ISBN: 978-1-948012-17-1

Ethics and Information Technology (ETIT)

DOI: <http://doi.org/10.26480/etit.02.2020.57.61>

COMPARATIVE ANALYSIS BETWEEN DIFFERENT TYPES OF FIGURATE NUMBER BASED DOUBLE LAYER IMAGE STEGANOGRAPHY IN SPATIAL DOMAIN

Pratik Halder^{a*}, Satrajit Das^b and Sukanta Kundu^c^aDepartment of Computer Science and Engineering, Gargi Memorial Institute of Technology, Kolkata, Pin: 700144, India.^bDepartment of Computer Science and Engineering, Gargi Memorial Institute of Technology, Kolkata, Pin: 700144, India.^cDepartment of Computer Science and Engineering, Gargi Memorial Institute of Technology, Kolkata, Pin: 700144, India.*Corresponding Author Email: pratikhalder2001@gmail.com

This is an open access article distributed under the Creative Commons Attribution License CC BY 4.0, which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

ARTICLE DETAILS

Article History:

Received 25 October 2020

Accepted 26 November 2020

Available online 03 December 2020

ABSTRACT

Presently, in this current decade, the main goal is to protect data during transmission over unsecured communication channel. Usually cryptography is used to provide security of data during transmission; beside this another effective technique steganography is mostly used to solve the issue. Our proposed work can hide up to 8 bits of secret information in each pixel intensity value of an image with minimal distortion which is very satisfactory result than other state-of-the-art works. Here the focus area is to enhance the level of reliability of the actual information during transmission. To provide this we have embed secret information by different types of figurate number system and compare with previously discovered triangular number based algorithm. We have compared the output various quality metrics analysis techniques and get satisfactory result. Our algorithm is also capable to resist statistical attacks like Chi – Square test, etc., and produce satisfactory result by all standard tests which are considered as benchmark test like StireMark.

KEYWORDS

Multi-bit Embedding, Spatial Domain, Figurate Number System, Information Security, Steganography.

1. INTRODUCTION

Steganography focuses on communication of secret data over some covered media viz., video, audio, image, text etc (Paul et al., 2012; Zhang et al., 2008). Generally available steganographic algorithms follow Least Significant Bit (LSB) based data hiding technique with less embedding capacity. Anyone can attack the system easily if the communication becomes transparent. So our main concentration is to hide the existence of secret information from cover media. Based on recent study, there have proposed pixel indicator based steganographic technique (Gutub et al., 2010). Other study also has proposed a multi-bit steganographic algorithm with increased capacity (Bailey et al. 2006). A previous study has demonstrated and implemented Catalan and Fibonacci number for encoding (Manes et al., 2012). Since no comparative analysis between various types of figurate number system based algorithm is available so we make this analysis to enhance the reliability of secret information while transmission.

We have proposed a comparative study between Different Types of Figurate Number Based Double Layer Image Steganography in Spatial Domain in this present work. Here we implemented double layer embedding technique which can hide up to 8 bits of secret information over cover medium. We use different types of figurate number system like square, pentagonal, hexagonal number system based algorithm here and compare with triangular number system based embedding algorithm and calculates efficiency between all these with triangular number system based embedding algorithm. Here we have shown the enhancement of the distortion and capacity. We have discuss different figurate number series in Section 2. We discuss our proposed method in Section 3, and different

types of statistical tests with other experimental results in Section 4. We also test our result by statistical attack test like Chi-Square test and compare efficiency with benchmark test like StirMark analysis where result is satisfactory.

2. BASIC IDEA

Our proposed steganographic comparison calculates efficiency between different types of figurate number system like square, pentagonal, hexagonal based algorithm with triangular number system based embedding algorithm.

Definition 1. A square number series or perfect square number series S_n is a figurate number which can be expressed by $S_n = n^2$ where n is an integer number. Few first plot of square number represented by dots is shown in figure.

