Study of Perfect Shuffle for Image Scrambling

H.B.Kekre*, Tanuja Sarode, Pallavi N.Halarnkar****

*Computer Engineering, MPSTME
**Computer Engineering, TSEC, MPSTME

***Abstract*-** In recent years, Digital data transmission has increased, providing security to this digital data is of high importance. As a result, people pay much more attention to image encryption. Many approaches for image encryption that have high security as well as simple encryption process have been proposed. In this paper, Perfect shuffle for image scrambling is introduced. Effects of perfect shuffles with different factors of the image size are discussed. The number of iterations required to get back the original image are related to the power of 2. Finally all these results are displayed by using 1024 X1024 Lena's image.

***Index Terms*-** Encryption, Scrambling, Perfect Shuffle, Down Sampling

I. INTRODUCTION

Image scrambling is a useful approach to secure the image data by scrambling the image into an unintelligible format. [1] introduces a new parameter based M-sequence which can be produced by a series shift registers. In addition, a new image scrambling algorithm based on the M-sequence is presented. The user can change the security keys, *r*, which indicates the number of shift operations to be implemented, or the distance parameter *p*, to generate many different M-sequences. This makes the scrambled images difficult to decode thus providing a high level of security protection for the images. The presented algorithm can encrypt the 2-D or 3-D images in one step. It also shows good performance in the image attacks such as filters (data loss) and noise attacks. The algorithm can be applied in the real-time applications since it is a straightforward process and easily implemented. [2] presents a novel image scrambling method using Poker shuffle, which is controlled dynamically by chaotic system. Compared with other scrambling techniques such as algebraic permutations and chaotic permutations, the proposed method has properties of nonlinearity, non-analytic formula and large key space. Moreover, its scrambling performance is satisfied and can deal with non-square image. All these features show that the proposed method is more secure and efficient for image scrambling encryption.

There are many methods for calculating the periodicity of Arnold transformation and getting the inverse transformation, the use of traditional Arnold transformation for the image scrambling is unsafe, for this issue [3] proposed an algorithm for digital image block location scrambling. It has improved the traditional Arnold transformation by adding two parameters a and b, furthermore it use Logistic map to generate the parameter sequences. The digital image is blocked, then carry out Arnold transformation with different parameters on each image block, after that put the transformed pixels on the corresponding position of the encrypted image, thus achieving image location scrambling. The results of simulation show that this algorithm can achieve good image encryption effect, and it has a large key space, key sensitivity. It basically meets the effectiveness and security requirements of image encryption.

Cryptography is done in two ways: (i) symmetric (private) key cryptography, where only single key is used to do encryption and decryption, (ii) asymmetric (public) key cryptography, where one key is used to do encryption and other key is used to do decryption. In [4], the author proposed a method, SD-AEI, for image encryption, which is an upgraded module for SD-EI combined image encryption technique and basically has three stages: 1) In first stage, each pixel of image is converted to its equivalent eight bit binary number and in that eight bit number, the number of bits, which are equal to the length of password are rotated and then reversed; 2) In second stage, extended hill cipher technique is applied by using involutory matrix, which is generated by same password used in second stage of encryption to make it more secure; 3) In third stage, the whole image file is randomized multiple number of times using Modified MSA Randomization encryption technique and the randomization is dependent on an unique number, which is generated from the password provided for encryption.

In [5] a novel scheme for optical information hiding (encryption) of two-dimensional images by combining image scrambling techniques in fractional Fourier domains is proposed. The image is initially random shifted using the jigsaw transform algorithm, and then a pixel scrambling technique based on the Arnold transform (ART) is applied. Then, the scrambled image is iteratively encrypted in the fractional Fourier domains using randomly chosen fractional orders. The parameters of the architecture, including the jigsaw permutations indices, Arnold frequencies, and fractional Fourier orders, form a huge key space enhancing the security level of the proposed encryption system. Optical implementations are discussed and numerical simulation results are presented to demonstrate the flexibility and robustness of the method [6] gives an Enhancement to Image security in which Data bits from textual message are encrypted through key to some suitable nonlinear pixel and bit positions about the entire image. As a result, a watermarked image is produced. After that three different image shares using any two components of R, G and B of entire watermarked image are formed. The key is also divided into three different logical blocks by digits. By combining any two blocks of key, key shares are formed and are assigned to image shares. Out of those three shares, only addition of any two is able to make the full image or key. At the

decryption end through appropriate arrangement of shares of key and image, make possible to retrieve hidden data bits from watermarked image and reform into its original content

In 1999, J.-C. Yen and J.-I. Guo proposed a novel image encryption algorithm called BRIE (Bit Recirculation Image Encryption). [7] points out that BRIE is not secure enough from strict cryptographic viewpoint. It has been found that some defects exist in BRIE, and a know/chosen-plaintext attack can break BRIE with only one know/chosen plain-image. Experiments were performed to verify the defects of BRIE and the feasibility of the attack.

