Research Article

ACCENTS Transactions on Information Security, Vol 3(9)
ISSN (Online): 2455-7196
http://dx.doi.org/10.19101/TIS.2018.39002

An efficient image encryption algorithm based on RK-RC6

Rupa Rajoriya[1*], Kailash Patidar[2] and Sudeesh Chouhan[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 image cryptography method by using random key (RK)-RC6 algorithm has been proposed. 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, and information loss calculations through the entropy. The comparative images have been considered like Leena, Barbara, Cameraman, Elina etc. have been considered for the experimentation. In the RK-RC6 algorithm, the procedure of RC6 algorithm is applied along with the random key variation overlapping procedure. This overlapping procedure is developed in Java to overlap the key generated by RC6 and randomize the key in every iteration. Then we have applied XOR for the bit shuffling procedure in the image to improve the security. In this procedure different random images are used so that the bit shuffling is different in different iteration and the image security can enhance. Result shows the improved security and less information loss in case of image encryption.

Keywords
RK-RC6, RC6, Information loss, Correlation coefficients.

1.Introduction
Image data security is an important aspect in the today world. It is important for the organization as well as for the user in the communication media in the different ways of using it.

Especially at the level of content and picture data demonstrated by [1] there are three key schedules for anchored correspondence open, specifically, cryptography, steganography and watermarking.

In [9] creators have suggested that by far most of the basic pictures, the neighboring's estimations pixels are unequivocally related i.e. the estimation of any given pixel can be sensibly foreseen from the estimations of its neighbors [10−12].

So remembering the ultimate objective to achieve the higher relationship entropy among pixels and extending the entropy quality.

Among these three, the first one, cryptography [2−4], deals with the change of methodology for changing over information amidst justifiable and unfathomable structures in the midst of information exchange. Steganography [5, 6], of course, is a system for disguising and isolating information to be passed on using a transporter flag [1]. The third one, watermarking [7, 8], is a technique for making genuine systems for disguising prohibitive information in the perceptual data.

In the event of content the information ought to stow away with pictures so greater security will force with RGB blends and varieties.

In [13] the most basic issues, which impact the standard information of cutting edge media, are the best approach to anchor burglary and ownership. The watermarking of the common strategies think about ding as another database for giving the copyright protection is a technique in perspective of embedding a specific engraving or stamp into the modernized things. While a couple of watermarking estimations have been proposed [14] in this heading.

*Author for correspondence

So in the resulting portion we discuss information Encryption strategy for picture encryption. We also discuss the significant edges which are used as a piece of picture encryption with their purposes of intrigue and disadvantages. Finally considering the talks we also suggest some future remark which might be beneficial in this bearing.

There are various basic strategies which are second-hand unavoidable cryptography, for instance, private or puzzle key cryptography, open major or kilter, automated stamp, and hash limits [15]. In private key cryptography, a single key is remaining for both encryption and disentangling. This obliges wander when in doubt part pass on offering a pantomime of the key and the key be struck by be passed swear off a sheltered channel to the following individual [13−22].Private-key estimations are level indestructible and viably realized in gear. Thusly they are on and well actually for mass estimations encryption. The tremendous please of the inside and out balanced encryption depend on upon plaintext, encryption estimation, key and unscrambling computation. The plaintext is the size ahead requiring the encryption count. It is joining of the contributions to the encryption count. The encryption count is the estimation used to proceed on manages the data stranger plaintext to figure calm. The secret key is a practically identical to repulse of the encryption figuring and of the plaintext and it is partner of the encryption's sources of info count [23, 24]. The figure content is the insubordinate substance find as yield [14, 15].The steganography method with cryptography will upgrade the security as the enigmatic substance and the randomization quality can be progressed.

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

2.Literature survey

In 2014, Mostaghim et al. [25] suggested the visual cryptography which is helpful in received data with the created message and will consolidate to the got offer to uncover the shrouded message. Their proposed plot is assessed as far as histogram, connection coefficient, key affectability and key space. Their outcomes are observed to be enhanced in contrast with the customary strategy.

