Image encryption by cellular automata and chaos map over Gpu processor

Abbas Hasanpooraskari, Mehran Abdali, Farokh Koropi

***Abstract*— Recently, a variety of chaos-based algorithms has been offered for image encryption. But, none of them has worked in the parallel computing environment. They also have used cellular automata in most encryption branches. The reason of using cellular automata is its simple structure, easy implementation, and its complicated behavior. Because of this characteristic, there is the possibility of doing complicated operations by cellular automata using simpler methods.**

In this paper, it has been talked about image encryption based on chaotic cellular automata and chaos mapping on graphic processors. We have also used hybrid cellular automata with chaos mapping that improves random number generation considerably and solve the problem of duplicate numbers in cellular automata. The chaos cellular automata have been used to increase the security of encryption and the encryption has been done in two stages. In order to increase the speed of encryption, we did the operation on graphic processors with parallelization capability. The results of analysis including coefficient correlation, similarity of adjacent pixels, sensitivity to the key, the key space and PSNR indicate the improvement of attained results. The speed of encryption operation has also increased considerably in the proposed method.

***Index Terms*— encryption, cellular automata, image processing, chaos theory, graphic processor**

I. INTRODUCTION

The amount of digital image transfer via computer and specially internet has increased rapidly in recent years. In most of the cases, the communication channels are not secure and are attacked by hackers and thieves. So, the security of images and hiding them is an important issue. Many different methods have been proposed for this subject. Among them chaos-based methods have special characteristics. Generally, chaotic systems have some characteristics that have changed them into the main part of the encryption system organizing. Hence, some of these methods create noise in the input while the encrypted image has a high PSNR in comparison with the primary image and is not a real copy of the original form. In one other research, the researchers calculated the value of MSE between the primary image and the encrypted image. Although the value is close to zero, it cant guarantee that the encrypted image is the same as the primary one. There are some other methods that are not based on Fourier transformation. For example, Martina et al (2004) offer the binomial orthogonal transfer. It can reduce the values between adjacent pixels. In 1989, kyas system was used for encryption for the first time [i]. Many researches have been done to introduce and analyze encryption algorithms based on kyas since then. These researches have discussed characteristics of kyas like sensitivity and dependence on initial values, being pseudo-random, and having non-periodic functions. As well as having these characteristics, a good encryption algorithm should be sensitive to wrong keys and have big space of keys so that it can resist the severe attacks of brute-force hackers. Furthermore, there is a series of two-dimensional chaotic mappings that is suitable for image pixel permutation. (Scharinger et al,(2006) have proposed a method for image pixel replacement by Kolmogorov encryption. Fridrich (2006) developed the previous method for general applications. Then Chen et al,2006 offered a new method for three-dimensional mapping by image encryption. Lian (2008) also proposed a method based on the standard algorithm mapping [ii]. As it was mentioned before, most of these algorithms include two parts of permutation and substitution. These two stages provide capabilities for image encryption but they can't be performed in parallel form and the program is operated in ordinal form and without any nucleus. It has an efficient effect on the speed of encryption. To solve the above problem, Qing Zhou et al proposed the idea of image blocking[ii]. Kwok-ko(2008) used add and shift during the permutation of image pixels to increase the speed of encryption[iii]. In this method, first, the image is divided into blocks and then using chaos special function, block permutation and pixel replacement is done simultaneously. The other factor that increases the speed of the proposed method is the usage of chaos spatial function to produce random numbers. As cellular automata have a simple structure and offers random operation, it has a good ability in producing pseudo-random numbers and using them in encryption. At first a mathematician called Pullam became interested in graphic structures that are produced by simple rules. The base of his model was a two-dimensional space that was divided into some cells. Each of the cells could have two states of on and off [iv].

II. USING GRAPHIC PROCESSORS

Central processor as the brain of computer performs a sequence of orders. There is one other group of processors that can do operation on data in each pulse. For example, the processors of graphic processor unit are of this kind.

Performing one order in several inputs is done by the help of several nucleuses. Nowadays, graphic processor units have more than 100 nucleuses that all of them are similar. The nucleus of a graphic processor unit is simpler than the nucleus

Manuscript received June 20, 2014.