Figure 1: Pictorial representation of square number formed by n^{th} term of square number series (<http://www.wikipedia.org>)

On the other hand $(n + 1)^{\text{st}}$ square number S_{n+1} can be calculated by following formula:

Quick Response Code	This paper was presented at	Access this article online	
	International Conference on Contemporary Issues in Computing (ICCIC-2020) - Virtual IETE Sector V, Salt Lake, Kolkata From 25th-26th July 2020	Website: www.intelcomp-design.com	DOI: 10.26480/etit.02.2020.57.61

$$S_{n+1} = S_n + 2n + 1 \quad (1)$$

Definition 2. Triangular number series of length N can be structured by collection of dots, which form an equilateral triangle which is shown in below diagram.

Figure 2: Equilateral triangle formed by n^{th} term of triangular number series (<http://www.wikipedia.org>)

We can also calculate n^{th} term of the series by following formula:

$$t_n = \sum_{k=1}^n k = 1 + 2 + 3 + 4 + \dots + n = \frac{n(n+1)}{2} \quad (2)$$

Definition 3. Pentagonal number series is also a figurate number system. Where n^{th} term of pentagonal number series can be calculated by following formula:

$$p_x = \frac{3n^2 - n}{2} \text{ for } n \geq 1 \quad (3)$$

Pictorial representation of pentagonal number is shown in diagram.

Figure 3: Pictorial representation of pentagonal number formed by n^{th} term of pentagonal number series (<http://www.wikipedia.org>)

Definition 4. Similarly, pictorial representation of hexagonal number series is shown below diagram where n^{th} term of hexagonal number series can be calculated by help of below formula.

$$h_n = 2n^2 - n = n(2n - 1) = \frac{2n \times (2n - 1)}{2} \quad (4)$$

Figure 4: Pictorial representation of hexagonal number formed by n^{th} term of hexagonal number series (<http://www.wikipedia.org>)

Definition 5. For a particular bit sequence α and its equivalent decimal number $D(\alpha)$, the possible set of figurate number system based representation $D(\alpha)$ can be defined as

$$F \triangleq \arg_{\alpha_{i,1 \leq i \leq k}}^{\max} \{D(\alpha_i)\} \quad (5)$$

3. PROPOSED METHOD

Here we discuss two level of embedding technique to maximize the capacity and minimize distortion as discussed in (Halder et al., 2015). In first level, we can choose any channel from RGB cover image, here we have chosen green (say, $I_{x,y}^{(G)}$) is normalized to, $I'_{x,y}^{(G)}$ as shown in Table 1.

Number of bits from secret information for embedding (say, n) per pixel intensity can be determined by $I'_{x,y}^{(G)}$ as given in

$$n = \begin{cases} 8, & \text{if } 9 \leq I'_{x,y}^{(G)} \leq 118, \\ 4, & \text{otherwise.} \end{cases} \quad (6)$$

Now, figurate number system based representation of $I'_{x,y}^{(G)}$ can be determined by Equation (7).

$$I'_{x,y}^{(G)} = \sum_{i=0}^{n-1} \alpha_i \cdot F_i, \quad (7)$$

where $\alpha \in [0, 1]$.

We have increased embedding capacity by maximum of 8 bits per pixel into two layers similar to which is the main objective of other researcher. Another objective of the work is to hide secret information on pixel intensity by three different types of figurate number system i.e., square, pentagonal and hexagonal number system which increase security also. We also analyze result between proposed three different figurate number system based embedding algorithms with triangular number based algorithm proposed in (Halder et al., 2015). Details analysis report is discussed in Section 4.

Table 1: Normalized Value of $I_{x,y}^{(G)}$	
Range of Intensity $I_{x,y}^{(G)}$	Normalize Value $I'_{x,y}^{(G)}$
0 to 19	9
20 to 41	10
42 to 71	27
72 to 89	37
90 to 109	51
110 to 131	61
132 to 161	71
162 to 181	81
182 to 201	91
202 to 223	101
224 to 247	118
248 to 255	125

3.1 First layer embedding technique

In first layer embedding, n bits of secret information is embedded by flipping n LSBs from figurate number representation of $I'_{x,y}^{(G)}$. If 4th bit value from LSB of figurate number representation (say, B_3) is 1 then 1 is appended otherwise 0 at LSB of F and consider it as F' .

