International Journal of Computer Sciences and Engineering Open Access
Research Paper Volume-4, Special Issue-6, Aug 2016 E-ISSN: 2347-2693

Bit-plane Oriented Image Encryption through Prime-Nonprime based Positional Substitution (BPIEPNPS)

Madhuchhanda Dasgupta[1*] and J. K. Mandal[2]

[1]*Dept. of CSE, JIS College of Engineering, Kalyani, India,*
[2] *Dept. of CSE, Kalyani University, Kalyani, India*

Available online at: www.ijcseonline.org

Received: Jun/26/2016 Revised: July/12s/2016 Accepted: July/22/2016 Published: Aug/12/2016

***Abstract*—** In this paper a bit-plane based novel image encryption technique has been proposed using pixel shuffling based on characteristics of bit position within a pixel. The image is decomposed into eight binary bit-planes and all the bit-planes are scrambled using Recursive Positional Substitution based on Prime - Nonprime method. The performance of the algorithm is a discussed against common attacks like brute force attack, cipher related attacks and Differential attacks. Test through histogram analysis, correlation co-efficient analysis are provided in simulations and security analysis to shows enhanced performance of the proposed algorithm.

***Keywords*—** image encryption; bit-plane decomposition; scrambling; pixel shuffling; histogram analysis

I. INTRODUCTION

Nowadays 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. Therefore, achieving secure image transmission is a big concern. With the increasing use of Internet, use of digital images has also been increased. For secure image transmission, image needs to protect from unauthorized uses. Moreover, applications in the automobile, medical, construction and fashion industry require designs, scanned data to be protected against espionage. Image encryption is an effective approach to protect images or videos by transforming them into completely different formats to ensure security [1].

Several image encryption algorithms have been developed to protect images. One method based on the cryptography concept considers images as data blocks or streams. It encrypts images block by block or streams by stream using different techniques. Data Encryption Standards (DES) [2] and Advanced Encryption Standard (AES) [3] are two examples of this approach. However, such encryption methods incur large computational costs and show poor error resilience.

Among existing image encryption technologies, an interesting technique based on image bit-plane decomposition has shown excellent encryption performance [4]. The technique first decomposes an image into several binary bit-planes using a specific decomposition method, such as traditional binary decomposition, gray code decomposition [5] and Fibonacci p-code decomposition [6]. After that image encryption can be accomplished by scrambling image pixel positions using different techniques in the spatial domain. One example is the recursive sequence based image scrambling approach [7]. It scrambles images using different recursive sequences such as the Fibonacci sequence, Cellular automata and chaotic maps [8]. Image encryption can also be accomplished by scrambling coefficient matrices/blocks in the transform domain [9]. These approaches have extremely low security levels due to the lack of security keys or the small key space.

To achieve higher levels of security, one solution is to change image pixel values while scrambling the positions of image pixels or blocks using different techniques. In this paper, we introduce Recursive Positional Substitution based on Prime - Nonprime(RPSP) method to scrambling the pixel values [10].

To further improve security, key-image decomposition is used and decomposed bit-planes are kept as a key bit-plane[11]-[14].

The algorithm decomposes the original image into its binary bit-planes using bit-plane slicing [15]. The bit-planes are encrypted by performing an XOR operation with a selected bit-plane of the key-image one by one. Scrambling method is applied to all the resultant bit-planes and then invert the order of bit-planes. The encrypted image is obtained by combining all the bit planes.

The rest of the paper is organized as followed. In Section II, the proposed method has been introduced. The algorithm is given in Section III and result analysis is shown

in Section IV. Comparison of the proposed scheme with existing technique is done in section V and conclusion is in section VI.

II. PROPOSED METHOD

In this section, we introduce a novel image encryption algorithm which has been termed as BPIEPNPS. The algorithm first decomposes the source image into eight binary bit-planes using bit-plane slicing. Again, the security key-image is decomposed into eight binary bit-planes and among eight bit-plane one bit-plane is chosen as security key-plane. To change bit values, the XOR operation is performed between source image bit-planes and security key bit-plane individually. A scrambling method, Recursive Positional Substitution based on Prime - Nonprime (RPSP) is used to encrypt each bit-plane. Next, all the bit-planes are inverts and combines them together to obtain the encrypted image. The block diagram of BPIEPNPS is shown in Fig. 1. The complete process of the scheme is described in section A to E respectively.

