Journal of Theoretical and Applied Information Technology
15th March 2017. Vol.95. No 5

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

SIMPLE IMAGE ENCRYPTION FOR MOBILE PHONES

[1,2]MANAL ABDULLAH AL-SHMRANI, [1]ABDUL RAOUF KHAN
[1]Department of Computer Sciences, King Faisal University, Saudi Arabia
[2]Departmeny of Computer Sciences, Hafar Al-Batin University, Saudi Arabia
E-mail: [2]elaan2011@hotmail.com , [1]raoufkhan@kfu.edu.sa

ABSTRACT

People generally save pictures in mobile phones or transmit to one another using several mobile applications. However, privacy of such images and pictures are of some importance to many people. Generally, for common people the threat to the privacy of the pictures may be very low; however, people prefer to have a certain level of security. In this paper, a simple encryption technique, based on two-dimensional cellular automata has been proposed. The local neighborhood pixel values of an image are used as part of the encryption key to encrypt the image, based on certain cellular automata rules. The quality of encryption technique and Peak Signal to Noise Ratio has been calculated and reported in this paper. A hardware architecture has been proposed to implement the scheme in mobile phones.

Keywords: *Image Encryption, Cellular Automata, Two Dimensional CA, Mobile Phone security , Privacy*

1. INTRODUCTION

The images contain information that is often private; security thus becomes increasingly important in the storage and transmission of digital images. In order to guarantee security, we need to process the images and make the contents of the image unintelligible by encrypting them. There are several conventional encryption methods, which are often used to encrypt images. In this paper, a simple approach is used to encrypt the images than that of the traditional cryptographic algorithms. This method is based on Cellular Automata (CA).

CA is simple mathematical idealizations of a system [1]. John Von Neumann [2] proposed an emerging concept of CA, which is discrete in nature and consists of cells in the form of grids. The cells update themselves according to some deterministic rules, depending on the present state of the cell and the state of neighborhood cells. This makes the images cells change their state at any step. We need to recover the images (decrypt) and therefore, the transformations must be reversible. CA Group Rules have the property of returning to the original state, after say (n) number of cycles. Thus, we need to apply the transformation, at the encryption side for say (k) number of times and apply the remaining $(n-k)$ number of transformations at the decryption side. CA offers various advantages including the simplicity of locally interconnected and being regular and modular. This makes CA a right candidate for VLSI implementations [3].

In this paper, an encryption scheme for mobile phones has been proposed. The scheme is based on experiments done on various standard images using two-dimensional Cellular Automata (2DCA).

2. REVIEW OF EARLIER WORK

CA is considered as an attractive research field due to its simplicity, regularity, modularity and local interconnections [3]. Furthermore, it is one of the efficient candidates for image cryptosystems due to its essential characteristics, such as unpredictability, homogeneity and parallelism. Another reason for the wide deployment of CA is its simple implementation in both hardware and software systems [4]. This in turn makes the CA an efficient option for involved applications.

The first experiment on CA based investigation was by Wolfram [5], who used it to evaluate the first secret main process. After that, various other investigations were performed, to explore several CA dependent cryptography systems. CA has been widely deployed in various image cryptography applications, such as image security system, image encryption, secret image sharing, watermarking and image scrambling [6]. Traditionally, CA has been deployed in constructing Random Number Generator (RNG) in various cryptographic devices

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

as the ones explored by Wolfram [5] and Nandi et al. [7]. Then other researchers studied the one dimensional CA (1DCA) RNG, where they proved that CA is suitable for producing pseudorandom numbers and illustrated their advantage in comparison with other deployed schemes [8]. Alvarez and Hernandz [9], proposed an efficient graphic cryptosystem using 1D reversible CA, to encrypt defined images by any number of colors.

