Research Article

ACCENTS Transactions on Information Security, Vol 6(24)
ISSN (Online): 2455-7196
http://dx.doi.org/10.19101/TIS.2021.621007

An efficient hybrid encryption approach with bit shuffling for image data security

Akrati Shrivastava* **and Animesh Kumar Dubey**
Department of Computer Science, PCST Bhopal, Madhya Pradesh

Received: 20-November -2021; Revised: 20-December-2021; Accepted: 22-December-2021
©2021 Akrati Shrivastava and Animesh Kumar Dubey. This is an open access article distributed under the Creative Commons Attribution (CC BY) License, which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

Abstract
In the current scenario there is the need of data security to make the communication more secure and reliable. In this paper image data security has been discussed. The major problem is to provide security in less time with minimum loss of data. In this paper a combination of RSA, RC4 and blowfish (R2B) algorithms have been used for the data encryption and decryption purpose. For experimentation different images have been considered from different databases. The experimentation has been considered based on mean squared error (MSE), encryption time and overall processing time. The results have been considered based on different iterations to reduce any computational biasness. The results clearly show the improvement in error rates, encryption time and overall processing time as comparison to the traditional approaches.

Keywords
Bit shuffling, RSA, RC4, R2B algorithm, MSE.

1.Introduction
The current world is the data world. In the today's communication scenario ample amount of data have been used for the communication using several means [1−3]. Text and image data have been used especially for the communication as per the software application flexibility. So, it is clear that only the intended person should receive the data. Due to this there is the need of proper data security in the middle of the communication [4−8]. So, cryptography and steganography approaches can be used to secure the data communication. There are several algorithms available which can be used for this purpose. In cryptography, there are two types of algorithms one is symmetric key cryptography and another one is asymmetric key cryptography. Only one key is applicable for the encryption and decryption in the symmetric key encryption [9, 10]. Examples are advanced encryption standard (AES), data encryption standard (DES), International Data Encryption Algorithm (IDEA), etc. In asymmetric key cryptography, one key is needed separately for encryption and another one is used for decryption [11, 12]. Digital signature algorithm (DSA), Rivest-Shamir-Adleman (RSA) algorithm, Diffie-Hellman, etc. are some of the examples of asymmetric key cryptography.

So, in this paper the main motivation is to secure the data especially the image data. The main aim is to develop a hybrid approach for providing better security. The general steps of encryption and decryption is shown in *Figure 1*.

In 2020, Pepe et al. [13] proposed a system for encryption and compression. Chaotic compressive sensing has been used for the encryption. Compression has been performed based on stacked autoencoder. It shows slower decrease in the peak signal-to-noise ratio (PSNR). In 2020, Madhu and Vasuhi [14] proposed an integrated approach based on cryptography and steganography. They have used rail fence cipher. Their results shou high performance in terms of improve PSNR and low mean squared error (MSE). In 2021, Mansoor et al. [15] proposed an image encryption system based on pixels. Their results are efficient in encryption time as well as security. In 2021, Shanthakumari et al. [16] used cryptography and steganography for enhancing security. They used blowfish algorithm. For improving the hiding capacity, they have used random number generator and range technique. They

*Author for correspondence

have also tested different attacks for the analysis. In 2020, Gupta and Vijay [17] discussed compression and encryption aspects. They used AES and DES algorithms. Their result shows improved security. In 2020, Preethi and Asokan [18] discussed regarding the quality of image after watermarking. They have used region of non-interest identification method with the quality factor calculation with the neural network system. They achieved improved performance in terms of PSNR, MSE and correlation coefficient. In 2020, Pramanik et al. [19] discussed the hybridization of cryptography and steganography. They have considered main two components inn their approach. These area size of the encrypted object and degree of security. In 2020, Agra and Nisa [20] discussed about image privacy and storing issues. They have used AES encryption algorithm for the security purpose. They have compared their approach with the related approaches and found the effectiveness of the method. In 2021, Zhao et al. [21] discussed the security issues in the ultra-high definition video. They have used double-blind subjective experiment. Encryption sequence has been used to show the dataset covers. It improves the security index.

Overall literature shows the need of hybrid encryption algorithm for the improvement of data security. This paper main aim is to explore the same with proper result discussion.

Figure 1 General process of encryption and decryption

2.Methods

In this paper an efficient combination of cryptography has been presented. The combination includes the RSA, RC4 and blowfish (R2B) algorithm. In this section the working mechanism of the algorithm has been presented with the step-by-step procedure.