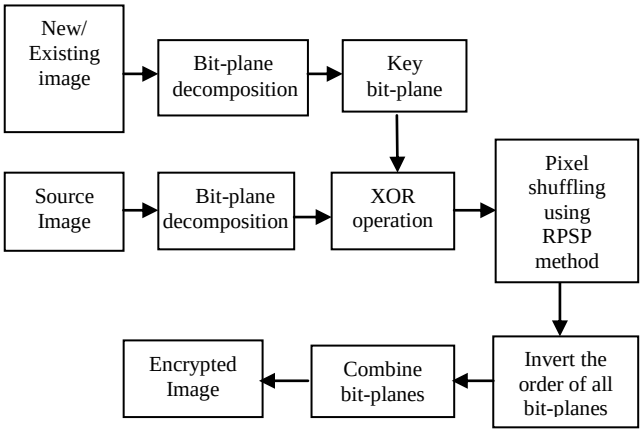

Fig. 1. The BPIEPNPS algorithm

A. Image Acquisition

For this purpose the USC-SIPI(USC University of Southern California - Signal and Image Processing Institute) Image Database has been used. Images are of various sizes such as 256×256 pixels, 512×512 pixels, 1024×1024 pixels are used here. All images are 8 bits/pixel for black and white images, 24 bits/pixel for color images.

Any new/existing image with the same size of the source image can be used as security key image.

B. Bit-plane slicing

In a image, if the intensity of each pixel is composed of 8 bits, it is in the range of 0 to 255 gray values. In bit-plane slicing, image is decomposed into 8 bit planes. First plane is the contribution of the least-significant bit(LSB) of the pixel and eight plane has the most significant bit(MSB) value for all the pixels of the image. All other planes accordingly responsible for different bit values which is shown in Fig. 2.

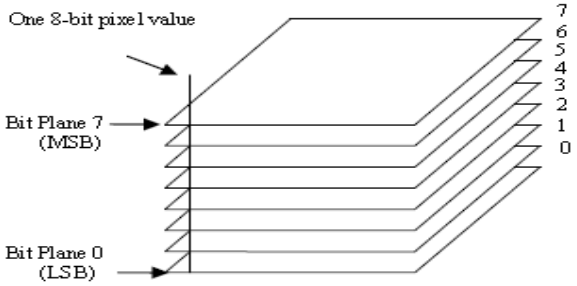

Fig. 2. Bit-plane representation of an 8-bit image.

Here, we consider grayscale image of size 512×512 as the source image which is in Fig. 3(a). and Fig. 3(b) through (i) are eight bit-planes of the source image, with Fig.3(b) corresponding to the lowest-order bit. The four higher-order bit planes, especially the last two, contain a significant amount of visually significant data. The lower-order planes contribute to more subtle intensity details in the image.

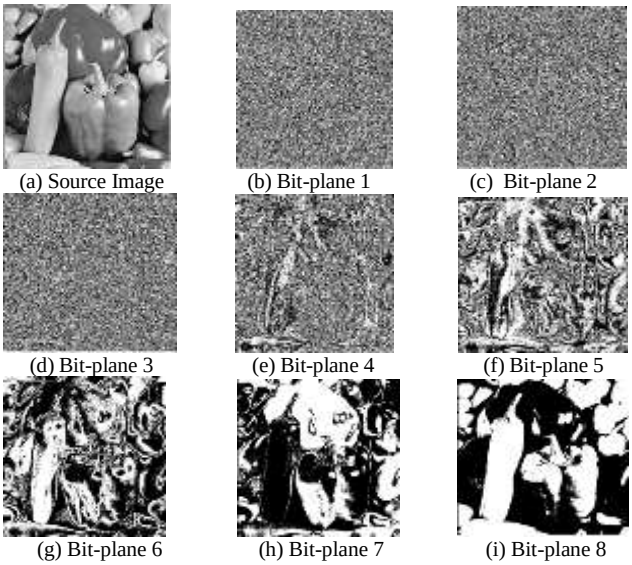

Fig. 3. 8 bit planes of input gray pepper image.

