DOI: https://doi.org/10.36094/sc.v89.2023.Sparse_Based_Image_Encryption.Choudhury.400

ARTICLE

Sci. and Cult. 89 (11–12) : 400-405 (2023)

SPARSE BASED IMAGE ENCRYPTION USING 6D-CHAOTIC SYSTEM AND RC6

HRISHIKESH MONDAL[1*], ARGHYA PATHAK[2], SUBHASHISH PAL[3],
ANUP KUMAR DAS[4] AND SOMNATH CHOUDHURY[5]

This paper proposes a symmetric key image encryption technique using 6D-chaotic system. Non-zero elements of the generated sparse matrix with the help of a well-trained dictionary for a greyscale image are only considered for encryption. The initial condition of the variates used in chaotic system has been generated from a 32-bit char user key after encrypting with RC6(32,16,12). The efficiency of the proposed cryptosystem, has been analyzed by performing the standard test like Entropy, SSIM, NPCR, UACI, Histogram analysis etc.

Introduction

In modern day telecommunication, smart phone becomes a popular gazette because of its multipurpose use. People not only using this device to connect themselves through phone call, email, WhatsApp, Facebook, twitter etc. they also using it for online banking, telemedicine, online shopping purposes. Sensitive information is passed in the form of text, image, speech and video which may subjected to hacking. Thus to protect the sensitive information from stealing or intervening by unauthorized person is the prior job for the cryptographer and they are continuously trying to develop more and more complex cryptosystem. Not only in public domain, the requirement of an efficient cryptosystem is very much essential in Military and security services.In data encryption, there exist very efficient algorithm such as RC4, RC5, RC6, blowfish, AES etc.[1-5] but are inefficient for image encryption as they take long time to process and need more space for communicating depending on the size of the images. In image cryptography, the primary goal is to break the correlation between the adjacent pixel by employing confusion and diffusion with the help of mathematical tools and models.

Present day, discrete wavelet transformation, DNA model, S-Box, Hash function, bit-interspersing are used along with chaos[6-13] to build efficient cryptosystem. Since chaotic system can produce pseudorandom numbers depending on its initial condition and parameter(s) value, it add extra security to encryption mechanism along with the user key and hard to break. A chaotic system is that dynamical system which produces strange attractor and is highly sensitive to its initial condition indicated by at least one of its Lyapunov exponent (LE) is positive. Later it has been found that Hyper chaotic system (with at least two positive LE) are more efficient than the normal chaotic system[14]. Presently neural network and AI are being used to design cryptosystem[15,16].

[1*] Department of Physics, Durgapur Government College, J. N. Avenue,   Durgapur 713214, India
e-mail: hm.13ph1505@phd.nitdgp.ac.in

[2] Department of Physics, National Institute of Technology, M. G. Road, Durgapur-713209, India
e-mail:ap.18ph1102@phd.nitdgp.ac.in

[3] Department of Physics, Dr. B. C. Roy Engineering College, Durgapur- 713206, India
e-mail: sp.20ph1501@phd.nitdgp.ac.in

[4] Department of Electronics and Communication Engineering, Dr. B. C. Roy Engineering College, Durgapur- 713206, India
e-mail: anup.das@bcrec.ac.in

[5] Department of Physics, Suri Vidyasagar College, Suri-731101, India, e-mail: somnathbratati21@gmail.com

The efficiency of a cryptosystem is judged by analyzing the parameters such as NPCR, UACI, SSIM, Information Entropy, Correlation coefficient, time of execution, data size of the encrypted information that will be send to the receiver end etc. To make the encryption fast and to reduce the data size, the researchers focused to reduce the image data as low as possible without losing significant information present within it by using compression techniques. These compression techniques are of two types, one is lossless where all information remains intact and another one is lossy where most of the insignificant information are redundant. Run Length Coding (RLE),Fractal Compression, Discrete Cosine Transform (DCT), Discrete Wavelet Transform (DWT), JPEG2000, Sparse representation technique[17-20] etc. are the example of the said compression technique respectively.

In this paper, we have adopted the sparse representation technique to reduce the volume of the data to be encrypt related to an image. The details about the encryption mechanism is discussed in the next section. In section 3, the results of the tests that we have performed is presented and lastly the conclusion in section 4.