Two-dimensional Cellular Automata (2DCA) was later explored to implement images as one block in its natural form $m \times n$ to implement 2DCA based encryption model. A novel scheme for the generation of pseudorandom numbers using 2DCA was presented by Chowdhury et al. [10]. The obtained outcomes demonstrated that the 2DCA outperformed the 1DCA when compared using the same terms of pseudorandom numbers quality. An advanced pixel randomness test was presented by Suyambu et al. [11] with the use of a non-parametric technique. Specific approaches for security analysis were initially used to access the encryption method strength, where then the used non-parametric technique was deployed for determining the pixel randomness. However, deployment in hardware design was not possible, due to the need for use of parametric techniques.

Another model for image encryption was proposed by Ping et al. [12], using 2DCA by applying specific nonlinear balanced rules. These rules were used to carry out the confusion operation, while local interactions between cells were used to get the diffusion operation. Based on deploying a secured 144-bit key, authors in [13] presented a simple, sensitive and fast image encryption model. Yampolskiy et al. [14] proposed a new scheme and showed how to utilize the ability of CA to generate pseudorandom patterns. The efficiency of this scheme is better than the original Visual Cryptography approach. In [15] Khan proposed an encryption scheme based on 2DCA rules. However, the scheme proposed is general in nature and is stressing on the idea only, no experimentation results and rule selection was performed.

In this paper, the encryption scheme proposed is based on experimental results, selection of rules can be made based on the quality of encryption. In the next section, a brief preliminary concepts and definitions of CA have been reported.

3. CA PRELIMINARIES

Cellular Automata (CA) are composed of cells available in a specific n-dimensional cellular space. Neighbors of a cell can be defined as those cells that are at a specific distance from the cell. The cell itself may be considered as one of the neighboring cells while going through a transformation. A 1DCA is the simplest CA form, where all cells are located on a line, each having two states only. The CA is said to change its state in the next clock period based on the present state of the cell and/or the present state of its neighboring cells. The number of neighboring cells involved to change the next state is generally referred to as CA rule. For example, rule 90 states that the next state of a cell depends on the present state of the right and the left cells. Similarly, rule 150 states that the next state of the cell depends on the present state of the right and the left cell and the cell itself. Mathematically, the rule transitions for these two rules are given below [4].

$$X_i(t+1) = X_{i-1}(t) \oplus X_{i+1}(t)$$

$$X_i(t+1) = X_{i-1}(t) \oplus X_i(t) \oplus X_{i+1}(t)$$

Where

$X_i(t+1)$ is the next state of the CA and $X_i(t)$ is the present state of the CA cell at position i.

A CA is considered as a regular or uniform CA, when one rule is deployed for all cells in it. Conversely, it is called hybrid when various rules are deployed for various cells in it. In addition, it is called periodic when its extreme cells are close for each other. But, when its extreme cells are linked with logic 0-state, the CA then is called a null boundary. Based on considering rules of logic gates, when neighborhoods are based on rules of EXOR or EXNOR only, the CA is known as an additive CA. Particularly; the linear CA uses the rules of XOR gate only. On the other hand, when the transformation of the CA is invertible, which means that the whole states in the diagram of state transition lie in a specific cycle, the CA is then called Group CA. Else, it is known as a non-group CA [16].

Previously, various investigations were conducted concerning the use of 1DCA in developing various encryption schemes. However, 2DCA is a natural choice of implementing image encryption as images and pictures are available in two dimensional form. Practically, cells in 2DCA are mainly pre-arranged in a 2D grid pattern where adjacent cells are connected together. The CA is mainly explored using a binary matrix with dimensions $m \times n$. The sates of a cell and its adjacent eight cells are updated according to the rule, involving one or more neighboring cells. The rules determine the next state of the CA. Table I shows the basic rule convention for 2DCA [16].

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

Table I: Two Dimesional CA rule convention

64	128	256
32	1	2
16	8	4

Assuming $X(t)$ represents the 2D matrix of binary information, as the initial sate of the 2DCA. Then, defined by a certain rule, the next state $X(t+1)$ will be the EXOR operation among the states of related neighbors, defined by that rule. Since there are nine neighbors of each cell (including the cell itself), the number of possible uniform rules are 512, including both group and non-group rules. In this paper, only group rules have been considered as it is important for the transformation to be invertible, to decrypt the images. The total number of 2DCA Group rules and their classifications have been reported in [17]. The next section, presents various experimental results along with PSNR.