Abbas Hasanpooraskari, Department of Computer, Baft Branch, Islamic Azad university, Baft, Iran

Mehran Abdali, Department of Computer, Baft Branch, Islamic Azad university, Baft, Iran

Farokh Koropi, Department of Computer, Baft Branch, Islamic Azad university, Baft, Iran

of a central processor. A GPU with n nucleus is able to perform an order on more than n input. This capability is suitable for performing some yarns with special characteristics. As we told before SIMD architecture provides the possibility of performing hundreds of threads using CUDA programming tool. The programming tool can map image pixels on each thread and threads perform the operation of each pixel in parallel form. This will increase the speed of encryption[v][vi][vii][viii].

III. INDEFINITE CELLULAR AUTOMATA

Being definite means when t time units pass the final configuration can be determined uniquely. Indefinite cellular automata don't have this characteristic. That is after t time unit pass, instead of unique configuration, we will have a group of configurations that we won't know which one will be produced. Generally, the indefinite cellular automata are written in foursome form (d, s, n, r). d shows the number that comes after indefinite cellular automata, S={s1,s2,…,sk} is the set of states of indefinite cellular automata. N={v1,v2,…,vn} is a set of arrows that show neighborhoods of a cell. R is a relation that is defined as follow:

$r:S^n \rightarrow 2^S$

2s represents all subsets of s. As local rule is considered as a relation, the general rule of indefinite cellular automata is also considered as a relation. All the concepts of definite cellular automata are true about indefinite cellular automata. For example, configuration has the same concept in definite and indefinite cellular automata. For example consider the following cellular automata:

NCA={d=1,S={0,1},N={-1,0,+1},r}

As it can be seen, it is an indefinite cellular automata because there are two states in some r transformations that we can choose one of them. we can't do any certain prediction about the final configuration in indefinite cellular automata, unless we determine the transform that we are going to use in each stage. This characteristic will help us to make an encryption system based on indefinite cellular automata.

IV. THE STAGES OF THE PROPOSED ALGORITHM

A. *Permutation of pixels*

To increase the chaos, the pixels of the image are permutated (replaced). This is done in a way that the position of pixels changes during some stages and processes. As we need to perform all the stages on the graphic processors, we should be able to apply the method on the pixels of the image separately and in a parallel form. So, we use Baker's two-dimensional discrete method. Kolmogorov mapping is used separately for each cell in the permutation stage that unsettles the position of image pixels. As a result all the pixels are settled parallel in new places that are determined by mapping process and this will increase the difference between the primary image and the encrypted image. The discrete model of 4-1 equation is stated [ii].

$$B_a(r,s) = \left(\frac{N}{n_i}(r - N_i) + s \bmod \frac{N}{n_i}, \frac{n_i}{N}\left(s - s \bmod \frac{N}{n_i}\right) + N_i\right) \qquad (1)$$

(r,s) determines the position of pixel in $N_i \le r < N_i + n_{i+1}, 0 \le s < N, i = 1, \dots, k$ limitation in which the K sequence is chosen as the true value of (n1,n2,…,nk) that each of these values divide the image to parts with the size of ni. In a true value that $\sum_s \mathrm{ns} = \mathrm{N}$, ns divides N into S parts. Geometric equivalence of 4-1 equation is shown in the picture. NxN image is first divided into vertical rectangles with the height of N and width of ns. Then each rectangle is divided into boxes with the height of qs and width of ns. Then k transform maps the available pixels of each box to a line.

So, according to the proposed model, in permutation phase a graphic processor is used for each pixel in each thread and a new situation is attained based on the above situation. This is done for all pixels in parallel form then all pixels of a thread related to a graphic processor are permutated simultaneously.

