ISSN (Online) : 2278-1021
ISSN (Print) : 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 3, Issue 2, February 2014

Image Scrambling Using R-Prime Shuffle on Image and Image Blocks

H.B.Kekre[1], Tanuja Sarode[2], Pallavi Halarnkar[3]

Sr. Professor, Computer Engineering, MPSTME, Mumbai, India [1]

Associate. Professor, Computer Engineering, TSEC, Mumbai, India [2]

PhD Research Scholar, Computer Engineering, MPSTME, Mumbai, India [3]

Abstract: With the Rapid development in technology, huge amount of information is transmitted across the network, the information is not limited to simple data but also includes multimedia information like digital images. Security of digital images is also of high concern. In this paper, we have extended R-Prime shuffle technique over the blocks of image. The method is applied to different block sizes in the image and also compared to the earlier R-Prime shuffle technique of Image Scrambling.

Keywords: Encryption, Decryption, Scrambling, Shuffling

I. INTRODUCTION

Nowadays Digital Images have become a major source of Information. This information when transmitted across the network, security of the same becomes important. Image scrambling technique are been used for providing security to digital Images. A number of methods have been proposed to calculate the periodicity of Arnold Transformation. In [1] the traditional Arnold Transformation is improved by adding two parameter a and b. To generate parameter sequences , logistic map has been used. Arnold transformation is been applied on each block with different parameters. The method gives good encryption effects. It also has a very large key space and key sensitivity.

An improved Image scrambling technique was proposed in [2]. When the image was scrambled in spatial domain, image unchangeable coefficient rule in Discrete Cosine Transform(DCT) and Wavelet Transformation was proved. Based on the constructed composite chaotic iterative dynamic system whose invariant distribution density was one, and in order to initialize for composite chaotic iterative dynamic system, it put forward two functions using image scramble constant as input parameter. Then a fragile and adaptive image scrambling algorithm and two new scrambling evaluative parameter were introduced called as similar degree and anti-tamper radius. The experimental results showed that the original image could be extracted without any accessional information. The technique was sensitive to all kinds of attacks. The anti tamper radius obtained was larger than the current scrambling techniques.

To overcome the drawbacks of the traditional queue transformation a improved method is proposed in [3]. This proposed variation only needs a single step instead of two steps to complete the scrambling process. The reference point can change in every stage. If intruder needs to decode the scrambled image, the step, the reference point and the direction should all be known for descrambling it.

A Image Scrambling method is proposed [4] based on a folding transform with folding matrix which is orthogonal and enables to fold images either up down or left-right. When an image is folded through this way repeatedly, it results in scrambling. The results show that the image scrambling algorithm has effective hiding ability with small computation burden as well as wide adaptability to images with different scales, and also robust under common attacks.

Sudoku Puzzle is used as a method for Image scrambling in [5]. The special property that every number from 1 to N appears only once in each row or column in an N*N Sudoku puzzle, a 1-1 relationship is setup between two Sudoku puzzles and these two Sudoku puzzles will be used to map the original images to a scrambled one. The method is applied at both pixel as well as bit levels in order to increase the security. Due to the large numbers of the bases (pre-filled units in the Sudoku puzzle), this algorithm significantly improves the security of the information included in the scrambled image. The original image cannot be restored without right keys.

A new scrambling technique, parameter based M-sequencing is proposed in [6] in addition to this a parametric based M-sequencing method is also proposed. The user can change the security keys 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 method can be applied to grayscale as well as color images in one step. It also shows good performance in the image attacks such as filters (data loss) and noise attacks.

Poker shuffle method is also used for image scrambling, which is controlled dynamically by chaotic system is given in [7]. Compared with algebraic permutations and chaotic permutations, the method has properties of nonlinearity, non-analytic formula and large key space. The method can also deal with non –square images.

An image scrambling technique for Binary images has been proposed in [8] by using the concept of bipartite graph and its degree along with applying the characteristic which the variance and mean square deviation can measure the discrete degree of nodes according to the pixels characteristic of the binary image. The method involves diving the image into same size blocks constructing the bipartite graph of every block, calculating its degree, building up a real sequence, analyzing the discrete degree of the sequence by applying the variance and mean square deviation, and, finally, deciding the scrambling degree of the binary image.

