ISSN (Print) : 2320 – 3765
ISSN (Online): 2278 – 8875

International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 2, Issue 8, August 2013

Image Scrambling using R-Prime Shuffle

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

Senior Professor, Dept. of Computer Engg., MPSTME, Mumbai, India[1]

Associate Professor, Dept of Computer Engg., TSEC, Mumbai, India[2]

Assistant Professor , Dept of Computer Engg, MPSTME, Mumbai, India[3]

Abstract: The recent growth of networked multimedia systems has increased the need for the protection of digital media. Digital media includes text, digital audio, images, video and software. Image Scrambling techniques are designed to make the image content unintelligible. In this paper, we have introduced a Novel approach for securing image data. The method proposed is a simple but powerful technique. The method uses R-Prime Shuffle to encrypt the image. It makes use of two different R-Prime numbers for rows and columns which make it more robust to decryption.

Keywords: Encryption, Scrambling, Shuffling, Security

I. INTRODUCTION

Information security becomes an important and urgent issue not only for individuals but also for business and governments. Security of image data is very important in many areas, such as privacy and copyright protection, security communication, and also in military applications Trust in digital data is characterized in terms of confidentiality, authenticity, and integrity (ISO 7498-2) [1]. Confidentiality is 'the property that information is not made available or disclosed to unauthorized individuals, entities or processes.' Authenticity is defined as 'the corroboration that the source of data received is as claimed.' Integrity is the 'the property that data has not been altered or destroyed in an unauthorized manner. Image Scrambling(Encryption) is a good method for providing security to image data by making image visually unreadable and also difficult to decrypt it for unauthorized users.

II. RELATED WORK

Wyner proposed an elegant one-dimensional (1-D) scrambling scheme without bandwidth expansion, making use of the discrete prolate spheroidal sequences (DPSS). The DPSS are optimal regarding their energy concentration in a given frequency subband. This method was given a two-dimensional (2-D) extension in [2]. However this method is not sufficiently secure against various cryptographical attacks [4], including ciphertext-only attack, known/chosen-plaintext attack and chosen-ciphertext attack. The cryptanalytic results suggest that the image scrambling scheme can only be used to realize perceptual encryption, instead of provide content protection for digital images

A new parameter based M-sequence which can be produced by a series shift registers is introduced in [3]. 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.

A region based selective image encryption technique is proposed [5] which provides the facilities of selective encryption and selective reconstruction of images. Simulation results are presented and a comparative analysis of the proposed technique with the conventional methods is discussed. Also, the efficiency considerations and advantages of the new technique over the conventional methods are highlighted.

ISSN (Print) : 2320 – 3765
ISSN (Online): 2278 – 8875

International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 2, Issue 8, August 2013

[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 method is proposed [10] to secure image-encryption techniques using a logistics –based encryption algorithm. In this technique, a Haar wavelet transform was used to decompose the image and decorrelate its pixels into averaging and differencing components. The logistic based encryption algorithm produces a cipher of the test image that has good diffusion and confusion properties. The remaining components (the differencing components) are compressed using a wavelet transform. Many test images are used to demonstrate the validity of the proposed algorithm. The results of several experiments show that the proposed algorithm for image cryptosystems provides an efficient and secure approach to real-time image encryption and transmission. To send the keys in secure form stenography will be used. Steganography is a technique that allows one application to communicate information to another application without a third party even knowing that the communication is occurring.

In [11], 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. This proposed technique, SDAEI, is very effective in encrypting any type of images and the results were very satisfactory. SD-AEI method is also compared with various other image encryption techniques and it was found that SD-AEI cryptographic method takes optimal amount of time when compared to other encryption techniques, for encrypting and decrypting an image file. This method can be used to encrypt any type of image file, especially secret images, where steganography has been applied, so that the contents in the image file can be kept more secure.

