Defence Science Journal, Vol. 69, No. 3, May 2019, pp. 259-265, DOI : 10.14429/dsj.69.14422

Cellular Automata with Synthetic Image – A Secure Image Communication with Transform Domain

R. Sundararaman[@,*], H.N. Upadhyay[@], A. Sridevi[@], R. Sivaraman[@], V. Anand[#], T. Srinivasan[#], and S. Savithri[#]

[@]*SASTRA Deemed University, Thanjavur - 613 401, India*
[#]*DRDO-Combat Vehicles Research and Development Establishment, Chennai - 600 054, India*
[*]*E-mail: raman@ece.sastra.edu*

ABSTRACT

Image encryption has attained a great attention due to the necessity to safeguard confidential images. Digital documents, site images, battlefield photographs, etc. need a secure approach for sharing in an open channel. Hardware – software co-design is a better option for exploiting unique features to cipher the confidential images. Cellular automata (CA) and synthetic image influenced transform domain approach for image encryption is proposed in this paper. The digital image is initially divided into four subsections by applying integer wavelet transform. Confusion is accomplished on low – low section of the transformed image using CA rules 90 and 150. The first level of diffusion with consecutive XORing operation of image pixels is initiated by CA rule 42. A synthetic random key image is developed by extracting true random bits generated by Cyclone V field programmable gate array 5CSEMA5F31C6. This random image plays an important role in second level of diffusion. The proposed confusion and two level diffusion assisted image encryption approach has been validated through the entropy, correlation, histogram, number of pixels change rate, unified average change intensity, contrast and encryption quality analyses.

Keywords: Image encryption; Confusion; Diffusion; Cellular automata; IWT; Synthetic image; Field Programmable Gate Array

1. INTRODUCTION

With the accelerated development of new technologies, information formats such as images, audio and video are shared over the cloud or Internet in a large scale. These forms are vulnerable to unauthorised access and attacks as this digital information have become openly accessible over the network. Hence, there arises a need for encryption techniques to address the security of communication. The traditional advanced encryption standard (AES) or data encryption standard (DES) algorithms are not convenient algorithms for image encryption because of the unique characteristics of images such as bulk capacity and redundancy[1]. Owing to these factors, image encryption process is being performed using chaos based maps and attractors. Chaos has several advantages namely ergodicity, randomness, highly sensitive to initial conditions, etc[2]. However, key space varies according to the variables and control parameters. Deoxyribonucleic acid (DNA) coding also plays a significant role over image encryption but it is likely prone to chosen plaintext attacks[3]. CA looks to be a good candidate for encrypting images due to the presence of large key space, rules and their ability to model complex systems[4].

The 1D CA contains array of interconnected cells, the status of which depend on previous, present and next cells. In CA, rules are the controlling elements which fix the characteristics and operations. Rules can be formed by computing logical function(s) among the neighbouring cells. For a 8 bit CA, total of 2^8 1D CA rules are possible[5]. An image encryption scheme based on hyper chaos and CA is proposed in[6]. The confusion step involves changing the position of the original image according to the hyperchaos and the synthetic image is created using the non-uniform CA which is used for diffusing the pixels of the confused image. A CA employing a quantum 1D CA could be accomplished by delicately building the evolution rules[7]. Most widely used CA rules are Rule 90, Rule 150 and Rule 42[8-10]. An image encryption approach using elementary CA in which state transition diagram shows that some rules behave as an attractor to confuse the pixel positions of an image is recommended[11]. Image confusion using intertwining logistic map and diffusion using reversible CA (RCA) is suggested[14]. A digital scrambling according to four classes of behaviours proposed by wolfram such as ordered behaviour, periodic behaviour, random or chaotic behaviour and complex behaviour is proposed[15]. This CA is most widely used for diffusion operation and confusion process has been carried out with logistic map and chaos memory combinations[16-18]. Considering the earlier works, the proposed work combines CA and IWT in an attempt to study the efficiency with chaotic maps or attractors.

Main contributions of the proposed work are:

(i) Dual confusion using the CA Rule 90 and 150 with two

Received : 31 August 2018, Revised : 07 March 2019
Accepted : 14 March 2019, Online published : 30 April 2019

different seeds has been carried out in IWT domain
(ii) First level of diffusion using the CA Attractor 42
(iii) Second level of diffusion using the FPGA generated random synthetic image
(iv) Hardware - software co-design resulting in large keyspace which provides resistance against brute force attacks.