C. Encryption through Recursive Positional Substitution based on Prime – Nonprime (RPSP)

We will consider image data to be transmitted encrypting using RPSP technique and after the transmission, the data is to be decrypted using the same technique.

For a block of finite size n, a finite number of iteration I are required to regenerate the source block. In each block, the bit positions are shuffled based on prime-non prime value of the bit position. There are four possible cases of it and those are discussed below:

1. A bit in the position i (1<=i<=n-2) in the source block s becomes the bit in the position (n-i) in the target block t, if (n-i) is a non-prime integer.
2. A bit in the position i (1<=i<=(n-2)) in the block s becomes the bit in the position j (1<=j<=(n-i-1)) in the block t, where j is the precedent prime integer (if any) of (n-i), if (n-i) is a prime number.
3. A bit in the position n in the block s remains in the same position in the block t.
4. A bit in the position (n-2) in the block s is transferred in the block t to the position unoccupied by any bit after rules 1,2 and 3 are applied.

Here, we are considering the blocks of each size 8 and the 8 bits shuffling is shown in the Table I. X indicates before shuffling bit position and Y is after shuffling bit position.

TABLE I. ILLUSTRATION OF MAPPING(X -> Y) FOR BLOCK OF SIZE 8.

X	Y	Logic Followed
1	5	Here 8-1=7, a prime number, the precedent prime of 7 is 5.
2	6	Here 8-2=6, a non-prime number.
3	3	Here 8-3=5, a prime number, the precedent prime of 5 is 3.
4	4	Here 8-4=4, a non-prime number.
5	2	Here 8-5=3, a prime number, the precedent prime of 3 is 2.
6	?	Here 8-6=2, a prime number, there is no precedent prime, allocation suspended.
7	1	Here, 8-7=1, a non-prime number.
8	8	Here 8 being the position of the LSB, no change in position.
6	7	One allocation is suspended earlier, since the position 7 is only the unoccupied position so far, that allocation is made there.

For any intermediate iteration, the source is the target block of the previous iteration.

The above prescribed method is explained for a sample block 01001011 in Fig. 4.

Source Block

0	1	0	0	1	0	1	1
1	2	3	4	5	6	7	8

Block after 1st iteration

1	1	0	0	0	1	0	1
1	2	3	4	5	6	7	8

Block after 2nd iteration

0	0	0	0	1	1	1	1
1	2	3	4	5	6	7	8

Block after 3rd iteration

1	1	0	0	0	0	1	1
1	2	3	4	5	6	7	8

Block after 4th iteration

1	0	0	0	1	1	0	1
1	2	3	4	5	6	7	8

Block after 5th iteration

0	1	0	0	1	0	1	1
1	2	3	4	5	6	7	8

Fig. 4. Different Intermediate and Target Blocks generation for the block 01001011.

It is observed that after 5th iteration the original pattern is obtained.

In image, each bit planes are divided into blocks which contains 8 bits each. We apply this RPSP method to all the bit-planes to shuffle the pixel values. In encryption, we apply this method for 3 iterations and in decryption 2 iterations are applied to get the original data.

D. Invert the order of all bit planes

After applying RPSP method, all the bit-planes order are inverted i.e., Most Significant bit (MSB) converts into Least Significant bit (LSB) and all other plains accordingly to make the encrypted image more robust.

E. Cipher Image generation

All inverted scrambled bit-planes are combined together to form the cipher image.

III. ALGORITHMS

A. Encryption:

Input: Original image of size M × N and Key image of same size of the original image.

Output: Encrypted Image of M × N.

Method: The BPIEPNPS Algorithm

Step 1 The original grayscale image is decomposed into eight binary bit-planes using bit-plane slicing.

Step 2 The key image is also decomposed into eight binary bit-planes and sixth bit-plane is chosen as the key bit-plane.

Step 3 The XOR operation is performed between the original image bit-planes and key bit-plane individually.
Step 4 RPSP encryption method is applied for 3 iterations to scramble all the resultant XOR-ed bit-planes.
Step 5 Invert the order of all scrambled bit planes.
Step 6 Combine all bit planes together to obtain the encrypted image.

