iJRASET
International Journal For Research in
Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH
IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 6 Issue: II Month of publication: February 2018

DOI: http://doi.org/10.22214/ijraset.2018.2059

A Comparative Study of ICA Arnold Catmap with Hybridization of ICA based Arnold Catmap using Reversible Cellular Automata

Sanjeev Sharma[1], Navleen kaur[2]
[1, 2] Department of Computer Science & Engineering, ACET, Amritsar, Punjab

Abstract: Image encryption has important role to assure all transmission of image over internet. Security of the multimedia data including image and video is one of the basic requirements for the telecommunications and computer networks. Cellular autoats is based on modifying the mixing matrix in Independent Component Analysis (ICA) using the chaotic Arnold's Cat Map (ACM) for encryption. This research implies that hybridized ICA and ACM has the better results but it can be improved further by utilizing optimistic decision making. This paper put a light on The research of image cryptography based on independent component analysis based arnold cat cryptography still has many problems, but independent component analysis based arnold cat cryptography have many advantages as compared to other encryption algorithms because of the vast parallelism, exceptional energy efficiency, and extra information density inherent in independent component analysis based arnold cat map. We have improved the performance of independent component analysis based Arnold cat based image cryptography technique using reversible cellular automata. The primary objective is to improve the computational speed. To propose hybrid (ICA) based on Arnold cat-map with reversible cellular automata based image encryption technique, to improve the encryption speed further.

Keywords: Arnold cat map, cellular automata, independent component analysis (ICA)

I. INTRODUCTION

Images contribute a lot now a days many organization send their confidential data or images over internet but to get image at receiver end security was the main problem was that how one can transfer important images on internet without any attack of intruder or hacker so to solve this problem [1]. We are having many encryption techniques given by various scientist and researchers to provide security to various organization and individuals so that they can transfer any confidential data over internet without with ease [2].

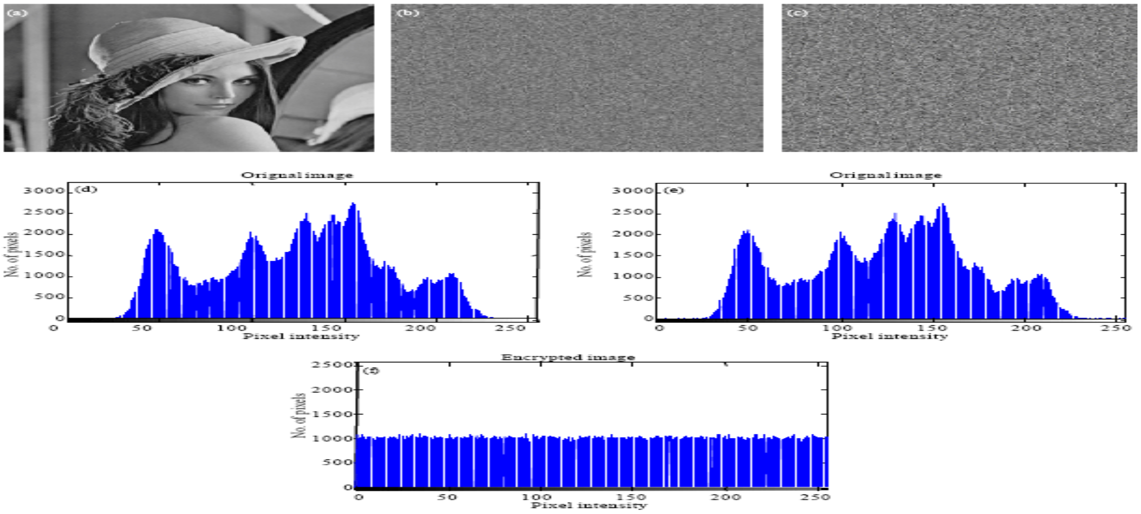


Fig.1 An illumination of Image Encryption and Decryption

Photo to be adviser multimedia will be playing a strong progressively natural part, since it is protection is necessary in various programs, like equally private and public companies including professional medical image solutions, discreet video clip conferencing, military picture directories, on-line personalize image , satellite television info program etc. [3]. Shield of encryption is an efficient technique to keep the information formula through rearranging details in to a different form [4]. we have so many image encryption algorithm or various techniques to perform an efficient image encryption but only some have concentrated over the security of the important documents such as many of documents of it companies having lots of confidential data to be transmitted over the internet but due to confidentiality issue we need a securer way to communicate or we can say we need a reliable technique [5]. We can transfer our important documents without any tension. So in this paper we have discussed some techniques below [6]

II. ARNOLD'S CAT MAP (ACM)

Arnold's change infers that a picture is hit with the change that will clearly randomizes the first association of its pixels. if iterated enough no of times, eventually the first picture reappears.[7] The quantity of considered cycles is known as the Arnold's time frame. The period relies upon the picture measure; i.e., for various size pictures, Arnold's period is unique.