Image encryption done on pixels is been proposed in [9]. Firstly the image is scrambled and to increase more security concept of watermark has been introduced to make decoding difficult. At last, choosing a camouflaged image to vision or the pixels of the true image, gives the final encrypted image. The key parameters are encrypted by Elliptic Curve Cryptography (ECC). The algorithm poses a large key space and the time needed for encrypting the interactive image tends to +∞.

A New Linear transform is used for Image scrambling in [10]. The forward transform is used for scrambling and its inverse is used for descrambling the scrambled 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 pixel positions are strongly irregularized using the method. Unscrambling using a wrong key fails and results in an unintelligible image which cannot be recognized.

Image scrambling based on Fibonacci transformation is proposed in [11]. The scrambling transformation discusses the uniformity and periodicity. 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 in [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 for 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 scrambling performance. The method resists JPEG compression attacks. Experiments results show that scrambling method validity in scrambling or recovering non equilateral image and robustness in enduring erasing, cropping and JPEG compressing attacks.

II. R-PRIME SHUFFLE TECHNIQUE

Spatial alignment of Digital images is of importance to many applications one such application is Image Quality. The pixels in a digital image has correlation between them. Image correlation is most widely used technique in Image processing domain. This technique is also called as Template Matching which is used to match the similarity between any two parts of the image. It can also be used to locate a object in a digital image. In this paper, Cross correlation using FFT is used as a measure of similarity between two Rows/Columns in a Digital Image.

R-Prime called as Relative Prime Shuffling technique in which a relative prime is a prime in which there are no common factors except 1. To choose a Relative Prime number for shuffling from the set, correlation concept is used. The Lowest correlation obtained between the different Relative Primes numbers(Row/Column positions) and 1st row/column is used as a key for carrying out the shuffling.[15]

A. *Encryption*

- The method used for Encryption is as follows
- Read the image
- Convert it to grayscale
- Based on the Size of the Image(MXN), find out all the Relative Prime Numbers and save them in a set S
- Using set S to find the correlation of the First row with remaining rows (positions w.r.t elements present in the set).
- Consider the lowest correlation as the key to shuffle the rows in the image
- Continue till all the positions in the image are considered
- Save the Relative Primes Numbers as a key considered for Row Shuffling
- Repeat the same procedure for Column shuffling

B. *Decryption*

- Use the Saved key for Row and Column Shuffling to get the Original Image back
- Use the column Relative Prime and rearrange the columns, this will give row shuffled image
- Using this row shuffled image and the key for row relative prime rearrange the rows which will give you Original Image back.
- Continue till all the positions in the image are rearranged

III. R-PRIME BLOCK SHUFFLE TECHNIQUE

R-Prime Block called as Relative Prime Block Shuffling technique. In this the image is divided into non overlapping blocks. For every block the Lowest correlation obtained between the different Relative Primes numbers (Row/Column positions) and 1st row/column in every block is used as a key for carrying out the shuffling in each block.

A. Encryption

The method used for Encryption is as follows

- Read the image
- Convert it to grayscale
- Divide the image in to non –overlapping blocks
- Based on the Size of the block, find out all the Relative Prime Numbers and save them in a set S
- Using set S to find the correlation of the First row with remaining rows (positions w.r.t elements present in the set) in the block.
- Consider the lowest correlation as the key to shuffle the rows in the block
- Consider the lowest correlation as the key to shuffle the columns in the block
- Continue till all the positions in the block are considered
- Repeat the step 4 to 8 till all the blocks in the image are considered
- Find out the first block correlation with remaining blocks in the image, the block having the lowest correlation is placed next to the first block and so on.
- Save the Relative Primes Numbers of rows and columns in all the blocks and the block no for the entire image as a key considered for R-Prime block shuffling

B. Decryption

- *Use* the Saved key for Row and Column Shuffling of all the blocks and the block number to get the Original Image back
- Use the block no to rearrange the blocks in the scrambled image
- Use column Relative Prime and rearrange the columns in the block, this will give row shuffled image
- Using this row shuffled image and the key for row relative prime rearrange the rows which will give you Original image.
- Repeat step 3-4 to get the original image back

IV. EXPERIMENTAL RESULTS

For Experimental purpose five images of Lena, Mountain, forest, lotus, and fruits of size 256X256 were used. The test was carried out on grayscale images however this method is extensible over 24-bit color images. The method is not limited to the type or extension of a digital image. Figure 1 (a)–(b) shows the correlation plot of first row with the remaining rows in the image and first column with remaining columns in the image for R-Prime Shuffling. Figure 2 (a)–(b) shows the correlation plot of first row with the remaining rows in the 3rd block of size(8X8) and first column with remaining columns in the 3rd block of size(8X8) for R-Prime Block Shuffling. Figure 3(a)-(d) shows the original image, Scrambled image after shuffling the rows, scrambled image after shuffling the columns of the row scrambled image, and finally the decrypted image obtained for R-Prime Shuffling technique.