Proposed Algorithm

6D-Chaotic System: When two three stage ROs are coupled together through the series combination of a resistor and a p-n junction diode, the system is capable to produce chaos. The dimensionless mathematical equations for such a system are

$$\left.\begin{aligned}
\dot{x}_{11} &= -x_{11} - a\,x_{13} \\
\dot{x}_{12} &= -x_{12} - a\,x_{11} \\
\dot{x}_{13} &= -b\,x_{13} - ab\,x_{12} - bc\,y \\
\dot{x}_{21} &= -x_{21} - a\,x_{22} \\
\dot{x}_{22} &= -x_{22} - a\,x_{21} \\
\dot{x}_{23} &= -d\,x_{23} - ad\,x_{22} + dc\,y
\end{aligned}\right\} \qquad (1)$$

where,

$$y = \begin{cases} x_{13} - x_{23} - 1 & \text{for} \quad (x_{13} - x_{23}) > 1 \\ 0 & \text{for} \quad (x_{13} - x_{23}) \le 1 \end{cases} \qquad (2)$$

This system shows chaos for a=3.6, b=0.1, c=11 and d=4. The details dynamical behavior about this system can be found in ref. [21].

RC6 Data Encryption Algorithm: In symmetric key encryption, same key is used to encrypt and decrypt the information. According to ref[8], a 32-bit char key is quite efficient to design a good cryptosystem. One must take care of the fact that each character must contribute equally for designing cryptosystem. In our paper, this matter is emphasized by processing the key with RC6 algorithm and then taken into account for encryption. RC6 is a popular data encryption algorithm which was first proposed by Rivest in 1998[3]. In RC6 (32,16,12) algorithm, four 8-bit HEX data is encrypted with a 32-bit HEX key after 12 round of processing and is very efficient against different types of attack reported so far.

Sparse Representation Technique: Sparse representation emerged as a powerful compressing technique in signal processing. Digital images have high data volume therefore sparse representation technique is used to compress the data size for enhancing the computational speed and to reduce allocated memory space. For a better sparse representation an effectively trained dictionary is required. Though there exist several algorithms for training dictionary, we have used feature sign search-based algorithm for this purpose and the details about the generation of the sparse matrix can be found in ref.[2].

Encryption Algorithm: The block diagram of the encryption algorithm is shown in Fig. 1. The details about it is given below step by step.

Step 1: A High-Resolution Dictionary (HD) which has been trained with a large number of images is used to generate the sparse matrix for the 256×256-pixel greyscale image under test after decomposing it into 16×16 pixel patches.

Step 2: The row and column position of the non-zero elements of the generated Sparse Matrix is represented by a 2-bit Hexadecimal number after reducing them by 1. This has been done to incorporate the elements in the 256th row and 256th column.

Step 3: The absolute value of the non-zero elements of the Sparse Matrix is represented by a 4-bit Hexadecimal number which is divided into two equal part the 2-bit LSB and 2-bit MSB. See table 1 for step 2 and 3.

Step 4: The 256 mean values which are essential to reconstruct the image are also represented by 2-bit hexadecimal number.

Step 5: A 32-bit char key (user key) is taken and we divide it equally in two equal parts. Each part is represented by 32-bit hexadecimal number where the consecutive 2-bit represents the asci value of each character. These two sets of 32-bit hexadecimal number is encrypted with RC6(32,16,12) data encryption algorithm using a 32-bit HEX key which has been generated by considering the asci values of the even position character of the 32-bit char key.

Step 6: From the two encrypted 32-bit hexadecimal number, the initial condition for the variates of the 6D chaotic system is formulated. Using this initial condition, the required numbers of random sequence in between 0 to 255 has been derived.

Step 7: The representation of the original information discussed in steps 2, 3 and 4 are arranged as a N bytes of 8 bit HEX string as shown in Table 2, where N is the sum of the number of positive elements, number of negative elements and 66. The number 66 is because of the fact that 64×4 contains the mean of the sparse matrix discussed in step 4 and 2 rows of '00000000' are used to separate positive value information from the negative value information and negative value information from the mean information. In this matrix, the 1st column represent the row value, 2nd represents the column value, 3rd and 4th are thetwo LSB and two MSB of the corresponding non-zero elements of the sparse matrix.

Step 8: Bit XOR operation is then performed with each element of this N×4 matrix and the generated pseudo-random numbers in between 0 and 255 from the 6D chaotic system after representing them by 8-bit binary number to generate the encrypted data which is to be send to the receiver end for decryption.

