ISSN (Print) : 2320 – 3765
ISSN (Online): 2278 – 8875

International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 5, Issue 7, July 2016

Image Encryption Technique: A Review

Hirdesh Varshney[1], Himanshu Gupta[2], Himanshu Chaurasia[3], P. C. Yadav[4]

M.Tech Scholar, Dept. of CSE, Bansal Institute of Engineering & Technology, Lucknow, Uttar Pradesh, India[1]

Asst. Professor, Dept. of ECE, GCRG Group of Institutions, Faculty of Engineering, Lucknow, Uttar Pradesh, India [2,4]

Asst. Professor, Dept. of CSE, GCRG Group of Institutions, Faculty of Engineering, Lucknow, Uttar Pradesh, India [3]

ABSTRACT: With the advancement and spreading of internet, online information sharing becomes prominent. This information can be of text, images, audio or video. However, the security of information in open network is very crucial hence encryption is required. This paper briefly reviews some image encryption techniques and then various chaos image encryption techniques are discussed.

KEYWORDS: Cryptography, Image encryption, Chaos logistic map.

I.INTRODUCTION

In today's world, since all networks are interconnected to global net, the security of data being transmitted and stored becomes crucial. To secure them from unauthorized access, an encryption is required but the present encryption schemes which are mostly used for text are not suitable for multimedia data due to-

- High redundancy
- Bulk data capacity
- Its perception
- Strong correlation among adjacent pixels

Image encryption [1] is a term used for masking of some information of adjacent pixels of image to protect it from unauthorized access. To better understand the encryption, a brief concept of cryptography is explained. It is of two types-

1. Private key
2. Public key

In private key cryptography, the sender and receiver concur on a common secret key before they communicate. However, a secure channel for key agreement between them is critical. Fig.[1] shows the basic diagram of private key cryptography.

The cipher text 'C' is meaningless without the use of secret key 'K'. But as the receiver uses same secret key 'K', the jumbled information is converted into original plain text 'P'.

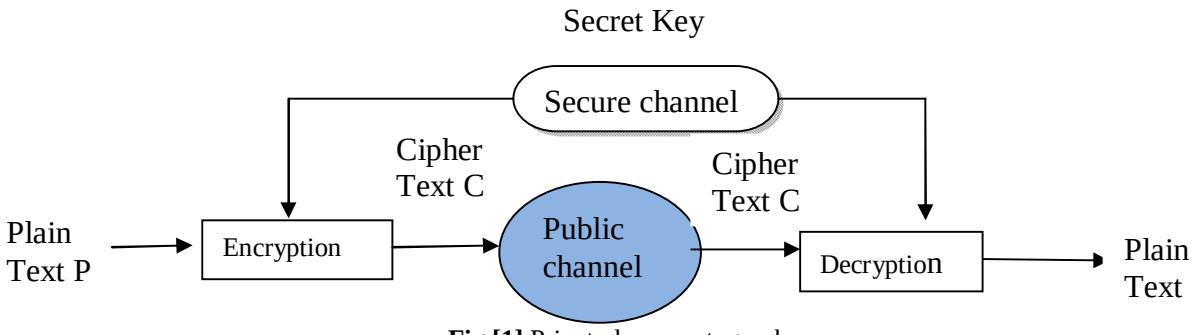

Fig.[1] Private-key cryptography

ISSN (Print) : 2320 – 3765
ISSN (Online): 2278 – 8875

International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 5, Issue 7, July 2016

In public key cryptography both sender and receiver has a pair of public and private key. Public key, used for encryption, is openly announced whereas private key, used for decryption, is confidential. Fig.[2] shows the basic diagram of public key cryptography.

