JCSE International Journal of Computer Sciences and Engineering Open Access

Research Paper Volume-6, Issue-3 E-ISSN: 2347-2693

An Image Encryption Using Chaos Algorithm Based on GLCM and PCA

Jyotsna[1*], Anubhooti Papola[2]

[1*]Computer Science and Engineering, Faculty of Technology, Uttarakhand Technical University, Dehradun, India
[2] Computer Science and Engineering, Faculty of Technology, Uttarakhand Technical University, Dehradun, India

[*]Corresponding Author: kunwar.jyotsna28@gmail.com, Tel.: 9520321588

Available online at: www.ijcseonline.org

Received: 21/Feb//2018, Revised: 27/Feb2018, Accepted: 20/Mar/2018, Published: 30/Mar/2018

***Abstract*— The Image encryption is the technique which can hide the sensitive text data. In the past times, various techniques has been proposed for image encryption which are broadly into wavelet transformation and discrete transformation, In this research paper, novel technique has been proposed which is based on textual feature extraction, selection and encryption. The GLCM algorithm is applied for the textual feature analysis, PCA algorithm is used for feature selection and block wise encryption is applied to generate final stego image. The proposed algorithm is implemented in MATLAB and it has been analyzed that it performs well in terms of PSNR and MSE.

***Keywords*— Chaos algorithms, GLCM, PCA, stego image

I. Introduction

Encryption is the process of transforming information using an algorithm to make it unreadable to anyone except those possessing special knowledge, usually referred to as a key. The output is known as the cipher text. The reverse process of transforming cipher text to plaintext is known as decryption.

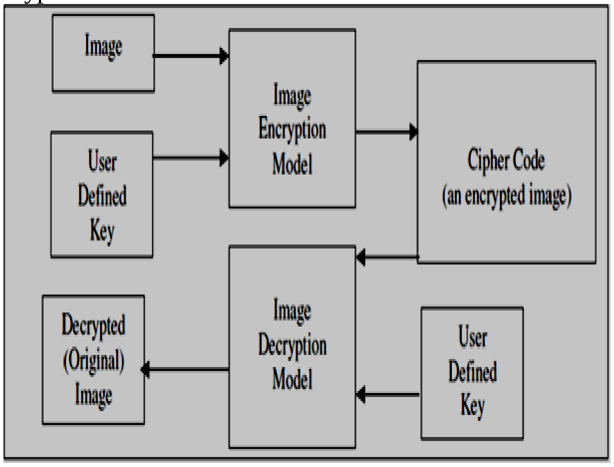

Figure 1.1: Image Encryption and Decryption Process block diagram

Encryption has long been used by militaries and governments to facilitate secret communication. It is now commonly used in protecting information within many kinds of civilian systems. For example, the Computer Security Institute reported that in 2007, 71% of companies surveyed utilized encryption for some of their data in transit, and 53% utilized encryption for some of their data in storage. Encryption can be used to protect data "at rest", such as information stored on computers and storage devices (e.g. USB flash drives). In recent years, there have been numerous reports of confidential data, such as customers' personal records, being exposed through loss or theft of laptops or backup drives. Encrypting such files at rest helps protect them if physical security measures fail. Digital rights management systems, which prevent unauthorized use or reproduction of copyrighted material and protect software against reverse engineering, is another somewhat different example of using encryption on data at rest. In response to encryption of data at rest, cyber-adversaries have developed new types of attacks. These more recent threats to encryption of data at rest include cryptographic attacks, stolen cipher text attacks, attacks on encryption keys, insider attacks, data corruption or integrity attacks, data destruction attacks, and ransom ware attacks. Data fragmentation and active defense data protection technologies attempt to counter some of these attacks, by distributing, moving, or mutating cipher text so it is more difficult to identify, steal, corrupt, or destroy. Encryption is also used to protect data in transit, for example data being transferred via networks.

