IJCSE International Journal of Computer Sciences and Engineering **Open Access**

Research Paper **Volume-5, Issue-1** **E-ISSN: 2347-2693**

A Novel Approach utilizing Permutation Polynomials over integer rings as a Cryptological Application for Effective Encryption of Digital Images

Neha Balu Wagh[1*], Megha Kolhekar[2]

[1,2] Department of Electronic and Telecommunication, University of Mumbai, India
[1,2] Fr. Conceicao Rodrigues Institute of Technology, Vashi, Navi Mumbai, India

Available online at: www.ijcseonline.org

Received:26/12/2016 Revised: 06/01/2017 Accepted: 20/01/2017 Published: 31/01/2017

***Abstract*— Internet Technology and its constant evolvement gives humans an opportunity to be an active explorer over social media and micro blogging sites. Due to which people have resorted to a route of Internet with images, a tempting platform which is hard avoid. This theme gained an overwhelming response as a communication medium for the obvious reason that people nowadays like to share or express their thoughts through images. Unlike text, images helps to annotate viewers' flow of emotions much conveniently with depth. But people relying more on power imagery to share information over unreliable channel, well-known as Internet invites exploitation and misapplication of confidential data which should be avoided. Considering the importance of the issue raised in the light of protecting images, encryption is a way to assure security. Image encryption techniques converts an original image to illegible form, so only authorized access is possible with a key. Over years, different image encryption schemes had been put forward with various issues being addressed according to the requirement of applications. In this paper, we proposed a novel image encryption algorithm based on permutation polynomials over integer rings which makes an attempt to overcome the limitations of existing methods. Here, the original image is scrambled by applying permutation polynomial to its rows and columns. Eventually, the experimental results and calculating the evaluation parameters using MATLAB shows that the proposed encryption scheme achieve satisfactory hiding aspect. Also, the comparison with respect to existing ones is made to analyze performance of the proposed technique.**

Keywords-Cryptography; Image Encryption; Permutation Polynomials; Internet; integer rings; MATLAB.

I. INTRODUCTION

The basic science of cryptography is to protect important information and avoid its misuse. According to the conventional context, Encryption is defined as a conversion process of confidential data into another, called as cipher-text, which cannot be easily understood by anyone except certified parties while transmission over unreliable channel. Decryption is a reverse procedure to retrieve the original data back. Figure 1 is a simplified model of encryption and decryption process[1]. Encryption follows a certain algorithm (e.g. DES) which can have pre-defined conditions for carrying out transformations depending on the key to convert plain-text into an unreadable as per various applications. The different data formats on which encryption can be performed are text, images and videos. Encryption is used to secure data in transit sent not just the Internet, but from all types of devices such as ATM[2]. Due to opportunities created by advances in communication technology, it is interesting how images have become an important aspect in a communication view. Sources said images enjoy its prominence present in the digital world wielding considerable influence, that can be seen in people seeking for powerful imagery to exchange their ideas with others. With this, image data is also at risk because it is shared over unreliable medium such as Internet. Image Encryption is defined as a process where an original image gets encrypted after transformation by using a method to produce a cipher-image. The original image is the retrieved by applying the reverse transformation. Figure 2 illustrates the process of image encryption.

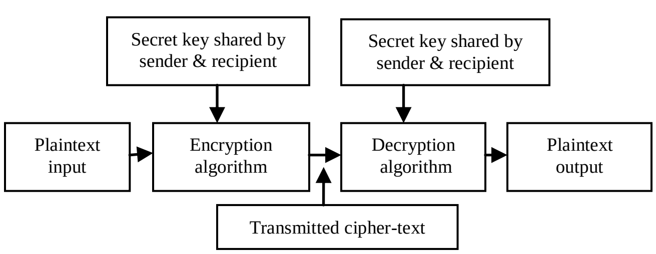


Figure 1. Standard model of encryption[1]

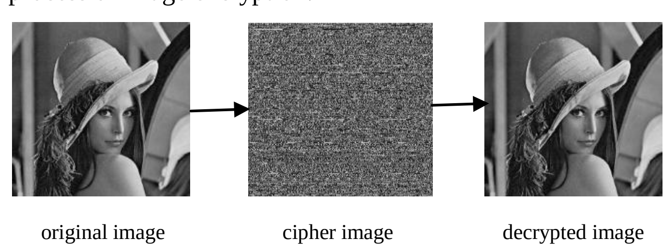


Figure 2. Standard process of image encryption

A natural image captured with any type of optical instrument displays a continuously varying array of shades and colour

*Corresponding Author:
Neha Balu Wagh
e-mail: nehabwagh@gmail.com , Tel.: +91- 8097864370

© 2017, IJCSE All Rights Reserved

tones that are represented in 2-D form. For encoding, image data will require conversion into 1-D form before enciphering[3]. Traditional encryption algorithms such as Data Encryption Standard(DES) and Advanced Encryption Standard(AES) as secret key ciphering standards, Rivest Shamir Adleman (RSA) as public key schemes, and the family of elliptic-curve-based encryption (ECC) are conventional methods[4,5]. They may not be the most recommendable prospects for encrypting images due to their notable features like repetitiveness to a high extent, and prominent inter-relation among pixels. Over a period of time, as a means securing the digital images is motivating many researchers to come up with improved encryption techniques. These encryption schemes can be categorized as value transformation [6-7], pixels position permutation [8-10], and chaotic systems [12-13].