In 2015, Hassan et al. [26] proposed a secure communication scheme. It is a hyperchaotic system utilized as a bearer for the encoded information to be transmitted. At the transmitter end, two various disarranged structures are coupled and used to fabricate another hyperchaotie system. One of the yields of the hyperehaotie system is used as a conveyor for the mixed data. At the not as much as attractive end, the discrete-time regularized least square (RLS) estimator is used to redo the jumbled banner and thus recoup the encoded data. Their propagation comes about are speaking to the reasonability of the proposed strategy.

In 2015, Li et al. [27] coordinated the idea of session key foundation and expanded tumultuous maps for the satisfaction to permit information senders and information beneficiaries to build up a safe normal session key through a confided in server over an unreliable channel. They have proposed a secure three-party authenticated key exchange protocol (3PAKE) which depends on expanded disorganized maps away administration without utilizing shrewd card and timestamp. It requires neither long haul mystery keys nor symmetric cryptosystems. It satisfies the insurance prerequisite against different assaults. Their proposed convention is more secure and pragmatic for genuine situations.

In 2015, Haroun et al. [28] presented a key generation method which depends on the remote blurring channels. It is utilized in light of the broadband disordered flag for information transmission with the goal that it is recurrence particular. Their proposed count abuses this property to create an exceptional shared key between two social affairs. The no periodicity of the turbulent sign gives a remarkable sign to key time, which can be used even with static obscuring channels. Their proposed system is great to timing contrasts between the social occasions in light of the way that the repeat scope of the signs is used. The key's abnormality is certified, and the effects of included substance white Gaussian noise and timing contrasts on the estimation's execution are reviewed.

In 2017, Singar et al. [29] suggested that the security is essential for storing and transmission of digital images. It is helpful in avoiding unauthorized entities. They have presented a novel approach using cell shuffling and scanning techniques for image encryption. The proposed strategy contain two phase, first separation 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 bound together normal change force and so forth , are utilized to check the nature of picture.

In 2018, Zou [30] suggested the image encryption is helpful in protecting the copyrights of the ownership of the images from the internet. They suggested that it is also helpful in increasing the security. A novel picture encryption strategy in view of secluded lattice change and arrange testing is introduced. The calculation has leeway that pictures can be scrambled by their dark data and their organize data in a similar time. As an application, the calculation is utilized to picture data stowing away in view of LSB. Investigations demonstrate that the strategy achieves a decent picture encryption impact, and furthermore can bear some image attacks.

In 2017, Brindha [31] suggested that the image encryption is important for the digital world. To make the calculation effective and more secure, various phases of encryption is better for improving the security. They have calculated, disorganized guide based different arrange picture encryption utilizing different capacities is talked about. The effect of disorganized guide parameters to different capacities is too exhibited. Because of the riotous guide, there is a solid affectability to the keys utilized as a part of the calculation. Histogram and key affectability investigation are performed to demonstrate the effectiveness of the proposed calculation.

In 2017, Liu et al. [32] proposed an improved encryption algorithm for image based on double random phase encoding (DRPE). Their algorithm uses discrete cosine transform (DCT) instead of discrete Fourier transform (DFT). They have used a logistic map for the random matrices generation in the place of random phase masks. It is helpful in decreasing the number of secret keys. They have tested the algorithm on five different types of attacks. Their results shows that their approach outperforms as compared to the traditional scrambling methods.

In 2017, Ray et al. [33] discusses about the data security in case of data transmission over image. They have applied different encryption algorithms on images. They have used image as data and utilize distinctive kinds of encryption strategies to scramble it and shield it from programmers.

After that we find different parameters from each picture encryption strategy and after that think about every strategy's parameters from each other.

In 2017, Fu et al. [34] presented a color image encryption algorithm. It is based on new 1-D chaotic map, tent-logistic map. It is produced by cascade chaotic system (CCS). Contrasted and comparing seed maps, the utilized confused guide has more parameters and complex turbulent properties while remaining straightforwardness, making it a decent possibility for building picture figures with an adequately vast key space and high computational productivity. In the change organize; the places of shaded sub pixels in the input picture are mixed utilizing a pixel-swapping instrument, which successfully maintains a strategic distance from the periodicity issue experienced by discretized rendition of territory safeguarding turbulent maps. The aftereffects of NPCR and UACI tests demonstrate that the proposed calculation takes just two figure rounds to accomplish an acceptable dissemination impact. Their result shows the strength of the proposed approach.