2. PROPOSED METHODOLOGY

The proposed scheme consists of confusion and diffusion units. Confusion process is carried out in transform domain and diffusion is performed in spatial domain. The overall functional block diagram of the proposed Image Encryption algorithm is depicted in Fig. 1(a).

The following steps are carried out during image encryption:

***Step 1*:** Divide the original RGB image of size M×N into Red, Green and Blue planes of size M×N.

Step 2: Decompose each plane into its sub-bands (LL, LH, HL, HH) each of size M/2 × N/2 using IWT

***Step 3*:** Generate the pseudo random number sequence $S = (S_1, S_2 \ldots S_{M/2\times N/2})$ through cellular automata CA Rules 90 and 150 with initial seed S_0 = E7D53FF0F012FFFFE7D53FF0 F00FEBFFF. Perform sorting in ascending order on the pseudo random sequence S as follows:

$$[I_S,\ Y_S] = \text{sort}\ (S) \qquad (1)$$

where $[\bullet,\bullet]$ = sort $(\bullet)$ is the sequence indexing function; I_S is the new index after sorting the data S and Y_S is the sorted sequence after sorting S.

Step 4: Perform first level of confusion on the pixels of LL subband of each plane LL ((M/2 × N/2)) in the following form:

$$Ca1(i) \Leftarrow LL(I_s(i)), \qquad where\ 1 \le i \le \left(\frac{M}{2}\times\frac{N}{2}\right) \qquad (2)$$

Step 5: Generate the pseudo random number sequence $P = (P_1, P_2 \ldots\ldots\ldots P_{M/2\times N/2})$ through CA rules 90 and 150 with initial seed P_0 = 67553CF0F192F9FEE7D53EF8F0CF6BE7. Perform sorting in descending order on the pseudo random sequence P as follows:

$$[J_S, Z_S] = \text{sort}\ (P) \qquad (3)$$

where $[\bullet,\bullet]$ = sort $(\bullet)$ is the sequence indexing function; J_S is the new index and Z_S is the sorted sequence. Perform second level of confusion on the pixels of confused LL subband Ca1 of each plane $Ca1$ (($M/2 \times N/2$)) in the following form:

$$Ca2(i) \Leftarrow Ca1(J_s(i)), \qquad where\ 1 \le i \le \left(\frac{M}{2}\times\frac{N}{2}\right) \qquad (4)$$

Step 6: Perform inverse IWT over the subbands LL, LH, HL, HH of each plane to produce the duo confused images DCI_{Red}, DCI_{Green}, DCI_{Blue}. The diagrammatic representation of the confusion procedure is illustrated in as Fig. 1(b).

Step 7: Generate pseudo random sequence $R = (R_1, R_2 \ldots\ldots R_{M\times N})$ using the CA 42 attractor with initial seed R_0=00110101. These generated bits are reshaped into the matrix R of size $M\times N$. The duo confused images of each plane is diffused using Eqns. (5). The same procedure is repeated for all the three plane.