In this paper, the technique of block wise encryption is the applied. In which, the whole image is divided into fixed size blocks and each block is encrypted individually. The encrypted blocks are combined together to form original image. To apply block wise encryption, technique of chaos. There are two stages in the chaos-based image cryptosystem. The confusion stage is the pixel permutation where the position of the pixels is scrambled over the whole image without exasperating the value of the pixels and the image ends up plainly unrecognizable. The pixel permutation is completed by a chaotic system. The chaotic behavior is controlled by the initial conditions and control parameters which are derived from the 16-character key. To improve the security, the second stage of the encryption process aims at changing the value of every pixel in the entire image a vital tool to shield image from attackers. To increase security of the image, chose method is applied which can be applied with the GLCM algorithm and PCA algorithm. The GLCM method will extract the textual features and PCA algorithm will select the extracted features, this leads to efficient block wise encryption and increase image security.

After the introduction in Section I the rest of this dissertation is organized as follows: Section II contains the related work, section III explains the methodology with flow chart, Section VI describes results and discussion, Section V concludes research work with future directions.

II. Related Work

Guosheng Gu, et.al, "A fast image encryption method by using chaotic 3D cat maps", 2014

An image encryption strategy utilizing a chaotic 3D feline map is introduced in this paper. The process of the expert postured algorithm contains the simultaneous operations of pixels' locations permutation and pixels' values substitution at each iterative stride of the chaotic map, which making the forward and reverse encryption needs just a single traverse of the image pixels. Additionally, a perturbation is introduced to eliminate the undesirable finite precision impact of PC in acknowledgment [20]. The principle advantages of such a secure technique are the simplicity and efficiency. Both simulations and analysis demonstrate the proposed algorithm can deliver a huge key space and resist the basic existing cipher attacks. These good cryptographic properties make it suitable for image applications. It is verified being immune to different types of cryptographic attacks also. One can without much of a stretch to extend the algorithm for shading images by employing encryption to the Red, Green, Blue channels independently. Simulations and analysis demonstrate the proposed efficient algorithm is confidential secure and expected to be helpful for applications.

Brahim Nini, et.al, "Analysis of the Use of Some Statistical Measures in Deciding about the Efficiency of an Image Encryption Algorithm", 2016

The majority of papers on image encryption give a few measures to bear witness to that the exhibited works fulfill the required criteria in the field. Some others propose a comparative study and decide on whether one work is superior to anything another continually utilizing these measures. These last are of various sorts where the correlation coefficient is one among them. It is a statistical measure used to analyze the resemblance between neighboring pixels in an acquired cipher. In this paper, a study about the relevance of this criterion is given to the decision about the quality of a calculation. The paper demonstrates that its significance is limited to have an idea about the resulting decor relation. Be that as it may, its utilization to decide about the quality of the calculation or to compare it to another is unrealistic [21]. The paper demonstrates that any figured value is surrounded by randomness. The correlation coefficient might be utilized as a part of the decision on the off chance that one can figure every single possible value in view of all combinations. This is not useful since it includes a huge number of

Operations. Besides, this implies a study of a convergence in light of the number of emphases of the calculation and this is typically infinite. This is the reason we advise authors not to depend on such statistical value in their decisions about the quality of algorithms.

Venkata Krishna, et.al, "A Novel Image Encryption Algorithm using AES and Visual Cryptography", 2016

With the present rise of the Internet, there is a need to securely transfer images between systems. In this context, we propose a secure image encryption calculation that utilizations both AES and Visual Cryptographic procedures to protect the image. The image is encrypted utilizing AES and an encoding mapping has been proposed to convert the key into shares in view of Visual Secret Sharing. The cryptanalysis of the calculation is then performed and is proved to be secure. The proposed calculation is then implemented utilizing python and the results are talked about alongside the possible future modifications. The confidentiality of shares is likewise tested by changing the key shares before coming to the destination [22]. In every one of the cases it has been observed that if any intruder will be fruitful in getting the encrypted shares from network, he or she can't retrieve the original secret image without accessibility of cipher. Likewise since the complexity of the encryption is twofold layered the hacker couldn't in any way, shape or form becomes acquainted with the algorithms utilized as a part of the encryption. So it is as yet hard to break the visual cryptography regardless of the possibility that the hacker gets his hands on the key shares over the network.