3.Methods

In this paper an efficient image cryptography method by using random key (RK)-RC6 algorithm has been proposed. 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, and information loss calculations through the entropy.

The famous comparative images have been considered like Leena, Barbara, Cameraman, Elina etc. James et al.[35] famous database has also been considered for the experimentation. This database is the collection of 1000 images. In the RK-RC6 algorithm, the procedure of RC6 algorithm is applied along with the random key variation overlapping procedure. This overlapping procedure is developed in Java to overlap the key generated by RC6 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. *Figure 1* shows the working procedure.

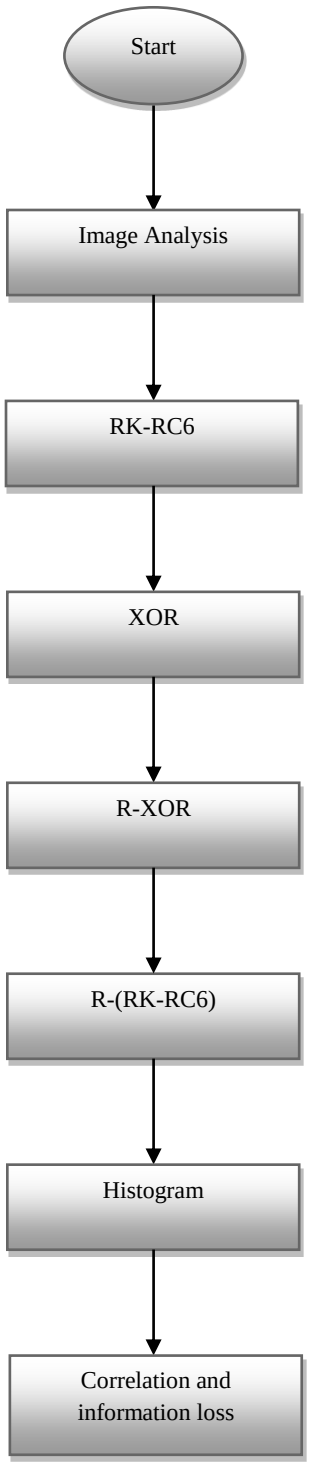

Figure 1 Flowchart

Algorithm RC6 [36]:
Input: Raw array data from the image as the input.
Output: Decrypted image.

Step 1: Input the array data.
Step 2: data is pre-processed for the initial level weight assignment.
Step 3: Iterations have been performed based on the r rounds
x = Initial value
y = Next value
w-bit round keys S[0,… , 2r + 3]
S[0] = x
do:
for i = 1 to (2r + 3) do
S[i] = S[i - 1] + y
Step 4: Block key generation has been performed based on the end of file.
Step 5: Then block based shifting has been applied for the data bit shifting
A = S[i] = (S[i] + A + B) <<< 3
Stage 8: Then again moving is performed with the 3 bit to make the substitution framework.
Stage 9: The entire procedure is connected to the block based accomplished.
Stage 10: The last key is produced by the r rounds.
Stage 11: End;

4.Result analysis

Here Leena, Barbara, Cameraman and Elaine images have been considered for the comparison. OI indicates original image and EI indicates encrypted image. *Figure 2* shows the entropy comparison for Leena image. *Figure 3* shows the entropy comparison for Barbara image. *Figure 4* shows the entropy comparison for Cameraman image. *Figure 5* shows the entropy comparison for Elaine image. The result shows the variations in the information loss are minor.

5.Conclusion

In this paper an efficient and secure image security framework has been developed. In this paper RK-RC6 algorithm has been proposed with the XOR bit shuffling. RK-RC6 has the efficiency of random key in each iteration along with the key size variability. It has the capability of improving the security. Image mapping and increasing the confusion we have also provided bit shuffling by the use of random images in case of XOR. The comparative study shows that the approach outperforms in comparison to the traditional mechanism. The comparison parameters are RGB, in which it shows significant difference in the original, encrypted and XOR image. Then information loss and correlation coefficients have been compared. Fewer variations have been obtained in case of information loss and correlation coefficients.

