IJCSE International Journal of Computer Sciences and Engineering Open Access
Research Paper Vol.-6, Issue-7, July 2018 E-ISSN: 2347-2693

An Efficient Image Encryption Technique using Discretized Baker Map in Shearlet Domain

[1]Tarlok Singh, [2]Pammy Manchanda

Department of Mathematics, Guru Nanak Dev University,Amritsar, India

Available online at: www.ijcseonline.org

Accepted: 17/Jul/2018, Published: 31/Jul/2018

***Abstract*:** An image encryption plays a significant role in various multimedia applications. An efficient image encryption technique using Discretized Baker Map and Shearlet transform is proposed. Initially, shearlet transform is used to convert an input image into sub-bands. Thereafter, Discretized Baker Map is utilized to design pseudo-random key that encrypts the coefficients of sub-bands. In the end, inverse of Shearlet transform is used to evaluate the ciphered image. Extensive analysis show that the proposed technique outperforms existing techniques in terms of entropy, correlation analysis, and differential analysis.

***Keywords*:** Image Encryption, Discretized Baker Map, Shearlet Transform, Security

I. INTRODUCTION

Nowadays multimedia applications such as images, audio and video are transmitted through the internet. Images need big storage space and it is hard to transfer when the images are big and also confidential images have to be transferred in a secured manner. The information about patients in the hospitals should be kept secret. The medical images have to be transferred in a secured manner. From this point, the need of image cryptography begins. Image encryption is the representation of an image in a cipher format. Color image encryption technique using differential evolution in non-subsampled Contourlet transform domain was proposed by Kaur and Kumar (2018a). Kaur and Kumar (2018b) used an efficient image compression method based on improved Lorenz chaotic system. Wang et. al. (2018) used compressive sensing and detour cylindrical diffraction for image encryption. The common issue in image encryption is to secure the amount of data required to represent an image. Fu et. al. (2018) and Gao et. al.(2018) have shown that image encryption consists of three steps. They are Sub-band decomposition, Permutation and Diffusion.Under the Sub-band decomposition, the appropriate transform is applied to the input image to obtain the coefficients. Encryption is used to permute the values of the image pixel. Thereafter, the combination process is applied to obtain the secret key. Data encryption is mainly used to make the text, image, audio and video to an unreadable or invisible content. Choosing of key size plays an important role in encryption. The larger the size of the key space more will be the security. Image encryption techniques based on chaotic map by Liu et. al.(2018), RT enhanced chaotic tent map by Zhu and Sun (2018), rectangular transform enhanced chaotic tent maps by Wu et. al. (2017), Joseph traversing and mixed chaotic map by Wang et. al. (2018), DNA encoding by Sun et. al. (2018), chaos mixing by Abanda and Tiedeu (2016) have been proposed.

Robust encryption of quantum medical images have been proposed by El-Latif et. al. (2018).

Image encryption works for all format of multimedia content. Especially medical images and video compression/encryption are in demand because image and video data are large in size. For digital image encryption there are two levels of security encryption available, that is low and high level. In low level security encryption, the encrypted image has degraded visual quality compared to the original image, but the recovered image is still visible and understandable. Liu et. al. (2018)shows that in high-level security, the content is completely scrambled and the image is not visible. Zhang et. al. (2017) gives that the basic idea of image encryption is to decompose and compress/encrypt the image level by level. For decomposition many multiscale transforms like Wavelet transform, Bandelet transform, Contourlet transform and Curvelet Transform are used to obtain the coefficients. Wavelet transform offers simultaneous localization in time and frequency domain and it is able to separate the fine details of an image. Wavelets are computationally very fast. Bao et. al. (2017) introduces sharing matrix and proposed lossless secret image sharing for image encryption. Li et. al. (2017) proved that Wavelet based Medical image encryption performs well and it produces good quantitative performance values. Kong et. al. (2018) proved that Bandelet transform has the ability to take the

