Indian Journal of Science and Technology, *Vol 10(20), DOI: 10.17485/ijst/2017/v10i20/113180, May 2017*
ISSN (Print) : 0974-6846
ISSN (Online) : 0974-5645

Hybrid Image Encryption Technique to Improve the Security Level by using (n, k, p) Gray Code and XOR Operation

Sudeept Singh Yadav[1]*,, Yashpal Singh[1], S.K. Sriwas[2]

[1]Department of Computer Science and Engineering, BIET, Jhansi – 284128, Uttar Pradesh, India; sudeept999@gmail.com, yash_biet@yahoo.co.in
[2]Department of Electronics and Communication, BIET, Jhansi – 284128, Uttar Pradesh, India; surendrasriwas@gmail.com

Abstract

Objectives: To enhance the performance of decomposition encryption methods, a modified image encryption technique is utilized in (n, k, p) Gray coding exhibit the application of (n, k, p) Gray coding in the encryption of images. **Methods/ Statistical Analysis:** We proposed a revised algorithm based on image encryption that improves the level of security for available (n, k, p) based bit plane decomposition encryption technique. The proposed hybrid methods starts with bit-plane decomposition of (n, k, p) Gray coding then shuffling each bit plane using random scrambling finally pixel substitution based on X-OR Operation. **Findings:** The experimental results and comparison demonstrates that proposed encryption algorithm have best performance in image encryption. **Applications/Improvements:** This algorithm could be utilized for securing protection in biological traits, imaging systems in medical field and digital video surveillance system. Our next plan will additionally enhance and examine the execution of (n, k, p)-Gray coding for data hiding and picture de-noising.

Keywords: Bit-Plane Decomposition, Image Encryption, (n, k, p)-Gray Code, Pixel Permutation, X-OR

1. Introduction

Recently, a big amount of digital information has been published, due to low cost, high availability and easy to transmit features of digital data, in computer readable formats, such as large archives of films, images, music, satellite pictures, books, newspapers and magazines have been made accessible for computer users. The major reason for fast growth of the internet is to access the huge amount of information in today digital world. In our community digital pictures have a more important role in comparison to the steady texts. So it needs serious protection of user's privacy for all applications and therefore there is need to pay much attention on security of digital images[1]. Image encryption[1,9] is one of the techniques available to secure the digital image. In the image encryption the original image is converted into unreadable format so that third party cannot understand them. Recently, in transmission of digital images most of the digital media requires more reliability in terms of security in mass storage.

During transmission of the pictures through the network is necessary to prevent the unauthorized access. It is the main motive of image encryption technique[3]. The main requirements for image encryption techniques are as high correlation between pixels, large redundancy and high capability as the image information has these special properties[4].

It is not very easy to use conventional encryption techniques due to special features of image information and it will also slow the process. Others requirement of image applications for transmission are - data compression, noise removal in actual-time processing, consistency in format of image, segmentation etc. there are major

*Author for correspondence

challenges to match the above requirements while maintaining high security and fidelity in real time operations on images[5-6].

Various methods are available now days for image encryption[5-8], Maximum of them is based on pixel shuffling such as image scrambling algorithm. The major drawback of pixel shuffling algorithm is that the value of the pixels remains unchanged and hence the image histogram remains same. Thus in concern with security the performance is not up to the mark. The solution is to combine the pixel shuffling and modification in gray level which results in better chaotic effect[22].

We combine pixel permutation and pixel substitution algorithm with (n, k, p)-gray-code[9], for making image encryption more rigid in different applications. A new term p introduced as distance parameter of existing (n, k) Gray code[10-11] method, as the value of n and p changes, the new value will also be changed.

Present Gray code value are suitable in different image processing areas such as compression[13], scrambling[15], filtering of image[12], recognition[14], estimation of motion for video processing[17] and stabilization of image[18].

In Section II we discussed the different techniques for image encryption. In Section III we studied in brief the (n, k, p)-Gray-code[9]. Section IV shows the algorithm using substitution and permutation with (n, k, p)-Gray-code. Section V presents various encryption quality measures. Section VI gives the comparative analysis of performances and the results of different methods. Section VII concludes the paper.

2. Various Image Encryption Techniques

These encryption techniques can be divided into three classes shown in Figure 1. Each class has various types of image encryption techniques.

- Position Permutation Based Algorithm
- Value Transformation Based Algorithm
- Hybrid Substitution Based Algorithm

2.1 Position Permutation based Algorithm

In this method the pixels are rescheduled of plain image. The rescheduling of the pixels can be performed by bit wise, pixel wise or block wise. Each pixel is rearranged by permutation key in bit wise technique. The main drawback of this method is that the conceptual information is reduced, while the high level security is in transposition of pixels and block level shuffling. In pixel permutation each pixel is reposition within the image data, while in block permutation pixels are grouped and reposition by using the same size key. Now days the position permutation based algorithm is widely used method.

