Colour Image Encryption using Expand-Shrink Operation in Chaos Encryption Algorithm

Rashmi P\textsuperscript{1,2}, Supriya M C\textsuperscript{3} and Kiran\textsuperscript{4}

\textsuperscript{1}Sri Siddhartha Academy of Higher Education, Tumakuru, India,  
\textsuperscript{2}Department of BCA, VVFGC, Mysuru, India.  
\textsuperscript{3} Department of MCA, SSIT, Tumakuru, Sri Siddhartha Academy of Higher Education, Tumakuru, India.  
\textsuperscript{4}Department of ECE, VVCE, Mysuru, India  
\textsuperscript{1}rashmibdp@gmail.com, \textsuperscript{3}supriya.mc9@gmail.com

Abstract. In recent decades, chaos based encryption algorithm is widely used in image encryption. Most of the chaos based encryption algorithm operate at bit level, which is ineffective in high resolution digital images. In this research paper, a new colour image encryption algorithm is proposed by using expand-shrink operation for confusion and diffusion operation in chaos algorithm. The proposed algorithm consists of confusion-diffusion strategy operated at pixel level. Original colour image is expanded based on intrinsic features of bit planes. Expanded image undergo confusion diffusion operation using Hilbert scan method. In addition, for diffusion operation uses circle map that generates random image. In the experimental section, the proposed algorithm achieved better performance in image encryption on various digital images.

Keywords: Confusion, Diffusion, Hilbert scan, Circle map, Expand, Shrink

1. Introduction
With the growth of computer science and innovative technologies, multi-media data (videos, sounds and pictures) are increasing shared in the internet and also stored in hard disk [1]. However, the unauthorized access of private and personal information are becoming a serious concern in digital world. The issues related to security are vital in many multimedia applications [2-3]. Image encryption is an efficient and classical way for solving the above stated issues. The conventional image encryption standards like AES and DES are utilized for text information. The researchers identified that the conventional image encryption standards are ineffective for multi-media information, because of their properties like high correlation among pixels, bulk data, etc. [4-5]. The basic structure of chaos based image encryption is developed by Fridrich in 1998. Based on this structure, 2 unrelated phases are carried out in chaos based image encryption that are named as diffusion and confusion phases [6].

The image pixels are re-located initially that leads to correlation reduction among the adjacent pixels. Whereas, the confusion operation is carried out in a closed manner [7, 24] and the basic components of the images (pixels values or bits) are not influenced by the external information. The 2D sequence determines the permuting unit (bit or pixel) location. Hence, there is no variations in the statistical
information between the confused and the plain images. Self-information is insufficient in the diffusion phase and a few external information need to be introduced. In a few cases, random sequences and one dimensional chaotic sequences are utilized to alter every image pixel values. The bits of pixel values and the basic elements of the images are distributed uniformly. The remaining research draft is organized as: Literature Survey is described in section 2. Related work is discussed in Section 3, and the explanation of the proposed method is illustrated in Section 4. The validation of the proposed method i.e. experimental results is represented in Section 5. Conclusion of the research work is explained in Section 6.

2. Literature survey
In recent decades, secure image transmission gaining more importance, due to the advance of computer vision and multimedia applications. Using chaotic sequence of one dimensional chaotic map, the initial values of the map are predicted easily. Additionally, high dimension chaotic map is undertaken to perform image encryption.

H. Lu, et al, [8] utilized chaotic map that plays a major role to improve Evolutionary Algorithms (EAs) to avoid local optima and speed up the convergence. In addition, dissimilar chaotic maps are utilized in dissimilar phases, where it have dissimilar effects on the EAs. In this paper, authors focused on the concerns in chaotic maps and gave guidance to improve the multi-objective EAs (MOEAs) by implementing several experiments. Additionally, a non-dominated sorting and elitist strategy; NSGA-II algorithm is undertaken to study the effect of chaotic maps. In addition, A. Nair, and K. Kiasaleh, [9] discussed about circle map as an interleaver that creates additional layer of randomness and scrambler effect, and it negates the impact of burst errors due to wireless channel conditions. By effectively using the good correlation and spreading properties of the circle map allows one to achieve this gain. The other critical aspect of the proposed method is the minimization of the size of the side information required for the de-interleaving purposes.