merit of the geometrical regularity of the structure of an image and is appropriate for the analysis of edges and textures of the images. Bandelet transform is also used to preserve the edges of the synthetic aperture radar images. In Liu
et. al. (2017), Contourlet transform provides geometrically driven representation. Curvelet transform is used for spatial localization and orientation sensitivity. Also, it has the advantage of approximating edge discontinuity. The study of existing encryption techniques reveals that designing an efficient image encryption technique is still an open area of research. Majority of existing techniques suffer from at least one of the following issues:
(i) Existing images encryption techniques Huang and Yang (2017) and Zhang et. al. (2018) demand certain attributes to encrypt or decrypt given set of images. Generally, these values are assigned manually without considering the input images. In Wang et. al (2017), poor assignment of attributes leads to inadequate encryption and decryption results. Hou et. al. (2017) improved image encryption
by assigning these attributes adaptively according to input image that may improve the performance of encryption techniques further.
(ii). Spatial domain-based image encryption techniques suffer from poor speed and easily crackable. However, the transform domain-based encryption techniques used in Xie et. al. (2016) are based upon certain constraints. Thus, it is required to utilize a transform domain which is less constrained than that of existing domains defined in Murugan and Gounder (2016). This enables us to design encryption technique with better frequency selectivity thereby achieving better sub-band decomposition for encryption process.
(iii). Existing chaos maps have the small range of bifurcation parameters. Thus, not so effective against several attacks. The overall goal of this chapter is to design an efficient image encryption technique, which can encrypt and decrypt the images with good speed, quality, and robustness against various security attacks. In this chapter, we propose a Discrete Shearlet Transform based image encryption technique. It is much less constrained than that of standard Contourlet Transforms. It enables us to design encryption technique with better frequency selectivity thereby achieving better sub-band decomposition for the encryption process. The Chaotic Baker Map is used to generate a pseudo-random key which encrypts the coefficients of Discrete Shearlet Transform. The Chaotic Baker Map has the ability to prevent many existing
cryptography attacks and cryptanalysis approaches.
The structure of this chapter as follows: Section 2 explains mathematical preliminaries. The proposed method is introduced in Section 3. Section 4 provides the required experimental setup to run the proposed method successfully. The last Section contains the conclusion of this chapter.

II. PROPOSED TECHNIQUE

In this section, chaotic baker map, Discrete shearlet transform and proposed technique are explained.

A. Chaotic Baker Map

The Baker map is a 2- D chaotic map, which transfers each element in a square matrix into a new position in the matrix. Its operation is cut in half, and the two haves are stacked on one another. The Baker map, *B*, can be described with the following formulas Elshamy et. al. (2013):

$$B(x, y) = (2x, y/2) \quad \text{when} \quad 0 \le x < 1/2, \tag{1}$$

$$B(x, y) = (2x-1, y/2+1/2) \quad \text{when} \quad 1/2 \le x \le 1 \tag{2}$$

Indeed, this simple case of dividing the square into two rectangles of the same size is not used in randomization. There are two versions of the chaotic Baker map, in which a transfer operator U, called the secret key, is used for the division of the Baker map. The secret key is a vector, which has k elements, such that the square matrix is divided into k vertical rectangles.

i. Generalized Baker map

The map can be generalized as follows Kawaguchi (1999)
An $N \times N$ square matrix is divided into k vertical rectangles of height N and width ni such that $1 + n2 + \cdots . nk = N$.

1- These vertical rectangles should be stretched horizontally.
2- Rectangles are stacked to have the left one at the bottom and the right one at the top.

ii. Discretized Baker map

This map transfers an element in a square matrix to another position in the matrix in a bijective manner. The discretized Baker map will be denoted as $B(n1, n2, \ldots\ldots, nk)$, where the sequence of k integers, $n1, n2, \ldots\ldots, nk$, is chosen such that each integer ni divides N, and $N_i = n_1 + \ldots.. + n_i$. The element at the indices (r, s), with $N_i \le r < N_i + n_i$ and $0 \le s \le N$ is mapped to the position :

$$B_{(n_1,\ldots..n_k)}(r,s) = \left[\frac{N}{n_i}(r - N_i) + s \bmod\left(\frac{N}{n_i}\right), \frac{n_i}{N}\left(s - s \bmod\left(\frac{N}{n_i}\right)\right) + N_i \right] \tag{3}$$

This formula is based on the following:

1. An $N \times N$ square matrix is divided into k vertical rectangles of height N and width ni.
2. Each vertical rectangle $N \times ni$ is divided into ni boxes, and every box contains N points.

3. Each of these boxes is mapped to a row of elements by mapping column by column (the left one at the bottom and the right one at the top).

