VOL. 12, NO. 11, JUNE 2017 ISSN 1819-6608
ARPN Journal of Engineering and Applied Sciences
©2006-2017 Asian Research Publishing Network (ARPN). All rights reserved.
www.arpnjournals.com

GRAY CODE (n, k, p) BASED PIXEL SUBSTITUTION AND AFFINE TRANSFORM BASED GRAY CODE BIT PLANE PERMUTATION TECHNIQUE FOR SECURE IMAGE ENCRYPTION

Sudeept Singh Yadav, Yashpal Singh and S. K. Sriwas
Bundelkhand Institute of Engineering and Technology, Jhansi, India
E-Mail: sudeept999@gmail.com

ABSTRACT

Image encryption techniques are used to prevent image from unauthorized access and it play a very important role to provide confidentiality or privacy. To make image encryption technique more robust for various applications in imaging systems, we combined pixel permutation and pixel substitution techniques along with the concept of (n, k, p) Gray code. The algorithm is based on (n, k, p) Gray code bit-plane decomposition and Affine transform based each bit plane pixel permutation. (n, k, p) Gray code transforms based bit plane shuffling and pixel scrambling provides robustness in image encryption. The experimental results have shown that the presented new encryption algorithm provides excellent performance in image encryption.

Keywords: Bit-plane decomposition, (n, k, p) Gray code, Image encryption, Pixel permutation, X-OR operation.

1. INTRODUCTION

In the past decade, due to low cost, high availability and easy to transmit features of digital data, large amount of digital information has been published in computer readable formats, such as big archives of films, large amount of images and music, satellite pictures, books, newspapers, and magazines have been made accessible for computer users. With the help of Internet it is possible for the human to access these huge amounts of information and it is major reason for rapid growth of the internet in the digital world today. In our society digital images play a more significant role rather than the traditional 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. Image encryption 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, many digital services require reliable security in storage and transmission of digital images [1].

Image encryption techniques are used to prevent image from unauthorized access and it provide confidentiality or privacy, when exchanging digital images over various types of networks. So encryption is mostly used preferred technique for protecting the transmitting information [2].

The main idea behind the image encryption technique [3] is to prevent the image from the unauthorized access when transmitting the image over the network. Since the image information contains high correlation among pixels, high capability and large amount of redundancy among the pixels that imposes special requirements on any encryption technique [4].

Due to image data special features it is very difficult to apply traditional encryption methods and it will be slow to process. Besides this sometimes, image applications have their own requirements such as data compression, real-time processing like noise removal, segmentation, fidelity reservation, image format consistence etc. for transmission. These requirements along with high security and high quality demands create great challenges to real-time imaging practice [5-6].

Nowadays, variety of methods are available that can do Image Encryption [5-8], and the most of them are pixel shuffling techniques in which pixels change their relative position within the image based on some predefined algorithm. Pixels shuffling based image encryption techniques have one major drawback that it cannot change the pixel value so the histogram of image remains unchanged. Hence, their security performances may not be well. So we need such encryption method that use the combination of the pixel permutation and gray level modification which can handles good chaotic effect.
To make image encryption technique more robust for various applications in imaging systems, we combined pixel permutation and pixel substitution techniques along with the concept (n, k, p) Gray code [9]. In (n, k, p) Gray code techniques, distance parameter p is integrates with the concept of the (n, k)-Gray code [10-11]. This (n, k, p)-Gray code changes as the values of the base n and the distance parameter p vary.

Existing Gray codes can be applicable in image processing area, including image filtering [12], compression [13], recognition [14], scrambling [15], and watermarking [16], as well as motion estimation for video processing [17] and image stabilization [18].

The later chapters are arranged as follows: Various image encryption techniques are briefly introduced in Section II. Section III introduces the detail of (n, k, p)-Gray code. Section IV describes our proposed method based on the (n, k, p)-Gray code based pixel substitution and Affine transform based substitution. Section V presents quality parameters to describe encryption quality. Section VI shows the result of proposed method and the comparative performance analysis. Section VII concludes the paper.

