Research Article

ACCENTS Transactions on Information Security, Vol 3(11)
ISSN (Online): 2455-7196
http://dx.doi.org/10.19101/TIS.2018.311003

An efficient key-scheduling and bit shuffling algorithm for image data encryption

Ravi Shankar Yadav[1]*, Kailash Patidar[2], Rishi Kushwah[3] and Gaurav Kumar Saxena[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 security framework has been proposed which is efficient in image data security as well as the image loss is minimum. In our approach we have used the combination of encryption algorithms. XOR operations are also applied for the bit randomization so that the proper bit shuffling is possible. Then histogram comparison has been provided for the image data for the different phases. Then the information loss is calculated based on the entropy values. Then for comparative analysis peak signal to noise ratio (PSNR) and mean square error (MSE) have been calculated. It provides the comparative and analytical comparison based on the different images. Our results show that it is efficient in terms of information loss, MSE and PSNR values.

Keywords

Encryption, Decryption, PSNR, MSE.

1.Introduction

In the age of communication there is the need of high level data security for the prospective of data communication. In this regard there is the need of image data security also.

Data security is crucial now a day [1−5]. Data cryptography plays an important role in the data security [6-8]. Encryption helps hiding information to make it impenetrable without special knowledge [9]. Transposition and substitution are the two ways for achieving this [10, 11].

So in the subsequent segment we examine data Encryption technique for picture encryption [12]. We additionally talk about the noteworthy edges which are utilized as a bit of picture encryption with their motivations of interest and hindrances [13]. At long last considering the discussions we likewise propose some future comment which may be helpful in this bearing.

There are various basic strategies which are unavoidable cryptography, for instance, private key cryptography, and hash [14−20]. In private key cryptography, a solitary key is staying for both encryption and unraveling. This obliges meander if all else fails part pass on offering an emulate of the key and the key be struck by be passed swear off a protected channel to the accompanying person [21−24]. Private-key estimations are level indestructible and suitably acknowledged in apparatus. In this way they are on and well really for mass estimations encryption. The enormous please of the all-around adjusted encryption rely upon plaintext, encryption estimation, key and unscrambling calculation. The plaintext is the size ahead requiring the encryption check. It is joining of the commitments to the encryption tally. The encryption check is the estimation used to continue on deals with the information stranger plaintext to figure quiet. The mystery key is a for all intents and purposes indistinguishable to rebuff of the encryption figuring and of the plaintext and it is accomplice of the encryption's wellsprings of information tally [25, 26].

*Author for correspondence

In this paper an efficient image encryption and decryption mechanism has been presented.

2.Literature survey

Bhowmick et al. [27] suggested that the AES and DES algorithms are computationally intensive. They have used RC4 algorithm to pseudo-random numbers generation. For the image column swapping middle square algorithm is used. These numbers are utilized to substitute the force of pixels of the go-between figure picture, which gives the last encoded picture. Different investigation tests are performed on the nature of the encoded picture. The consequences of these tests demonstrate that the proposed calculation is secure and proficient.

Chuman and Kiya [28] suggested encryption-then-compression (EtC) systems for the privacy protection. Their main motivation is to evaluate the security of block scrambling based encryption schemes. Despite the fact that this plan has enough key spaces for ensuring savage power assaults, each square in encoded pictures has nearly indistinguishable connection from that of unique pictures. In this way, it is required to think about the security from various perspectives from number hypothesis based encryption techniques with provable security, for example, RSA and DES.

Awudong and Li [29] suggested that the single chaotic encryption method is not sufficient for the current data security. Another picture encryption conspire is composed by consolidating calculated mapping, sine mapping and DNA encoding. Test results demonstrate that this technique has Fast encryption speed, expansive key space, solid against assault capacity, great strength, reversible encryption strategies and it additionally delicate to beginning worth.

