International Journal of Engineering Inventions
e-ISSN: 2278-7461, p-ISSN: 2319-6491
Volume 13, Issue 1 [January. 2024] PP: 61-69

Image Steganography - Mid Point Circle And Chaotic Map Based Random Pixel Block Selection Approach

K. Anandharaj[1], J. Abdul Samath[2]
Ph.D Research Scholar[1], Assistant Professor[2]
1 PG & Research Department of Computer Science, Chikkanna Government Arts College, Tirupur – 641602

Abstract:
In this paper, a technique of secure data hiding in image is proposed that new image steganography method based on chaotic map also a Mid Point Circle Algorithm. The data has been embedded in the least significant bits of Red (3), Green (2) and Blue (3) positions of random pixels of circle image. The proposed method changes the LSB of only some of the pixels based on the above comparison. Based on parameters like PSNR and MSE the efficiency of the method is checked after implementation. Then the comparison did with some existing techniques. This is how, image steganography showed interesting and assure results when compared with other techniques.

Keywords*: Information hiding, Image Steganography, Mid Point Circle. Chaotic map, Least Significant Bit.*

Date of Submission: 02-01-2024 Date of acceptance: 13-01-2024

I. INTRODUCTION

The Internet is at the top of everyone's list of needs in today's world. It's the main way to share files, resources, etc. Internet Security is a major concern to ensure the security and authorization of the users and the data. Encryption has been used for a long time to protect the data. It converts plain text to encrypted text using certain encryption algorithms. It makes the plain text or message unbreakable but also makes the message suspect. Encryption isn't a very effective way to secure data because there are many ways to hack the encrypted text. An experienced hacker can easily decrypt the encrypted text by using a hit and trace method. Steganography is an alternative method to hide the data. It doesn't attract any hacker's attention and provides security. Steganography is a technique for hiding a secret message in a image, video, or audio file. The image is a cover image since it contains the hidden content. The image that is created is the stego image once the secret message is embedded. LSB substitution is a well-known steganography technique. By substituting n LSBs of the image element with n bits of the secret message, it embeds the secret message. The stego-image security of the straightforward LSB approach can now be enhanced with a genetic algorithm of optimal LSB substitution, which is based on the LSB substitution methodology.

The basic structure of image steganography is composed of the following:

- ✓ Secret-message: The data is to be hidden and delivered.
- ✓ Cover-image: An original image is used as a media to embed the secret-message.
- ✓ Stego-image: After the cover-image embeds the secret-message, the resulting image is known as the stego-image.
- ✓ Stego-key: Additional information is used for embedding and extracting the secret-message. The stego-key is a shared key known to the sender and receiver only[1].

II. LITERATURE REVIEW

Wang et al. [2] have proposed a new hiding data scheme with distortion tolerance. The proposed scheme not only can prevent the quality of the processed image from being seriously degraded, but also can at once achieve distortion tolerance. They show that the proposed scheme indeed can obtain a high-quality image and is more to the other schemes in terms of its distortion tolerance.

Zhang et al. [3] this paper is based on four-pixel differencing and modified least significant bit (LSB) substitution, used to improve the embedding capacity and provide an imperceptible visual quality. The common difference value of a four-pixel block is exploited to classify the block as a smooth area. By the k-bit modified LSB substitution method is used to hide the secret data into each pixel and we can readjust the work to manage the perceptual distortion. This will provide a suitable image quality as well as a wide embedding capacity. But this method does not give a stronger security.

Gutte et al. [4] the secret communication system has two layered security levels. First level is through encryption of the text using extended substitution algorithm and second one is through embedding the encrypted

text into LSBs unpredictably. The verification of both the Steganography schemes along with Extended Substitution Algorithm has been done and it is clear from the experimentation that inserting the data at three LSB positions does not change image parameters like PSNR, Mean, Standard deviation, Entropy in much extent. Therefore, it retains the image quality similar to two LSB scheme. It can be used to secure all type of data like alphabets (small as well as capital), special characters and mathematical symbols. The variable *y* takes values as 0, 1, 2, 3. Embedding the cipher at LSBs is decided by variable *y*. As the LSB in each pixel are not same but decided according to variable value, it is stronger approach and helps in minimizing the error.