Abul Hasnat, et.al, "A Novel Image Encryption Algorithm Using Pixel Shuffling and Pixel Intensity Reversal", 2016

Visual cryptography is process to shroud information of digital images which has turned into an active area of research during the most recent decades. On account of intrinsic features of images (i.e. bulk data capacity, high redundancy and so forth) encryption of images is not quite the same as that of texts and it is for the most part hard to handle by traditional methods. Show study proposes a novel symmetric image encryption calculation utilizing pixel shuffling and reversed binary string of pixel intensity value. Here, the measure of the proposed Key_row and Key_col vectors are same as the no of rows and no of columns of the original image. For every pixel, at first binary example of pixel intensity value is reversed. In the following step, the new intensity value is stored at a shuffled position [23]. The pixel

position is shuffled utilizing two key vectors-Key row and Key_col. The proposed strategy is connected on benchmark images and assessment of execution is done utilizing distinctive standard metric for key testing-histogram, correlation, entropy, NPCR and UACI between the original and encrypted image. Theoretical analysis and experimental results both affirm that proposed calculation possesses high security and can resist statistical and differential attacks.

Xingyuan Wang, et.al "An Effective and Fast Image encryption algorithm based on Chaos and Interweaving of rank"2016

An effective and fast image encryption algorithm proposed on the basis of chaos and interweaving of ranks. The pairs are interwoven from all the four directions of rows and columns. The shuffling and diffusion of the systems are better which can help in enhancing the performance. The plain image is scanned by the four pointers. Further four points are generated by logistic map which help in determining the rows or columns that are to be switched. The various experiments are conducted which help in analyzing the proposed algorithm. It is seen through the analysis that the proposed algorithm has good feature of security and speed. This helps in preventing various attacks to enter the systems.

III. METHODOLOGY

This work is based on image encryption and base paper technique is applied on enciphering application in which image is transmitted unsecured channels. To encrypt the image for the transmission over unsecured channels image is divided into blocks. The image when divided into blocks and these divided blocks are rearranged to encrypt the image. The blocks are shuffled into fixed pattern and this pattern is decided by the key which used for encryption. The key is derived based on relationship between pixels of the image. The proposed technique performs well and it is been analyzed that proposed technique provide good results against various attacks. In future, we will work on key generation phase to drive key based on textural features of the image so that pixel loss will be minimum at the time of decryption. The proposed algorithm can be applied in the following steps:-

1. Pre-processing Phase: - In the pre-processing phase, the two image are taken as input. The first image is the original image and second image is the image which needs to encrypt. The first image is used to generate key and second image will be encrypted with the key of first image

2. Feature extracted: - In the second phase, the textual features of the first image is extracted using the glcm algorithm. The glcm algorithm will extract the features like energy, entropy etc. image.

In the next step, the keys are generated from the one image. The second one image is divided into blocks and each block is encrypted individually to generate final encrypted image. The chaos-based image cryptosystem fundamentally consists of two stages. The plain image is given at its input. There are two stages in the chaos-based image cryptosystem. The confusion stage is the pixel permutation where the position of the pixels is scrambled over the whole image without exasperating the value of the pixels and the image ends up plainly unrecognizable. The pixel permutation is completed by a chaotic system. The chaotic behavior is controlled by the initial conditions and control parameters which are derived from the 16-character key. To improve the security, the second stage of the encryption process aims at changing the value of every pixel in the entire image a vital tool to shield image from attackers.

The confusion stage is the pixel permutation where the position of the pixels is scrambled over the whole image without irritating the value of the pixels and the image ends up noticeably unrecognizable. In this way these initial conditions and control parameters fill in as the secret key. It is not exceptionally secure to have just the permutation stage since it might be broken by any assault. To improve the security, the second stage of the encryption process aims at changing the value of every pixel in the entire image. The process of diffusion is likewise brought out through a chaotic map which is for the most part dependent on the initial conditions and control parameters.