Table 1. **Generation of Information Matrix**

Sparse Element	Information	Values	HEX Value
Positive	Row position	110	6D
	Column Position	256	FF
	Value	+1115	045B
Negative	Row position	256	FF
	Column Position	208	CF
	Value	-2125	084D

Table 2. **Arranging Information Matrix**

Sparse Element	Matrix's Row Representation
Positive Element	[6D FF 04 5B]
Negative Element	[FF CF 08 4D]

Decryption Algorithm: Reverse algorithm has been followed to reconstruct the original image from the cypher data using the same key. The image generated from the decrypted data differs slightly from the original image because of the tolerance parameter's value used when sparse compression techniquehas been adopted during encryption. This decrypted image shown in Fig. 3 are almost visually same that indicates information loss is insignificant.

Cryptanalysis

The cryptanalysis results have been discussed briefly in this section. We are presenting here the results of the security tests for three images only though we have taken almost ten input images of size 256 × 256 to test the cryptosystem.

Correlation Coefficient: Generally, the basic aim of the image cryptography is to break high correlation among the adjacent pixels of the original image. The correlation coefficient is measured by the following equation and its value for the encrypted image is expected to be nearly zero.

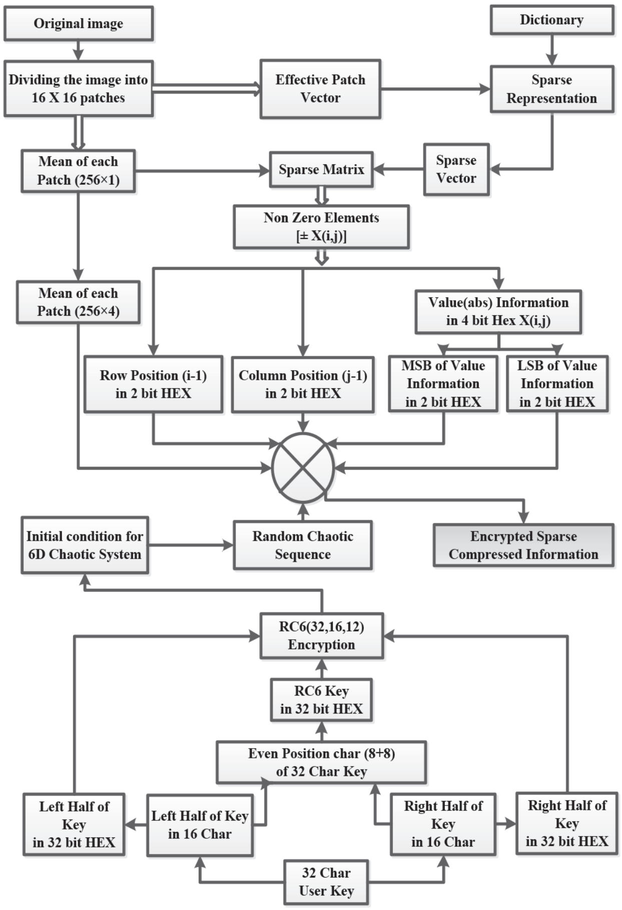

Original image
Dictionary
Dividing the image into 16 X 16 patches
Effective Patch Vector
Sparse Representation
Mean of each Patch (256×1)
Sparse Matrix
Sparse Vector
Non Zero Elements [± X(i,j)]
Mean of each Patch (256×4)
Value(abs) Information in 4 bit Hex X(i,j)
Row Position (i-1) in 2 bit HEX
Column Position (j-1) in 2 bit HEX
MSB of Value Information in 2 bit HEX
LSB of Value Information in 2 bit HEX
Initial condition for 6D Chaotic System
Random Chaotic Sequence
Encrypted Sparse Compressed Information
RC6(32,16,12) Encryption
RC6 Key in 32 bit HEX
Even Position char (8+8) of 32 Char Key
Left Half of Key in 32 bit HEX
Left Half of Key in 16 Char
Right Half of Key in 16 Char
Right Half of Key in 32 bit HEX
32 Char User Key

Fig. 1. Block diagram of the encryption technique.

$$C_r = \frac{\sum_{i=1}^{N}\left(I_i^a - \bar{I}^a\right)\left(I_i^b - \bar{I}^b\right)}{\sqrt{\sum_{i=1}^{N}\left(I_i^a - \bar{I}^a\right)^2 \sum_{i=1}^{N}\left(I_i^b - \bar{I}^b\right)^2}} \tag{3}$$

The values of the correlation coefficient for the original and their encrypted images under test are given in the Table 3. The pictorial output of it has shown in the Fig. 2.