Cataltaş and Tütüncü [30] suggested that the mind blowing advancement of innovation has made the utilization of correspondence and data advancements imperative as a result of the conceivable outcomes it offers. These potential outcomes expanded the security issues on close to home data what's more, correspondence security issues, for example, telephone calls, recovering email substance, replicating private data on PCs. Encryption calculations utilized in traditional security approaches, while guaranteeing the classification of data, can't give the rule of "imprecision" that has moved toward becoming progressively vital as of late. A coded or encoded content can be explained by cutting edge machines when concentrated on it. Consequently, steganography and watermarking techniques that put the intangibility of the presence of a mystery message into the essential objective are particularly the focal point of enthusiasm after 2000's years. In this contemplate, least significant Bit (LSB) technique.

Aryal et al. [31] proposed a block-permutation-based encryption (BPBE) method with reversible data hiding (RDH). Histogram shifting (HS) have been used for RDH. The BPBE method was used for the encryption. The BPBE strategy performs four procedures for encryption, to be specific, square scrambling, square rotation inversion, negative positive change, and the shading segment rearranging. The proposed calculation is executed on the connected picture from a substantial database. In this way, the quantity of the isolated squares can be expanded, and the shading scrambling of the encoded picture is expanded.

Singar et al. [32] suggested that the Data containing sound, video and pictures trades over the web is open and not anchor. Security is required for putting away and transmission of computerized pictures to keep away from unapproved substances. This paper shows the novel approach utilizing cell rearranging and examining systems for picture encryption. The proposed technique contain two phase, first partition the picture in to number of squares and after that rearranged the first picture and in second stage the winding wave examine design are connected to get encoded picture. Various parameters, as connection coefficient, data entropy, PSNR, MSE, number of pixels change rate, normal force and brought together normal change power and so on , are utilized to check the nature of figure picture.

Dragoi and Coltuc [33] proposed a new vacating room after encryption reversible data hiding scheme. The proposed plot utilizes standard selective or encryption and acquires the fundamental highlights of emptying room after encryption plans, specifically joint and separate strategies for information inserting. The proposed plot misuses both the connection between neighboring pixels and the relationship between shading channels by foreseeing the first pixel esteems on shading channel contrasts. The trial results demonstrate that the proposed plan can take out the principle downside of the clearing room after encryption system, in particular the vast inserting mutilations.

3.Approach

The implementation environment has been developed and designs in Netbeans 7.2 environment and by using Java programming language. It consists of image encryption and decryption, histogram, information loss calculations through the entropy, MSE and PSNR values for comparison. In this dissertation standard encryption algorithm with substitution and the key generation mechanism has been applied through blowfish. By this approach we have the benefit of the hybridization so that security of the approach has been enhanced and the partial hybridization provides the speedup in the computation time. This overlapping procedure is developed in Java to overlap the key generated by blowfish and randomize the key in every iteration. Then we have applied XOR for the bit shuffling procedure in the image to improving the security. In this procedure different random images are used so that the bit shuffling is different in different iteration and the image security will enhance.

Five different key images are used randomly for the XOR operation. XOR is a binary operation, it remains for "select or", that is to say the subsequent piece assesses to one if just precisely one of the bits is set. This operation is performed between each two relating bits of a number for data shuffling.

The reversible process is applied for retrieving the data after encryption for decoding component with the different keys for a single file in many trials. The keys are applied for data decryption. It is secured by the encryption secret key. Histogram and information loss calculation are calculated also.

4.Results

In this section we have compared the results from the previous approach presented. Information loss comparison is shown below in terms of entropy comparison. Here Food, Barbara, Cameraman, Sea and Bus images have been considered for the comparison. *Figure 1 to 5* shows the entropies obtained from different figures. *Figure 6* shows the comparison which shows the effectiveness of our approach.