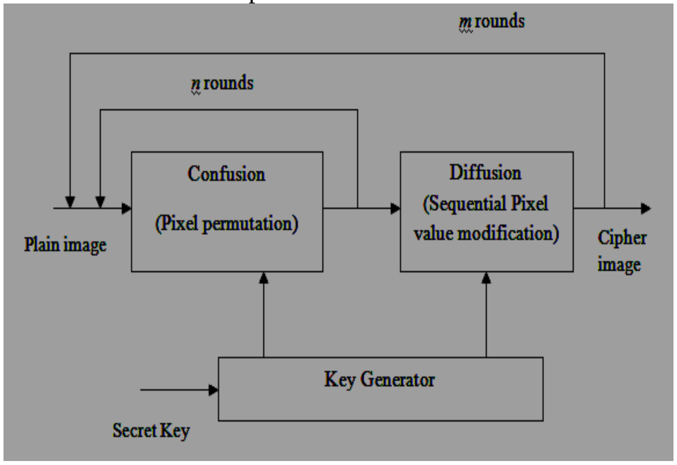

Figure: 3.1 Architecture of Chaos-based image cryptosystem

In the diffusion stage, the pixel values are modified sequentially by the sequence produced from one of the three chaotic systems chosen by outside key. The entire confusion-diffusion round repeats for various times to accomplish an agreeable level of security. The haphazardness property characteristic in chaotic maps makes it more reasonable for image encryption.

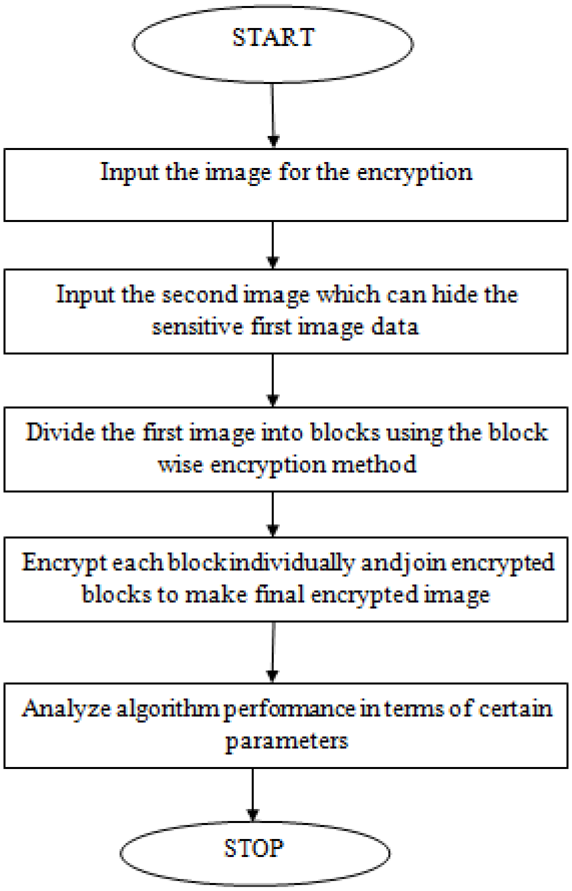
START
Input the image for the encryption
Input the second image which can hide the sensitive first image data
Divide the first image into blocks using the block wise encryption method
Encrypt each block individually and join encrypted blocks to make final encrypted image
Analyze algorithm performance in terms of certain parameters
STOP

Fig3.2 proposed Flowchart

IV. RESULTS AND DISCUSSION

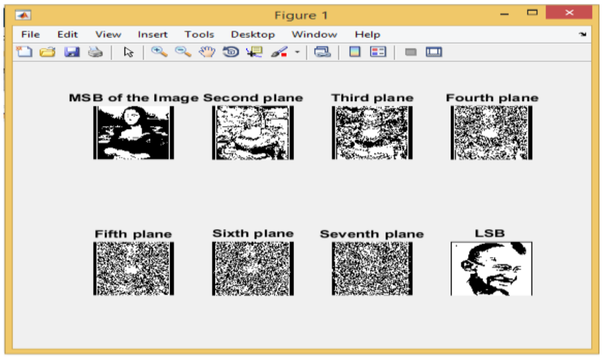

Fig 4.1: Selection of image

As show in figure 2, the first image is selected and second image is fixed which can divide the whole image into blocks and each block is divided into parts to generate final encrypted image.

