Research Article

ACCENTS Transactions on Information Security, Vol 5(20)
ISSN (Online): 2455-7196
http://dx.doi.org/10.19101/TIS.2020.517004

An efficient image cryptography mechanism based on the hybridization of standard encryption algorithms

Vivek Ranjan[1*], Kailash Patidar[2] and Rishi Kushwaha[2]
M.Tech Scholar, Department of Computer Science Engineering, Sri Satya Sai University of Technology & Medical Sciences, Sehore, Madhya Pradesh, India[1]
Assistant Professor, Department of Computer Science Engineering, Sri Satya Sai University of Technology & Medical Sciences, Sehore, Madhya Pradesh, India[2]

Abstract
In our approach the combination of RC4 and Blowfish algorithms with chaos mapping (RC4BC) has been presented for the image encryption. In the first phase image dataset has been considered. Then weight values have been calculated based on the image pixels. It has been calculated based on the attribute pixel, corelated pixels and the analytical factors of the edges. Then substitution has been performed through RC4 encryption mechanism. The substitution has been performed based on 8 sub blocks for the first time. After that different random substation has been applied based on the reallocation of bytes up to 16 rounds. Final substitution has been performed by the blowfish and chaos mapping. By this method the pixels of the images are rotated and shuffled with the XOR operation along with 16-byte reshuffling in each iteration. A total of 50 rounds have been considered for the shuffling, rotation and mapping. Then for comparative analysis peak signal to noise ratio (PSNR) and mean square error (MSE) have been calculated. Our results show that it is efficient in terms of MSE and PSNR values.

Keywords
RC4, Blowfish, RC4BC, MSE, PSNR.

1.Introduction
In the current scenario there is the need of research and development in digital cryptography research [1─3]. Encryption and decryption procedure can be applied based on the nature of key applicability. It can be categorized as public key cryptography and private key cryptography [4]. There are different other techniques for chaos determination [5]. There are several other hiding mechanisms which can be incorporated for the secure message transmission [6]. Data security aspect has been used widely including medical domain, cloud computing and big data [7─10].

In general, two types of security mechanism have been adopted. One is cryptography and another one is steganography. Cryptography mechanism includes encryption and decryption process. Steganography is the process for hiding data into another data [11]. These techniques can be applied on text, images and videos.

This paper covers the image data security mechanism based on RC4 and Blowfish algorithms with chaos mapping (RC4BC). In 2020, Gladwin and Gowthami [12] discussed about data security and privacy threats. They have proposed a robust approach which is based on elliptic curve cryptography (ECC) and hill cipher. They have used least significant bits (LSB) watermarking for the image embedding. Key has been generated based on ECC. Hill cipher has been used for the ciphertext generation. Their combined approach has the capability of increasing data authorship and ownership. In 2020, Al-Kadei et al. [13] discussed about existing RSA algorithm. They have suggested the need of changes in existing RSA algorithm. It is so because of the long key sizes, big memory spaces and long execution time. They have developed three experiments. It has been developed for the execution time examination. Their result indicates the improvement in the execution time. In 2020, Duan et al. [14] discussed about the sensitive information hiding. They have proposed a new high capacity image steganography method. For the secret image steganography, they have used discrete cosine transform (DCT). The encryption