Where size of image is denoted by N, p,q are positive integer and det(A)=1, (Xn,Yn) is the positions of the sample in N data such that And (x_{n+1}, y_{n+1}) is the transformed position after cat map, Cat map has two typical factors, which bring chaotic movement: tension(multiply matrix in order to enlarge x, y) and fold (taking mod in order to bring x, y in unit matrix).[9]

$$\begin{bmatrix} X_n + 1 \\ y_n + 1 \end{bmatrix} = A \begin{bmatrix} X_n \\ y_n \end{bmatrix} (modN) \begin{bmatrix} 1p \\ qpq + 1 \end{bmatrix} \begin{bmatrix} X_n \\ y_n \end{bmatrix} (modN) \dots (1)$$

Equation.1 changes all the positions of the pixels, when all the pixels are shuffled. The image we get is scrambled image .the no of iteration depends upon the size of the image i.e. no of iterations= Arnold period secret key [10]

A. Arnold's Cat Map (ACM) algorithm

```
1) Input any arbitrary image
2) Use num as variable which is represented the No. of
3) Determine the No. of rows and columns. Which are represented by the variables row and col      respectively.
4) for inc=1 to num
   for row1= 1 to row
   for col1= 1 to col
   nrowp=row1
   ncolp=col1
   forite =1 to inc
5) Shuffle the positions of the pixels of the image using Eq. (1)
   end
      Result the new encryption image
   end
   end
   end
```

III.INDEPENDENT COMPONENT ANALYSIS (ICA)

ICA describes a generative model for viewed multivariate data, which ordinarily is capable of finding the underlying factors In this model, data variable are believed to be immediate or nonlinear.ICA always looks for component that are statistically independent and non guassian [11].ICA always find principal component which is dissimilar from other components present

$$\begin{bmatrix} S_1(t) \\ \vdots \\ S_n(t) \end{bmatrix} = \tilde{S} \boxed{A} \rightarrow x(t) \rightarrow \boxed{B} \rightarrow y(t) = \begin{bmatrix} y_1(t) \\ \vdots \\ y_n(t) \end{bmatrix} \tilde{S}(t) \dots . (2)$$

$$x(t) = AS(t) \dots \dots . (2)$$

Where $s(t) = [s_1(t), \dots, (t)]^T$ is a $m \times 1$ column vectr Collecting the source images, similarly vector $x(t)$ collects then observed signals, A is a $n \times m$ matrix of unknown mixing Coefficients, $n \geq m$ and t is the time index.