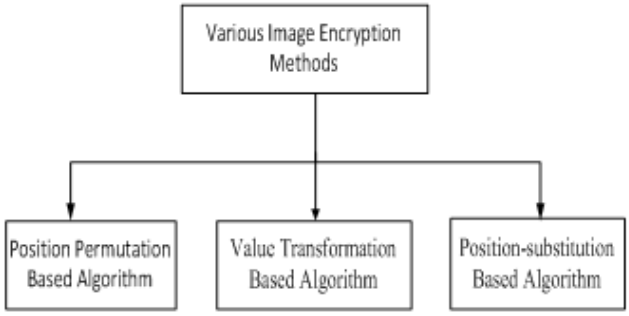

Figure 1. Various Image Encryption Methods.

2.2 Value Transformation Based Algorithm

In this algorithm each pixel value is changed by new value. The analysis of estimated value of newly generated pixel is processed by some computation on these pixels. This method is a computational analysis, the pixel value is taken as input p and follows the procedure based on defined rules and produces another value for the same pixel. Some other transposition algorithms may also available such as - Affine Transform, Encryption using SCAN, Block Based Image Encryption Algorithm and Double Random Phase Encoding.

2.3 Hybrid Substitutions based Algorithm

The above two algorithms are mixed in this technique. In this algorithm firstly pixel values are transforming by new values after that for substituting the pixel values is done by a key generator. This algorithm is used for the different various techniques.

3. (N, K, P) Gray Code

Consider there are two non-negative integer I and G of k-bits with base n, which is defined as $(i_{k-1},\ldots,i_2,i_1,i_0)_n$ and $(g_{k-1},\ldots,g_2,g_1,g_0)_n$ respectively. .i.e. $A=\sum_{i=0}^{k-1} a_i n^i$

and $G = \sum_{i=0}^{k-1} g_i n^i$. The (n, k, p)-Gray code[9] of A is called G and if the sequences are satisfied with the following equations:

$$g_i = \begin{cases} a_i, & if\ i > k-p-2 \\ (a_i + a_i + p + 1) \bmod n, & if\ 0 \le i \le k-p-2 \end{cases}$$

as $n \ge 2$, $0 \le p \le k\text{-}2$ and $0 \le i \le k\text{-}1$.

We can define the (n, k, p) Gray code by following matrix form. Consider If p = 0, then the matrix can be shown as:

$$\begin{pmatrix} g_0 \\ g_1 \\ g_2 \\ . \\ . \\ . \\ g_{k-2} \\ g_{k-1} \end{pmatrix} = \left(\begin{pmatrix} 1 & 1 & 0 & 0 & . & . & . & 0 \\ 0 & 1 & 1 & 0 & . & . & . & 0 \\ 0 & 0 & 1 & 1 & . & . & . & 0 \\ . & . & . & . & . & . & . & . \\ . & . & . & . & . & . & . & . \\ . & . & . & . & . & . & . & . \\ 0 & 0 & . & . & . & 0 & 1 & 1 \\ 0 & 0 & . & . & . & 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} a_0 \\ a_1 \\ a_2 \\ . \\ . \\ . \\ a_{k-2} \\ a_{k-1} \end{pmatrix} \right) \bmod n$$

By changing the value of distance parameter p and base n the different (n, k, p)-Gray-codes are generated.

This transformation is known as the (n, k, p)-Gray-code transformation

$G = (C_p\ A) \bmod n$

Given as the coefficient matrix

$$C_p = \begin{pmatrix} c_{11} & c_{12} & . & . & . & c_{1k} \\ c_{21} & c_{22} & . & . & . & c_{2k} \\ . & . & & . & & . \\ . & . & & . & & . \\ . & . & & . & & . \\ c_{k1} & c_{k2} & . & . & . & c_{kk} \end{pmatrix}$$

Where

$$C_{xy} \begin{cases} 1, & if\ x = y \\ 1, & if\ y = x + p + 1 \le k \\ 0, & otherwise \end{cases}$$

x, y, i, j, p, m and k are integers, $1 \le x, y \le k$ and $0 \le p \le k\text{-}1$.