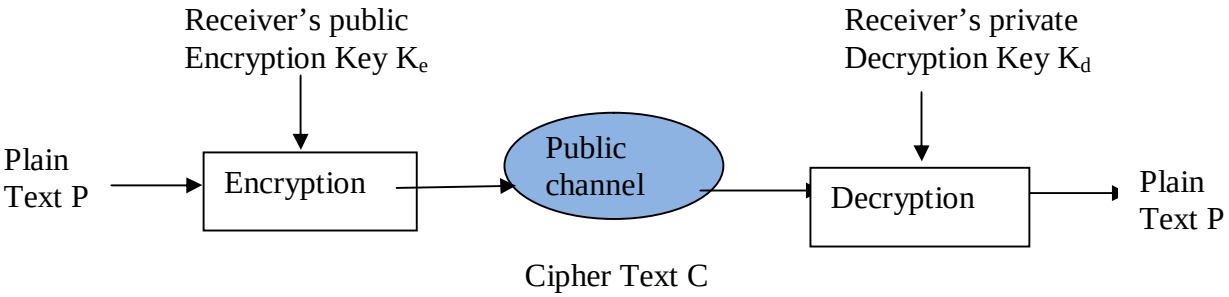

Fig.[2] Public-key cryptography

In the basic image encryption model, the encryption is done via permutation, substitution and their combination. Image encryption-decryption, likewise textual encryption-decryption requires an algorithm and a secret key. Fig.[3] shows the basic image encryption model

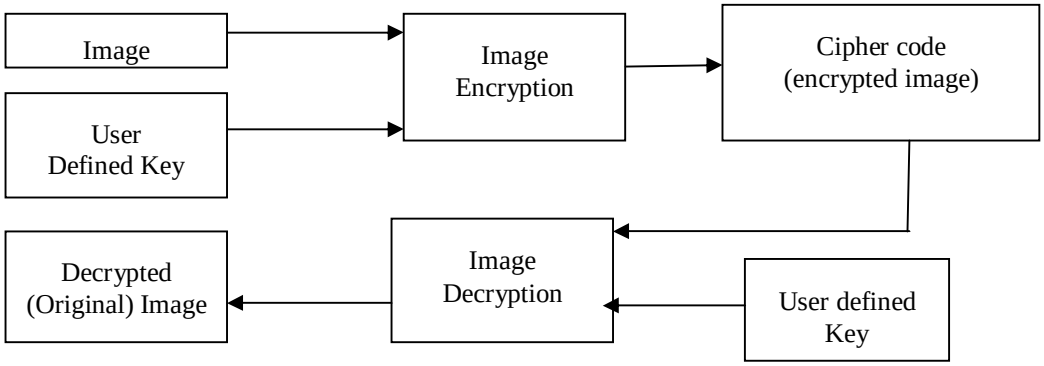

Fig.[3] Image Encryption Model

Due to the inherent properties of chaos, such as quasi-randomness, dependence on initial conditions, ergodicity, system parameters and sensitivity, so many researches has been done in the last decade and it becomes a promising alternative aver the conventional cryptography algorithms.

II. LITERATURE REVIEW

Depending upon the requirement so many private key image encryption models are proposed by researchers. Here, some of them are briefly covered. But main focus is given to chaos based image encryption techniques. In the survey of many existing schemes, a moderate or even low security is found. Finally, to increase the efficiency required for real-time operation purpose, a modified chaotic image encryption technique is proposed.
The main private key image encryption techniques being used today are-

a) **Selective Bit Plane Image Encryption:** When encryption time is important aspect then this encryption scheme is used. In this, in spite of encrypting whole image, a small portion of image is encrypted. But there is no convincing approach to determine which portion of bit plane is to be used for encryption [2] [3].

b) **SCAN based Encryption:** When image security is important aspect then this encryption scheme is used. In this, the plain image is described by SCAN language after serializing into 1D data stream. SCAN letters corresponds to several scanning orders and combination of them is SCAN string. Different SCAN strings form different kinds of secret images. This SCAN string is the encryption key for the given 2D image array. During encryption, noise is combined with SCAN string at particular image points. Since only the authenticated user knows the correct SCAN

ISSN (Print) : 2320 – 3765
ISSN (Online): 2278 – 8875

International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 5, Issue 7, July 2016

combinations hence it provides secure image encryption. But due to lack of compression, the size of image becomes an issue [4] [5] [6].

c) Image Compression based Encryption: Before combining encryption and compression some special measures are required. Generally, entropy encoders are used by many researchers for this. In entropy encoding, for security point of view, multiple statistical models are used in certain secret order to encode and decode. But for proper reconstruction input should be identical to the output of encoder. These schemes also depend upon codec [7] [8].

