Implementation of Novel Framework for Image Encryption using Tinkerbell 3D Cat Map

Gourab Biswas[1] **and Chittaranjan Pradhan**[2,*]

[1,2]Kalinga Institute of Industrial Technology, Bhubaneswar, India

Abstract: In the current scenario ensuring data security has become an essential aspect due to the rise in data movement in public networks. The traditional methods of cryptography is now replaced by the quicker and more efficient chaotic maps which are being used in this data security aspect. The Tinkerbell 2D cat map is a common instance among the chaotic maps. In this article a completely new method of Image encryption and decryption employing a three-dimensional variant of the classical Tinkerbell chaotic map is proposed. The third dimension provides a more defined window of perception which is intriguing and secure. The capability of the suggested approach is surveyed thoroughly in terms of both colours and monochromatic images and its performative appraisal has been explored on the basis of several indices such as NPCR, PSNR, UACI etc. It is observed that the proposed 3D extension of Tinkerbell chaotic map has provided superior results than the older versions in terms of the performance-evaluation matrices. The results are similar for MSE, PSNR and NCC measures. Histogram analysis of original image, encrypted image, and decrypted image verify the results and concludes that a 3D chaotic map provides additional security as the images encrypted in the example had very uniform histograms. The applicability of the 3D chaotic map to encrypt and decrypt image is confirmed clearly in this research through various color and grayscale images tested using the proposed map.

Keywords: Chaotic map, Encryption, Image security, Decryption, Tinkerbell 2D cat map, Tinkerbell 3D cat map.

Introduction

As human exponentially depend on data transmission through public channels, such as the Internet, data security is becoming more crucial. In the context of data security, chaotic maps appear to be faster and more trustworthy than the regular forms of cryptography. The Tinkerbell 2D cat map is an repeatedly used choice of a chaotic map. Here a new scheme of an image encryption and decryption is presented by extending the Tinkerbell chaotic map to three dimensions. The additional dimension adds both complexity and security to the scheme. The proposed scheme is effective for encryption of colored and gray-scale images. It shows better performances in miscellaneous performance-evaluation aspects. The evaluations indicate that the 3D Tinkerbell chaotic map exhibits better performance than a 2D chaotic map in encryption evaluation matrices. Along with that the outcomes are similar for the decryption-evaluation schemes. The histogram scanning of the original and the processed images also showcase the encryption works well. As the histogram of the encrypted images are notably homogeneous in the demonstrations. This research demonstrates utility of image processing using 3D chaotic mapping of the image for both gray scale and RGB images using the Tinkerbell map [1].

For the purpose to uplift the reliability level of the encryption operation and ensure the information security of the digital image. This paper puts forward a way to encrypt image and decrypt that based on the 3D Tinkerbell Chaotic Map in Python. The method is to update the original 2D Tinkerbell map into 3D map which can elevate the complexity, improve the performance of the chaotic sequence and ensure the safety of the encrypted data. The third variable is extended based on the existing two dimensional Tinkerbell map to obtain a more chaotic sequence and to optimize the map for better complexity. It is deduced that the chaotic system's three dimensional chaotic trajectory following the Z axis will make the chaotic trajectory more complicated and irregular. It further results in the three dimensional chaotic trajectory in more uneven and unpredictable manner. This is also shown by experimentation that the multimedia data exhibits better nonlinear chaotic characteristics in this case and that the corresponding decryption operation is very secure. In this new 3D Tinkerbell chaotic map approach the existing methods are still being used which have been executed before for encryption and decryption of the information contained in digital images. In the paper, the image data is highly parallel. It is determined that 3D trajectory of the chaotic system is better than the 2D chaotic trajectory and the encryption scheme and algorithm are safer and more dependable. The 3D Tinkerbell chaotic map proposed in this paper has high sensitivity to the initial value and better pseudo randomness. It is indeed an efficient and safe digital image information security encryption method.