ISSN (Print) : 2320 – 3765
ISSN (Online): 2278 – 8875

International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 2, Issue 8, August 2013

[12] proposes a new invertible two-dimensional map, called Line map, for image encryption and decryption. It maps an image to an array of pixels and then, maps it back from the array to a same sized image. A Line map consists of two submaps: the left Line map and the right Line map, which are used for image encryption and decryption. In order to overcome the shortcoming of conventional image encryption approaches based on two-dimensional (2-D) maps which can be used only for permutation, this paper presents a novel image encryption approach based on the Line maps, which can perform two processes of image encryption simultaneously, permutation and substitution, using the same maps. The proposed image encryption does not have information loss. Other advantages include that it is fast and there is no restriction on the length of security key that is desirable for different security requirements. Simulation results show the effectiveness of the new image encryption scheme.

An image encryption algorithm based on DNA sequences for the big image is presented in [13].The main purpose of this algorithm is to reduce the big image encryption time. This algorithm is implemented by using the natural DNA sequences as main keys. The first part is the process of pixel scrambling. The original image is confused in the light of the scrambling sequence is generated by the DNA sequence. The second part is the process of pixel replacement. The pixel gray values of the new image and the one of the three encryption templates are generated by the other DNA sequence are XORed bit-by-bit in turn. The experimental result demonstrates that the image encryption algorithm is feasible and simple. Through performance analysis, this algorithm is robust against all kinds of attacks and owns higher security

Mixed Image Element (MIE) encryption algorithm is a new and promising image encryption algorithm, however, its security is affected by the unreasonable choice of camouflaged images. To analyze this factor, the definitions of image integral similarity, image partial similarity and MIE classification attack, as well as their mathematic models are proposed in [14]. The influence of image integral similarity on the security of MIE encryption algorithm in detail with an example is analyzed. The experimental results demonstrate that the algorithm performs best when the image integral similarity is 0.5, it gets worst when the image integral similarity approaches 0 or 1. This conclusion provides an important theoretical foundation for the practical application of MIE encryption algorithm. The influence of image partial similarity is also analyzed in detail with an example. The experiment shows how to find a true image element for a specific image with the image partial similarity. Finally, two remedial measures are given to defend the MIE classification attack, which is meaningful for completing MIE encryption algorithm.

III. 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 strong correlation between columns and rows. 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. Two Numbers are said to be relatively prime if they don't have any common factor except one. 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.

A. Encryption

The method used for Encryption is as follows

1) Read the image
2) Convert it to grayscale
3) Based on the Size of the Image(MXN), find out all the Relative Prime Numbers and save them in a set S
4) Using set S to find the correlation of the First row with remaining rows (positions w.r.t elements present in the set).
5) Consider the lowest correlation as the key to shuffle the rows in the image
6) Continue till all the positions in the image are considered
7) Save the Relative Primes Number as a key considered for Row Shuffling

ISSN (Print) : 2320 – 3765
ISSN (Online): 2278 – 8875

International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 2, Issue 8, August 2013

Repeat the same procedure for Column shuffling

B. Decryption

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

IV. EXPERIMENTAL RESULTS

For Experimental purpose five standard images 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 shows the plot for correlation obtained between the first row of the image with all the Relative Prime numbers considered in the set. The lowest correlation is considered as a key for shuffling. Figure 2 shows a plot for correlation between the first column and the set of Relative Prime numbers. Figure 3(a) shows the original image, (b) shows the image obtained after the shuffling of rows in the original image. To make the quality of the image imperceptible to human eye, the procedure is repeated for columns using the image obtained in 3(b) which gives a scrambled image shown in figure 3(c). The method for decryption is simple enough which gives a 100% retrieval of the original image shown in figure 3(d). Table No 1 gives the experimental results obtained for the technique. The Relative Prime numbers used for rows and columns for different images are displayed for e.g for Lena for row shuffling the relative prime used is 239 and for columns it is 143. The Average correlation between rows and columns of the original image and encrypted image is displayed in Table No 1.