©2006-2017 Asian Research Publishing Network (ARPN). All rights reserved.

2. VARIOUS IMAGE ENCRYPTION METHODS

The image encryption algorithms can be represented into three major categories. Each category has various types of image encryption methods.

- Position Permutation (Transposition) based Algorithm.
- Value Transformation (Substitution) Based Algorithm.
- Position- Substitution Based Algorithm

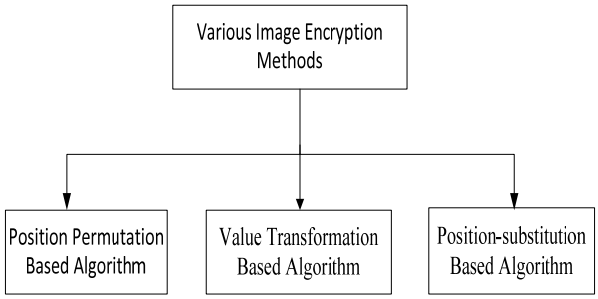


Figure-1. Various image encryption methods.

A. Position Permutation (Transposition) based algorithm

In Position permutation method elements of the plain image are rearranged. The rearrangement of element can be possible by bit wise, pixel wise or block wise. In bit wise permutation bits of image each pixel are shuffled using some permutation key But drawback of permutation of bits is that it decreases the perceptual information, whereas the transposition of pixels and blocks produce high level security. In the pixel wise permutation every pixel is permuted to another position within the image. In the block wise permutation pixels are taken as a group and permuted with the same size key. The Position Permutation Based Algorithm is mostly used technique for the image encryption.

B. Value Transformation based algorithm

In values Transformation Based algorithm value of each pixel is modified to some other new value. The evaluation of the new value of pixel is computed by performing some algorithm on pixel. Algorithm is a mathematical computation where pixel value is taken as input performs the operation based on some formulas and produces a new value for that pixel. Lot of value Transformation Based Algorithm are available such as Encryption Using SCAN, Double Random Phase Encoding, Affine Transform, Block-Based Image Encryption algorithm etc.

C. Position- Substitution based algorithm

Position Substitution technique is the combination of both position permutation and value transformation technique. In this technique first pixels value are transform to other values and then a key generator is used to substitute the pixel values. The Position-Substitution Based Algorithm is use for the various techniques.

3. (N, K, P)-GRAY CODE

Suppose I and G are two non-negative integer of k-bits with base n, which is represented as $(i_{k-1},...,i_2,i_1,i_0)_n$ and $(g_{k-1},...,g_2,g_1,g_0)_n$ respectively. .i.e. $A=\sum_{i=0}^{k-1} a_i n^i$ and $G=\sum_{i=0}^{k-1} g_i n^i$. G is called the (n, k, p)-Gray code [9] of A, if the sequences are satisfied with

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

Where $0\le i\le k-1,\ n\ge 2, and\ 0\le p\le k-2$.

The definition of the (n, k, p)-Gray code can be represented in the matrix format. For example, if p = 0, it can be written 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 selecting values of the base n and distance parameter p, the (n, k, p)-Gray code generates different Gray codes.

The following transformation is called the (n, k, p)-Gray code transform

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

Where 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

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

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

©2006-2017 Asian Research Publishing Network (ARPN). All rights reserved.

4. PROPOSED METHODOLOGY

A. Image Encryption

The phase of Image encryption process starts by selecting a gray scale image of M×N pixel size with L bit per pixel, which is to be converted into (n, k, p) gray code before transmitting to the other end. Suppose X is the original 8-bit gray-level cover-image of M×N pixels. It is denoted as:

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

The proposed encryption scheme consists of three procedures, i.e. (n, k, p) Gray code conversion, Gray code bit plane decomposition and Random Scrambling using affine Transform.

a) (n, k, p)-Gray-code transforms

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

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

b) Bit plane decomposition of (n, k, p) gray code

Gray level of a pixel of an image is composed by multiple bits, their all bits in same level creates a binary plane, called bit plane. Since every pixel is form by k bits plane, So when we decompose it, we can get k bit plane image which is described by $G^{(l)}$, where l=0, 1….k-1.

