# A novel Approach of Steganography using Bit plane Slicing and Catalan-Lucas Number Sequence

Mrs. ShilpaPund-Dange
Assist. Professor, Department of Computer Science,
Modern College, Shivajinagar, Pune-5.
*Email Id:shilpashlok24@gmail.com*
Phone number:992388532

Dr. Chitra G Desai
Professor and Head, Department of Computer Science
NDA, Khadakwasla, Pune, India
*Email Id: chitragdesai@gmail.com*
Phone number:9422202272

***Abstract*—** This paper represents a novel approach of steganography using ModifiedSteganographic algorithm with Catalan-Lucas Series. In this algorithm,Catalan Lucas number sequence represents each RBG component of the image by 16 bits instead of 8 bits. By applying Bit Plane Slicing technique, the cover image is sliced into 48 virtual planes and the message to be hidden is also sliced into 16 virtual planes. These 16 planes of the secret message are hidden into some of the 48 virtual planes of the cover image using the proposed algorithm. This process generates three keys at the sender which are required to extract the message from the stego image at the receiver. This method provides high data security and hiding capacity. The experimental results and the PSNR values are also discussed with the advantages from the security perspective.

**Keywords**— *Catalan, Lucas, Slicing, Spatial, Steganography,Zeckendorf.*

*****

## I. INTRODUCTION

Security of data is a very important issue nowadays. The aim of steganography is to hide the secret message inside a digital cover like image,text,audio,video etc. such that it is notperceptible to the human eye. Steganography has been used in various forms since 2500years [12]. In the Digital era, with the increase in computer power, the development of digital signal processing, coding theory and information theory, steganography turns into digital[1].This paper focuses on image Steganography. In order to make the technique more secure and less predictable, a new set of virtual bit planes are generated using pixel value decomposition and message bits are embedded in this bit planes.

## II. DIFFERENT STEGANOGRAPHIC PROTOCOLS:

There are basically three types of steganographic protocols [10, 11]:

1) Pure key steganography: There is no need to exchange any stego key in this method. It is the simplest, but the most unsecured method for secret communication.

2) Secret key steganography: In Secret key Steganography, the receiver needs a secret key for data extraction.

3) Public key steganography: In this type, two keys are required; one is a publickey used for embedding a message while another is the private key which is used for extracting a message.

The proposed algorithm follows Secret key Image Steganography. Image steganography can be carried out by two techniques: 1.TransformDomain 2. Spatial Domain. The paper focuses on Spatial Domain Technique.

## III. BIT PLANE SLICING

An RGB colorimage is a$M \times N \times 3$ array of the color pixel. A pixel intensity value is a decimal number. Each color pixel is a triplet corresponding to red, green and blue colorcomponents [5].If the RGB image is of class unit8 then the range of intensityvalue is [0-255]. The number of bits used to represent the pixel values of the components determines the bit depth of the image. If each component of the image takes 8-bits means the bit depth of the image is 24[9]. A **bit plane**[4,11] of an image is a set ofbitscorresponding to a given bit position in each binary number. It is the contribution of the specific bit to make the total appearance of the image. If the image is composed of 8 bits/pixel, then the $0^{th}$order LSB of all the pixelsare extracted as plane 0 and the $7^{th}$ order MSB of all the pixelsare extracted as plane 7. LSB planes of an image have theleast participation in the perceptibility of the image. MSB bit planes play animportant role in the perceptibility of the image. In the proposed method, among 16 bits/pixel the first order MSB (left to right) of all the pixels are extracted as plane 1 and $16^{th}$ order LSB of all the pixels are extracted as plane 16.

## IV. MATHEMATICAL FOUNDATION BEHIND STEGANOGRAPHY

The proposed algorithm uses a combination of Lucas number sequence and Catalan number sequence for pixel value decomposition and representation.