B. Decryption:
Input: Encrypted Image of M × N and Key image of same size of the original image.
Output: Original image of M × N.
Method: Decryption method
Step 1 The decryption process first decomposes the encrypted image into its eight binary bit-planes.
Step 2 The order of all bit-planes is restored to the original order.
Step 3 Unscrambles all bit-planes using RPSP method which is applied for 2 iterations to get original pattern.
Step 4 Decomposes the security key image into eight binary bit-planes.
Step 5 Performs XOR operation between the original image bit-planes and sixth key bit-planes of the security key-image.
Step 6 The decrypted image is obtained by combining all resultant bit-planes.

IV. EXPERIMENTAL RESULTS AND DISCUSSIONS

A. Statistical Analysis

It is well known to pass through the statistical analysis on cipher image .Ideally, a cipher should be strong against any statistical attack and in order to prove the security of the proposed image encryption method, the following statistical tests are performed.

1) Histogram Analysis

To prevent the access of information to attackers, it is important to ensure that encrypted and original images do not have any statistical similarities. The histogram analysis clarifies that, how the pixel values of images are distributed.

An example is shown in Fig. 5. which shows histogram analysis on test image using proposed algorithm. The histogram of the original image contains great sharp rises followed by sharp declines as shown in Fig. 5(e) and the histogram of the encrypted image in Fig. 5(g) has uniform distribution which is significantly different from original image and has no statistical similarity in appearance which means that this encryption scheme is very robust and secure.

Corresponding Author: *Madhuchhanda Dasgupta,madhu.banik@gmail.com*
Department of CSE., JIS College of Engineering, India

The original image is totally recovered in Fig. 5(d) and this can be verified by the histogram of the difference between the original image and the recovered image.

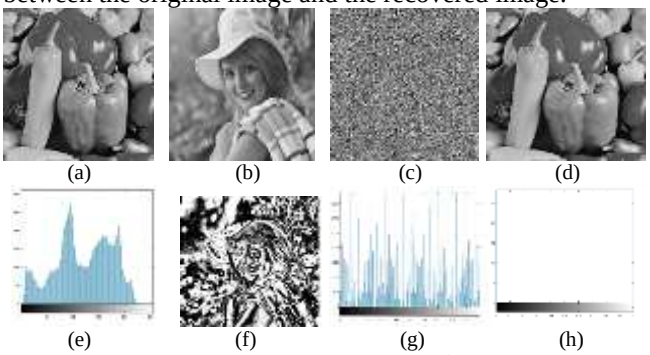

Fig 5.(a) The original grayscale pepper image of size 512×512; (b) A 512×512 grayscale elaine as key-image; (c)The encrypted image;(c) The recovered image; (e) Histogram of input pepper image; (f) Sixth bit-plane of key-imge; (g) Histogram of encrypted image; (h) Histogram of the difference between (a) and (d).

2) Correlation Co-efficient Analysis

An encryption algorithm intends to break the relationship of adjacent pixels within an image and prevent the original information. Here, Correlation analysis is to test the relationships of adjacent pixels in the original and encrypted images.

In an image, each pixel is highly correlated with its adjacent pixels. So correlation coefficient factor is a measure to find the correlation between the original and the cipher image pixels. Ideally, there should be low correlation between original and cipher image and high correlation between original image and reconstructed image.

A correlation coefficient approaches to 1 indicates a strong relation while the coefficient close to 0 means extremely low correlation.

Table II. Correlation coefficient between the plain image and the cipher image.

Image Name	Correlation between the original and cipher image
Pepper	-0.00368
Boat	0.00227
Couple	-0.00218
Lena	-0.00543

B. Security Analysis

Security is one of the major aspects to be taken care for the encryption algorithms. Here, an image itself is used as key which is very difficult for the attackers to know the key image. The original image is completely reconstructed without any loss or distortion only when the correct key image is used. Some of the possible attacks are:

1) Brute Force Attack

In Brute force attack the attacker performs an exhaustive search of all the possible combinations of

security keys of the encryption algorithms. Theoretically, this approach is feasible if the attacker knows the encryption algorithm and the key space is limited.

In the proposed method, the security key spaces are sufficiently large since the large number of possible any new/existing image could be used as a key-image and as a result, that withstand the brute force attack.