An example of the permutation of an 8 × 8 matrices is shown in Fig. 1. The secret key is chosen to be (2,4,2), hence $N = 8, n1 = 2, n2 = 4,$ and $n3 = 2$. Fig. 1.(a) shows the generalized Baker map and Fig. 1.(b) shows the discretized Baker map. In this paper, the discretized Baker map is used to randomize both the in-phase and in-quadrature components of the output of the IFFT stage after transferring them to a 2-D format.

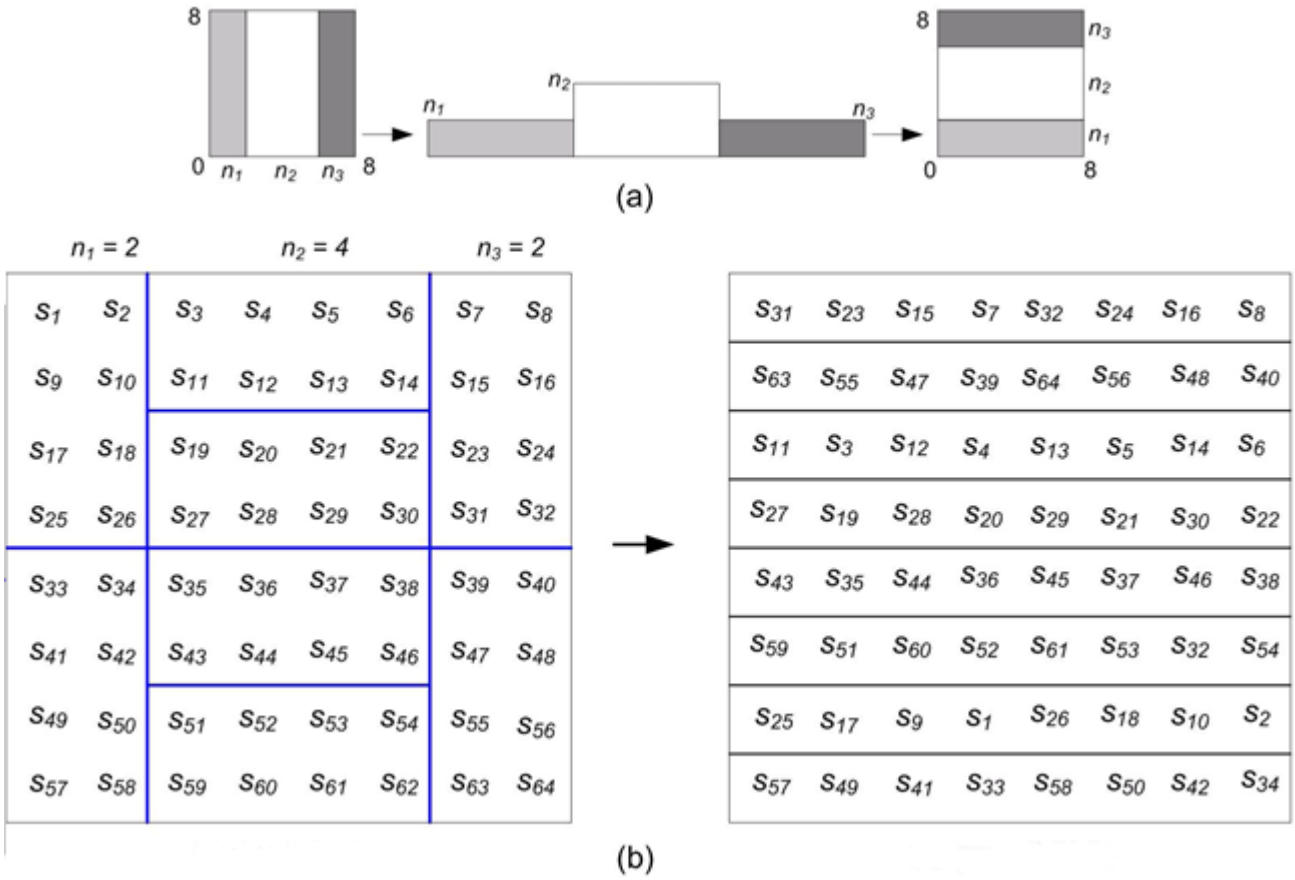

Fig. 1. (a) Generalized Baker map. (b) Discretized Baker map for N = 8.