Now 2nd & 3rd LSB of other intensity, (we have chosen blue intensity here say, $I_{x,y}^{(B)}$) to store the value of B_2 and B_3 and consider it to $I'_{x,y}^{(B)}$. Beside this 2nd LSB and LSB of red channel (say, $I_{x,y}^{(R)}$) is used to store the value of B_2 and B_3 and consider it to $I'_{x,y}^{(R)}$.

3.2 Second layer embedding technique

By this layer another n bits of secret information can be embed in same channel. Maximum of 8 bits secret information can be embedded after completion of both layer embedding technique.

3.3 Minimization of distortion

Distortion of stego image will increased with proportion to capacity. Though the capacity of proposed method is very high we have added an adjustment process to minimize distortion. Difference between cover and stego image can be calculated by Equation (8). We adjust stego value of green intensity (say, $I_{x,y}^{*(G)}$) by Equation (9) with respect to $\epsilon_{x,y}$.

$$\epsilon_{x,y} = I_{x,y}^{(G)} - I_{x,y}^{*(G)} \quad (8)$$

$$I_{x,y}^{*(G)} = \begin{cases} I_{x,y}^{(G)} + 15, & \text{if } \epsilon_{x,y} > 15, \text{ set } I_{x,y}^{*(G)} = \{1\} \\ I_{x,y}^{(G)} - 15, & \text{if } \epsilon_{x,y} < -15, \text{ set } I_{x,y}^{*(G)} = \{1, 0\} \\ I_{x,y}^{(G)} & \text{otherwise, set } I_{x,y}^{*(G)} = \{0\} \end{cases} \quad (9)$$

We summarize the proposed embedding process in Algorithm 1.

3.4 Extraction Algorithm

Extraction algorithm is just opposite of embedding algorithm. Details extraction algorithm is discussed in Algorithm 2.

4. EXPERIMENTAL RESULTS AND ANALYSIS

In this section we have find out the outcome of proposed methodology and make a comparison with the state-of-art technique.

We have consider five hundred 24 bit color images and three hundred 8 bit grayscale images of type cartoon, flower and text (<http://www.freepik.com>), literature of Shakespeare (<http://www.shakespeare-online.com>) for the experiment.

Input: Bit stream of secret information and cover image

Output: Stego image

- 1 Normalize $I_{x,y}^{(G)}$ as per Table 1;
- 2 Calculate n (embedding capacity) of $I_{x,y}^{(G)}$ by Equation (6);
- 3 Take any proposed figurate number system based representation F of $I_{x,y}^{(G)}$ by Equation (5);
- 4 Replace n LSB of F with equal length of secret information;
- 5 if $(9 \leq I_{x,y}^{(G)} \leq 118)$ then
- 6 Replace two LSB of $I_{x,y}^{(R)}$ with two LSB of F' and
- replace 2nd and 3rd LSB of $I_{x,y}^{(B)}$ with immediate two bits of F' ;
- end
- else
- 7 2nd LSB of $I_{x,y}^{(B)} = F_{i:i=1}$;
- 8 LSB of $I_{x,y}^{(R)} = F_{i:i=0}$;
- End
- 9 Set $I_{x,y}^{(B)} \leftarrow I_{x,y}^{(B)}$;
- 10 Set $I_{x,y}^{(R)} \leftarrow I_{x,y}^{(R)}$;
- 11 if 4th bit (from LSB) of figurate number system based representation F_3 is 1 then
- 12 Attach 1 at the LSB of binary representation of F to generate F' ;
- end
- else
- 13 Attach 0 at the LSB of binary representation of F to generate F' ;
- end
- 14 Repeat Step 1 to Step 4 once;
- 15 Set $LSB I_{x,y}^{(B)} \leftarrow LSB F'$;
- 16 Set $I_{x,y}^{(B)} \leftarrow I_{x,y}^{(B)}$;
- 17 Set $I_{x,y}^{(G)} \leftarrow I_{x,y}^{(G)}$;
- 18 Adjust value of $I_{x,y}^{(G)}$ by Equation (9);
- 19 Set $I_{x,y}^{(R)} \leftarrow I_{x,y}^{(R)}$;
- 20 Construct stego image by $I_{x,y}^{(R)}$, $I_{x,y}^{(G)}$ and $I_{x,y}^{(B)}$;

Algorithm 1: Embedding algorithm.