4. Proposed Methodology

4.1 Image Encryption Process

Initially, we choose a gray scale image of M x N pixel, where each pixel stored in L bit. Further it will be transformed into (n, k, p) gray code before transmitting to other side. Consider X is the original 8-bit gray-level cover image of M x N pixels. It is represented as:

$$X = \{x_{ij} \mid 1 \le i \le M\ ,1 \le j \le N\ , x_{ij} \in \{0,1,...,255\}\}$$

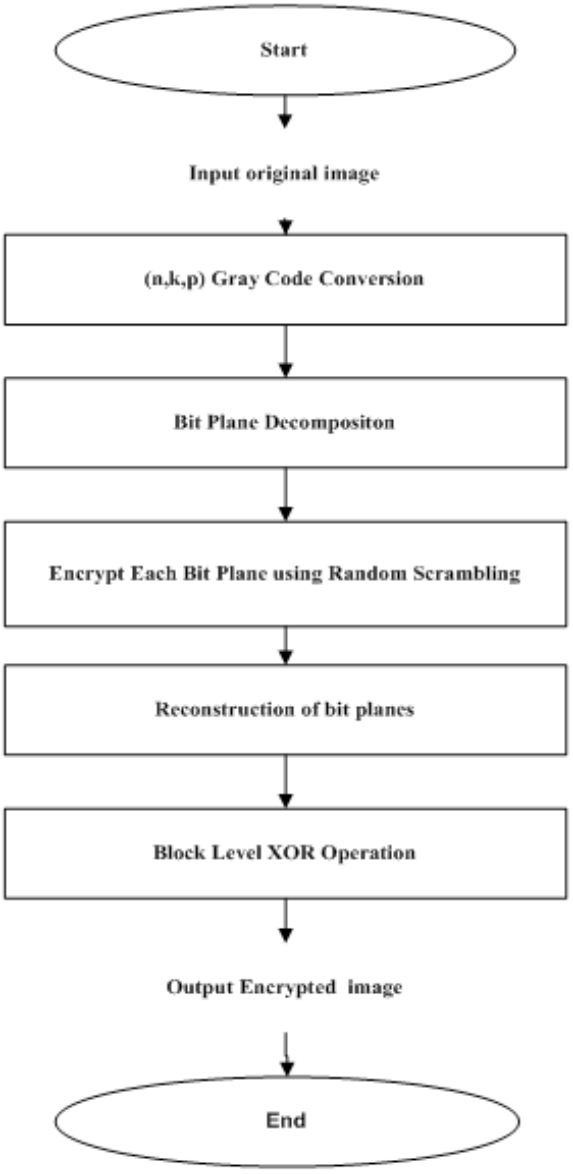

Figure 2. Block Diagram of proposed method.

The encryption scheme consists of four steps, i.e. (n, k, p)-gray-code transformation, decomposition of gray code bit plane, Random Scrambling and Reconstruction of bit plane, at last pixel substitution using X-OR Operation. Figure 2 shows the block diagram of proposed method.

4.1.1 (n, k, p)- Gray-Code Transformation

Firstly, G is considered as the (n, k, p)-gray-code of k bits base-n nonnegative gray image X, if the sequences are satisfied with

$$\mathbf{G} = (C_p \mathbf{X}) \bmod n$$

4.1.2 (n, k, p)-Gray-Code Decomposition of Bit Plane

An image is formed be several bits in gray level and also all bits are in the same level. i.e. all pixel is composed by k bits plane, therefore when we try to decompose the (n, k, p)-gray-code image, we obtained k bit-plane image which is shown by $G^{(l)}$, where l=0, 1….k-1.

Image G is decomposed in to l^{th} bit plane is evaluated by the formula expressed as below.

$$G^{(l)} = B^{(l)}(G)_{\text{Gl}}$$

At the position (m, n), l^{th} bit of pixel G(m,n) is:

$$G^{(l)}(m,n) = B^{(l)} = \begin{Bmatrix} 1 \; if \left(g(m,n)/2^{(l)}\right) \bmod 2 = 1 \\ 0 \qquad\qquad otherwise \end{Bmatrix}$$

Higher security is most important parameter so here we are using decomposition of image into its bit plane, because in this method we use eight different bit planes and each bit plane treated as in depend entity to encrypt.