Table 3. Correlation coefficients for Lena, Cameraman and Terracotta images in horizontal (H), vertical (V) and diagonal (D) directions.

Direction	Images	Lena	Cameraman	Terracotta
H	Original	0.9257	0.9271	0.8780
	Encrypted	0.0267	-0.0078	-0.0069
V	Original	0.9582	0.9529	0.8175
	Encrypted	-0.0013	-0.0002	-0.0031
D	Original	0.9014	0.8980	0.7784
	Encrypted	0.0055	-0.0023	-0.0022

Entropy: Entropy measures the randomness of a physical. Higher be the randomness, greater be the value of entropy. Irregularity of the pixel intensity of the encrypted image with respect to original one is measured by the entropy and its maximum value is 8 for 8-bit encryption. Using the following equation, entropy of the cipher image is measured.

$$e(c) = -\sum_{i=0}^{255} p(c_i)\log_2 p(c_i) \tag{4}$$

Where $p(c_i)$ is the probability of occurrence of c_i. The entropy values for different test images are listed in the Table 4.

Table 4. Value of Entropy, SSIM and Compression Ratio (CR) for different encrypted images.

Image Name	Entropy	SSIM	CR
Lena	7.9906	0.8720	3.8189
Cameraman	7.9904	0.8154	3.3437
Terracotta	7.9941	0.8719	1.7235

Histogram Analysis: The statistical nature of the pixel intensities of a digital image can be understood by the histogram plot. More be the flatness of the plateau of the histogram for the encrypted image, it is difficult to extract information from it. The histogram for theoriginal and encrypted images are shown in the Fig. 4.

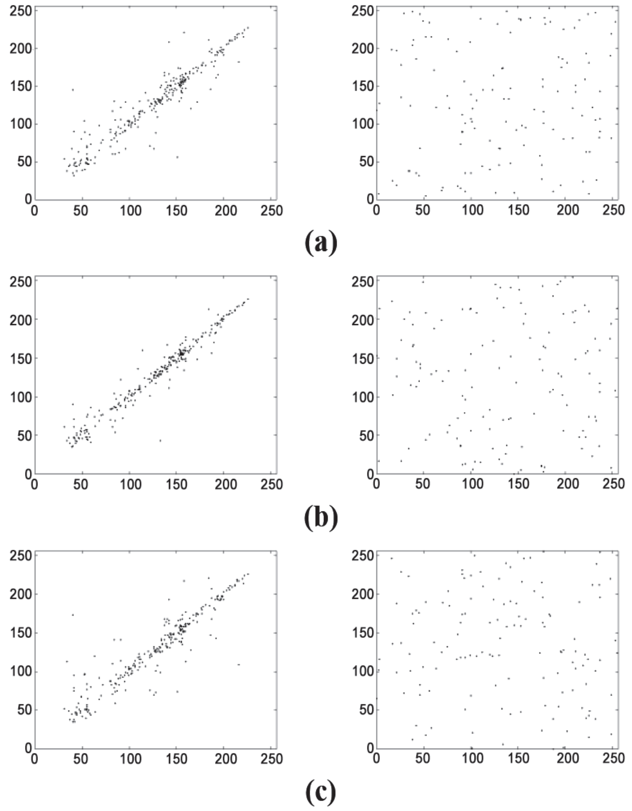


Fig. 2. Pixel correlation of original (in the left column) and encrypted(in the right column) Lena Image in (a) Horizontal direction (b) Vertical direction (c) Diagonal direction.