$$D1_{red} = (DCI_{red})\ \text{XOR}\ (R) \qquad (5)$$

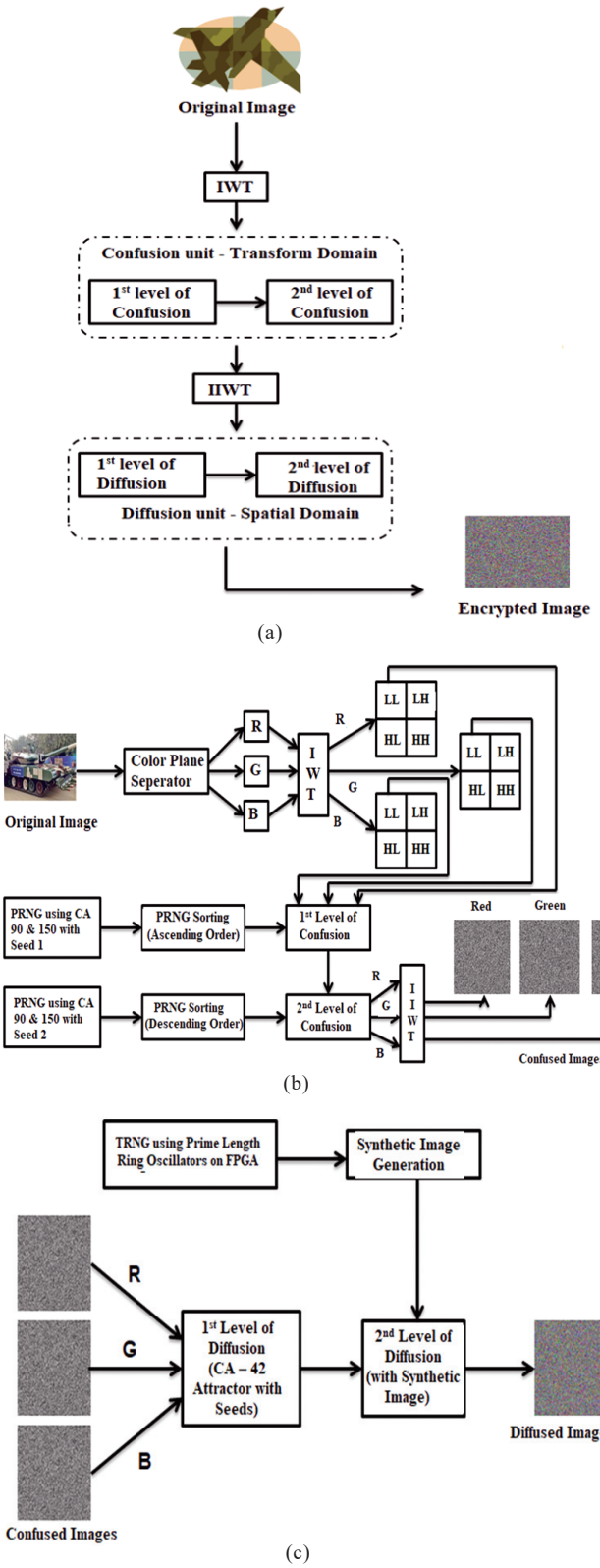


Figure 1. (a) Overall functional diagram of the proposed method, (b) Confusion procedure, and (c) Diffusion procedure.

Step 8: Generate True random number sequences of length $Q = (Q_1, Q_2, \ldots Q_{M\times N})$ using the prime length ring oscillators designed on Cyclone V FPGA using four rings with 13, 17, 23 and 31 inverters, respectively. Reshape these random numbers

into the synthetic image of size M × N.

***Step* 8.1:** Diffuse the synthetic image and image obtained from Step 7 according to the equation (6).

$$(D1_{red}) \text{ XOR } (Q) = DDI_{red} \quad (6)$$

***Step* 8.2:** Execute the same for all the planes to obtain DDI_{green} and DDI_{blue}.

***Step* 8.3:** Combine these dual confused and diffused planes to form the encrypted image E. The schematic representation of the diffusion procedure is given in Fig. 1(c).

3. RESULTS AND DISCUSSION

In order to validate the strength of obtained cipher images, differential, histogram, entropy, correlation and key sensitivity analyses have been performed. Two military tank images of size 128×128 and two USC-SIPI database images of size 256×256 were considered for analyses which are as shown in Figs. 2(a)-2(d). The corresponding encrypted images are also shown in Figs. 3(a)-3(d). The algorithm and analyses were carried out using MATLAB R2016b platform on a system with 4 GB RAM, 1 TB hard disk and an Intel Core i5, windows 10 OS.

3.1 Correlation analysis

Correlation between the pixels is an important feature which has a considerable value in the original images and near zero value in the case of encrypted images. To test the correlation, 4000 pair of adjacent pixels were considered and the correlation along horizontal, vertical, diagonal directions were determined using the Eqns. (7)-(10). The correlation coefficients of the four test images have been presented in Table 1. The values are very low showing the strength of encryption.

$$E(a) = \frac{1}{N}\sum_{i=1}^{N} a_i \quad (7)$$

$$D(a) = \frac{1}{N}\sum_{i=1}^{N} (a_i - E(a))^2 \quad (8)$$

$$Cov(a,b) = \frac{1}{N}\sum_{i=1}^{N} (a_i - E(a))(b_i - E(b)) \quad (9)$$

$$\gamma_{ab} = \frac{Cov(a,b)}{\sqrt{D(a)}\sqrt{D(b)}} \quad (10)$$

where a and b represent the two adjacent pixels values of the encrypted image. Cov(a, b), E(a) and D(a) are the covariance, expectation and variance of the variable a, respectively. Figures 4(a)-4(c) and Fig. 4(d)-4(f) show the horizontal, vertical and diagonal correlation coefficients of the original and encrypted Arjun tank image, respectively.