II. LITERATURE SURVEY

In 2008, Mohammad Ali Bani Younes and Aman Jantan suggested a block-based modification method that basically combines image transformation with a Blowfish cipher[6]. The plain image was divided into blocks, which were reorganized using a transformation algorithm. Further, this transformed image was encrypted with the aid of Blowfish algorithm. The results depicted noticeable decrease in inter-connection between image components.

In 2008, Tiegang Gao and Zengqiang Chen presented an algorithm, which employed a new algorithm of total shuffling matrix, where the locations of image pixels were shuffled[8]. In order to reduce inter-relation between original and cipher images, the states combination of two chaotic systems are used. The results concluded that it has a low time complication, and benefits of key space being large, good security and random behaviour in distribution of gray scale values for ciphered image.

In 2011, Li Zhang*, Xiaolin Tian and Shaowei Xia presented a new scrambling algorithm for image encryption[9]. It incorporated both the Logistic chaotic sequence and Rubik's Cube. This algorithm started with splitting a plain image into several blocks to generate cubes. Thereafter, cubes were rotated according to Rubik's Cube by using the procedure of Logistic system. Then, using those cubes to go back to a new scrambled image. The outcome of experiment shows that this scrambling plan has a good robustness.

.

In 2012, Khaled Loukhaoukha, Jean-Yves Chouinarda, and Abdellah Berdai proposed a novel image encryption scheme in which original image is scrambled using a principle called Rubik’s cube[10]. Further, the application of XOR operator to rows and columns of the scrambled image using two private keys is done. Numerical simulations had been executed to check the validity and security of the algorithm.

In 2011, Joshi Rohit A, Joshi Sumit S and G.P. Bhosale proposed an improved image encryption scheme with increased protection level using chaotic maps[12]. This algorithm consists of two steps. In first step, a chaotic sequence is generated by making use of Henon Map. Later in second step, every pixel of the plain image is encrypted as a function of chaotic order. The analysis governs that the algorithm produces a desired performance.

In 2014, Nilesh Y. Choudhary and Ravindra K. Gupta, proposed an approach that requires permuting the blocks within the bounds of image as directed by Arnold Map[13]. Then the permutated blocks are combined yielding permutated images. This process is replicated for various block sizes. A partially encrypted image is obtained in the end.

Thus, we have surveyed the different ways that supported the aim of encrypting images. It was observed that there some performance issues such as lengthy procedures, less complexity, existence of correlation between original and encrypted even after transformation and no flexibility to encrypt images of different sizes. This became a motivation for us to design a new method which will strive to overcome the above limitations. The rest of this paper is organized as follows. Section III briefly explains the concept of Permutation Polynomials which is the core of this report. Section IV describes design and implementation of the propose scheme. Section V gives the experimental results and evaluation parameters to validate the proposed image encryption algorithm. Section VI concludes the paper.

III. THEORY OF PERMUTATION POLYNMIALS

This section briefly explores the subject of permutation polynomials and the fundamental results published in respective area.

In history, the general study of Permutation Polynomials started with Hermite who considered permutation polynomials over finite prime fields[14]. Although he contributed a great deal to community of permutation polynomials, it usually not easy to apply this on a given class of polynomials. L.E. Dickson was the first person to study Permutation Polynomials of arbitrary finite fields[14]. In 1999, the author Ronald L. Rivest put lot of efforts to give an exact characterization of permutation polynomials modulo n[16]. Permutation Polynomials has attracted a great attention in the study of finite fields and their applications in cryptography. In both arithmetic and combinatorial aspects of finite fields, permutation polynomial became a significant topic of discussion. It have important applications in Coding Theory, Cryptography such as in RC6 block cipher, Finite Geometry, Combinatory and Computer Science among other fields[14][17]. In 2005, the author Jing Sun and Oscar Y. Takeshita introduced a class of deterministic interleavers for turbo codes based on permutation polynomials over integer rings[18]. In our work, we focus on the properties of

© 2017, IJCSE All Rights Reserved

permutation polynomials (PPs) that have been used for crypto-logical application. The concept of generating permutation polynomials is based on principle of bijection. A bijection is one-on-one correspondence[19].