E.S. El-Alfy, and K. Al-Utaibi, [10] developed a new image encryption algorithm on the basis of logistic map for generating 4 chaotic sequences. These sequences are transformed into 4 key streams by utilizing chaotic sequence methodology. The generated key streams are utilized for controlling the multipoint mutation and cross-over operations that results in image diffusion and confusion, correspondingly. K.U. Shahna, and A. Mohamed, [11] implemented a new symmetric cryptography framework for encrypting the images by utilizing Henon map, bit level cyclic shift and Hilbert curve. In this literature study, the image pixel scrambling and key stream generation are carried-out in both bit level and pixel level for ensuring the double scrambling, which is achieved by using cyclic shift and Hilbert curve operations. By using double scrambling methodology, the near pixel correlation values are minimized. Finally, a novel methodology is undertaken for cyclic shift operation. The scrambles image is encrypted utilizing key streams in the diffusion process. Various encryption types discussed using different methods [14-18]. Expand and shrink to enhance the strength of chaos based image encryption technique described in [19]. Performance of the communication for 4x4 indoor MIMO-VLC system are analysed under different noise constraints [21]. Glow-worm Swarm Optimization (GSO) and Support Vector Machine (SVM) is used for decision making process in battery storage to reduce the electricity tariff [22]. In [23] hybrid approach based on chaotic map and henon map presented for encrypting color images.

3. Related work

3.1. Hilbert scan pattern
The Hilbert scan pattern is an effective scan pattern technique in image encryption that scans $2^m \times 2^m$ array points. In this technique, the scan path is constructed from left top, left bottom, right top and right bottom of the square grid [12]. In this technique, Hilbert curve is utilized for shuffling the position of the pixels in the original digital images for obtaining the scrambled image.

In Hilbert scan pattern, the order 0 represents that the Hilbert curve is empty, and the order -1 is attained by using 4 zero ordered curves with 3 straight connector lines. In addition, the higher order curves are also obtained in the similar manner. The Hilbert curve of order 1, 2, 3, and 4 are corresponds to $2 \times 2$, $4 \times 4$, $8 \times 8$, and $16 \times 16$ square grids, which are stated in the figure 1 (a), (b), (c), and (d).
Figure 1. Hilbert curve of order 1, 2, 3, and 4 corresponds to $2 \times 2$, $4 \times 4$, $8 \times 8$, and $16 \times 16$ square grids, respectively.

Figure 2. $8 \times 8$ matrix permutation using Hilbert scan pattern.

3.2. Circle map
Circle map is a dynamical system, which is initially determined by Andrey Kolmogorov. However, the author states that the circle map is a simplified model that is used to driven the mechanical rotors. Especially, a spinning wheel is coupled to spring the motor. Equation (1) denotes the formula to calculate the circle map, where it is a simplified model in electronics [13]. Mathematically, the circle map is represented in equation (1).

$$x_{k+1} = \left\{x_k + b - \left(\frac{a}{2\pi}\right) \sin(2\pi x_k) \right\} \mod 1$$

(1)

With $a = 0.5$ and $b = 0.2$, and it generates the chaotic sequence $(0, 1)$. 
4. Proposed method
Block diagram of the proposed algorithm is shown in figure 3. This block diagram mainly consists of confusion and circle map based diffusion operation. Steps involved in encryption process.

**Step 1:** Consider RGB image of size $N \times N \times 3$.

**Step 2:** Then, the expand operation is performed on RGB image. In the expand operation, the higher two bits of $R, G, and B$ channels of every pixels are extorted for generating a new pixel with six bits. In which the lower two bits are generated from $R$ channel, middle two bits are generated from $G$ channel and the higher two bits are generated from $B$ channel. Then, a new image is achieved using these image pixels, which is determined as $\beta$ channel. Hence, the residual six bits in every pixel of the $R, G, and B$ channels are remains unchanged. The height and width of the original image is represented as $N$, here totally $4N \times N$ image with six bits for every pixels are achieved on the basis of $R, G, B, and \beta$ channels. The obtained 4 images forms permutation expanded matrix that is graphically indicated in figure 2. Further, the channel $\beta$ comprises of around 80% of plain image information.