Decomposition of image G into l^{th} bit plane is computed by the formula expressed as below.

$$G^{(l)} = B^{(l)}(G)$$

If *G(m, n)* is a pixel located at (m, n), then the l^{th} bit of *G(m,n)* is:

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

The purpose of using decomposition of image into its bit plane is for providing higher security because in our method we use eight different bit plane and each bit plane treated as in depend entity to encrypt.

c) Image encryption using affine transform

To encrypt the image we redistribute the pixel values to different location using affine transform technique with four 8-bit keys. Affine transform fractures the correlation between adjacent pixels of an image. Affine cipher is one-to-one mapping that is a symbol in the plaintext can be transformed to a unique symbol in the cipher text. In Affine cipher, the relationship between the plaintext P and the cipher text C is

$$C = (K_0 + K_1 \times P) \bmod N$$

$$P = (C + (-K_0)) \times K_1^{-1}) \bmod N$$

Where $0 < \mu < 4 \ and \ a_p \in [0,1]$

Where $\gcd(K_1, N) = 1$, K_1^{-1} is the multiplicative inverse of K_1 and $-K_0$ is the additive inverse of K_0.

In the propose technique we have used a 32 bit symmetric key. The 32 bits of key is divided into 4 sub-keys K1, K2, K3, and K4 of 8 bits each. The key is chosen is in such a way that the second sub-key is relatively prime to width of the image and the fourth sub-key is relatively prime to the height of the image i.e. $\gcd(K_2, M) = 1, \ and \ \gcd(K_4, N) = 1$ The reason of choosing $\gcd(K_2, M) = 1, \ and \ \gcd(K_4, N) = 1$ is that the transformed coordinate will be unique in the range of 1 and M due to $\gcd(K_2, M) = 1,$ and 1 to N due to $\gcd(K_4, N) = 1$. If the sub-keys are not prime to height and width of the image, the transformation process may map more than one location to same destination.

We have each bit plane image $G^{(l)}$ of size M × N with pixel locations ranging from (1, 1) to (M, N). The pixel location (p, q) where $p \in \{0,1,2,...,M-1\}$ and $q \in \{0,1,2,...,N-1\}$ of secret bit plane image $X_C^{(l)}$ is transformed to new location(p', q') by

$$p' = (K_0 + K_1 \times p) \bmod M$$

and,

$$q' = (K_2 + K_3 \times q) \bmod N$$

After applying the affine transform on each and every bit plane image, we get encrypted image X_C and now it is transformed by sender to receiver.

Note that on every bit plane shuffling, we also apply the circular left shift key operations so that same location on every bit plane images may take the different location. We means that first time we apply K1,K2,K3,K4 and next time K2,K3,K4,K1 and so on.

B. Image Decryption

At the receiver side the input is a gray scale encrypted image X_C of M × N pixel size with L bit per pixel. This is to be converted into its original form as before sending.

a) Bit plane decomposition of encrypted image

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

©2006-2017 Asian Research Publishing Network (ARPN). All rights reserved.

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

We then decrypts each bit-plane image $X_C^{(l)}$ using affine transform.

b) Image decryption using affine transform

We have an encrypted bit plane image $X_C^{(l)}$ of size M×N with pixel locations ranging from (1, 1) to (M, N). For each pixel location (p', q') where $p' \in \{0,1,2,...,M-1\}$ and $q' \in \{0,1,2,...,N-1\}$ of decrypted bit plane image $X_D^{(i)}$ is transformed to original location (p, q) of original image plane $G^{(l)}$ by

$$p = (K_0 + K_1 \times p') \bmod M$$

$$and,$$

$$q = (K_2 + K_3 \times q') \bmod N$$

On every bit plane shuffling, same key operations is applied.