3.2 Histogram Analysis

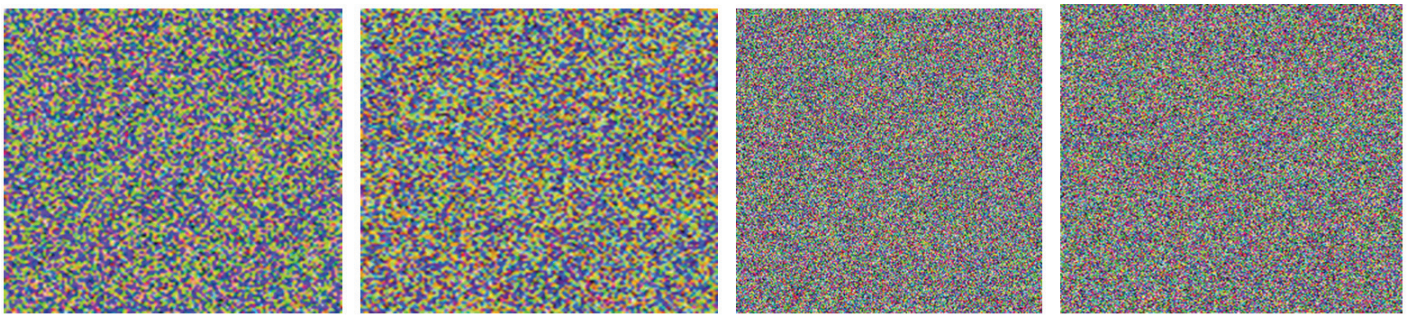
Histogram represents the visual distribution of pixels in an image. Figures 5(a)-5(c) show the histograms of the original arjuntank image of red, green and blue planes and Figs. 5(d)-5(f) show the corresponding histograms of the encrypted arjuntank image. From the Figs. 5(d)-5(f), it can be inferred that the image pixels have been evenly distributed in each plane. This proves the randomness of the cipher image to resist statistical attack.

3.3 Entropy Analysis

Entropy is an important feature which provides the probability of distribution of the gray levels in an image. For an encrypted grayscale image, this value must be close to 8 which represents the best level of uncertainity. Entropy can be expressed as,

(a) (b) (c) (d)

Figure 2. Original images : (a) Varunastra, (b) Arjun tank, (c) Airplane, and (d) Peppers.



(a) (b) (c) (d)

Figure 3. Encrypted images : (a) Varunasastra, (b) Arjun tank, (c) Airplane, and (d) Peppers.

Table 1. Horizontal, vertical and diagonal correlation coefficients

Images		Plane	H	V	D
Varunastra	Original	Red	0.9620	0.9704	0.9416
		Green	0.9382	0.9461	0.9047
		Blue	0.9497	0.9579	0.9232
	Encrypted	Red	0.0021	-0.0076	-0.0056
		Green	0.0102	-0.0012	-0.0124
		Blue	0.0057	0.0031	0.0039
Arjuntank	Original	Red	0.9026	0.8692	0.8143
		Green	0.9034	0.8641	0.8124
		Blue	0.8949	0.8458	0.7927
	Encrypted	Red	-0.0033	0.0014	-0.0200
		Green	0.0106	-0.0083	0.0036
		Blue	-0.0018	0.0013	-0.0024
Peppers	Original	Red	0.9712	0.9849	0.9578
		Green	0.9455	0.9788	0.9268
		Blue	0.9402	0.9713	0.9150
	Encrypted	Red	-0.0052	0.0046	0.0037
		Green	0.0024	0.0019	-0.0002
		Blue	0.0024	-0.0026	0.0020
Airplane	Original	Red	0.9055	0.8869	0.8252
		Green	0.8923	0.8961	0.8309
		Blue	0.9088	0.8574	0.8215
	Encrypted	Red	0.0024	0.0008	-0.0033
		Green	0.0014	0.0012	0.0007
		Blue	-0.0019	-0.0058	-0.0013

H – Horizontal, V – Vertical, D – Diagonal

$$H = -\sum_{i=1}^{N} P(x_i)\log_2 P(x_i) \tag{11}$$

where $P(x_i)$ is probability of the symbol x_i. Table 2 provides the entropies of the test images in each plane.