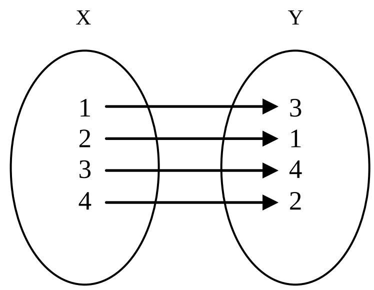


Figure 3. Illustration of mapping[19]

From Fig.1, a bijective function f: X→Y is one-on-one mapping of elements (X) to elements (Y). If a bijective function forms a set to itself then it is called a permutation[19]. H. Zhao and P. Fan in 2007 presented a paper for generating m^{th} order permutation polynomial over integer rings[20]. The ring is the set of positive integers commonly defined as Z_N . In further sub-sections, we will see the definition and conditions which are pre-requisites to design an image encryption algorithm using permutation polynomials.

A. Definition of Permutation Polynomials

Let Z_N denote the integer ring $\{0,1,2,\ldots,N-1\}$, where N is a positive integer; then a m^{th} order polynomial over Z_N is given by equation (1) [20]

$$f(x) = \{a_m x^m + a_{m-1} x^{m-1} + \ldots + a_1 x + a_0\}(\bmod N) \qquad (1)$$

where $x \in Z_N$, m is the degree of polynomial. If $f(x)$ generates a permuted number sequence of $x \in Z_N$, it is referred to as a permutation polynomial over Z_N .

I. Advantages

1. Compared to quadratic equations, higher degree permutation polynomials provides non-linearity.
2. Algebraic structure with unique properties such as bijection.
3. $f(x) = a$ has a unique solution for each $a \in Z_N$.

II. Disadvantages

1. It is quite difficult to give an exact characterization and to design permutation polynomials.
2. The selection of coefficients for permutation polynomials should be exact otherwise it won't be possible to encrypt images and retrieve it properly.

B. The purpose of selecting permutation polynomials

An effective encryption scheme should be such that it won't give unauthorized people a chance to crack the code in order to access the confidential content. Constructing permutation polynomials is fairly hard which is why it poses to be a hindrance for unauthorized users to retrieve the content from encrypted data. Among the other existing image encryption algorithm which involves the use of transform and conventional methods, arrangement of pixels and properties of permutation polynomials provides simple and quick process. Thus, the purpose of achieving better image encryption methods is served.

We have proposed a novel digital image encryption and decryption technique that exploits the cryptographic properties of permutation polynomials. The coefficients of permutation polynomial are defined over a finite integer ring. In this scheme, firstly a permutation polynomial is generated with its degree inputted by the user. Then that permutation polynomial is applied to gray-scale image in which the image pixel elements gets permuted yielding an encrypted image. In later sections, the design and implementation of our proposed work is explained.

III. PROPOSED METHOD OF IMAGE ENCRYPTION

This section discusses the design and implementation of the proposed Image Encryption and Decryption technique using Permutation Polynomials over integer rings.

A. Design of proposed image encryption algorithm:

To design the proposed image encryption scheme using permutation polynomials as an encryption tool, selection of coefficients for permutation polynomials is priority which is based on the conditions defined in and its demonstration is shown in Figure 4[20].

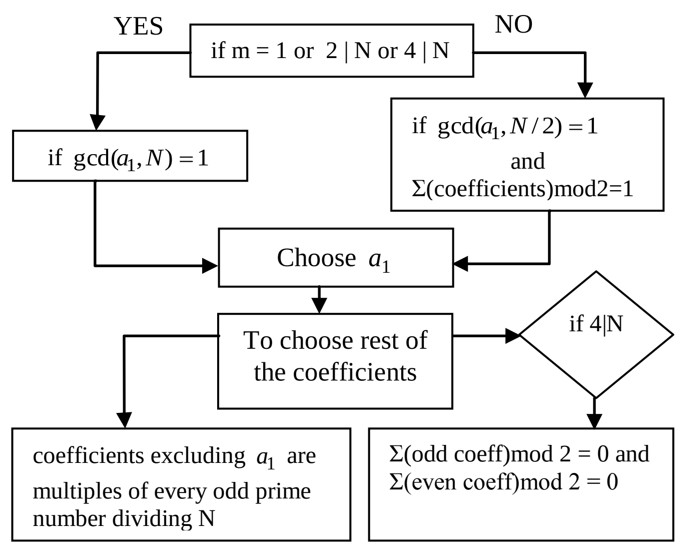


Figure 4. Conditions to choose the coefficients of permutation polynomials[20]

From the recent survey [16] and research point of view, it is assumed that Z_N is to be a finite ring and the coefficients of

© 2017, IJCSE All Rights Reserved

$f(x)$ are integers. In flow for design of image encryption, selection of the degree *m* depends upon the user and coefficients relies on image size *N*. The encryption method will be more effective when there is non-linearity and less correlation among image pixels. Therefore, keeping the degree of the PPs greater than 1 is beneficial. As shown in Figure 4, we have conditions explained as [20]:

a) If $m = 1$, coefficient a_1 is randomly chosen if $\gcd(a_1, N) = 1$, i.e. a_1 and N are relatively prime.
b) If $m > 1$, coefficient a_1 is randomly chosen if $\gcd(a_1, N/2) = 1$.
c) The remaining coefficients are chosen if the coefficients are multiples of odd prime number (a_1) dividing N.
d) Coefficients get selected if 4 divides N and modulus 2 operation on sum of even/odd coefficients gives zero as a result.