**Step 3:** Expanded image positions are shuffled randomly by using Hilbert scan pattern as shown in figure 2.

**Step 4:** Based on the secret key, a random vector sequence is generated using circle map, as shown in the equation (1).

- Update the random vector $X$ by multiplying it with 1014.
- Modulo 256 operations is carried out to get updated random numbers in a range of 0 to 255.

$$\alpha = Modulo(X, 256)$$

**Step 5:** Perform Bit XOR operation between confused image and random image $R$.

**Step 6:** Resultant image undergo shrink operation to produce final RGB encrypted image.

![Figure 3. Architecture of proposed colour image encryption](image-url)
5. Experimental Results

In this section, the validation of the proposed algorithm is conducted by encrypted analysis and histogram analysis. In this study, MATLAB 2015a is utilized to implement the proposed algorithm along with the configuration of 4 GB RAM, i5 processor of 3.4 GHz Intel Core with 3570 CPU. The test colour images are selected for validating the proposed encryption algorithm. Figures 5 and 6 indicates the encryption results, and it stated that the various size images are also encrypted by the proposed algorithm. The final result images are meaningless and noise-free images that shows the proposed algorithm encrypt the images in an effective way.

Histogram of an image is a graphical representation of pixels distribution based on the intensity levels. For any plain image, an effective encryption algorithm always generates a cipher image of the uniform histogram. Figures 7 and 8 shows the histograms of the various RGB original image and the corresponding cipher images. It is determined that the histogram of encrypted image is close to the uniform distribution.
Figure 6. Result of proposed method for Parrot input image

Figure 7. Histogram Analysis of proposed method for Lena input image

Figure 8. Histogram Analysis of proposed method for Parrot input image
The pixel correlation is the degree of association of the gray values between pixels. Figures 9 and 10 show the pixel pair distribution of the test images and pixel pair the corresponding cipher images. The formula of correlation coefficient is defined as follows [20]

\[ C_{xy} = \frac{\text{cov}(x, y)}{\sqrt{D(x)D(y)}} \]

6. Conclusion
In this research, a colour image encryption using expand shrink operation for confusion and circle map based diffusion operation is proposed. This algorithm consists of confusion diffusion strategy, which is operated at bit level. Original colour image is expanded based on intrinsic features of bit planes.
Expanded image undergo confusion-diffusion operation. Here for diffusion operation utilizes circle map. This research article concluded that the proposed algorithm is suitable for real time encryption and also it effectively improves the security of the system. While related to existing algorithms, the proposed algorithm delivers an effective performance in image encryption.

Acknowledgement
The work described in this paper is supported by Sri Siddhartha Academy of Higher Education, Tumakuru, India. Authors would like to thank Hon’ble Vice Chancellor Dr. Balakrishna P Shetty and Registrar Dr. M Z Kurian for providing a strong platform for research work.