Table 2. Entropy analysis

Images	Entropy	Red	Green	Blue
Varunastra	Original	7.4205	7.6718	7.6326
	Encrypted	7.9874	7.9860	7.9864
Arjuntank	Original	7.7832	7.7475	7.5992
	Encrypted	7.9866	7.9862	7.9866
Airplane	Original	6.7780	6.8795	6.2680
	Encrypted	7.9970	7.9970	7.9969
Peppers	Original	7.1681	7.0215	6.8049
	Encrypted	7.9970	7.9971	7.9972
Ref.[12]	Encrypted	-	-	7.9717
Ref.[13]	Encrypted	-	-	7.9700

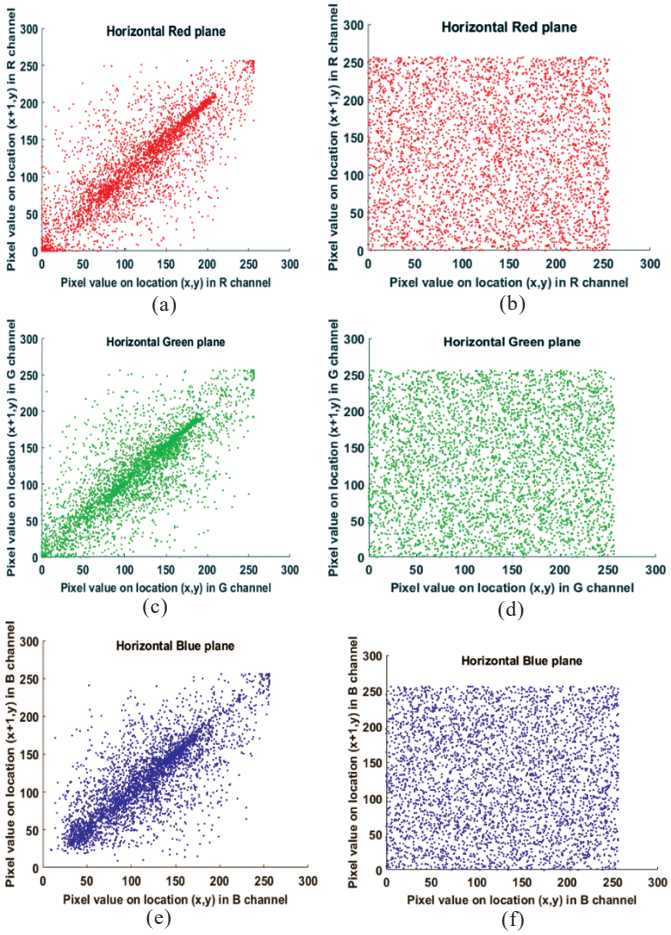


Figure 4. Correlation of Arjuntank: (a - c) Original horizontal correlation of red, green, blue planes; (d-f) Encrypted horizontal correlation of red, green, blue planes.

The obtained entropies of encrypted images are above 7.9 thus showing the uniformity of intensity values throughout the encrypted images. The average entropy of the algorithm proposed in this work for red, green and blue planes of the considered test images are 7.9920, 7.9915, 7.9911, respectively, which are higher than the entropy of test images of algorithms proposed[12,13].

3.4 Differential Analysis

Number of pixels change rate (NPCR) and unified average change intensity (UACI) evaluate the sensitivity of the proposed encryption algorithm to produce completely different cipher images even for a tiny change in original image[19]. It can be estimated using Eqns. (12)-(14).

$$NPCR = \frac{\sum_{k=1}^{H\times W} B_k(pixel\,value(i,j))}{R \times C} \times 100\% \tag{12}$$

$$UACI = \frac{\sum_{k=1}^{H\times W} |C1(i,j) - C2(i,j)|}{R \times C \times 255} \times 100\% \tag{13}$$

$$B_k\ (pixel\,value(i,j)) = \begin{cases} 0, & if\ C1\ (i,j) = C2\ (i,j) \\ 1, & otherwise \end{cases} \tag{14}$$