Next we will see the implementation of our proposed work on how permutation polynomials encrypt the images.

B. Implementation of proposed encryption algorithm:

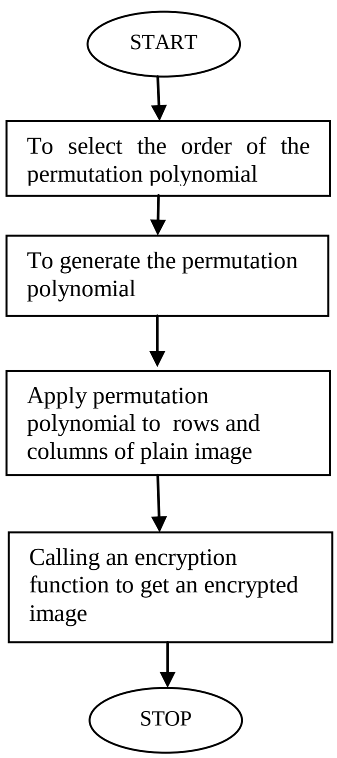


Figure 5. Proposed Image Encryption

Figure 5 gives the brief idea how encrypted image is obtained after application of PPs.
Let I be the representation of a gray scale image of the $r \times c$ size. Here, I characterizes the pixel values matrix of image I and *integer* $N = r \times c$. The procedure for encryption is as shown in Figure and follows as:

1) Get the degree *m* of permutation polynomial *f(x)* from the user.

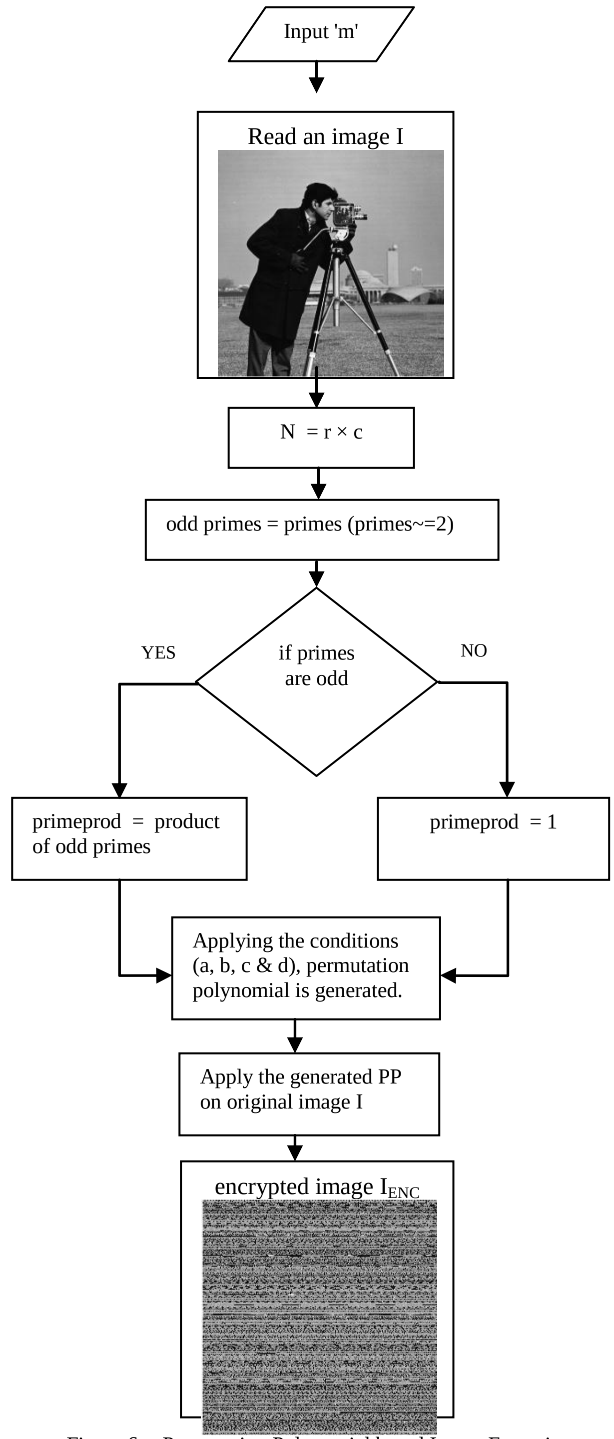


Figure 6. Permutation Polynomial based Image Encrytion

© 2017, IJCSE All Rights Reserved

2) Read the gray scale image I and store the number of rows and columns of that image in an array. The integer N is the multiplication of $r \times c$.
3) Factor N into primes and collect unique primes. If primes powers of 2 exists, remove it to obtained the product.
4) Applying the conditions (a) and (b) in order to choose the coefficient a_1 randomly. These conditions helps to extract the value of if GCD = 1
5) According to the condition (c), the values for remaining coefficients to a_1 to a_{m-1} are chosen from the specific range based on N.
6) To apply condition (d) and if true, get the final result. The final result is permutation polynomial over integer N.
7) Permute the $r \times c$ pixels of image with generated permutation polynomial to get the encrypted image.