Chaotic maps have been widely used in image encryption for their extreme sensitivity to tiny changes of initial conditions. The chaos based algorithms have suggested a new and efficient way to deal with the problem of fast and highly secure image encryption. In [8] the chaotic features of traditional trigonometric function is analyzed and a new chaotic image encryption algorithm is proposed. The algorithm uses a chaotic map based on trigonometric function as a mask to confuse the plain-image and employs several different types of operations to shuffle the image pixels according to the outcome of another chaotic map. Thereby it significantly increases the resistance to statistical and differential attacks. The results of experiment, statistical analysis, correlation coefficient analysis and key sensitivity tests show that the algorithm is of great security and practicability.

Advanced Encryption Standard (AES) is a well known block cipher that has several advantages in data encryption. However, it is not suitable for real-time applications. In [9], a modification to the Advanced Encryption Standard (MAES) is presented and analyzed to reflect a high level security and better image encryption. The modification is done by adjusting the ShiftRow Transformation. Detailed results in terms of security analysis and implementation are given. Experimental results verify and prove that the proposed modification to image cryptosystem is highly secure from the cryptographic viewpoint. The results also prove that with a comparison to original AES encryption algorithm the modified algorithm gives better encryption results in terms of security against statistical attacks

A new linear transform for scrambling images is proposed in [10]. The forward transform scrambles the image and the inverse transform unscrambles the image. Transformation matrices for both scalar and blocked cases are defined. Recursive and non-recursive algorithms based on the new transform are also given. The experimental results show that the positions of the pixels are strongly irregularized using the transform. Unscrambling using a wrong key fails and results in an unintelligible image which cannot be recognized.

A new digital image scrambling method based on Fibonacci numbers is presented[11]. The uniformity and periodicity of the scrambling transformation are discussed. The scrambling transformation has the following advantages: (1) Encoding and decoding is very simple and they can be applied in real-time situations. (2) The scrambling effect is very good, the information of the image is re-distributed randomly across the whole image.(3) The method can endure common image attacks, such as compression, noise and loss of data packet

The properties and periodicity of the two dimensional Fibonacci transformation of digital images are discussed[12] on the background of image information security problem research, and a new computation method and an accurate formula of whose period are also given , its application in digital image scrambling is illustrated with examples.

In [13] a new spatial domain image scrambling method is proposed which is based on Fibonacci and Lucas series, that can be used in various spatial domain image processing techniques of data hiding and secret communications such as Steganography and Watermarking and can increase the security of the hidden message

A new scrambling algorithm based on random shuffling strategy is proposed in [14], which can scramble non equilateral image and has a low cost to build coordinate shifting path. The algorithm has a good one time scrambling performance. It can be used to scramble or recover image in real time and can also resist the JPEG compression attacks. Experiments show the scrambling method validity in scrambling or recovering non equilateral image and robustness in enduring erasing, cropping and JPEG compressing attacks

II. PERFECT SHUFFLE

A shuffle is a permutation of n elements. Clearly, each shuffle produces a new permutation or returns to a previous one. Therefore at some point the process would return to the original order. However, there are ***n!*** permutations of a set of ***n*** elements. The perfect shuffle is a non-random process. A perfect shuffle deck of cards with an even number of cards is accomplished by splitting the deck of cards into an upper half and a lower half and then interlacing the cards alternately, one at a time from each half of the deck.
There are two ways to perfectly shuffle a deck of 2n cards. Both methods cut the deck in half and interlace perfectly. The out shuffle O leaves the original top card on top. The in shuffle I leaves the original top card second from the top.

In this paper, Out shuffle (O renamed to S1) and In shuffle (I renamed to S2) both are applied to Digital Images. The different factors for the size of a digital image($2^k X 2^k$) are used for generating different combinations of patterns. Every pattern considered has 2^m rows and 2^n columns in shuffle S1, which are interchanged in shuffle S2 (2^n rows and 2^m columns), where k= m+n.

