Research Article

ACCENTS Transactions on Information Security, Vol 6(23)
ISSN (Online): 2455-7196
http://dx.doi.org/10.19101/TIS.2021.621006

An improve image security algorithm using hybrid cryptography approach

Shubham Shashikant Patil[1]*, Kailash Patidar[2], Gourav Saxena[3] and Narendra Sharma[3]
M.Tech Student, Computer Science and Engineering, SSSIST, Sehore, Madhya Pradesh, India[1]
Professor, Department of Computer Science, School of Engineering, Sri Satya Sai University of Technology &Medical Sciences, Sehore, Madhya Pradesh, India[2]
Assistant Professor, Department of Computer Science, School of Engineering, Sri Satya Sai University ofTechnology & Medical Sciences, Sehore, Madhya Pradesh, India[3]

Received: 15-May-2021; Revised: 20-July-2021; Accepted: 24-July-2021

Abstract

This paper explores the image data security concepts along with the experimentation. An efficient combination of RC4-RC6 with Blowfish (RC2 (46B)) algorithm has been applied for the image data encryption. Wang database has been considered for the experimentation. It consists of 1,000 test images. In this approach image was selected from the database. Then image data preprocessing has been performed and matrix values have been obtained for the further processing. Then substitution was performed based on RC2 (46B). This substitution is efficient as it provides the best selection from the combination of the RC6 and RC4. Then the blowfish algorithm was applied after the substitution and first key generation. XOR was performed on the obtained bit. So that the maximum place value replacements were performed successfully. Then reverse mechanisms were adopted for the decryption of the data and finally the original image has been recovered. The results clearly depict that the performance of the proposed framework is better as the error rates are less or minor. It indicates the average error rate of 0.15. In terms of average time for encryption and decryption is 92 ms. The loss in terms of image pixels is also minimized as the error rate variation found from the images are minor. So, it is also efficient in terms of information entropy.

Keywords

Image data security, Unauthorized access, Cryptography, Steganography.

1.Introduction

In the current communication trend, data transmission through different media is increasing day by day [1]. The main data used in the communication are text, images and video. The wide use of data sending and receiving in terms of different pictures increases the demand of image data security. There are different dimensions in the image security research work. There is a lot of research work is going on including different dimensions and aspects [2–10]. These aspects include cryptography and steganography techniques along with other mechanism for security breach detection also [11–15].

Security mechanism in general handled by cryptography and steganography algorithms [16–21].

In general, the mechanism of encryption and decryption of data is handled through cryptography algorithms [22, 23].

The data hiding mechanism has been adopted in case steganography [24]. This paper covers the study, analysis and discussion in case of image data security. The need for data security in terms of breach control, access control and network security are very important. Activity monitoring, may be performed based on these factors [22–25]. The role of data integrity is also very important. It consists of constraints, data filtration, attributes, threshold and combined actuation.

Figure 1 shows the simple steps of the encryption and decryption procedure. It covers the encryption of the plaintext data into the ciphertext form and again, it is converted to the plaintext. *Figure 2* shows the overall procedure for data sharing and security protocols. It covers the method adaptation aspects, weighting and

*Author for correspondence

preprocessing, data categorization, resource sharing and security protocols.