4. RESULTS AND DISCUSSION

The 2DCA group rules have been classified into four different categories, based on certain Characterization Matrix [17]. The images were initially encrypted based on primary rules [16]; however, the results showed that the image encryption quality was not perfect as shown in Fig.1. In each case, the image was first converted into binary image before applying the CA rule.

Fig. 2 shows the results of encryption with class 2 rules (rule 17 and rule 30) for number of iterations. The results shows improved encryption quality for class 2 rules. Consequently, all other rules in Class 1, class 2, class 3 and class 4 group rules were applied. The Group Rules showed the confusion and diffusion property of encryption of pixel values of the images. Statistical analysis of the results were carried out as reported next.

4.1 *Measurement of Encryption Quality*

In practice, the PSNR is considered as a helpful system performance measure, where it represents the ratio among a component mean square difference between two images and the maximum possible difference that can be present among them.

Figure 1Encryption using primary rules

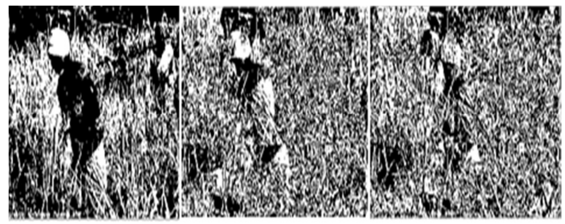

Figure 2: Encryption With Rule 17 After 0, 30 & 40 Iterations

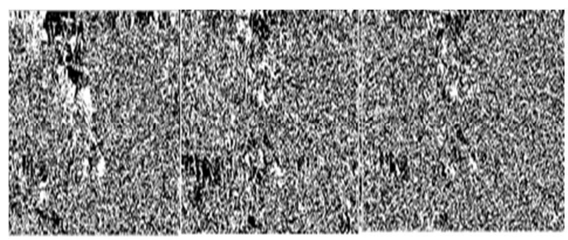

Figure 3Encryption With Rule 31 After 0, 30 & 40 Iterations

The PSNR is mainly represented in a decibel value. Its value is directly related to the recovered image quality. Let P and P' be the given image and encrypted image respectively, then the PSNR is represented as

$$PSNR = 20 \times (log_{10})(225 \div \sqrt{MSE})$$

Where MSE is Mean Square Error [18]

4.1 *Determining the RULE for Encryption*

The best rule from each class is determined using statistical analysis that has less correlation coefficient. Encryption Quality of the rule is determined by high PSNR value. In addition, an analysis of association between two horizontally and vertically neighboring pixels in several given images and their related encrypted images have been calculated. Table II, Table III, Table IV and Table V list correlation coefficient (CC) and PSNR value of all the class 1, class 2, class 3 and class 4 group rules, respectively.

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

These results demonstrate that the PSNR and CC for rule 33 of Class 1, rule 31 of Class 2, rule 225 of Class 3 and rule 135 of Class 4 are the best rules from each class, which confirms that 2D Group Rules is the best method for encryption in terms of encryption effectiveness and quality. These rules show that there the correlation between the two adjacent cell values, in the encrypted images, is negligible. Hence, the results show that the proposed rules have good permutation and substitution properties.