Next step is to merge the antiscrambled (decrypted) bit-plane images according to their original levels on bit-planes and gained an (n, k, p) Gray image G by using the formula used at encryption.

c) Inverse (n, k, p)-Gray code transform

The following transformation is called the inverse (n, k, p)-Gray-code transform:

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

Where all matrices and *m, n, p, k* are given previously and c_p^{-1} is the inverse matrix of C_p.

5. EVALUATION METRICS

In this investigation, the set of criteria for comparing the selected algorithms are: the MSE, PSNR, UAIC, NPCR and CC.

A. Mean Square Error (MSE)

MSE is one of the most widely used quality measurement technique to check quality of encryption technique. The MSE [19] can be defined as the measure of average of the squares of the difference between the intensities of the encrypted image and the original image. It is represented as:

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

Where C(i, j) is the original image and C' (i, j) is the encrypted image. If the value of MSE is large then it means that the quality of image is poor, in turn, quality of encryption is better.

B. Peak Signal to Noise Ratio (PSNR)

The PSNR describes the measure of reconstruction of the encrypted image. This quality parameter is used for discriminating between the cover and encrypted image. The easy computation is the advantage of this measure. It is formulated as:

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

A low value of PSNR means that the constructed image is of poor quality hence encryption quality is high.

C. UACI and NPCR

Two common measures are used to test the influence of one pixel change on the whole encrypted image by the proposed algorithm [20]:

Number of Pixel Change Rate (NPCR)

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

Unified Average Change Intensity (UACI)

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

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

D(i, j) is determined by C_1(i, j) and C_2(i, j), if pixel value at (i, j) location in both C_1 and C_2 image are same then the value of D(i,j) is set to 1 otherwise it is set to 0 W and H: columns and rows of the image.

D. The Correlation Coefficient

Correlation coefficient is one of the most useful quality parameter to check the correlation among pixels within the image. It measures the correlation between pixels in the plain and the cipher images at the same indices [19]. This parameter can be calculated as follows:

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

Where x and y are the gray-scale values of two pixels in the plane and cipher images at the same location. In numerical computations, the following discrete formulas can be used:

©2006-2017 Asian Research Publishing Network (ARPN). All rights reserved.

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

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

$$\mathrm{cov}(x,y) = \frac{1}{L}\sum_{l=1}^{L}\left(x_l - E(x)\right)\left(y_l - E(y)\right)$$

6. EXPERIMENTAL RESULTS

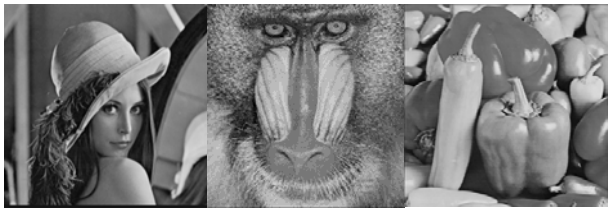
In the experiment, we do image encryption using permutation and substitution technique and we are taken different images of size 512× 512 shown in Figure-2.

A. (n, k, p) Gray code bit plane decomposition analysis

The main advantages of this decomposition method is that it can decompose an image not only into binary bit planes (for base n = 2) but also into non binary bit planes (for base n > 2). When the value of base-n and distance parameter p changes, the (n, k, p)-Gray-code bit planes will be also changed.

For a specific image, the number of bit planes k is determined by the base-n value. For example, a gray scale image with gray levels between 0 and 255 can be decomposed into 8 ($k = \log_2 255 = 8$) binary bit planes for n = 2. Figure-3 shows an example of this demonstrates that the most significant bit plane does not change while the content of several of the least significant bit planes differs as the p values change. This is because, according to definition the (n, k, p)-Gray code keeps the most significant bit unchangeable.

The (n, k, p) Gray code bit-plane decomposition can decompose an image into binary and nonbinary bit planes. Both the decomposed results and the number of the (n, k, p)-Gray-code bit planes are parameter dependent. Those allow it to be used for many applications in image system.



(a)Lena (b) Baboon (c)Papper

(d)Plane (e) Butterfly (f)Cat

Figure-2. Test images of size 512×512.