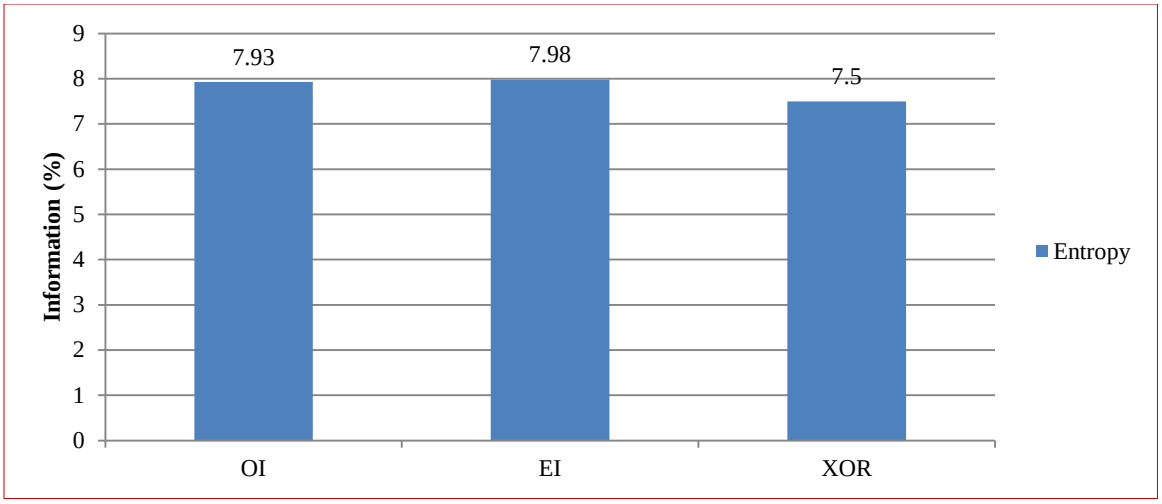

Figure 2 Entropy comparison for Leena image

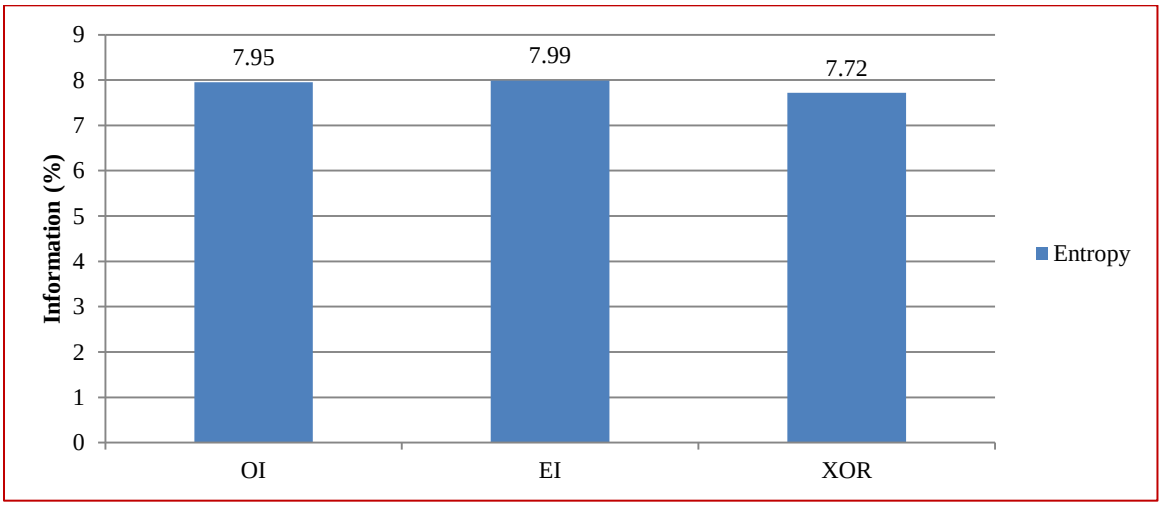

Figure 3 Entropy comparison for Barbara image