Literature Review

P. R. Krishna et. al came up with an idea of encryption algorithm using the Tinkerbell map for ensuring secured remittance of image data [2]. T. A. Dhopavkar et. al introduced a rendition which assembles Tinkerbell and Duffing maps in enhancing security. A Tinkerbell map-based encryption technique was presented by P. R. Krishna et al. to ensure high-security picture data transfer [2]. In a work published, T. A. Dhopavkar et al. combine Duffing maps with Tinkerbell to improve security. Strong security is provided by the encryption technique against data breaches and illegal access [3].

By integrating the Tinkerbell chaotic map into the hybrid encryption model, R. Enayatifar et al. suggested the hybrid model-based chaotic image encryption. Randomness and complexity were pushed for in the encryption process by Tinkerbell's dynamics [4]. Tinkerbell map, an image encryption technique with great efficiency on chaotic dynamics, was proposed by M. Khan et al. Tinkerbell map's chaotic nature contributes to the encryption process's good complexity and unpredictability [5].

With the inspiration of the work of S. Kumar et. al [6], we are motivated to extend a 3D chaotic map to a 4D version for color image encryption. They took the 3D system applied to image scrambling and made it more complex with a 4th dimension in order to enhance color image encryption.

Related Work

2D Tinkerbell Chaotic Map

The Tinkerbell chaotic map is a discrete time system known for its chaotic behavior. Its drastic sensitivity to an initial condition is one of the features that characterize the systems as chaotic. The name "Tinkerbell" finds its origin through the resemblance of its attractor's plot to the capricious and unpredictable flight patterns of Tinkerbell, the fairy from folklore.

The 2D Tinkerbell map is defined by the set of nonlinear recurrence relations updating two variables, x and y. The governing equation of this map is as given below (eq. 1) [7, 8]:

$$\begin{aligned} X_{n+1} &= X_n^2 - Y_n^2 + aX_n + bY_n \\ Y_{n+1} &= 2X_nY_n + cX_n + dY_n \end{aligned} \qquad (1)$$

Where,

X_n and Y_n are the coordinates at the n^{th} iteration.

Usually used values of the parameters are: a=0.9, b=−0.6013, c=2.0, d=0.5. These parameters control the specific behavior of the map.

3D Tinkerbell Chaotic Map

Being a direct extension of the classical 2D Tinkerbell map, the 3D Tinkerbell chaotic map provides an additional dimension, while also making the chaotic system more complex and secure. A chaotic map that has more than two dimensions can be utilized in applications requiring much more complexity and nonpredictability, poly-systems, advanced encryption schemes, and high-dimensional data modeling.

$$\begin{aligned} X_{n+1} &= X_n^2 - Y_n^2 + aX_n + bY_n \\ Y_{n+1} &= 2X_nY_n + cX_n + dY_n \\ Z_{n+1} &= Z_n + d * (X_n - Y_n) \end{aligned} \quad (2)$$

Characteristics of 3D Tinkerbell Map

Enhanced Complexity: With the extension of the third dimension, the chaotic behavior of the TinkerBell map acts with more complexity and complicates the predictions and relinquishs better analysis.

Higher-Dimensional: Due to the additional dimension, the 3D chaotic map generates more dimensions and the complication increases compared to the 2D variants of this system.

High Security: With the Inclusion of an additional dimension to the cryptographic application, the extra dimensional timing and chaotic aspect improves security in the encryption schemes for the following advantages: An unpredictable pattern to transform the genuine image or signal to hide when the extra dimension is included in 2D Tinker Bell maps. The extra time involved to encrypt and decrypt the image, bewildering even the brute force attack.

Proposed Work

The traditional encryption method using 2D Tinkerbell Chaotic maps may no longer provide sufficient security against modern cryptographic challenges, leading to the introduction of the 3D Tinkerbell Cat map. This new method enhances data protection by adding an extra parameter, thus increasing the complexity and security of the encryption process. First suitable parameter values are initialized. Then 3D Tinkerbell Chaotic map is produced and bit-wise XOR operation is carried out among the pixel values and the generated values to encrypt the image. Decryption is also done using the same method taking the encrypted image as input.