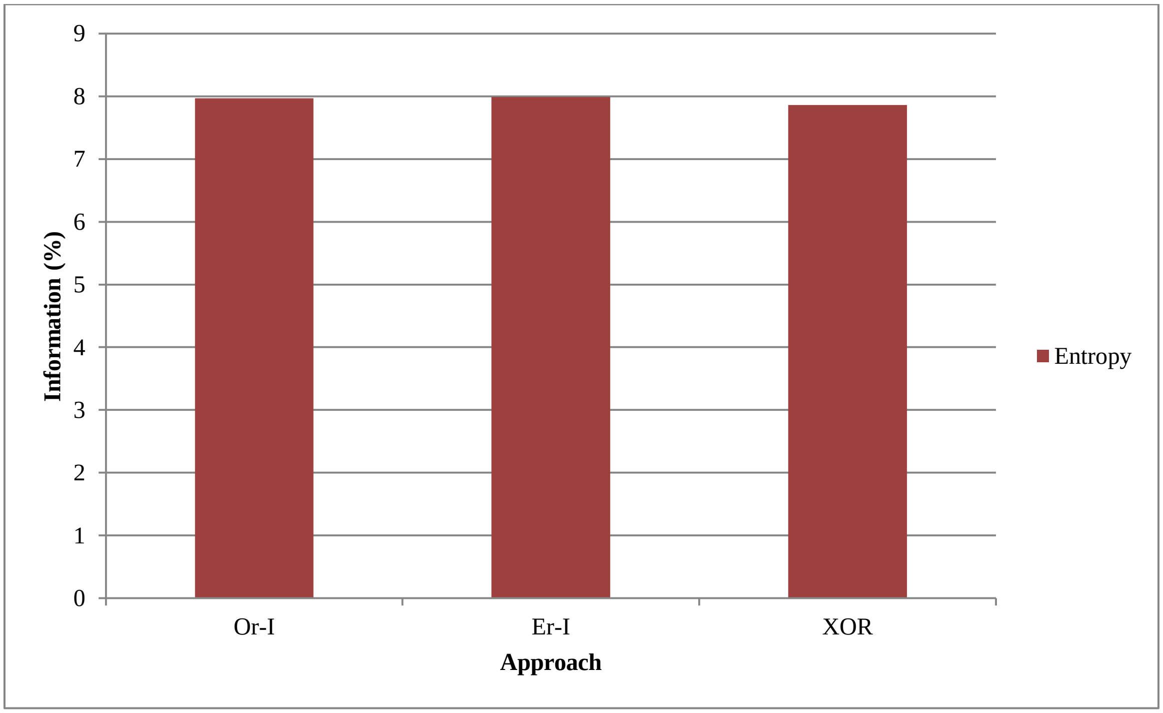

Figure 1 Entropy comparison for Food image

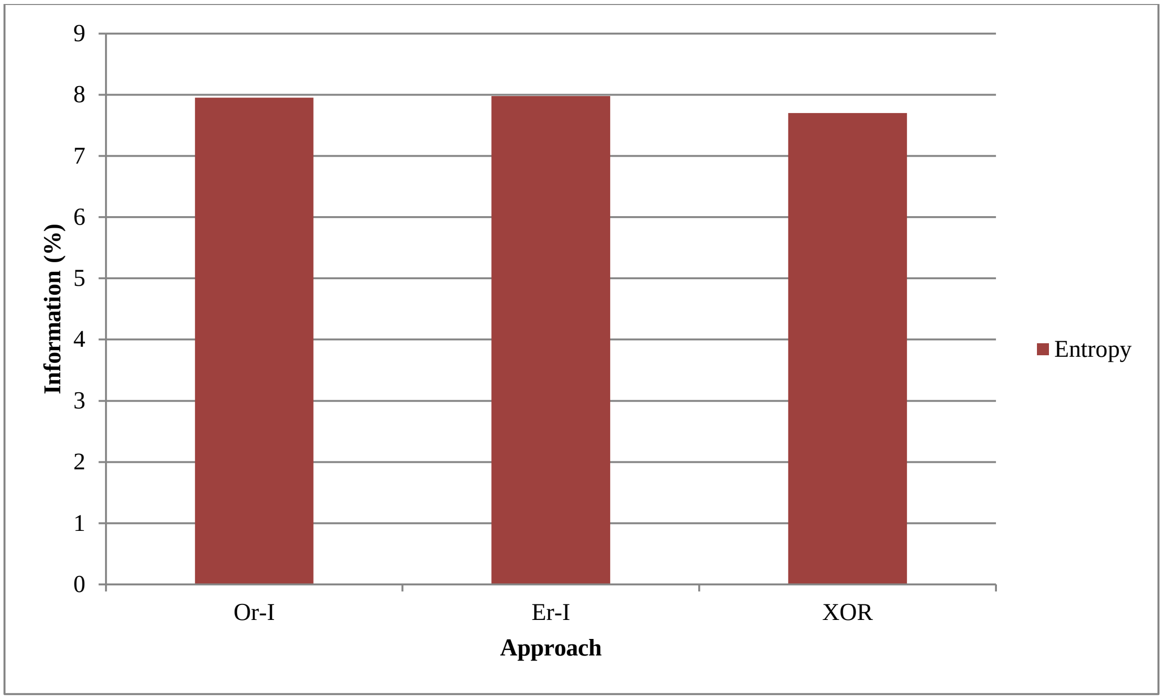

Figure 2 Entropy comparison for Barbara image

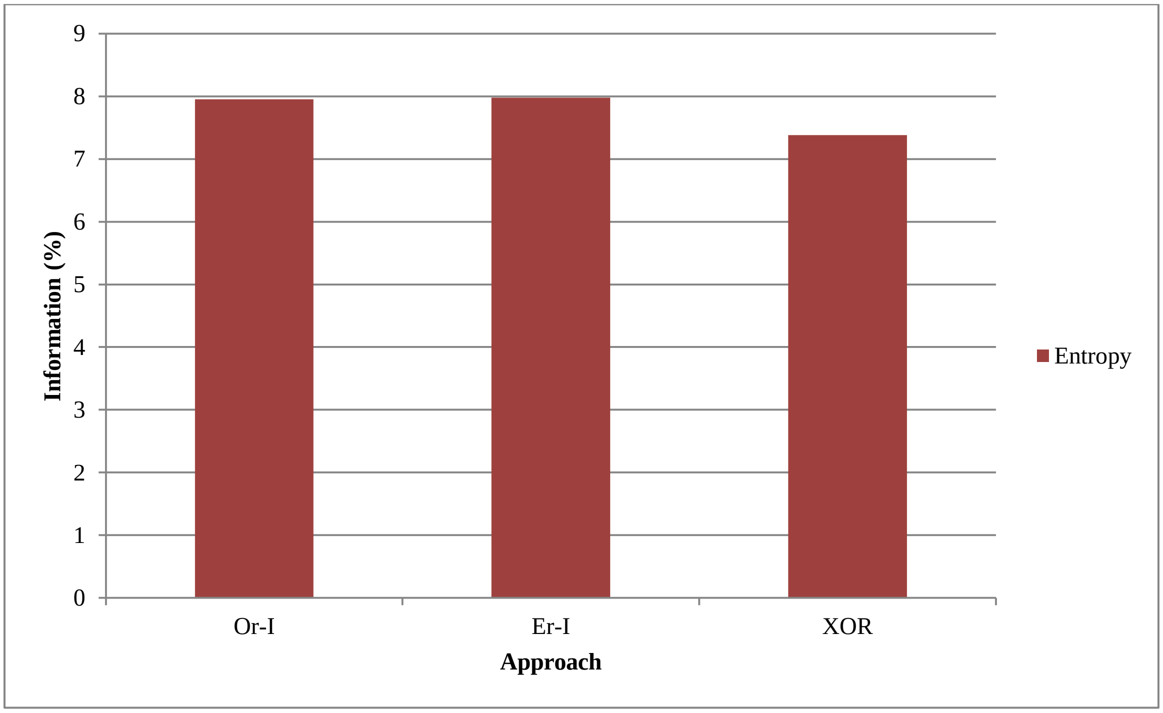

Figure 3 Entropy comparison for Cameraman image

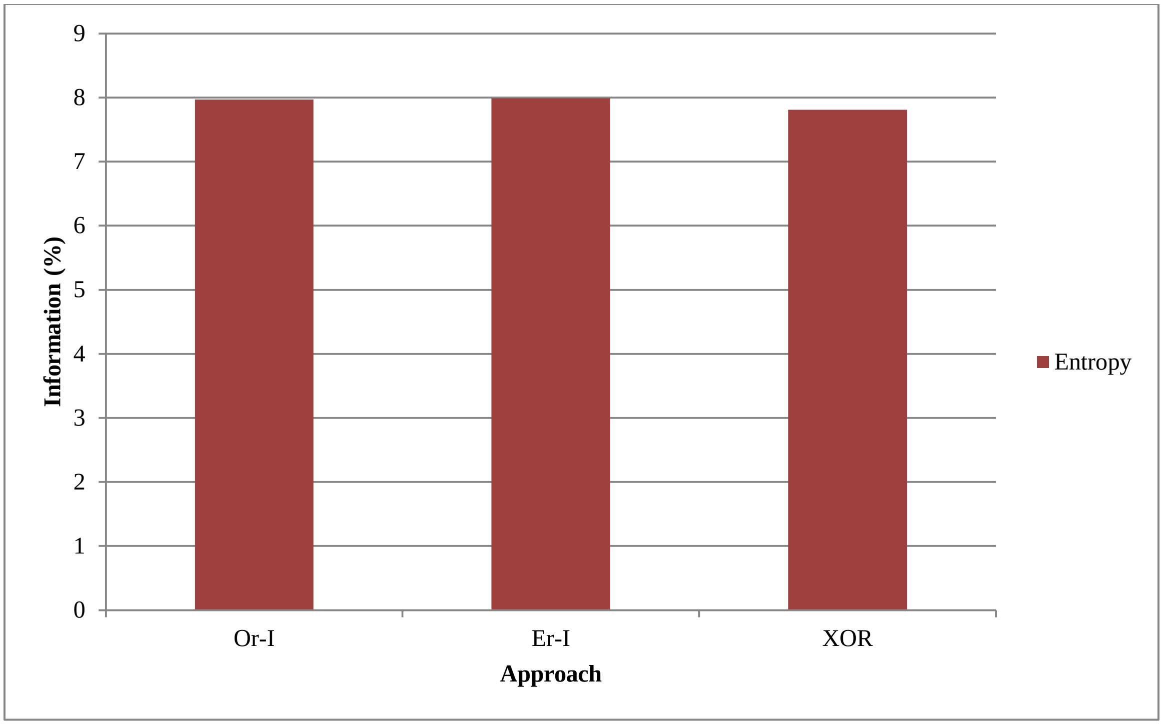