Table II: CC and PSNR of Class 1 Group Rules

rule	Image	Horizontal correlation Coefficient	Vertical correlation Coefficient	PSNR
1	Camera man	0.810077333	0.806549564	Infinite
	Lena	0.841393604	0.900828565	Infinite
3	Camera man	0.675336014	0.676188527	50.432765
	Lena	0.701934776	0.80887329	51.0691279
33	**Camera man**	**0.675054789**	**0.676188527**	**50.432765**
	Lena	**0.701824158**	**0.80887329**	**51.0691279**

Table III: CC and PSNR of Class 2 Group Rules

Rule	Image	Horizontal Correlation Coefficient	Vertical Correlation Coefficient	PSNR
5	Lena	0.608399	0.733031	51.043881
	Camera man	0.6449	0.6307	50.4331
7	Lena	0 .464838	0.628585	51.707945
	Camera man	0.5477	0.5302	50.7801
9	Lena	0.618008	0 .730532	51.043291
	Camera man	0.6694	0.6472	50.4328
11	Lena	0.471966	0.619169	50.780140
	Camera man	0.5400	0.5250	51.1157
13	Lena	0.487267	0.625796	51.021524
	Camera man	0.5433	0.5175	51.3220
15	Lena	0 .373149	0.536379	51.184142
	Camera man	0.4537	0.4276	50.7268
17	Lena	0.601410	0.722815	51.043291
	Camera man	0.6534	0.6412	50.4331
19	Lena	0.467095	0.612564	50.745861
	Camera man	0.5336	0.5241	50.5350
21	Lena	0.462400	0.617988	50.645155
	Camera man	0.5365	0.5246	52.4254
23	Lena	0 .357344	0.527532	51.312740
	Camera man	0.4462	0.4304	51.0430
25	Lena	0.483639	0.620596	51.031512
	Camera man	0.5419	0.5225	51.4527
27	Lena	0.373665	0.525484	51.272143
	Camera man	0.4414	0.4259	50.9804
29	Lena	0.367109	0.522176	51.049783
	Camera man	0.4566	0.4446	51.0695
31	**Lena**	**0.281308**	**0.444712**	**52.008634**
	Camera man	**0.3706**	**0.3550**	**52.6702**
37	Lena	0.480175	0.620635	50.896589
	Camera man	0.5281	0.5178	50.9637
41	Lena	0.496401	0.626967	50.416154
	Camera man	0.5498	0.5326	50.6400
45	Lena	0.392138	0.529960	50.959764
	Camera man	0.4448	0.4227	51.0562
49	Lena	0.468883	0.611249	51.085962
	Camera man	0.5326	0.5200	51.0219

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

53	Lena	0.372026	0.518929	51.302712
	Camera man	0.4401	0.4293	50.7617
57	Lena	0.468883	0.611249	51.085962
	Camera man	0.5326	0.5200	51.0219
61	Lena	0.372026	0.518929	51.302712
	Camera man	0.4401	0.4293	50.7617

Table IV: CC and PSNR of Class 3 Group Rules

Rule	Image	Horizontal Correlation Coefficient	Vertical Correlation Coefficient	PSNR
65	Camera man	0.532621525	0.519956414	51.02192
	Lena	0.571340209	0.726107332	51.48564
77	Camera man	0.390251735	0.479373906	51.15115
	Lena	0.392825426	0.580742983	51.02305
97	Camera man	0.31273236	0.473887593	51.16938
	Lena	0.477761874	0.651899653	51.46562
129	Camera man	0.386741119	0.524740134	51.15193
	Lena	0.578865102	0.718851906	50.88622
131	Cameram an	0.480269249	0.582119963	51.04641
	Lena	0.495207783	0.648675824	51.43
161	Camera man	0.415239629	0.375749285	51.23831
	Lena	0.493140661	0.503199784	51.06913
193	Camera man	0.573702473	0.645799015	50.66619
	Lena	0.583999343	0.719727357	50.77978
195	Camera man	0.478719645	0.582575242	51.3442
	Lena	0.486689696	0.646249632	51.39629
225	**Camera man**	**0.376542118**	**0.222953988**	**51.19744**
	Lena	**0.229457427**	**0.466129232**	**51.30675**
257	Camera man	0.474498125	0.383239573	51.09617
	Lena	0.40033623	0.51952894	51.09923
259	Camera man	0.495207783	0.648675824	51.22254
	Lena	0.480269249	0.582119963	51.37628
289	Camera man	0.565274451	0.598729364	50.67381
	Lena	0.478432157	0.646583544	51.22372
321	Camera man	0.392809093	0.518897015	51.19236
	Lena	0.388179221	0.578604626	51.06913
323	Camera man	0.317754281	0.464985842	51.14806
	Lena	0.466176458	0.644358966	51.1157
353	Camera man	0.249496721	0.330331661	51.19119
	Lena	0.683252776	0.730492291	51.15386
385	Camera man	0.56960173	0.612047951	51.10841
	Lena	0.808763697	0.806549564	51.39998
387	Camera man	0.834678	0.867123	51.98793
	Lena	0.667857671	0.723172359	51.25096
417	Camera man	0.360570345	0.411950391	51.13223
	Lena	0.47088951	0.579436063	51.35109
449	Camera man	0.396326514	0.485480212	51.2708
	Lena	0.383034129	0.52118679	51.07179
451	Camera man	0.466176458	0.644358966	50.94302
	Lena	0.317754281	0.464985842	51.09617
481	Camera man	0.37896262	0.489502629	50.98564
	Lena	0.695203058	0.80887329	50.78761