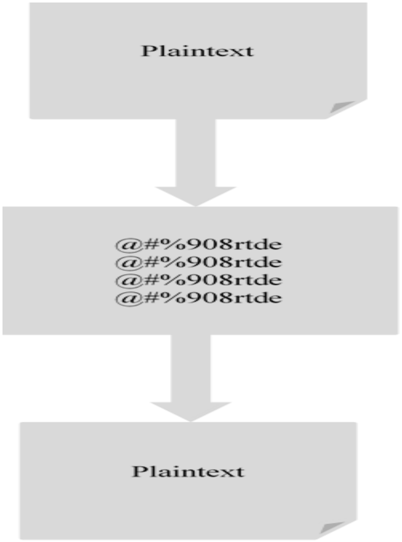

Figure 1 Simple steps for the encryption and decryption

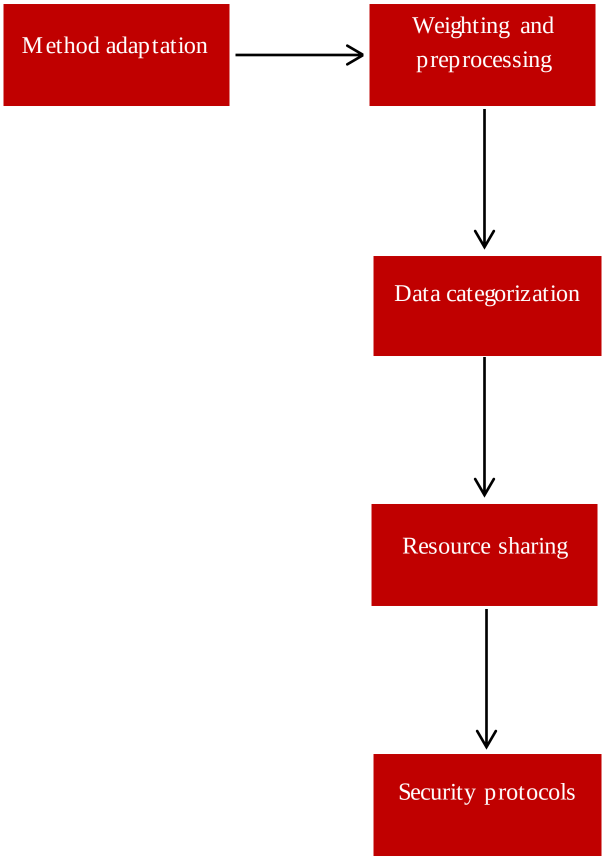

Figure 2 Overall procedure for data sharing and security protocols

In 2020, Kushnir et al. [26] discussed the crucial aspects of security through chaotic encryption. The image encryption technique has been proposed by using two chaotic mappings. They used fuzzy logic for the same. Statistical analysis was performed based on the histogram, entropy and correlation coefficient computation. In 2020, Han et al. [27] proposed an encryption algorithm based on medical domain. The main procedure is oriented through the Hermite chaotic neural network. Training was performed based on Hermite chaotic neural network. Experimentation was performed on medical image. The results indicate the improved performance in terms of key space and sensibly. In 2020, Kaur and Jindal [28] analyzed and explored the image authentication techniques. Singular value decomposition (SVD) was used along with the extraction. Important features of images were extracted based on this QR code. In 2020, Abdulrahman and Varol [29] discussed and analyzed the importance of image segmentation. They have processed their approach based on color density. It has been used for segment evaluation. Their approach was used in medical, cultural and industrial fields. They reviewed image segmentation, threshold functions and different aspects apply for images. In 2020, Zhang et al. [30] discussed and analyzed the properties of unpredictability. It is used in terms of initial values and parameters and chaotic systems. They proposed a 2D logistic scheme for the coupling modulation model. It is based on chaotic ring transformation. Diffusion operation has been performed on pixel values. It is found to be more secure and strong. In 2020, Abdallah [31] discussed about computed tomography. They used water-based segmentation. It is used for the detection of the margin's tissues within the images. Contrast augmentation and segmentation were used for the lesion detection. It has been endorsed by the achievability and efficiency. It is found to be effective in the smaller lesion detection. In 2020, Yadahalli et al. [32] discussed about the steganography techniques. It is employed based on the confidential messages in terms of data transmission. They have used least significant bit method along with the discrete wavelet transform method. Their results indicate the effectiveness of the approach. In 2020, Luo and Zhu [33] discussed and analyzed the deep learning model. They used x-ray pictures for the experiment. They used data augmentation method. It is found to be more effective. It is found to that more complex backbone can be found to be more sensitive. In 2020, Kukharska et al. [34] discussed about the steganographic data transformation. Their proposed approach provides the facility of embedding secret information along with the changes of images between its pixel values. The

Arnold's transformation was used for the rearrangement. The results indicate that the visual image quality was unchanged for the hidden information detection. In 2020, Kumar et al. [35] discussed about image segmentation. Their main aim is to identify the nucleus of white blood cells. They evaluated the efficiency based on the edge detection algorithm (log & Canny) methods, k-means algorithm, linear transformed image and color-based technique. They provided the comparative analysis of the same. Their results indicate that the k-means based segmentation is found to be suitable. In 2020, Arpacı and Kurt [36] discussed about different GUI tools. It has been designed and implemented for the cryptographic applications. Their tool is efficient to improve the security of the encryption process. It includes security tests for different domains like noise attack, key sensitivity and differential attacks. So, this paper mainly shows the insights and the current trends in the image data security for the exploration of the need and challenges. The main objective of this paper is to apply improve image security algorithm using hybrid cryptography approach.

