A Multi-path Based Embedding Scheme at Perfect Maze

Sujit Roy [1], *Subrata Kumar Das* [2], *and A. H. M. Kamal* [3]

Abstract

Steganography is a process of hiding data in a media, e.g., image, audio, video, etc. There are lots of areas where steganography can be used. Many researchers are devoting their valuable efforts to hide messages before sending them to a destination through maze-based steganography. However, maze-based steganography has the drawback of reducing embedding capacity. Another problem of maze application at embedding is the imperfection of its solution paths. Imperfect paths are not used for embedding by the maze. That is why while selecting multiple paths, the process of Niwayama et al. in 2010 prunes many paths considering their overlapping or crossing affairs with other ones. In this paper, a solution to those stated problems of Niwayama et al. is outlined and successful results found are demonstrated here too. First, an imperfect maze is tried to be changed virtually to a perfect maze. Then solution paths from start to end are generated. While generating solution paths, the longest path among them is considered to cross or join a point along their pathways. Therefore, one path among those imperfect paths is considered embedded at and extraction was not employed by any earlier proposal, so far we know. Contribution to the stated research area will increase the embedding capacity. For measuring the longest path, the tie is broken by comparing x coordinates and then, if required, y coordinates. The illustrated result in the result analysis section details the justification of our claim.

Keywords : **Steganography**

I. INTRODUCTION

We communicate in different ways, such as, through messages, audios, videos through letters, mobile phone, internet, and other types of media. Among various media, the internet is the most favourite, reliable, and it secures media for transmitting and receiving information. Information can be passed securely by using different schemes such as Message Authentication Code (MAC), Cryptography, Steganography, etc. Steganography is a method to secrete and preserve the secrecy of information in a delivery service. A steganography procedure is usually evaluated in terms of image quality and the embedding capacity. In other words, an ideal steganographic design should have a big embedding capacity and outstanding stego object image quality. The data hiding scheme is characterized by three different features that are capacity, security, and robustness. Capacity refers to the amount of information that can be hidden in the cover medium. Security prevents an eavesdropper from detecting hidden information. Robustness (against attacks) indicates the amount of modification the stego medium can withstand before an adversary that can demolish the hideaway information. The cryptographic technique can help to scuttle a message so that one cannot read if it is exposed.

Manuscript Received : December 22, 2021 ; Revised : January 12, 2022 ; Accepted : January 15, 2022. Date of Publication : February 5, 2022.

S. Roy [1] is *Lecturer* with Department of Computer Science and Engineering at Bangamata Sheikh Fojilatunnesa Mujib Science & Technology University, Jamalpur - 2012, Bangladesh. Email : roysojib09102029@gmail.com ;
ORCID iD : https://orcid.org/0000-0003-0116-9927
S. K. Das [2] is *Associate Professor* with Department of Computer Science and Engineering at Jatiya Kabi Kazi Nazrul Islam University, Mymensingh - 2220, Bangladesh. Email : sdas_ce@yahoo.com ; ORCID iD : https://orcid.org/0000-0003-4640-7255
A. H. M. Kamal [3] is *Professor* with Department of Computer Science and Engineering of Jatiya Kabi Kazi Nazrul Islam University, Mymensingh - 2220, Bangladesh. Email : ahmkctg@yahoo.com ; ORCID iD : https://orcid.org/0000-0001-8031-666X

DOI : https://doi.org/10.17010/ijcs/2022/v7/i1/168954

Steganography hides the very continuation of a message so that if it is successful, it generally attracts no distrust at all. Also, the steganography technique secrets itself in carriers, such as graphics files, text files, images files, audio files, videos, data transmissions, etc. Maze game can be used as a carrier media to hide concealed data. In [1] and [2] the authors proposed the basic idea of embedding data in a maze but this method has two disadvantages. This paper aims to gain more embedding capacity for the perfect maze-based Steganography method locating the solution path from one cell to the target cell. Now, in this paper, we find out multiple solution paths to embedding high capacity. Path selection must not be overlapping.

This paper aims to gain more embedding capacity for the perfect maze-based Steganography method. Locate the solution path from one cell to the target cell. Now, in this paper, we find out multiple solution paths to embedding high capacity. Path selection must not be overlapping.

A. Maze Generation Algorithms

We can randomly generate rectangle mazes with arbitrary rows and columns and find their paths from entry to exits. There are many different processes for generating maze such as the hunt and kill maze algorithm, recursive division method, randomized Kruskal's algorithm, randomized Prim's algorithm, Aldous Broder algorithm, Wilson's algorithm, and various maze generation algorithms for building it.

The maze generator algorithm maintains sets of cells representing connected components in the maze.

Some of steps are as follows:

Step 1 : We can first choose a Start point and an End point in creating a maze.

Step 2 : The path to the exit must be available from the start point.

Step 3 : The grids that are not included in the path must be reachable from start.

Step 4 : There should not be any cycle in the maze.

Step 5 : In the generated maze all the grid should be available.

Step 6 : The number of walls should be considered so that the player does not reach the exit rapidly.

Step 7 : Finally, we can choose one possible largest solution path in the perfect maze.