d) Chaotic Image Encryption: Due to the inherent properties of chaos, chaotic dynamics gains interest over traditional cryptography techniques of researchers. Chaos based cryptography is based on the complex dynamics of non-linear systems or maps which are deterministic but simple. Hence, it is able to provide a fast and secure encryption which is the prime requirement for multimedia data transmission. Some of the image encryption models based on chaos theory are reviewed-

i. G. A. Satish Kumar et al. in *'A novel algorithm for image encryption by integrated pixel scrambling plus diffusion[IISPD]utilizing duo chaos mapping applicability in wireless systems'* proposed an algorithm in which permuting address for rows and columns is calculated by bit XOR adjacent pixel values of original image. After scrambling pixels, diffusion is performed which is based on two chaotic maps. Since, it has higher key space, higher degree of scrambling and lower time complexity, it is very useful in real time applications [9].

ii. Fuyan Sun et al. in *'A novel image encryption scheme based on spatial chaos map'* proposed an image encryption scheme in which spatial chaos map is used to encrypt image in space pixel by pixel. The pixels are then confused in multiple direction of space. Due to the natural properties of spatial chaotic system, image cannot be distinguished in space [10].

iii. Hossam El-din H. Ahmed in *'An efficient chaos based feedback stream cipher (ECBFSC) for image encryption and decryption'* proposed a chaos based feedback stream cipher which is based on chaos map and 256 bit external secret key. Weightage is being provided to the external secret key corresponding to their positions which is used to determine the initial conditions for the chaotic map [11].

iv. Linhua Zhang et al. in *'An image encryption approach based on chaotic maps'* implements spatial S box and design a key scheme for the prevention of gray code attack and statistic attack [12].

v. Ji Won Yoon et al. in *'An image encryption scheme with a pseudorandom permutation based on chaotic maps'* proposed an encryption algorithm in which large pseudorandom permutation is used to generate small permutation matrices [13].

vi. G. A. Satish Kumar et al. in *'Image encryption using random pixel permutation by chaotic mapping'* proposed an image encryption scheme in which PMMLCG and chaotic logistic map is used for random pixel permutation. Through permutation and transformation of pixels in plain image, the chaos characteristics are spread into encrypted image. Because of loss less encryption and highly resistive to various attacks, this scheme is vital for military and medical [14].

vii. Vinod Patidar et al. in *'A new substitution-diffusion based image cipher using chaotic standard and logistic maps'* proposed an image encryption scheme based on two chaotic logistic maps and an 80 bit external key. The external secret key was used to derive the initial conditions for both logistics maps. The initial conditions of second logistic map was modified according to the numbers generated in the range of 1 and 24, by the first logistic map. It is noticed that by modifying initial conditions in this way, system dynamics becomes more random [15].

viii. J. C. Yen et al. in *'A new image encryption algorithm and its VLSI architecture'* proposed an image encryption method, BRIE (bit recirculation based image encryption) in which secret key is based on two integers and initial conditions of logistic map. The bit recirculation of pixels is controlled by a chaotic pseudo random binary sequence [16].

ix. Jiri Fridrich in *'Symmetric ciphers based on two dimensional chaotic maps'* proposed symmetric image encryption scheme based on 2D chaotic map. A two or higher dimensional discretized chaotic map is adopted for pixel permutation together with another 1D map for diffusion. This approach is mainly good for large block size and has a high encryption rate [17].

ISSN (Print) : 2320 – 3765
ISSN (Online): 2278 – 8875

International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 5, Issue 7, July 2016

x. J. Scharinger in *'Fast encryption of image data using chaotic kolmogrov flow'* proposed an image encryption based on kolmogrov flow. In it the whole image is treated as a single block and a key controlled chaotic system is used for permutation. The confusion in data is done through shift register based pseudo random generators [18].

xi. Jui-Cheng et al. in *'A new chaotic key based design for image encryption and decryption'* proposed an image encryption method, CKBA (chaotic key based algorithm), in which a chaotic system is used to generate a binary key sequence which is then used to rearrange pixels and then masking with XOR is done [19].

xii. G. Chen et al. in *'A symmetric image encryption based on 3D chaotic cat maps'* proposed an encryption method in which for designing a real time secure image encryption scheme 2D chaotic map is generalized to 3D. The 3D cat map is used to shuffle the positions of image pixels and security is being achieved by another chaotic map which is used to confuse the relationship between original image and encrypted image [20].