*Author for correspondence

process of the transformed image has been performed based on the ECC. They have used SegNet also for the improvement of steganographic capacity. Their approach achieved highest peak signal-to-noise ratio (PSNR) and structural similarity index (SSIM). In 2020, Abhinav et al. [15] discussed about reversible data hiding. They have proposed a new scheme for the block size reduction. It has been developed in such manner that it may reduce the bit error rate. In 2020, Sharma et al. [16] proposed an approach which is the combination of image steganography and generative adversarial network. They have used multiple layers of encryption for processing the image matrix. The new image is then passed to the generative adversarial network for the conversion it into the new model. In 2020, Hu et al. [17] discussed about the computer-aided cancer diagnosis. They have discussed in case of histopathology whole slide images (WSIs). They have proposed a retrieval framework. It is based on deep hashing network. They have proposed a loss function. They have applied this approach on the ACDC-LungHP dataset. It has been found to be prominent in case of large-scale database. In 2020, Santos et al. [18] discussed about chaos-based encryption. They have analyzed cryptography techniques. They have analyzed problems regarding finite precision. They have suggested that the performance improvement is possible through Lyapunov exponents. In 2020, Yadahalli et al. [19] discussed about the steganography. They have applied LSB and DWT method for the image steganography. They have considered different image parameters for the detail analysis on the resultant images. In 2020, Kalaichelvi and Apuroop [20] discussed about the steganography methods. They have applied CAPTCHA codes for the validation at the receiver end. They have used randomized CAPTCHA code. It has been used for additional security. In 2020, Ye et al. [21] discussed about the encryption problem in digital image. They have proposed an image scrambling algorithm. This algorithm is based on Arnold transform and XOR operation. For the changes in pixel position they have used Arnold transform. Then XOR operation has been performed on the scrambled image. Their results suggest that their approach is found to be useful in case of digital images. In 2020, Srivastava et al. [22] discussed about the increase in the duplicate copies of the original images. They have proposed a hashing technique based on LBP. They have preprocessed it for any type of minor effects removal. They have applied LBP for the feature's identification. Their approach is found to be prominent in online detection of image copies. In 2020, Harini et al. [23] discussed about the digital image communication. They have used integer wavelet transform (IWT) for the image separation. It has been separated in approximation coefficients and detailed coefficients. They have achieved the entropy of 7.97. In 2020, Pramanik et al. [24] discussed about data transmission. They have investigated and analyzed blend cryptography and steganography. They have considered cryptography and steganography both. It has been considered based on encrypted object size and the degree of security. It has been used for the purpose of message authentication, message integrity and non-repudiation purpose. In 2020, Maurya et al. [25] discussed about visual cryptography. They have proposed an extended visual cryptography technique (EVCT). They have considered medical images. It has been encrypted and three cover images have been considered for embedding. For the secret image they have considered 3×3 block size. Their approach is found to be lossless and less complex. In 2020, Rane et al. [26] discussed about the visual cryptography. They have proposed an online voting System. It has been proposed for Maharashtra Carrom association. They have used CAPTCHA code and image share technology for maintaining the security. Their approach is helpful in maintaining anonymity and security. In 2020, Kushnir et al. [27] discussed about chaotic encryption. They have proposed an image encryption system. It is based on two chaotic mapping that uses fuzzy logic. They have analyzed the statistical analysis. It has been performed based on histogram, entropy of information and correlation coefficient. In 2020, Han et al. [28] proposed a medical image encryption algorithm. It is based on Hermite chaotic neural network. It has been used to train the Hermite chaotic neural network. This is used for the encryption purpose for the medical image. It is found to be effective in terms of key sensitivity and key space. In 2020, Kaur and Jindal [29] discussed about the image authentication techniques. They have used singular value decomposition (SVD). It has been used for the extraction of the important features of images. QR code has been created based on quick response code.

2.Methods

Our approach is divided into five parts:

1. Image dataset: In the first phase image dataset has been considered from James Z. Wang [30] database. Ten image classes are there in this database having 100 images for each class.
2. Weight matching: Then weight values have been calculated based on the image pixels. It has been

calculated based on the attribute pixel, corelated pixels and the analytical factors of the edges. The combined weight is then assigned to the calculated edge value for the further preprocessing. It has been assigned and reevaluated in all the cases.

3. RC4: Then substitution has been performed through RC4 encryption mechanism. The substitution has been performed based on 8 sub blocks for the first time. After that different random substation has been applied based on the reallocation of bytes up to 16 rounds. The substitution key is generated and permutated also in this phase. It is then used for the encryption and decryption process
4. Blowfish and Chaos substitution: Final substitution has been performed by the blowfish and chaos mapping. By this method the pixels of the images are rotated and shuffled with the XOR operation along with 16-byte reshuffling in each iteration. A total of 50 rounds have been considered for the shuffling, rotation and mapping.
5. Decryption: The same reversible process has been used for the decryption of the image.

The above process is also clearly depicted from *Figure 1*.