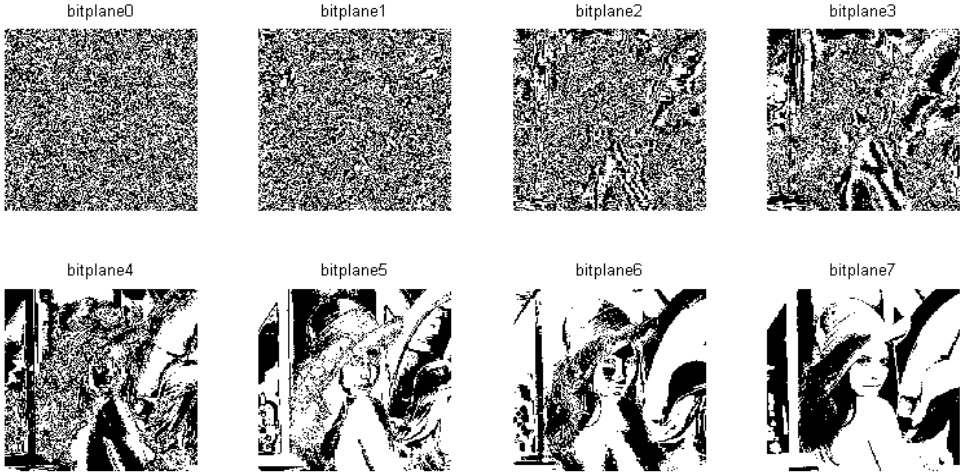


Figure-3. (n, k, p)-Gray code bit-plane decomposition of a grayscale image; n = 2, k=8 and p = 0.

©2006-2017 Asian Research Publishing Network (ARPN). All rights reserved.

A. Simulation Results and Analysis

We apply the hybrid method that use the (n, k, p) Gray-code transforms based pixel substitution and Affine Transform based every (n, k, p) bit plane pixels permutation technique.

To demonstrate our method we used the gray image Lena as Shown in Figure-4(a), the results after (n, k, p) Gray code pixel substitution and affine transform based every bit plane pixel permutation are shown as in Figure-3(b). From the Figure it is clear that the pixel shuffling effect is very good and the encrypted image seems as a salt and paper noise.

Figure-4 (a) shows the histogram of original image of Lena. Histogram of the encrypted image permuted by the proposed method is shown in Figure-4(b). From the Figure-3 it is clear that the histogram of the both image are not same so we can say that in encrypted image, the gray values of pixels are changed .

B. Adjacent pixel correlation analysis

Adjacent pixel correlation analysis is to show an algorithm's capability for withstanding statistic attacks [21]-[22]. Here, we analyse the intensity distribution of two horizontally, vertically, and diagonally adjacent pixels in the original and its corresponding encrypted images by the presented new encryption algorithm.

Some 2048 pixels are randomly selected from the original image and the encrypted image, respectively. Figure-5 plots the distribution of these 2048 sample pixels and their adjacent pixels at the horizontal, vertical, and diagonal directions. The first and second column shows the distribution of adjacent pixels in the encrypted image and original image respectively. As can be seen, pixels are located in or around the diagonal line. This means the adjacent pixels in the original images are equal or close to each other. They have high correlations. On the other hand, the first column in Figure-5 shows the distributions of adjacent pixels in the encrypted image. These adjacent pixels show less correlation. Their pixel values significantly vary and spread out in the entire range of the image pixel values. This demonstrates that the presented encryption algorithm is able to withstand the statistic attack.

The average quality parameters among different images by the corresponding proposed method are tabulated in Table-1. Figure-6 and Figure-7 shows the graph of proposed method on different images with respect to NPCR and PSNR respectively.