To explain how Shuffle S1 and Shuffle S2 are applied to a digital Image, let us consider Shuffle S1.
Let the image size be 2^k X 2^k(total number of pixels in an image M^2). As we know a digital image is a matrix having rows and columns. The pixels need to be shuffled in a certain order inside the matrix. Based on the size of the digital image , there are different factors for e.g. For an image size of 256X256 factors are 2,4,8,16,32,64,128. To arrange all the pixels using perfect shuffle(S1) we could consider a rectangular block of size (rows X columns = Total Size of the image), where rows and columns are chosen in such a way that a product of the two factors results in total size of the image. For e.g.(2X128 = 256 , 4X64 = 256) in which the rectangular

block will have 2 (2^1) rows and 128 (2^7) columns. In this rectangular block the pixel positions are written serially row wise and read column wise. Interchanging the two factors and rearranging the rectangular block according to the two factors results in second type of shuffle(S2) for e.g. (128 X2 =256 , 64X4=256) in which the rectangular block will have 128 (2^7) columns and 2 (2^1) rows.

In Perfect shuffle S1 let 2^m be the number of rows and 2^n be the number of columns, where k= m+n. The Write arrow in Figure 1.1 and 1.2 indicates the direction of writing the pixel positions from the digital image and the read arrow indicates the direction of reading the pixel positions of the digital image to apply the Perfect shuffle S1 to a digital Image.

Case I: m=1, n= n,

Write → 2^n

Read ↓ 2^1

	1	2	3	.	.	.	2^n
1	1	2	3	.	.	.	2^n
2	2^n+1	2^n+2	2^n+3	.	.	.	2^{n+1}

Figure 1.1 Rectangular Block of Shuffle S1 for Case I

Case II

Let us consider a general case in which m=m and n=n for shuffle S1.

Write → 2^n

Read ↓ 2^m

	1	2	3	.	.	.	2^n
1	1	2	3	.	.	.	2^n
2	2^n +1	2^n +2	2^n +3	.	.	.	2.2^n
.	.	.	.	.	.	.	.
.	.	.	.	.	.	.	.
2^m-1	.	.	.	.	.	.	$(2^m-1)*2^n$
2^m	$(2^m-1)*2^n$ +1	$(2^m-1)*2^n$ +2	$(2^m-1)*2^n$ +3	.	.	.	2^{n+m}

Figure 1.2 Rectangular Block of Shuffle S1 for Case II

In Perfect shuffle S2 let 2^n be the number of rows and 2^m be the number of columns, where k= m+n. The Write arrow in Figure 2.1and 2.2 indicates the direction of writing the pixel positions from the digital image and the read arrow indicates the direction of reading the pixel positions of the digital image to apply the Perfect shuffle S2 to a digital Image.

Case I : m=1 , and n=n

Write → 2^1

Read ↓ 2^n

	1	2
1	1	2
2	3	4
3	5	6
.	.	.
.	.	.
.	.	.
2^n	2^n	2^{n+1}

Figure 2.1 Rectangular Block of Shuffle S2 for Case I

Case II Let us consider a general case in which m=m and n=n for shuffle S2.

Write → 2^m

	1	2	3	.	.	2^m-1	2^m
1	1	2	3	.	.	2^m-1	2^m
2	2^m+1	2^m+2	2^m+3	.	.	2.2^m-1	2.2^m

	3	2.2^m+1	2.2^m+2	2.2^m+3	.	.	$2.\ 2^m-1$	3.2^m
2^n	.	.	.	.	.	.	.	.
Read	.	.	.	.	.	.	.	.
	2^n-1	$(2^n-2).\ 2^m+1$	.	.	.	.	.	$2^n-1.\ 2^m$
	2^n	$(2^n-1).\ 2^m+1$	.	.	.	.	$2^{n+m}-1$	2^{n+m}

Figure 2.2 Rectangular Block of Shuffle S2 for Case II

Let us consider an image of size 1024X1024 and Shuffle S1 when applied to an image of size 1024 X 1024, The factors 2 and 512 are used to generate the rectangular block . The rectangular block has 2^1 rows and 2^9 columns as shown in the Figure 3.1 below

(Pattern 2X512)

2^1	2^9						
	1	2	3	.	.	.	2^9
1	1	2	3	.	.	.	512
2	513	514	515	.	.	.	1024

Figure 3.1. Factors 2 and 512 (2^1 and 2^9) used to generate the rectangular block for shuffle S1