4.1 Analysis of Visual Distortion and Embedding Metric

Definition 6. Average Embedding Capacity (AEC) can be formulated by

$$AEC = \frac{\text{Total Bits of Secret Information}}{\text{Total Number of Image Pixels}} \quad (10)$$

Definition 7. Mean Square Error (MSE) can be formulated by

$$MSE = \frac{1}{XY} \sum_{x,y} (I(x,y) - J(x,y))^2 \quad (11)$$

Definition 8. Peak-Signal-to-Noise-Ratio (PSNR) can be formulated by

$$PSNR = 10 \log_{10} \left(\frac{I_{MAX}^2}{MSE} \right) \quad (12)$$

where I_{MAX} is highest intensity value of pixel.

Input: Stego image

Output: Secret information

- 1 Calculate n (embedding capacity) of $I_{x,y}^{(G)}$ by Equation (6);
- 2 Re-adjust $I_{x,y}^{(G)}$ by Equation (9);
- 3 Set $T \leftarrow LSB I_{x,y}^{(R)}$;
- 4 Exclude LSB of $I_{x,y}^{(G)}$;
- 5 Set $I_{x,y}^{(G)} \leftarrow I_{x,y}^{(G)}$;
- 6 if $T = 1$ then
- 7 Set $F_3 \leftarrow 1$;
- end
- else
- 8 Set $F_3 \leftarrow 0$;
- end
- 9 Take $F I_{x,y}^{(G)}$ by Equation (5) and step 6 to 8;
- 10 if $n = 8$ then
- 11 Set $M_{i:i \in \{1,2\}} \leftarrow 3^{rd} LSB \text{ and } 2^{nd} LSB \text{ of } I_{x,y}^{(B)}$;
- 12 Set $M_{i:i \in \{3,4\}} \leftarrow$
least 2 significant bits of $I_{x,y}^{(R)}$;
- 13 Set $M_{i:i \in \{5,6,7,8\}} \leftarrow$
least 4 significant bits of F ;
- end
- else
- 14 Set $M_{i:i \in 1} \leftarrow 2^{nd} LSB \text{ of } I_{x,y}^{(B)}$;
- 15 Set $M_{i:i \in 2} \leftarrow$ least significant bit of $I_{x,y}^{(R)}$;
- 16 Set $M_{i:i \in \{3,4\}} \leftarrow$ least 2 significant bits of F ;
- end
- 17 Bits stream of secret information M .

Algorithm 2: Secret information extraction algorithm.

We describe comparative analysis of AEC, PSNR of different image in Table 2. This table also describes result analysis between triangular number based embedding algorithm and proposed new different figurate number system based embedding algorithm. Here, we see the satisfactory result.

Table 2: Performance Analysis

Image Name	Dimension	AEC Triangular number Based Algorithm	ofAEC Square number Based Algorithm	ofAEC Pentagonal number Based Algorithm	ofAEC Hexagonal number Based Algorithm	ofPSNR Triangular number Based Algorithm	ofPSNR Square number Based Algorithm	ofPSNR Pentagonal number Based Algorithm	ofPSNR Hexagonal number Based Algorithm
Lena.bmp	256 × 256	8	7.8725	7.9314	7.9567	34.3596	33.1426	34.1589	34.5416
C3.bmp	280 × 210	7.9843	7.9914	7.9326	7.9419	36.2936	35.1473	36.1739	36.5147
C6.bmp	259 × 194	7.6972	7.9536	7.9423	7.9647	38.8701	36.1785	34.5541	34.6418

We also have shown the graphical representation of above table data in Figure 5.

4.2 Bitplane Analysis

We get the biplane image from the grey level image (Gutub et al., 2010). We can represent the image pixel using 8 bit plane where MSB is left most

bit plane and right most bit plane is LSB. Table 3 shows the disintegration result of cover and stego image by different figurate number and triangular number based embedding algorithm in 8 different bitplane. The outcome of these different images shows no dis-similarity between them.

