stego media[8]. Commonly used cover media are image, audio, video; text, etc.. Text steganography lacks security and hiding capacity. Audio and video are complex and large media. Images are light and frequently transmitted media. However, image gives good space to implant large data. Therefore, image steganography has arised as a hastily rising area of research. A steganography system can be assessed using some parameters such as transparency or imperceptibility, robustness, hiding capacity or payload, undetected ability or security, self-recoverability, and some computational complexity [9].

Steganography can be classified into irreversible and reversible technique. In an irreversible process, the receiver can extract only secret messages from the stego media [10-11]. However, these methods are unable to rebuild the cover media from the stego media. On the other hand, reversible schemes both extracts the secrets from the stego media as well as rebuild the cover from that stego without further assistance of sender or any third party [12-19]. Many researchers compress the secret message with necessary information [20] to both reduce the size of to be implanted data and the security of the system. In that case, a lossless [21-22, 25] compressor is needed.

Among various image steganography techniques, edge detection based data implantation methods as famous due to

978-1-6654-5883-2/22/$31.00© 2022 IEEE

2022 IEEE Delhi Section Conference (DELCON) | 978-1-6654-5883-2/22/$31.00 ©2022 IEEE | DOI: 10.1109/DELCON54057.2022.9753404

their security and ability to preserve image quality. Edge detection based schemes first apply an edge detector to identify edge pixels. Then, the schemes implant in only edge pixels or different number of bits in both edge and non-edge pixels. Many researchers embed fewer secret message bits into the smooth or non-edge area and more secret bits into the sharp or edge area of the cover image [20, 26-30] to maintain the visual quality of stego media. In such cases, LSB substitution is a common technique for implanting data. In [20], authors propose a new steganography technique using canny edge detector, 2k correction, and Huffman encoding and coherent bit length. This scheme presents a good visual quality but a low embedding payload. Hybrid edge detector based scheme were observed in [26, 30] to find sharp edges. Due to their nature of computing sharp edges, these schemes achieved poor embedding capacity and low visual quality. In [28], authors proposed a block-based scheme to solve several limitations of [27]. That method is also unable to exploit the full embedding space. To manage better stego quality, authors in [29] employs only edge pixels to conceal data.

None of the edge detection based stated researches, even so far we studied ever, were found which that is a reversible one. That limitation encourages us to look for a solution. Nevertheless, our proposed reversible method was generating a to-be embedded data that was larger than the embedding space. For this, we intended to apply a compressor with a good compression factor. A compression factor, known as compression ratio, plays a vital rule in compacting data [23-24]. According to a survey of [25] on lossless image compression techniques, Huffman coding can save 71% memory space, Shannon-Fano saves 69% storage, Run- Length coding can saved 48% working memory. Statistics of compression ratio, as stated in [25], made us hope full to apply such a compression technique in our proposed method and thus, we achieved the goal.

Main contributions of this article are:

1) We used a chaotic method to encrypt the secret message.
2) To find a compressed stream of to be embedded data, we applied an analyzed compression factor so that the compressed stream was no more than the length of collected LSBs.
3) To manage stego quality, we implanted secrets in edge pixels only.
4) This is an edge detection-based reversible steganography method. So far we know, this is an unique contribution in the field of edge detection based image steganography.

The rest of the paper is organized as follows. Section II provides the details of related works. Section III narrates our proposed scheme. Section IV presents some experimental results. Finally, section V concludes the article.

II. Related Work

Schemes in [26-27] could not fully utilize embedding space of the cover image due to their necessity of carrying side information. Bai et al. [28] overcome that problem and they did not did not use extra space for storing edge information. That method, first, cleared 5 LSBs of each of the cover pixel and then applied an edge detector, e.g., canny, fuzzy, to find the edge pixels and non-edge pixels

Before Another research conducted by Kumar *et al.*[29] proposed an edge-based steganography system and implants secret message bits only edge pixels. This method cleared 2 LSB from every pixel of the cover image and then applies a fuzzy edge detector to find the edge image. Based on the edge image 2 secret message bits are implanted into the edge pixel. Consequently, the stego image has a low embedding payload.