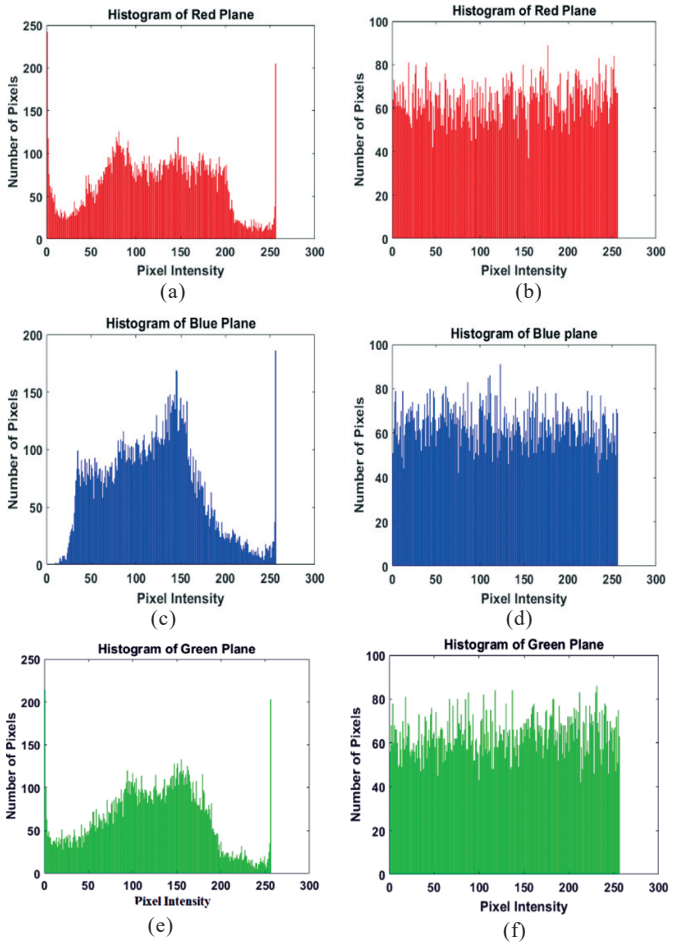


Figure 5. Histogram of Arjun tank: Original (a)-(c) red, green, blue planes; Encrypted (d)-(f) red, green, blue planes.

where R and C are row and column of the image. $C1$ and $C2$ are the encrypted images. NPCR and UACI values of the taken test images are depicted in Table 3 which are good values.

Table 3. Differential analysis

Images	Plane	NPCR	UACI
Varunastra	Red	99.6521	37.1472
	Green	99.5972	34.6690
	Blue	99.5667	33.5870
Arjuntank	Red	99.6033	31.1643
	Green	99.5544	30.3690
	Blue	99.5911	29.4197
Peppers	Red	99.6307	32.0231
	Green	99.6002	34.7858
	Blue	99.6628	35.3778
Ref.[12]	-	99.5643	33.5724
Airplane	Red	99.6277	31.9226
	Green	99.6124	32.7550
	Blue	99.6338	33.1808

3.5 Encryption Quality Analysis

Visual inspection of the images is also an important parameter to evaluate the efficiency of the algorithm. Three parameter have been considered for this quality analysis. They are maximum deviation (MaxD), irregular deviation (IDev) and deviation from uniform histogram (DHist) which were calculated using the Eqns. (15)-(17). The findings of this analysis are presented in Table 4.

$$MaxD = \frac{D_1 + D_{N-1}}{2} + \sum_{i=1}^{N-2} D_i \tag{15}$$

$$IDev = \sum_{i=0}^{N-1} H_{Di} \tag{16}$$

$$DHist = \frac{\sum_{Ci=0}^{255} |H_{ci} - H_c|}{M \times N} \tag{17}$$

Table 4. Encryption quality analysis

Images	Plane	MaxD	DHist	IDev
Varunastra	Red	9104	0.4858	10922
	Green	9108	0.4869	11182
	Blue	8897	0.5173	11204
Arjuntank	Red	7408	0.5138	10035
	Green	7941	0.5121	9885
	Blue	9690	0.4878	9617
Airplane	Red	67492	0.0493	20686
	Green	66329	0.0514	20029
	Blue	78919	0.0524	17726
Peppers	Red	46096	0.0516	34528
	Green	54948	0.0508	47930
	Blue	69646	0.0511	50160

3.6 Contrast Analysis

Contrast of the encrypted image[20] is analysed and from the obtained results, it was inferred that the images have uniform contrast after encryption. Table 5 depicts the values of contrast of the original and encrypted images.

Table 5. Contrast analysis

Images	Contrast	R	G	B
Varunastra	Original	1.8745	1.6555	1.5502
	Encrypted	10.4305	10.5069	10.5174
Arjun tank	Original	2.6989	2.4890	2.1077
	Encrypted	10.5266	10.4227	10.2981
Airplane	Original	1.3843	1.7453	0.6565
	Encrypted	10.4475	10.4667	10.4905
Peppers	Original	0.8443	0.7843	0.6340
	Encrypted	10.5021	10.5308	10.5361

3.7 Keyspace Analysis

Keyspace analysis is performed to understand whether the number of keys used in the proposed algorithm are sufficient

to resist brute force attacks. The secret keys used in this work include that of CA 90, CA 150, CA 42 and synthetic image generation using prime length of ROs on FPGA. For encrypting a M×N RGB image, the total keyspace of the proposed algorithm is $2^{16} \times 8^{(65536)\times 3} \times (\Delta T \times NI)$ where ΔT represents the delay in ROs and NI stands for the number of inverters used. It can be justified that the proposed algorithm is computationally large enough to resist the brute force attack with this large keyspace.