The complete approach is divided into following parts:

1. Implementation environment
2. Dataset
3. Approach
4. Working process

Implementation environment

This algorithm is implemented in Java. The integrated development environment used for the implementation was NETBEANS.

Dataset

The famous 1000 image dataset have been considered from Wang et al. [22]. It consists of total of 1000 images of ten different classes. It means for each class 100 images are there. The images are related to Mountains, African men, Buses, Dinosaur etc. We have also gathered some related image data like Leena image, Barbara images etc. for the experimentation. of this dataset

Approach

In our work first the data is selected from the image database. It is then preprocessed for the weight matrix calculation. Then R2B encryption algorithm has been applied. The random shift operation has been used for the final key generations. Then for bit shuffling XOR with random key has been applied. Then for the reverse procedure key with XOR has been applied and finally R2B decryption has been performed.

Algorithm steps are as follows:

Step 1: Image selection from the dataset.
Step 2: Weight matrix calculation and preprocessing has been performed.
Step 3: Different iterations have been performed to calculate the matrix and converted it into pixel object.
Step 4: R2B Encryption has been applied on the image data.
Step 5: Key Generation with random shift has been performed and analyzed.
Step 6: XOR with random key has been used for bit shuffling.
Step 7: For the decryption process Key with XOR and R2B Decryption has been applied.

Working process

The complete working procedure is shown in *Figure 2*. It shows the iterative steps of data processing along with the encryption and decryption procedure. The randomization procedure helps in the generation

of new key at each of the process. XOR with random key provides the encryption with the random bit. It will help in the improvement of data security.