xiii. Jiankun Hu et al. in *'A pixel based scrambling scheme for digital medical images protection'* proposed an encryption technique for large size digital medical images. In this simple pixel level XOR operations are used to generate cryptographic key in such a way that the structural parameters of encryption becomes a part of it [21].

xiv. Long Bao et al. in *'A new chaotic system for image encryption'* proposed a technique that constitutes three distinct 1D chaotic maps. The logistic map acts as a controller to generate random sequences. Then to obtain confusion and diffusion substitution-permutation network (SPN) structure is used [22].

xv. Anchal Jain et al. in *'A two layer chaotic network based image encryption techniques'* proposed a scheme in which two layer chaotic neural network is used for encryption and decryption. To design weights and biases for neural network a logistic chaotic map and for initial conditions an external key is used [23].

xvi. Hazem Mohammad Al-Najjar in *'Digital image encryption algorithm based on multidimensional chaotic system and pixels location'* proposed an encryption scheme based on multidimensional chaotic system. The system dispels pixels and changes the value of it. By substitution and scrambling, pixels values changes and scattered. The proposed algorithm is insensitive to initial conditions and secure to any force attack [24].

xvii. Riah Ukur Ginting et al. in *'Digital color image encryption using RC4 stream cipher and chaotic logistic map'* proposed an algorithm which after converting external key into initial value generates pseudo random numbers with the help of chaotic logistic map. Then masking of plain image with pseudo sequence is done via XOR for encryption [25].

xviii. Sukhjeevan Kaur et al. in 'Image encryption using chaotic map and prime modulo multiplicative linear congruential *generator'* proposed an algorithm in which XOR masking is done on generated chaotic map random sequence and original image pixel and scrambling is done for confusion using sequence generated by PMMLCG and chaotic map [26].

xix. Arihant Kumar Banthia et al. in *'Image encryption using pseudo number generators'* investigate two methods for image encryption, linear congruential generator and chaotic logistic map. In the investigation it is found that both techniques give good results depending upon input parameters [27].

III. PROPOSED WORK

From the survey of various image encryption techniques it is found those chaotic image encryption schemes is very good but to further improve it, a new technique is proposed. In this, chaotic map in combination of LCG is used. With the help of LCG random numbers are generated which is then used for row and column shuffling using chaos map and finally for masking bitwise XNOR is used.

ISSN (Print) : 2320 – 3765
ISSN (Online): 2278 – 8875

International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 5, Issue 7, July 2016