In [30], authors provided a new steganography system to increase the payload capacity and imperceptibility quality. The method cleared 5 LSBs. In that processed image, they applied hybrid edge detector and dilating operation to find the hybrid edge image. Based on the hybrid edge image, cover image pixels are classified as edge and non-edge pixels. They, finally, embedded x and y bits into each edge and non-edge pixel, respectively.

None of the stated schemes are reversible.

III. Proposed Method

Primary motivation of our research is to present an edge-based reversible steganography method. The secondary target is to manage high imperceptibility of stego image. The proposed scheme consists of three parts - preprocessing, data implantation and data extraction. Data hiding and extraction process of the proposed reversible steganography method is shown in Fig.1 and Fig.2, respectively. Underneath are the implementation steps of the proposed system.

A. Preprocessing

1. Copy the cover image I_o to I_c and preserve the values of first two pixels to P_2.

2. Clear n-LSBs of every pixel of I_c. Say, the processed result is stored in I_c. Now apply apply an edge detection algorithm to that processed image I_c to find an edge image I_e. I_e is a binary image. A one in I_e means that the corresponding pixel in I_c belongs to an edge.

3. Based on edge image I_e, divide the pixels of I_c as edge and non-edge groups.

4. Collect n LSBs from every edge pixel of cover image.

Say, the stream of collected LSBs is *StrmLSB*.

5. Encrypt the secret message M using chaotic method. Say, the encrypted message is M_e.

6. Concatenate the binary value of first two pixels, bit stream of collected LSBs of edge pixels and encrypted message stream.

The concatenated stream S_c, thus, will be formed by equation (1).

$$S_c = P_2 || StrmLSB || M_e \quad (1)$$

7. Set a value for compression factor f, where $0 > f \geq 1$. Measure the length of *StrmLSB*. Say, it is L_{LSB}.

8. Compress the concatenated stream using Eq(2) and store the result in S_{cc}.

$$S_{cc} = F_c(S_c, f) \quad (2)$$

where F_c is a lossless compression function.

If F_c cannot maintain its lossless property due to a small value of f, announce a message of its inability in embedding data and stop executions.

9. Measure the length L_cc of compressed stream S_{cc}.
10. If $L_cc > L_{LSB}$ update f by $f = f \times 95\%$ and goto step8.
11. Convert the value of L_cc into 16-bit binaries.
12. Replace first two pixels of I_c by these 16 bits.

B. Data embedment

Now, the to-be embedded message is S_{cc} and the embedding media is I_c. The scheme follows the following steps to implantthe target secrets.

1) Using image I_e, the scheme maps to corresponding edge pixels in I_c and does it sequentially. Each time, the method takes an edge pixel $I_c(i, j)$ from (i, j) position of I_c, grabs n number of binaries from S_{cc} and executesthe following two steps.
2) It converts that grabbed binaries into decimal value. Say,this is D_m.
3) Form the stego pixel $I_s(i, j)$ for $I_c(i, j)$ using Eq(3).

$$I_s(i, j) = I_c(i, j) + D_m \quad (3)$$

C. Data extraction

The extraction procedure has the stego image I_s. The scheme then performs the following operations to extract the implanted secrets S_{cc} as well as to rebuild the cover image I_o.