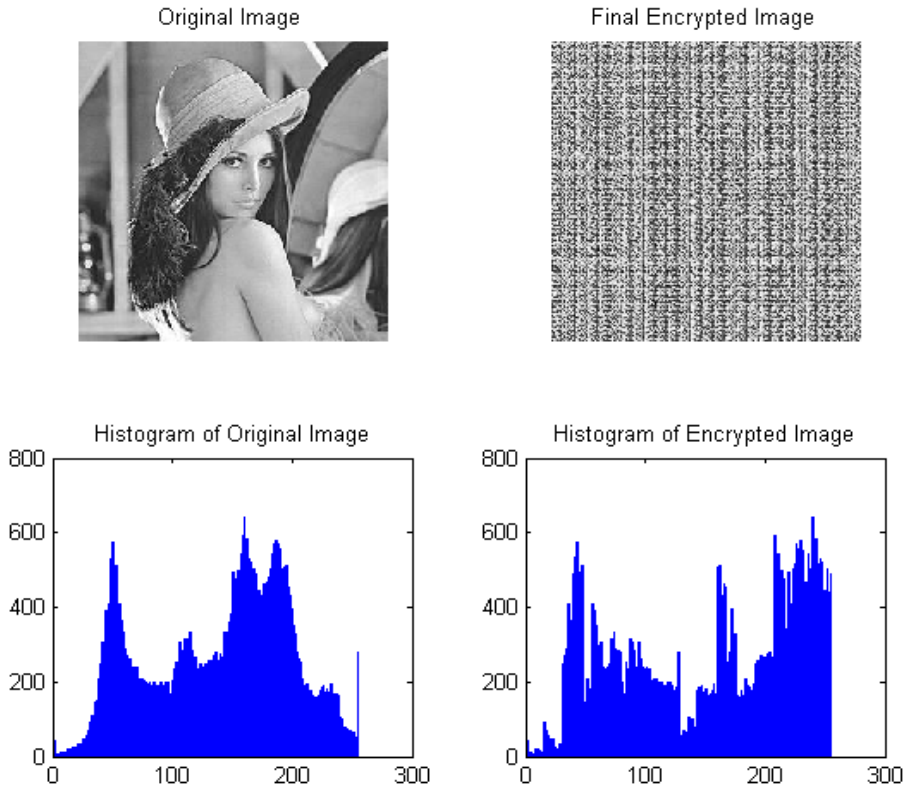


Figure-4. Image encryption method (a) Original image and its histogram. (b) Encrypted image and its histogram; n = 2, k = 8, and p = 0.

©2006-2017 Asian Research Publishing Network (ARPN). All rights reserved.

Table-1. Result of quality parameters on different images.

Image name	PSNR	NPCR	UACI	CC
Lena	17.2270	99.6124	18.1912	3.0601e-005
Baboon	18.5895	99.6567	19.2850	3.0526e-005
Papper	18.1491	99.5407	17.6853	3.0408e-005
Airplane	23.7892	99.5941	7.9112	3.0733e-005
Butterfly	19.5353	99.6353	16.8299	3.0304e-005
Cat	17.3752	99.5789	16.5421	3.1046e-005