After performing the above process, an encrypted image I_{ENC} is created. The flow chart for encryption of digital images using permutation polynomial as a key is demonstrated in Figure 6. An encrypted image is then a array of matrix whose pixel position is different from setting of original image.

Key Distribution: We still have yet to decide on how the key is to be shared while transmission. For now, the image is retrieved explicitly with the same permutation polynomial with was use for encryption. In order to get original image back the reverse procedure is followed called as decryption.

8) The encrypted image is reshaped and the permute function which uses permutation polynomials as a key to retrieve the original image I_{DEC} back as shown in Figure 7 below.

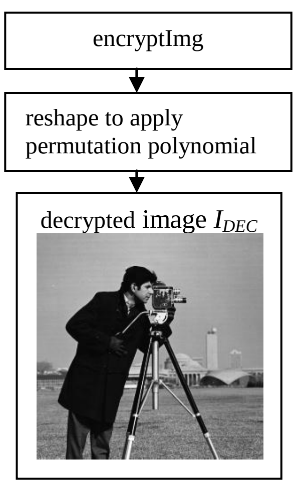
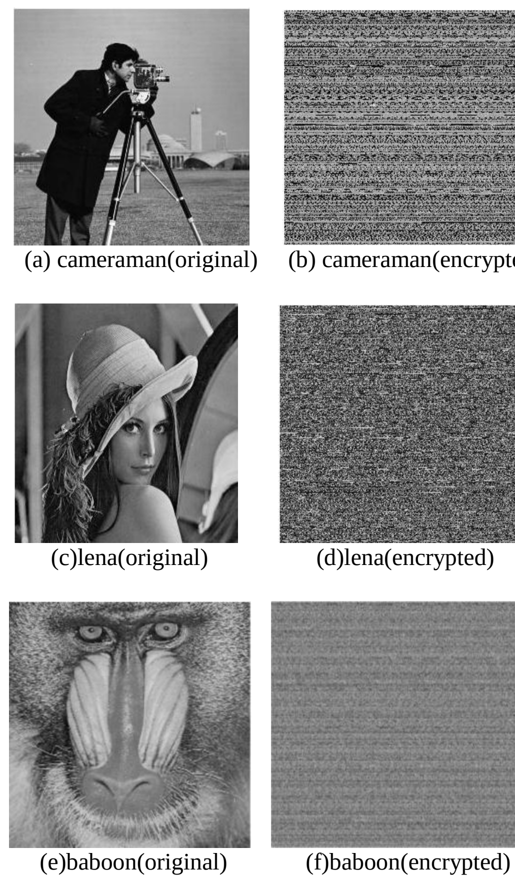


Figure 7. Flowchart of decryption

Decryption process is done. The results of experiment using *MATLAB* [27] tool is dicussed in next section.

IV. IMPLEMENTATION RESULTS

A simulation-based experiment was carried out and the standard set of evaluation parameters were used to investigate the proposed image encryption algorithm using permutation polynomials using integer rings. A study of some existing image encryption methods was presented in[21]. And its following work of how the proposed algorithm has contributed to overcome the issues is discussed and the overall performance is assessed. To test the effect of one-on-one-pixel change on the plain-image and the encrypted image, two standard visual quantities were employed for evaluation: Number of pixels change rate (NPCR) and Unified average changing intensity (UACI). They were first shown in 2004 and their details is described in [22]. NPCR and UACI were first introduced in 2004[22], in fact both of which the credits belong to Yaobin Mao and Guanrong Chen[22]. Two gray-scale images of size 256 × 256(camera-man, lena) pixels and one gray-scale image size of 512 × 512 (baboon) were used.



(a) cameraman(original) (b) cameraman(encrypted)

(c)lena(original) (d)lena(encrypted)

(e)baboon(original) (f)baboon(encrypted)

Figure 8. Original and encrypted images

Figure 8 depicts these test images with its respective encrypted images and it can be observed that there is no intuitive resemblance between original and their encrypted parts.