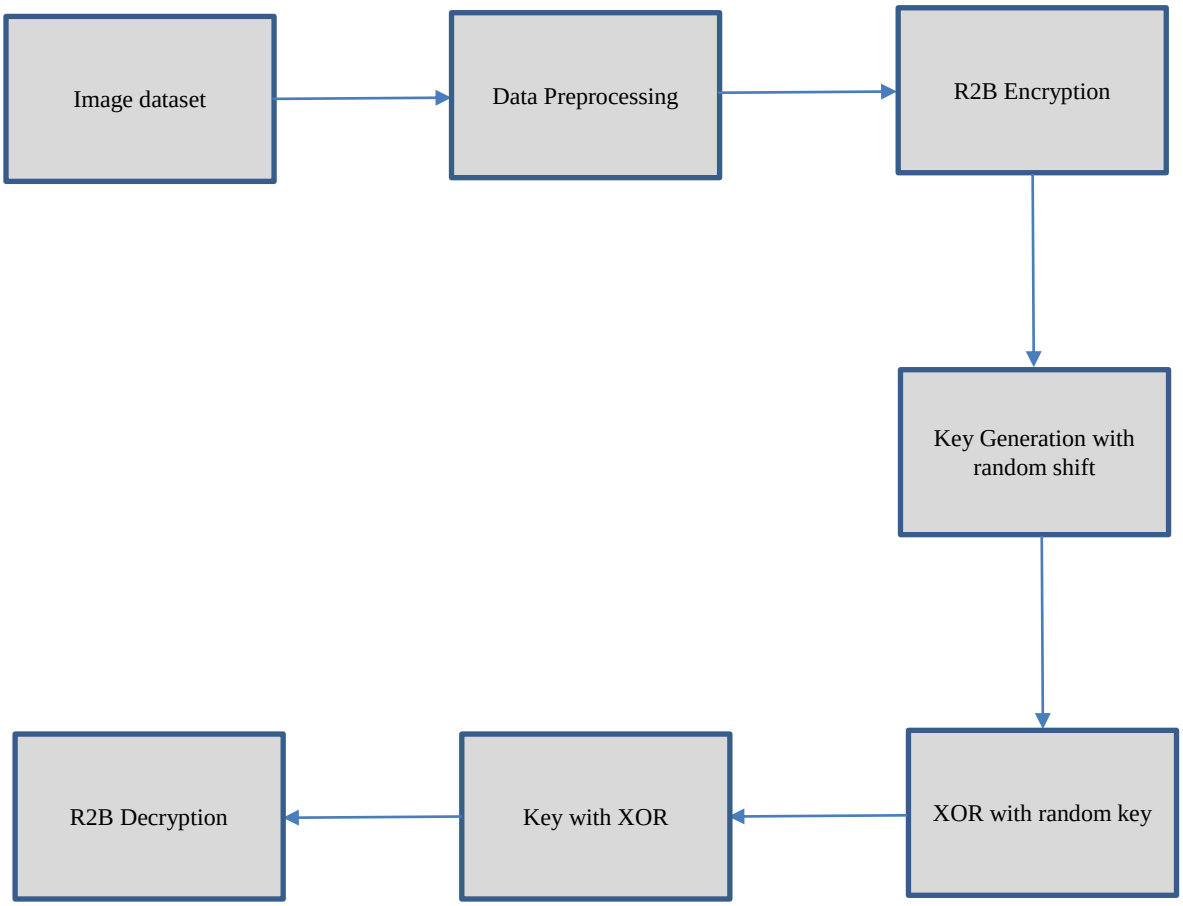

Figure 2 Working procedure of the complete approach

3.Results and discussion

For the experimentation different images have been considered with variable number of iterations. The first comparison has been performed based on error metrics that is MSE. The MSE values in case of our approach is found to be minimum. The average error rate is 0.25 approximately. The comparison shows that our approach is better in terms of MSE. *Figure 3* shows the MSE comparison with different images with average error rates. *Figure 4* shows the time comparison with different images with average time (encryption process). Encryption time in case of our approach is also less in comparison to the previous approach. It is shown in second. The average encryption time is also less in case of different iterations. *Figure 5* shows the time comparison with different images with average time (process time). It shows the complete time of processing of an image. So based on the results it can be said that our approach has less error rates with less overall processing time. Based on different key configuration it is also robust and secure.