4. CONCLUSIONS

An RGB image encryption scheme using both software and hardware has been proposed in this work. CA rules have been used in IWT for encryption stages. FPGA generated random synthetic image was utilised for diffusion stage which makes the algorithm strong to depend on a reconfigurable hardware during encryption. The various analyses performed have proved the efficiency of the proposed encryption algorithm. Future work will be on implementation of the proposed algorithm along with chaotic maps as a whole on FPGA platform.

REFERENCES

1. Daemen, J. & Rijmen, V. The design of Rijndael, Information Security and Cryptography, Springer, 2002.
2. Somasundaram, K. & Kalavathi, P. Medical image binarization using square wave representation. Communications in Computer and Information Sciences, (CCIS) Book series, 2011, **140**, 312. doi: 10.1007/978-3-642-19263-0_19
3. Chai, X.; Chen, Y. & Broyde, L. A novel chaos-based image encryption algorithm using DNA sequence operations. *Opt. Lasers Eng.,* 2017, **88**, pp. 197–213. doi: 10.1016/j.optlaseng.2016.08.009
4. Sarkar, P. A brief history of cellular automata. *ACM Comput. Surv.*, 2000*,* **32**(1), 80–107. doi: 10.1145/349194.349202
5. Nayak, D.R.; Patra, P.K. & Mahapatra, A. A survey on two dimensional cellular automata and its application in image processing. arXiv Prepr., 2014, 1–10.
6. Niyat, A. Yaghouti; Moattar, M.H. & Torshiz, M. Niazi. Color image encryption based on hybrid hyper-chaotic system and cellular automata. *Opt. Lasers Eng.,* 2017, **90**, 225–237. doi: 10.1016/j.optlaseng.2016.10.019
7. Yang, Y.; Tian, J.; Lei, H.; Zhou, Y. & Shi, W. Novel quantum image encryption using one-dimensional quantum cellular automata. *Inf. Sci. (Ny).*, 2016*,* **345**, 257–270. doi: 10.1016/j.ins.2016.01.078
8. Cellular Automata Rule 90. http://mathworld.wolfram.com/Rule90.html (Accessed on 16 March, 2019).
9. Cellular Automata Rule 150. http://mathworld.wolfram.com/Rule150.html (Accessed on 16 March, 2019).
10. A Property of the Rule 150 Elementary Cellular Automaton. https://arxiv.org/abs/1401.4779 (Accessed on 16 March, 2019).
11. Jin, J. An image encryption based on elementary cellular automata. *Opt. Lasers Eng.,* 2012*,* **50**(12), 1836–1843. doi: 10.1016/j.optlaseng.2012.06.002
12. Bakhshandeh, A. & Eslami, Z. An authenticated image encryption scheme based on chaotic maps and memory cellular automata. *Opt. Lasers Eng*., 2013, **51**(6), 665–673. doi: 10.1016/j.optlaseng.2013.01.001
13. Abdo, A.A.; Lian, S.; Ismail, I.A.; Amin, M. & Diab, H. A cryptosystem based on elementary cellular automata. *Commun. Nonlinear Sci. Numer. Simul.,* 2013, **18**(1), 136–147. doi: 10.1016/j.cnsns.2012.05.023
14. Wang, X. & Luan, D. A novel image encryption algorithm using chaos and reversible cellular automata. *Commun. Nonlinear Sci. Numer. Simul.,* 2013, **18**(11), 3075–3085. doi: 10.1016/j.cnsns.2013.04.008
15. Dalhoum, A.L. Abu; Madain, A. & Hiary, H. Digital image scrambling based on elementary cellular automata. *Multimed. Tools Appl*., 2016, **75**(24), 17019–17034. doi: 10.1007/s11042-015-2972-z
16. Hanis, S. & Amutha, R. Double image compression and encryption scheme using logistic mapped convolution and cellular automata. *Multimed. Tools Appl.*, 2017*,* **77**(6), 1–16.
17. Souyah, A. & Faraoun, K.M. An image encryption scheme combining chaos-memory cellular automata and weighted histogram. *Nonlinear Dyn.,* 2016, **86**(1), 639–653. doi: 10.1007/s11071-016-2912-0
18. Chai, X.; Chen, Y.; & Broyde, L. A novel chaos-based image encryption algorithm using DNA sequence operations. *Opt. Lasers Eng.,* 2017, **88**, 197–213. doi: 10.1016/j.optlaseng.2016.08.009
19. Wu, Y.; Noonan, J.P. & Agaian S. NPCR and UACI Randomness Tests for Image Encryption. *Cyber J: Multidiscip. J. Sci. Technol. J. Sel. Areas Telecomm.,* 2011, pp. 31 – 38.
20. Belazi, A.; El-Latif, A.A. Abd & Belghith, S. A novel image encryption scheme based on substitution-permutation network and chaos. *Signal Processing*, 2016, **128**, 155–170. doi: 10.1016/j.sigpro.2016.03.021