Figure 4(a)-(d), 5(a)-(d), 6(a)-(d) shows the original image, Scrambled image after shuffling the rows and columns in (8X8, 16X16 and 32X32) blocks of the original image, scrambled image after shuffling the blocks of the row and column block scrambled image, and finally the decrypted image obtained for R-Prime Block Shuffling technique.

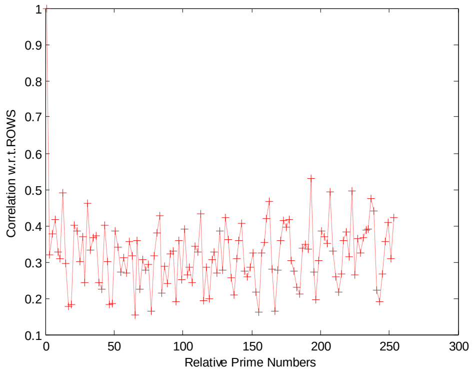

Fig. 1(a) Correlation of All the Relative Prime(Row Positions) with Row 1 using R-Prime Shuffle

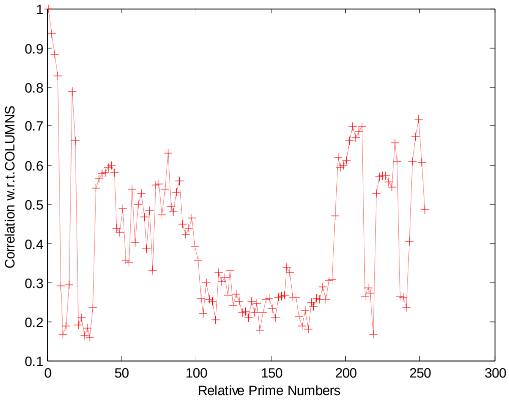

Fig. 1(b) Correlation of All the Relative Prime(Column Positions) with Column 1 using R-Prime shuffle

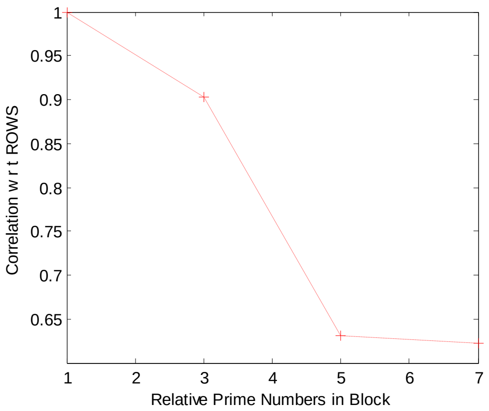

Fig. 2(a) Correlation of All the Relative Prime(Row Positions) with Row 1 in Block 3 (Block Size 8X8) using R-Prime Block shuffling

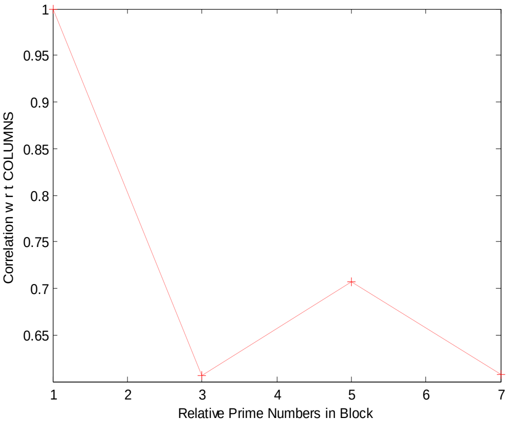

Fig. 2(b) Correlation of All the Relative Prime(Column Positions) with Column 1 in Block 3 (Block Size 8X8) using R-Prime Block shuffling