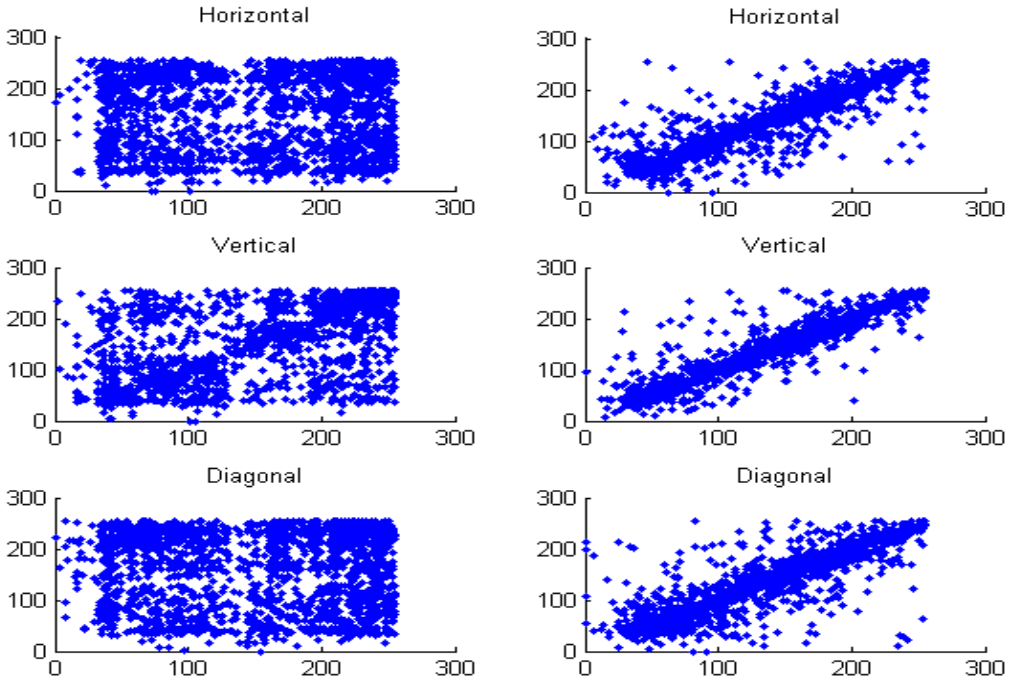


Figure-5. Correlation of adjacent pixels at different directions before and after image encryption.

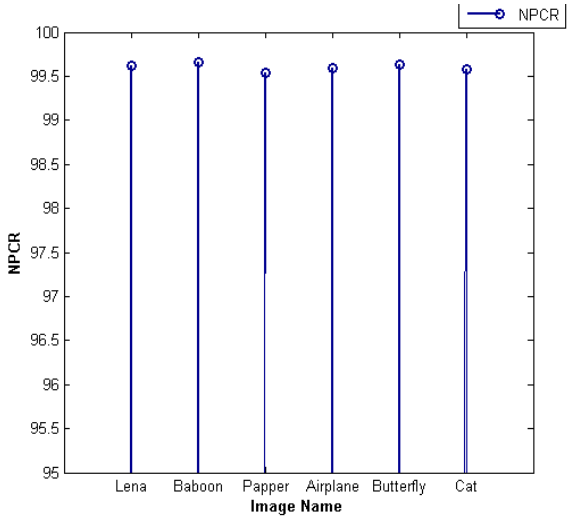


Figure-6. NPCR comparison on different images by proposed Encryption Method.

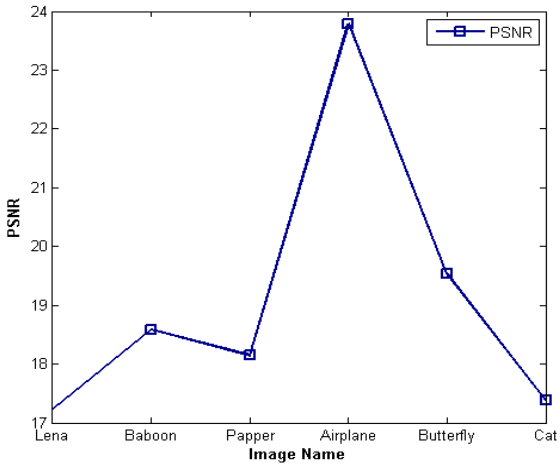


Figure-7. Average PSNR comparison on different image.

©2006-2017 Asian Research Publishing Network (ARPN). All rights reserved.

CONCLUSION

To demonstrate the applicability of the (n, k, p) Gray code in image encryption, we have introduced a hybrid image encryption algorithm to improve the security level of existing bit-plane decomposition and Affine Transform based encryption methods. The new algorithm offers the users flexibility to select any method for bit-plane shuffling and pixel scrambling.

The experimental results and comparison have shown that the presented new encryption algorithm shows excellent performance in image encryption. It could be used for protecting privacy in biometrics, medical imaging systems, and video surveillance systems. Our future research will further improve and analyse the performance of the (n, k, p)-Gray code in image encryption.