B. Maze Generation Algorithms

A perfect maze is defined as a maze that has one and only one path from any point in the maze to any other one, such as no inaccessible sections, no circular path, and no open area. Given that a perfect maze has a one solution path, we can solve the maze by performing a depth-first traversal from start cell to end cell. Imperfect mazes have multiple solution paths, and we find the longest solution path among them. A non-perfect maze has some other points that are:

(i) Inaccessible sections

(ii) Circular paths, and

(iii) Open areas

II. RELATED WORKS

In 2020, Mutnuru, Sah, and Kumar [3] cited a method focused on multimedia data and how it can be protected from unwanted attacks. Güvenoglu [4] proposed a method that is more robust. The data is hidden before the data hiding process is encrypted with the AES encryption algorithm. Hue, Hoang, Thanh, and Braeken [5] presented a public key based chaotic cryptosystem for image encryption operating in the integer eld and this system was built based on the discrete Cat-Hadamard map to encrypt bitmap images based on bit plane decomposing processes. In [6] the researchers proposed an Image Steganographic scheme using an 88 Sudoku puzzle for secure data transmission. Mahato, Yadav and Khan [7] proposed a method that generates a minesweeper grid that is visually indistinguishable by humans from other minesweeper games currently present online. Sharma, Gupta, Trivedi, and Yadav [8] proposed an individual to send confidential data between two parties. It enables a user to hide data in different digital mediums. Steganography is of many types such as image steganography, text steganography, audio/video steganography, etc. Güvenoglu [4] proposed method is tested with detailed security analysis. Ou and Chen [9] studied a steganographic method using a generated tetrimino sequence based on online Tetris games, in which secret messages are embedded. Ali and Saad

proposed a new image steganography method which hides the secret message inside the cover image by representing the secret message characters using the Braille method of reading and writing for blind people that can save more than one-fourth of the required space for embedding in 2013 [10]. In the same year, Hemalatha Acharya, Renuka and Kamath [[11] provided a novel image steganography technique which hides multiple secret images and keys in the color cover image using Integer Wavelet Transform (IWT) and they also showed that there is no visual difference between the stego image and the cover image. Farahani and Pourmohammad [12] presented a Discrete Wavelet Transform (DWT) based perfect secure and high capacity image steganography which is used for steganography of the pictorial messages in a cover image in 2013. In 2012, Sukumar and Santha [13] studied a steganographic method using Back Tracker Algorithm for maze-based data hiding.

Ibrahim and Kuan [14] also explained a new algorithm to hide data inside an image using the steganography technique. This algorithm used binary codes and pixels inside an image. Pasquier and Erdoğan [15] studied the impact of different operators, crossover, and mutation, over diversity and performance. In 2007, Andrew proposed steganalysis methods for extensions of least-significant bit (LSB) overwriting to both of the two lowest bit planes in digital images and investigated how detectors for standard LSB replacement can be adapted to such embedding and how the methods of 'structural steganalysis' may be extended and applied to make more sensitive purpose-built detectors for two-bit plane steganography [16]. Earlier, Kamau and Macharia [17] proposed an enhanced LSB method that employs a selective and randomized approach in picking a specific number of target image bits to swap with the secret data bits during the embedding process for increasing the level of imperceptibility and hiding capacity in the LSB insertion method. In [18] it is shown that approach of information hiding can be extended to copyright protection for digital media: audio, video, and images. Artz [19] mentioned a sample of the steganography tools. Lee, Lee and Chen [20] also proposed an improved algorithm for increasing the embedding capacity and preserving the 'perfect' property Lee and Chen [21] also described an image steganographic model which is based on variable-size LSB insertion while maintaining image fidelity to maximize the embedding capacity. Niwayama, Chen, Ogihara, and Kaneda [22] introduced a data hiding strategy known as HK embedding algorithm that inserts secret data in a maze. A set of reversible data hiding methods was presented in [23-34].

III. PROPOSED MODEL

The main objective of the proposed method is to consider a solution path rather than multiple paths to gain more embedding capacity. We define here a new efficiency methodology on a perfect maze based steganography method to enhance the embedding capacity. Our proposed algorithm helps to generate a perfect maze and to locate the solution path from the starting cell to the end cell. In this research work, there are three main ideas in the proposed method. The embedding capacity is increased due to embedding bits into multi-paths instead of only one path. In our proposed strategy, at first, we can generate an imperfect maze to convert perfect maze one. Second, we can find out the solution path rather than multi-path to gain more embedding capacity.

A. Embedding Phase

In Fig. 1, we input a storage maze, select that, and find out the solution path from the starting cell to the ending cell. Now applying embedding algorithms, we order solution paths according to their starting cells to end from up to down and then left to right. The message stream and cover images are the input and the stego image is the output of this algorithm.

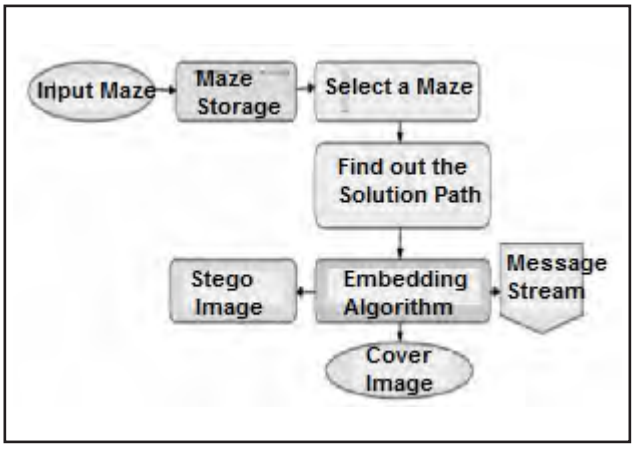


Fig. 1. Architecture of Stego Maze in Embedding Phase

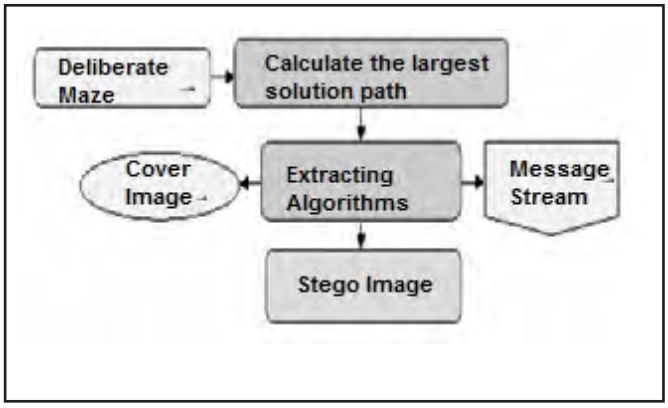


Fig. 2. Architecture of Stego maze in Extracting Phase

B. Extracting Phase

In Fig. 2, consider a maze and calculate the solution path from any starting cell to the final one. Stego image is the input, considering that the cover image and the message stream are the output of the extracting algorithms.