B. Discrete Shearlet Transform

In the last decade, a new generation of multi-scale transforms emerged which combines classical multi-resolution analysis power with the high performance directional information processing ability. Shearlet, Curvelet, and Contourlet are examples of such transforms. Unlike classic Wavelets the elements of these transforms create a pyramid of well-localized waveforms such that contains different orientations with high anisotropic shapes in addition to various scales and locations. According to their rich structure they can overcome to the poor directional of the multi-scale systems and can be used in the latest algorithms of the signal and image processing. Shearlet presents unique combination of significant features: having understandable and simple mathematical structure which is taken from the affine systems theory. It provides optimally sparse representation; also, its directionality is controlled by shear matrices instead of rotations. Shearlet transform is employed in many problems such as applied mathematics, signal processing such as operator decomposition, inverse problems, edge detection, and image restoration. Shearlet is a framework of the affine system which extracts geometrical features of multi-dimensional signals. This transform is an affine system and includes a shearlet function which is parametrized with scaling, shear and translation such that shear parameter captures direction of the singularities.

For image I, Shearlet transform is a mapping in the form of relation (4):

$$I \rightarrow SH_{\psi} I(a, s, x) \qquad (4)$$

Which depends to scale $a > 0$, direction s and location x. Shearlet transform is expressed as:

$$SH_{\psi} I(a, s, x) = \int I(y) \Psi_{\text{as}}(x - y) dy = I \times \Psi_{\text{as}}(\text{x}) \qquad (5)$$

Shearlets are constructed by dilating, shearing and translation which each mother function $\psi \epsilon L_2(R^2)$ is obtained by:

$$\Psi_{j,k,m}(x) = |\det\ A|^{\frac{j}{2}} \Psi(S^k A^j x - 1) \quad (6)$$

A and S are 2×2 invertible matrices that represent geometrical transformations and dilation as:

$$A = \begin{pmatrix} a & 0 \\ 0 & \sqrt{a} \end{pmatrix}, S = \begin{pmatrix} 1 & s \\ 0 & \sqrt{1} \end{pmatrix} \quad (7)$$

So that, for each mother function we have DST as:

$$SH\left\{\Psi_{j,k,m} = 2^{\frac{3}{4}j} \Psi(s_k A_2 j - m) : j, k \epsilon \mathbb{Z}^2\right\} \quad (8)$$

According to the good capability of DST for capturing directional characteristics and good localization, DST is a suitable choice for watermarking. In Fig. 2, tiling of the frequency plane for DST is illustrated.

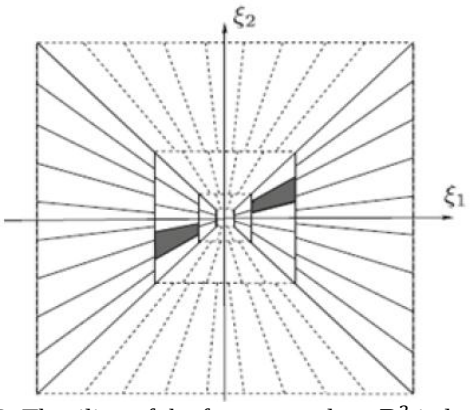

Fig. 2. The tiling of the frequency plane $\mathbb{R}^2$ induced by the Shearlets.

Fig. 3, shows the filter bank decomposition for Shearlet transform. According to that, first the image is decomposed to a low-pass sub-band and a band-pass sub-band by Laplacian Pyramid (LP). Then, band-pass sub-band which demonstrates the difference between the original image and the sub-band low-pass filters is delivered to an appropriate shearing filter to complete multi-directional decomposition. This process is performed continuously on the low-pass sub-bands to obtain a multi-scale decomposition.

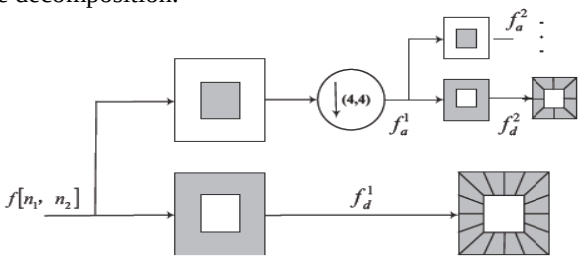

Fig. 3. The filter bank decomposition of Shearlet transform**.**

DST decomposes an image into $2 \times 2^{nj} + 1$directional sub-bands in horizontal cone and vertical cone in each scale respectively which j is decomposition level and nj is direction parameter$(ndir)$. For example, when $ndir = [2\ 1\ 0]$, total number of directions in both directions, horizontal cone and vertical cone, is $2 \times (9 + 5 + 3) = 34$.