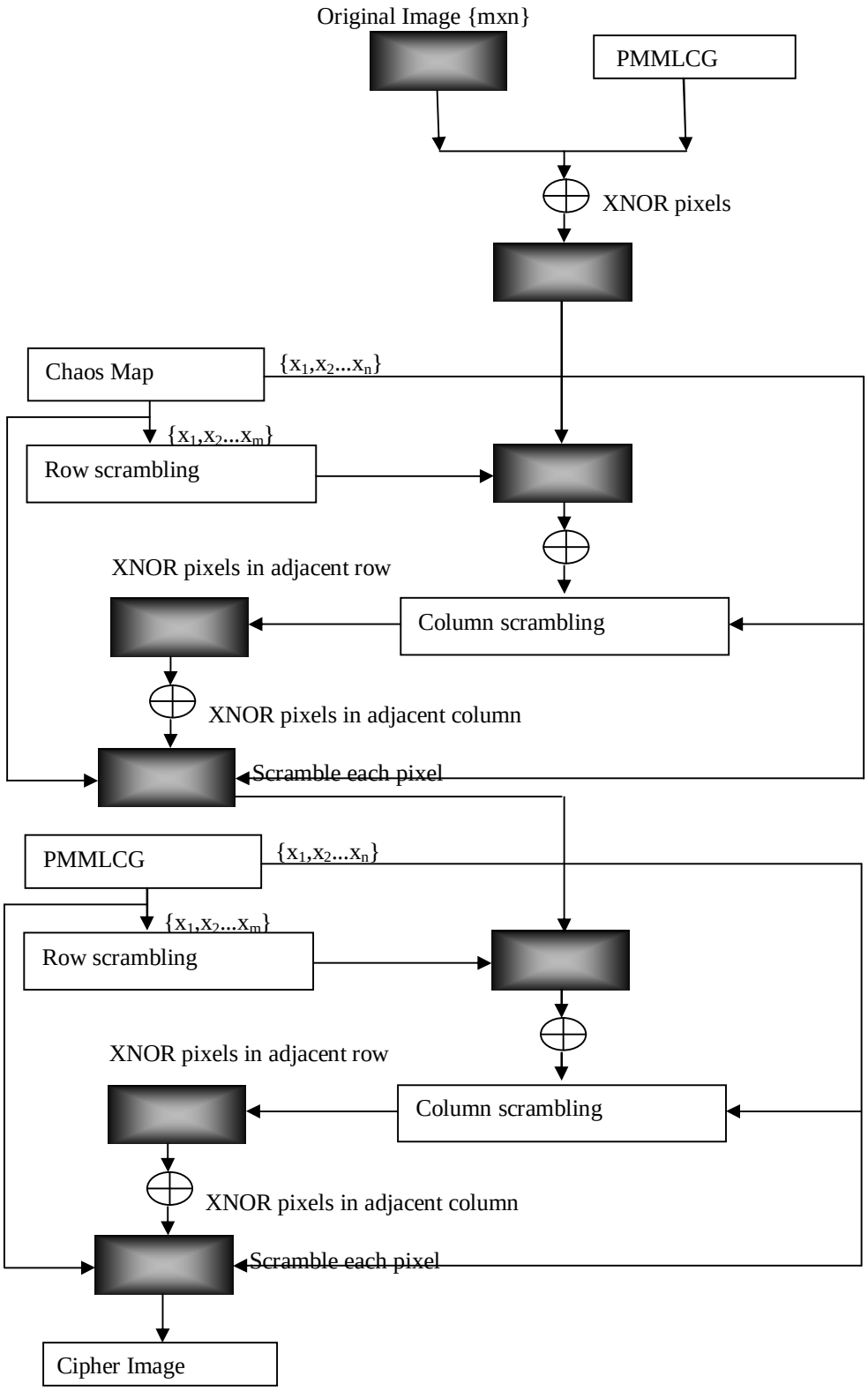

Fig.[4] Proposed Image Encryption Model

ISSN (Print) : 2320 – 3765
ISSN (Online): 2278 – 8875

International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 5, Issue 7, July 2016

IV.CONCLUSION

Since the digital data is communicated in open network hence its security is very important. In this paper, basic concept of encryption is explained and review of some very well known image encryption technique is done. From the survey it is found that although all schemes have their merits and demerits but chaos based encryption scheme is best. And to further increase the overall efficiency, another algorithm is proposed. In the proposed algorithm the two best known schemes are utilized hence it can be very effective in encryption.