IV. RESULT AND ANALYSIS

In Table I, we deliberate the comparison between Niwayama and our proposed approaches. In this table, deliberate maze1, the number of solution paths of the proposed method is three, and the author's solution path is two. We consecutively consider different solution paths of different mazes in the subsequent table.

In Table II, we consider the comparison of Niwayama's method and the proposed method. In this table, consider maze (30*30), the capacity of the Proposed Method is 580 bits, and author's capacity is 500 bits. We will sequentially consider different capacities of different mazes in the subsequent table.

In the subsequent Table III, consider Maze 3, the capacity of Niwayama et al.'s method capacity is 4123 bits and our proposed method capacity is 5854 bits. The ratio of the capacity (gain) of two methods is 1.419.

The achieved capacity and gain of the multi-path of the embedding strategy between the proposed method and the author's method is represented in Table IV. Considering maze 1, the multi-path of the embedding capacity of Niwayama's method capacity is 17500 bits and our proposed method capacity is 19850 bits. The ratio of the capacity (gain) of the two methods is 1.134.

TABLE I.
COMPARISON OF SOLUTION PATHS

No. of Maze	Solution Paths in			
	Maze 1	Maze 2	Maze 3	Maze 4
Niwayama et al.	2	6	10	14
Proposed Method	3	8	13	19

TABLE II.
COMPARISON OF EMBEDDING CAPACITY

No. of Maze	Capacity(bits)			
	Maze (30*30)	Maze (50*50)	Maze (100*100)	Maze (500*500)
Niwayama et al.	500	1900	6700	210000
Proposed Method	580	2250	8200	235000

TABLE III.
COMPARISON SINGLE PATH OF THE EMBEDDING CAPACITY AND GAIN

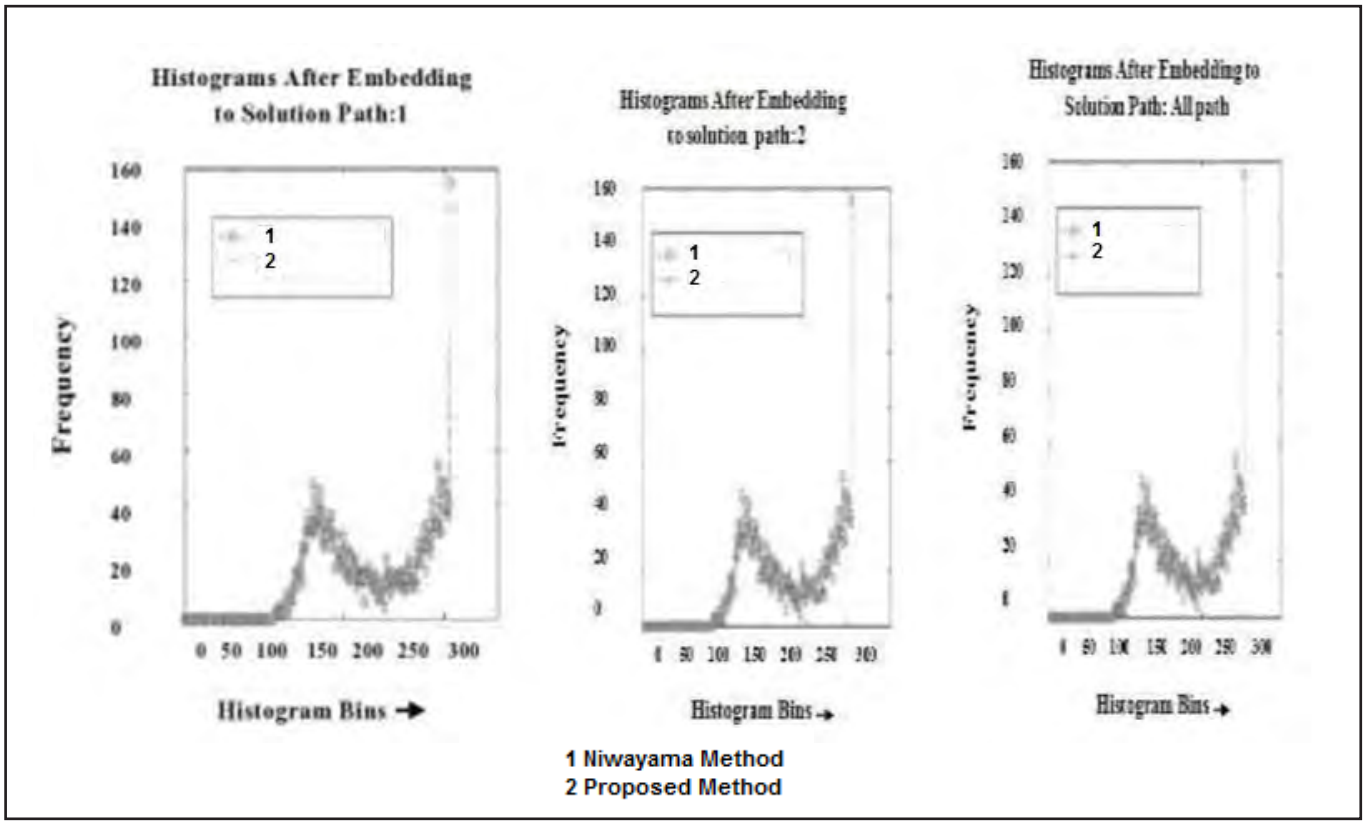
No. of Maze	Capacity(bits)		
	Niwayama et al.	Proposed Method	Gain
Maze 1	1700	1985	1.168
Maze 2	3133	4432	1.415
Maze 3	4143	5854	1.419
Maze 4	4250	6760	1.590