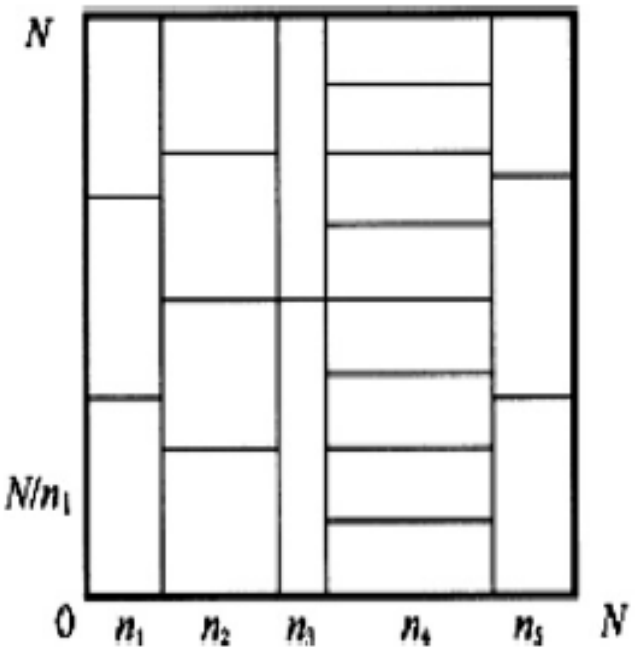

Figure1. The geometric equivalence of Baker model

B. *Placement*

In placement phase, first, the pixels of images are blocked in 8*8 blocks. So, the unit of work in this stage is a block of pixels. As it was told before, the problem of automata is the production of a short sequence of numbers. In this algorithm, one other cellular automata and chaos mapping are used as external stimulators to stimulate cellular automata. Using chaos mapping, cellular automata produce a model for the second cellular automata that performs encryption. This model is combined with image block in the second cellular automata and as an external stimulator in second cellular automata, makes the encryption process complicated, improve it, and increases the entropy of the encrypted image. The automata used to produce the model have the following characteristics: two-dimensional, developed, indefinite, and variable.

First, each dimension of cellular automata is selected. The cellular automata are created in selected dimensions and their initial values are given. The initial values of the cellular automata are determined using chaos mapping. To do so,

Logistic mapping is used and each pixel is encrypted in the thread related to graphic processor.

C. the idea of image placement algorithm with indefinite cellular automata

We know that the purpose of encryption is to hide data to prevent people attain them. If we consider that A is the primary image, we are looking for a way to change the primary image to the encrypted image of C and the data from which we use is considered as the key (k). Indefinite cellular automata make it possible to begin from the primary image of M as the primary configuration for indefinite cellular automata and then attain a group of encrypted pictures of C that are the final configuration. It is not very important that which encrypted images are produced. Now, it can be predetermined that which transfers of r equation should be used in each phase of indefinite cellular automata and this information can be used as the key for encryption. If we update the indefinite cellular automata based on selected key, then the indefinite cellular automata is changed into definite cellular automata. In fact, the selected key helps to remove uncertainty in indefinite cellular automata. For example, if the two selected rules are r2 and rl then K(i) help us in (i) stage of encryption to the encryption process clearly so that if K(i) is zero we use rl rule and if it is one we use r2 rule.

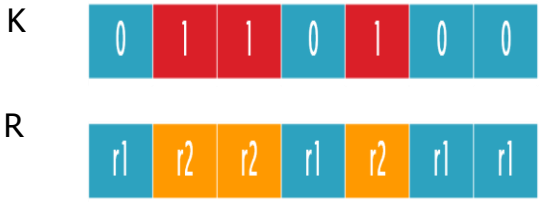

Figure 2: the method of selecting rules base on the key

The main problem of automata is the production of a short sequence of numbers so that a set of produced numbers are repeated regularly. To solve this problem, combined rules or in other word combined automata is offered that improve the condition of random number production to a great extent. But the problem of this solution is that it uses several rules and as a result the hardware became more complicated.
Generally, stochastic behavior of a system depends on 3 factors[ix]: 1) the effect of external random stimulator, 2) the effect of the initial random value like the operation of chaotic functions or 3) the effect of the internal structure of system but not the effect of external factors and not the initial random state like the rule number 30 of cellular automata that initial value and external stimulator don't have any effect on its performance. Based on the experiments, it is shown that some automata rules are sensitive to external stimulators. It seems that stimulating cellular automata with external random factors will lead to more random states in automata that are illustrated in entropy increase. In this study, it is tried to use this characteristic of automata for encryption so that by using two cellular automata and chaotic mapping as the external stimulator the entropy of automata is increased. The entropy increase indicates the increase in the number of states. So the repetitive patterns reduce in encrypted data and the encryption process done by minatory become more complicated.