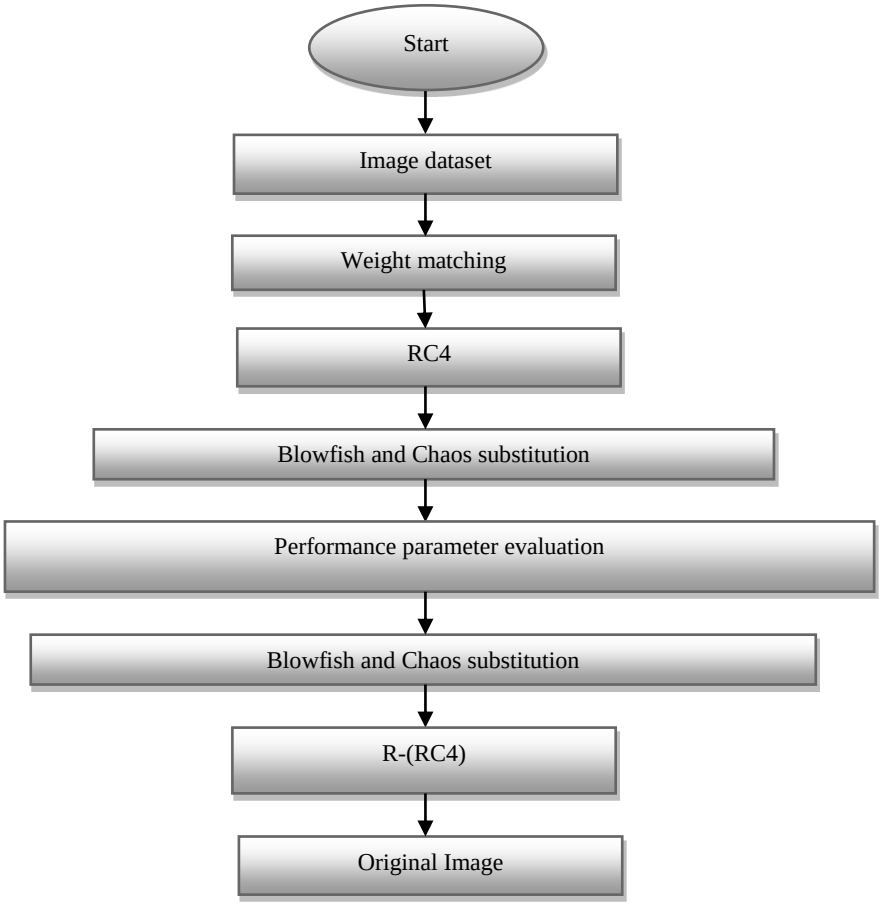

Figure 1 Working procedure flowchart

3.Results

For the performance evaluation of the RC4BC algorithm two performance evaluation parameters have been considered. These are mean square error (MSE) and peak signal to noise ratio (PSNR).

Mean square error (MSE) = $\frac{\sum_{M,N}[I_1(m,n)-I_2(m,n)]}{M \times N}$

M and N are the number of rows and columns

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

R is the maximum fluctuation in the input in the image data type.

Figure 2 and *3* shows the MSE and PSNR values obtained by our approach.