Figure 5: AEC value of different stego image by different embedding algorithm

4.3 Histogram Analysis

The pictorial representation of the frequency distribution of a set of data item is termed as histogram analysis. This is used to identify the frequency differences of each color of an image. We have shown histogram analysis of proposed work in Figure 6 which shows the original and stego image are almost same to each other.

Table 3: Bitplane Analysis of Sample Baboon.bmp where 2nd and 3rd Row Showing Stego Version by Proposed Two Different Figurate Number System (Hexagonal and Pentagonal) and Stego Version by Triangular Number System at Bottom

All bit planes	bit plane 7	bit plane 6	bit plane 5	bit plane 4	bit plane 3	bit plane 2	bit plane 1	bit plane 0

All bit planes	bit plane 7	bit plane 6	bit plane 5	bit plane 4	bit plane 3	bit plane 2	bit plane 1	bit plane 0

All bit planes	bit plane 7	bit plane 6	bit plane 5	bit plane 4	bit plane 3	bit plane 2	bit plane 1	bit plane 0

All bit planes	bit plane 7	bit plane 6	bit plane 5	bit plane 4	bit plane 3	bit plane 2	bit plane 1	bit plane 0

Original Image

Stego Image by Triangular Number Series Based Algorithm

Stego Image by Square Number Series Based Algorithm

Stego Image by Hexagonal Number Series Based Algorithm

Histogram of above image

Histogram of above image

Histogram of above image

Histogram of above image

Figure 6: Sample cover image and its histogram (leftmost), stego image and its histogram by triangular number series based algorithm (2nd from left), stego image and its histogram by square number series Based Algorithm (3rd from left) and stego image and its histogram by pentagonal number series based algorithm (rightmost).

4.6 Normalized Correlation

Similarity index between stego and cover image can be measured in different ways like Sum of Squared Differences (SSD). This similarity measure gives a good result if the both images have approximately same intensities and contrast.

4.4 Chi-Square Test

We will check our proposed methodology through statistical test chi-square (χ^2) test. Using this we have shown a comparison with expectations result and actual results. The given input data set should be random, raw, and exclusive in nature. The χ^2 statistic can be described by:

$$\chi^2_{K-1} = \sum_{i=0}^n \frac{(I_i^{(G)} - I_i^{*(G)})^2}{I_i^{*(G)}} \quad (13)$$

Our experimental result shows that value of χ^2 for square, pentagonal and hexagonal number system based embedding algorithm are 8.89654, 8.8798 and 8.9514 for degree of freedom 15. This value is much higher than standard table value. Hence it can conclude that proposed method can effectively protect from different steganalysis attack.

4.5 StireMark Analysis

We have used a benchmark tool Stir Mark 4.0 to test the robustness and strength. Table IV shows satisfactory result of cover image and its stego version by different figurate number based embedding algorithm (<http://www.petitcolas.net/fabien/watermarking/stirmark>).

We have used Normalized Correlation Function (N_c) by Equation 14.

$$N_c = \frac{\sum_{i=1}^M (I_i^{(G)} \cdot I_i^{*(G)})}{\sum_{i=1}^M (I_i^{*(G)})^2} \quad (14)$$

By this method we compare cover and stego image we get all result ≈ 1 , which is satisfactory.

4.7 Universal Image Quality Index

The best way to measure the degree of structure distortion of an image is Universal Image Quality Index (UIQI) [8]. The different factors associated with Loss of Correlation, Luminance Distortion and Contrast Distortion. We have applied salt and pepper noise and we get satisfactory result with $\sigma = 0.05$.

4.8 Intransigence against Sterilization Technique

This technique put the steganographic information confined in digital image into a situation in which there is a danger of loss, harm, or failure. In comparison with the previous methodology which can test the result using only two bit from LSB of pixel intensities, this methodology works better as we are taking 8 bit (which is very high) to check the result (Paul et al., 2012; Paul et al., 2011). Hence we can conclude that this method can get rid of steganographic information confined in digital image.