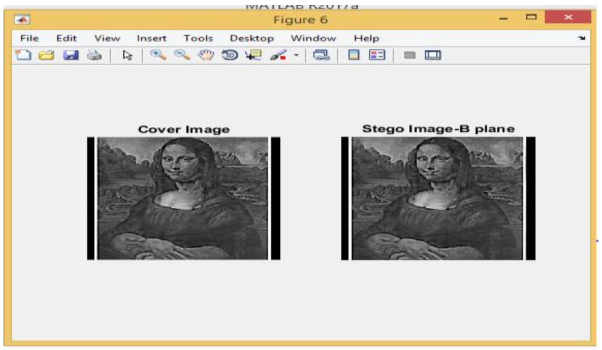

Fig 4.2 Stegno Image Generation

As shown in figure 4, the stegno image generated from the original images by inserting text into the B plane of the image

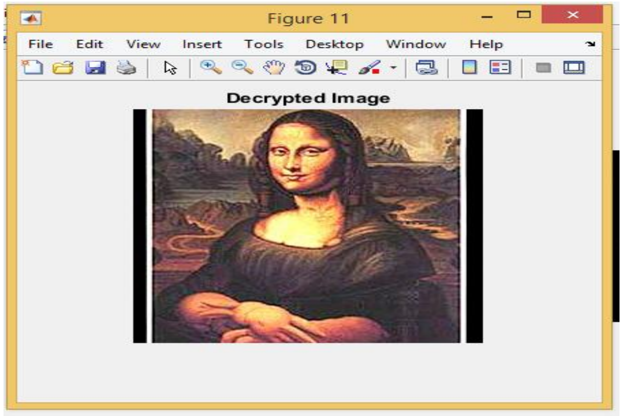

Fig 4.3: Decryption of image

As shown in figure 5, the inverse technique is applied which will remove text from the image and generate decrypted image

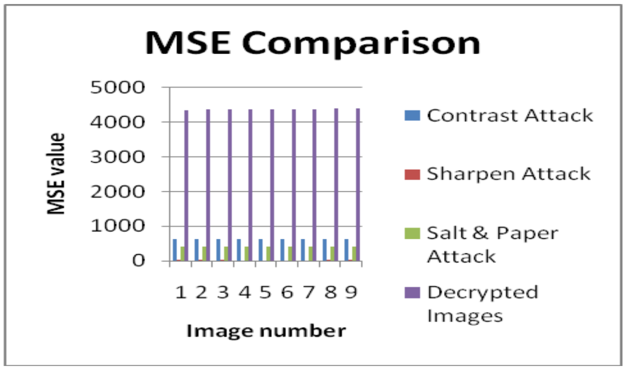

Fig 4.4: MSE Comparison

As shown in figure 4.4, the MSE values of various scenarios like salt & pepper, contract, sharpen and decryption is compared and it has been analyzed that proposed algorithm has least impact of the attacks.

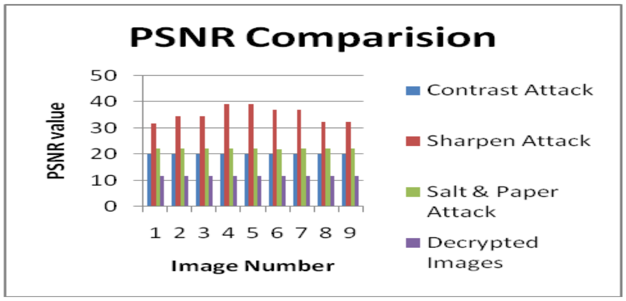

Fig 4.5: PSNR Comparison

As shown in figure 4.5, the PSNR values of the contrast, sharpen, salt & pepper and decryption is compared and it has been analyzed that sharpen is the attack which has minimum impact on the proposed algorithm.

