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

Vivek Ranjan*, Kailash Patidar and Rishi Kushwaha

M.Tech Scholar, Department of Computer Science Engineering, Sri Satya Sai University of Technology & Medical Sciences, Sehore, Madhya Pradesh, India

Assistant Professor, Department of Computer Science Engineering, Sri Satya Sai University of Technology & Medical Sciences, Sehore, Madhya Pradesh, India

©2020 Vivek Ranjan et al. 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 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, correlated 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.

*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 3x3 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) = \( \frac{\sum_{M,N}|l_1(m,n) - l_2(m,n)|}{M \times N} \)
m and n are the number of rows and columns

PSNR = 10 \log_{10} \left( \frac{R^2}{MSE} \right)
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
[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.
[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.
[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, Dhivy 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.


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