C. Proposed image encryption technique

This section provides various steps to encrypt an input image using the proposed technique.

Begin (Image as I and Encryption factor (∂))

Step i. First of all, read I and load its quantized values.

Step ii. Now generate secret key by implementing the Discretized Baker map as k using Eq. (3).

Step iii. Apply discrete shearlet transform using Eq. (4) to Eq. (8) to decompose the input I into sub bands as (S_b).

Step iv. Now utilize k to permute and diffuse the S_b as follows:

$$E_b = k \times S_b + (1 - \partial) \times S_b \quad (9)$$

Here, E_b shows the encrypted sub band.

Thereafter, obtain the permuted and diffused sub band as follows:

$$E_b = E_b \% p_k \quad (10)$$

Here, p_k represents the peak image value. For an 8-bit image it is 255. Also, % represents the modulo operation.

Step v. Now apply the inverse of the discrete shearlet transform on the E_b to obtain the final encrypted image as E.

Return encrypted image (E)

III. PERFORMANCE ANALYSIS

The experimental environment is designed using MATLAB 2017a on Intel (R) core-5 @ 2.40 GHz with 16 GB RAM. The proposed technique is tested on five well-known benchmark color images and compared with 4 competitive image encryption techniques designed by Guodong and Huang (2018), Lin et. al. (2018), Ghebleh et. al. (2018), and Ran et. al. (2018).

Fig. 3 shows the visual analysis of the proposed technique. Fig. 3 (a) and (b) demonstrate the input images and their respective histograms, respectively. The encrypted images and their respective histograms are represented in Fig. 3 (c) and (d). Figure 3 (e) shows the decrypted images. Fig. 3 indicates that the input and decrypted images are identical to each other. From the histograms of encrypted images, it is observed that the proposed technique uniformly distributes the pixels.

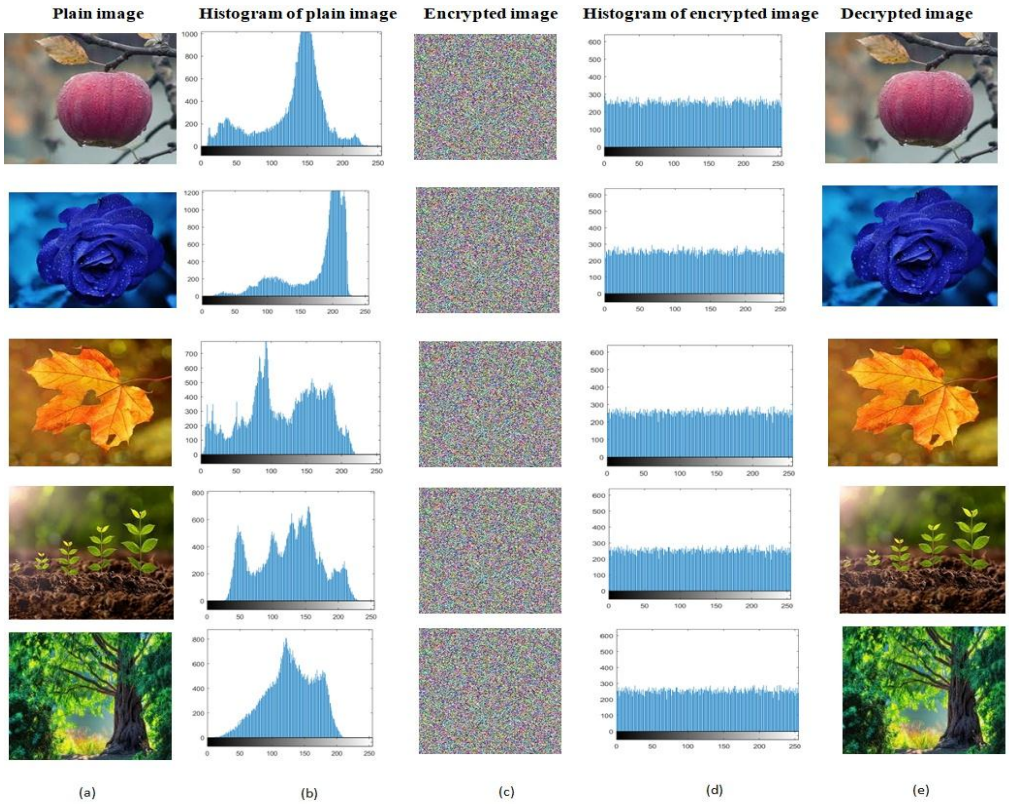

Fig. 3: Performance analysis: (a) plain image, (b) histogram of plain image, (c) encrypted image, (d) histogram of encrypted image, and (e) decrypted image