TABLE IV.
COMPARISON OF MULTI-PATH OF THE EMBEDDING CAPACITY AND GAIN

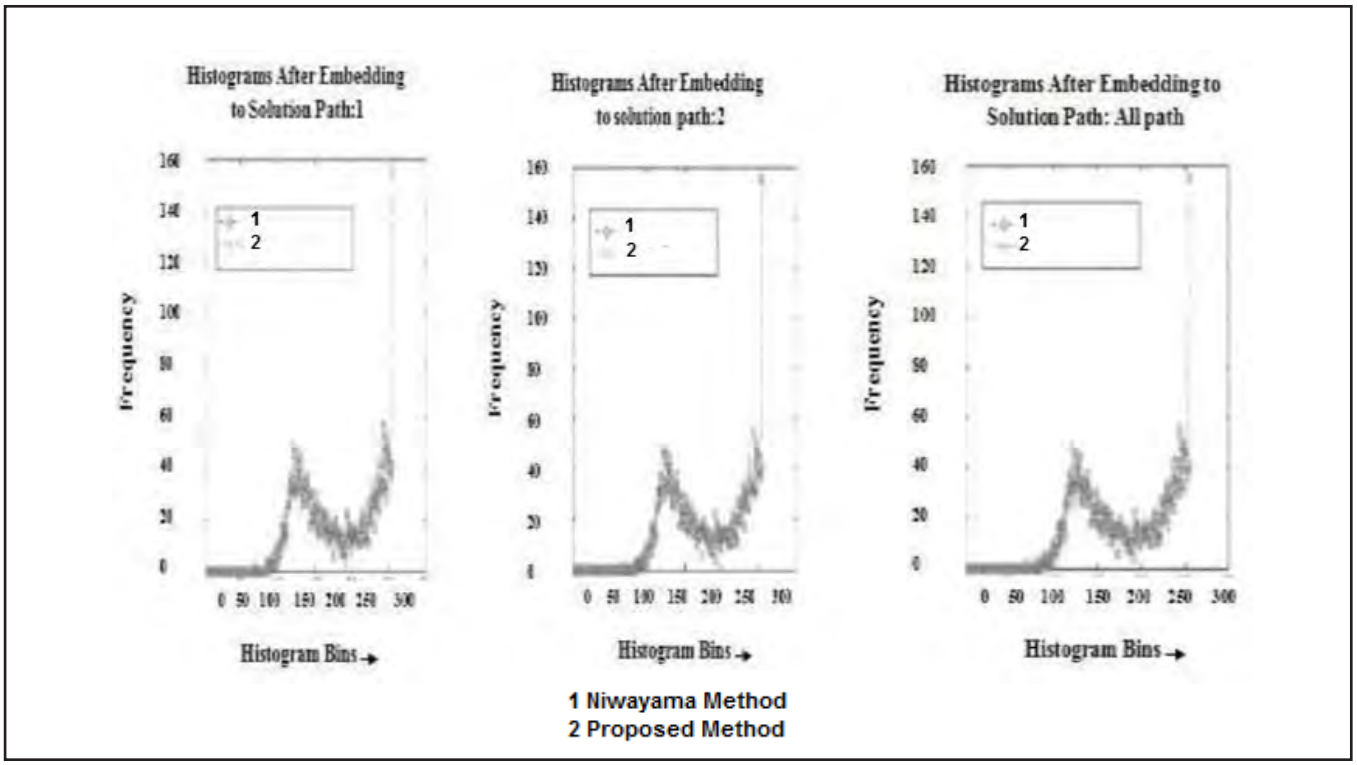
No. of Maze	Capacity(bits)		
	Niwayama et al.	Proposed Method	Gain
Maze 1	17500	19850	1.134
Maze 2	31533	44632	1.415
Maze 3	41550	67680	1.628
Maze 4	51221	88941	1.736

A. Mathematical Analysis

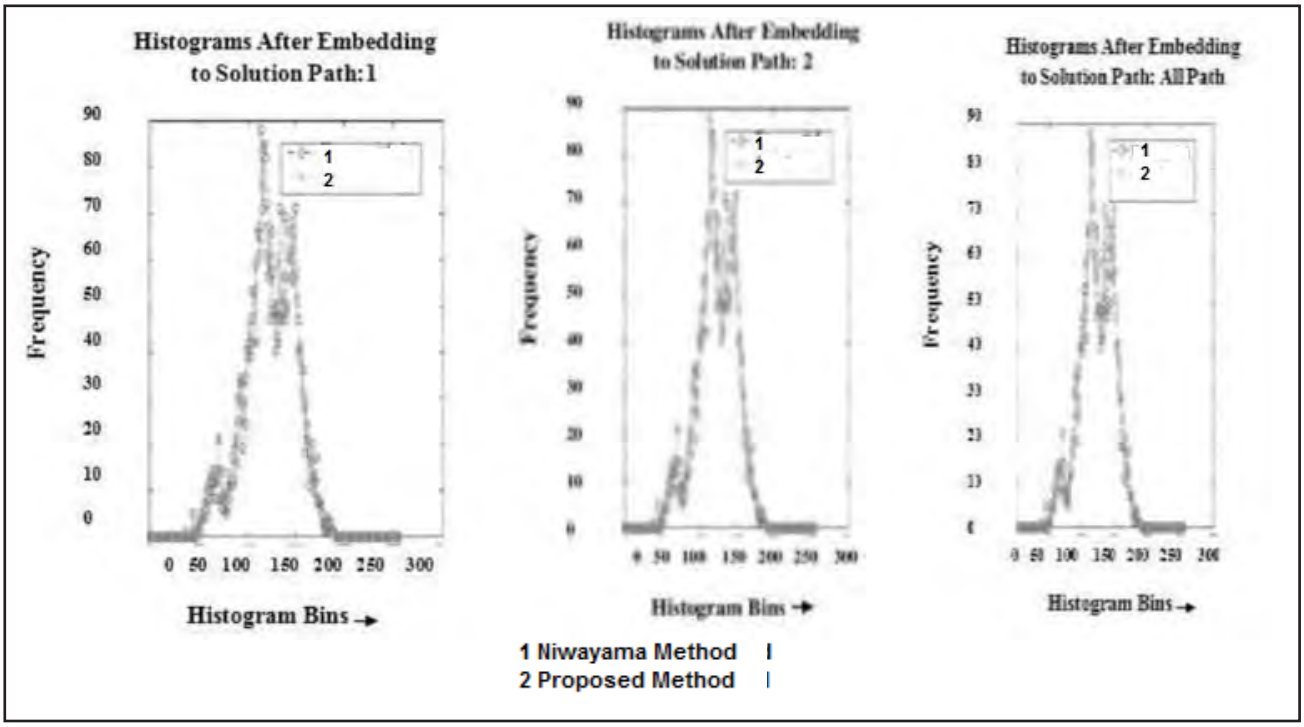
The Mean Square Error and the Peak Signal to Noise Ratio are the two error metrics used for image compression quality and image processing etc. The Mean Square Error constitutes the cumulative squared error between the compressed image and the real image, but