© 2017, IJCSE All Rights Reserved

The encrypted image should be unrelated and differ from its original form. The two commonly used difference measures NPCR and UACI previously stated are used to quantify the same requirement. Let $I_0(i,j)$ and $I_{enc}(i,j)$ be the pixels of original and encrypted images, I_0 and I_{enc}, at the i^{th} pixel row and j^{th} pixel column, respectively [23]. The mathematical expressions for NPCR and UACI parameters are given by equations (2) and (3) below.

$$NPCR = \sum_{i=1}^{M}\sum_{j=1}^{N} D(i,j) \times \frac{100\%}{M \times N} \quad [23] \qquad (2)$$

$$where\ D(i,j) = \begin{cases} 0, if\ \ Io(i,j) = Ienc(i,j) \\ 1, if\ \ Io(i,j) \neq Ienc(i,j) \end{cases}$$

The UACI measure helps to identify the average intensity of difference in pixels between the two images. For the image I_0 (i,j) and encrypted image $I_{enc}(i,j)$, the expression for UACI is given as [23]

$$UACI = \left[\sum_{i=1}^{M}\sum_{j=1}^{N} \frac{\left| Io(i,j) - Ienc(i,j) \right|}{255} \right] \times \frac{100\%}{M \times N} \quad [23] \qquad (3)$$

To reach the performance of an optimal image encryption algorithm, the desired NPCR values must be large and UACI values must be likely around 33%[22]. Table 1 gives the NPCR and UACI values for the plain-images and their encrypted forms. The obtained values are approaching to unity for NPCR measure. The UACI values are also befitting.

TABLE I. EVALUATION PARAMETERS

No. of Images	***Rubik Cube***		***Arnold Map***		***Proposed Method***	
	NPCR	UACI	NPCR	UACI	NPCR	UACI
cameraman	96.57	19.97	98.09	21.09	98.87	26.92
lena	97.35	19.92	99.88	21.88	99.29	23.64
baboon	99.60	17.21	99.03	16.68	99.31	18.81

After performing the randomness tests, it can be concluded that the proposed algorithm is able to generate random-like cipher text. It also gives much better evaluation results compared to existing image encryption techniques mentioned in [21] on quantitative basis. It is apparent from the above results that the prime aim of an encryption scheme to not let attackers learn about the inherent relations between original and cipher text is achieved. Further to study how original image and its encrypted counterpart are related, correlation coefficient is computed between image pixels. Correlation Coefficient are used to find how strong a relationship is between data. It is a value representing the similarity between two images with respect to pixel intensity. Its defined as given by equation (4)

$$\gamma_{xy} = \frac{\sum_m \sum_n (x_{mn} - \bar{x})\,(y_{mn} - \bar{y})}{\sqrt{\left(\sum_m \sum_n \left(x_{mn} - \bar{x}\right)^2\right)\left(\sum_m \sum_n \left(y_{mn} - \bar{y}\right)^2\right)}} \quad [13] \qquad (4)$$

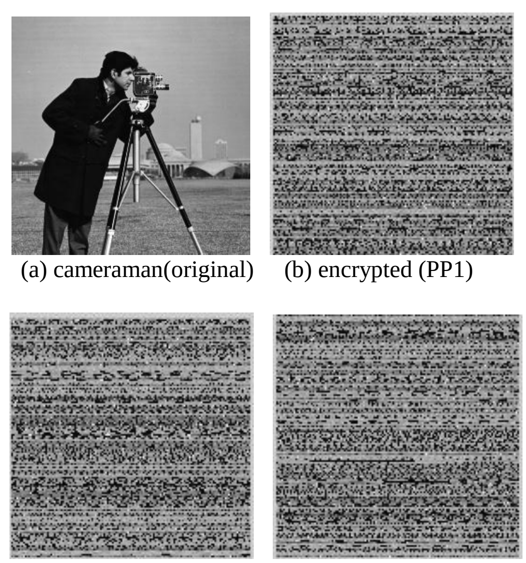
where $\bar{x}$ and $\bar{y}$ are respective mean of two images x and y on which comparison is made. The subscripts m and refer to the pixel location.

TABLE II. CORRELATION COEFFICIENT

No. of images	***Permutation Polynomial over integer rings***
cameraman	0.0025
lena	0.0014
baboon	0.0099

Table II certainly depicts that very low similarity exists between original and encrypted images. The proposed scheme using permutation polynomials is able to hide all attributes of the original image, thus achieving confidentiality which is of vital importance.

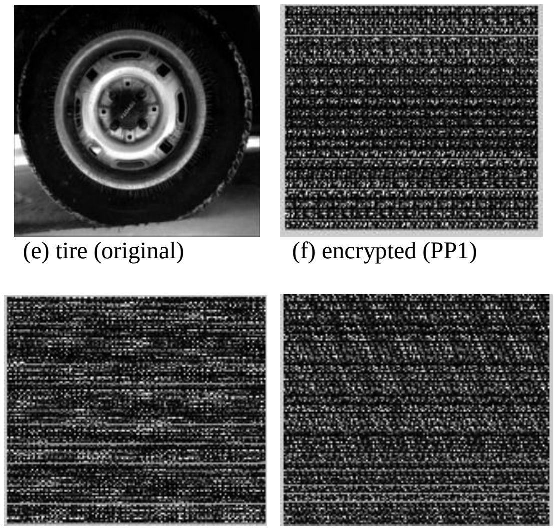
The Key Sensitivity analysis test is performed to check whether a change is produced in cipher image if there is a slight change in permutation polynomial[22]. The following Figure 9 shows the example for proposed image encryption using different permutation polynomials PP1, PP2 and PP3 respectively. Observing the results from Figure 9, it is certainly clear that encrypted images obtained from three different permutation polynmials represents significant variation. So decryption is only possible when one has an authority to access the aspects of permutation polynomials.