A. Histogram analysis

Histograms show the intensity distribution of an image. The histograms of encrypted images should be uniformly distributed so that any kind of statistical information cannot be gained by attacker. Fig. 3 (b) and 3 (d) show the histograms of plain and encrypted images, respectively. From Fig. 3 (d), it can be observed that the histogram of encrypted images are uniformly distributed. Thus, it is secure against any kind of statistical attack.

B. Correlation coefficient

It tells the relationship among the adjacent pixels of an encrypted image. This relationship should be minimized so that attacker cannot find any kind of information about pixels. It is computed as

$$r = \frac{N\sum yz - (\sum y)(\sum z)}{\sqrt{[N\sum y^2 - (\sum y)^2][N\sum y^2 - (\sum y)^2]}}$$

where N represents the total number of pixel pairs i.e. (y, z). Tables 1, 2, and 3 show Horizontal correlation (HC), Vertical correlation (VC), and Diagonal correlation (DC) of proposed technique and other existing techniques. From the tables, it can be observed that the proposed technique has minimum correlation as compared to other techniques.

Table 1 Horizontal correlation analysis

Methods	Apple	Flower	Leaf	Plant	Tree
Ye and Huang (2018)	0.254	0.277	0.247	0.235	0.288
Teng et al.(2018)	0.233	0.215	0.281	0.221	0.280
Ghebleh et al. (2018)	0.158	0.147	0.169	0.155	0.200
Ran et al. (2018)	0.112	0.128	0.121	0.110	0.105
Proposed method	**0.052**	**0.047**	**0.033**	**0.025**	**0.013**

Table 2 Vertical correlation analysis

Methods	Apple	Flower	Leaf	Plant	Tree
Ye and Huang (2018)	0.298	0.254	0.247	0.300	0.241
Teng et al. (2018)	0.149	0.152	0.140	0.266	0.195
Ghebleh et al. (2018)	0.136	0.109	0.111	0.210	0.166
Ran et al. (2018)	0.098	0.077	0.080	0.170	0.129
Proposed method	**0.030**	**0.021**	**0.011**	**0.076**	**0.054**

Table 3 Diagonal correlation analysis

Methods	Apple	Flower	Leaf	Plant	Tree
Ye and Huang (2018)	0.175	0.150	0.200	0.199	0.110
Teng et al. (2018)	0.165	0.148	0.182	0.187	0.109
Ghebleh et al. (2018)	0.154	0.139	0.176	0.143	0.094
Ran et al. (2018)	0.168	0.122	0.151	0.097	0.086
Proposed method	**0.099**	**0.043**	**0.078**	**0.021**	**0.008**

C. Differential analysis

To check the proposed technique against differential attacks, Number of pixel change rate (NPCR) and Unified average change intensity (UACI) parameters are used. Differential analysis checks the sensitivity of proposed technique towards plain image. In this, two encrypted images are considered $C_1(i,j)$ and $C_2(i,j)$ having difference of one pixel. NPCR and UACI are computed as follows:

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

$$UACI = \frac{1}{W \times H}\left[\sum_{i,j} \frac{|C_1(i,j) - C_2(i,j)|}{255}\right] \times 100\% \qquad (14)$$

where W and H are width and height of encrypted images. If $C_1(i,j) = 2(i,j)$, then the $D(i,j) = 1$, otherwise $D(i,j) = 0$. Tables 4 and 5 show the NPCR and UACI analyses of proposed techniques and existing image encryption techniques. From tables, it can be observed that proposed technique provides better NPCR and UACI as compared to other techniques.