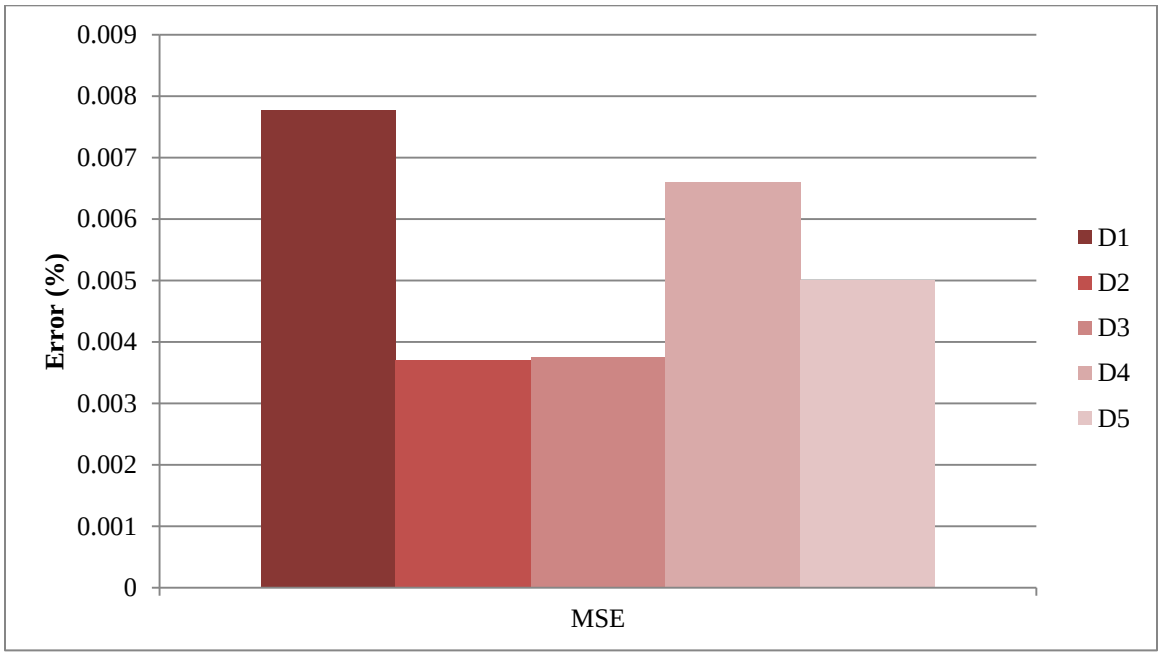

Figure 2 MSE comparison for images

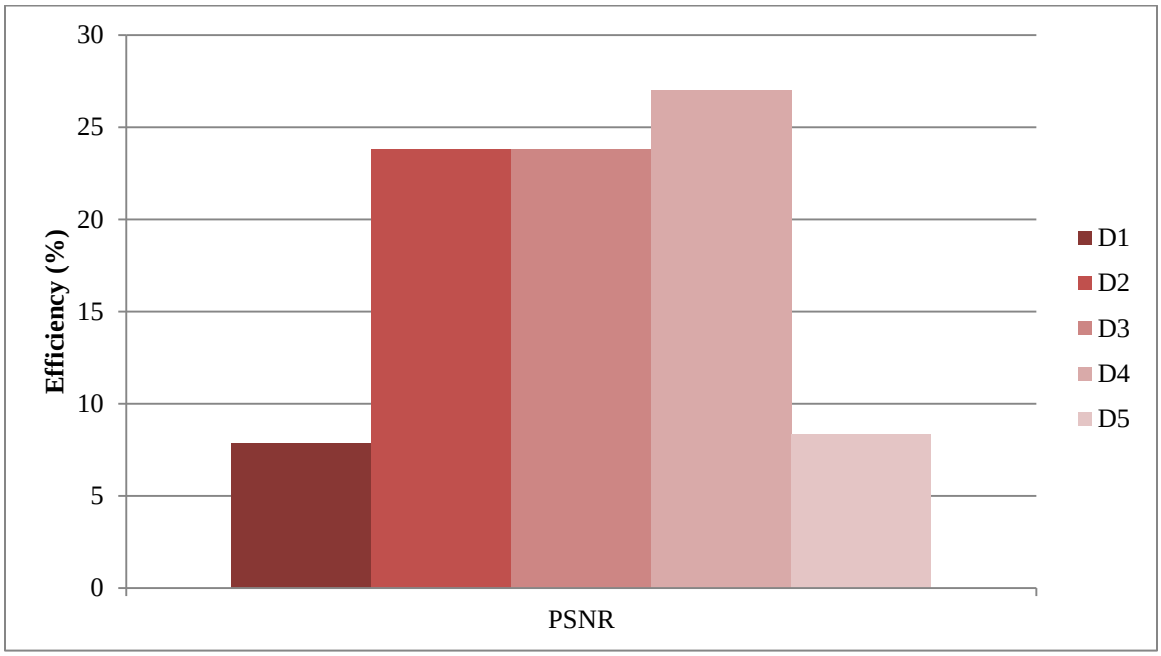

Figure 3 PSNR comparison for images

4.Conclusion

For image data security RC4BC algorithm has been presented. Ten image classes have been considered for the experimentation. Then weight values have been calculated based on the image pixels. Then substitution has been performed through RC4 encryption mechanism. The substitution has been performed based on 8 sub blocks for the first time. After that different random substation has been applied based on the reallocation of bytes up to 16 rounds. Final substitution has been performed by the blowfish and chaos mapping. A total of 50 rounds have been considered for the shuffling, rotation and mapping. Then MSE and PSNR have been compared and analyzed.

Acknowledgment

None.

Conflicts of interest

The authors have no conflicts of interest to declare.

References

[1] Hu G, Feng Z, Wang L. Analysis of a type of digital chaotic cryptosystem. In international symposium on circuits and systems. proceedings 2002 (pp. III-III). IEEE.

[2] 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.

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

[4] 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.

[5] 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.

[6] 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.

[7] 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.

[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] 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.

[10] Provos N, Honeyman P. Hide and seek: An introduction to steganography. IEEE Security & Privacy. 2003; 1(3):32-44.

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

[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] 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.

[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] 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 IEEE international symposium on biomedical imaging 2020 (pp. 244-8). 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] 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.

[20] 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.

[21] 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 (pp. 151-4). IEEE.

[22] 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.

[23] Harini M, Dhivya R, Rengarajan A. Implementation of image encryption based on chaos-IWT–an image security. In international conference on computer communication and informatics 2020 (pp. 1-4). IEEE.

[24] 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.

[25] Maurya R, Kannojiya AK, Rajitha B. An extended visual cryptography technique for medical image security. In international conference on innovative mechanisms for industry applications 2020 (pp. 415-21). IEEE.

[26] Rane SS, Phansalkar KA, Shinde MY, Kazi A. Avoiding phishing attack on online votig system using visual cryptography. In international conference on computer communication and informatics 2020 (pp. 1-4). IEEE.

[27] 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.

[28] 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 (pp. 2644-8). IEEE.

[29] 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.

[30] James Z. Wang, Jia Li, Gio Wiederhold, ``SIMPLIcity: Semantics-sensitive integrated matching for picture libraries," IEEE Trans. on Pattern Analysis and Machine Intelligence, 2001; 3(9): 947-63.