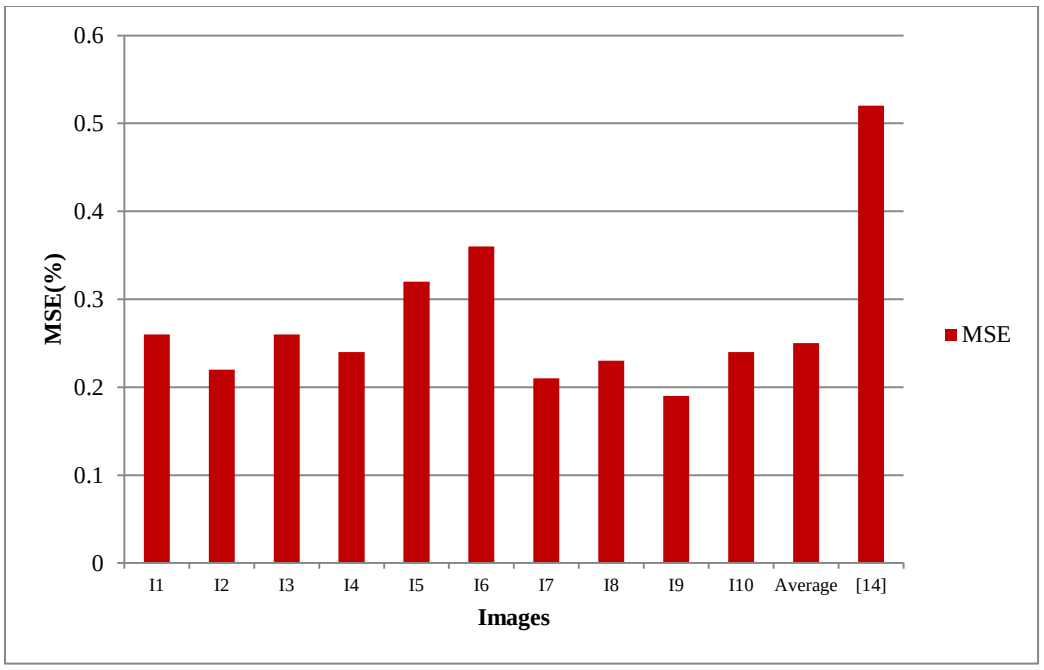

Figure 3 MSE comparison with different images with average error rates

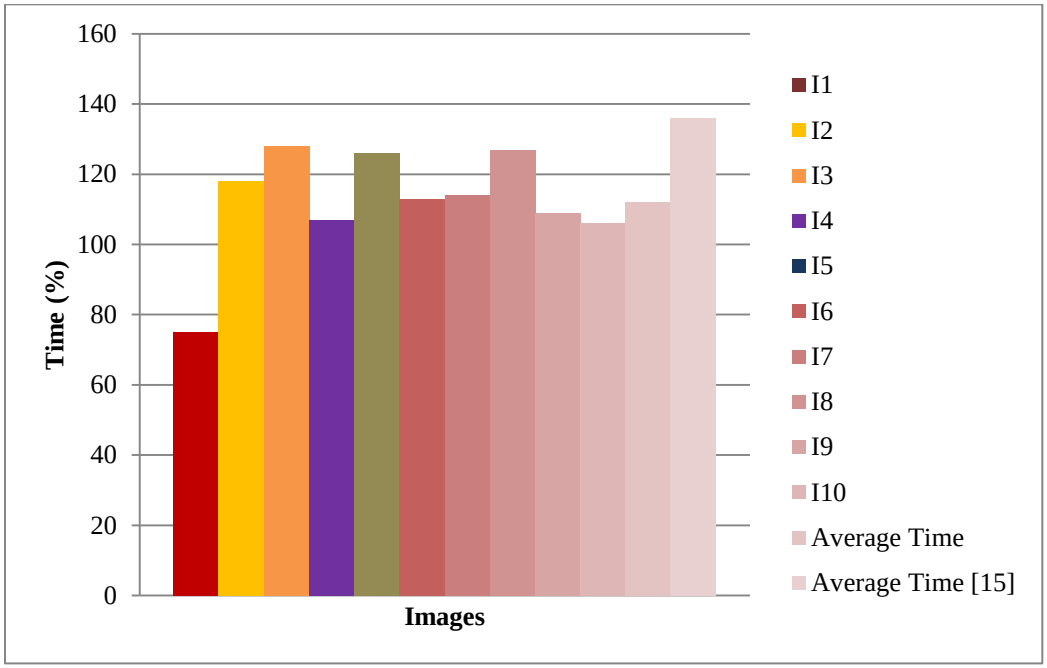

Figure 4 Time comparison with different images with average time (Encryption Process)

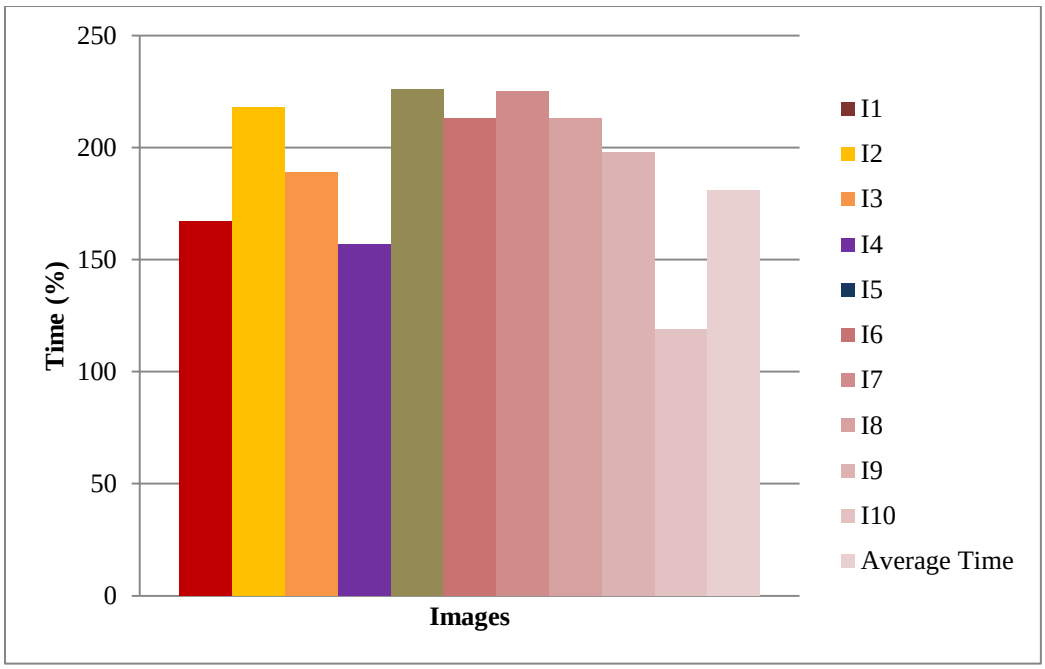

Figure 5 Time comparison with different images with average time (Process Time)

4.Conclusion

In this paper an efficient image data encryption has been presented based on R2B algorithm. It provides a robust encryption algorithm due to the combination of RSA, RC4 and blowfish algorithm. Due to complex mathematics of RSA, it provides a robust design. The time taken for the encryption and decryption is less due to RC4 as it requires less memory. The operations in the blowfish are also less and tedious which improves the overall processing time. The combination makes the framework robust and complex to decipher it. The result indicates the improvement in terms of MSE, encryption time and overall processing time.

Acknowledgment

None.

Conflicts of interest

The authors have no conflicts of interest to declare.

References

[1] Alwan ZA, Farhan HM, Mahdi SQ. Color image steganography in YCbCr space. International Journal of Electrical & Computer Engineering (2088-8708). 2020; 10(1):202-9.