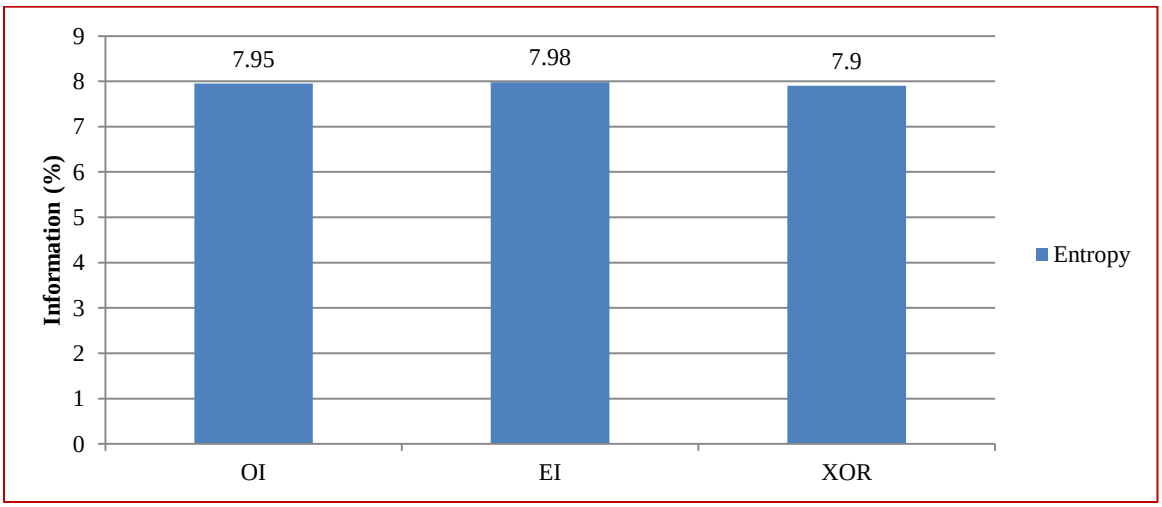

Figure 4 Entropy comparison for Cameraman image

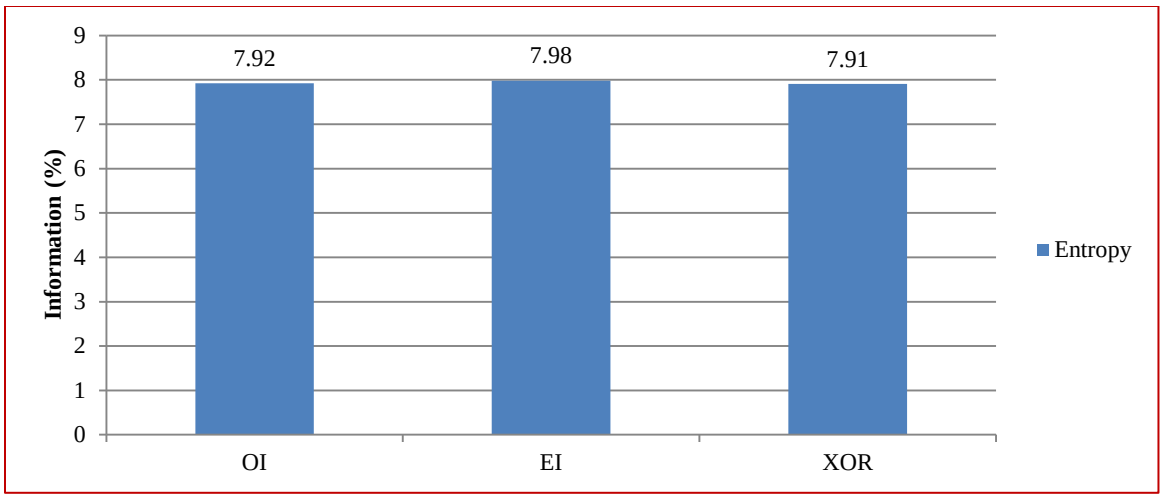

Figure 5 Entropy comparison for Elaine image

Acknowledgment
None.