4.1.2.1 Random Scrambling and Reconstruction

This subsequent step used random Scrambling technique on every bit plane of decomposed image[2]. Firstly change the bit-plane image $G^{(l)}$ into a one dimensional vector $V^{(l)}$. After that by using a random natural number generator that takes two different seeds to obtained random sequence R_S and R_D. The length of V is same as the length of R_S and R_D. The formula of bit plane Scrambling is shown as.

$$V(R_S(i)) \leftrightarrow V(R_D(i)) \; i = 0, 1, \ldots, (M \times N - 1)$$

When for every bit plane scrambling has been done, then merge all the Scrambled bit plane images to make a transform image X^T (Scrambled). Next we reconstruct the all scrambled bit plane image as their original level on bit plane. The Reconstruction of Scrambled image is calculated by the following formula.

$$X_T = \sum_{l=0}^{L-1} B^{-1(l)}\left(G^{(l)}\right)$$

At position (m, n) for a given pixel, we obtained.

$$X_T(m,n) = \sum_{l=0}^{L-1} 2^{(l)} \times G^{(l)}(m,n)$$

Each bit plane image is scrambled by using different scrambling random sequences, while every bit plane is being separately scrambled then the bits situated at the same coordinates in different bit-planes are almost not stay on the original positions. For each pixel, it's all bits of gray level, therefore; maybe come from those pixels located different positions. Consequently, the reconstructed gray levels of image are changed unavoidable. It is confirm that at the same time this method can perform positions exchange scrambling and gray level change scrambling[2].

4.1.2.2 Block Level XOR Operation

The Block level XOR operation changes the values of pixels thus makes the image meaning-less. Block level XOR operation is denoted by $\oplus$. There are 2 pixel × 2 pixel block partitioned of transformed image X_T.

Then Xt is encrypted of every block Bi,j with block level XOR operation using 32 bit key size which is further subdivided into four keys of 8 bits i.e. K1, K2,K3, K4 respectively.

$$P'_{11} = P_{11} \oplus K_1$$

$$P'_{12} = P_{12} \oplus K_2$$

$$P'_{21} = P_{21} \oplus K_3$$

$$P'_{22} = P_{22} \oplus K_4$$

Where $P_{i,j}$ represents the value of pixel at (i, j) position, in the image of every block and also the encoded image is called cipher image X_C. In this algorithm 32 bit long key used which is enough to prove the strength of this method.

4.2 Image Decryption

We get the input cipher gray-scale image Xc of M x N pixel, where each pixel stored in L bit and the output image is original as sending before encryption.

4.2.2.1 Block Level X-OR Operation

Step first is to perform the block level XOR operation on encrypted image X_C. Further cipher image X_C is divided into 2 × 2 pixel blocks. Using block level XOR operation for each pixel Bij of Xc is decrypted with identical keys (K_1, K_2, K_3, K_4), which is used at the encryption end[19].

$$P_{11} = P'_{11} \oplus K_1$$
$$P_{12} = P'_{12} \oplus K_2$$
$$P_{21} = P'_{21} \oplus K_3$$
$$P_{22} = P'_{22} \oplus K_4$$

4.2.2.2 Bit Plain Decomposition of Encrypted Image

Bit plane decomposition of the Decrypted image X_D into l^{th} bit-plane is computed using the formula described as.

$$X^{(l)}(m,n) = B^{(l)} = \begin{Bmatrix} 1 if \left(x(m,n) / 2^{(l)} \right) \bmod 2 = 1 \\ 0 \qquad\qquad otherwise \end{Bmatrix}$$

Transform the bit-plane image $X_D^{(l)}$ into a 1-D vector V(l).

4.2.2.3 Anti Scrambling and Reconstruction

In this step antiscrambling is applied on every bit plane image of decrypted image X_D. Then in the encryption process we will use a random natural number generator and same number of keys to generate random sequences[21] R_S and R_D that have equal length as vector V then antiscrambles one dimensional vector V as given formula:

$$V^{(l)}(R_S(i)) \leftrightarrow V^{(l)}(R_D(i)) i = 0,1,....(M \times N - 1); l = 0,1,....L-1$$

At last step antiscrambled bit-plane images are merged, and we found (n, k, p)-Gray images G by using the formulas at encryption time.

4.2.2.4 Inverse (n, k, p)-Gray-Code Transformation

An inverse (n, k, p)-gray-code transformation formula is given below:

$$A = (C_p^{-1} G) \bmod n$$

Where *p, k, m, n* and all matrices presented in previous steps and the inverse matrix of *Cp* is c_p^{-1}.

5. Evaluation Metrics

In this encryption process, there are some specific criteria for comparing with some well known algorithms such are: the MSE, PSNR, UAIC, NPCR and CC.

5.1 Mean Square Error (MSE)

This technique is very famous for checking the quality of encrypted image[19]. It is expressed as the average of the squares of the differences of their intensities of cipher images and plain images. The formula as given below:

$$MSE = \frac{1}{MN} \sum_{i=1}^{M} \sum_{j=1}^{N} (C(i,j) - C'(i,j))^2$$

On basis of mean square error value is large then the quality of image is very poor means the quality of encryption is better and C (i, j) is the primary image and C'(i, j) is cipher image.