A. R-PRIME SHUFFLING

Fig 3(a) Original Image

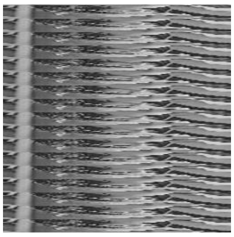

Fig 3(b) Row scrambled Image

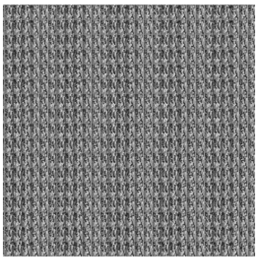

Fig 3(c) Row and Column Scrambled Image

Fig 3(d) Descrambled Image

B. R-PRIME BLOCK SHUFFLING

Fig 4(a) Original Image

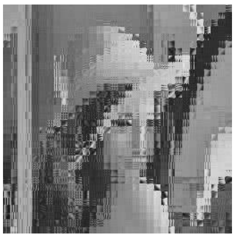

Fig 4(b) Row scrambled Image Block size(8X8)

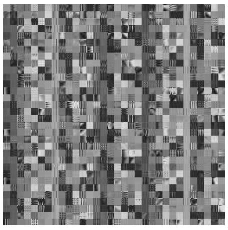

Fig 4(c) Row and Column Scrambled Image

Fig 4(d) Descrambled Image

Fig 5(a) Original Image

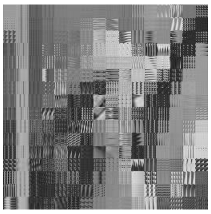

Fig 5(b) Row scrambled ImageBlock size(16X16)

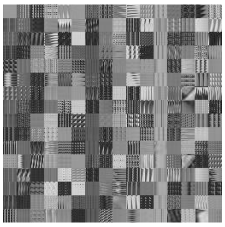

Fig 5(c) Row and Column Scrambled Image

Fig 5(d) Descrambled Image

Fig 6(a) Original Image

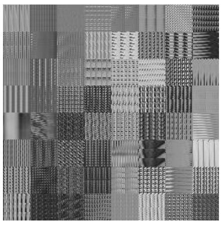

Fig 6(b) Row scrambled ImageBlock size(32X32)

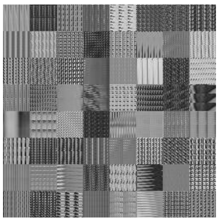

Fig 6(c) Row and Column Scrambled Image

Fig 6(d) Descrambled Image

TABLE I
VALUES OF AVERAGE ROW AND COLUMN CORRELATION IN ORIGINAL AND SCRAMBLED IMAGE, AND TIME TAKEN FOR R-PRIME SHUFFLE

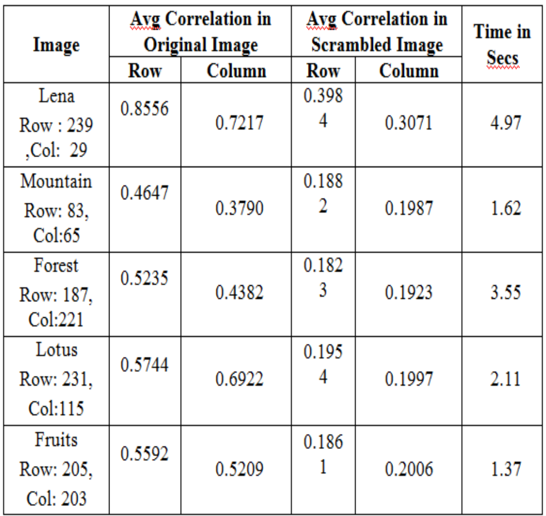

Image	Avg Correlation in Original Image		Avg Correlation in Scrambled Image		Time in Secs
	Row	Column	Row	Column	
Lena Row : 239 ,Col: 29	0.8556	0.7217	0.3984	0.3071	4.97
Mountain Row: 83, Col:65	0.4647	0.3790	0.1882	0.1987	1.62
Forest Row: 187, Col:221	0.5235	0.4382	0.1823	0.1923	3.55
Lotus Row: 231, Col:115	0.5744	0.6922	0.1954	0.1997	2.11
Fruits Row: 205, Col: 203	0.5592	0.5209	0.1861	0.2006	1.37

TABLE II
VALUES OF AVERAGE ROW AND COLUMN CORRELATION IN ORIGINAL AND SCRAMBLED IMAGE, AND TIME TAKEN FOR R-PRIME BLOCK SHUFFLING