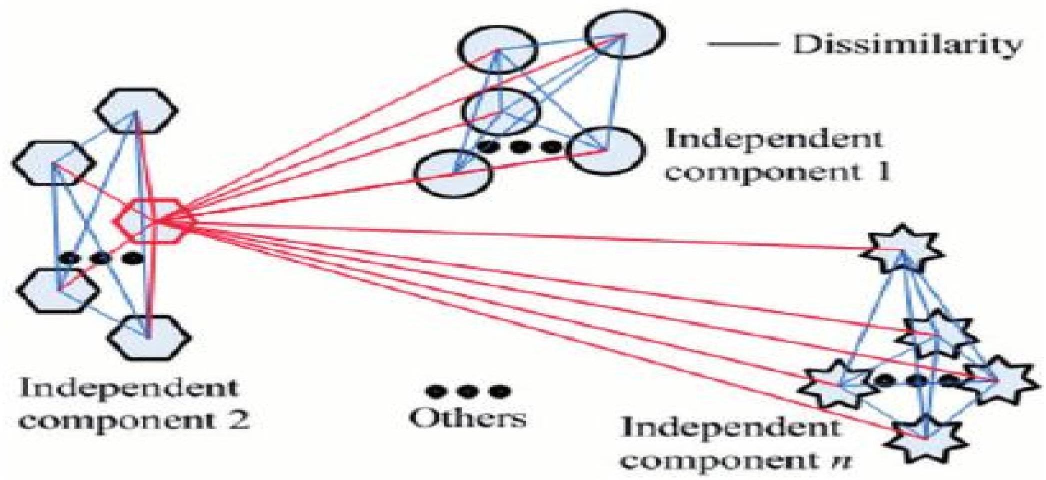


Fig. 2 shows the principal component from independent components

A. Applications Of Ica

1) Speech enhancement
2) Image process in
3) BSS (blind source separation
4) Biomedical signal processing

IV. REVERSIBLE CELLULAR AUTOMATA

Reversible cellular automata are automata in which each arrangement has a novel ancestor. It is a normal lattice having cells, each having a state drawn from a limited arrangement of states, with administer for changing all cells at the same time in view of the neighbor.[12] To such an extent that the past condition of any cell before a refresh can be resolved interestingly from the adjusted conditions of the considerable number of cells. Numerous strategies are known for characterizing cell automata decides that are reversible; these contain the square cell automata strategy, in which each refresh isolates the cells .. Furthermore, the second request cell automata technique.[13] In which the refresh administer contains states from two past strides of the automata.