### *A. Lucas number Sequence [13,15]*

$$L_n = \begin{cases} 2 & n = 0 \\ 1 & n = 1 \\ L_{n-1} + L_{n-2} & n>1 \end{cases}$$

$L_{(12)}$= 199, 123, 76, 47, 29, 18,
$L_{12}$ $L_{11}$ $L_{10}$ $L_9$ $L_8$ $L_7$

11 7,4, 3, 2, 1
$L_6$ $L_5$ $L_4$ $L_3$ $L_2$ $L_1$

*B. Catalan number sequence[3,15]*

$$C_n = \frac{(2n)!}{(n+1)!\,n!}$$

$C_{(6)}$= 132, 42, 14, 5,2, 1
$C_6$ $C_5$ $C_4$ $C_3$ $C_2$ $C_1$

*C. An extension of Zeckendorf's Theorem [7,15]*

Let $(a_n)_{n\in N^*}$ be a strictly increasing sequence of positive integers, with $a_1$= 1, $a_2$= 2 and $a_n + a_{n+1} \geq a_{n+2}$and $n \in N^*$.Then every positive integer$x$ with $a_n \leq x < a_{n+1}$,$n \in N^*$, can be uniquely represented as a sum of distinct, nonconsecutive terms of sequence $(a_n)$, with the restriction that the term$a_n$ appears in the sum.

Each pixel has an integer value *x* on the close interval [0-255] , can be represented as a sum of distinct nonconsecutive terms, we only need few term for encoding. It's clear from the Catalan series that every integer in the range [0-255] cannot be represented as a sum of distinct Catalan numbers. Hence the union two sets i.e. Catalan and Lucas is taken as -

CL= $C_{(6)}$U $L_{(12)}$

= 199, 132, 123, 76, 47, 42, 29,
$CL_{16}$ $CL_{15}$ $CL_{14}$ $CL_{13}$ $CL_{12}$ $CL_{11}$ $CL_{10}$

18, 14, 11, 7,5, 4, 3,2 1
$CL_9$ $CL_8$ $CL_7$ $CL_6$ $CL_5$ $CL_4$ $CL_3$ $CL_2$ $CL_1$.

Here we get 16 bit representation and 16 virtual planes.
E.g.234 is represented as 1000001000010001.
120 is represented as 0001010000000010.
Each pixel consists of three components which are R,G and B . So each intensity value of R, G, B is represented by 16 bits. Hence by using Catalan-Lucas Sequence method, each pixel is converted into 48 bit and ultimately 48 bit planes.

## 4. Modified Steganographic algorithm using Catalan-Lucas Series [14]

**Declaration:** $M \times N$: Size of the cover image.
$L$ : Length of Payload

**Embedding (Input: Cover Image, Payload file) :**

1. Read an RGB image as a cover image.
2. Separate the R, G and B component of the cover image as $C_r$, $C_g$and $C_b$.
3. Apply Catalan-Lucas series algorithm (CL series algorithm) for converting a decimal number into a 16-bit binary number.
4. Each array $C_r$, $C_g$ and $C_b$is sliced into 16 bit planes.
5. Read the file which is to be embedded say Payload.
6. Convert each character of the payload into its ASCII equivalent which forms a1-dimentional array of size$L$. Transform it into $P[M,N]$ array. Apply padding by 0s to $P[M,N]$ if necessary.
7. Apply CL series algorithm on $P[M,N]$ and store in $PL[16,M,N]$.
8. Array $PL$ is sliced into 16 bit planes.
9. Embedding Process

a) First, six planes of $PL(P1,\ldots,P6)$ are X-ORed with mid-level bit planes $(C_{r5,\ldots\ldots,}C_{r10})$ and the result is stored in the low-level bit planes $(C_{r11\ldots\ldots}C_{r16})$ for $C_r$.
b) Next six planes of $PL(P7,\ldots,P12)$ are X-ORed with mid-level bit planes $(C_{g5,\ldots\ldots,}C_{g10})$and the result is stored in the low-level bit planes $(C_{g11,\ldots\ldots,}C_{g16})$ for $C_g$.
**c)** Last four planes of $PL(P13,\ldots,P16)$ are X-ORed with mid-level bit planes $(C_{g9\ldots\ldots}C_{g12})$ and the result is stored in the low-level bit planes $(C_{b1\ldots\ldots}C_{b16})$ for $C_b$ .

10. Construction of StegoImage:
a) R,G and B components of the required image are constructed using high-level bit planes $(C_{r1\ldots.}C_{r4})$,mid-level bit planes $(C_{r5\ldots\ldots}C_{r10})$ with no change and the modified low-level bit planes $(C_{r11\ldots.}C_{r16}) = K1$ ,$(C_{g11\ldots\ldots}C_{g16}) = K2$ and $(C_{b13\ldots}C_{r16}) = K3$ where $K1, K2, K3$ formed the keys for R, G, and B planes respectively.
b)Convert the image into decimal form by merging RGB components by applying by summing up the place values.
11. Send the stego image and the keys $K1, K2, K3$ so formed to the receiver.