ACKNOWLEDGMENTS

The authors wish to thank Director, DRDO-Combat Vehicles Research and Development Establishment, Avadi for providing support to carry out this research work. Also, they express sincere thanks to SASTRA Deemed University for infrastructure support.

CONTRIBUTORS

Dr R. Sundararaman completed his BTech (Electronics & Instrumentation Engg.), MTech (Advanced Communication Systems) and PhD in the domain of Hardware Steganography in the years 2005, 2007 and 2015 respectively from SASTRA University, Thanjavur, India. He is currently working as a Senior Asst. Professor in the Dept. of ECE, School of EEE, SASTRA Deemed University. He has recently carried out a CVRDE, DRDO, Govt. of India funded project in the domain of Random Key Generation. Earlier, he was also a

Co-Principal Investigator in a SAG-DRDO, New Delhi funded project on Image Steganography. His research areas include FPGA based Random Key Generation, Hardware Security and Image Security.
In this work, he designed the image encryption algorithm and integrated the article structure.

Dr H.N. Upadhyay completed his master of science in Physics and his PhD in Electronics Engineering from IT-BHU, Varanasi, India. He is now working as Dean (Student Affairs) of SASTRA Deemed University, Thanjavur. His research interests include VLSI design, opto and microelectronics and medical electronics. He has published more than 50 research articles in peer reviewed journals. He has supervised 6 PhD Thesis.
In this work, he performed the verification of algorithm and proof correction of the article.

Ms A. Sridevi completed her BTech in Electronics & Communication Engg. and MTech in Communication & Networking in the years 2009 and 2015 respectively. She is currently pursuing her Ph.D. in the domain of Multimedia Information Security at SASTRA Deemed University, Thanjavur, India. Her research areas include information security, multimedia communication, neural networks and embedded system.
In this work, she performed the software simulation of the algorithm.

Mr R. Sivaraman completed his BTech (Electronics & Communication Engineering) in 2014 from SRC, SASTRA University, Kumbakonam and MTech in VLSI Design from SASTRA University, Thanjavur in 2016. He is currently working as a Teaching Assistant and pursuing PhD in the domain of Information Security in School of Electrical and Electronics Engineering, SASTRA Deemed University, Thanjavur, India. His research areas include information security, design of hardware peripherals and embedded system.
In this work, he performed security analyses and compiled the analyses part of the article.

Mr V. Anand received his BE in Electronics & Communication Engineering in 2012 from Thiagarajar College of Engineering, Madurai. From 2015 onwards, he was with Combat Vehicles Research and Development Est. (CVRDE), Chennai where his research interests include active protection systems, situational awareness systems, battlefield management systems, tactical communication and navigation systems for armoured fighting vehicles.
In this work, he has performed requirements engineering and performance validation.

Mr T. Srinivasan has received his BE in Electronics & Communication Engineering from Madras University and ME in Avionics from Anna University. From 2000 to 2013, he was with the Defence Research and Development Laboratory, Hyderabad where his specialisation include Navigation, Guidance, Control and Estimation, Flight Simulation, Monte-Carlo Studies and System Engineering of Air-to-Air missiles. He is currently with Combat Vehicles Research and Development Establishment and his research interests include active protection systems, situational awareness systems, battlefield management systems, tactical communication and navigation systems for armoured fighting vehicles.
In this work, he has performed requirements engineering and performance validation.

Ms S. Savithri completed her BE in Electronics & Communication Engg. and ME in Communication Systems in the years 1981 and 1989 respectively from College of Engineering, Guindy, Anna University, Chennai. She was with Combat Vehicles Research and Development Establishment from 1987 onwards. Her areas of interest include EMI/EMC validation, active protection systems, situational awareness systems, battlefield management systems, tactical communication and navigation systems for armoured fighting vehicles.
In this work, she has provided technical inputs and guidance for the overall work.