Table V: CC and PSNR of Class 4 Group Rules

Rule	Image	Horizontal correlation Coefficient	Vertical cCorrelation Coefficient	PSNR
73	Camera man	0.451356726	0.435144731	50.73385
	Lena	0.477761874	0.651899653	51.46562
79	Camera	0.3870206	0.5178066	51.128

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

	man	22	54	
	Lena	0.571340209	0.726107332	51.48564
81	Cameraman	0.462664734	0.572799648	50.93307
	Lena	0.477761874	0.651899653	51.46562
89	Camera man	0.38874701	0.526992662	51.25888
	Lena	0.58964844	0.727081547	50.3764
105	Camera man	0.473255473	0.578402698	51.2712
	Lena	0.701824158	0.80887329	51.06913
113	Camera man	0.569002982	0.644014663	50.99833
	Lena	0.58964844	0.727081547	50.3764
121	Camera man	0.401285736	0.482680171	51.17365
	Lena	0.583999343	0.719727357	50.77978
133	Camera man	0.478719645	0.582575242	51.3442
	Lena	0.486689696	0.646249632	51.39629
135	**Camera man**	**0.310521053**	**0.400443952**	**51.23673**
	Lena	**0.40786302**	**0.648657762**	**51.21194**
145	Camera man	0.402049863	0.519029483	51.15115
	Lena	0.592379025	0.726481177	50.86226
177	Camera man	0.490312359	0.584737704	51.04565
	Lena	0.490786302	0.648657762	51.21194
209	Camera man	0.402049863	0.519029483	51.15115
	Lena	0.592379025	0.726481177	50.86226
241	Camera man	0.475459288	0.584715654	51.11992
	Lena	0.706041281	0.805938199	51.06913
261	Camera man	0.578517602	0.652560401	51.46979
	Lena	0.595607427	0.723953765	50.75923
263	Camera man	0.48219287	0.583051067	51.47645
	Lena	0.706041281	0.805938199	51.06913
265	Camera man	0.574799228	0.649001027	50.76737
	Lena	0.592379025	0.726481177	50.86226
269	Camera man	0.48068724	0.586375393	50.93749
	Lena	0.49639933	0.650541558	50.8406
271	Camera man	0.312215832	0.407873005	51.08472
	Lena	0.693140661	0.803199784	51.06913
389	Camera man	0.570364762	0.653767053	51.02005
	Lena	0.580048998	0.72512674	51.37424

The four rules (33, 31, 225 and 135) were applied to the input image, after converting the image to binary, as shown in Fig 4. The resulting encrypted and decrypted images are as shown in Fig 5, Fig 6, Fig 7 and Fig 8.