Juneja and Sandhu [5] this paper defines an advance for Information Security in RGB Color Images using a Hybrid Feature detection method. Two element based Least Significant Bit (LSB) Substitution Technique and Adaptive LSB substitution technique for data hiding. The proposed approach achieved Improved Imperceptibility, Capacity than the various existing techniques along with Better Resistance to various Steganalysis attacks like Histogram Analysis, Chi-Square and RS Analysis as proven experimentally.

Bhardwaja and Khanna [6] have presented two levels of security through a process of two steps, rather than hidden the message bits directly in cover image, they were twisted in a random regulates and generated by 2D Arnold Cat Map after that encrypted message is hidden behind a cover image using basic LSB method. MSE (Mean Square Error) and PSNR (Peak Signal to Noise Ratio) are two common quality measurements to measure the difference between the cover-image and the stego image. Results showed that the projected method gave better results than simple LSB with higher PSNR and lower MSE.

III. PROPOSED ALGORITHM

In this section, the proposed technique is presented. The proposed technique is divided into two algorithms; the embedding algorithm, and the extraction algorithm. The embedding algorithm will plan to hide the byte of the secret message in three pixels only based on Midpoint circle randomization in the cover image. It takes the cover image and the secret message characters as an input and converts each byte from the secret message to its binary format using the ASCII encoding format (each byte equal 8-bits Image pixel is converted into three layers (Red, Green, and Blue) layer. Each pixel in the (Red, Green and Blue) layers is converted to its binary using the ASCII encoding format. In the embedding technique, (3-2-3) layer is used (i.e. two layers (Red and Green) are used in the first iteration), in the second iteration only one layer is used (i.e., Blue). In the next iteration, two layers are used (Red and Green) and so on. The method of using of two layers then one layer then two layers leads to more secure and getting better PSNR value. The secret message is embedded randomly in the pixel locations using Logistic map instead of sequential. This method of embedding is considered more secure than the embedding in a sequential manner. The whole technique is illustrated in the Fig 4.

3.1 Midpoint circle algorithm

In the computer graphics circle generation algorithm, because of the need to display or output graphics on the dot matrix output device, a raster scan conversion algorithm [7,10] is also needed to perform pixel point conversion. Directly using the point coordinate equation to calculate the position of the point on the circle requires multiplication and square root operations, which will increase the computational cost and algorithm complexity. Therefore, the method of drawing the midpoint circle is introduced.

In this algorithm, we split the circle into 8 different Octant. If we are able to plot the points in first Octant, then by balance we can plot the points in other 7 Octant. Let (x, y) be the point in first octant, then the points in other octants can be determined as shown in the given table 1[11]:

Octant	1	2	3	4	5	6	7	8
Point	(x, y)	(y, x)	(y, - x)	(x, - y)	(- x, - y)	(-y, - x)	(- y, x)	(- x, y)