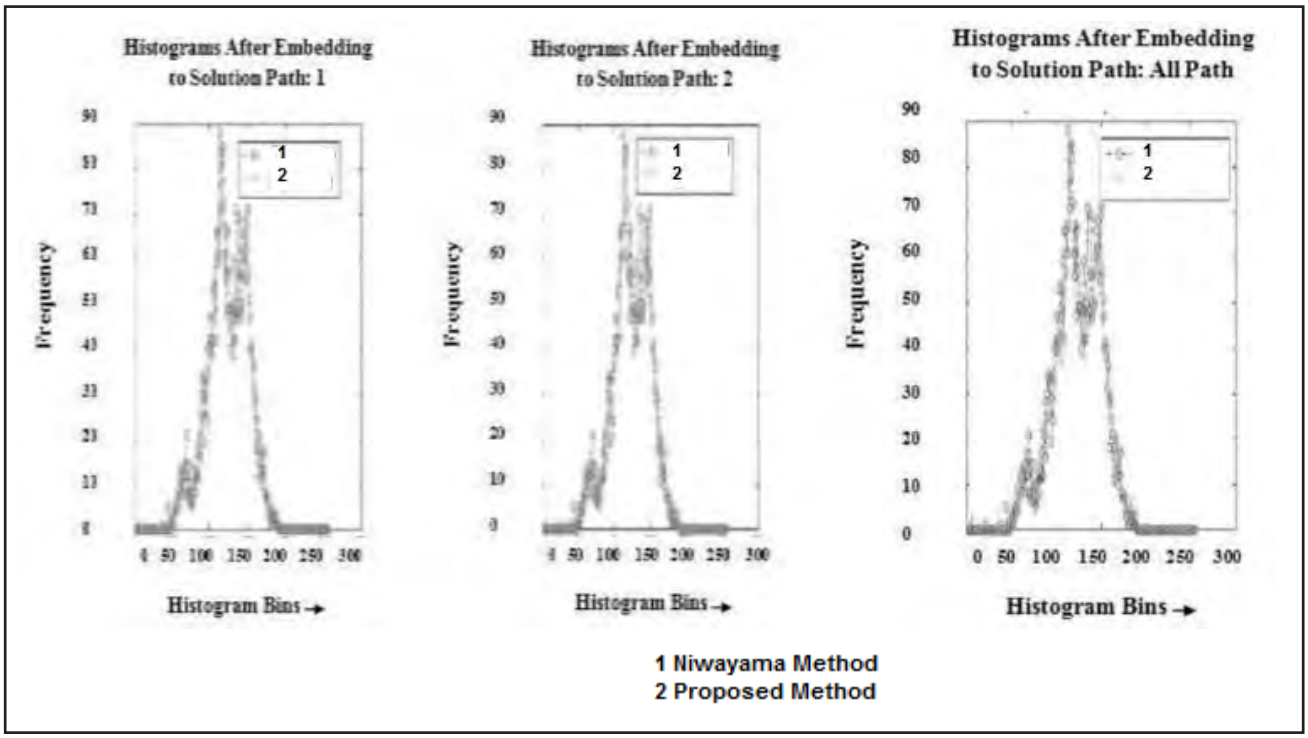
(a) Capacity 1 bpps



(b) Capacity 6 bpps



(c) Capacity 1 bpps



(d) Capacity 6 bpps

Fig. 3. Graphical Representation of Analysis (a) For single path of the embedding capacity (b) For single path of the embedding capacity (c) For multi paths of the embedding capacity (d) For multi paths of the embedding capacity