Figure 4 Entropy comparison for Sea image

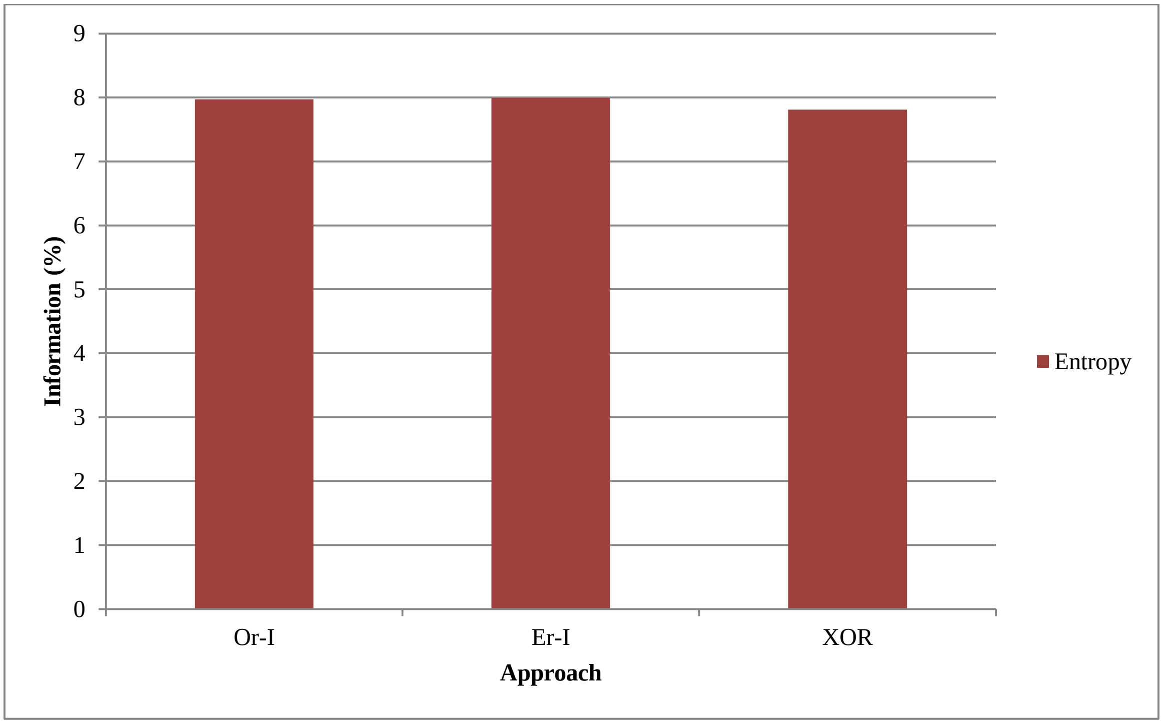

Figure 5 Entropy comparison for Bus image

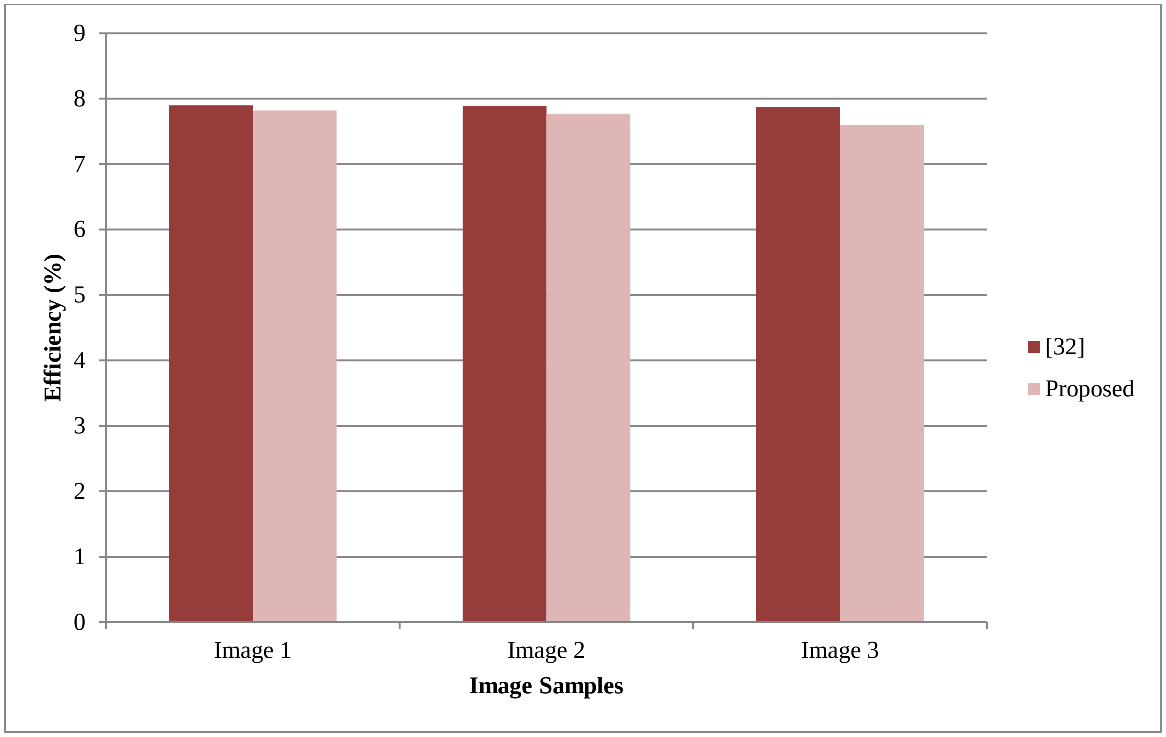

Figure 6 Entropy Comparison from [32]

5.Conclusion

In this paper an efficient key-scheduling and bit shuffling algorithm for image data encryption have been presented. Our approach provides the analytical view of the analysis and experimental way of this design. This approach is efficient in terms of encryption the data in proper way to analyze the concept to handle it in the way to elaborate the security requirements. The results shows the effectiveness of the approach.

Acknowledgment

None.

Conflicts of interest

The authors have no conflicts of interest to declare.

References

[1] Seng LK, Ithnin N, Said SZM. The approaches to quantify web application security scanners quality: a review. International Journal of Advanced Computer Research. 2018; 8 (38): 285-312.