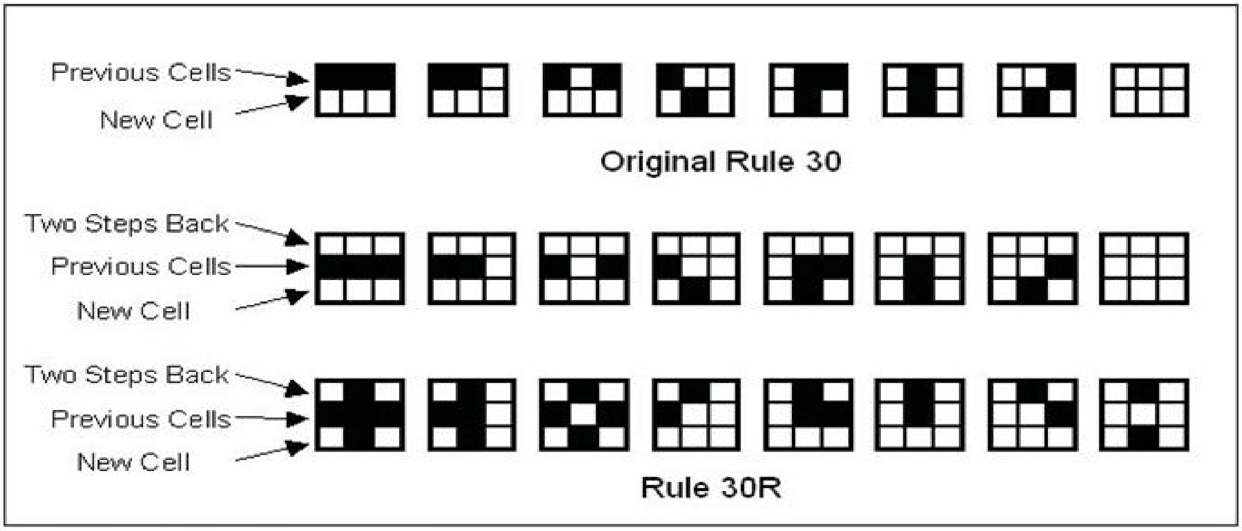
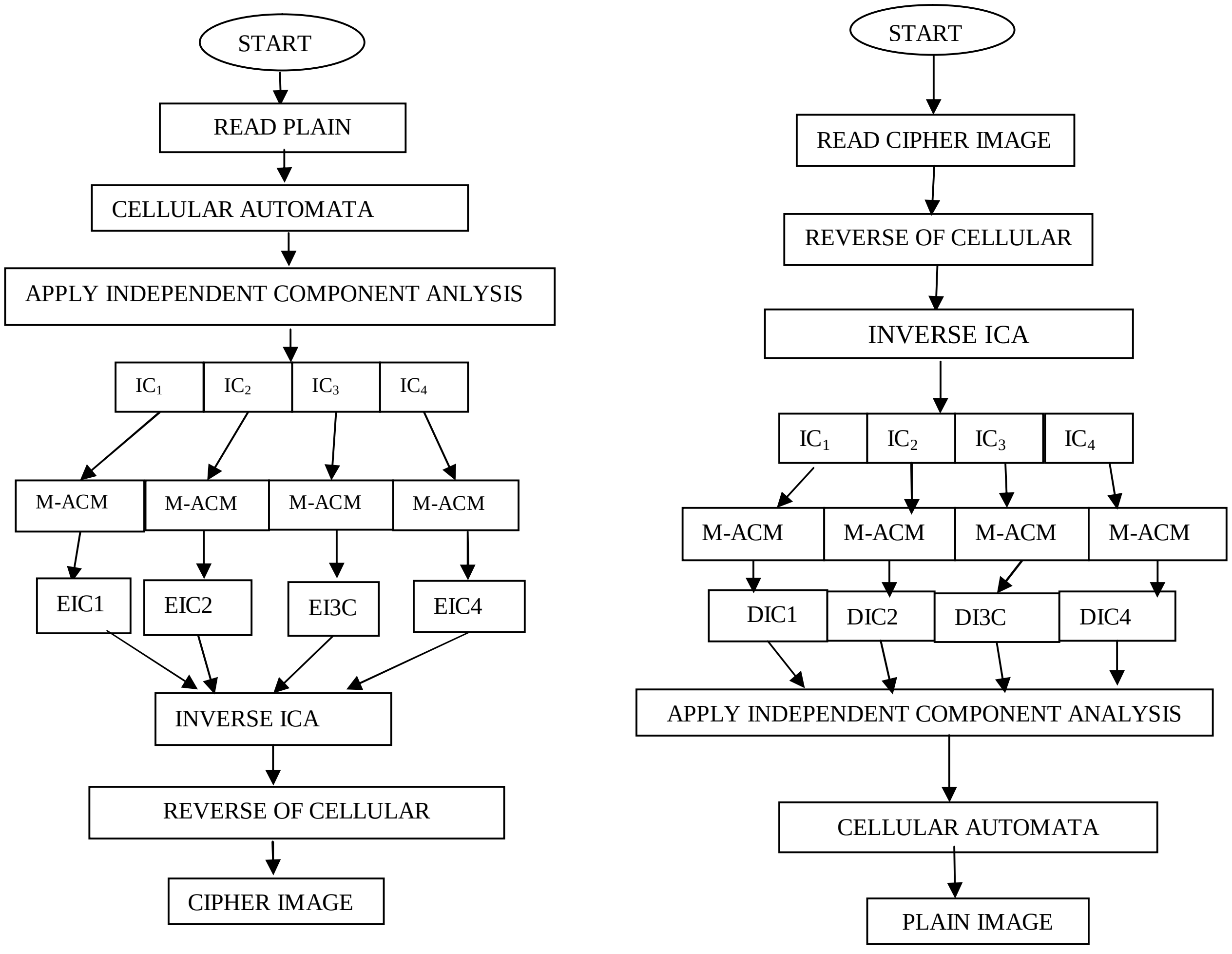


Fig. 3 shows the Reversible Cellular Automata

The Cellular Automata (CA) has fundamental highlights of the physical laws, for example, consistency and region. While most CA are not reversible without anyone else's inputs[14], we can program reversibility in CA so that we can observe the validity of the second law within CA. Cellular automata is reversible only if its global map is invertible that is for every state of automata the global map specifies only one successor. [15]. Cellular automata showing how each and every cell is covered during process of cellular automata.

V. METHODOLOGY

The flow chart of Image encryption and decryption as shown below:



(a) (b)

Fig. 4 shows the flowchart of image encryption and decryption.

VI. RESULT ANALYSIS AND DISCUSSION

For experimentation and implementation the proposed technique is evaluated using MATLAB tool. The evaluation of proposed technique is done on the origin of following parameters such as SDR, PSNR, Execution Time, Computational Speed based on different images. Fig (a)-(f) is indicating the quantized research into the SDR, PSNR, SSIM, Execution time, Computational Speed. As SDR value is less which implies proposed algorithm is indicating the superior results when compared to access methods as the noise is less in each case. As PSNR ought to be higher which implies proposed algorithm is indicating the superior results when compared to access methods as the PSNR is higher in each case. As SSIM ought to be higher which implies proposed algorithm is indicating the superior results when compared to access methods as the SSIM is higher in each case. As Execution time ought to be lower which implies proposed algorithm is indicating the superior results when compared to access methods as the Execution time is lower in each case.