2.Methods

This paper explores the image data security concepts along with the experimentation. An efficient combination of RC4-RC6 with Blowfish (RC2 (46B)) algorithm has been applied for the image data encryption. The proposed work was categorized in the following section:

Implementation Details

The Java language has been used for the development of the hybrid RC2 (46B) algorithm. The integrated development environment (IDE) considered was NetBeans. Our framework is capable in the computation of different security aspects along with the performance measures.

Data Selection and Preprocessing

The image data has been considered from different repository with different sizes. In general Wang database [37] has been considered. It consists of 1,000 test images. It is further categorized into 10 different categories. Each category contains 100 images of the same pattern. These are related to Buses, African men, Dinosaur, Seas, Buildings, Roses, Elephant, Horses, Mountains and Food. These data are preprocessed in terms of matrix weight for further encryption and decryption process.

Approach

The approach of the complete procedure can be better understood through the flowchart shown in *Figure 3*. The complete procedure is shown below. In this approach image was selected from the database. Then image data preprocessing has been performed and matrix values have been obtained for the further processing. Then substitution was performed based on RC2 (46B). This substitution is efficient as it provides the best selection from the combination of the RC6 and RC4. Then the blowfish algorithm was applied after the substitution and first key generation. XOR was performed on the obtained bit. So that the maximum place value replacements were performed successfully. Then reverse mechanisms were adopted for the decryption of the data and finally the original image has been recovered. The complete mechanism was performed based on permuted value. The steps of the permutation used here are shown in permutation steps.

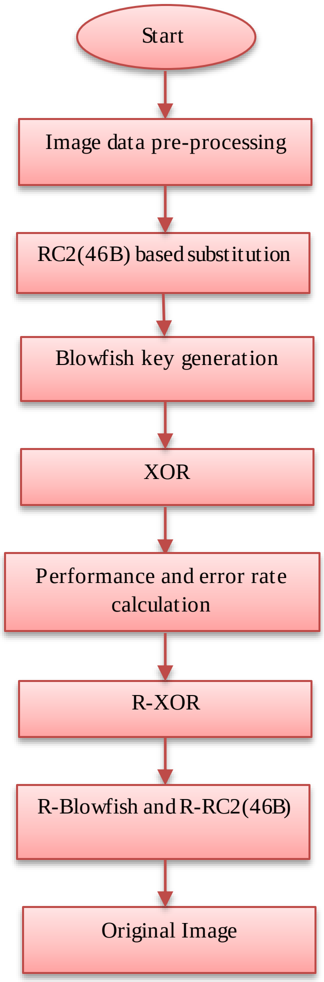
Start
Image data pre-processing
RC2(46B) based substitution
Blowfish key generation
XOR
Performance and error rate calculation
R-XOR
R-Blowfish and R-RC2(46B)
Original Image

Figure 3 Flowchart of the complete approach

Permutation Steps

Step 1: Image data have been selected from the dataset.
Step 2: It is preprocessed in the form of weight matrix.;

Step 3: It has been stored in the double dimension array.
Step 4: Double dimension image conversion has been performed based on Java methods.
Step 5: It has been passed to convert it into an object.
Step 6: Different iterations have been performed in achieving the relevant numeric content.
Step 7: This data has been appended with the methods discussed above.

3.Results and discussion

For result comparison and analysis different categorization was selected and considered. Some of the classes considered here are African Man, Elephant, Food, Barbara, Sea, Cameraman and Bus. The average error rates in case of different classes are found to be minimum in our case. This error rate shows the mean square error rate (MSE). It shows the average error rate in case of a total of 10 iterations. It is shown in *Figure 4*. Here C1-C10 belongs to the categorization classes.

Figure 5 shows the encryption time comparison for the different categorization class images. *Figure 6* shows the decryption time comparison for different categorization class images. The results clearly depict that the performance of the proposed framework is better as the error rates are less or minor. It indicates the average error rate of 0.15. In terms of average time for encryption and decryption is 92 ms It is also low due to the efficient selection of the methods of the combined framework. As the calculation of the cryptographic system depends on the combined algorithm, but the encryption and decryption were performed based on the better substitution performer. So, the time taken in the encryption and decryption is also low. This is the main benefit from our approach. The loss in terms of image pixels is also minimized as the error rate variation found from the images are minor. So it is also efficient in terms of information entropy.