[2] Mitra A, Rao YS, Prasanna SR. A new image encryption approach using combinational permutation techniques. International Journal of Computer Science. 2006; 1(2):127-31.

[3] Elbirt AJ, Paar C. An instruction-level distributed processor for symmetric-key cryptography. IEEE Transactions on Parallel and distributed Systems. 2005; 16(5):468-80.

[4] Ganesan P, Priyanka BR, Sheikh M, Murthy DHR, Patra GK. A secure key exchange protocol using link weights and dynamic tree parity machine (TPM). 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] Sangwan N. Text encryption with huffman compression. International Journal of Computer Applications. 2012; 54(6).

[7] Bokhari MU, Alam S, Masoodi FS. Cryptanalysis techniques for stream cipher: a survey. International Journal of Computer Applications. 2012; 60(9):29-33.

[8] Masram R, Shahare V, Abraham J, Moona R. Analysis and comparison of symmetric key cryptographic algorithms based on various file features. International Journal of Network Security & Its Applications. 2014; 6(4):43-52.

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

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

[11] Wu YT, Shih FY. An adjusted-purpose digital watermarking technique. Pattern Recognition. 2004; 37(12):2349-59.

[12] Younes MA, Jantan A. Image encryption using block-based transformation algorithm. IAENG International

Journal of Computer Science. 2008; 35(1).

[13] Nanavati SP, Panigrahi PK. Wavelets: applications to image compression-I. Resonance. 2005; 10(2):52-61.

[14] 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.

[15] Vitali AL, Borneo A, Fumagalli M, Rinaldo R. Video over IP using standard-compatible multiple description coding: an IETF proposal. Journal of Zhejiang University-Science A. 2006; 7(5):668-76.

[16] 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.

[17] Shrivastava A, Singh L. A new hybrid encryption and steganography technique: a survey. International Journal of Advanced Technology and Engineering Exploration. 2016; 3(14):9-14.

[18] 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.

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

[20] 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.

[21] 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):225-132.

[22] Sridevi, Manajaih DH. Modular arithmetic in RSA cryptography. International Journal of Advanced Computer Research. 2014; 4(17):973-8.

[23] 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 software engineering (CONSEG), 2012 CSI Sixth International Conference on 2012 (pp. 1-8). IEEE.

[24] Tavse P, Khandelwal A. A critical review on data clustering in wireless network. International Journal of Advanced Computer Research. 2014; 4(16):795-8.

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

[26] De PS, Maiti P. DEDD Symmetric-Key Cryptosystem. International Journal of Advanced Computer Research (IJACR). 2013; 3(8):171-6.

[27] Bhowmick A, Sinha N, Arjunan RV, Kishore B. Permutation-Substitution architecture based image encryption algorithm using middle square and RC4 PRNG. In international conference on inventive systems and control 2017 (pp. 1-6). IEEE.

[28] Chuman T, Kiya H. On the security of block scrambling-based image encryption including JPEG distorsion against jigsaw puzzle solver attacks. In international workshop on signal design and its applications in communications 2017 (pp. 64-8). IEEE.

[29] Awudong B, Li G. Research on image encryption technology based on multi chaotic mapping. In 2017 international conference on smart city and systems engineering (ICSCSE) 2017 (pp. 127-31). IEEE.

[30] Çataltaş Ö, Tütüncü K. Comparison of LSB image steganography technique in different color spaces. In international artificial intelligence and data processing symposium 2017 (pp. 1-6). IEEE.

[31] Aryal A, Imaizumi S, Horiuchi T, Kiya H. Integrated algorithm for block-permutation-based encryption with reversible data hiding. In Asia-Pacific signal and information processing association annual summit and conference 2017 (pp. 203-8). IEEE.

[32] Singar CP, Bharti J, Pateriya RK. Image encryption based on cell shuffling and scanning techniques. In recent innovations in signal processing and embedded systems (RISE), international conference on 2017 (pp. 257-63). IEEE.

[33] Dragoi IC, Coltuc D. Reversible data hiding in encrypted color images based on vacating room after encryption and pixel prediction. In international conference on image processing 2018 (pp. 1673-7). IEEE.