Table 4 NPCR analysis

Methods	Apple	Flower	Leaf	Plant	Tree
Ye and Huang (2018)	99.52	99.46	99.48	99.50	99.54

Teng et al. (2018)	99.48	99.46	99.40	99.38	99.39
Ghebleh et al. (2018)	99.37	99.35	99.29	99.15	99.30
Ran et al. (2018)	99.59	99.52	99.57	99.60	99.62
Proposed method	**99.78**	**99.69**	**99.65**	**99.70**	**99.71**

Table 5 UACI analysis

Methods	**Apple**	**Flower**	**Leaf**	**Plant**	**Tree**
Ye and Huang (2018)	33.11	33.15	33.08	33.20	33.25
Teng et al. (2018)	33.24	33.26	33.14	33.19	33.23
Ghebleh et al. (2018)	33.30	33.29	33.23	33.32	33.33
Ran et al. (2018)	33.18	33.34	33.16	33.35	33.37
Proposed method	**33.45**	**33.48**	**33.50**	**33.51**	**33.42**

IV. CONCLUSION

In this paper, a novel image encryption technique using discretized baker map in shearlet domain is proposed. First of all, an input image is decomposed into sub bands using shearlet transform. Afterwards, discretized baker map is implemented for generating the secret key for encryption process. Then, obtained secret key is used to permute and diffuse the evaluated sub bands from shearlet transform. In the end, inverse shearlet transform is applied on the permuted and diffused sub bands to obtain final encrypted image. The performance of the proposed technique is tested on five benchmark images. Extensive analysis shows that the proposed technique provides more robustness against differential analysis.

REFERENCES

[1] M. Kaur and V. Kumar, "Colour image encryption technique using differential evolution in non-subsampled contourlet transform domain," in IET Image Processing, vol. 12, no. 7, pp. 1273-1283, 7 2018a.

[2] M. Kaur and V. Kumar, "Efficient image encryption method based on improved Lorenz chaotic system," in Electronics Letters, vol. 54, no. 9, pp. 562-564, 5 3 2018b.

[3] J. Wang, Q. H. Wang and Y. Hu, "Image Encryption Using Compressive Sensing and Detour Cylindrical Diffraction," in IEEE Photonics Journal, vol. 10, no. 3, pp. 1-14, June 2018.

[4] X. Q. Fu, B. C. Liu, Y. Y. Xie, W. Li and Y. Liu, "Image Encryption-Then-Transmission Using DNA Encryption Algorithm and The Double Chaos," in IEEE Photonics Journal, vol. 10, no. 3, pp. 1-15, June 2018.

[5] Z. Gao, D. Chen, W. Zhang and S. Cai, "Colour image encryption algorithm using one-time key and FrFT," in IET Image Processing, vol. 12, no. 4, pp. 472-478, 4 2018.

[6] C. Zhu and K. Sun, "Cryptanalyzing and Improving a Novel Color Image Encryption Algorithm Using RT-Enhanced Chaotic Tent Maps," in IEEE Access, vol. 6, pp. 18759-18770, 2018.

[7] S. Sun, "A Novel Hyperchaotic Image Encryption Scheme Based on DNA Encoding, Pixel-Level Scrambling and Bit-Level Scrambling," in IEEE Photonics Journal, vol. 10, no. 2, pp. 1-14, April 2018.

[8] M. Preishuber, T. Hütter, S. Katzenbeisser and A. Uhl, "Depreciating Motivation and Empirical Security Analysis of Chaos-Based Image and Video Encryption," in IEEE Transactions on Information Forensics and Security, vol. 13, no. 9, pp. 2137-2150, Sept. 2018.

[9] X. Wang, X. Zhu and Y. Zhang, "An Image Encryption Algorithm Based on Josephus Traversing and Mixed Chaotic Map," in IEEE Access, vol. 6, pp. 23733-23746, 2018.

[10] L. Liu, S. Hao, J. Lin, Z. Wang, X. Hu and S. Miao, "Image block encryption algorithm based on chaotic maps," in IET Signal Processing, vol. 12, no. 1, pp. 22-30, 2 2018.

[11] Y. Zhang, "A Chaotic System Based Image Encryption Scheme with Identical Encryption and Decryption Algorithm," in Chinese Journal of Electronics, vol. 26, no. 5, pp. 1022-1031, 9 2017.

[12] A. Abd El-Latif, B. Abd-El-Atty and M. Talha, "Robust Encryption of Quantum Medical Images," in IEEE Access, vol. 6, pp. 1073-1081, 2018.

[13] L. Bao, S. Yi and Y. Zhou, "Combination of Sharing Matrix and Image Encryption for Lossless (k,n) -Secret Image Sharing," in IEEE Transactions on Image Processing, vol. 26, no. 12, pp. 5618-5631, Dec. 2017.