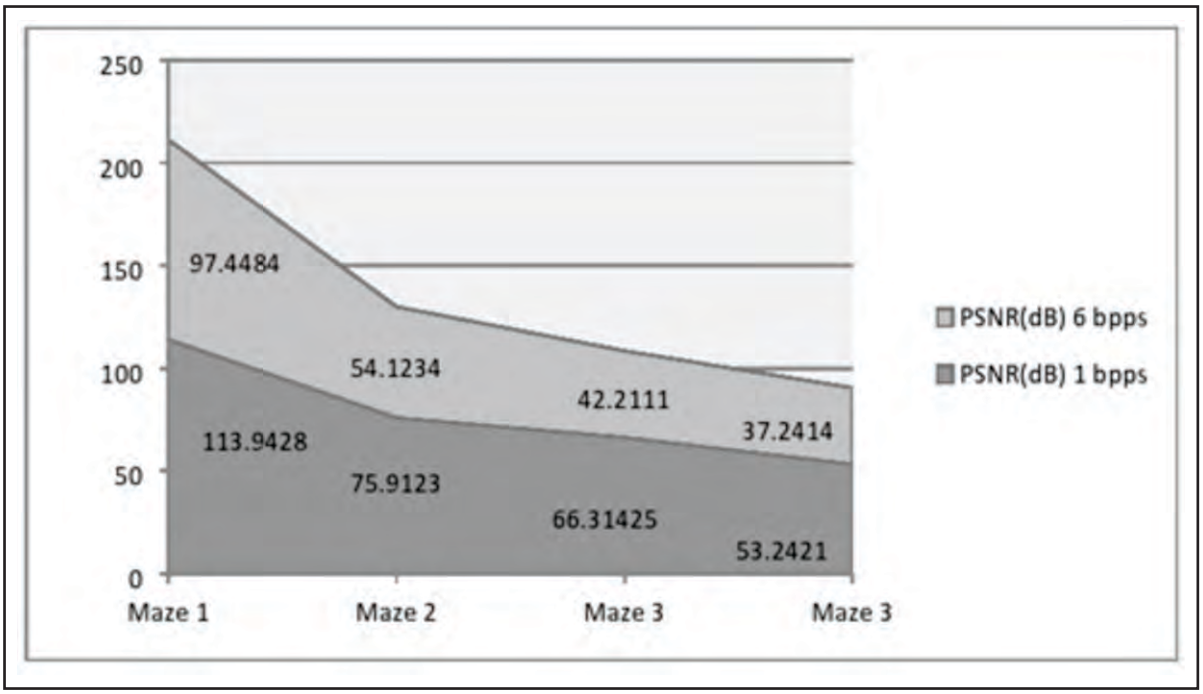


Fig. 4. Comparison of the Capacity for 1 bpps and 6 bpps

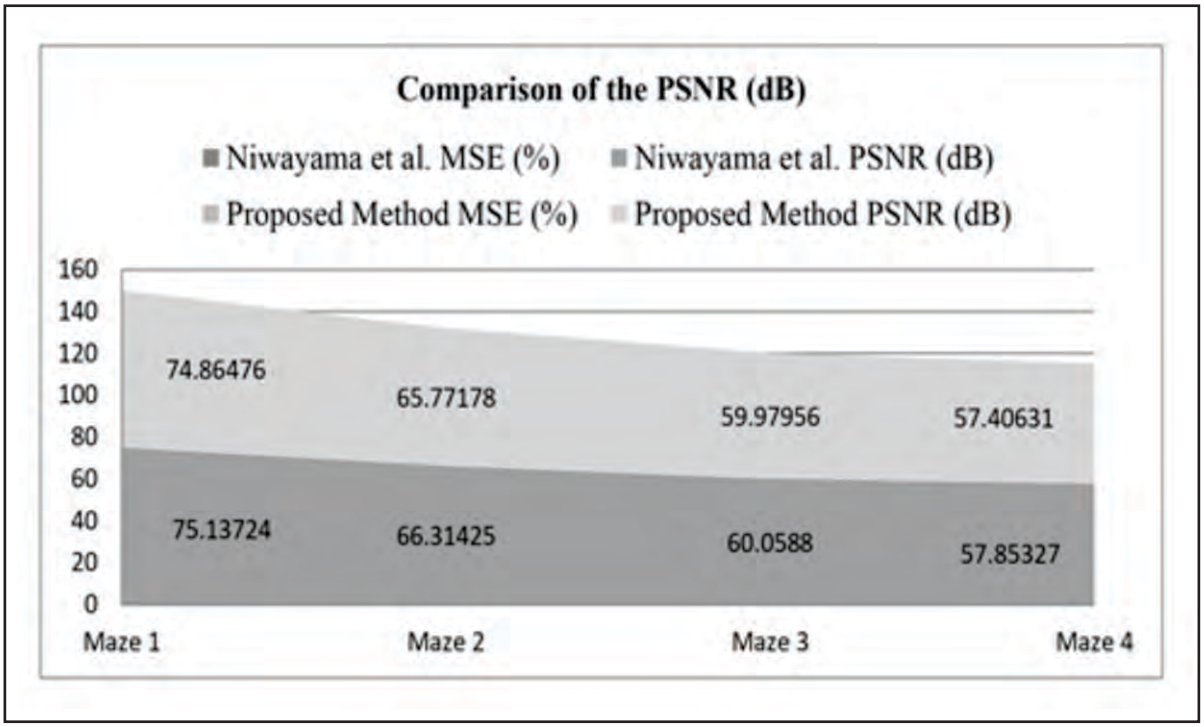


Fig. 5. Graphical Representation of Analysis : Comparison of the PSNR Niwayama et al. and Proposed Method

Peak Signal to Noise Ratio represents a measure of the peak error. In the proposed method, higher the value of Mean Square Error, higher the error, and approximately lower the Peak Signal to Noise Ratio. Peak Signal to Noise Ratio is applied to measure the quality of reconstruction of loss and lossless compression (e.g. for image compression). At first, we calculate the mean-squared error using eq. (1):

$$MSE = \frac{\sum_{m=1}^{M} \sum_{n=1}^{N} (I_1(m,n) - I_2(m,n))^2}{(M * N)} \qquad (1)$$

In (1), M and N are the number of rows and columns in the input images correspondingly. Second, we calculate the Peak Signal to Noise Ratio using the following equation :

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

In eq. (2), R is the maximum fluctuation in the input image data type. For example, if the input image has a double-precision floating-point data type, then R is 1. If it has an 8-bit unsigned integer data type, R is 255 etc.

In Table V, the Mean Square Error (MSE) of our proposed method is high because of the highest rate of data, and that's why Peak Signal to Noise Ratio (PSNR) is low. On the other hand, the MSE of Niwayama's method is lower, and PSNR is comparatively high.

In Table V, consider Maze 1, the Niwayama et al.'s method PSNR is 75.13724 dB and in the proposed method PSNR is 74.86476 dB. In this table the proposed method Mean Square Error is high because of huge rate of data, so Peak Signal to Noise Ratio (PSNR) is low.

B. Statistical Analysis

In Fig. 3, we consider the graphical representation of two methods: the Niwayama method and the proposed methods. Histogram bins are considered horizontally and frequency is vertical. In Fig. 4, a comparison of the Capacity (1 bpps) and Capacity (6 bpps) is shown.