Figure 4: Input image converted to binary image

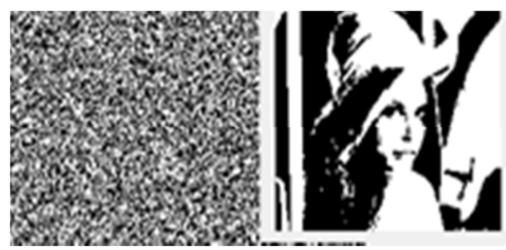

Figure 5: Encrypted and Decrypted Image with rule 33

Figure 6 Encrypted and Decrypted Image with Rule 31

Journal of Theoretical and Applied Information Technology
15th March 2017. Vol.95. No 5

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

Figure 7: Encrypted and Decrypted Image with rule 225

Figure 8: Encrypted and Decrypted image with rule 135

5. PROPOSED ARCHITECTURE

The design of all digital circuits has been influenced by Very Large Scale Integration (VLSI) technology. Regular, modular and cascadable structures are in demand for implementing complex functions in terms of hardware components. CA structure has also been found a better alternative to implement such functions, because of the fact that CA based circuits have the advantage of regularity, shorter delays and structure being modular and cascadable [3]. In this section, an architecture for implementing the encryption scheme based on the above stated rules is discussed. The scheme can be implemented in mobile phones, by inserting a CA memory preceding the main memory as illustrated in Fig 9. Images shot by the mobile camera must go through the CA chip, for encryption, before being stored in the main memory of the mobile. Similarly, before images being properly displayed must again be decrypted in the CA memory. The encryption process must have an encryption "key", chosen by the user. The key value depends on the rule to be applied and the number of CA cycles (iteration) chosen. The user can use the key value in the form of a PIN value, which can be encoded into CA rules to be applied and the number of cycles the CA will run.

The general architecture of the CA memory is illustrated in Fig 10. Since each cell of a CA is representing a logic 0 or 1, each cell is represented by a D-type Flip-Flop having the output Q representing the CA state. The output Q of each Flip-Flop is updated, on each clock, based on the state of its neighboring D- Flip Flops, representing a rule.

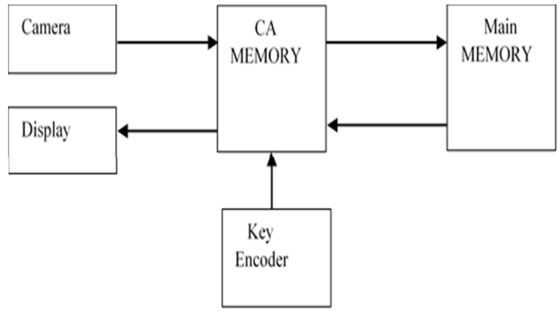

Figure 9: Proposed Scheme

The inputs to EXOR circuit depend on the rule to be applied. Depending upon the number of rules considered for encryption, the selection of one of the rules is to be done. The selection can be done using a multiplexer circuit as shown in Fig 10. Now the multiplexer circuits needs to be a k-to-1 line multiplexer, with two select lines. Moreover, the value of S_0 and S_1 will be part of the encryption key.

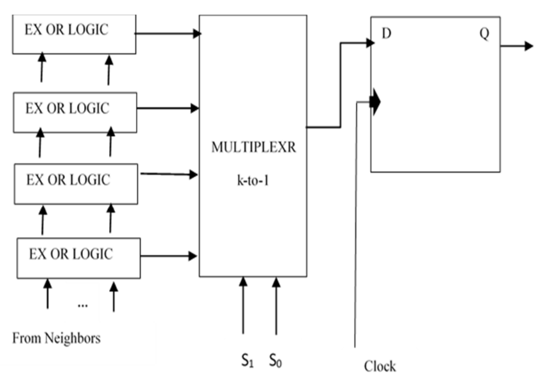

Figure 10: CA Memory Architecture

6. CONCLUSION

In this paper, an image encryption scheme using 2DCA group rules has been proposed. The encryption scheme is not complex in nature, but privacy of images can still be achieved, by applying several group rules and the number of cycles the CA is run. The user will input a 4 to 5 number PIN value, which can be encoded to the proper selection of the rule no and the CA cycle. Moreover, the scheme can be easily implemented using VLSI technology.