(a) cameraman(original) (b) encrypted (PP1)

(c) encrypted (PP2) (d) encrypted (PP3)

© 2017, IJCSE All Rights Reserved



(e) tire (original) (f) encrypted (PP1)

(g) encrypted (PP2) (h) encrypted (PP3)

Figure 9. Original and encrypted images

Due to which it becomes computationally difficult for the third party to acquire the contents of encrypted image. Images shared in various micro-blogging sites are variant and often have non-square or different sizes. The key feature that is provided by the proposed image encryption scheme is flexibility to encrypt non-square images thus overcoming the limitation of exiting image encryption schemes by Arnold Map [13]. As Arnold Map only supports its application on square images whereas the key structure of image encryption by Rubik Cube does not allow to work on odd-sized images (eg. rocktowers).

V. CONCLUSION

The following conclusion can be made from the results and discussions done. The simulation-based implementation of the proposed image encryption algorithm using Permutation Polynomials using integer rings shows decrease in correlation between original and encrypted images. Experimental results show that the scheme is able to produce randomness in cipher-image. The estimated changed rate in number of pixels (NPCR) and Unified Averaging Changing Intensity(UACI) measures are close to theoretical values and are comparable to existing encryption methods. The proposed scheme also supports encryption of variant image sizes outperforming the limitation of existing schemes as discussed in[21].

VI. FURTHER WORK

In the work presented in this paper, we have performed the encryption operation on an image in the spatial domain. The polynomial coefficients corresponding to the spectral sub bands of an image can also be obtained by applying a suitable wavelet transform to it. This paper is based on the encryption in the spatial domain and presently we are working on the applicability of the proposed method in the transform domain. The reason s for using wavelet transform i.e. Discrete Wavelet Transform (DWT) are that it has multi-resolution characteristics, both spatial and frequency domain features. It provides a coarse level representation of an image with varying scales and resists intentional and unintentional attacks with more sustainability[24]. In future, the work can be extended to enhance the security of digital videos in terms of cryptography as well as steganography which is theoretically discussed in [25] and implemented by using conventional methods in [26].

ACKNOWLEDGMENT

I would like to thank my supervisor Mrs. Megha Kolhekar for her valuable feedback to all my inputs which helped me to complete the work well. I specially acknowledge my family members because of their encouragement and co-operation. I would also mention special thanks to Sir Vikram Budvik who pursued his M.Sc. from Purdue University, USA helped me.

REFERENCES

[1] William Stallings, “Cryptography and network security: principles and practice”, Sixth Edition- **2014**, ISBN:978-93-325-1877-3

[2] What is encryption, http://www.searchsecurity.techtarget.com/ definition/encryption, Nov **2014**.

[3] Basic Properties of Digital Images, http://www.olympus-lifesciencce.com/en/primer/digitalimaging/digitalimagebasics/

[4] Cryptography: The Science of Secrecy, http://www.ankitjain. info/articles/Cryptography_ankit2.htm

[5] Sudipta Sahana and Abhipsa Kundu, "A Novel Approach on Adaptive Block Steganography Based Crypting Technique for Secure Message Passing", International Journal of Computer Sciences and Engineering, Volume-02, Issue-12, Page No (42-46), Dec -2014

[6] Mohammad Ali Bani Younes and Aman Jantan, “An image encryption approach using block based transformation algorithm,” IAENG International Journal of Computer Science, 35:1, IJCS_35_1_03, Feb **19**, **2008**.

[7] Shivlal Mewada, Sharma Pradeep, Gautam S.S., “Classification of Efficient Symmetric Key Cryptography Algorithms”, International Journal of Computer Science and Information Security (IJCSIS) USA, Vol. 14, No. 2, pp.(105-110), Feb 2016 .ISSN: 1947-5500.

[8] Tiegang Gao and Zengqiang Chen, “Image encryption based on a new total shuffling algorithm,” Chaos, Solitons and Fractals, ISSN 0960-0779, Volume-**38**(**1**), Page No (**213-220**), **2008**.

[9] Li Zhang, Xiaolin Tian and Shaowei Xia, “A scrambling algorithm of image encryption based on Rubik's cube rotation and Logistic sequence,” IEEE International Conference: Multimedia and Signal Processing (CMSP), Volume-**1**, Page No (**312-315)**, 2011.

[10] Khaled Loukhaouka, Jean-Yves Chouinard and Abdellah Berdai, “A secure image encryption algorithm based on

Rubik's cube principle," Hinsawi Publishing Corporation, Journal of Electrical and Computer Engineering, Volume-**2012**, Laval University, **2012**.