The proposed image processing models are shown in Fig1 and fig2 respectively.

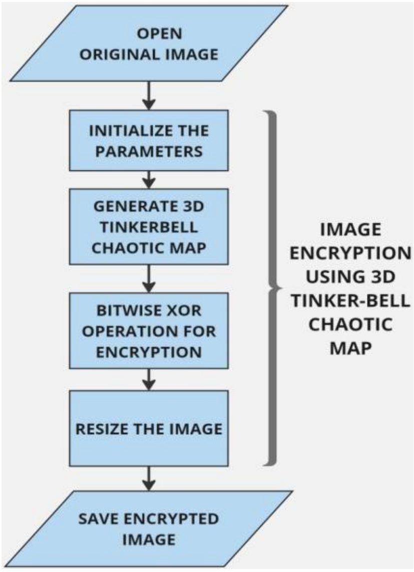


Fig 1. Proposed Encryption model

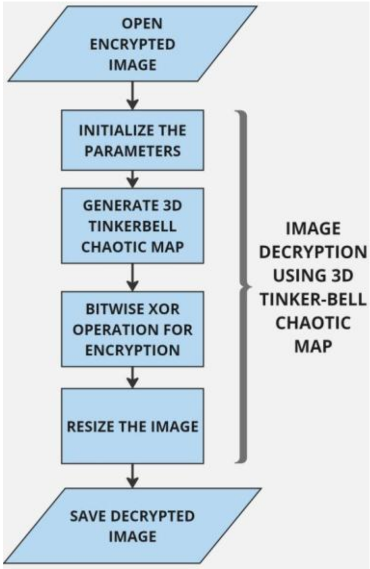


Fig 2. Proposed Decryption model

The 3D Tinkerbell Cat map is expected to show higher NPCR and UACI values, indicating stronger resistance to differential attacks, and achieve lower MSE, higher PSNR, and NCC values closer to 1, showcasing superior decryption performance. The encrypted images using the 3D map should exhibit more uniform histograms, suggesting enhanced security, while the decrypted images' histograms should align closely with those of the original images, confirming accurate decryption. Overall, the 3D method is anticipated to outperform the 2D method, providing stronger protection against differential attacks and higher decryption accuracy, making it a more secure choice for modern cryptographic needs.

Result Analysis

In this analysis, two images—a flower (Fig. 3) and sunglasses (Fig. 4)—are used to compare the effectiveness of encryption and decryption using both the 2D and 3D Tinkerbell Cat maps. To process these images, Python 3.11.4 is used in Windows i7 11th Gen environment.

Fig. 3. Flower (size: 256 x 256

Fig. 4. Sunglasses (size: 512 x 512)

Fig. 5 and Fig. 6 show the image encryption and decryption using 2D Tinkerbell cat map.

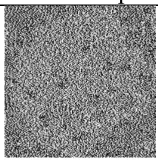
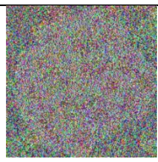
 Encryption of Gray Image using 2D Tenkerbell cat map	 Decryption of Gray Image using 2D Tenkerbell cat map	 Encryption of Color Image using 2D Tenkerbell cat map	 Decryption of Color Image using 2D Tenkerbell cat map

Fig. 5. Encryption and Decryption of Flower image using 2D Tinkerbell map

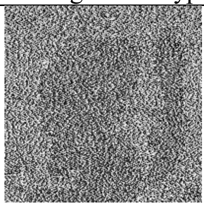
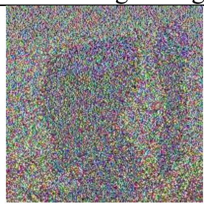
 Encryption of Gray Image using 2D Tenkerbell cat map	 Decryption of Gray Image using 2D Tenkerbell cat map	 Encryption of Color Image using 2D Tenkerbell cat map	 Decryption of Color Image using 2D Tenkerbell cat map

Fig. 6. Encryption and Decryption of Sunglasses image using 2D Tinkerbell map

The encryption and decryption of the sample images using 3D Tinkerbell cat map are shown in Fig. 7 and Fig. 8.