Table 1: Eight Octants in Midpoint Circle Algorithm

This algorithm gives

$$f(x, y) = x^2 + y^2 - r^2 \quad (1)$$

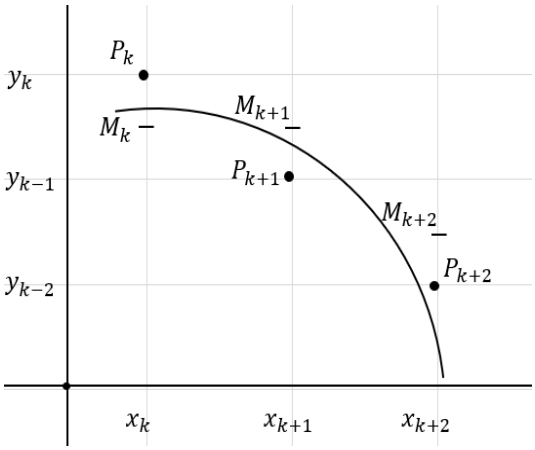

Fig.1. First Octant Midpoint Circle

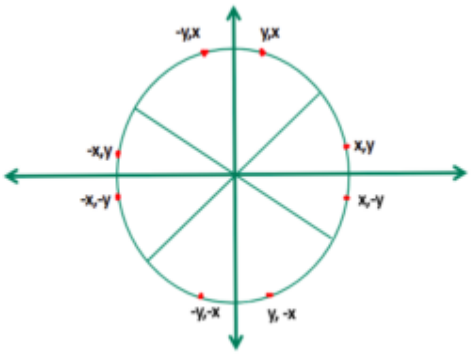

Fig.2. Midpoint Circle

Taking a circle cantered at the source with a radius of 'r' units, its equation can be defined as $x^2 + y^2 = r^2$. From this, we derive a function f(x, y) represented as $f(x, y)=x^2+y^2-r^2$ The circle encompasses all points (x, y) suit f(x, y)=0, assuming x and y as real values[12]. Points satisfying f(x, y) lie outside the circle's boundary. This delineation is visually presented in Fig. 1.

Any point in the first octant may be select as (x_k, y_k), and it is assumed that this point is moving clock wise in the XY-plane.

Fig. 3: Eight Octants

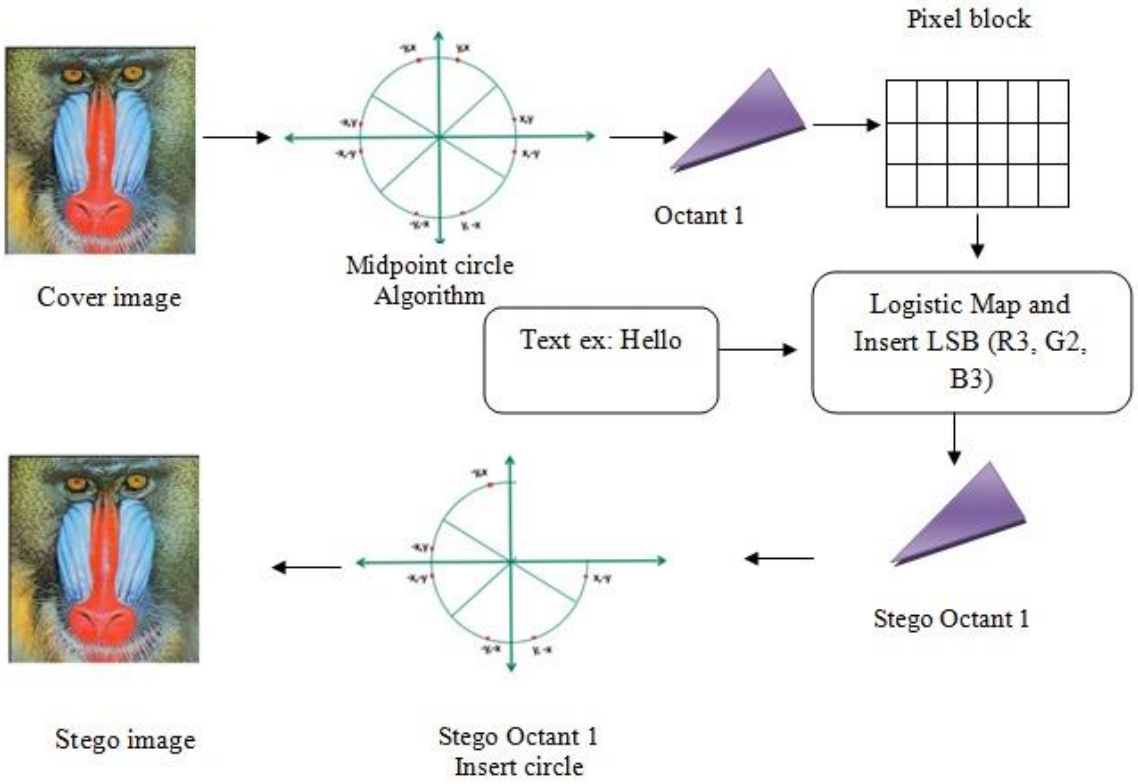

Fig. 4: Proposed Embedded Architecture

3.2 Random Pixel Block Selection Using Logistic Map

It is the simplest form of chaotic method, which is developed by May [16]. Logistic map is described in Equation (2).