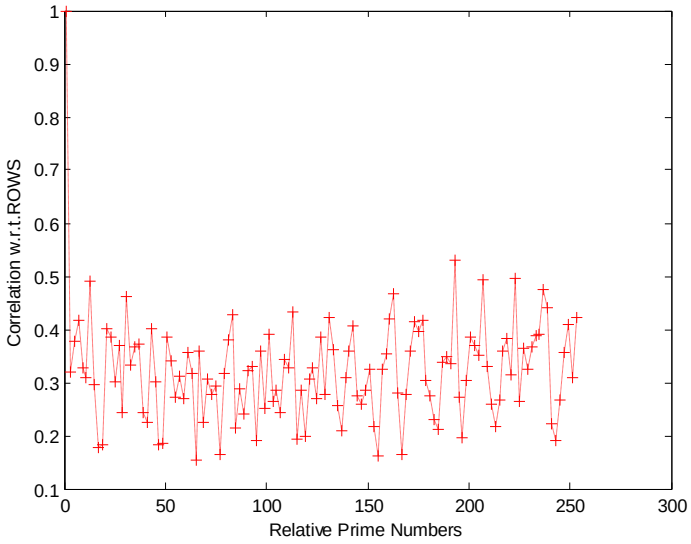


Fig. 1 Correlation of All the Relative Prime(Row Positions) with Row 1

ISSN (Print) : 2320 – 3765
ISSN (Online): 2278 – 8875

International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 2, Issue 8, August 2013

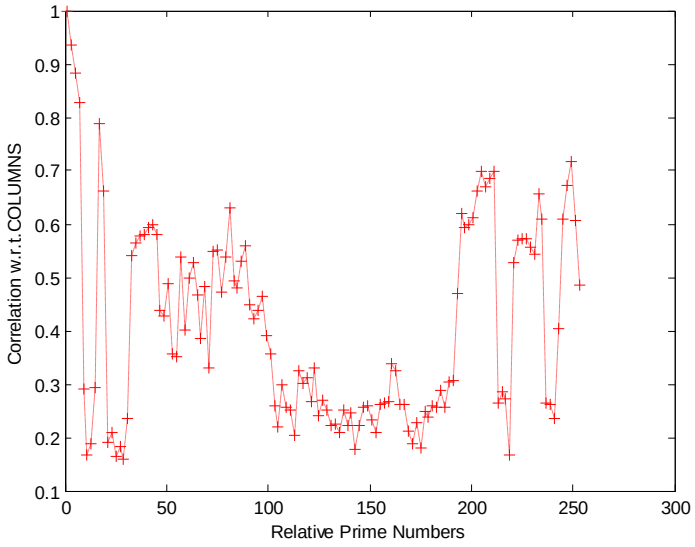
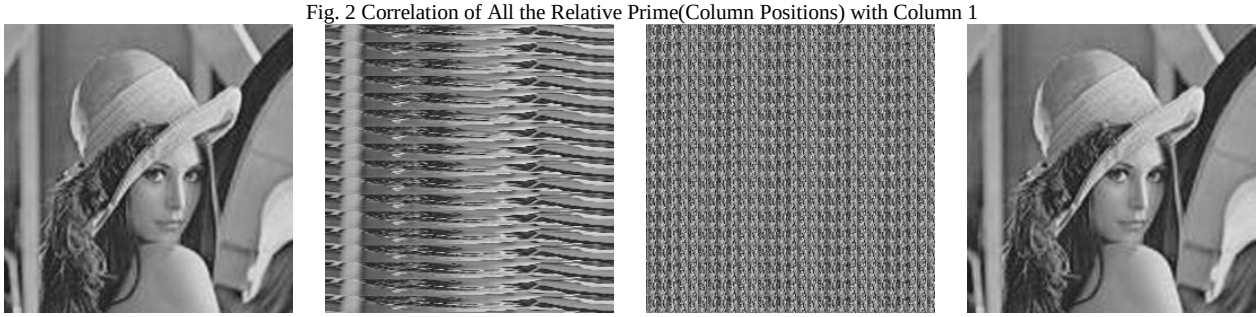


Fig. 2 Correlation of All the Relative Prime(Column Positions) with Column 1



(a) Original Image (b) Image Encryption using Row Shuffling (c) Image Encryption using Row and Column Shuffling (d) Decrypted Image