**Extraction ( Input: Stego Image, Keys $K1, K2, K3$ ) [14]**

1. Read aRGBstego image.
2. Separate the R, G and B component of thestego imageas $C_r$, $C_g$ and $C_b$.
3. Apply CL series algorithm.
4. Each array$C_r$, $C_g$ and $C_b$ is sliced into 16 bit planes.
5. Accept $K1, K2$ *and* $K3$ keys from a sender for extraction of payload.
6. The payload bit planes are recovered by X-ORing the respective bit planes of each component.
7. Recover the payload by combining bit planes so obtained.
8. Convert the binary values into a decimal bysumming up the place values.
9. The payload is obtained from the stego image.

### A. *An algorithm for converting a decimal number into a 16-bit binary number using Catalan-Lucas Series and Zeckendrof's Theorem.[15]*

**Declaration: Consider** a series of the union of Catalan and Lucas number sequence
$p$=[199 132 123 76 47 42 29 18 14 11 7 5 4 3 2 1]. It's an array of 16 decimal numbers.

1. Declare an array of 16 elements say *ARY*, initialize all its elements to zeros.
2. Accept number '$n$' which is to be converted into 16 bit binary.
3. Find out the number in array $p$ which is greater than orequal to $n$. Say it is $F_n$.
4. If n is equal to $F_n$, then find out the array index of the position of $F_n$ and convert bit 0 to 1 on that respective position of array *ARY*.
5. If n is less than $F_n$, then find out the array index of the position of $(F_{n-1})$ and convert bit 0 to 1 on that respective position of array *ARY*and perform$n = n - (F_{n-1})$.
6. Go to Step 3 and continue up to $n = 0$.

## V. OBSERVATIONS:

1) For Steganography module, the size of the message which is successfully encrypted and decrypted depends on the dimensions (row×column) of the cover image. The length of the message to be encrypted must be less than or equal to the image size (row×column). Depending on the image size the computation efforts are increased.

2) If message is represented in 16 bits, embedding of 16 message planes take place as -

In R plane, 6 message planes are embedded.

In G plane, 6messageplanes are embedded.

In B plane, 4 message planes are embedded.

Each and every pixel is used for embedding. Hence the embedding capacity is high.

3) If message is represented in 8-bit binary system, we can hide two message files simultaneously by embedding the data in the image planes as -

For I$^{st}$ File

In R-plane, 4 message planesare embedded

In G-plane,2 message planesare embedded

In B-plane, 2 message planes are embedded

For II$^{nd}$ File

In R-plane, 2 messageplanesareembedded.

In G-plane,4 message planes are embedded.

In B-plane, 2 message planes areembedded.

Separate keys are required for extraction of each file which doubles the embedding rate.

4) PSNR is often expressed on a logarithmic scale in decibel (dB). PSNR value greater than or equal to 30dB is hard to detect by the human eye [2]. PSNR value below 30 dB indicates a fairly low quality. The details about thesize ofpayload, size of a cover image and PSNRvalues are given in the table below:

TABLE I. Details of the Payload size, Cover image size and PSNR values.

| Size of Payload File | No.of Characters in a file | Sizeof cover Image | No. of pixels of a cover image | Size of stego image | PSNR (dB) |
|---|---|---|---|---|---|
| 14.3 KB | 14662 | 121 KB | 41616 | 121 KB | 38.64 |
| 48 KB | 49575 | 148 KB | 50544 | 148 KB | 39.1 |
| 14.3 KB | 14662 | 192 KB | 65536 | 192 KB | 39.74 |
| 87 KB | 89126 | 768 KB | 262144 | 768 KB | 41.00 |
| 118 KB | 121394 | 768 KB | 262144 | 768 KB | 41.66 |
| 125 KB | 128499 | 768 KB | 262144 | 768 KB | 40.33 |

5)If the message to be embedded is very large, it needs a large size cover image for embedding which increases the computation efforts.

6) For Steganography module, BMP images with variant intensity are most suitable. It can workfor JPEG and PNG images also with acceptable PSNR but the size of the image get changed.

Hence, a proposed novel approach of Steganography using Bit plane slicing and Catalan-Lucas number Sequence is more efficient for data hiding. It gives the hiding capacity of 16-bits per pixel.