$Xn+1 = R \times Xn\,(1 - Xn)$ (2)

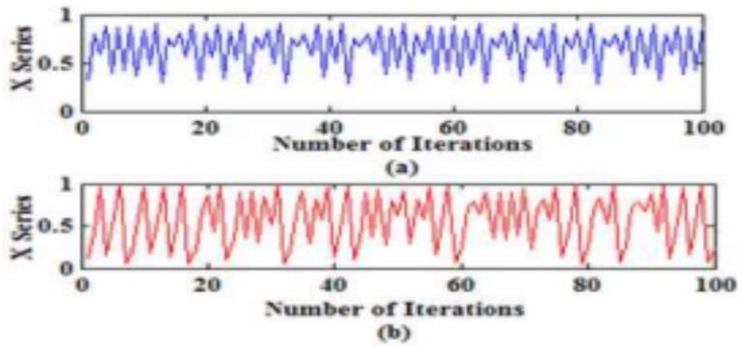

Fig. 5. Randomness logistic map chaotic series

(a). X= 3.95 and R = 0. 12 N= 100 (b) X = 3:85 and R = 0:25 N= 100

For selecting Pixel Block selection sequence is generated by using logistic map. For Example: Xo=0.80, r =3. 55. and n = 8 then multiply the sequence with the number of 100 round the result (Table 2).

X= round (Logistic map * 100) (2)

N	R	RXn	(1-Xn)	Xn	Xn*100	Pixel Block
0				0.8	80	81
1	3.55	2.84	0.2	0.57	57	57
2	3.55	2.0164	0.432	0.87	87	87
3	3.55	3.092351	0.128915	0.40	40	40

4	3.55	1.415211	0.601349	0.85	85	85
5	3.55	3.021177	0.148964	0.45	45	45
6	3.55	1.597668	0.549953	0.88	88	88
7	3.55	3.119178	0.121358	0.38	38	38

Table 2: Selection on Random Pixel in Circle Octants1

Fig.6: illustrates the exact use of chaotic behavior in random pixel Block selection. This phenomenon could be used for storing the text information in the random selection of pixels Block.

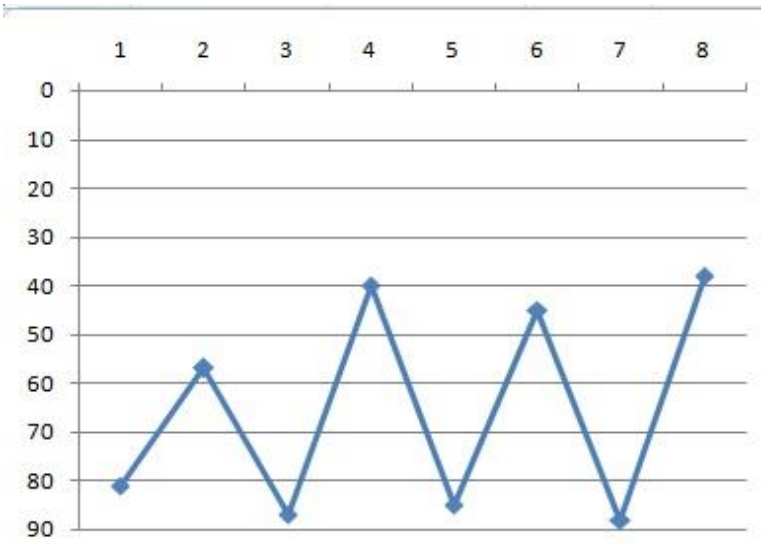

Fig 6: Random Pixel Block Selection

1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20
21	22	23	24	25	26	27	28	29	30	31	32	33	34	35	36	37	**38**	39	**40**
41	42	43	44	**45**	46	47	48	49	50	51	52	53	54	55	56	**57**	58	59	60
61	62	63	64	65	66	67	68	69	70	71	72	73	74	75	76	77	78	79	80
81	82	83	84	**85**	86	**87**	**88**	89	90	91	92	93	94	95	96	97	98	99	100

Table 3. Pixel Block

3.3 Encoding Algorithm

The process of inserting text messages on image using the Midpoint circle method has the various stages described in the insertion process flow diagram. The process can be seen in the following pseudo code of Algorithm 1.