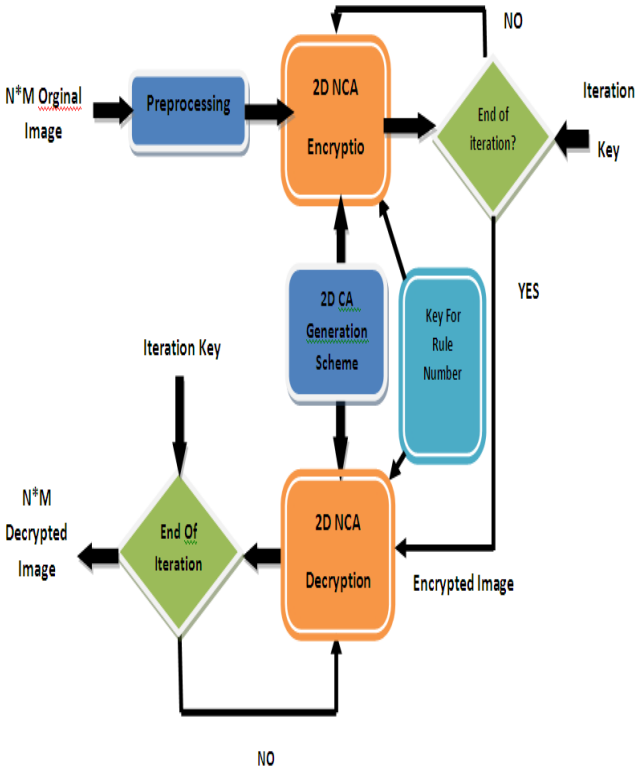

Figure 3: the structure of placement operation by means of cellular automata

D. The phases of making placement algorithm

In this method the combination of indefinite developed cellular automata and chaos mapping is proposed to improve encryption and security. The rules of the two automata are determined by chaos mapping and saved as a part of the key. The first cellular automata is used for pattern production and the second cellular automata is used for image encryption or production pattern. Chaos mapping is used to determine the initial value of the first cellular automata.

As it was mentioned before the problem of automata is the production of a short sequence of numbers. In this algorithm, one other cellular automata and chaos mapping are used as external stimulator to stimulate the cellular automata. The first cellular automata using chaos mapping produce a pattern for the second cellular automata that do the encryption operation. This pattern is combined with the value of image in the second cellular automata and acting as an external stimulator in the cellular automata makes encryption complicated, improves encryption and increases entropy. the used cellular automata for pattern production has the following characteristics: two-dimensional, developed, indefinite and variable size.

At first each dimension of the cellular automata is determined. The cellular automata with selected sizes are produced and the initial values are given.
R,C =selected

$$CA_{Scheme}=create(R,C) \quad (1)$$

Initializing the cellular automata based on chaos mapping
Cellular automata is initialized by chaos mapping. To do so, we use the following mapping:

$$Xn=3.95*Xn1*(1-Xn1) \quad (2)$$

In the proposed algorithm, there is no limitation in using chaos mapping and every function can be used. The above function is chosen as an example because it behave well in (0,1) interval to produce random numbers with a uniform distribution probability.

updating cellular automata

After we initialized the cellular automata, these values are updated by means of cellular automata rules until the final pattern is produced. As the cellular automata is indefinite, the values of each line of cellular automata are updated based on the rules of each line. Rules and the method of applying these rules are determined by the chaos mapping and saved in the key. In order to update the ci cell, this cell, the values of adjacent cells, and the previous value of the cell as the cell is a developed one, are determined.