References
[1] Chen S and Lü J 2002 Parameters identification and synchronization of chaotic systems based upon adaptive control Phys. Lett. 299 353–358
[2] Papadopoulos H E and Wornell G W, 1995 Maximum-likelihood estimation of a class of chaotic signals IEEE Trans. Inform. Theory 41 312–317
[3] Xiaofu W and Songgeng S 1999 A general efficient method for chaotic signal estimation IEEE Trans. Signal Process 47 1424–1428
[4] Arroyo D, Rhouma R, Alvarez G, Li S and Fernandez V 2008 On the security of a new image encryption scheme based on chaotic map lattices, Chaos 18 033112
[5] Hua Z, Zhou Y and Chen C P 2013 A new series-wound framework for generating 1D chaotic maps in: Digital Signal Processing and Signal Processing Education Meeting (DSP/SPE) 118–123
[6] Wu X, Wang D, Kurths J and Kan H 2016 A novel lossless color image encryption scheme using 2D DWT and 6D hyperchaotic system Inform. Sci. 349 137–153
[7] Liu H, Wang X 2011 Color image encryption using spatial bit-level permutation and high-dimension chaotic system Opt. Commun. 284 3895–3903
[8] Hui L, Wang X, Fei Z Qiu M 2014 The Effects of Using Chaotic Map on Improving the Performance of Multiobjective Evolutionary Algorithms Hindawi Publishing Corporation Mathematical Problems in Engineering 1-16
[9] Anish N, Kiasaleh K 2016 Chaotic Circle Map Interleaver for OFDM Int. Conf. on Computing, Networking and Communications (ICNC), Workshop on Computing, Networking and Communications (CNC) 1-6
[10] El-Sayed M E and Al-Utaibi K A 2011 An Encryption Scheme for Color Images Based on Chaotic Maps and Genetic Operators ICNS 2011: The Seventh International Conference on Networking and Services 92-97
[11] Shahn K U and Mohamed A 2016 A novel image encryption scheme using both pixel level and bit level permutation with chaotic map Applied Soft Computing Journal 90 1568-4946
[12] Sivakumar T and Venkatesan R 2014 Image encryption based on pixel shuffling and random key stream Int. J. Comput. Inform. Technol. 3
[13] Zheng W M 1994 Kneading plane of the circle map, Chaos, Solitons and Fractals, 4 1221–1233
[14] Parameshachhari B D, Kiran, Rashmi P and Supriya M C 2019 Controlled Partial Image Encryption Based on LSIC and Chaotic map 4th Int. Conf. on Multimedia and Image Processing (ICMIP 2019), University of Malaya, Kuala Lumpur, Malaysia 19-21
[15] Kiran, Parameshachhari B D and Panduranga H T 20147 Partial Encryption of Medical Images by Dual DNA Addition using DNA Encoding Proc. Int. conf. on Recent Innovations is Signal Processing and Embedded Systems (RISE-2017) 27-29
[16] Parameshachhari B D, Rajashekrappa, Sumithar Devi K A and Sunjiv Soyjaudh K M 2014 Partial Image Encryption Algorithm Using Pixel Position Manipulation Technique 4th Int. Conf. on Artificial Intelligence and applications in Engineering and Technology (ICAIE2014), Kota Kinabalu, 177-181
[17] Parameshachhari B D, Sumithar Devi K A and K M Sunjiv Soyjaudh Partial Image Encryption Approach Using SCAN Mapping and Band Permutation Published at Proceedings of ICSIP 2013, 222–226
[18] Parameshachari B D, Sumithar Devi K A and K M Sunjiv Soyjaudh Secure Partial Image Encryption Scheme Using Scan Based Algorithm, International Journal of advances in Engineering & Technology, 6, 264-273

[19] Naveenkumar S K, Panduranga H T and Kiran 2014 Chaos Based Image Encryption using Expand-Shrink Concept, International Journal of Informatics and Communication Technology (IJ-ICT) 3 103-112

[20] Wonyoung J and Lee S. Y 2020 Partial image encryption using format-preserving encryption in image processing systems for Internet of things environment, International Journal of Distributed Sensor Networks 16 1-17

[21] Subramani P, Rajendran GB, Sengupta J, Pérez de Prado R, Divakarachari PB 2020 A Block Bi-Diagonalization-Based Pre-Coding for Indoor Multiple-Input-Multiple-Output-Visible Light Communication System, Energies, 13 1-16

[22] Parameshachari B D et al. 2019 Demand side management of small scale loads in a smart grid using glow-worm swarm optimization technique Elsevier Microprocessors and Microsystems 71 1-9

[23] Rashmi P, Supriya M C and Kiran 2019 Encryption of Color image to enhance security using Permutation and Diffusion Techniques International Journal of Advanced Science and Technology Scopus Indexed Journal 28 375-384

[24] Narayanan K.L., and Ramesh G.P. 2017 Discrete Wavelet Transform Based Image Compression using Frequency Band Suppression and Throughput Enhancement. International Journal of MC Square Scientific Research, 9 176-182