Table 1: Quantitative comparison

	Parameter values	Base	Proposed
Encrypted image	PSNR	13.3917	13.0129
	MSE	3001.26	3274.83
	Correlation Coefficient	0.01	0.01
	Entropy	7.9990	7.9989
Contrast Attack	PSNR	20.0542	20.0537
	MSE	647.22	647.30
	Correlation Coefficient	0.96	0.01
	Entropy	4.2319	4.2200
Sharpened Attack	PSNR	23.6209	23.4842
	MSE	284.70	293.80
	Correlation Coefficient	0.97	0.98
	Entropy	7.003	6.9047
Salt & pepper Attack	PSNR	22.4476	23.484
	MSE	373.00	293.80
	Correlation Coefficient	0.96	0.91
	Entropy	7.9012	7.9036
Decrypted image	PSNR	13.3848	13.0130
	MSE	3006.02	3274.75
	Correlation Coefficient	0.01	0.00
	Entropy	7.6833	3.4237
Elapsed time		0.011795 sec	0.011994 sec

As shown in table 1, the PSNR and MSE values of the base paper, algorithm is analyzed in the form of different attacks like salt & pepper, Sharpened Attack and Contrast Attack

V.CONCLUSION AND FUTURE SCOPE

In previous work, it is been concluded that image encryption is the efficient technique which provides security to the image data. In this paper, chaos technique is been proposed which is based on textual feature of the images. The two images are taken as input in which first image is used to generate key and second image is encrypted with the key of first image using block wise encryption. The textual features of the first image are analyzed using glcm algorithm and PCA algorithm is applied to select textual features of the image. The block wise encryption is applied which generate encrypted image. The reliability of the encrypted image is analyzed by applying various attacks on the image like contrast, sharpen and salt & pepper attack. The technique can be further improved using increasing the pixel size for better security and further tested under the different parameters.

.

REFERENCES

[1] A Shamir, "How to Share a Secret", 1979, Communications of the ACM, vol. 22, no. 11, pp. 612-613

[2] J. Fridrich, "Symmetric ciphers based on two-dimensional chaotic maps", 1998, Int J Bifurcat Chaos, vol. 8, no. 6, pp. 1259–1284

[3] Jiri Fridrich, "SYMMETRIC CIPHERS BASED ON TWO-DIMENSIONAL CHAOTIC MAPS", 1998, International Journal of Bifurcation and Chaos, Vol. 8, No. 6, 1259-1284

[4] L. Kocarev, "Chaos-based cryptography: a brief overview", 2001, IEEE Circ Syst Mag, vol. 1, no 3, pp.6–21

[5] G. Chen, Y. Mao and C. K. Chui, "A symmetric image encryption scheme based on 3D chaotic cat maps", 2004, Chaos, Solitons & Fractals; vol. 21, pp. 749–761

[6] M. Naor and A. Shamir, "Visual Cryptography", 2006, Advances in Cryptography-Eurocrypt, LNCS, vol. 950, pp. 1-12

[7] S. Mohammad, R. Farshchi and I. D. Ebrahimi, "A Novel Encryption Algorithm for Transmitting Secure Data based on Genetic Hyper Chaos Map", 2011, Proc. of International Conference on Computer Communication and Management, Singapore, vol. 5, pp. 623-627

[8] D. Chattopadhyay, M. K. Mondal and D. Nandi, "Symmetric key chaotic image encryption using circle map", 2011, Indian Journal of Science and Technology, vol. 4, no. 5, pp. 593-599

[9] Guoji Zhang, Qing Liu, "A novel image encryption method based on total shuffling scheme", 2011, Optics Communications 284 2775–2780