Table 3: StireMark Analysis of (280 × 280) Size RGB Cover Image, Stego Version by Different Figurate Number Based Proposed Algorithm and Stego Version by Triangular Number Based Algorithm

Test Name	Factor	Cover Image	Triangular Based Algorithm	numberSquare Based Algorithm	numberPentagonal Based Algorithm	numberHexagonal Based Algorithm
Add Noise	20	7.55 dB	7.54 dB	7.51 dB	7.65 dB	7.65 dB
Median Cut	3	28.32 dB	28.22 dB	28.56 dB	28.44 dB	28.17 dB
Self Similarities	1	25.72 dB	25.67 dB	25.44 dB	25.46 dB	25.41 dB
Small Distortions	Random0.95	14.17 dB	13.21 dB	14.22 dB	13.59 dB	14.96 dB
Conv Filter	1	14.35 dB	14.33 dB	14.69 dB	14.28 dB	14.11 dB
Random Line	10	181.62	181.77	181.95	181.57	181.65
Rotation Scale	-2	13.18 dB	13.21 dB	13.66 dB	13.65 dB	13.54 dB

5. CONCLUSIONS

In this paper we have discussed proposed a comparative study between Different Types of Figurate Number Based Double Layer Image Steganography in Spatial Domain. We have proved that proposed algorithm is able to hide up to 8 bits of secret information in each pixel value of a given image in spatial domain which is very higher than available state-of-the-art work. We also focused the embedding efficiency as well as information security in this proposed work which is very satisfactory. The previous work was fully focused on embedding efficiency but information security is similarly important in this field. We have changed the embedding algorithm by implementing different types of figurate number series like square, pentagonal, hexagonal number system based algorithm and compare with triangular number system based embedding algorithm. By implementing different types of number system in embedding algorithm in random fashion, it is very difficult to predict the appropriate embedding technique by unauthorized access which results more security. Here we have prevented visual attacks, statistical attacks as-well-as the test provided by the benchmark method. Also we have shown empirical support and theoretical justification that minimize distortion and maximize embedding capacity without keeping any perceptible signature rather than available state-of-art works.

REFERENCES

- Bailey K. and Curran K., 2006. An evaluation of image based steganography methods, In Journal of Multimedia Tools and Applications, 30(1), 55-88.
- Gutub A. A., 2010. Pixel Indicator Technique for RGB Image Steganography, In Journal of Emerging Technologies in Web Intelligence, 2(1), 56-64.
- Halder P. and Mukherjee I., 2015. A novel double layered image steganography in spatial domain using triangular number system, 2015 IEEE International Conference on Research in Computational Intelligence and Communication Networks (ICRCICN), Kolkata, 411-416. Doi: 10.1109/ICRCICN.2015.7434274.
- http://www.freepik.com
- http://www.petitcolas.net/fabien/watermarking/stirmark
- http://www.shakespeare-online.com
- http://www.wikipedia.org
- Kejgir S. and Kokare M., 2009. Optimization of Bit Plane Combination for Efficient Digital Image Watermarking, In International Journal of Computer Science and Information Security (IJCSIS), 4.
- Manes N., Zimeras K., Georgiakodis S., and F. 2012. Data Hiding Techniques in Steganography Using Fibonacci and Catalan Numbers, 9-th International Conference on Information Technology: New Generations (ITNG), 392-396.
- Paul G. and Mukherjee I., 2011. Double Bit Sterilization of Stego-images, In Proceedings of the 10-th International Conference on Security and Management (SAM), Las Vegas, U.S.A., 743-746, ISBN: 1-60132-196-1.
- Paul G. and Mukherjee I., 2012. Sterilization of Stego-images through Histogram Normalization, 11-th International Conference on Security and Management (SAM), Las Vegas, U.S.A., 448- 454, ISBN: 1-60132-230-5.
- Paul G., Davidson I., Mukherjee I. and Ravi S. S., 2012. Keyless Steganography in Spatial Domain using Energetic Pixels, In Proceedings of the 8-th International Conference on Information Systems Security (ICISS), IIT-Guwahati, India, 134-148, 7671, LNCS, Springer Verlag.
- Wang Z. and Bovik A. C., 2002. A Universal Image Quality Index, In IEEE Signal Processing Letters, 20.
- Zhang X., Wang S. and Zhou Z., 2008. Multibit Assignment Steganography in Palette Images, In IEEE Signal Processing Letters, 15.