As Computational Speed ought to be higher which implies proposed algorithm is indicating the superior results when compared to access methods as the Computational Speed is higher in each case.Also, quantitatively evaluations of proposed method with different images for image encryption are below. Fig 5-9 shoes the source images

A. Parameters

1) *SSIM:* Structural similarity index is a novel method for measuring the similarity between the two images. It is quality measure of one of the image compared, provided the other image is regarded as of perfect quality. SSIM gives much indication of image quality.
2) *Computational Speed*- This parameter is use to compare the speed of cryptography performed by existing technique compared to our purposed technique showing the difference between the speeds between both the techniques .it give results with respect to time. Lesser the time more will be the computational spee
3) *Execution Time*-It is performance measure parameter it calculates the time taken by the machine to perform a particular task for e.g. here execution time will measure the time taken by CPU in cryptography. So lesser the time taken by CPU better is the performance
4) *PSNR*- PSNR is commonly used to measure the quality of reconstruction of image compression codecs. The signal here is original image or data and the error is noise introduced by the compression. When comparing compression PSNR is approximation to human perception of reconstruction quality . generally higher the PSNR value higher is the quality

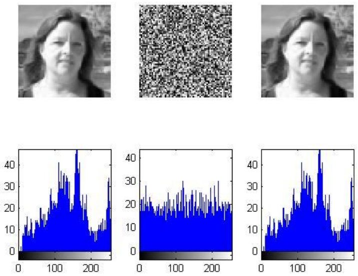


Fig.5

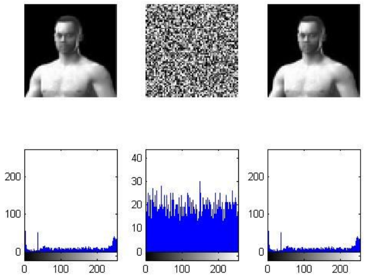


Fig.6

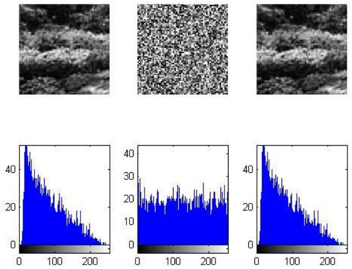


Fig.7

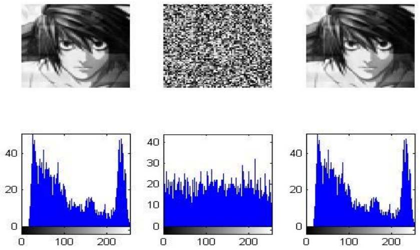


Fig.8

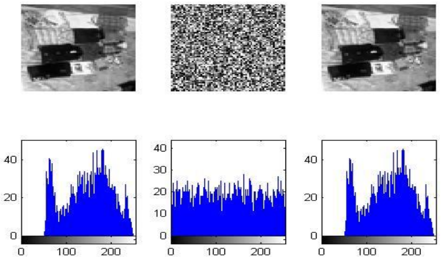


Fig.9

TABLE I :

IMAGE	EXISTING	PROPOSED
1.	62.403	70.8461
2.	63.251	71.2587
3.	50.1822	70.5785
4.	50.7396	70.5592
5.	51.7527	71.2192
6.	50.8307	70.315
7.	56.6228	71.1065
8.	64.3895	70.5458
9.	53.4554	70.8417
10.	60.0284	70.8184

TABLE III:

IMAGE	EXISTING	PROPOSED
1.	14.4525	12.5375
2.	15.6567	13.8451
3.	14.4977	12.5852
4.	15.2829	12.9111
5.	14.8752	12.5622
6.	14.6403	12.5381
7.	14.5732	12.6834
8.	14.5374	12.0647
9.	14.6221	12.6288
10.	14.5528	12.6313

TABLE IIIII:

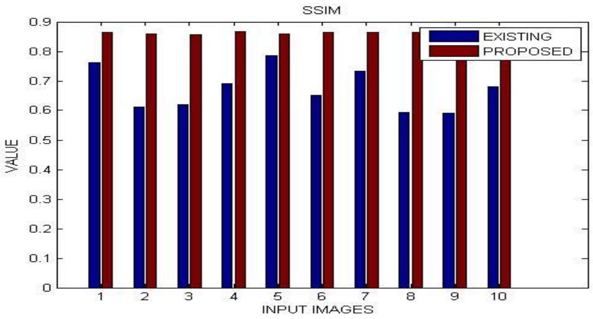
IMAGE	EXISTING	PROPOSED
1.	0.19337	0.073153
2.	0.19346	0.073287
3.	0.78964	0.075442
4.	0.74056	0.07561
5.	0.65903	0.070078
6.	0.73283	0.077766
7.	0.37618	0.070993
8.	0.15384	0.0575727
9.	0.54171	0.073191
10.	0.25417	0.073387

TABLE IVV:

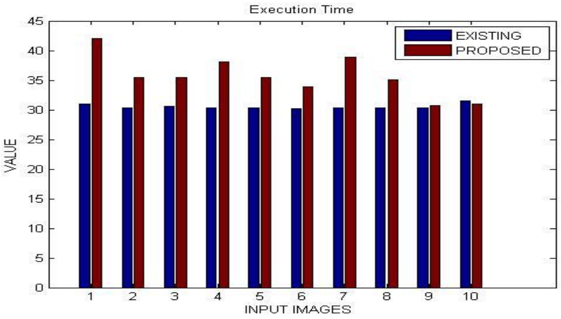
IMAGE	EXISTING	PROPOSED
1	0.76101	0.86398
2	0.76141	0.86394
3	0.61198	0.86071
4	0.61878	0.86048
5	0.63113	0.86853
6	0.61989	0.8575
7	0.69052	0.86715
8	0.78524	0.86031
9	0.6519	0.86392
10	0.73205	0.86364

TABLE V:

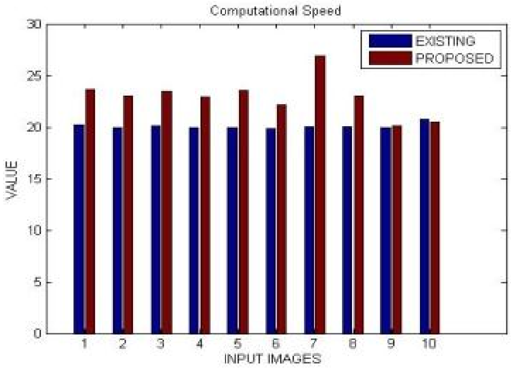
IMAGE	EXISTING	PROPOSED
1	10.2157	8.0385
2	11.2971	0.76101
3	10.2444	0.61198
4	10.9123	8.4359
5	10.5142	8.2165
6	10.3568	8.2104
7	10.2914	8.3465
8	10.2761	8.2187
9	10.317	8.2888
10	10.2937	8.2848



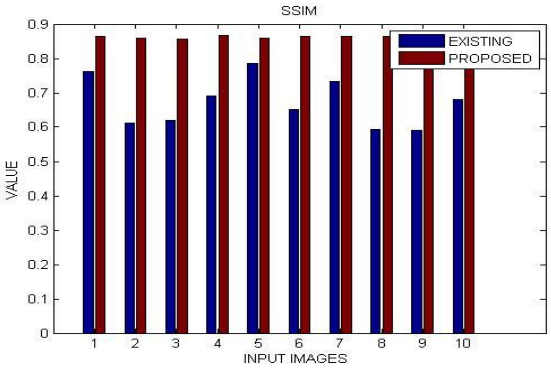
(a)



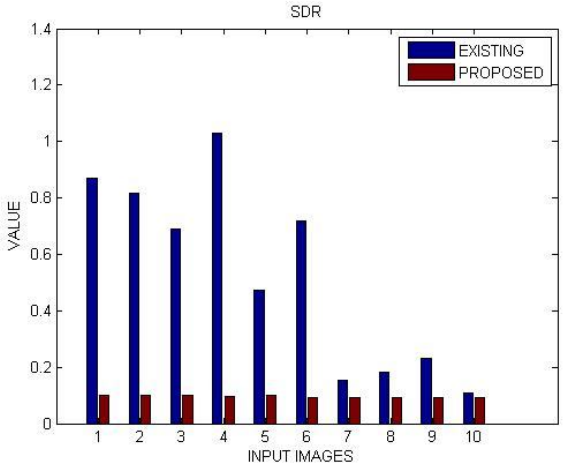
(b)