Another pattern using 8 and 128 as the factors is shown as an example for shuffle S1 in Figure 3.2

(Pattern 8X128)

2^3	2^7						
	1	2	3	.	.	.	2^n
1	1	2	3	.	.	.	128
2	129	130	131	.	.	.	256
.	.	.	.	.	.	.	.
.	.	.	.	.	.	.	.
2^m-1	.	.	.	.	.	.	896
2^m	897	898	899	.	.	.	1024

Figure 3.2. Factors 8 and 128 (2^3 and 2^7) used to generate the rectangular block for shuffle S1

The above two Patterns (Factors 2X512 and 8X128) are shown for shuffle S2, These factors needs to be interchanged i.e. (512X2 and 128X8). The rectangular block obtained by using 512X2 is shown in Figure 4.1 and rectangular block using 128X8 is shown in Figure 4.2

(Pattern 512X2)

	2^1	
	1	2
1	1	2
2	3	4
3	5	6
2^9 .	.	.
.	.	.
.	.	.
2^n	1023	1024

Figure 4.1. Factors 512 and 2 (2^9 and 2^1) used to generate the rectangular block for shuffle S2

(Pattern 128X8)

2^7	2^3						
	1	2	3	.	.	2^m-1	2^3

1	**1**	**2**	**3**	**.**	**.**	**7**	**8**
2	**9**	**10**	**11**	**.**	**.**	**15**	**16**
3	**17**	**18**	**19**	**.**	**.**	**23**	**24**
.	**.**	**.**	**.**	**.**	**.**	**.**	**.**
.	**.**	**.**	**.**	**.**	**.**	**.**	**.**
2^n -1	**1007**	**.**	**.**	**.**	**.**	**.**	**1015**
2^n	**1016**	**.**	**.**	**.**	**.**	**1023**	**1024**

Figure 4.2. Factors 128 and 8 (2^7 and 2^3) used to generate the rectangular block for shuffle S2

III. EXPERIMENTAL RESULTS

For Experimental purpose, Lena grayscale image of size 1024 X 1024 was used. Perfect Shuffle S1 and S2 were applied on the image for 10 iterations. The output obtained for Shuffle S1 and Shuffle S2 is shown in Figure 5.1 and 5.2. The factors used for S1 and S2 are 2 and 512. The #number indicates the output obtained for the successive iterations. For e.g #1 indicated the output obtained for Iteration No 1.