Fig. 3

TABLE I
EXPERIMENTAL RESULTS FOR R-PRIME SHUFFLE TECHNIQUE

Image	AvgCorrelation for Original Image		Avg Correlation for Encrypted Image		MSE	Time (sec)
	Rows	Columns	Rows	Columns		
Lena Row :239 Column :143	0.8556	0.7217	0.3984	0.2763	0.00	1.39
Baboon Row: 233 Column: 53	0.7351	0.7068	0.2709	0.2344	0.00	1.48
Pepper Row : 59 Column: 111	0.5995	0.6281	0.2425	0.2287	0.00	5.72
Mahalakshmi Row: 145 Column: 141	0.3190	0.3419	0.1860	0.1860	0.00	1.35
RadhaKrishna Row: 13 Column: 71	0.4774	0.5316	0.2261	0.2060	0.00	1.52

ISSN (Print) : 2320 – 3765
ISSN (Online): 2278 – 8875

International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 2, Issue 8, August 2013

V. CONCLUSION

R-Prime shuffling technique is a simple yet powerful technique which can be used for image scrambling. The technique is robust as different Relative Prime numbers are used for row and column shuffling. From the experimental results it can be observed that there is a reduction of approximately 50% in the correlation between rows and columns of the encrypted image. 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. As long as the Relative Prime number considered is kept secret it is not possible to decrypt the scrambled image. Hence this technique can be used to secure the image by storing the scrambled image and not the original image.

REFERENCES

[1] ISO 7498-2:1989, Information Processing Systems, Open Systems Interconnection, Basic Reference Model—Part 2: Security Architecture, http://www.iso.org, International Organization For Standardization; 1989.
[2] Dimitri Van De Ville, Wilfried Philips, Rik Van De Walle, Ignace Lemahieu, "Image Scrambling Without Bandwidth Expansion", IEEE Transactions On Circuits And Systems For Video Technology, Vol. 14, No. 6, June 2004, pp 892-897.
[3] 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 (Volume:7), Pp 3695 – 3698, July 2008
[4] S. Li, C. Li, K.-T. Lo, and G. Chen, "Cryptanalysis of an image scrambling scheme without bandwidth expansion," *IEEE Transactions on Circuits and Systems for Video Technology*, vol. 18, no. 3, pp. 338-349, 2008.
[5] K. C. Ravishankar and M. G. Venkateshmurthy, "Region based selective image encryption", International Conference on Computing and Informatic (ICOCI'06), Kuala Lumpur, Malaysia, (2006) June.
[6] Sabyasachi Samanta, Saurabh Dutta, Goutam Sanyal, "An Enhancement of Security of Image using Permutation of RGB-Components", "3rd 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. IEEE Int. Conference on Image Processing (ICIP'2002 pp II-925 - II-928 vol.2
[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] Nidhi Sethi and Deepika Sharma, "A New Cryptology Approach for Image Encryption" in Proc 2nd IEEE International Conference on Parallel, Distributed and Grid Computing, 2012 pp. 905-908.
[11] Somdip Dey, "SD-AEI: An Advanced Encryption Technique For Images", Proc. Of IEEE 2012 Second International Conference on Digital Information Processing and Communications (ICDIPC2012), Lithuania, pp. 68-73.
[12] Yong Feng ; Xinghuo Yu , "A novel symmetric image encryption approachbased on an invertible two-dimensional map" in proc 35th Annual conference on Industrial Electronics, 2009. IECON '09. pp 1973 – 1978.
[13] Shihua Zhou, Qiang Zhang, Xiaopeng Wei, "Image Encryption Algorithm Based on DNA Sequences for the Big Image", in Proc International Conference on Multimedia Information Networking and Security, 2010 pp. 884-888.
[14] Xiaoqiang Zhang, Shilong Ma, Guiliang Zhu, Weiping Wang, Mengmeng Wang, "Image Similarity Analysis on MIE Encryption Algorithm",in Proc *2nd International Conference on Future Computer and Communication 2010,* volume 2 pp V2-421-425

BIOGRAPHY

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.

ISSN (Print) : 2320 – 3765
ISSN (Online): 2278 – 8875

International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 2, Issue 8, August 2013

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.