Research Article

ACCENTS Transactions on Information Security, Vol 4(14)
ISSN (Online): 2455-7196
http://dx.doi.org/10.19101/TIS.2019.414004

An efficient image security mechanism for data handling and key priorities

Kanhaiya Prakash Patil[1*], Kailash Patidar[2], Rishi Kushwah[3] and Manoj Kumar Yadav[3]
M.Tech Scholar, Department of Computer Science, School of Engineering, Sri Satya Sai University of Technology & Medical Sciences, Sehore, Madhya Pradesh, India[1]
Professor and HOD, 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 of Technology & Medical Sciences, Sehore, Madhya Pradesh, India[3]

Abstract
In this paper an efficient and secure approach has been proposed for the image data. It includes the combination of k-means based and RC6 based encryption and decryption mechanism. K-means provides proper data aggregation with the coverage of highest adjacent pixels with the edges in the similar group. K-means has been applied on the array based data on the adjacent pixel values for the aggregation with the edges. It is calculated based on the similarity score based on the distance algorithms. It provides the grouping and correlates the cluster groups with the adjacent pixels. The output value of the k-means approach will then applied to the RC6 for the encryption process. RC6 algorithm has been applied on the cluster group for the efficient encryption with the bitwise shuffling and XOR mechanism repetition. The results indicate in terms of time that our approach provides the cryptography process in better way.

Keywords
Image data encryption and decryption, K-means, RC6, XOR.

1.Introduction
Security in different area is an important aspect in current scenario in the today's internet era. As the todays communication there are different mechanisms is available for sending huge data specially images. So image data security is important in the current scenario. The need of security and robustness in the use is increasing and it is the current demand with the ease from the user side. The main two mechanism used for the image data security are cryptography and steganography. Cryptography approaches provides a way for converting the plain text to cipher text and then the reversible process [1−7].

Deciphering is possible only by applying the desired key [8−10]. This mechanism provides the way to data security so that data can be available for the authorized person in the due time frame and error free means same as it is send from the sender. Information movement incorporates a spread picture, shrouded picture, mystery message, and mystery key and inserted calculations [11−17].

The spread picture is that the unique message is secured by a sound message or a video message covered up by a learning action [18]. In steganography the data is hidden in another data means the data is concealed so that the unauthorized users cannot access the data [18−22]. In general cryptography can be divided in three categories. These are symmetric key encryption, asymmetric key encryption and hash functions [20−22]. Advanced encryption standard (AES), RC4, RC5, RC6 and DES are some of the algorithms fall in the category of symmetric key encryption. Rivest–Shamir–Adleman (RSA), digital signature algorithm (DSA), elliptic curve cryptography (ECC) and public key cryptography standards (PKCS) are some of the algorithms fall in the category of asymmetric key encryption. Message digest (MD5) and secure hash algorithm (SHA) are the examples of hash functions.

The main aim of this paper is to explore the proposed efficient image encryption technique.

*Author for correspondence

2.Literature survey

In 2019, AlKhamese et al. [23] discussed about the cloud computing and their security aspects. They have suggested that the important aspects in terms of the cloud user are data storage, proper retrieval and it should be secure in the entire manner. They have discussed about steganography and cryptography approaches. For this they have emphasis on the literature for the review and study. They also highlighted several aspects in terms of security.

In 2019, Zerouali et al. [24] discussed about the Containerized applications specifically in the docker images. They have suggested that there are several works have been done in the direction of vulnerabilities detection. But there is the need of working in terms of dependencies. They have provided an elaboration on NPM package of Java Script and proved that the outdated dependencies may increase the security risk.

In 2019, Sankaran et al. [25] discussed about the watermarking techniques for the digital images. They have suggested that the medical image watermarking is tough as it is the decision factors for the disease diagnosis. So they have suggested that the main aim is to efficient watermarking for the image data security. So they have concentrated on distortion free watermarking. It is based on the pixel weight. They have used two level DWT.

In 2019, Tamal et al. [26] discussed watermarking technique for the sensitive data hiding. They have proposed integer wavelet transform (IWT) based fragile medical image watermarking for tamper detection. Their segmentation are based on two regions first is region of interest (ROI) and second is region of non-interest (RONI).They have used SHA-512 for the hash value generation of the first region. Compressed bits have been used for RONI. They have experimented on the medical images based on peak signal to noise ratio (PSNR), mean squared error (MSE) and normalized correlation (NC). Their results found to be efficient for the efficient watermarking.