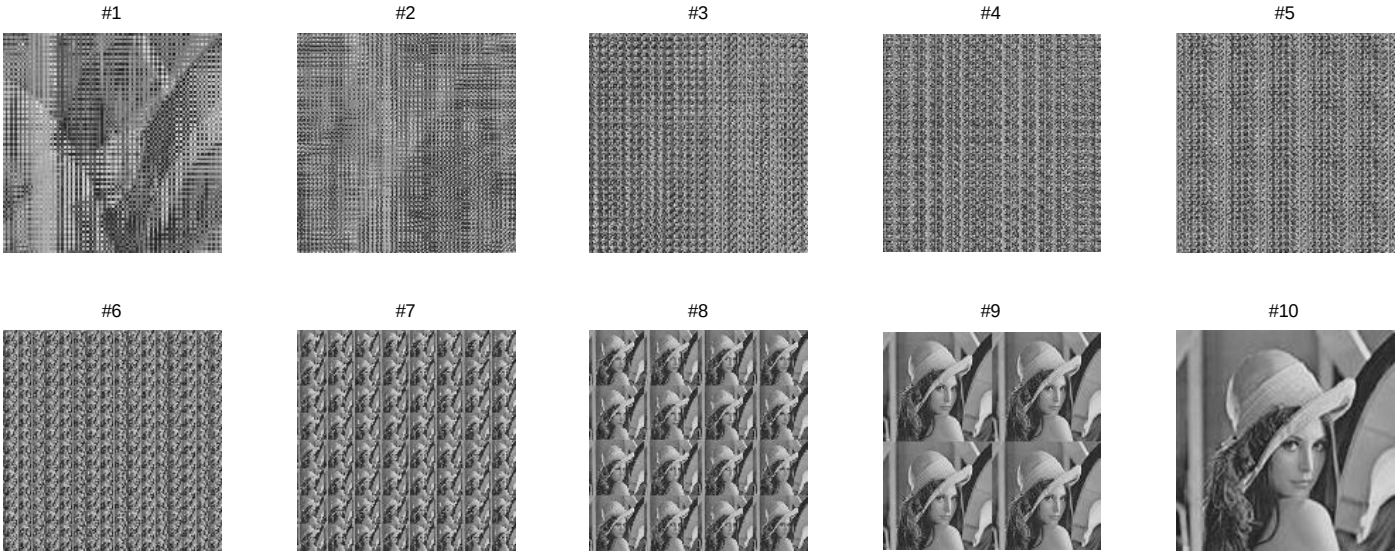

Figure 5.1 Perfect Shuffle S1 and pattern 2X512 (Iteration Number 1 to 10)

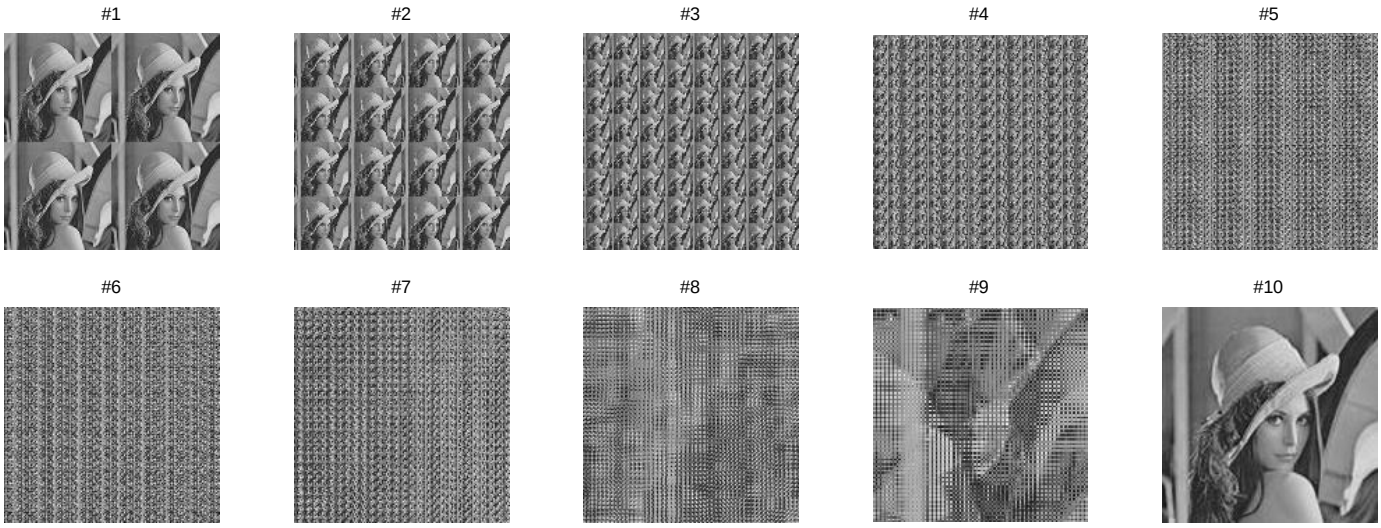

Figure 5.2 Perfect Shuffle S2 and pattern 512X2 (Iteration Number 1 to 10)

As seen from figure 5.1 and 5.2, The application of Perfect Shuffle results in down sampling effect on a digital Image. In Figure 5.1 Perfect shuffle S1, The number of iterations considered were 10 . The 10^{th} iteration results in the original image back. The output obtained in S2 is just the reverse of the output obtained in S1.

IV. Analysis of output obtained in Shuffle S1 and Shuffle S2.

To analyze the output obtained in shuffle S1 and Shuffle S2, i.e the number of Lena's generated at a particular iteration can be estimated based on the factors / pattern used in shuffle S1 and S2. For e.g Factors of 1024 **(**2,4,8,16,32,64,128,256,512,1024). Based on the above factors of 1024, the combination of these factors used for 1024 are (2X512, 4X256, 8X128, 16X64 and 32X32).
Let us number the output obtained in Figure 5.1 from #1 to #10. In the last iteration (10^{th}) it can be seen that we obtain the original image. In the 9^{th} Iteration the original image is down sampled into 4, in the 8^{th} iteration it is down sampled to 16 and so on. Every $(n-1)^{th}$ iteration results in down sampling of the image 4 times the images down sampled in the n^{th} iteration. This can be used to estimate the number of lena's that will be generated due to down sampling for any other pattern considered for the image size of 1024X1024.