Algorithm I: Encoding process

```
input : stego, messages,
output : stego_image
1.      image ← read()
2.      messages ←read()
3.      ascii ←text_to_ascii(messages)
4.      binary ←ascii_to_binary(ascii)
5.      Mid Point Circle Algorithm
 Midpoint On image Sequence Generate from Equation 1.
  for(i=o1;i<8;i++)
    Count total no pixel ←co-ordinate in First O1.
    Generate Pixel Block Store Each pixel Co-Ordinate.
```

```
 End
6.      Chaotic Map Random Pixel operation
7.      Random Pixel  Block Generate X number ← generate_Random Pixel
(Chaotic Sequence X={x1, x2, x3…. xn}) Sequence Generate from Equation 2.
8.       for each i1 image
9.      If (Iteration (Odd=True))
Select Pixel LSB (R3, G2) + Mi
        Else
Select Pixel LSB (B3) + MI
    End If
10.     i1 ← insertion()
11.     stego_image
12.     output(Stegoimage)
```

3.4 Decoding Algorithm

The insertion process is repeated up to as many characters as the message and is repeated all the way to the entire image of the container image. The Pseudo code for extraction process is shown in following Algorithm 2.

Decoding Algorithm

```
input : stego_image,
output : text
1.      stego← read()
2. Mid Point Circle Algorithm
 Midpoint On image Sequence Generate from Equation 1.
  for(i=o1;i<8; i++)
    Count total no pixel ←co-ordinate in First O1.
    Generate Pixel Block Store Each pixel Co-Ordinate.
 End


3.      Chaotic Map Random Pixel operation identified by iterating the chaotic map with key
4.      X random_Pixel  Block Generate X number ← identified_Random Pixel Block
5.      for each i1 image
6.      If (Iteration (Odd=True))
7.      Select Pixel Retrieve value LSB (R3, G2)
8.      Else
9.      Select Pixel Retrieve Value LSB (B3)
10.     End If
11.     binary ← extract()
12.     output(binary)
13.     ascii ← binary_to_ascii(binary)
14.     text ← ascii_to_text(ascii)
15.     output(text)
```

IV. RESULT AND DISCUSSION

All the experiments are performed in MATLAB 7 (R2015a) on a PC with 2.50 GHz Intel(R) Core, 4.00 GB RAM and 500 GB HDD under windows 10 environment. All the images are of size 1024×1024 and are in Jpg format. The performance evaluation metrics used are Peak Signal to Noise Ratio (PSNR), Mean Square Error (MSE). In this work, considered to calculate PSNR, MSE and Embedded time for various images. PSNR of cover and stego image less than 30 is perceptible to human eyes. Image quality is better when PSNR value is higher. PSNR is measured in decibels. peak signal to noise ratio (PSNR),

a. Lena b. Fruit c. Lake

d. Baboon e. Pepper f. Airplane

Fig 7. The test images

The resulting stego images are compared with original cover images to calculate MSE and PSNR values, The proposed 3-2-3 algorithm provides better results compared previous method in terms of MSE and PSNR, NAE, SSIM values. The results of proposed method and previous method are provided in Table 3. To show the clear difference between MSE and PSNR values obtained by proposed method.

	Existing		Proposed	
Test Images	**PSNR**	**MSE**	**PSNR**	**MSE**
lena	58.31	0.134	63.61	0.042
Fruit	52.89	0.473	59.53	0.294
Lake	49.97	0.843	57.28	0.152
Baboon	46.71	1.046	52.86	0.793
Pepper	52.80	0.754	61.53	0.384
Airplane	58.34	0.476	63.51	0.154

Table 4: Comparison existing and proposed algorithm

The results are further illustrated with graphical representation to visualize better as shown in Fig. 8.