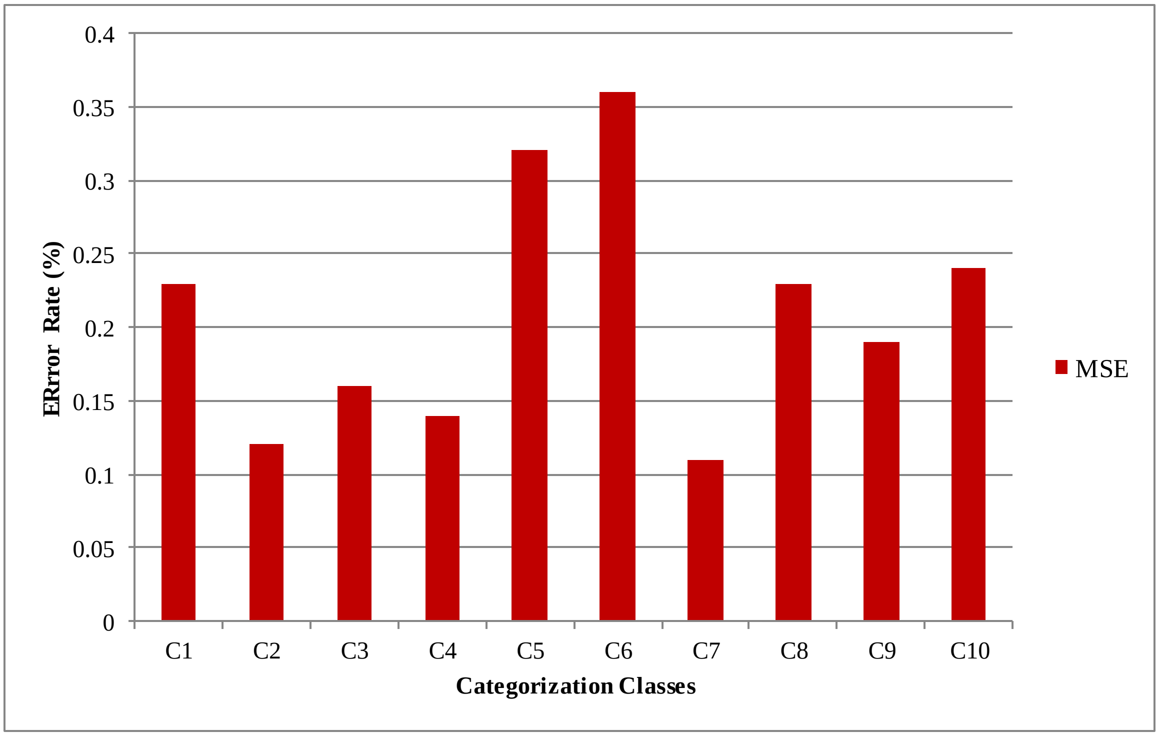

Figure 4 Error rates comparison considering different categorization classes

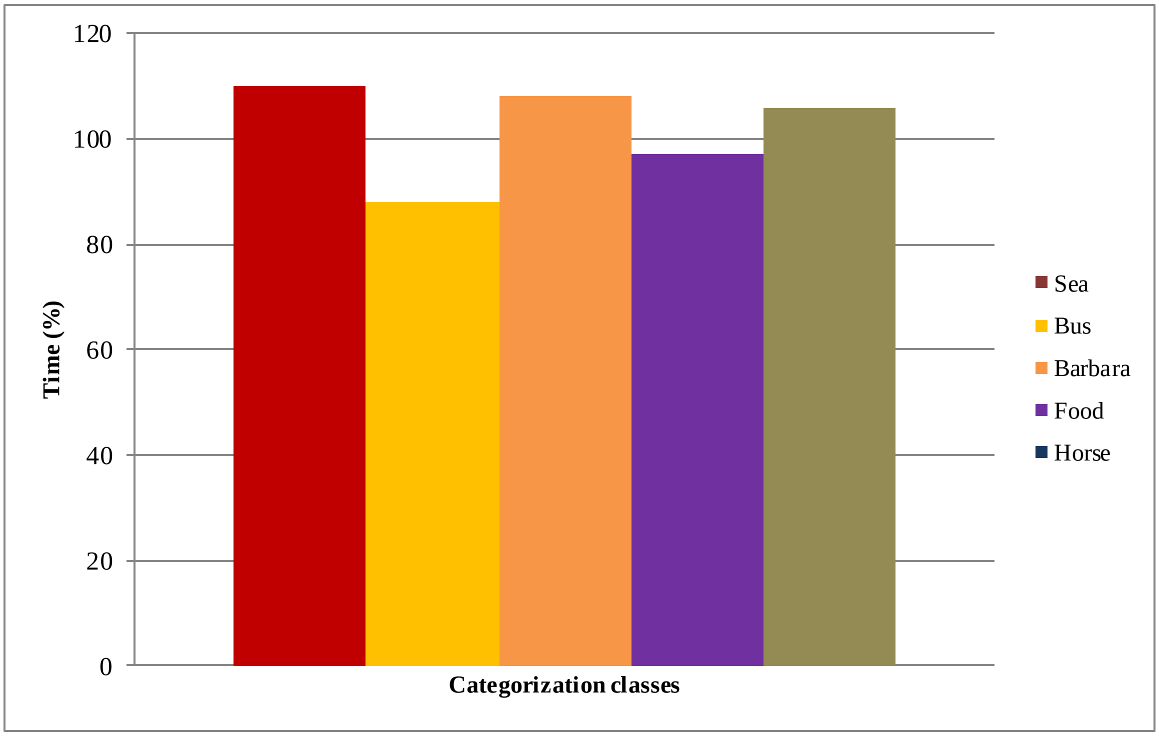

Figure 5 Encryption time comparison for different categorization class images

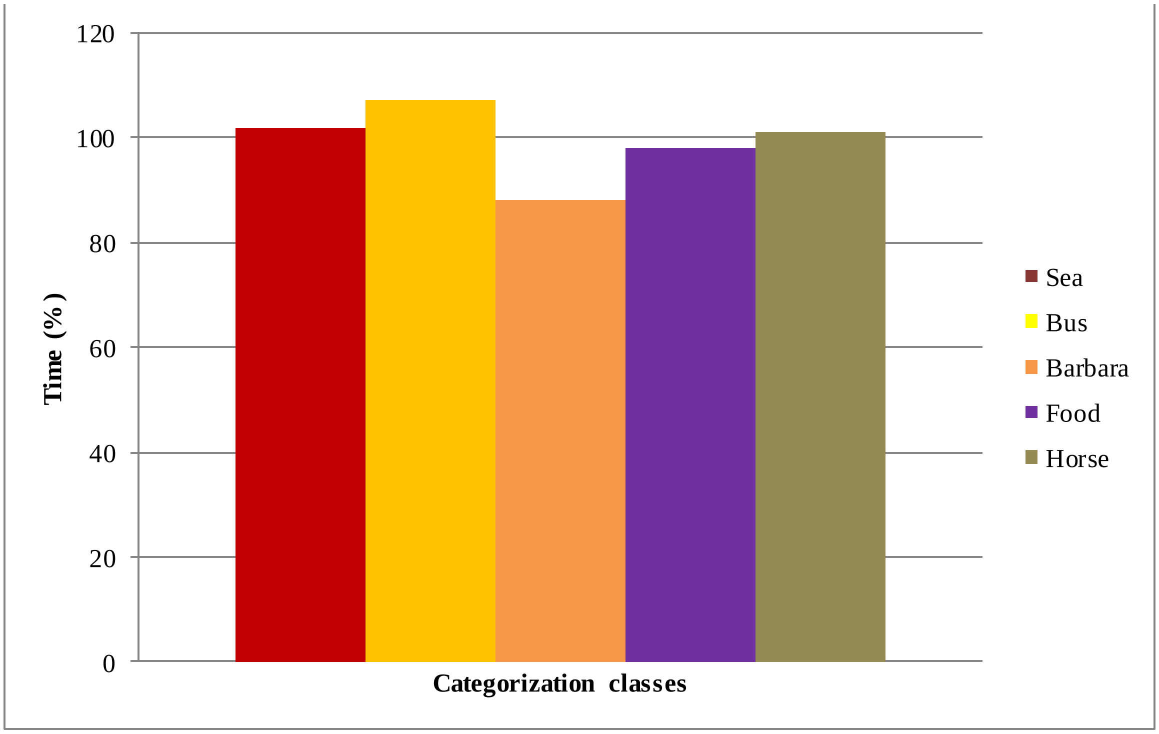

Figure 6 Decryption time comparison for different categorization class images

4.Conclusion

This paper shows the exploration of an efficient combination of RC4-RC6 with Blowfish (RC2 (46B)) algorithm. It has been applied for the image data encryption. This paper explores the approach in terms of method explanation along with the experimentation. This approach is efficient in terms of proper data preprocessing, a variety of image classes and variations in sizes. This approach is found to be better in terms of MSE rates. It is also prominent in encryption and decryption times. The variations are less so the information loss is also minimized. So this approach is efficient also in terms of information entropy.