For e.g. Let us try to find out the number of lena's that will be generated for Pattern 4X256 in shuffle S1. This pattern can be written in power of 2.

$$4= 2^2 \text{ and } 256 = 2^8$$

As the image size considered is 1024 which is 2^{10}. The maximum number of iterations can be limited to 10. For pattern 2^2x2^8. The Power of 2 for the number of rows in the rectangular block will be the first image to be generated. The #2 will be the first output figure that will be obtained for iteration number 1, for the next iteration we can go in a circular sequence and #4 will be the output image obtained. An increment of two will result in the output of successive iterations. For this pattern we get the original image after 4 iterations. The circular sequence followed is shown below in Figure No 6.1

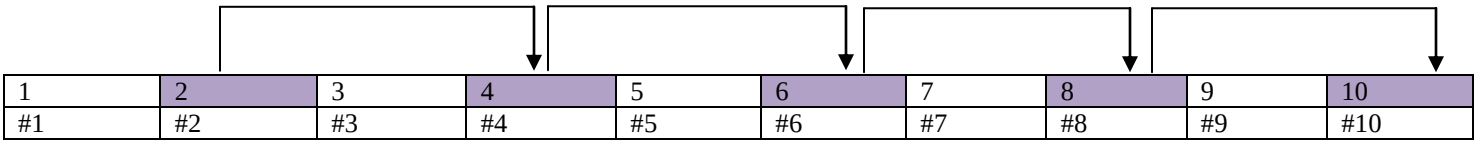

Figure 6.1 Circular sequence followed for 4X256 Pattern

The same procedure when applied to all the different patterns we obtain the table as shown below for Shuffle S1 and S2.

Table 1.1. Experimental Results obtained for Perfect Shuffle S1 and Shuffle S2 for 10 iterations.

Type of Shuffle		Iterations / Power of 2	1	2	3	4	5	6	7	8	9	0
S1	2X512	1	#1	#2	#3	#4	#5	#6	#7	#8	#9	#10
	No of Lena's		65,536	16,384	4096	1024	512	256	64	16	4	1
S2	512x2	9	#9	#8	#7	#6	#5	#4	#3	#2	#1	# 10
	No of Lena's		4	16	64	256	512	1024	4096	16384	65536	1
S1	4x256	2	# 2	#4	#6	#8	#10					
	No of Lena's		16,384	1024	256	16	1					
S2	256x4	8	#8	#6	#4	#2	#10					
	No of Lena's		16	256	1024	16384	1					
S1	8x128	3	# 3	# 6	# 9	# 2	# 5	# 8	# 1	# 4	# 7	# 10
	No of Lena's		4096	256	4	16,384	512	16	65,536	1024	64	1
S2	128x8	7	#7	#4	#1	#8	#5	#2	#9	#6	#3	#10
	No of Lena's		64	1024	65536	16	512	16384	4	256	4096	1
S1	16X64	4	# 4	# 8	# 2	# 6	# 10					
	No of Lena's		1024	16	16,384	256	1					
S2	64x16	6	#6	#2	#8	#4	#10					
	No of Lena's		256	16,384	16	1024	1					
S1	32X32	5	# 5	# 10								

	No of Lena's		512	1								
S2	32X32	5	# 5	# 10								
	No of Lena's		512	1								

V. CONCLUSION

In this paper, while studying the properties of Perfect shuffling for the purpose of scrambling, following observations have been made

1) **Down Sampling Effect**: One of the most interesting observation made was the down sampling effect which occurs on the image when perfect shuffle is applied to it. This down sampling effect results in particular number of images of the original image as can be seen in the result, we have studied this effect and have given a relation as to how to correlate the number of images generated based on the factors used for Perfect shuffling.
2) **Repetition of the original image:** As it can be seen from Table No 1.1, Based on the pattern used, a circular sequence when applied to the Powers of 2, we get the original image back after certain number of iterations.
3) **No of Lena's Generated:** From experimental results it can be very easily found out the number of Lena's generated if we start from the Original image in the last iteration. For e.g 2X512 Pattern for Perfect Shuffle S1.
4) **S1 and S2 are complement to each other:** The results obtained in Figure 5.1 and 5.2 clearly indicates that perfect shuffle S1 and S2 are complement of each other.
5) **Scrambling:** The Main objective of studying Perfect Shuffle was its use for Image scrambling, Table 1.1 can be used as a reference for Image scrambling , where we can choose a particular pattern from scrambling and limit the number of iterations. For eg. In 2X512 pattern the Iteration Number #1, #2,#3,#4, #5 and #6 can be very well used for scrambling purpose, as the number of lena's generated are huge in number, which are not perceptible to a human eye.