In 2019, Naqash et al. [27] discussed about the image security through cryptography algorithms key. Then they have suggested the concealing program with the algorithms. The proprietor of the image plays out the cryptography key on the first picture and after that utilization the information hider key to additionally encode the picture. The proprietor doesn't perceive the substance in light of the fact that the picture contains more data. With the assistance of a cryptography key, the collector first unravels it at that point utilize the information concealing key to totally disentangle the picture and see the outcome. Spread pictures are utilized which causes the information to additionally decode it. The first picture is encoded by the spread picture that will cover the first picture. It will additionally decode it. Two encryption procedures are utilized in this framework one is cryptography and the other is learning disguising. Cryptography is the system which is utilized to figure the picture. It encodes the picture along these lines that it is difficult to perceive. Cowl pictures are utilized which join with the first picture by make a spread around it. This will at that point encode by the particular key. Information covering is a technique through which the information is implanted in the picture a particular encoded key is utilized that will scramble the learning covering and at that point it will join with the cryptography and make it increasingly secure. Two diverse keys are utilized distinctively in these two techniques that progressively secure the information.

In 2019, Abdelwanees et al. [28] discussed about Consultative committee for space data systems (CCSDS). They have discussed thin in terms of multispectral images. Their main aim of this paper is to reduce the earth observation satellites (EOS) data transmission. They have investigated regarding the possibility of joint encryption compression for these images so that the images can be safe in the transmission phase.

3.Approach

In this paper a robust and efficient image security method have been applied based on k-means and RC6. The k-means is used here for the clustering of alike pixels so that the XOR shuffling can be varied based on the cluster group. RC6 have been applied for the key generation and encryption of the image data. This process is better understood with the flowchart as shown in *Figure 1*. It is efficient as it can handle adjacent nodes very efficiently as it is based on the distance rank and the similarity score generated from the subsequent iterations.