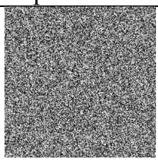
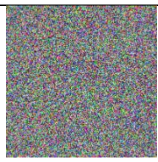
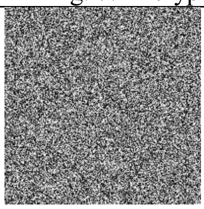
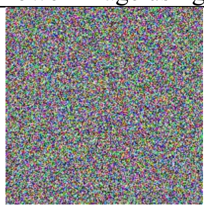
 Encryption of Gray Image using 3D Tenkerbell cat map	 Decryption of Gray Image using 3D Tenkerbell cat map	 Encryption of Color Image using 3D Tenkerbell cat map	 Decryption of Color Image using 3D Tenkerbell cat map

Fig. 7. Encryption and Decryption of Flower image using 3D Tinkerbell map

 Encryption of Gray Image using 3D Tenkerbell cat	 Decryption of Gray Image using 3D Tenkerbell cat	 Encryption of Color Image using 3D Tenkerbell cat	 Decryption of Color Image using 3D Tenkerbell cat

map	map	map	map

Fig. 8. Encryption and Decryption of Sunglasses image using 3D Tinkerbell map

The security and performance of these methods are evaluated using several metrics: NPCR and UACI to determine resistance to differential attacks, and MSE, PSNR and NCC to assess decryption performance and the time taken by the process to execute is also calculated to detect the security and robustness. Additionally, histogram analysis of the original, encrypted, and decrypted images is conducted to estimate security.

The result of altering an original picture pixel in an encrypted image is verified using the NPCR parameter [9, 10]. Let A and B be two pictures that differ by only one pixel. The NPCR is computed as eq. 3.

$$NPCR = \frac{\sum_{i,j} K(i,j)}{a * b} * 100\% \qquad (3)$$

Where, K matrix can be described as eq. 4.

$$K(i,j) = \begin{cases} 0, if\ A(i,j) = B(i,j) \\ 1, if\ A(i,j) \neq B(i,j) \end{cases} \qquad (4)$$

The parameter, UACI may be used to compute the percentage of pixel discrepancies between images A and B as per eq. 5 [9, 10].

$$UACI = \frac{\sum_{i,j} \frac{|A(i,j) - B(i,j)|}{255}}{p * q} * 100\% \qquad (5)$$

Where, p and q denote the image’s width and height respectively.

The NPCR and UACI analysis is shown in Table. 1.

Table 1. Analysis of NPCR and UACI

	NPCR value (%)	**UACI value (%)**
Encryption of Fig-3 using 2D Tinkerbell map	99.407958984375	45.525716145833336
Encryption of Fig-3 using *3D* Tinkerbell map	99.481201171875	47.64134425742954
Encryption of Fig-4 using 2D Tinkerbell map	99.56130981445312	50.23517634405635
Encryption of Fig-4 using *3D* Tinkerbell map	99.58648681640625	49.85867818196615

PSNR block calculates the peak signal-to-noise ratio in dBs between two images. This is the signal-to-noise difference measured from the ratio. Higher values of PSNR maintain better quality for the encrypted image. Also the MSE and PSNR are used together for the performance evaluation. The MSE computes the cumulative squared error between the original and encrypted images where the peak signals to noise ratio measures the peak error. The lower value of MSE will show smaller errors.

To compute PSNR, the block first determines the mean-squared error using the eq. 6.

$$MSE = \frac{\sum_{m,n}[I_1(x,y) - I_2(x,y)]^2}{x * y} \qquad (6)$$

Where, x and y are the number of rows and columns in the input images. Then, the block computes the PSNR using eq. 7.

$$PSNR = 10log_{10}\left(\frac{R^2}{MSE}\right) \qquad (7)$$

Where, R is the maximum fluctuation in the input image [1].