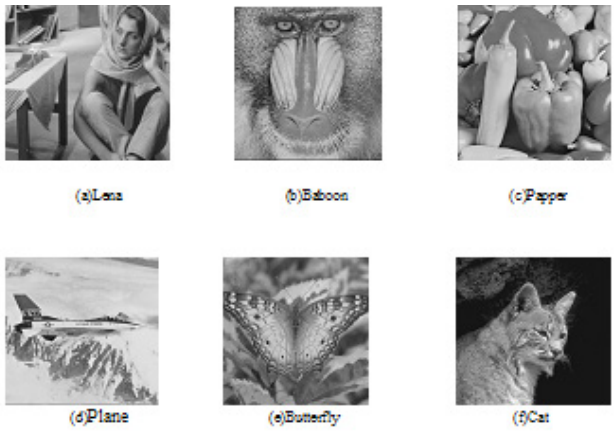

Figure 3. Test Images of size 512×512.

5.2 Peak Signal to Noise-Ratio (PSNR)

This PSNR describes the evaluation of reconstructed encrypted image[24]. For making differences into the cover and encrypted image the parameter peak signal to noise ratio is used. The main advantage is to easy to compute. It can be calculated as:

$$PSNR = 20 \log 255^2 / MSE$$

If the PSNR value is low then encrypted image is of poor quality hence encryption quality is high.

5.3 UAIC and NPCR

To check the impact for changing one pixel on the whole cipher image have mainly two common computations where the proposed algorithm[20]:

Number of Pixel Change Rate (NPCR)

$$NPCR = \frac{\Sigma_{i,j} D(i,j)}{W \times H} \times 100\%$$

Unified Average Intensity Change (UAIC)

$$UACI=\frac{1}{W\times H}\left[\Sigma_{i,j}\frac{C_1(i,j)-C_2(i,j)}{255}\right]\times 100\%$$

Where C1 is original image and C2 is ciphered image. The size of C1 is same as C2. The gray-scale values of the pixels are C_1 (i, j) and C_2(i, j) at grid (i, j).

By using C_1(i, j) and C_2(i, j) we can calculate D(i, j) and if both C_1 and C_2 image are same at pixel value at location (i, j) then the value is set to 1 of D(i, j) otherwise the value is 0. Columns and rows are W and H defined respectively of the image.

6. The Correlation Coefficient

To check the Correlation among pixels of image the most widely quality parameter is the correlation coefficient. It calculates the correlation at the same indices between the pixels in plane and cipher images[19]. It can be calculated as following formula:

$$r_{xy}=\frac{\operatorname{cov}(x,y)}{\sqrt{D(x)}\sqrt{D(y)}}$$

The gray scale values of two pixels at the same locations in the plane and cipher images are represented by x and y. Numerically it is calculated by following formula as:

$$E(x)=\frac{1}{L}\sum_{l=1}^{L}X_l$$

$$D(x)=\frac{1}{L}\sum_{l=1}^{L}\left(x_l-E(x)\right)^2$$

$$\operatorname{cov}(x,y)=\frac{1}{L}\sum_{l=1}^{L}\left(x_1-E(x)\right)\left(y_1-E(y)\right)$$

7. Experimental Results

In this observation Figure 3, shows the several images of size 512 × 512, and performed the image encryption using permutation and substitution method.

7.1 (n, k, p)-Gray-Code Bit-Plane Decomposition Analysis

This decomposition technique is beneficial to decompose an image for non-binary bit-planes i.e. base is greater than two and also for binary bit-planes i.e. base is equal to two. The (n, k, p)-gray-code bit planes changes as the values of base n and distance parameter p changed. The bit planes k is calculated on the bases of base value. A grayscale image can be decomposed into eight binary bit-planes for base taken as two. Figure 4 present that as the value of distance parameter p changes then the most significant bit does not change but the least significant bit planes content differs. As the definition of the (n, k, p)-gray-code contains the MSB remains same.

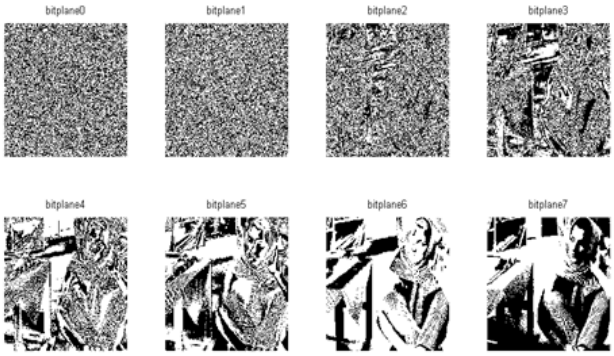

Figure 4. (n, k, p) Gray code bit plane decomposition of a grayscale image; n = 2, k = 8 and p = 0.