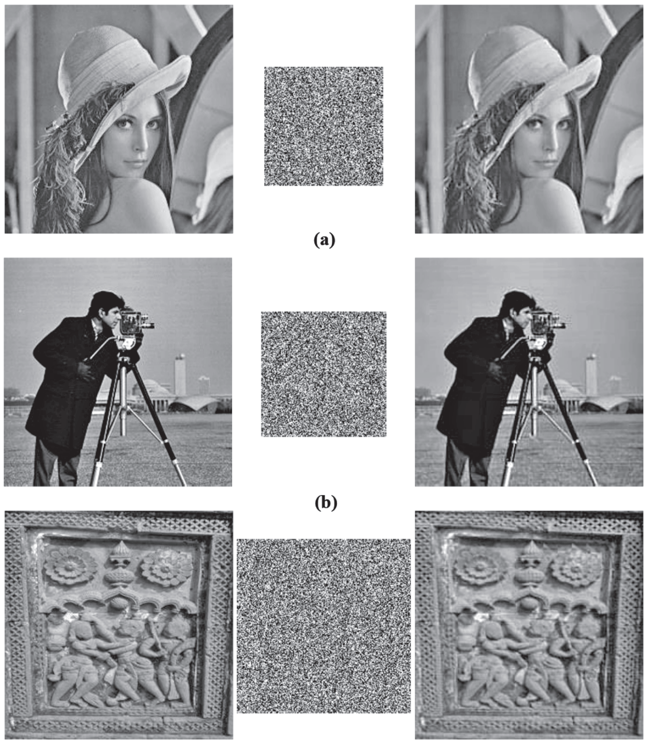
PSNR and SSIM: The PSNR (signal to noise ratio) and SSIM (Structural similarity index matrices) examines the quality of the reconstructed image compared to original image are measured using eq. (5) and eq. (7). High value of PSNR and nearly unity value of SSIM's represents better reconstruction. The measured value for the proposed cryptosystem is listed in table 5.

$$PSNR = 10\log\left(\frac{O_{\max}^2}{MSE}\right) \tag{5}$$

Where,

$$MSE = \frac{1}{MN}\sum_{i=1}^{M}\sum_{j=1}^{N}\left[O_{ij} - R_{ij}\right]^2. \tag{6}$$

Where O_{max} is the maximum pixel value of an image of M×N dimension and O and R denote the original and reconstructed image respectively.



(a)

(b)

(c)

Fig. 3. Original (In the left column), encrypted (in the middle) and Decrypted ((In the right column) Images. (a) Lena (b) Cameraman (c) Terracotta.

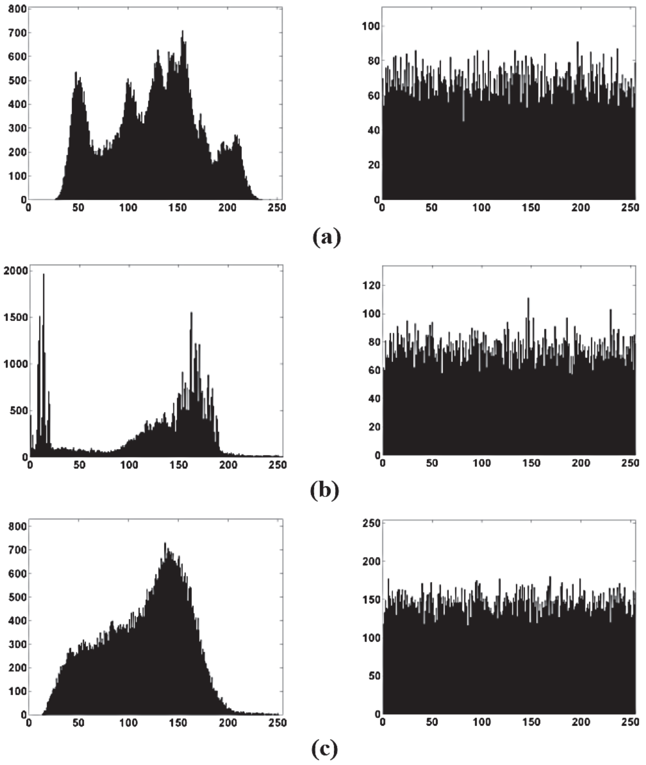


Fig. 4. Histogram of Original (in the Left) and Encrypted Images (In the Right) for (a) Lena (b) Cameraman (c) Terracotta.