Normalized cross-correlation (NCC) is frequently employed as a metric to assess the similarity or dissimilarity between two images. One notable advantage of NCC over standard cross-correlation is its reduced sensitivity to linear changes in illumination amplitude across the compared images. Additionally, NCC values are constrained within the range of -1 to 1 [1].

Table. 2 show the MSE, PSNR and NCC analysis.

Table 2. Analysis of MSE, PSNR and NCC

	MSE value	**PSNR value**	**NCC value**
Decryption of Fig-3 using *2D&3D* Tinkerbell map	10.0977	38.0886 dB	0.9983
Decryption of Fig-4 using *2D&3D* Tinkerbell map	19.1509	35.3089 dB	0.9934

The histogram analysis of both images in original format, encrypted format and decrypted format are shown in Fig. 9 – Fig. 14.

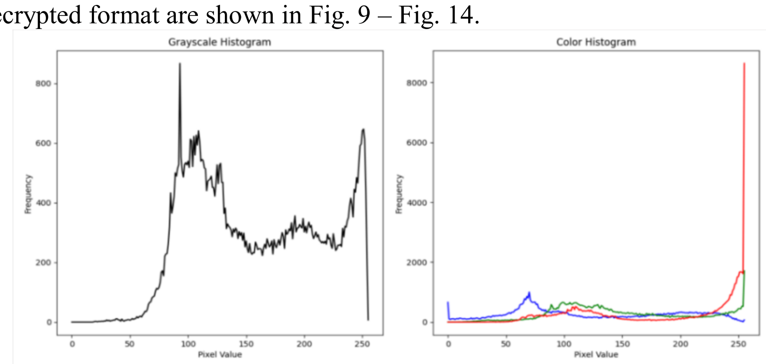


Fig. 9. Histogram of Flower image

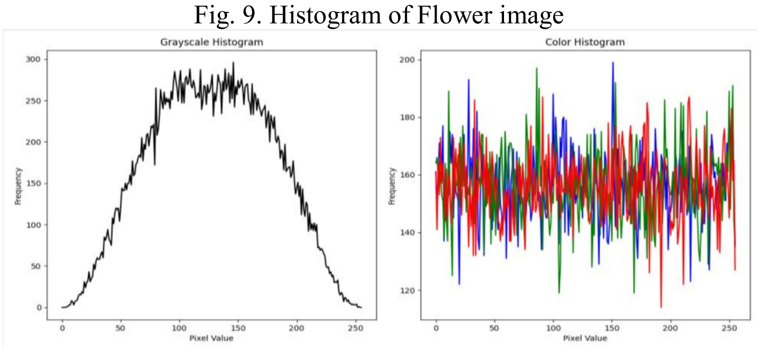