2) Ciphertext Related Attack

The plaintext is the original information to be encrypted. The ciphertext is the encrypted plaintext.

In this kind of attack, attacker tries to deduce the security keys by only studying the ciphertext. This attack can be used to recover the original image data by studying the cipher image.

From the experimental results it is shown that the encrypted images are visually unrecognizable and totally different from the original images. It does not contain any information about the original image. In histogram, the distribution of pixel is uniform for encrypted image. This ensure that the BPIEPNPS algorithm can withstand ciphertext related attack.

3) Differential attack

In differential attack, the attacker intends to recover the security key by slightly changing the original images and then exploring the changes of the corresponding encrypted images. A well-designed encryption algorithm ensures that a tiny change in the original image will result in a significant change in the encrypted image.

The number of pixel change rate (NPCR) and unified average changing intensity (UACI) are two most common measures which are used to evaluate the strength of image encryption algorithm. To test the influence of pixel change in the plain image and the number of average changed intensity between cipher text images, these two measures were used. The tests have been performed on the proposed method for sample images and the results are in Table III.

V. COMPARISON WITH AN EXISTING ENCRYPTION ALGORITHM

We have compared our scheme with DecomCrypt [2].
We have selected first 10 test images from the database http://decsai.ugr.es/cvg/dbimagenes/g512.php. These images are grayscale images with a size of 512 × 512. In Table III, the comparison results are given and it is seen that the proposed technique obtained good comparative value.

TABLE III. COMPARISON OF ENCRYPTION QUALITY

	NPCR		**UACI**	
Image	***Proposed Method***	***DecomCrypt [2]***	***Proposed Method***	***DecomCrypt [2]***
1	0.9951	0.9959	0.3367	0.3454
2	0.9952	0.9959	0.3321	0.3342
3	0.9964	0.9962	0.3347	0.3363
4	0.9320	0.9376	0.2880	0.2879
5	0.9961	0.9964	0.3701	0.3703
6	0.9958	0.9963	0.3440	0.3445
7	0.9953	0.9962	0.3327	0.3341
8	0.9950	0.9959	0.3339	0.3342
9	0.9958	0.9960	0.3337	0.3344
10	0.9964	0.9961	0.3341	0.3346

VI. CONCLUSION

In this paper, we have proposed a novel image encryption algorithm integrating bit-level permutation with pixel shuffling. Here encryption is performed only on gray scale images. In this proposed algorithm, first the image is decomposed into eight bit-planes and Recursive Positional Substitution based on Prime - Nonprime method is used to scramble the bit values of the pixel. The proposed technique is evaluated by different security tests i.e. statistical tests, correlation-coefficient test and different encryption quality tests like NCPR, UACI which shows enhanced performance of the proposed scheme.

ACKNOWLEDGMENT

The authors acknowledge the support provided by the DST PURSE Scheme at University of Kalyani, and staff of Department of Computer Science and Engineering, University of Kalyani, Kalyani, as well as at JIS, Kalyani. The authors also thank their colleagues for their constant support in their research work.

REFERENCES

[1] Iyer K. C. and Subramanya A., "Image Encryption by Pixel property Separation", International Association for Cryptologic Research (IACR), 2009.

[2] National Institute of Standards and Technology, "Data Encryption Standard (DES)," http://csrc.nist.gov/publications/fips/fips46-3/fips46-3.pdf, 1999.

[3] National Institute of Standards and Technology, "Advanced Encryption Standard (AES)," http://csrc.nist.gov/publications/fips/fips197/fips-197.pdf,2001.

[4] Zhou Yicong, Cao Weijia, Philip Chen C.L.," Image encryption using binary bitplane", ScienceDirect, Signal Processing, 197-207, www.elsevier.com/locate/sigpro. 2014,