Differential Attack Analysis: Whether a cryptosystem is venerable to differential attacks is judged by NPCR and UACI parameters. NPCR measures the pixel change rate between two encrypted images when at least one-pixel element of the original image is changed or increased whereas UACI measures the difference between the average pixel intensity before and after pixel shifting for the encrypted images. The calculated values of NPCR and UACI for different images are measured using eq. (7) and eq. (8) and are listed in Table 5. The maximum theoretical values of NPCR and UACI is 99.6% and 33% respectively.

$$NPCR = \frac{1}{MN}\sum_{i=1}^{M}\sum_{j=1}^{N}\delta_{ij}\times 100\% \qquad (7)$$

Where (i, j) indicates the pixel value position and δ_{ij} provides the information related to variation rate as following:

$$\delta_{ij} = \begin{cases} 0 & I_{ij}^{bs} = I_{ij}^{as} \\ 1 & I_{ij}^{bs} \neq I_{ij}^{as} \end{cases}$$

$$UACI = \frac{1}{mn}\sum_{i=1}^{M}\sum_{j=1}^{N}\frac{\left|I_{ij}^{bs} - I_{ij}^{as}\right|}{255}\times 100\% \qquad (8)$$

Table 5. Values of NPCR, UACI and PSNR of the encrypted images.

Image Name	NPCR	UACI	PSNR
Lena	99.4816	38.6355	29.1500
Cameraman	99.3318	39.4396	28.7952
Terracotta	99.5481	35.6032	29.2004

Conclusion

The mechanism for effective compression and encryption in this study uses a sparse representation technique and 6D chaotic system along with RC6 to encrypt the non-zero sparse element. The compression strength can be judged by counting the number of nonzero elements in the sparse vectors and it is different for different images due to the presence of various features in them and also on the threshold value set while generating it. The results of the test parameters such as NPCR, UACI, Correlation coefficient, PSNR, Information entropy etc. establish the quality of the proposed algorithm. ❐

References

1. R.L. Rivest, The RC5 encryption Algorithm, In: Proceedings of Workshop on Fast Software Encryption, 86–96, (1994).
2. A. Pathak, H. Mondal, J.Karmakar, S. Pal, D. Nandi and M.K. Mandal, *IETE Technical Review*, 1-13, (2023).
3. R. Rivest, M. Robshaw, R. Sidney, and Y. Yin, The RC6TM Block Cipher, First Advanced Encryption Standard (AES) Conference, Ventura, CA, (1998).
4. B. Schneier. Description of a New Variable-Length Key, 64-Bit Block Cipher (Blowfish). Fast Software Encryption, Cambridge Security Workshop Proceedings. Springer-Verlag, 191–204, (1993).
5. J. Daemen, V. Rijmen, *Springer*, (2002).
6. F. Özkaynak, *Nonlinear Dynamics*, **92** (2), 305-313, (2018).
7. S. Pal, A. Mahanty, A. Pathak, J. Karmakar, H. Mondal, and M. Mandal, *ECTI Transactions on Computer and Information Technology (ECTI-CIT)*, **17** (1), 105-116, (2023).
8. M. Kar, A. Kumar, D. Nandi, and M.K. Mandal, *IETE Technical Review*, **37** (2), 12-23, (2020).
9. B. Idrees, S. Zafar, T. Rashid and W. Gao, *Multimedia Tools and Applications*, **79**(9), 6135-6162, (2020).
10. X. Zhang, Z. Zhou, and Y. Niu, *IEEE Photonics Journal*, **10**, 3901014, (2018).
11. R. Han, *Wireless Communications and Mobile Computing*, 2022.
12. A.H. Brahim, A.A. Pacha, and N.H. Said, *Information Security Journal: A Global Perspective*, 1-17, (2021).
13. W.J. Jun, and T.S. Fun, *IEEE Access*, **9**, 120596-120612, (2021).
14. K. Guan, Important notes on lyapunov exponents, arXiv preprint arXiv:1401.3315, (2014).
15. H. Lin, C. Wang, L. Cui, et al., *Nonlinear Dynamics*, **110**, 841–855, (2022).
16. D. Xu, G. Li, W. Xu, C. Wei, *Ain Shams Engineering Journal*, **14**(3),(2023).
17. J. Karmakar, D. Nandi, and M.K. Mandal, *Multimedia Tools and Applications*, **79**(37), 28277-28300, (2020).
18. M. Elad, *Springer.* **2**(1), 1094-1097, (2010).
19. M. Rabbani, *Journal of Electronic Imaging*, **11**(2), (2002).
20. R.N. Kumar, B,N. Jagadale, J.S. Bhat, *SN Appl. Sci.* **1**, 266, (2019).
21. H. Mondal, A. Pathak, T. Banerjee and M.K. Mandal, *ECTI Transactions on Electrical Engineering, Electronics, and Communications*, **21**(1), 248668-248668, (2023).