(d)



(e)



(f)

VII. CONCLUSIONS

In this research paper, we have analysed existing ‘Image encryption based on Independent Component Analysis and Arnold’s Cat Map’. The proposed ‘hybrid independent component analysis based on arnold cat-map and with reversible cellular automata based image encryption technique gives better results as the speed is increased This paper has shown comparison existing image encryption technique on the basis of parameters like SDR,PSNR, execution time and computational speed. This proposed image encryption technique shows better results as compared to existing technique. However, in this paper we have not considered the DNA based image encryption techniques to improve the results further. Therefore, in near future we will modify the proposed technique by using the DNA based image encryption techniques.

REFERENCES

[1] Ravishankar KC, Venkateshmurthy MG. Region based selective image encryption. In: International conference on computing & informatics, ICOCI ’06; 2006.
[2] GaoHaojiang, Zhang Yisheng, Liang Shuyun, Li Dequn. A newchaotic image encryption algorithm. Chaos SolitFract2006;29:393–9.
[3] Yu Hai, Zhu Zhiliang, Chen Guanrong. An efficient encryption algorithm based on image reconstruction. In: International workshop on chaos fractals theories and applications; 2009
[4] Kamali SH, Shakerian R, Hedayati M, Rahmani M. A new modified version of advanced encryption standard based algorithm for image encryption. In: 2010 International conference on electronics and information engineering (ICEIE 2010
[5] Paul AJ, Mythili P, Paulose Jacob K. Matrix based crypto-graphic procedure for efficient image encryption. In: Recent advances in intelligent computational systems conference (RAICS); 2011
[6] Gautam A, Panwar M, Gupta PR. A new image encryptionapproach using block based transformation algorithm. IJAEST2011;8(1):90–6
[7] Fei Xiang, Xiao-congGuo. An image encryption algorithm based on scrambling and substitution using hybrid chaotic systems. In: Seventh international conference on computational intelligence and security; 2011. p. 882–5.
[8] Ye Ruisong, Zhao Haiying. An efficient chaos-based imageencryption scheme using affine modular maps. Int J ComputNetwork Inform Security (IJCNIS) 2012;4(7):41–50.
[9] Liu Rui, Tian Xiaoping. New algorithm for color image encryp-tion using chaotic map and spatial bit level permutation. J TheorAppl Inform Technol 2012;43(1):89–93
[10] PradhanChittaranjan, SaxenaVilakshan, Bisoi Ajay Kumar.Imperceptible watermarking technique using Arnold’s transformand cross chaos map in DCT domain. Int J ComputAppl 2012;55(15)
[11] Ashtiyani M, MoradiBirgani P, KarimiMadahi SS. Speech signalencryption using chaotic symmetric cryptography. J BasiApplSci Res 2012;2(2):1678–84
[12] Hyvarinen A, Oja E. Independent component analysis: algorithmsand applications. Neural Networks 2000;13:411–30
[13] Comon P, Jutten C. Handbook of blind source separationindependent component analysis and applications. AcademicPress is an imprint of Elsevier; 2010.
[14] Cardoso JF. Blind signal separation: statistical principles. ProcIEEE 1998;86(10):2009–25
[15] Cardoso JF, Souloumiac A. Blind beamforming for non Gaussiansignals. IEEE Proc F 1993;140(6):362–70
[16] Dong Tianbao, Lei Yingke, Yang Jingshu. An algorithm forunderdetermined mixing matrix estimation. Neurocomputing2012:1–9 (Elsevier)
[17] Virtanen Tuomas, GemmekeJort F, Raj Bhiksha. Active-setnewton algorithm for overcomplete non-negative representationsof audio. IEEE Trans Audio Speech Lang Process 2013;21(11):2277–89
[18] Wang Zhou, Bovik Alan C, Sheikh Hamid R, SimoncelliEero P.Image quality assessment: from error visibility to structuralsimilarity. IEEE Trans Image Process 2004;13(4).