In this section, the dimensions of cellular automata, automata rules, the initial value of chaos mapping, and the number of repetitions in mapping are saved as a part of the private key. The main idea of the proposed idea is changing the values of pixels. After producing the pattern by the first cellular automata, image encryption is done by means of the second cellular automata. A two-dimensional indefinite cellular automata is used to do the encryption. First, the image is placed on the cells of the second cellular automata as the primary configuration. As the cellular automata is indefinite, we gain the rule that should be applied in each phase based on the key. Each line updates its cells based on the rule of that line and produced pattern. The rules of each line are determined based chaos mapping and saved in the key. We consider the ci cell, the value of adjacent cells, an d corresponding pattern of that cell in the first cellular automata

decoding algorithm

In algorithm, decoding is done based on the key, initial value, chaos mapping, the number of repetition, and the rules. Cellular automata are created based on gained dimensions. This automata is initialized by the chaos mapping and determined parameters in the key. Then we gain the rule that should be applied in each line and update the values of each line based on these rules until the final pattern for decoding is produced. After the pattern is produced, the values of the encrypted image are placed on the second cellular automata as the primary configuration. The cells are combined with the adjacent cells and the values of produced cells based on the rules of each line. Then using 4-1 equation again, pixels return to their initial situation until the main image is gained.

CA decryption:

$$D(i)=[CA_{img}(i)-R_i\ (E(i),CA_{scheme}(i),N(i\ ,\ j)\ )]\ \text{Mod}\ \ L \qquad (3)$$

$$N(\ i\ ,\ j)=\{I(k,l)|k=\{i-r,..,i+r\}\ \ ,\ l=\{j-r\ldots,j+r\}\} \qquad (4)$$

experimental results

In this method the images of usc-sipi are used. The images of this bank are applied in image processing and machine vision and are collected by southern California university. The images of this bank are classified based on their characteristics.

A. the histogram analysis of the image

Histogram shows the number of pixels in each grey surface for each of the images. Generally, it can be shown that the smoother the image histogram in proposed algorithm, the less is he possibility of statistic attacks on it.

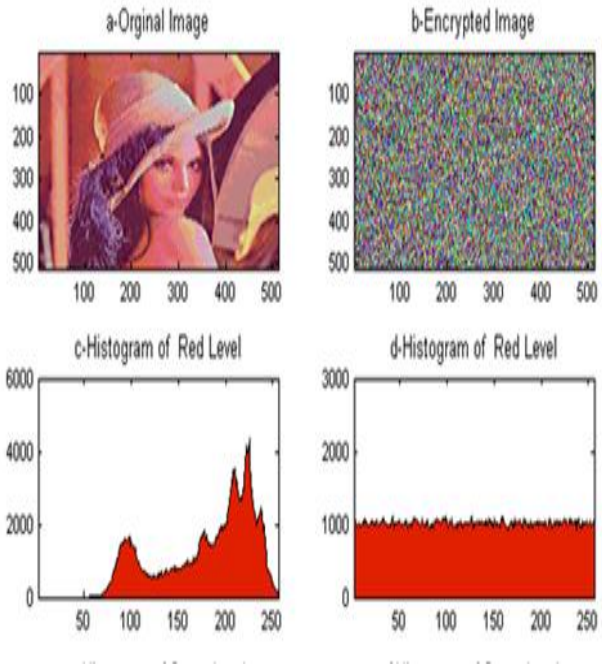

Figure 4: image (a) the main image, frame (c): respectively Lena image with the size of 256*256 in red surface, (b) encrypted image, frame (d) the histogram of encrypted image in red surface

As it can be seen clearly in the above picture, the histogram of encrypted image is a smooth one and it is quite different with the histogram of the primary image. This characteristic prevents hackers from finding any document for attack success and the proposed plan is secure in this regard.

B. publishing characteristic

Publishing states the relationship between the main image and the key. It means that changing one pixel from the main image changes several pixels of the encrypted picture, vice versa.