1. Pick the first two pixel values from the stego image and convert them into binaries. That binary value is L_cc.
2. Take a copy, I_{sc} of the stego image I_s. Clear n LSBs of every pixel of I_{sc}. Let LSB cleared image is now I_{sc}.
3. Apply same edge detector, as was applied at preprocessing stage, on image I_{sc} to find edge image I_e.
4. Mapping with edge image I_e, find all edge pixels in I_s. Collect n LSBs from every of those edge pixels, sequentially.
5. At that stage, apply the lossless decompression function, as of Eq(4), to recover the concatenated stream S_c.

$$S_c = F_c(S_{cc}, 1/f) \quad (4)$$

6. Separate first 16 bits of S_c and convert these into two pixel values. Replace the first two pixels of I_{sc} with two converted pixels.
7. Let the number of edge pixel is N_e. Then we can compute the length of LSBs that was collected from edge pixels at embedding side by Eq(5).

$$L_{LSB} = n \times N_e \quad (5)$$

8. Collect next L_{LSB} bits from S_c, which is, indeed, *StrmLSB*. Set a pointer to first bit of *StrmLSB*.
9. Using I_e and current file reading pointer, find next edgepixel in I_s, replace n LSBs of that pixel of I_s with $n$bits of *StrmLSB*.
10. Move edge pixel searching pointer and proceed n bit reading pointer by n. When the placing of bits of *StrmLSB* in I_s will be completed, we will find the cover image I_c. Otherwise the scheme will send the execution pointer to step 9.
11. The remaining bits in S_c is M_e. Now apply decryption algorithm to recover original message M.

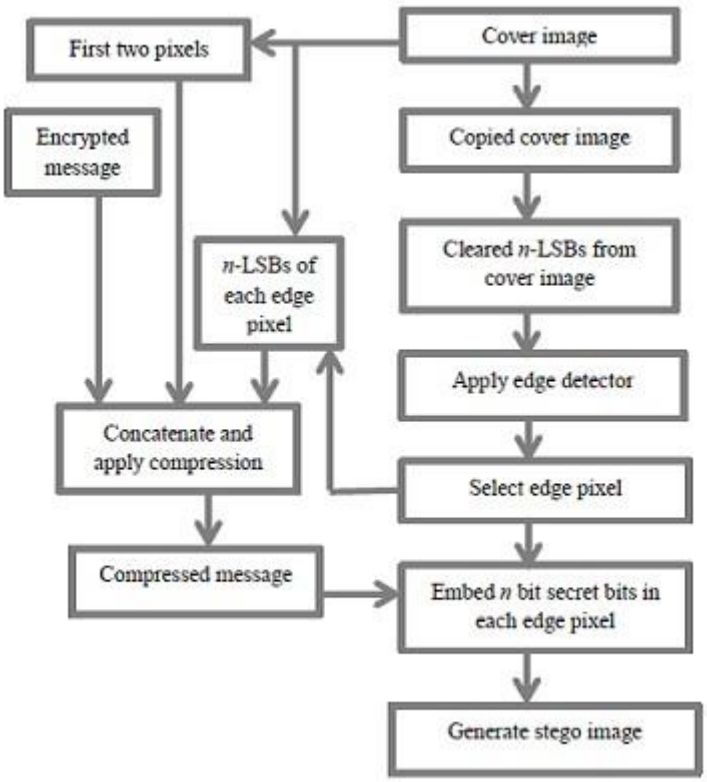

Fig. 1. Embedding procedure.

V. EXPERIMENTAL RESULTS

We implemented that proposed method in MATLAB 2017 on WINDOWS 7. In our experiment, we used the images of BOSS dataset. As a sample, some frequently used images in researches are shown in Fig.3 and their respective stego images are shown in Fig.4. Our experiment applies the traditional and renowned Canny edge detector to detect the edge pixels in the n-bits cleared image. The detector returns us a binary edge images. In an edge image, the pixel value 1 represents

an edge pixel and 0 indicates a non-edge pixel. Based on that edge image, we implanted *n*-number of bits in edge pixel only. Whereas Bai[28] and Setiadi[30] implant *m*-number of bits in non-edge pixel and *n*-number of bits in edge pixel. We did it to manage better stego quality. The results are shown in Table 1.