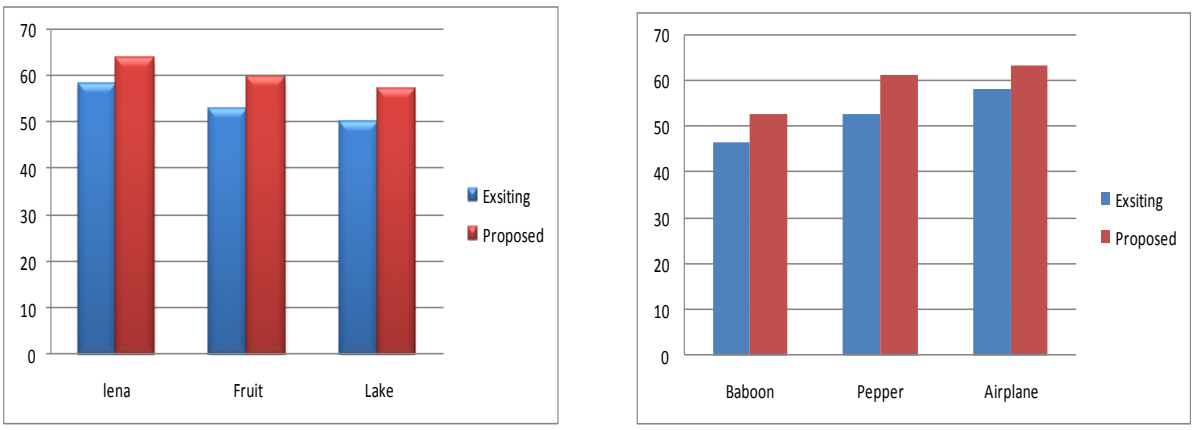

Fig 8. Performance analysis of test images for PSNR

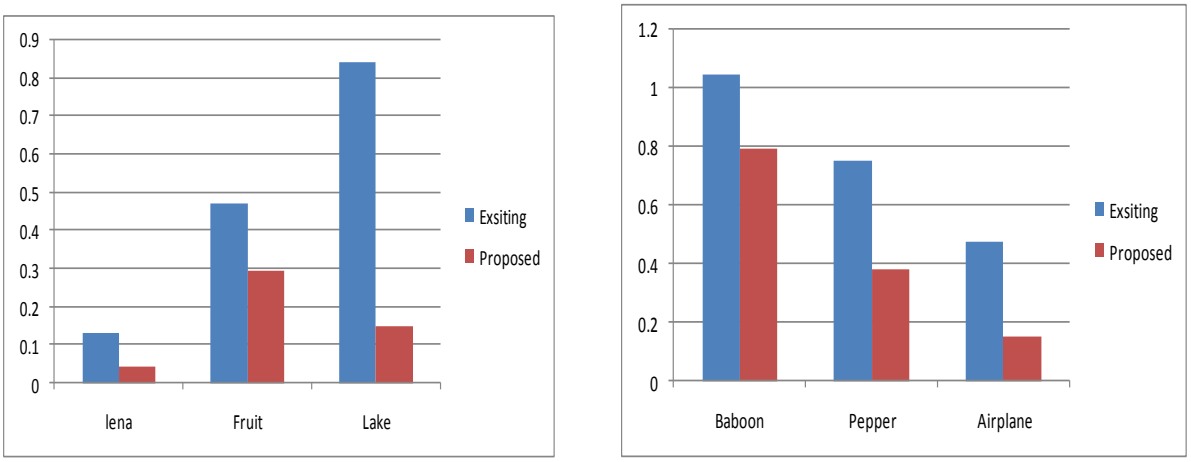

Fig 9. Performance analysis of test images for MSE

V. Conclusion

In this paper, we proposed a steganographic method based on Midpoint circle algorithm and chaotic map for random pixel block selection substitution. The result in table 4 , show that the proposed method is able to achieve high PSNR values in color images . The embedding time increases with the increase in no of bits embedded. The proposed method for shuffling the R, G, B component while embedding and the same for extraction, so one can prioritize which colour blocks should be used first for embedding (usually the least important in the image. In future, the proposed technique with slight modification could be applied on as video, even on encrypted files. Because, the chaotic sequences once generated could be employed both for steganography as well as encryption also.

REFERENCES

[1]. Xiaoli Huan, Hong Zhou, Jiling Zhong,"LSB based Image Steganography by using the Fast Marching Method", International Journal of Advanced Computer Science and Applications, Vol. 10, No. 3,P.0 1-5 1-5, 2019.