The effect of changing one pixel in the main image on the encrypted image can be measured by means of two scales: NPCR and UACI[x][xi]. NCPR can be defined as the rate of pixel changes in encrypted image as one pixel changes in the main image. UACI is defined as the average of these changes. NPCR and UACI are defined as follow:

$$NPCR = \frac{\sum_{i,j} D(i,j)}{W*H} \times 100\% \qquad (4)$$

$$UACI = \frac{1}{W\times H}\left[\sum_{i,j}\frac{|C_1(i,j)-C_2(i,j)|}{255}\right] \times 100\% \qquad (5)$$

In which W and H are respectively determiners of the length and the width of the images and c1 and c2 are two encrypted images taken from two images that are different only in one pixel. D is defined as follow:

$$D(i,j) = \begin{cases} 1, & if\ C_1(i,j) = C_2(i,j) \\ 0, & otherwise \geq 0 \end{cases}$$

This experiment was done on the following pictures that are different in just one pixel and its results are as follow:

Table 1: the obtained results of NPCR and UACI

NPCR	0.9962
UACI	0.3344

V. THE SIMILARITY OF ADJACENT PIXELS

If the points of the diagram are closer to the main diameter, the two adjacent pictures are more similar to each other. The purpose of encryption is to minimize this similarity in the encrypted image so that it will not be possible to attain the image by comparing the similarities of pixels. In this section, the similarities of adjacent, vertical, horizontal, and diagonal pixels of Lena's image are investigated in red, green, and blue pages. The results are shown.

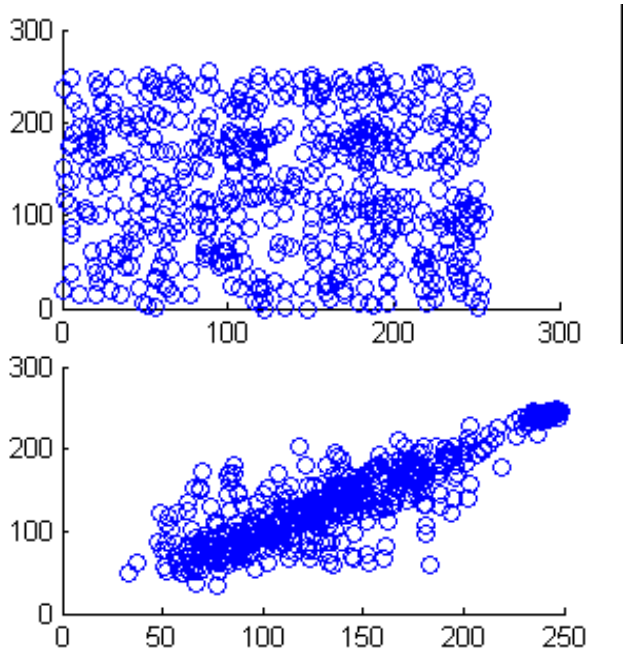

Figure 5: the similarity of vertical adjacent pixels of the red page in the primary image(right) and encrypted image (left)

D. the analysis of sensitivity to the key

A suitable method of encryption should be sensitive to small changes of the key so that changing a bit in the key will lead to a very different result. To test this idea, we encrypted one image with two different keys. In the following part , we will investigate the effect of wrong key on image encryption. So we decode Lenas image that is encrypted by k1 key with k2 key. The results show that a little change in the key will cause the main image not be loaded and a completely different result is gained from the picture.

E. the key space analysis

In a suitable method the space of the key should be big enough to resist unlimited attacks. In the 2N proposed method, 25 combinations of the key can be found. The experimental results show that such a number of combinations of keys is enough to resist the unlimited attacks. The breaking algorithm of this system of encryption has time complication of (2N) and is a part of NP.