[5] Zhou Yicong, "Image Encryption Algorithms Based on Generalized P-Gray Code Bit Plane Decomposition", Conference Record of the Forty-Third Asilomar Conference on Signals, Systems and Computers, ISSN: 1058-6393, DOI: 10.1109/ACSSC.2009.5469840, IEEE.H,2009.
[6] Y. Zhou, K.Panetta, S.Agaian, C.L.P. Chen, "Image encryption using p-Fibonacci transform and decomposition", Opt. Commun. 285(5) , 594-608 2012.
[7] Kekre H.B., Sarode Tanuja, Halarnkar Pallavi, " Image Scrambling Using R-Prime Shuffle on Image and Image Blocks", International Journal of Advanced Research in Computer and Communication Engineering, Vol. 3, Issue 2. ISSN(print): 2319-5940,February 2014.
[8] Mandal J. K. et al., "Adaptive Partial Image Encryption Technique based on Chaotic Map", Fourth International Conference of Emerging Applications of Information technology, 2014.
[9] Sun Qiudong, Yan Wenying, Huang Jiangwei, Ma Wenxin, " Image Encryption Based on Bit-plane Decomposition and Random Scrambling", 978-1-4577-1415-3/12, IEEE 2012.
[10] Mandal, J. K., Dutta, S. "Development & Analysis of a Ciphering Model through Recursive Positional Substitution based on Prime-Nonprime of Cluster", Association for the Advancement of Modeling and Simulation Techniques in Enterprises (AMSE, France), 2008.
[11] Zhou Yicong, Panetta Karen, Agaian Sos, "Image Encryption Using Binary Key-images", IEEE International Conference on Systems, Man, and Cybernetics San Antonio, TX, USA - October 2009.
[12] Wadi Salim Mushin, Zainal Nasharuddin, "Decomposition by binary codes-based speedy image encryption algorithm for multiple applications", IET Image Processing (Volume:9, Issue: 5), DOI: 10.1049/iet-ipr.2014.0514, 2015.
[13] Singh Anurag, Dhanda Namrata, " DIP Using Image Encryption and XOR Operation Affine Transform", IOSR Journal of Computer Engineering (IOSR-JCE), Vol. 17, Issue 2, 2015.
[14] Somaraj Shrija, Hussain Mohammed Ali, " Securing Medical Images by Image Encryption using Key Image", IJCA, Vol. 104 - No. 3, 2014.
[15] Gonzales R.C., Woods R.E., Digital Image Processing, 3rd edition, Pearson Prentice Hall.

AUTHORS PROFILE

Madhuchhanda Dasgupta is currently working as an Assistant Professor in the Department of Computer Science and Engineering, in JIS College of Engineering, Kalyani, West Bengal. She has received M.Tech in Computer Science and Engineering from Kalyani Govt. Engineering College and B.Tech in Computer Science and Engineering from University of Kalyani. she has 3 years of industry experience and 6 years teaching experience. Her area of interest includes Image Processing, Pattern Recognition and Automata.

M. Tech.(Computer Science, University of Calcutta), Ph. D.(Engg., Jadavpur University) in the field of Data Compression and Error Correction Techniques, Professor in Computer Science and Engineering, University of Kalyani, India. Former Dean Faculty of Engineering, Technology & Management 2008-2012(two consecutive terms), 29 years of teaching and research experiences. Served as Professor, Computer Applications, Kalyani Govt. Engineering College for two years. Served as Associate and Assistant Professor at University of North Bengal for sixteen years. Life Member of Computer Society of India since 1992 and life member of Cryptology Research Society of India. Member of AIRCC. Honorary Vice Chairman of CSI Kolkata Chapter. Chairman elect CSI Kolkata Chapter 2016-17. Working in the field of Network Security, Steganography, Remote Sensing & GIS Application, Image Processing, Wireless and Sensor Networks. Domain Expert of Uttarbanga Krishi Viswavidyalaya, Bidhan Chandra Krishi Viswavidyalaya for planning and integration of Public domain networks. Chief Editor, Advanced Computing: An International Journal, Associate Editor (Guest), Microsystem Technologies, Springer, Editor, Journal of Data Science, Inderscience, Editor of Proceedings of ETCS 2012, NIDS-98 and ERC-95 of CSI. Fifteen Scholars awarded Ph.D., Two submitted till January 2016 and 8 scholars are pursuing for their Ph. D. degree. Published five books from LAP- Lambert Academic Publishing, Germany and one book from IGI Global publishers, Indexed by Thomson Royter. Total number of publications 360 including 135 publications in various International Journals. Edited fifteen volumes as volume editor from Science Direct, Springer, CSI etc., Organizing various international Conferences of Springers and Science Direct.