[2]. Y.B. Lin, C.M. Wang and I.C. Lin. "Hiding data in spatial domain images with distortion tolerance." Computer Standards & Interfaces 31(2009): 458-464.

[3]. X. Liao, Q.y. Wen, and J. Zhang. "A steganographic method for digital images with four-pixel differencing and modified LSB substitution." Journal of Visual Communication and Image Representation 22.1 (2011): 1-8

[4]. R. S. Gutte, Y. D. Chincholkar, and P. U. Lahane. "Steganography for two and three LSBs using extended substitution algorithm." ICTACT Journal on communication technology 4.01 (2013): 685-690

[5]. M. Juneja and P. S. Sandhu. "Improved LSB based Steganography Techniques for Color Images in Spatial Domain." IJ Network Security 16.6 (2014): 452-46

[6]. R. Bhardwaja and D. Khanna. "Enhanced the security of image steganography through image encryption." India Conference (INDICON) 17 (2015):1-4.

[7]. Jiaguang Sun.Computer Graphics[M].Beijing:Tsinghua university press,1998.

[8]. ZHU Xiao-lin, GAO Cheng-hui, HE Bing-wei, HUANG Min-chun, CHEN Jie. An Improved Method of Hough Transform Circle Detection Based on the Midpoint Circle- Producing Algorithm[J]. JOURNAL OF ENGINEERING GRAPHICS, 2010, 31(6):29-33.

[9]. Wang Zhixi, Wang Runyun. Improvement of Bresenham's Circle Generation Algorithm[J]. COMPUTER ENGINEERING, 2004, 30(12):178-180.

[10]. Shi Zhixin. Research on Basic Raster Graphics Generation Algorithm[D]. ShanDong University, 2007.

[11]. Javed Idrisi, " Generalization of Midpoint Circle Drawing Algorithm", March 2021

[12]. N. S. Nithya , M. Javed Idrisi," Enhancements in Circle Rendering: An Improved Approach to the Midpoint Circle Drawing Algorithm", International Journal of Networked and Distributed Computing, November 2023.

[13]. May R. M., et al., Simple mathematical models with very complicated dynamics," Nature, vol.261, 459- 467, 1976.

[14]. Ammad Ul Islam, Faiza Khalid, "An Improved Image Steganography Technique based on MSB using Bit Differencing", International conference on innovative computing techninology, Pg: 265-269, 2016.

[15]. Souvik Kumar, Kuntal Ghosh, "Data Hiding by Image Steganography Applying DNA Sequence Arithmetic & LSB Insertion", Journal for Research Volume 02, Issue 04 , pg: 49-57,June 2016.

[16]. Varsha, Rajender Singh Chhillar, "Data Hiding Using Steganography and Cryptography", International Journal of Computer Science and Mobile Computing, Vol. 4, Issue. 4, pg.802 – 805, April 2015.

[17]. Subhash Panwar, Shreenidhi Damani, " Digital Image Steganography Using Modified LSB and AES Cryptography", International Journal of Recent Engineering Research and Development (IJRERD), Volume 03 – Issue 06, Pg. 18-27, June 2018.

[18]. Aishwarya Pandey, Jharna Chopra, "Steganography Using AES and LSB Techniques", International Journal of Scientific Research Engineering & Technology (IJSRET), Volume 6, Issue 6, Pg: June 2017620-623.

[19]. Aung Myint Aye, LSB Based Image Steganography for Information Security System, International Journal of Trend in Scientific Research and Development (IJTSRD), Volume - 3 Issue – 1,PP: 394-400 Nov – Dec 2018.

[20]. Naveen Verma, Preeti Sondhi," LSB Based Stegnography to Enhance the Security of an Image", International Journal of Trend in Scientific Research and Development (IJTSRD), Volume: 3, Issue: 4 , PP: 1480-1484 May-Jun 2019.

[21]. Pravin B. Desai, Pradip S. Bhendwade," Image Steganography Using LSB Algorithm", International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineerin, Vol. 5, Issue 8, PP: 6883-6890 August 2016.

[22]. Pooja Rani, Preeti Sharma, "Cryptography Using Image Steganography",International Journal of Computer Science and Mobile Computing, Vol. 5, Issue. 7, pg.451 – 456, July 2016.