Fig. 10. Histogram of Encrypted Flower image using 3D Tinkerbell cat map

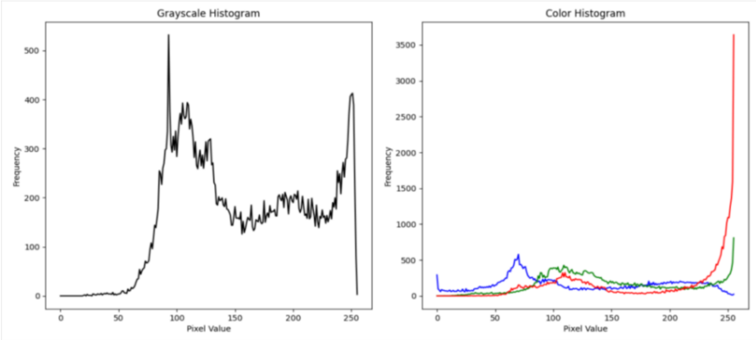


Fig. 11. Histogram of Decrypted Flower image using 3D Tinkerbell cat map

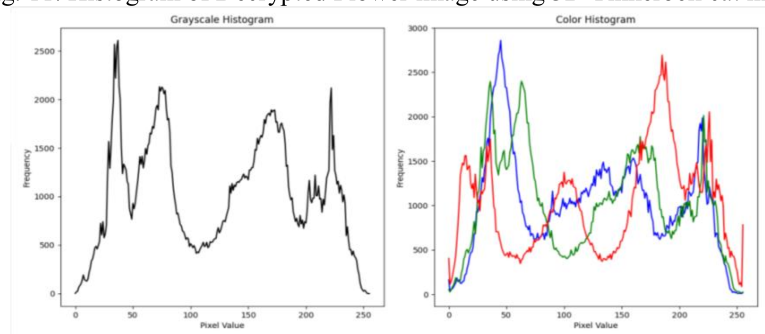


Fig. 12. Histogram of Sunglasses image

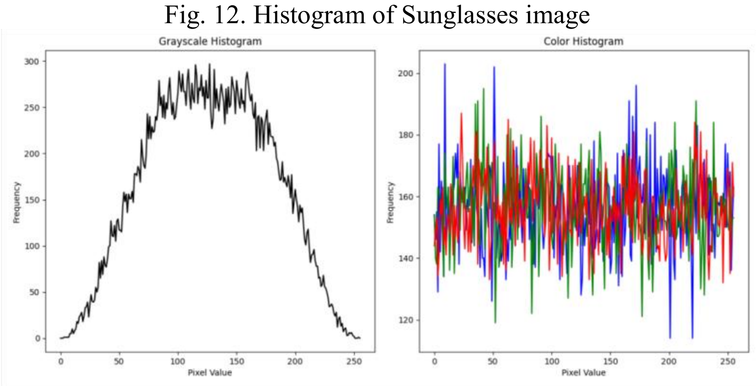


Fig. 13. Histogram of Encrypted Sunglasses image using 3D Tinkerbell cat map

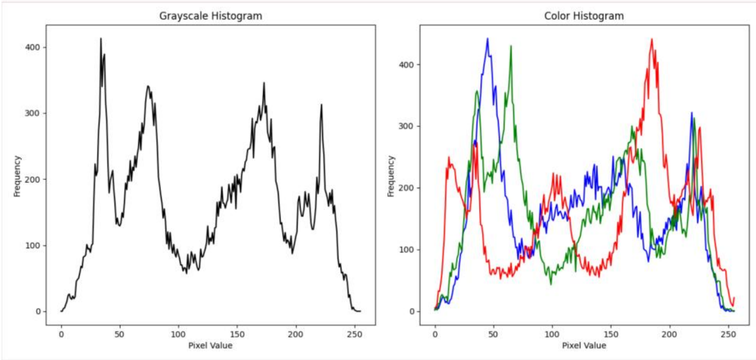


Fig. 14. Histogram of Decrypted Sunglasses image using 3D Tinkerbell cat map

The time taken for encryption process and decryption process in both methods are shown in Table. 3.

Table 3. Encryption and Decryption Time

	Encryption Time (sec)	Decryption Time (sec)
Fig-3 Using 2D Tinkerbell Cat Map	0.0870	0.0955
Fig-3 Using 3D Tinkerbell Cat Map	0.1328	0.1442
Fig-4 Using 2D Tinkerbell Cat Map	0.0911	0.0899
Fig-4 Using 3D Tinkerbell Cat Map	0.2116	0.1367