Original images can be decomposed by decomposition method into binary and non binary bit planes. The result of decomposition and number of the (n, k, p)-gray-code bit planes depends on parameters that is used for different applications in image encryption techniques.

7.2 Simulation Results and Analysis

We have shown the process to transforms the new (n, k, p)-gray-code for bit-plane by rearranging steps and doing pixel-scrambling then X-OR based pixel substitution.

To exhibited our strategy we utilized gray-images of Lena as Shown in Figure 5(a). The outcome after (n, k, p)-gray-code bit-plane permutation and after that pixel substitution with the help of secret key[16] R_S=240 and R_D=65 are presented in Figure 5(b). By observing figure it is clear that pixel rearranging impact is very nice and cipher image looks like a blur and noisy.

Figure 5(a) demonstrates the histogram of plain image of Lena. In Figure 5(b) proposed permuted method has shown Histogram of the encrypted image. In the Figure 5 it is clearly stated that the histogram of the both the images are different, so we can state that the gray value estimations of pixels are changed in encrypted image.

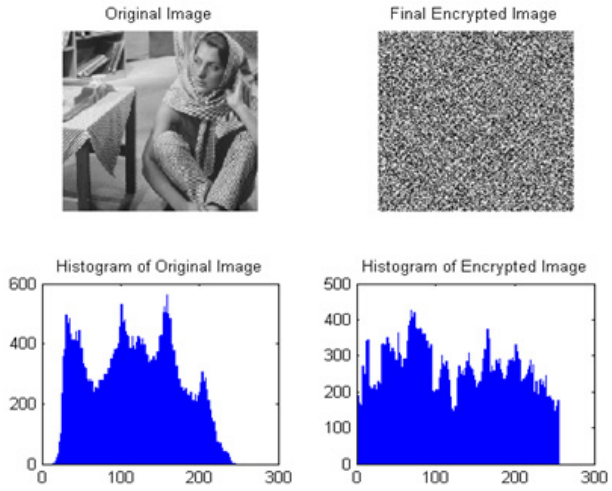

Figure 5. Image encryption method (a) Original image and its histogram. (b) Encrypted image and its histogram; n = 2, k = 8, and p = 0.

7.3 Neighboring Pixel Correlation Analysis

Neighboring pixel correlation examination is exhibiting an algorithm's expertise for resists statistic attacks[25,26]. Here, we correlate length dissolution of two vertically, horizontally and diagonally adjoining elements in the unusual and their interchangeable cipher images individually exposed polished encryption algorithm.

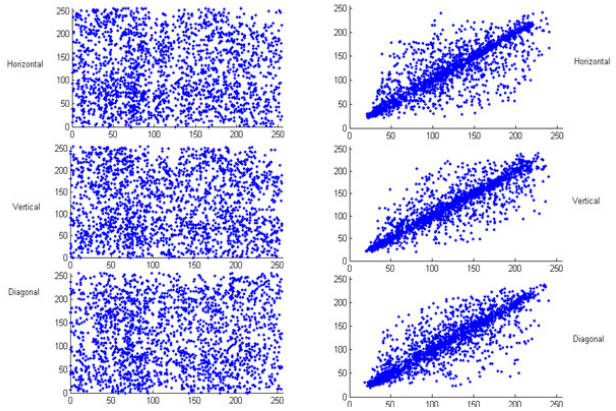

Figure 6. Correlation of adjacent pixels at different directions before and after image encryption.

We have taken 2048 pixels from the plain image and cipher image, respectively. In Figure 4 the encrypted image shows the distribution of appropriate pixels, where adjacent pixels represents less correlation. There is variation in pixel values and it spread out through whole range of image element values. It shows that the proposed algorithm is experienced to go through the statistic attack[26], where as in Figure 6, the sample pixels and their neighboring pixels shows distribution plots at horizontal, vertical and diagonal directions where the distribution of neighboring pixels in the original image shown in second

Table 1. Result of Quality Parameters on Different Image

Image Name	Peak Signal To Noise Ratio (PSNR)	Number Of Pixel Change Rate (NPCR)	Unified Average Change Intensity (UACI)	Correlation Coefficient (CC)
Lena	18.1714	99.2353	15.3380	3.0503e-005
Baboon	19.4404	99.1655	13.6381	3.0488e-005
Papper	18.1302	99.3415	13.7817	3.0645e-005
Airplane	16.7303	98.9863	7.2696	3.0284e-005
Butterfly	19.0364	99.0634	14.7127	3.0478e-005
Cat	16.5594	99.2041	24.3690	3.0414e-005