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

REFERENCES

[1] A. Singh1, S. Sangeeta,"Cryptographic Algorithm Using Cellular Automata Rules" , *International Journal Of Computer Application*, Vol 3, No 4, Pp 57-64, 2014.

[2] J. V. Neumann, "The Theory Of Self-Reproducing Automata", (Edited By A. W. Burks) *Univ. Of Illinois Press* Urbana, 1996.

[3] P.P. Chaudhuri, D.R. Chowdhury, "Additive Cellular Automata Theory And Application", Vol.1. *John Wiley And Sons*, 1997.

[4] X.Zhang, C.Wang; S. Zhong And Q. Yao, "Image Encryption Scheme Based On Balanced Two-Dimensional Cellular Automata", *Mathematical Problems In Engineering*, Vol. 2013, Article Id 562768, 10 Pages, 2013.

[5] S. Wolfram, "Cryptography With Cellular Automata", Advances In Cryptography: Crypto'85 Proceedings, *Lecture Notes In Computer Science*, Vol. 218, Springer, Pp 429-432, 1986.

[6] R. Ye And H. Li, "A Novel Image Scrambling And Watermarking Scheme Based On Cellular Automata". *Proc. International Symposium Electronics Commerce And Security*, Ieee Cs Press, Pp 938-941, 2008.

[7] S. Nandi, B. K. Kar, "Theory And Applications Of Cellular Automata In Cryptography", *Ieee Transactions On Computers,* Vol. 43. No 12, Pp 1346-1357, 1994.

[8] M. Tomassini, M. Sipper, M. Perrenoud,"On The Generation Of High-Quality Random Numbers By Two-Dimensional Cellular Automata", *Ieee Transactions On Computers*, Vol.49. No 10, Pp 291-305, 2000.

[9] G. Alvarez, A. Hernandez, "A New Graphic Cryptosystem Based On One-Dimensional Memory Cellular Automata", *Proceedings Ieee 39th Annual 2005 International Conference On Security Technology*, 2005.

[10] D.R. Chowdhury, I.S. Gupta, And P.P. Chaudhuri, "A Class Of Two-Dimensional Cellular Automata And Applications In Random Pattern Testing", *J. Electronic Testing: Theory And Applications*, Vol.5, Pp.65-80, 1994.

[11] B. Suyambu, R. Radha, R. Rama, "New 2d Ca Based Image Encryption Scheme And A Novel Non-Parametric Test For Pixel Randomness", Arxiv:1505.00920v1 [Cs.Cr], 2015.

[12] P.Ping, X.Feng. W.Zhi-Jiang, "Color Image Encryption Based On Two Dimensional Cellular Automata", International *Journal Of Modern Physics C*, Vol. 24, No 10, 2013.

[13] P. Pareek, "Design And Analysis Of Novel Digital Image Encryption Scheme", *Ijnsa*, Vol. 4, No. 2, 2012.

[14] R. Yampolskiy, J. Rebolledo, M. Hindi, "Password Protected Visual Cryptography Via Cellular Automaton Rule 30", *Transcations On Dhms Ix, Lecture Notes In Cs* 8363, Pp 57-67,2014.

[15] A.R. Khan, "Image Encryption Using Cellular Automata", *Information Journal*, Vol. 16 No. 8a, Pp 5581-5590, 2014.

[16] A. R Khan, Et Al, "Vlsi Architecture Of Cellular Automata Machine", *Computers And Mathematics With Applications*, Vol. 33 No.5, Pp 79-94, 1997.

[17] A. R Khan, " Classification Of 2d Cellular Automata Uniform Group Rules", *European Journal Of Scientific Research*, Vol. 64, No. 3, Pp 51-57, 2011.

[18] C. Peng; Y. Li, "A New Algorithm For Image Encryption Based On Couple Chaotic System And Cellular Automata", *International Conference On Mechatronic Sciences, Electric Engineering And Computer (Mec)*, Pp. 1645-1648,2013.