Acknowledgment

None.

Conflicts of interest

The authors have no conflicts of interest to declare.

References

[1] Kocarev L. Chaos-based cryptography: a brief overview. IEEE Circuits and Systems Magazine. 2001; 1(3):6-21.

[2] Sasubilli SM, Dubey AK, Kumar A. Hybrid security analysis based on intelligent adaptive learning in Big Data. In International Conference on Advances in Computing and Communication Engineering 2020 (pp. 1-5). IEEE.

[3] Qiu J, Wang P. An image encryption and authentication scheme. In International Conference on Computational Intelligence and Security 2011 (pp. 784-7). IEEE.

[4] Sasubilli SM, Dubey AK, Kumar A. A computational and analytical approach for cloud computing security with user data management. In International Conference on Advances in Computing and Communication Engineering 2020 (pp. 1-5). IEEE.

[5] Hu G, Feng Z, Wang L. Analysis of a type of digital chaotic cryptosystem. In International Symposium on Circuits and Systems. Proceedings 2002 (Vol. 3, pp. III-I). IEEE.

[6] Boiko J, Kovtun I, Petrashchuk S. Productivity of telecommunication systems with modified signal-code constructions. In International Scientific-Practical Conference Problems of Infocommunications. Science and Technology 2017 (pp. 173-8). IEEE.

[7] Millérioux G, Amigó JM, Daafouz J. A connection between chaotic and conventional cryptography. IEEE Transactions on Circuits and Systems I: Regular Papers. 2008; 55(6):1695-703.

[8] Zahan A, Hossain MS, Rahman Z, Shezan SK. Smart home IoT use case with elliptic curve based digital signature: an evaluation on security and performance analysis. International Journal of Advanced Technology and Engineering Exploration. 2020;7(62):11-9.

[9] Ni Z, Shi YQ, Ansari N, Su W. Reversible data hiding. IEEE Transactions on Circuits and Systems for Video Technology. 2006; 16(3):354-62.

[10] Nazmudeen NH, Farsana FJ. Satellite image security improvement by combining DWT-DCT watermarking and AES encryption. International Journal of Advanced Computer Research. 2014; 4(2):645-52.

[11] Seethalakshmi AV, Hemachitra HS. Complex type seed variety identification and recognition using optimized image processing techniques. ACCENTS Transactions on Image Processing and Computer Vision. 2020; 6 (19): 23-31.

[12] Gladwin SJ, Gowthami PL. Combined cryptography and steganography for enhanced security in suboptimal images. In International Conference on Artificial Intelligence and Signal Processing 2020 (pp. 1-5). IEEE.

[13] Al-Kadei FH, Mardan HA, Minas NA. Speed up image encryption by using RSA algorithm. In international conference on advanced computing and communication systems 2020 (pp. 1302-7). IEEE.

[14] Duan X, Guo D, Liu N, Li B, Gou M, Qin C. A new high capacity image steganography method combined with image elliptic curve cryptography and deep neural network. IEEE Access. 2020; 8:25777-88.

[15] Dubey AK, Dubey AK, Namdev M, Shrivastava SS. Cloud-user security based on RSA and MD5 algorithm for resource attestation and sharing in java environment. In CSI international conference on software engineering 2012 (pp. 1-8). IEEE.

[16] Sharma V, Shukla M, Srivastava S, Mandal R. Generative network based image encryption. In International Conference on Intelligent Computing and Control Systems 2020 (pp. 1-5). IEEE.

[17] Abhinav A, Manikandan VM, Bini AA. An improved reversible data hiding on encrypted images by selective pixel flipping technique. In international conference on devices, circuits and systems 2020 (pp. 294-8). IEEE.

[18] Santos TA, Magalhães EP, Basílio NP, Nepomuceno EG, Karimov TI, Butusov DN. Improving chaotic image encryption using maps with small Lyapunov exponents. In Moscow workshop on electronic and networking technologies 2020 (pp. 1-4). IEEE.