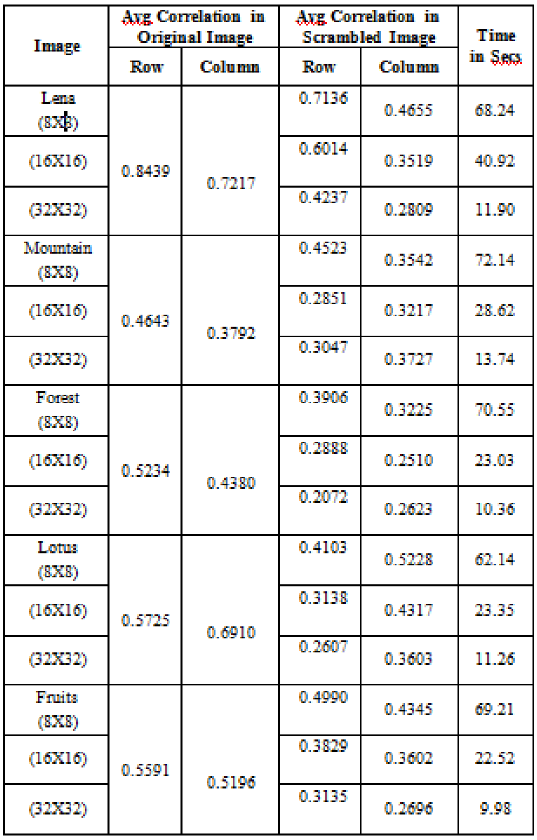

Image	Avg Correlation in Original Image		Avg Correlation in Scrambled Image		Time in Secs
	Row	Column	Row	Column	
Lena (8X8)	0.8439	0.7217	0.7136	0.4655	68.24
(16X16)			0.6014	0.3519	40.92
(32X32)			0.4237	0.2809	11.90
Mountain (8X8)	0.4643	0.3792	0.4523	0.3542	72.14
(16X16)			0.2851	0.3217	28.62
(32X32)			0.3047	0.3727	13.74
Forest (8X8)	0.5234	0.4380	0.3906	0.3225	70.55
(16X16)			0.2888	0.2510	23.03
(32X32)			0.2072	0.2623	10.36
Lotus (8X8)	0.5725	0.6910	0.4103	0.5228	62.14
(16X16)			0.3138	0.4317	23.35
(32X32)			0.2607	0.3603	11.26
Fruits (8X8)	0.5591	0.5196	0.4990	0.4345	69.21
(16X16)			0.3829	0.3602	22.52
(32X32)			0.3135	0.2696	9.98

V. CONCLUSION

R-Prime shuffling technique is a simple yet powerful technique which can be used for image scrambling. In this paper we have used R-prime shuffling on the Blocks of the Digital Image, to increase the security of the image data. The technique is robust as different Relative Prime numbers are used for row and column shuffling for every block. A combination of all the R-primes from each block with respect to rows and columns can be used as a key for Image Scrambling.

From the experimental results it can be observed that there is a reduction of approximately 50% to 60% in the correlation between rows and columns of the encrypted image in R-Prime shuffling technique applied to full image and to the blocks. From time taken it can be concluded that the technique takes few seconds for the encryption process. It does not involve a high time complexity. This algorithm does perfect scrambling as MSE between the original and descrambled image is zero.

REFERENCES

[1] 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.

[2] Shengbing Che, Zuguo Che and Bin Ma, "An Improved Image Scrambling Algorithm", in Proc Second International Conference on Genetic and Evolutionary Computing,2008, pp. 495-499.

[3] Hai-Yan Zhang, "A New Image Scrambling Algorithm Based On Queue Transformation", in Proc Sixth International Conference on Machine Learning and Cybernetics, Hong Kong, 19-22 August 2007. pp. 1526-1530.

[4] Sanfu Wang, Yuying Zheng and Zhongshe Gao, "A New Image Scrambling Method through Folding Transform" in Proc International Conference on Computer Application and System Modeling (ICCASM 2010),volume 2 , pp. 395-399.

[5] Yang Zou, Xiaolin Tian, Shaowei Xia, Yali Song, "A Novel Image Scrambling Algorithm Based On Sudoku Puzzle", in proc 4th International Congress on Image and Signal Processing 2011, pp. 737-740.