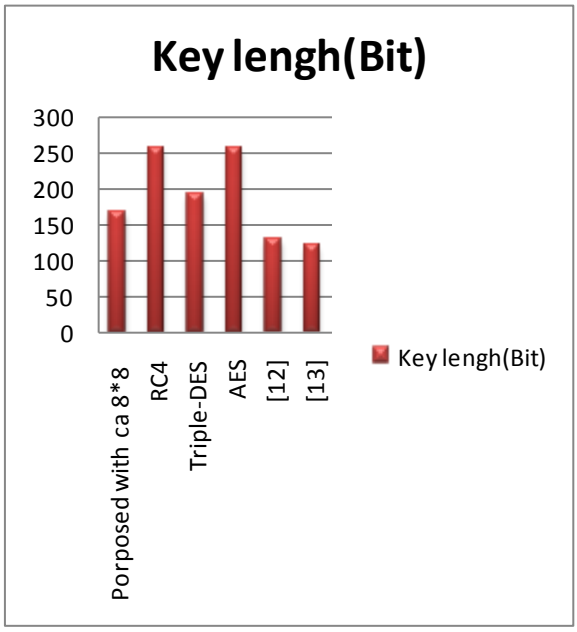

Figure 6: comparing the methods based on the key length

VI. CONCLUSION

In this article, a method was proposed to encrypt the images using Kyas functions and cellular automata on graphic processors. Cellular automata have a good ability in producing quasi -random numbers because of its simple structure and offering random operation and consequently can be used in encryption. But the problem of automata is that its random state is limited and the governed rules of automata have small interval and repetition of possible states. This makes it easy for the hackers to decode more easily and the possibility of using cellular automata in encryption is reduced.

In this research, we investigated the following three general issues:

First, to solve the mentioned problem the combined cellular automata with chaotic mapping is offered that improves random number production considerably and solve the problem of producing repetitive numbers in cellular automata.

Second: the indefinite cellular automata is used and encryption is done in two stages to increase the security.

Third: we do this operation on graphic processors with parallelizing capability to increase the speed of encryption. The value of PSNR between the encrypted image and the primary image shows that the encrypted image is different from the primary image. Furthermore, the MSE between the properly encrypted image and the primary image is zero and after decoding by the right keys, an image completely equal to the primary image is attained. If there is any kind of changes in the keys the image can't be decoded properly. This change can be occurred in Kyas function image or in key image.

REFERENCES

[1] Chatzichristofis Savvas A, Mitzias Dimitris A, Sirakoulis Georgios Ch, Boutalis Yiannis S. A novel cellular automata based technique for visual multimedia content encryption. Opt Commun 2010;283(21):4250–60

[2] Qing Z, Kwok-wo W, Xiaofeng L, Tao X, Yue H," Parallel image encryption algorithm based on discretized chaotic map". Chaos, Solitons & Fractals Volume 38, Issue 4, November 2008, Pages 1081-1092

[3]Behnia S, Akhshani A, Mahmodi H, et al, "A Novel Algorithm for Image Encryption Based on Mixture of Chaotic Maps", Chaos Solutions & Fractals, Vol. 35, No. 2, pp.408-419 (2008)

[4] E. Biham, A. Shamir, "Differential Cryptanalysis of DES-like Cryptosystems", Journal of Cryptology, vol. 4, pp. 3-72, IACR, 1991. (An extended abstract appears in Crypto'90)

[5] W. Liu, B. Schmidt, G. Voss, W. Mullerwitting, " streaming algorithms for biological sequence alignment on GPUs". IEEE Trans. Parallel and distributed systems, 2007, pp. 1270-1281.

[6] V.Simek, R. Asn," GPU Acceleration of 2D-DWT Image Compression in MATLAB with CUDA". IEEE Trans. Computer Modeling and Simulation, 2008, pp 284.

[7] NVIDIA Company, (2007): NVIDIA CUDA compute unified device architecture programming guide version 1.1.

[8] N. Leischner, Osipov, P. Sanders,"GPU Sample sort". IEEE Trans. Parallel & distributed processing,2010.

[9] S. Wolfram, "A New Kind Of Science", Copyright @ 2002 By Stephan Wolfram, Llc.

[10] Chen G, Moa YB,Chui Ck,"A symmetric image encryption scheme based on 3D Chaotic cat maps",solitons& Fractals 2004,pp.74-90

[11] Mao Yb,Chen G,Lian SG,"A Novel fast image encryption scheme based on the 3D chaotic baker map",Int J Bifurcat Chaos,2004,pp.3613-3624

[12] Machhout Mohsen, Guitouni Zied, Zeghid Medien And Tourki Rached," Design Of Reconfigurable Image Encryption Processor Using 2-D Cellular Automata Generator",International Journal Of Computer Science And Applications, Technomathematics Research Foundation Vol. 6, No, 4, Pp 43 - 62 , 2009

[13] Rong-Jian Chen , Shi-Jinnhorng, "Novel Scan-Ca-Based Image Security System Using Scan And 2-D Von Neumann Cellularautomata", International Journal Of Signalprocessing: Image Communication ,Elsevier, 2010