V. CONCLUSION

In this study, a maze-based method has been proposed for encrypting and decryption algorithms. When we compared the proposed method with other methods in the literature, it seems to have a very high success embedding capacity rate from the perfect maze. At first, we consider our proposed method is an imperfect maze convert to a perfect maze. There is some solution path from the starting cell to the ending cell. Gain more embedding capacity from the perfect maze. We can first get the multi-paths from some start cells to one end cell. The maze generated by Hunt and Kill Maze Generating algorithm is perfect; we can build a corresponding tree. Our proposed method can afford high embedding capacity than that of one-path Hunt and Kill embedding maze generating algorithm. Therefore, it significantly improves data security over the existing Hunt and Kill Maze Generating embedding algorithm by providing that encryption to sharing data. When embedding bits into one solution path, our new method provides approximately twice the embedding capacity of the one-path Hunt and Kill Maze Generating algorithm. The imperfect maze is converted to the perfect maze that cannot be renowned visually by humans, and this perfect maze is commonly used in finding the largest maze for embedding capacity.

AUTHORS' CONTRIBUTION

The authors made substantial contributions to the following task of the research: initial conception, selecting the final research topics, and supervision of this research work. Sujit Roy developed the methodology,

TABLE V.
COMPARISON OF THE PROPOSED METHOD WITH OTHER METHODS

No. of Maze	Niwayama et al.			Proposed Method		
	MSE(Percent)	PSNR (dB)	Capacity 1 bpps	MSE(Percent)	PSNR (dB)	Capacity 6 bpps
Maze 1	0.00199231	75.13724	113.9428	0.00212131	74.86476	97.4484
Maze 2	0.015193396	66.31425	75.9123	0.01721478	65.77178	54.1234
Maze 3	0.064150525	60.05880	66.31425	0.06533185	59.97956	42.2111
Maze 4	5.8201e-004	57.85327	53.2421	6.6501e-004	57.40631	37.2414

design, analysis, and wrote the full manuscript. The manuscript preparation, review, and editing was done by Subrata Kumar Das. All the authors read and approved the final manuscript.

CONFLICT OF INTEREST

The authors declare that there is no conflict of interest.

FUNDING ACKNOWLEDGMENT

The authors did not receive any financial support for this research.

REFERENCES

[1] D.-C. Lou, N.-I. Wu, C.-M. Wang, Z.-H. Lin, and C.-S. Tsai, "A novel adaptive steganography based on local complexity and human vision sensitivity," *J. Syst. Softw.,* vol. 83, no. 7, pp. 1236–1248, 2010.

[2] K. Bailey and K. Curran, "An evaluation of image based steganography methods," *Int. J. Digit. Evid.,* vol. 2, no. 2, pp. 1–40, 2003.

[3] S. Mutnuru, S. K. Sah, and S. Y. P. Kumar, "Selective encryption of image by number maze technique," *Int. J. Cryptogr. Inf. Syst.,* vol. 10, no. 2, pp. 1-10, 2020, doi: 10.5121/ijcis.2020.10201

[4] E. Guvenoglu, "Maze based image encryption algorithm," *Int. Res. J. Eng. Technol.,* vol. 2, no. 8, pp. 1578–1585, 2015, doi: 10.31202/ecjse.571030

[5] T. T. K. Hue, T. M. Hoang, H. X. Thanh, and A. Braeken, "Bit plane decomposing image encryption based on discrete Cat-Hadamard map," in *2018 IEEE Seventh Int. Conf. Commun. Electronics (ICCE),* 2018, pp. 344–349, doi: 10.1109/CCE.2s018.8465711

[6] D. Debanjali, A. Bandopadhyay, S. Jana, A. K. Maji, and R.K Pals, "A novel image steganographic scheme using 8x8 Sudoku puzzle," in *Adv. Comput. Syst. Secur.,* pp. 85-100. Springer, Singapore, 2017.

[7] S. Mahato, D. K. Yadav, and D. A. Khan, "A minesweeper game-based steganography scheme," *J. Inf. Secur. Appl.,* vol. 32, pp. 1–14, 2017, doi: 10.1016/j.jisa.2016.11.005

[8] S. Sharma, A. Gupta, M. C. Trivedi, and V. K. Yadav, "Analysis of different text steganography techniques: A survey," in *2016 2nd Int. Conf. Comput. Intell. Communication Technol. (CICT),* 2016, pp. 130–133, doi: 10.1109/CICT.2016.34

[9] Z.-H. Ou and L.-H. Chen, "A steganographic method based on tetris games," *Inf. Sci.,* vol. 276, pp. 343–353, 2014, doi: 10.1016/j.ins.2013.12.024

[10] A. A. Ali and A.-H. S. Saad, "Image steganography technique by using Braille method of blind people (LSBraille)," *Int. J. Image Process.,* vol. 7, no. 1, pp. 81–89, 2013.

[11] Hemalatha, S., U. D. Acharya, Renuka, A., and P. R. Kamath, "A secure and high capacity image steganography technique," *arXiv Prepr. arXiv1304.3629v1,* 2013.

[12] M. R. D. Farahani and A. Pourmohammad, "A DWT based perfect secure and high capacity Image Steganography method," in *2013 Int. Conf. Parallel Distrib. Comput., Appl. Technologies,* 2013, pp. 314–317, doi: 10.1109/PDCAT.2013.56

[13] T. Sukumar and K. R. Santha, "Maze based data hiding using back tracker algorithm," *Int. J. Eng. Res. Appl.,* vol. 2, no. 4, pp. 499-504, 2012, doi: 10.1.1.416.3524&rep=rep1&type=pdf

[14] R. Ibrahim and T. S. Kuan, "Steganography algorithm to hide secret message inside an image," *arXiv Prepr. arXiv1112.2809v1,* 2011.

[15] T. Pasquier and J. Erdogan, "Genetic algorithm optimization in maze solving problem," *Inst. Super. d'Electronique Paris,* 2016.