REFERENCES

[1] Behrouz A. Forouzan, "Cryptography and Network Security".
[2] B. Furht, D. Socek, A.M. Eskicioglu, "Fundamentals of Multimedia Encryption Techniques", in B. Furht and D. Kirovski (Eds.), Multimedia Security Handbook, Ch. 3, CRC Press, 2005.
[3] Sukalyan Som, Sayani Sen, Suman Mahapatra, Sarbani Palit, "A Selective Bitplane Based Encryption of Grayscale Images with Tamper Detection, Localization and Recovery Based on Watermark", Proc. of Second International Conference India, Springer, vol. 1, pp. 793-802, 2015.
[4] S. S. Maniccam, N. G. Bourbakis, "SCAN based lossless image compression and encryption", IEEE International Conference on Information Intelligence and Systems, pp. 490-499, 1999.
[5] Panduranga H. T, Naveen Kumar S. K, "Hybrid approach for Image Encryption Using SCAN Patterns and Carrier Images", International Journal on Computer Science and Engineering, vol. 2, pp. 297–300, 2010.
[6] Chao-Shen Chen, Rong-Jian Chen, "Image encryption and decryption using SCAN methodology", IEEE Seventh International Conference on In Parallel and Distributed Computing, Applications and Technologies, pp.61-66, 2006.
[7] C.P. Wu, C.C. Kuo, "Design of Integrated Multimedia Compression and Encryption Systems", IEEE Trans. Of Multimedia, vol. 7(5), pp. 828-839, 2005.
[8] H. Cheng, Xiaobo Li, "Partial encryption of compressed images and videos", IEEE Transactions on Signal Processing, vol. 48(8), pp. 2439-2451, 2000.
[9] G. A. Sathish Kumar, K. Bhoopathy Bagan, V. Vivekanand, "A novel algorithm for image encryption by integrated pixel scrambling plus diffusion [IISPD] utilizing duo chaos mapping applicability in wireless systems", Procedia Computer Science 3, pp. 378-387, 2011.
[10] Fuyan Sun, Shutang Liu, Zhongqin Li, and Zongwang Lu, "A novel image encryption scheme based on spatial chaos map", Chaos, Solitons & Fractals, vol. 38(3), pp. 631-640, 2008.
[11] Hossam El-din H. Ahmed, Hamdy M. Kalash, Osama S. Farag Allah, "An efficient chaos-based feedback stream cipher (ECBFSC) for image encryption and decryption", INFORMATICA- 31, pp. 121-129, 2007.
[12] Linhua Zhang, Xiaofeng Liao, Xuebing Wang, "An image encryption approach based on chaotic maps", Chaos, Solitons & Fractals, vol. 24(3), pp. 759-765, 2005.
[13] Ji Won Yoon, Hyoungshick Kim, "An image encryption scheme with a pseudorandom permutation based on chaotic maps", Communications in Nonlinear Science and Numerical Simulation, vol. 15(12), pp. 3998-4006, 2010.
[14] Sathishkumar, G. A., Ramachandran Srinivas, K. Bhoopathy Bagan, "Image encryption using random pixel permutation by chaotic mapping", IEEE Symposium on Computers & Informatics, pp. 247-251, 2012.
[15] Vinod Patidar, N.K. Pareek, K.K. Sud, "A new substitution–diffusion based image cipher using chaotic standard and logistic maps", ELSEVIER , Communications in Nonlinear Science and Numerical Simulations, vol. 14(7), pp. 3056– 3075, 2009.
[16] J. C. Yen, J. I. Guo, "A new image encryption algorithm and its VLSI architecture", IEEE workshop on Signal Processing Systems, pp. 430–437, 1999.
[17] Jiri Fridrich, "Symmetric ciphers based on two dimensional chaotic maps", Int. J. of Bifurcation and Chaos, vol. 8(6), pp. 1259–1284, 1998.
[18] J. Scharinger, "Fast encryption of image data using chaotic Kolmogrov flow", J. of Electronic Imaging, vol. 7(2), pp. 318–325, 1998.
[19] Jui-Cheng, J. I. Guo, "A new chaotic key based design for image encryption and decryption", Proceedings of the IEEE International Symposium Circuits and Systems, vol. 4, pp. 49–52, 2000.
[20] Guanrong Chen, Yaobin Mao, Charles K. Chui, "A symmetric image encryption based on 3D chaotic cat maps", Chaos, Solitons & Fractals, vol. 21(3), pp. 749–761, 2004.
[21] Jiankun Hu, Fengling Han, "A pixel-based scrambling scheme for digital medical images protection", Journal of Network and Computer Applications, vol. 32(4), pp. 788-794, 2009.
[22] Long Bao, Yicong Zhou, C. L. Philip Chen, Hongli Liu, "A new chaotic system for image encryption", IEEE international Conference on System Science and Engineering, pp. 69-73, 2012.
[23] Anchal Jain, Navin Rajpal, "A two layer chaotic network based image encryption techniques", IEEE national Conference on Computing and Communication Systems, pp. 1-5, 2012.
[24] Hazem Mohammad Al-Najjar, "Digital image encryption algorithm based on multi-dimensional chaotic system and pixels location", Int. J. of Computer Theory and Engineering, vol. 3(4), pp. 354-357, 2012.
[25] Riah Ukur Ginting, Rocky Yefrenes Dillak, "Digital color image encryption using RC4 stream cipher and chaotic logistic map", IEEE Internation Conference on Information Technology and Electrical Engineering, pp. 101-05, 2013.
[26] Sukhjeevan Kaur, Shaveta Angurala, "Image encryption using chaotic map and prime modulo multiplicative linear congruential generator", Int. J. of Innovative Research in Computer and Communication Engineering, vol. 3(3), pp. 2339-2345, 2015.
[27] Arihant Kr. Banthia, Namita Tiwari, "Image encryption using pseudo random number generators", Int. J. of Computer Applications, vol. 67(20), pp. 1-8, 2013.