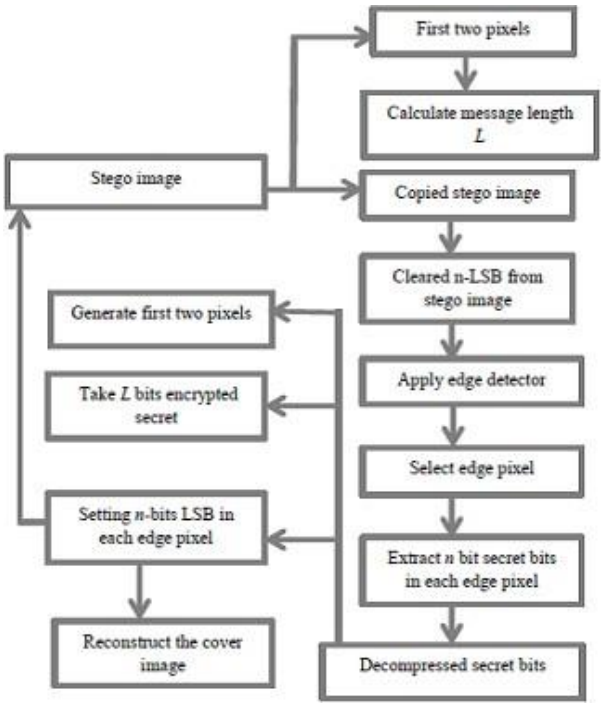

Fig. 2. Extraction procedure.

Fig. 3. Test images.

Fig. 4. Stego images.

There, (m, n) = (0, 2) means that 2-bits are implanted in each edge pixel and no bits are implanted in the non-edge pixel by a method. In fact, we experimented (m, n) = (0, 2) and (m, n) = (0, 3) for the proposed method. We also ex- perimented (m, n) = (1, 2), (1, 3), (2, 3), (1, 4), (2, 4), (3, 4) for competting methods such as Bai [28] and Setiadi [30]. However, for convenience, we have only shown the results of (0, 2) and (0, 3) for the proposed method and (1, 2), (1, 3) for the competting methods Measured payloads are tabulated in Table 1. The table shows that Setiadi [30] gives the highest payload and then Bai [28]. Our proposed method embeds the lowest bits in the same images because Setiadi[30] implants secret bits in both edge and non-edge pixel whereas we implanted in only edge pixels. Additionally, they increase the number of edge pixels by dilation on hybrid edge detector. We avoid that technique to have high stego quality. Though, Bai[28] did not apply dilation operation, they implant secrets in both edge and non-edge pixels.

Table I: Comparison of payloads.

JPG Image	Methods					
	(m,n) = (0,2)	(m,n) = (1,2)		(m,n) = (0,3)	(m,n) = (1,3)	
	Proposed	Bai	Setiadi	Proposed	Bai	Setiadi
F16	12528	72630	85272	18846	79724	105008
Babon	23852	78405	99521	35130	91274	133506
Basket	17444	74063	88769	26205	82590	112002
Boat	15312	74192	90120	22878	82848	114704
Barbara	12400	72996	85821	18474	80456	106106
Lena	11856	73341	86883	17805	81146	108230
Livingroom	16956	75120	92921	25536	84704	120306
Pepper	11046	72972	86175	17109	80408	106814
Walkbridge	21814	77010	96658	32982	88484	127780
Wheel	15960	73228	87249	24054	80920	108962

According to our objective, we concentrate our focus on image quality. To measure that success on having good stego quality, we computed structural similarity index measurement (SSIM). To test the robustness, we also computed correlation and entropy.The SSIM is measured by following Eq (6).

$$SSIM = \frac{(2\mu_c\mu_s + C_1)(2\sigma_{cs} + C_2)}{(\mu_c{}^2 + \mu_s{}^2 + C_1)(\sigma_c{}^2 + \sigma_s{}^2 + C_2)} \dots\dots(1)$$

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

The SSIM values are demonstrated in Fig.5. This figure states that the proposed method represents better results in about all the images.

Entropy is a statistical measure of disorder or randomness to measure the amount of manipulation of an image. The image containing large value of entropy indicates image is manipulated more and small value represents a little manipulation.