Table 2. Level of security protection in different algorithms

Techniques Parameters	BPE-XOR	SBE-AES	SBE-LBP	(n, k, p) gray code	Proposed method
Decomposition result	fixed	fixed	fixed	parameter dependent	parameter dependent
Data Encryption	XOR based	AES	XOR	MOD	Random Shuffling Plus XOR
Pixel Scrambling	No	No	No	Parameter Dependent	Yes
Shuffling Process	No	No	No	Parameter Dependent	Yes
Change image Data Value	Yes	Yes	Yes	Yes	Yes

column and these picture elements are found neighboring the diagonal line, which shows neighboring pixels in the original image is close to each other or are equal shows high correlation among pixels.

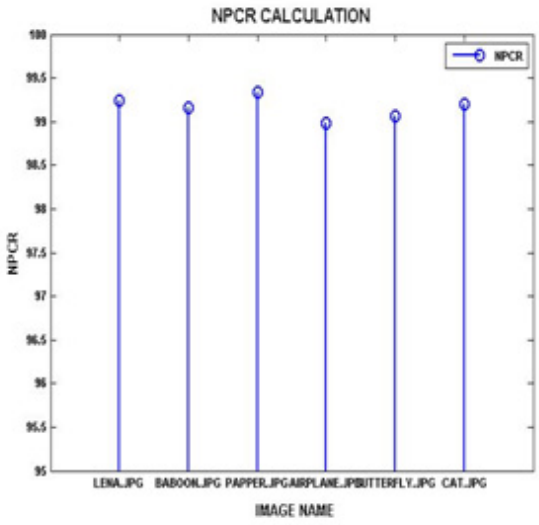

Figure 7. Shows NPCR comparison on different images by proposed Encryption Methods.

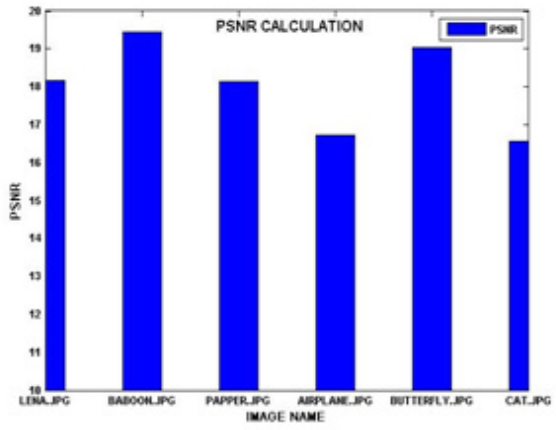

Figure 8. Shows Average PSNR comparison on different images by proposed Encryption Methods.

Table 1 shows the average quality parameter among different images by the given proposed methods.

Figure 7 and Figure 8 shows the graphical representation of comparison on different images in proposed method with respect to NPCR and PSNR respectively.

Table 2 shows the improved encryption standards for the SBE-AES, BPE-XOR, SBE-LBP calculations and (n, k, p)-gray-code by Y. Zhou and et. al[9]. As far as security and from encryption perspective, the proposed hybrid algorithm has a bigger number of points of interest than existing techniques. Accordingly, the proposed algorithm presents more chances for enhancing security protection contrasted with the available bit-plane decomposition based techniques.

8. Conclusion

The hybrid image encryption algorithm is proposed in this paper using (n, k, p)-gray-code[9] in image encryption to improve the security level of existing bit-plane decomposition based encryption algorithm. The proposed algorithm starts with (n, k, p)-gray-code bit-plane decomposition then rearranging each bit plane using random scrambling finally pixel substitution based on X-OR Operation. The experimental results of proposed method have shown the best performance in image encryption algorithm. It could be utilized for securing protection in biological traits, imaging systems in medical field and digital video surveillance system. Further this paper will additionally improve and analyzing the execution of the (n, k, p)-gray-code in data hiding and picture de-noising.