[14] C. Li, D. Lin and J. Lü, "Cryptanalyzing an Image-Scrambling Encryption Algorithm of Pixel Bits," in IEEE MultiMedia, vol. 24, no. 3, pp. 64-71, 2017.

[15] D. Kong, L. Cao, X. Shen, H. Zhang and G. Jin, "Image Encryption Based on Interleaved Computer-Generated Holograms," in IEEE Transactions on Industrial Informatics, vol. 14, no. 2, pp. 673-678, Feb. 2018.

[16] H. Liu, A. Kadir and X. Sun, "Chaos-based fast colour image encryption scheme with true random number keys from environmental noise," in IET Image Processing, vol. 11, no. 5, pp. 324-332, 4 2017.

[17] L. Liu, S. Miao, H. Hu and M. Cheng, "N-phase logistic chaotic sequence and its application for image encryption," in IET Signal Processing, vol. 10, no. 9, pp. 1096-1104, 12 2016.

[18] X. Wu, B. Zhu, Y. Hu and Y. Ran, "A Novel Color Image Encryption Scheme Using Rectangular Transform-Enhanced Chaotic Tent Maps," in IEEE Access, vol. 5, pp. 6429-6436, 2017.

[19] H. Huang and S. Yang, "Colour image encryption based on logistic mapping and double random-phase encoding," in IET Image Processing, vol. 11, no. 4, pp. 211-216, 4 2017.

[20] L. Y. Zhang et al., "On the Security of a Class of Diffusion Mechanisms for Image Encryption," in IEEE Transactions on Cybernetics, vol. 48, no. 4, pp. 1163-1175, April 2018.
[21] X. Wang, G. Zhou, C. Dai and J. Chen, "Optical Image Encryption With Divergent Illumination and Asymmetric Keys," in IEEE Photonics Journal, vol. 9, no. 2, pp. 1-8, April 2017.
[22] J. Hou, R. Xi, P. Liu and T. Liu, "The switching fractional order chaotic system and its application to image encryption," in IEEE/CAA Journal of Automatica Sinica, vol. 4, no. 2, pp. 381-388, April 2017.
[23] Y. Abanda and A. Tiedeu, "Image encryption by chaos mixing," in IET Image Processing, vol. 10, no. 10, pp. 742-750, 10 2016.
[24] Y. Xie, J. Li, Z. Kong, Y. Zhang, X. Liao and Y. Liu, "Exploiting Optics Chaos for Image Encryption-Then-Transmission," in Journal of Lightwave Technology, vol. 34, no. 22, pp. 5101-5109, Nov.15, 15 2016.
[25] B. Murugan and A. G. Nanjappa Gounder, "Image encryption scheme based on block-based confusion and multiple levels of diffusion," in IET Computer Vision, vol. 10, no. 6, pp. 593-602, 9 2016.
[26] A. M. Elshamy et al., "Optical Image Encryption Based on Chaotic Baker Map and Double Random Phase Encoding," in Journal of Lightwave Technology, vol. 31, no. 15, pp. 2533-2539, Aug.1, 2013.
[27] H. Kawaguchi, "Evaluation of the Lorentz group Lie algebra map using the Baker-Cambell-Hausdorff formula," in IEEE Transactions on Magnetics, vol. 35, no. 3, pp. 1490-1493, May 1999.
[28] J. F. van Diejen, "The dynamics of zeros of the solitonic Baker-Akhiezer function for the Toda chain," in International Mathematics Research Notices, vol. 2000, no. 5, pp. 253-270, 2000.
[29] Ye, Guodong, and Xiaoling Huang. "Spatial image encryption algorithm based on chaotic map and pixel frequency." Science China Information Sciences 61, no. 5 (2018): 058104.
[30] Teng, Lin, Xingyuan Wang, and Juan Meng. "A chaotic color image encryption using integrated bit-level permutation." Multimedia Tools and Applications 77, no. 6 (2018): 6883-6896.
[31] Ghebleh, M., A. Kanso, and D. Stevanović. "A novel image encryption algorithm based on piecewise linear chaotic maps and least squares approximation." Multimedia Tools and Applications 77, no. 6 (2018): 7305-7326.
[32] Ran, Qiwen, Ling Wang, Jing Ma, Liying Tan, and Siyuan Yu. "A quantum color image encryption scheme based on coupled hyper-chaotic Lorenz system with three impulse injections." Quantum Information Processing 17, no. 8 (2018): 188.