[16] A. D. Ker, "Steganalysis of embedding in two least-significant bits," *IEEE Trans. Inf. Forensics Secur.,* vol. 2, no. 1, pp. 46–54, 2007, doi: 10.1109/TIFS.2006.890519

[17] G. M. Kamau, "An enhanced least significant bit steganographic method for information hiding," *JKUAT Institutional Repos.,* 2014.

[18] M. M. Amin, M. Salleh, S. Ibrahim, M. R. Katmin, and M. Z. I. Shamsuddin, "Information hiding using steganography," in *4th Nat. Conf. Telecommunication*

Technol., 2003. NCTT 2003 Proc., 2003, pp. 21–25, doi: 10.1109/NCTT.2003.1188294

[19] D. Artz, "Digital steganography: hiding data within data," *IEEE Internet Comput.,* vol. 5, no. 3, pp. 75–80, 2001, doi: 10.1109/4236.935180.

[20] H.-L. Lee, C.-F. Lee, and L.-H. Chen, "A perfect maze based steganographic method," *J. Syst. Softw.,* vol. 83, no. 12, pp. 2528–2535, 2010, doi: 10.1016/j.jss.2010.07.054

[21] Y.-K. Lee and L.-H. Chen, "High capacity image steganographic model," *IEE Proc. - Vision, Image Signal Process.,* vol. 147, no. 3, pp. 288–294, 2000, doi: 10.1049/ip-vis:20000341

[22] N. Niwayama, N. Chen, T. Ogihara, and Y. Kaneda, "A steganographic method for mazes," in *Proc. of Pacific Rim Workshop Digit. Steganography,* 2002.

[23] A. H. M. Kamal and M. M. Islam. "Enhancing embedding capacity and stego image quality by employing multi predictors," *J. Inform. Secur. Appl.,* vol. 32, pp. 59–74, 2017, doi: 10.1016/j.jisa.2016.08.005

[24] A. H. M. Kamal and M. M. Islam, "Boosting up the data hiding rate through multi cycle embedment process," *J. Visual Commun. Image Representation,* vol. 40, part B, pp. 574–588, 2016, doi: 10.1016/j.jvcir.2016.07.023

[25] A. H. M. Kamal and M. M. Islam, "Enhancing the performance of the data embedment process through encoding errors," *Electronics,* vol. 5, no. 4, p. 79, 2016, doi: 10.3390/electronics5040079

[26] A. H. M. Kamal and M. M. Islam, "Capacity improvement of reversible data hiding scheme through better prediction and double cycle embedding process," in *2015 IEEE Int. Conf. Adv. Netw. Telecommun. Syst. (ANTS),* pp. 1–6, doi: 10.1109/ANTS.2015.7413636

[27] A. H. M. Kamal and M. M. Islam, "An image distortion-based enhanced embedding scheme," *Iran J. Comp. Sci.,* vol. 1, pp. 175–186, 2018, doi: 10.1007/s42044-018-0016-3

[28] A. H. M. Kamal and M. M. Islam, "A prediction error based histogram association and mapping technique for data embedment," *J. Inform. Secur. Appl.*, 48, 2019, 102368.

[29] A. H. M. Kamal, M. M. Islam, and Z. Islam, "An embedding technique for smartcard-supported e-healthcare services," *Iran J. Comput. Sci.,* vol. 3, no. 2, 195-205, 2020, doi: 10.1007/s42044-020-00055-1

[30] 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," in *2016 Int. Conf. Netw. Syst. Secur.* (NSysS). IEEE, 2016, pp. 1–8, doi: 10.1109/NSysS.2016.7400691

[31] A. H. M. Kamal and M. M. Islam, "Facilitating and securing offline e-medicine service through image steganography," *Healthcare Technol. Lett.,* vol. 1, no. 2, pp. 74–79, 2014, doi: 10.1049/htl.2013.0026

[32] A. H. M. Kamal, "Steganography: Securing message in wireless network," *Int. J. of Comput. Technol.,* vol. 4, no. 3, pp. 797–801, doi: 10.1.1.799.6634

[33] S. Habiba, A. H. M. Kamal, and M. M. Islam, "Enhancing the robustness of visual degradation based HAM reversible data hiding," *J. Comput. Sci.,* vol. 12, no. 2, pp. 88–97, 2016, doi: 10.3844/jcssp.2016.88.97

[34] A. H. M. Kamal, "Securing the smart card authentications process by embedment random number of data bits into each pixel," *Int. J. u-and e-Service, Sci. Technol.*

About the Authors

Sujit Roy is Lecturer with the Department of Computer Science and Engineering at Bangamata Sheikh Fojilatunnesa Mujib Science & Technology University, Jamalpur, Bangladesh. He obtained his B.Sc. and M. Sc. degree in Computer Science and Engineering from Jatiya Kabi Kazi Nazrul Islam University (JKKNIU), Trishal, Mymensingh, Bangladesh. He has written many research papers in various international journals. He has research interest in Cloud Computing, Image Processing, Data Mining, IoT, Internet and Web Application, and Wireless Communications.

Subrata Kumar Das received B.Sc. in 2004 and M. Sc. in 2005 from Department of Computer Science and Engineering, Islamic University, Kushtia, Bangladesh. He joined the Department of Computer Science and Engineering of Jessore University of Science and Technology, Jessore, Bangladesh as a Lecturer in 2009. In 2012 he was promoted to Assistant Professor in the same department. Later, he joined the Department of Computer Science and Engineering at Jatiya Kabi Kazi Nazrul Islam University, Mymensingh, Bangladesh, as an Assistant Professor and is currently acting as Associate Professor. His research interest is in the fields of Big Data Analytics, Health Informatics, Networking and Distributed Systems, and Network Security.

A. H. M. Kamal is Professor at the Department of Computer Science and Engineering of Jatiya Kabi Kazi Nazrul Islam University, Bangladesh. He received his Ph.D. from Bangladesh University of Engineering and Technology which is a top ranked university in Bangladesh. His research focuses on image steganography, information security, medical imaging, and electronic commerce. He has published a good number of articles in different renowned journals with good impact factors. Two Ph.D. students are working under his supervision.