9. References

1. Ozturk I and Sogukpınar I. Analysis and comparison of image encryption algorithms. Transactions on Engineering, Computing and Technology. 2004; 3:1305-5313.
2. Tamilselvi R, Ravindran G. Image encryption using pseudo random bit generator based on logistic maps with radon transform. Indian Journal of Science and Technology. 2015; 8(11):1-7. Crossref.
3. Potdar V and Chang E. Disguising text cryptography using image cryptography. UK: International Network Conference in Plymouth. 2004 6 - 9 July.
4. Li X, Knipe J and Cheng H. Image Compression and Encryption Using Tree Structures. Pattern Recognition Letters. 1997; 18(8):2439-51.
5. Zhang G and Liu Q. A novel image encryption method based on total shuffling scheme. Optics Communications. 2011; 284:2775-80. Crossref.
6. Zhang Y, Xia J, Cai P and Chen B. Plaintext related two-level secret key image encryption scheme. TELKOMNIKA. 2012; 10:1254-62. Crossref.

7. Wang X and He G. Cryptanalysis on a novel image encryption method based on total shuffling scheme. Optics Communications. 2011; 284:5804-07. Crossref.
8. Eslami Z and Bakhshandeh A. An improvement over an image encryption method based on total shuffling. Optics Communications. 2013; 286:51-5. Crossref.
9. Yicong Zhou, Karen Panetta, Sos Agaian, Philip Chen CL. (n, k, p)-Gray Code for Image Systems. IEEE Transactions On Cybernetics. 2013 April; 43(2):515-29. Crossref PMid:22922727.
10. Guan D-J. Generalized Gray code with applications. Proceedings of the National Science Council, ROC(A). 1998; 22(6):841-8.
11. Sankar KJ, Pandharipande VM and Moharir PS. Generalized Gray codes. Proceedings of International ISPACS. 2004; p. 654-9.
12. Ben-Artzi G, Hel-Or H and Hel-Or Y. The Gray-code filter kernels. IEEE Transactions on Pattern Analysis and Machine Intelligence. 2007 Mar; 29(3):382-93. Crossref PMid:17224610.
13. Tseng H-W and Chang C-C. Anti-pseudo-gray coding for VQ encoded images over noisy channels. IEEE Communications Letters. 2007 May; 11(5):443-5. Crossref.
14. Chen W-S, Chih K-H, Shih S-W and Hsieh C-M. Personal identification technique based on human IRIS recognition with wavelet transform. Proceedings of IEEE ICASSP. 2005; 2:949-52.
15. Ding W, Yan W and Qi D. Digital image scrambling. Progress in Natural Science. 2001; 11(6):454-60.
16. Nasir I, Ying W and Jianmin J. A new robust watermarking scheme for color image in spatial domain. Proceedings of 3rd International IEEE Conference on SITIS. 2007; p. 942-7. Crossref.
17. Erturk S. Locally refined Gray-coded bit-plane matching for block motion estimation. Proceedings of 3rd ISPA. 2003; 1:128-33. Crossref.
18. Ko S-J, Lee S-H, Jeon S-W and Kang E-S. Fast digital image stabilizer based on Gray-coded bit-plane matching. IEEE Transactions on Consumer Electronics. 1999 Aug; 45(3):598-603. Crossref.
19. Jawad Ahmad and Fawad Ahmed. Efficiency Analysis and Security Evaluation of Image Encryption Schemes International Journal of Video and Image Processing and Network Security IJVIPNS-IJENS. 2012; 12(04).
20. Yue Wu, Joseph P Noonan and Sos Agaian, NPCR and UACI Randomness Tests for Image Encryption Cyber Journals: Multidisciplinary Journals in Science and Technology. Journal of Selected Areas in Telecommunications (JSAT), April Edition. 2011.
21. Roy S, Sadhukhan S, Sadhu S, Bandyopadhyay SK. A novel approach towards development of hybrid image Steganography using DNA sequences. Indian Journal of Science and Technology. 2015 Sep; 8(22):1-7. Crossref.
22. Leila Habibpour, Shamim Yousefi, Mina Zolfi Lighvan, Hadi S Aghdasi. 1D Chaos- based Image Encryption Acceleration by using GPU. 2016 Feb; 9(6).
23. Aloha Sinha, Kehar Singh. A technique for image encryption using digital signature. Optics Communications. 2003; 218(4-6):229-34.
24. Saravana Kumar G, Parthasarathy V, Praveen Kumar E, Thiyagarajan S, Siva Saravana Babu S, Sudhakar S. A Comprehensive Compression and Encryption Scheme for Secured Medical Images Communication. Indian Journal of Science and Technology. 2016 April; 9(16).
25. Chen G, Mao Y and Chui CK. A symmetric image encryption scheme based on 3D chaotic cat maps. Chaos Solitons Fractals. 2004 Jul; 21(3):749-61. Crossref.
26. Pareek NK, Patidar V and Sud KK. Image encryption using chaotic logistic map. Image and Vision Computing. 2006 Sep; 24(9):926-34. Crossref.