Conflicts of interest
The authors have no conflicts of interest to declare.

References
[1] 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.
[2] 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.
[3] 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.
[4] Naik MR, Sathyanarayana SV. Key management infrastructure in cloud computing environment-a survey. ACCENTS Transactions on Information Security. 2017; 2(7):52-61.
[5] Beşdok E. Hiding information in multispectral spatial images. AEU-International Journal of Electronics and Communications. 2005; 59(1):15-24.
[6] Trivedi S, Chandramouli R. Secret key estimation in sequential steganography. IEEE Transactions on Signal Processing. 2005; 53(2):746-57.
[7] Wu Y. On the security of an SVD-based ownership watermarking. IEEE Transactions on Multimedia. 2005; 7(4):624-7.
[8] Wu YT, Shih FY. An adjusted-purpose digital watermarking technique. Pattern Recognition. 2004; 37(12):2349-59.
[9] Younes MA, Jantan A. Image encryption using block-based transformation algorithm. IAENG International Journal of Computer Science. 2008; 35(1).
[10] Nanavati SP, Panigrahi PK. Wavelets: applications to image compression-I. Resonance. 2005; 10(2):52-61.
[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] 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.
[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):9-14.
[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(17):973-78.

[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 sixth international conference on software engineering 2012 (pp. 1-8). IEEE.
[22] Tavse P, Khandelwal A. A critical review on data clustering in wireless network. International Journal of Advanced Computer Research. 2014; 4(16):795-8.
[23] Shukla N. Data mining based result analysis of document fraud detection. International Journal of Advanced Technology and Engineering Exploration. 2014; 1(1):21-5.
[24] De PS, Maiti P. DEDD symmetric-key cryptosystem. International Journal of Advanced Computer Research. 2013; 3(8):171-6.
[25] Mostaghim M, Boostani R. CVC: chaotic visual cryptography to enhance steganography. In international conference on information security and cryptology 2014 (pp. 44-8). IEEE.
[26] Hassan MF. Synchronization of hyperchaotic systems with application to secure communication. In international systems conference 2015 (pp. 121-6). IEEE.
[27] Li CT, Lee CW, Shen JJ. A secure three-party authenticated key exchange protocol based on extended chaotic maps in cloud storage service. In international conference on information networking 2015 (pp. 31-6). IEEE.
[28] Haroun MF, Gulliver TA. Secret key generation using chaotic signals over frequency selective fading channels. IEEE Transaction Information Forensics and Security. 2015; 10(8):1764-75.
[29] Singar CP, Bharti J, Pateriya RK. Image encryption based on cell shuffling and scanning techniques. In international conference on recent innovations in signal processing and embedded systems 2017(pp. 257-63). IEEE.
[30] Zou Z. A novel image encryption method based on modular matrix transformation and coordinate sampling. In international conference on applied system invention 2018 (pp. 1121-4). IEEE.
[31] Brindha M. Multiple stage image encryption using chaotic logistic map. In international conference on intelligent sustainable systems 2017 (pp. 1239-43). IEEE.
[32] Liu Z, Yang ML, Yan WQ. Image encryption based on double random phase encoding. In international conference on image and vision computing 2017. IEEE.
[33] Ray A, Potnis A, Dwivedy P, Soofi S, Bhade U. Comparative study of AES, RSA, genetic, affine transform with XOR operation, and watermarking for image encryption. In international conference on recent innovations in signal processing and embedded systems (2017 (pp. 274-8). IEEE.
[34] Fu C, Zheng Y, Chen M, Wen ZK. A color image encryption algorithm using a new 1-D chaotic map. In international conference on communication technology 2017 (pp. 1768-73). IEEE.
[35] James Z. Wang, Jia Li, Gio Wiederhold. SIMPLIcity: semantics-sensitive integrated matching for picture libraries. IEEE Transactions on Pattern Analysis and Machine Intelligence 2001; 23(9): 947-63.
[36] Rivest RL, Robshaw MJ, Sidney R, Yin YL. The RC6TM block cipher. In first advanced encryption standard (AES) conference 1998.