[10] J. Mohamedmoideen Kader Mastan, G. A. Sathishkumar, K. Bhoopathy Bagan, "A Color Image Encryption Technique Based on a Substitution- Permutation Network", 2011, Proc of First International Conference ACC Kochi, India, vol.193, no. 3, pp. 524-533

[11] S. V. Sathyanarayana, M. A. Kumar and K. N. Hari Bhat, "Symmetric Key Image Encryption Scheme with Key Sequences Derived from Random Sequence of Cyclic Elliptic Curve Points", 2011, International Journal of Network Security, vol.12, no.2, pp.166–179

[12] Y. Wu, J. P. Noonan and S. Agaian, "NPCR and UACI Randomness Tests for Image Encryption", 2011, Cyber Journals: Multidisciplinary Journals in Science and Technology, April Ed. pp. 31-38

[13] Taneja, N., Raman, B., Gupta, I., "Selective image encryption in fractional wavelet domain", 2011, Int. J. Electron. Commun., 65, pp. 338–344

[14] Rashmi P., Bharathi R.K., Shruthi Prabhakar, Reshma Banu, Rachana C.R., "Performance Analysis of Self Adaptive Image Encryption Technique", International Journal of Scientific Research in Network Security and Communication, Vol.5, Issue.3, pp.44-58, 2017.

[15] R. Afarin and S. Mozaffari, "Image encryption using genetic algorithm", 2013, Proc. 8th Iranian Conference on Machine Vision and Image Processing

[16] L. Abraham and N. Daniel,"Secure Image Encryption Algorithms: A Review", 2013, International Journal of Scientific & Technology Research Vol. 2, no. 4, pp. 186-189

[17] M. A. Mokhtar, S. N. Gobran and E. A. El-Badawy, "Colored Image Encryption Algorithm Using DNA Code and Chaos Theory", 2014, International Conference on Computer and Communication Engineering (ICCCE), pp. 12-15

[18] S. Rohith, K. N. H. Bhat and A. N. Sharma, "Image encryption and decryption using chaotic key sequence generated by sequence of logistic map and sequence of states of Linear Feedback Shift Register", 2014, International Conference on Advances in Electronics, Computers and Communications (ICAECC)

[19] S. Sowmya and S. V. Sathyanarayana, "Symmetric Key Image Encryption Scheme with Key Sequences Derived from Random Sequence of Cyclic Elliptic Curve Points over GF(p)", 2014, International Conference on Contemporary Computing and Informatics (IC3I)

[20] Guosheng Gu, Jie Ling, "A fast image encryption method by using chaotic 3D cat maps", 2014 Elsevier GmbH. All rights reserved

[21] Venkata Krishna Pavan Kalubandi, Hemanth Vaddi, Vishnu Ramineni, Agilandeeswari Loganathan, "A Novel Image Encryption Algorithm using AES and Visual Cryptography", 2016 2nd International Conference on Next Generation Computing Technologies (NGCT-2016)

[22] Abul Hasnat, Dibyendu Barman, Satyendra Nath Mandal, "A Novel Image Encryption Algorithm Using Pixel Shuffling and Pixel Intensity Reversal", 2016, IEEE

[23] Xingyuan Wang, Chuanming Liu, Huili Zhang, "An effective and fast image encryption algorithm based on Chaos and interweaving of ranks", 2016, Springer Science+Business Media Dordrecht

[24] Wiam Zamrani, Esmail Ahouzi, Angel Lizana, Juan Campus and Maria Josefa Yzuel, "Towards the Growth of Optical Security Systems for Image Encryption by Polarized Light", 2016, IEEE

Authors Profile

Ms Jyotsna completed Bechuler of Computer Science from Uttarakhand Technical University Dehradun in 2016 and she is cuently pursuing Master of Tchnology under uttarakhand Technical University Dehradun,india.

Mrs Anubhooti Papola working as an assistant professor in Uttarakhand technical University in department of computer science .She is doing her PhD in computer science and engineering from Uttarakhand technical University. She is post graduate from Graphic Era University and graduate from HNB Gharwal University.