## VI. ADVANTAGES OF NEWLY PROPOSED STEGANOGRAPHY MODEL FROM SECURITY PERSPECTIVE

1. Generally, an image is represented in 8 bit, in the proposed system; it is represented in 16 bits. The hacker is not aware of this.
2. A number represented using Famous number sequence is well known.But the combination of Catalan series and Lucas series is used in the proposed method.
3. Among 16 planes, data is embedded in few planes,it increases the ambiguity, which makes it difficult for the hacker to detect the exact planes.
4. Every time the key generated is payload dependent. If the key is compromised it's not useful for another payload (message).
5. As every pixel is participated for embedding, it increases the embedding capacity. It's 16 bits/pixel.
6. Three keys K1, K2 and K3 are generated. So unless the hacker knows all the keys, extraction is not possible.
7. The proposed technique is best suitable for .bmp with variant intensity images because the size of the image remains unchanged even after converting it into 16 bits.
8. There is no need of a cover image to recover the payload.
9.It gives PSNR value more than 30 dB. Hence, the distortion of the image is not perceptible.

## VII.CONCLUSION

This paper presents a novel Approach of Steganography using Bit plane slicing and Catalan Lucas number Sequence. The experiments are carried out on Intel(R) Core i5 -2410 M CPU with 6144 MB RAMS, on Matlab R2015a. The experimental study shows that it yields better PSNR value and higher embedding capacity. Thissteganographicalgorithm is more suitable for the BMP imageshaving bit depth 24. As the resulting stego image is having the same size as that of the cover image, it nullifies the chance of detection of hidden information. The method provides many inherent security features.

## REFERENCES

[1] Abbas Cheddad," Steganoflage: A New Image Steganography Algorithm," Ph.D. dissertation, University of Ulster School of Computing & Intelligent Systems,Faculty of Computing & Engineering, 2009.

[2] Chakraborty, S., Jalal, A.S. andBhatnagar, "An efficient bit plane X-ORing algorithm for irreversible image steganography', Int. Journal of trust management in computing and communications. (2012).

[3] D. Sravana Kumar, C H. Suneetha, A. Chandrasekhar," Novel Encryption Schemes Based on Catalan Numbers", International Journal of Engineering Research and Applications (IJERA) ISSN: 2248-9622 www.ijera.com Vol. 2, Issue 2,Mar-Apr 2012, pp.161-166.

[4] GwanggilJeon, "Watermarking Application Using Bit Plane Allocation",International Journal of Security and Its Applications Vol.8, No.5 (2014), pp.139-148 http://dx.doi.org/10.14257/ijsia

[5] J.R. Krenn," Steganography and Steganalysis", http://www.krenn.nl/univ/cry/steg, Jan,2004.

[6] Matlab , R2015a, Mathworks.

[7] N.Aroukatos, K Manes, S. Zimeras and F. Georgiakodis, "Technique in Image Steganography using Famous Number Sequence " International Journal of Advanced Computer Science, Jan 2015.

[8] Pratiksha Kale, Prof. MahipBartere: A Survey On Image Steganography Technique, International Journal of Pure and Applied Research in Engineering and Technology, Vol.3 (9) pp143-152, March 2015.

[9] Rafael C. Gonzalez, Richard E. Woods and Steven L. Eddins., Digital Image Processing.

[10] S.G.K.D.N. Samaratunge, (August 2007): New Steganography Technique for Palette Based Images, Second International Conference on Industrial and Information Systems, ICIIS 2007.

[11] ShrikantKhaire," Review: Steganography – Bit Plane Complexity Segmentation (BPCS)Technique" International Journal of Engineering Science and Technology Vol. 2(9), 2010, 4860-4868.

[12] "Steganography:Past,Present,Future",https://www.sans.org/reading_room/whitepapers/stenganography/steganography-past-present-future-552 , 2001.

[13] "The First 200 Lucas numbers and their factors", http://www.maths.surrey.ac.uk/hostedsites/R.Knott/Fibonacci/lucas200.html.

[14] ShilpaPund-Dange, Chitra G Desai, "Data Hiding Technique using Catalan-Lucas Number Sequence", International Journal of Science and Technology, Volume 10, Issue 4, January 2017.

[15] ShilpaPund-Dange, Chitra G Desai, "Comparison of Steganography technique using 8-bit binary representation and Catalan-Lucas representation" International Journal of Innovative Computer Science and Engineering, Volume-4, Issue-1,Jan-Feb 2017.

https://www.instamojo.com/resolutioncenter/cases/C862797581