REFERENCES

[1] Yicong Zhou, Karen Panetta, Sos Agaian, "An Image Scrambling Algorithm using Parameter Based M-Sequences", *in Proc* International Conference on Machine Learning and Cybernetics, 2008. Pp. 3695-3698.

[2] Xiaomin Wang, Jiashu Zhang, "An Image Scrambling Encryption Using Chaos Controlled Poker Shuffle Operation", *in Proc* International Symposium on Biometrics and Security Technologies, 2008. ISBAST 2008. pp. 1-6.

[3] Zhenwei Shang Honge Ren Jian Zhang, "A Block Location Scrambling Algorithm of Digital Image Based on Arnold Transformation", *in Proc* 9th International Conference for Young Computer Scientists 2008, pp 2942-2947

[4] Somdip Dey, "SD-AEI: An Advanced Encryption Technique For Images" , An Advanced Combined Encryption Technique For Encrypting Images Using Randomized Byte Manipulation" , *in Proc* Second International Conference on Digital Information Processing and Communications (ICDIPC).pp. 68-73 , 2012.

[5] Shi Liuy and John T. Sheridan, "Optical Information Hiding By Combining Image Scrambling Techniques In Fractional Fourier Domains", ISSC 2011, Trinity College Dublin, June 23-24.

[6] Sabyasachi Samanta, Saurabh Dutta, Goutam Sanyal, "An Enhancement of Security of Image using Permutation of RGB-Components", "*in Proc* Third International Conference on Conference on Electronics Computer Technology (ICECT 2011)", 8--10 April, pp. v2-404-v2-408

[7] Shujun Li , Xuan Zheng, "On the Security of an Image Encryption Method" *in Proc* International Conference on Image Processing ICIP'2002, pp II-925 - II-928 vol.2 IEEE

[8] Chenghang Yu, Baojun Zhang, Xiang Ruan, "The Chaotic Feature of Trigonometric Function and Its Use for Image Encryption" *in Proc* Eighth International Conference on Fuzzy Systems and Knowledge Discovery (FSKD), 2011. pp 390-395.

[9] Seyed Hossein Kamali, Reza Shakerian, Maysam Hedayati, Mohsen Rahmani, "A New Modified Version of Advanced Encryption Standard Based Algorithm for Image Encryption", *in Proc* International Conference on Electronics and Information Engineering (ICEIE 2010), Volume 1, pp V1-141-145.

[10] Ravankar,A.A., Sedukhin, S.G., "Image Scrambling Based on a New Linear Transform", *in Proc* International Conference on Multimedia Technology (ICMT), 2011

[11] Jiancheng Zou, Rabab K. Ward, Dongxu Qi, "A New Digital Image Scrambling Method based on Fibonacci Numbers" ,*in Proc*. IEEE ISCAS 2004, vol. III, pp. 965 – 968.

[12] W. Zou, J. Huang and C. Zhou, "Digital Image Scrambling Technology Based On Two Dimension Fibonacci Transformation And Its Periodicity", Third International symposium on Information Science and Engineering, (2010) December 24-26, Shanghai: China.

[13] Minati Mishra, Priyadarsini Mishra, M.C. Adhikary And Sunit Kumar, "Image Encryption Using Fibonacci-Lucas Transformation", International Journal on Cryptography and Information Security (IJCIS),Vol.2, No.3, September 2012.

[14] Shao Z. Qin, B. Liu J. Qin and H Li., "Image Scrambling Algorithm Based on Random Shuffling Strategy", in ICIEA 2008, pp. 2278-2283.

AUTHORS

First Author – Dr. H.B.Kekre, PhD in System Identification, MPSTME, NMIMS and hbkekre@yahoo.com.
Second Author – Dr. Tanuja Sarode, PhD in Vector Quantization, TSEC and tanuja_0123@gmail.com
Third Author – Ms. Pallavi N Halarnkar, ME Computer, MPSTME, NMIMS and Pallavi.halarnkar@gmail.com.
Correspondence Author – – Ms. Pallavi N Halarnkar, Pallavi.halarnkar@gmail.com, 09699865323