[2] Abdullah HN, Zeboon HT, Mansor AJ. Digital image encryption by random pixel selecting using chaotic sequences. Journal of Al-Ma'moon College. 2015(26):228-36.

[3] Gupta P, Singh S, Mangal I. Image encryption based on Arnold cat map and S-box. International Journal of Advanced Research in Computer Science and Software Engineering. 2014; 4(8):807-12.

[4] 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 (ICACCE) 2020 (pp. 1-5). IEEE.

[5] Qiu J, Wang P. An image encryption and authentication scheme. In seventh international conference on computational intelligence and security 2011 (pp. 784-7). IEEE.

[6] Jolfaei A, Mirghadri A. A new approach to measure quality of image encryption. International Journal of Computer and Network Security. 2010; 2(8):38-44.

[7] 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 (ICACCE) 2020 (pp. 1-5). IEEE.

[8] 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.

[9] 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 sixth international conference on software engineering (CONSEG) 2012 (pp. 1-8). IEEE.

[10] Zhang X. Lossy compression and iterative reconstruction for encrypted image. IEEE transactions on information forensics and security. 2010; 6(1):53-8.

[11] Kovalchuk A, Izonin I, Strauss C, Podavalkina M, Lotoshynska N, Kustra N. Image encryption and decryption schemes using linear and quadratic fractal algorithms and their systems. In DCSMart 2019 (pp. 139-50).
[12] Huang M, Yang C, Zhang Y. Selective encryption of H. 264/AVC based on block weight model. In 18th international conference on communication technology (ICCT) 2018 (pp. 1368-73). IEEE.
[13] Pepe A, Fu HY, Liu X, Khan FN. Multimedia data encryption and compression via hybrid chaotic compressive sensing and latent vector transmission. In international conference on advanced infocomm technology (ICAIT) 2020 (pp. 107-10). IEEE.
[14] Madhu D, Vasuhi S. Image steganography: 2-Bit XOR algorithm used in YCbCr color model with crypto-algorithm. In 4th international conference on computer, communication and signal processing (ICCCSP) 2020 (pp. 1-5). IEEE.
[15] Mansoor AJ, Abdullah HN, Al-Gailani MF, Ziboon HT. Chaotic encryption system based on pixel value and position transformation for color images. In international multi-conference on systems, signals & devices (SSD) 2021 (pp. 433-9). IEEE.
[16] Shanthakumari R, Varadhaganapathy S, Vinothkumar S, Bharaneeshwar B. Data hiding in image steganography using range technique for secure communication. In international conference on advances in electrical, computing, communication and sustainable technologies (ICAECT) 2021 (pp. 1-7). IEEE.
[17] Gupta N, Vijay R. Effect on reconstruction of images by applying fractal based lossy compression followed by symmetrical encryption techniques. In 11th international conference on computing, communication and networking technologies (ICCCNT) 2020 (pp. 1-7). IEEE.
[18] Preethi P and Asokan R. Neural network oriented RONI prediction for embedding process with hex code encryption in DICOM Images. International Conference on advances in computing, communication control and networking 2020 (pp. 739-43). IEEE.
[19] Pramanik S, Bandyopadhyay SK, Ghosh R. Signature image hiding in color image using steganography and cryptography based on digital signature concepts. In 2nd international conference on innovative mechanisms for industry applications (ICIMIA) 2020 (pp. 665-9). IEEE.
[20] Agra S, Nisa AK. Analyzing the effectiveness of metamorphosing images using color maps. In third international conference on smart systems and inventive technology (ICSSIT) 2020 (pp. 1279-85). IEEE.
[21] Zhao Y, Yang C, Tang B. Construction of perceptual security dataset for video selective encryption based on double-blind subjective experiment. In international conference on information communication and software engineering (ICICSE) 2021 (pp. 30-5). IEEE.
[22] 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.

Akrati Shrivastava is a M.Tech in Computer Science & Application, PCST RGPV Bhopal. BE in Computer Science & Engeenering TIT RGPV Bhopal. Her Areas of Interest are Computer Science & Application.

Email: akratishrivastava380@gmail.com

Animesh Kumar Dubey is working as Assistant professor with the department of Computer Science and Engineering, at Patel College of Science and Technology, Bhopal, India. He has completed his Bachelor of Engineering (B.E.) and MTech. degree with Computer Science Engineering from Rajeev Gandhi Technical University, Bhopal (M.P.). He has more than 15 publications in reputed, peer-reviewed national and international journals and conferences. His research areas are Data Mining, Optimization, Machine Learning, Cloud Computing and Artificial Intelligence.
Email:animeshdubey123@gmail.com