The entropy is calculated by equation (2).

$$entropy = -sum(p.* \log_2(p)) \dots\dots\dots\dots\dots(2)$$

Where, p contains the normalized histogram counts returned from imhist.

The entropy values are depicted in Fig. 6. This figure states that the proposed method shows small manipulation than others. So, our proposed method is better than others.

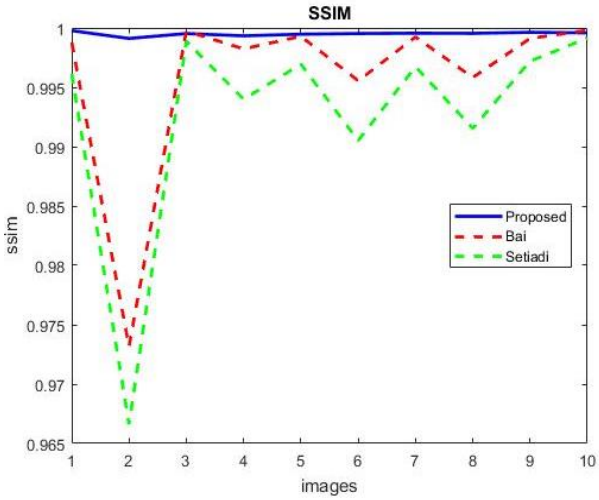

Fig. 5. SSIM values.

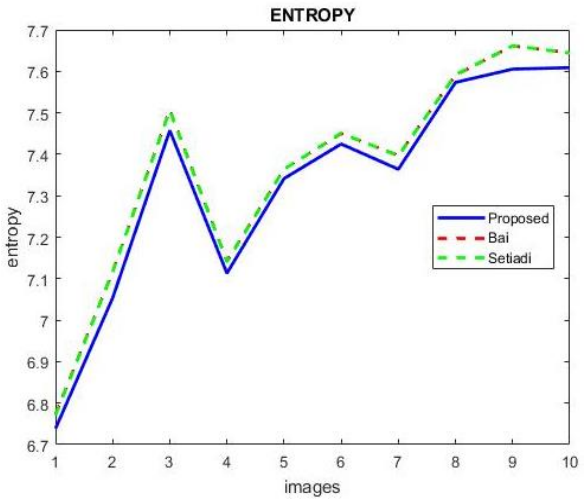

Fig.6. Entropy

Correlation is a statistical measure of similarity betweentwo images. Correlation can be measured in following by using MATLAB build-in function. But, the equation that we followed is given in Eq(8).

$$correlation = \frac{\sum(A_i - \bar{A})(S_i - \bar{S})}{\sqrt{\sum(A_i - \bar{A})^2 \sum(S_i - \bar{S})^2}} \qquad (8)$$

Where, A is a cover image and S is stego image and $\bar{A}, \bar{S}$ represent the average value of contents in A and S, respectively.

The correlation values are depicted in Fig.7. This figure states that the results in proposed method is better than others.

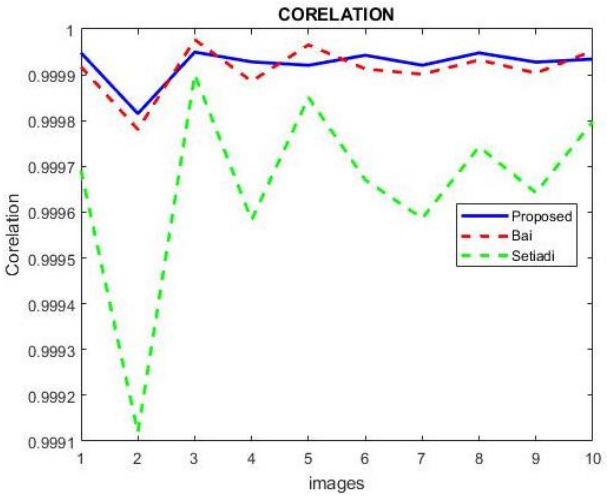

Fig.7. Correlation

VI. CONCLUSION

This article proposes a reversible image steganography method that implants secrets on edge information only. Consequently, the scheme presents higher image quality. The security is also high as it uses an edge detector, encrypt message, concatenates that with collected edge's LSBs, performs a compression and maintains the values of used parameters inall these phases as private. In our future work, we wish to make the scheme reversible without keeping any side record of cover values.