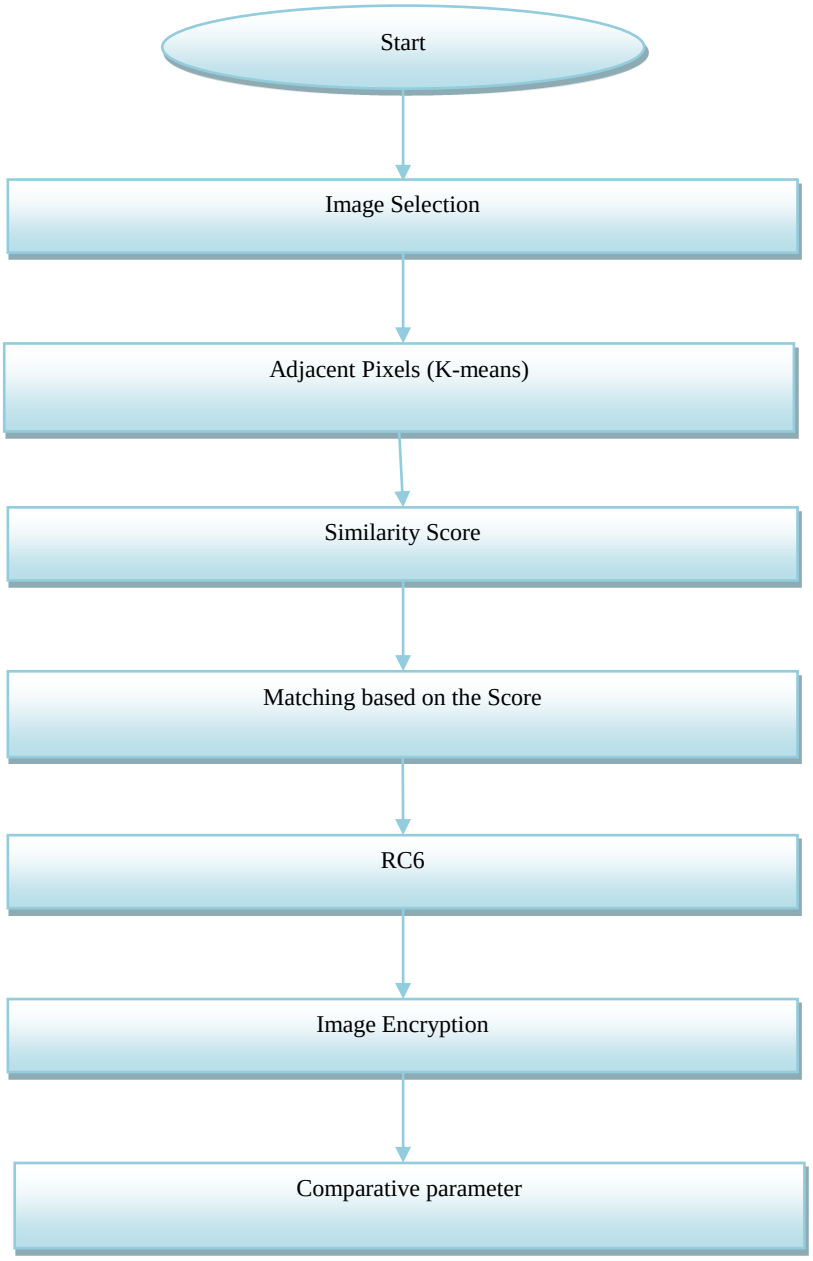

Figure 1 Proposed flowchart

4.Results

The results have been discussed here based on the encryption time spent for the different sizes considered in the experimentation. *Figure 2 to 4* shows the time comparison from reference [29]. It shows the efficiency of our approach in terms of previous method.