[6] Yicong Zhou, Karen Panetta, Sos Agaian, " An Image Scrambling Algorithm Using Parameter Based M-Sequences", in Proc Seventh International Conference On Machine Learning And Cybernetics, Kunming, 12-15 July 2008. pp.3695-3698.

[7] Xiaomin Wang, Jiashu Zhang, "An image scrambling encryption using chaos-controlled Poker shuffle operation", Proceedings of International Symposium on Biometrics and Security Technologies, Islamabad, 23-24 April 2008, pp. 1-6.

[8] FU ai-ying,ZENG qing-wei, XU zhi-hai,DENG geng-sheng, "Binary Image Scrambling Evaluation Method Based on the Mean Square Deviation and the Bipartite Graph", in Proc International Symposium on Computer, Communication, Control and Automation 2010.pp237-239.

[9] Guilliang Zhu, Weiping Wang, "Digital Image Encryption algorithm based on pixel", ICIS-2010 IEEE International Conference 29-31 Oct 2010, pp-769-772.

[10] Ravankar A.A Sedukhin S.G, "Image Scrambling based on a New Linear Transform", International Conference on Multimedia Technology (ICTM) 2011

[11] Jiancheng Zou, Rabab K. Ward, Dongxu Qi, "A new digital image scrambling method based on Fibonacci numbers" in Proc. IEEE ISCAS 2004, vo. 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, 2008.

[15] H.B.Kekre, Tanjua Sarode, Pallavi Halarnkar, "Image Scrambling using R-Prime Shuffle ", International Journal of Advanced Research in Electrical, Electronics and Intrumentation Engineering, (IJAREEIE), vol.2 Issue 8. August 2013, pp. 4070-4076.

BIOGRAPHIES

Dr. H. B. Kekre has received B.E (Hons.) in Telecomm Engineering from Jabalpur University in 1958, M.Tech (Industrial Electronics) from IIT Bombay in 1960, M.S.Engg. (Electrical Engg.) from University of Ottawa, Canada in 1965 and Ph.D. (System Identification) from IIT Bombayin 1970. He has worked as Faculty of Electrical Engg. and then HOD Computer Science and Engg. at IIT Bombay. After serving IIT for 35 years he retired in 1995. After retirement from IIT, for 13 years he was working as a professor and head in the Department of Computer Engg. and Vice Principal at Thadomal Shahani Engineering. College, Mumbai. Now he is Senior Professor at MPSTME, SVKM‟s NMIMS University. He has guided 17 Ph.Ds, more than 100 M.E./M.Tech and several B.E./ B.Tech projects, while in IIT and TSEC. His areas of interest are Digital Signal processing, Image Processing and Computer Networking.

He has more than 450 papers in National / International Journals and Conferences to his credit. He was Senior Member of IEEE. Presently He is Fellow of IETE, Life Member of ISTE and Senior Member of International Association of Computer Science and Information Technology (IACSIT). Recently fifteen students working under his guidance have received best paper awards. Currently eight research scholars working under his guidance have been awarded Ph. D. by NMIMS (Deemed to be University). At present eight research scholars are pursuing Ph.D. program under his guidance.

Dr. Tanuja K. Sarode has received M.E. (Computer Engineering) degree from Mumbai University in 2004, Ph.D. from Mukesh Patel School of Technology, Management and Engg. SVKM‟s NMIMS University, Vile-Parle (W), Mumbai, INDIA. She has more than 11 years of experience in teaching. Currently working as Assistant Professor in Dept. of Computer Engineering at Thadomal Shahani Engineering College, Mumbai. She is member of International Association of Engineers (IAENG) and International Association of Computer Science and Information Technology (IACSIT). Her areas of interest are Image Processing, Signal Processing and Computer Graphics. She has 150 papers in National /International Conferences/journal to her credit.

Ms. Pallavi N.Halarnkar has received M.E. (Computer Engineering) degree from Mumbai University in 2010, currently persuing her Ph.D. from Mukesh Patel School of Technology, Management and Engg. SVKM‟s NMIMS University, Vile-Parle (W), Mumbai, INDIA. She has more than 8 years of experience in teaching. Currently working as Assistant Professor in Dept. of Computer Engineering at Mukesh Patel School of Technology, Management and Engg. SVKM‟s NMIMS University, Vile-Parle (W), Mumbai. She has 20 papers in National /International Conferences/journal to her credit.