3D encrypted image is having a uniform histogram which means the original image information is effectively hidden from unauthorized access. This uniformity again indicates that the encryption process is highly effective since it avoids any pattern or information leakage of the original image from the resulting encrypted image. NPCR & UACI are the tools to check sensitivity against minor alteration in the original image. The 3D Tinkerbell map enacts in a better way than the 2D map in both the evaluation schemes. This enriched version of sensitivity further emphasizes the supremacy of the security features of the 3D map. As it projects a level of unpredictability and complexity towards an attack, therefore increasing its resistance to attacks. Some other examples of metrics taken for evaluating the overall performance of the encryption scheme are MSE, PSNR, and NCC. It is found in studies that both the 3D and the 2D Tinkerbell maps produce equivalent scores in these metrics. Briefly, the 3D map does not lose out in performance in image quality and fidelity. One the other hand in light of some studies it is seen that the increased dimension of the 3D Tinkerbell map takes extra time to process both the encryption and the decryption in comparison to the analogous version of the 2D Tinkerbell map. The remarkable weaving of heightened security and increased computational time apprehends its sustainable form in these particular cases. Along with longer processing time, the multifaceted attributes of added dimensions of the 3D Tinkerbell map catches the intellect minds to prefer it as a better component to secure sensitive data exchanged over public networks.

Conclusion

In conclusion, the paper illustrates a pioneering image of encryption and decryption scheme utilizing the three dimensional Tinkerbell chaotic map. The enhanced security features are developed because of the added complexities which comes hand in hand with the 3D chaotic map. Extensive evaluations and analysis including histogram analysis of the approach reveal superior performance and security features when compared to its 2D counterpart.

Notable upliftments in NPCR and UACI are perceived due to the 3D Tinkerbell chaotic map's proliferate and immensely secured methods. The longer processing time is also an indicator of increased complexity and uneven nature. The most beneficial segment of this tool is that the 3D Tinkerbell map assists to defend sensitive data. The 3D Tinkerbell map can also make a significant performance at the fields of scientific applications which include digital watermarking where the more powerful and secure forms of encryption are concerned. With great potential it can provide secure solutions in these very areas and can open an exciting path to carry forward deeper investigations and developments.

References

1. C. Pradhan, V. Saxena and A. K. Bisoi, “Non blind digital watermarking technique using DCT and Cross chaos map”, International Conference on Communications, Devices and Intelligent Systems (CODIS), IEEE, Kolkata, 2012, pp. 274-277.
2. P. S. Krishna, Ch. V. M. S. Teja, R. Devi S. and Thanikaiselvan V., “A Chaos Based Image Encryption using Tinkerbell Map Functions”, International Conference on Electronics, Communication and Aerospace Technology (ICECA), IEEE, Coimbatore, 2018, pp. 578-582.
3. T. A. Dhopavkar, S. K. Nayak and S. Roy, “IETD: a novel image encryption technique using Tinkerbell map and Duffing map for IoT applications”, Multimedia Tools and Applications, Springer, vol. 81, 2022, pp. 43189-43228.
4. R. Enayatifar, H. J. Sadaei, A. H. Abdullah, M. Lee and I. F. Isnin, “A novel chaotic based image encryption using a hybrid model of deoxyribonucleic acid and cellular automata”, Optics and Lasers in Engineering, Elsevier, vol. 71, 2015, pp. 33-41.
5. M. Khan and T. Shah, “An efficient chaotic image encryption scheme”, Neural Computing and Applications, Springer, vol. 26, 2015, pp. 1137-1148.
6. S. Kumar and C. Pradhan, “Color Image Encryption Technique using 4D Logistic Map”, Progress in Computing, Analytics and Networking, Springer, 2020, pp. 75-82.
7. Tenkerbell map, https://en.wikipedia.org/wiki/Tinkerbell_map.

8. A. Ouannas, A.-A. Khennaoui, S. Bendoukha, T. P. Vo, V.-T. Pham and V. V. Huynh, “The Fractional Form of the Tinkerbell Map Is Chaotic”, Applied Sciences, MDPI, vol. 8 (12), 2018.
9. Y. Wu, J. P. Noonan and S. Agaian, “NPCR and UACI Randomness Tests for Image Encryption”, Cyber Journals: Multidisciplinary Journals in Science and Technology, 2011, 31-38.
10. H. Khanzadi, M. Eshghi and S. E. Borujeni, “Image Encryption using Random Bit Sequence based on Chaotic Maps”, Arabian Journal for Science and Engineering, vol. 39, 2014, pp. 1039-1047.