[11] Md Asif Mushtaque, "Comparative Analysis on Different parameters of Encryption Algorithms for Information Security", International Journal of Computer Sciences and Engineering, Volume-02, Issue-04, Page No (76-82), Apr - 2014

[12] Joshi Rohit A, Joshi Sumit S and G.P. Bhosale, "Improved image encryption algorithm using chaotic map," International Journal of Computer Applications (0975-8887), Volume-**32**, Issue-**09**, Page N (**6-10**), October **2011**.

[13] Nilesh Y.Choudhary and Ravindra K.Gupta, "Partial image encryption based on block-wise shuffling using Arnold catmap," International Journal of Computer Applications, Volume-**97**, Page No (**33-37**), Issue-**10**, July **2014**.

[14] R.A. Collin and C. Small, "On Permutation Polynomials over finite fields," Internat. J. Math. & Math. Sci., Volume-**10**, Issue-**03**, Page No (**535-544**), **1987**.

[15] R.Lidl and GL Mullen, "When does a polynomial over a finite field permute the ekements of the field," The American Math, Monthly, Volume-**95**, Issue-**03**, Page No (**243-246**), **1988**.

[16] Ronald L Rivest, "Permutation Polynomial Modulo 2^w," Laboratory for Computer Science, Massachusetts Institute of Technology, Cambridge, MA 02139, October **25**, **1999**.

[17] Ashok Sharma, RS Thakur and Shailesh Jaloree, "Investigation of Efficient Cryptic Algorithm for Storing Video Files in Cloud", ISROSET-International Journal of Scientific Research in Computer Science and Engineering, Volume-04, Issue-06, Page No (8-14), Dec 2016

[18] Ashok Sharma, R S Thakur and Shailesh Jaloree, "Investigation of Efficient Cryptic Algorithm for image files Encryption in Cloud", ISROSET-International Journal of Scientific Research in Computer Science and Engineering, Volume-04, Issue-05, Page No (5-11), Oct 2016

[19] Shivlal Mewada, Sharma Pradeep, Gautam S.S., "Exploration of Efficient Symmetric Algorithms", IEEE 2016 3rd International Conference on Computing for Sustainable Global Development (INDIACom)", pp(663 – 666), March, 2016, ISBN 978-93-80544-20-5

[20] H.Zhao and P. Fan,"Simple method for generating mth order permutation polynomials over integer rings," Electronics letters, Volume-43, Issue-08, April 12, 2007.

[21] Wagh Neha Balu, "Permutation based Digital Image Encryption and Decryption Methods," CiiT International Journal of Digital Image Processing, Volume-**08,** Issue-**10**, Page No (**320-323**), Dec **2016.**

[22] Yue Wu, Joseph P. Noonan, and Sos Agaian, "NPCR and UACI Randomness Tests for image encryption," Cyber Jounals: Multidisplinary Journals in Science and Technology, Journal of Selected Areas in Telecommunications (JSAT), April **2011**.

[23] Shrija Somaraj and Mohammed Ali Hussain, "Performance and Security Analysis for image encryption using Key image," Indian Journal of Science and Technology, Volume-**08**, Issue-**35**, Dec **2015**.

[24] Chaitanya Vijaykumar Mahamuni and Neha Balasaheb Wagh, "Study of CBIR Methods for Retrieval of Digital Images based on Colour and Texture Extraction," International Conference on Computer Communication and Informatics (ICCCI-2017), Jan 05th-07th, **2017**, Coimbatore, pp (**305-311**) IEEE Xplore Digital Library.

[25] Mr. Chaitanya V. Mahamuni, "A Comphrensive Study of Cryptography and Content Hiding Techniques for Security of Digital Videos," International Journal of Advance Foundation and Research in Computer (IJAFRC), Volume-**02**, Issue-**12**, Page No (**46-52**), Dec **2015**.

[26] Mr. Chaitanya V. Mahamuni,"Digital Video Watermarking using DWT and PCA in encrypted domain," Research Chronicler International Multidisplinary Research Journal (RCIMRJ), Volume-02, Issue-03, March **2014.**

[27] MATLAB-Wikipedia, http://en.wikipdeia.org/wiki/MATLAB, Initial release-**1984**.

Author Biographies

Neha Balu Wagh was born on 16th August 1990 at Yavatmal, Maharashtra, India. She has completed B.E. (Electronics and Telecommunication Engineering) from A.C.Patil College of Engineering, Kharghar, University of Mumbai with First Class. She presently pursues M.E. (Electronics and Telecommunication Engineering) from Fr.C.R..I.T, Vashi, University of Mumbai. Her research work till date is related to image retrieval, and digital image encryption and decryption.

Mrs. Megha Kolhekar has completed MTech from IIT Bombay and presently pursues PhD from the same institute in finite fields. She has completed her B.E.(Electronics Engineering) in the grade of First Division from (RKNEC) affilated to Rashrant Tukdoji Maharaj Nagpur University, Nagpur, Maharshtra, INDIA. She is an Associate Professor at FCRIT Vashi and her research interests are related to Image Processing, Cryptography, Network Security and Wireless Communication.

© 2017, IJCSE All Rights Reserved