ACKNOWLEDGMENT

This research was financially supported by the ICT division of the 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] A.Shaik, V. Thanikaiselvan and R. Aritharajan, "Data Security Through Data Hiding in Images: A Review", Journal of Artificial Intelligence, vol.10, pp. 1-21, 2017.

[2] R. Gupta, S. Gupta and A. Singhal, "Importance and Techniques of Information Hiding : A Review", International Journal of Computer Trends and Technology, vol.5, 2014.

[3] W. Zhijun, The Information Hiding Model for Speech Secure Communication, Elsevier, Science Press, ISBN: 978-0-12-801328-1, 2015.

[4] F.A.P. Petitcolas, R.J. Anderson and M.G. Kuhn, "Information hiding – a survey", Proc. IEEE, vol.87, pp:1062-1078.

[5] Slideshare.net/qaisarayub/watermarking-in image processing.

[6] H.Tao, L. Chongmin, J.M. Zain and A.N. Abdalla, "Robust Image Watermarking Theories and Techniques: A Review", Journal of Applied Research and Technology, vol.12, 2014.

[7] P. Parashar and R.K. Singh,"A Survey:Digital Image Watermarking Techniques", International Journal of Signal Processing and Pattern Recognition, vol., pp.111-124, 2014.

[8] H. Sultana, "A study on steganography and steganalysis", International Journal of Scientific and Engineering Research, vol.9, 2018.

[9] Z.-Ming. Lu and S.-Ze Guo, Lossless Information Hiding in Images, 2017.

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

[11] 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.

[12] 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.

[13] 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.

[14] 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.

[15] 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.

[16] 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.

[17] 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.

[18] 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.

[19] 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.

[20] S. Sun, "A Novel edge based image steganography with 2k correction and Huffman encoding,", Inf. Process. Lett, 2015.

[21] D. Mathpal, M. Darji and S. Mehta, "A Resarch Paper on Lossless Data Compression Techniques", International Journal for Innovative Research in Science and Technology, vol.4,2017.

[22] K. Muthuchamy,"A study on various data compression types and techniques", International Journal of Research and Analytical Reviews, vol.5, 2018.

[23] B. Gupta, M.Gupta and B. Chadha,"Image Compression Technique under JPEG by Wavelets Transformation", International Journal of Advanced Research in Computer Science and Software Engineering, vol.4, 2014.

[24] A. Alarabeyyat, S.A.-Hashemi, T. Khdour, M.H. Btoush, S.B.-Ahmad, R.A.-Hashemi,"Lossless Image Compression Technique Using Combination Methods", Journal of Software Engineering and Applications, vol.5, pp. 752-763, 2012.

[25] M.A. Rahman and M. Hamada, "Lossless Image Compression Techniques: A-State-of-the-Art Survey", Symmetry, vol.11, 2019.

[26] W.J. Chen, C.C. Chang and T.H.N.Le,"High payload steganography mechanism using hybrid edge detector", Expert Syst. Appl., vol.37,2010.

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

[28] J. Bai, C.-Chen Chang, T.-Son Nguyen, C. Zhu and Y. Liu, "A high payload steganographic algorithm based on edge detection", Displays, vol.46, pp. 42-51, 2017.

[29] S. Kumar, A. Singh and M. Kumar, "Information hiding with adaptive steganography based on novel fuzzy edge identification", Defence Technology, 2018.

[30] D.R.I.M. Setiadi, "Improved payload capacity in LSB steganography uses dilated hybrid edge detection", Journal of King Saud University-Computer and Information Sciences, 2019.