[19] Hu D, Zheng Y, Zhang H, Sun S, Xie F, Shi J, Jiang Z. Informative retrieval framework for histopathology whole slides images based on deep hashing network. In international symposium on biomedical imaging 2020 (pp. 244-8). IEEE.

[20] Yadahalli SS, Rege S, Sonkusare R. Implementation and analysis of image steganography using least significant bit and discrete wavelet transform techniques. In international conference on communication and electronics systems 2020 (pp. 1325-30). IEEE.

[21] Kalaichelvi T, Apuroop P. Image steganography method to achieve confidentiality using CAPTCHA for authentication. In international conference on communication and electronics systems 2020 (pp. 495-9). IEEE.

[22] Ye H, Huang S, Liu W. Research on image scrambling method based on combination of Arnold transform and exclusive-or operation. In information technology, networking, electronic and automation control conference 2020 (Vol. 1, pp. 151-4). IEEE.

[23] Srivastava M, Siddiqui J, Ali MA. Local binary pattern based technique for content based image copy detection. In international conference on power electronics & IoT applications in renewable energy and its control 2020 (pp. 374-7). IEEE.

[24] Samvatsar M, Kanungo P. An analytical review and analysis for the data control and security in cloud computing. International Journal of Advanced Technology and Engineering Exploration. 2020; 7(73):241-6.

[25] Pramanik S, Bandyopadhyay SK, Ghosh R. Signature image hiding in color image using steganography and cryptography based on digital signature concepts. In international conference on innovative mechanisms for industry applications 2020 (pp. 665-9). IEEE.

[26] Kushnir M, Kosovan H, Kroialo P, Komarnytskyy A. Encryption of the images on the basis of two chaotic systems with the use of fuzzy logic. In international conference on advanced trends in radioelectronics, telecommunications and computer engineering 2020 (pp. 610-3). IEEE.

[27] Han B, Jia Y, Huang G, Cai L. A medical image encryption algorithm based on Hermite chaotic neural network. In information technology, networking, electronic and automation control conference 2020 (Vol. 1, pp. 2644-8). IEEE.

[28] Kaur S, Jindal A. Singular value decomposition (SVD) based image tamper detection scheme. In international conference on inventive computation technologies 2020 (pp. 695-9). IEEE.

[29] Abdulrahman A, Varol S. A review of image segmentation using MATLAB environment. In international symposium on digital forensics and security 2020 (pp. 1-5). IEEE.

[30] Zhang H, Zhu J, Zhao S, He Q, Zhong X, Liu J. A new image encryption algorithm based on 2D-LSIMM chaotic map. In international conference on advanced computational intelligence 2020 (pp. 326-33). IEEE.

[31] Abdallah Y. Segmentation of brain stroke lesions using marker-based algorithms in CT images. In international conference on computer applications & information security 2020 (pp. 1-4). IEEE.

[32] Yadahalli SS, Rege S, Sonkusare R. Implementation and analysis of image steganography using least significant bit and discrete wavelet transform techniques. In international conference on communication and electronics systems 2020 (pp. 1325-30). IEEE.

[33] Luo Y, Zhu L. Research on data augmentation for object detection based on x-ray security inspection picture. In international conference on advances in electrical engineering and computer applications 2020 (pp. 219-22). IEEE.

[34] Kukharska N, Lagun A, Polotai O. The steganographic approach to data protection using Arnold algorithm and the pixel-value differencing method. In international conference on data stream mining & processing 2020 (pp. 174-7). IEEE.

[35] Kumar PR, Sarkar A, Mohanty SN, Kumar PP. Segmentation of white blood cells using image segmentation algorithms. In international conference on computing, communication and security 2020 (pp. 1-4). IEEE.

[36] Arpacı B, Kurt E. An innovative tool for the chaotic image encryption, decryption and security tests. In international conference on electrical, communication, and computer engineering 2020 (pp. 1-8). IEEE.

[37] Wang JZ, Li J, Wiederhold G. SIMPLIcity: Semantics-sensitive integrated matching for picture libraries. IEEE Transactions on Pattern Analysis and Machine Intelligence. 2001; 23(9):947-63.

Shubham Patil received the B.E degree in Information Technology from North Maharashtra University, Jalgaon, Maharashtra in 2013. He is Currently pursuing M.Tech from SSSUTMS, Sehore, MP.

Email: meet2shub@gmail.com