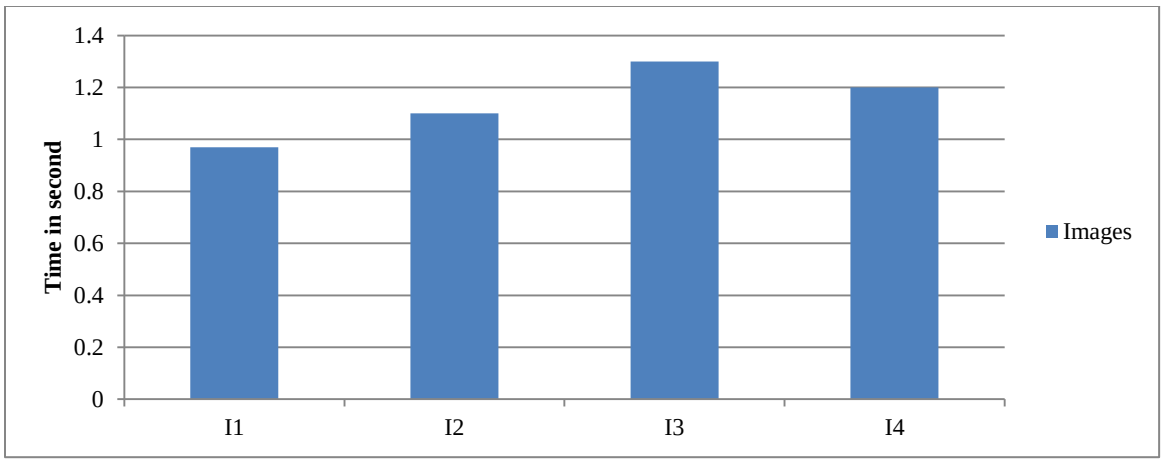

Figure 2 Time for data 100-110 KB

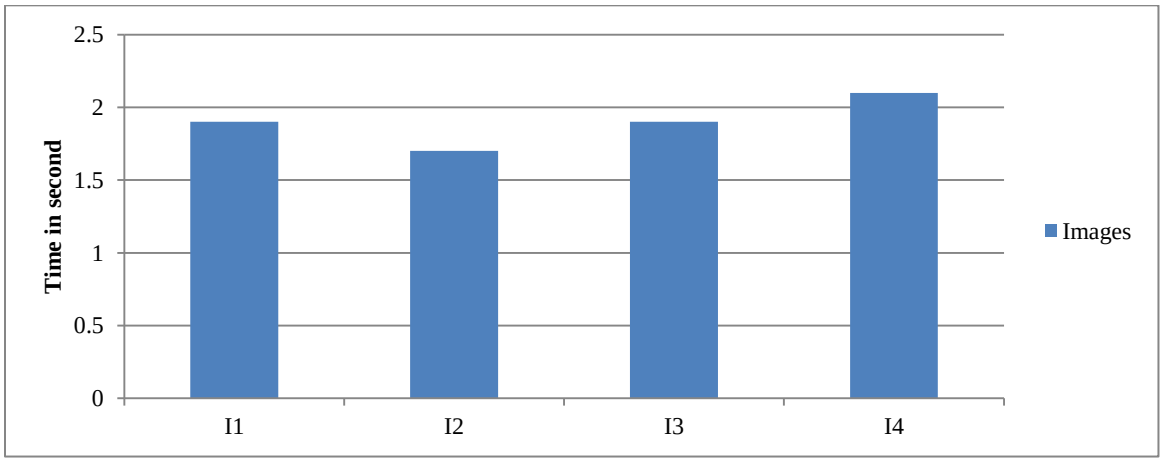

Figure 3 Time for data 300-310 KB

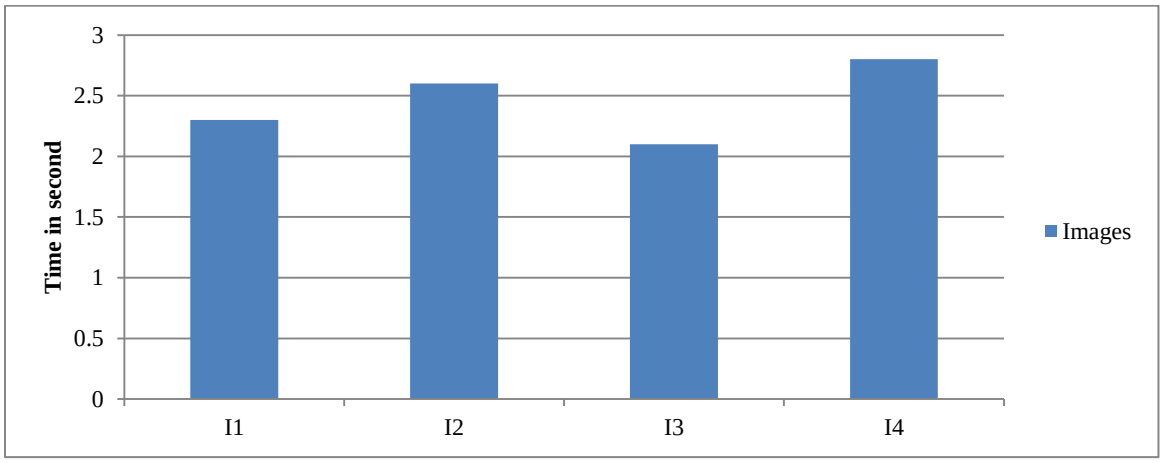

Figure 4 Time for data 500-510 KB

5.Conclusion

In this paper an efficient and robust k-means based method with RC6 security for the image data have been proposed. In this approach k-means has been applied on the initial dataset for the adjacent pixel collaboration with similarity score grouping. It provides the edge based vector and cluster groups so the encryption technique will easily propagate the pixels and it save time. Then RC6 algorithm has been applied on the cluster group for the efficient encryption with the bitwise shuffling and XOR mechanism repetition. After encryption the same reverse process has been applied for the decryption. The results indicate that our approach acquire less time comparison to the related methods.

Acknowledgment

None.

Conflicts of interest

The authors have no conflicts of interest to declare.

References

[1] Lini A, Neenu D. Secure image encryption algorithms: a review. International Journal of Scientific & Technology Research. 2013; 2(4):186-9.

[2] Arumugam M, Singh RK. Data hiding and extraction using a novel reversible method for encrypted image. IJREAT International Journal of Research in Engineering & Advanced Technology. 2013; 1(1):1-5.

[3] Kim HJ, Sachnev V, Shi YQ, Nam J, Choo HG. A novel difference expansion transform for reversible data embedding. IEEE Transactions on Information Forensics and Security. 2008; 3(3):456-65.

[4] Ganesan P, Priyanka BR, Sheikh M, Murthy DHR, Patra GK. A secure key exchange protocol using link weights and dynamic tree parity machine. ACCENTS Transactions on Information Security. 2017; 2(8):78-81.

[5] Naik MR, Sathyanarayana SV. Key management infrastructure in cloud computing environment-a survey. ACCENTS Transactions on Information Security. 2017; 2(7):52-61.