REFERENCES

[1] Öztürk and I. Sogukpınar. 2004. Analysis and comparison of image encryption algorithms, Transactions on Engineering, Computing and Technology. 3: 1305-5313.

[2] Aloha Sinha, Kehar Singh, A technique for image encryption using digital signature, Optics Communications. 2 I 8 (2203): 229-234.

[3] V. Potdar and E. Chang, 6 - 9 July, 2004. Disguising text cryptography using image cryptography, International Network Conference in Plymouth, UK.

[4] X. Li, J. Knipe, and H. Cheng. 1997. Image Compression and Encryption Using Tree Structures, Pattern Recognition Letters. 18(8): 2439 2451.

[5] G. Zhang and Q. Liu. 2011. A novel image encryption method based on total shuffling scheme, Opt. Commun. 284: 2775-2780.

[6] Y. Zhang, J. Xia, P. Cai and B. Chen. 2012. Plaintext related two-level secret key image encryption scheme. TELKOMNIKA. 10: 1254-1262.

[7] X. Wang and G. He. 2011. Cryptanalysis on a novel image encryption method based on total shuffling scheme. Opt. Commun. 284: 5804-5807.

[8] Z. Eslami, and A. Bakhshandeh. 2013. An improvement over an image encryption method based on total shuffling, Opt. Commun. 286: 51-55.

[9] Yicong Zhou, Karen Panetta, SosAgaian, C. L. Philip Chen. 2013. (n, k, p) Gray Code for Image Systems", IEEE Transactions on Cybernetics. 43(2): 515-529.

[10] D.-J. Guan. 1998. Generalized Gray code with applications. Proc. Nat. Sci. Counc. ROC (A). 22(6): 841-848.

[11] K. J. Sankar, V. M. Pandharipande and P. S. Moharir. 2004. Generalized Gray codes. In: Proc. Int. ISPACS. pp. 654-659.

[12] G. Ben-Artzi, H. Hel-Or and Y. Hel-Or. 2007. The Gray-code filter kernels. IEEE Trans. Pattern Anal. Mach. Intell. 29(3): 382-393.

[13] H.-W. Tseng and C.-C. Chang. 2007. Anti-pseudo-gray coding for VQ encoded images over noisy channels. IEEE Commun. Lett. 11(5): 443-445.

[14] W.-S. Chen, K.-H. Chih, S.-W. Shih and C.-M. Hsieh. 2005. Personal identification technique based on human IRIS recognition with wavelet transform, in Proc. IEEE ICASSP. 2: 949-952.

[15] W. Ding, W. Yan and D. Qi. 2001. Digital image scrambling, Progr. Nat. Sci. 11(6): 454-460.

[16] I. Nasir,W. Ying, and J. Jianmin. 2007. A new robust watermarking scheme for color image in spatial domain, In: Proc. 3rd Int. IEEE Conf. SITIS. pp. 942-947.

[17] S. Erturk. 2003. Locally refined Gray-coded bit-plane matching for block motion estimation, In: Proc. 3rd ISPA. 1: 128-133.

[18] S.-J. Ko, S.-H. Lee, S.-W. Jeon and E.-S. Kang. 1999. Fast digital image stabilizer based on Gray-coded bit-plane matching, IEEE Trans. Consum. Electron. 45(3): 598-603.

[19] Jawad Ahmad and Fawad Ahmed, Efficiency Analysis and Security Evaluation of Image Encryption Schemes International Journal of Video & Image Processing and Network Security IJVIPNS-IJENS. 2(04).

[20] Yue Wu, Joseph P. Noonan, and SosAgaian. 2011. 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.

[21] G. Chen, Y. Mao, and C. K. Chui. 2004. A symmetric image encryption scheme based on 3D chaotic cat maps, Chaos Solitons Fractals. 21(3): 749-761.

©2006-2017 Asian Research Publishing Network (ARPN). All rights reserved.

[22] N. K. Pareek, V. Patidar and K. K. Sud. 2006. Image encryption using chaotic logistic map, Image Vis. Comput. 24(9): 926-934.