[6] Liu W, Zeng W, Dong L, Yao Q. Efficient compression of encrypted grayscale images. IEEE Transactions on Image Processing. 2010; 19(4):1097-102.

[7] Trivedi S, Chandramouli R. Secret key estimation in sequential steganography. IEEE Transactions on Signal Processing. 2005; 53(2):746-57.

[8] Wu Y. On the security of an SVD-based ownership watermarking. IEEE Transactions on Multimedia. 2005; 7(4):624-7.

[9] Puech W. Image encryption and compression for medical image security. In first workshops on image processing theory, tools and applications 2008 (pp. 1-2). IEEE.

[10] Younes MA, Jantan A. Image encryption using block-based transformation algorithm. IAENG International Journal of Computer Science. 2008; 35(1).

[11] Zandvakili H, Hamid RR, Chabok R. Patient satisfaction and efficacy of accent high-intensity focused ultrasound for face lifting. International Journal of Advanced Computer Research. 2016; 6(26):167-71.

[12] Jahangee A, Naqash T. Efficient implementation of 1024-Bit symmetric encryption protocol for low range devices. In international conference on computing, mathematics and engineering technologies 2018 (pp. 1-7). IEEE.

[13] Chauhan N, Waoo AA, Patheja PS. Attack detection in watermarked images with PSNR and RGB intensity. International Journal of Advanced Computer Research. 2013; 3(9):41-5.

[14] Shrivastava A, Singh L. A new hybrid encryption and steganography technique: a survey. International Journal of Advanced Technology and Engineering Exploration. 2016; 3(14):8-13.

[15] Joshi S, Jain P. A secure data sharing and communication with multiple cloud environments with java API. International Journal of Advanced Computer Research. 2012; 2(2): 135-43.

[16] Sinha A, Singh K. A technique for image encryption using digital signature. Optics Communications. 2003; 218(4-6):229-34.

[17] Li S, Li C, Chen G, Zhang D, Bourbakis NG. A general cryptanalysis of permutation-only multimedia encryption algorithms. IACR's Cryptology ePrint Archive: Report. 2004.

[18] Bhalshankar S, Gulve AK. Audio steganography: LSB technique using a pyramid structure and range of bytes. International Journal of Advanced Computer Research. 2015; 5(20):233-48.

[19] Khanapur NH, Patro A. Design and implementation of enhanced version of MRC6 algorithm for data security. International Journal of Advanced Computer Research. 2015; 5(19):225-32.

[20] Sridevi, Manajaih DH. Modular Arithmetic in RSA Cryptography. International Journal of Advanced Computer Research. 2014; 4(4):973-8.

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

[22] Shukla N. Data mining based result analysis of document fraud detection. International Journal of Advanced Technology and Engineering Exploration. 2014; 1(1):21-5.

[23] AlKhamese AY, Shabana WR, Hanafy IM. Data security in cloud computing using steganography: a review. In international conference on innovative trends in computer engineering 2019 (pp. 549-8). IEEE.

[24] Zerouali A, Cosentino V, Mens T, Robles G, Gonzalez-Barahona JM. On the impact of outdated and vulnerable javascript packages in docker images. In international conference on software analysis,

evolution and reengineering 2019 (pp. 619-23). IEEE.
[25] Sankaran KS, Rayna HA, Mangu V, Prakash VR, Vasudevan N. Image water marking using DWT to encapsulate data in medical image. In international conference on communication and signal processing 2019 (pp. 0568-71). IEEE.
[26] Tarmal TA, Saha C, Hossain MF, Rahman S. Integer wavelet transform based medical image watermarking for tamper detection. In international conference on electrical, computer and communication engineering 2019 (pp. 1-6). IEEE.
[27] Naqash T, Iqbal A, Shah SH. Review on safe reversible image data hiding. In annual computing and communication workshop and conference 2019 (pp. 0929-32). IEEE.
[28] Abdelwanees E, Bayoumy AD, Abdelaziz AM. Secure transmission of space images using joint encryption compression. In international conference on innovative trends in computer engineering 2019 (pp. 538-43). IEEE.
[29] Thein N, Nugroho HA, Adji TB, Mustika IW. Comparative performance study on ordinary and chaos image encryption schemes. In international conference on advanced computing and applications 2017 (pp. 122-6). IEEE.