Indian Journal of Science and Technology, *Vol 10(4), DOI: 10.17485/ijst/2017/v10i4/110896, January 2017*
ISSN (Print) : 0974-6846
ISSN (Online) : 0974-5645

Data Hiding Technique using Catalan-Lucas Number Sequence

Shilpa Pund-Dange[1] and Chitra G. Desai[2]*

[1]Department of Computer Science, SPPU, Pune - 411007, Maharashtra, India
[2]Department of Computer Science, NDA, Khadakwasla, Pune - 411023, Maharastra, India; chitragdesai@gmail.com

Abstract

In this paper, a novel data hiding technique is proposed which is an improvement over an existing data hiding techniques. Generally, a pixel intensity value of an image is represented by 8-bit binary sequence. In the proposed technique, a pixel is represented by using 16-bit Catalan Lucas sequence. By using bit plane slicing, 16 virtual planes are generated for each R, G and B component respectively. This paper introduces a new approach for hiding data within few bit planes among 48. Data means a secret message is also decomposed into 16 bits to get 16 bit planes. First 6 bit planes of the secret message are embedded into the middle planes of R using XOR operation and the result is stored in LSB planes of R. Next 6 bit planes of the secret message embed similarly within G plane. The last 4 planes are embedded into the middle planes of B using XOR operation and the result is stored in LSB planes of B. Three keys are generated in the embedding phase. Extraction is carried out by using keys in a reverse way by XO Ring the respective bit planes. This method greatly increases the security as a secret key is known to the authentic user only. The hiding capacity is 16 bits/pixel with the acceptable PSNR value.

Keywords: Catalan, Lucas, Steganography, Stego Image, Zeckendorf's Theorem

1. Introduction

In recent years, the security and confidentiality of sensitive data have become very important due to the fast growth of internet and communication technologies. Therefore, how to protect private data from the unauthenticated user during transmission, become an important issue nowadays. In Object Oriented Programming, the term data hiding also called as data encapsulation means hiding the implementation details of the class from the user. In terms of steganography, data hiding is to hide a secret message in a cover media like text, images, audio, video, protocol[6] in such a way that no any intruder will be able to notice it. A traditional method of representation of the image's pixel intensity value is 8 bit-binary. To increase the hiding capacity, different techniques have emerged. First pixel decomposition technique after binary is Fibonacci Technique where each pixel is represented by 12 bit and hence 12 virtual planes are generated [9]. The next decomposition technique used is the prime number sequence[13] where each pixel is represented by 15 bit and hence 15virtual planes are generated. In Natural number sequence[12], each pixel is represented by 23 bit and hence 23 virtual planes are generated. The combination of Fibonacci and Catalan sequence[11], each pixel is represented by 15 bit and hence 15 virtual planes are generated. Lucas number sequence[8], each pixel is represented by 12 bit and hence 12 virtual planes are generated. Here, we are using a combination of Catalan and Lucas sequence [3] each pixel is represented by 16 bit and hence 16 virtual planes are generated. In all the above methods which use number sequences, all pixels do not participate in the embedding process[8]. Therefore the hiding capacity is less. In the proposed method, since all pixels have participated in the embedding process the hiding capacity is high.

*Author for correspondence

2. Catalan-Lucas based Decomposition

2.1 Lucas Number Sequence

Lucas Number Sequence is discovered by a French mathematician Edouard Lucas, in the 1870s while studying the Linear Recursive Sequences. For Fibonacci sequence the initial conditions are $F_0 = 0, F_1 = 1$. But for Lucas Sequence starts with $F_0 = 2, F_1 = 1$[15].

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

e.g. .....15127, 9349, 5778, 3571, 2207 1364 843, 521, 322,199, 123, 76, 47, 29,18,11,7,4,3,1,2.

2.2. Catalan Number Sequence

Catalan numbers[2] were discovered by Eugene C. Catalan, Belgian mathematician in 1838. Catalan numbers are sequence of natural numbers. The Catalan number C_n is defined as

$$C_n = \frac{(2n)!}{(n+1)!n!} \qquad n \in N^*$$

e.g. 1430, 429, 132, 42, 14,5,2,1

Fibonacci, Lucas, Catalan sequences are frequently used in Combinatorics also called as combinational mathematics.

2.3. An Extension of Zeckendorf's Theorem

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[3,6,7,12].

According to Zeckendorf's theorem[10], every positive integer is uniquely represented as a sum of distinct Fibonacci numbers without consecutive 1s. It was first discovered by Eduourd Zeckendorf in 1939[12] which were applied for many number sequences.

Each pixel has an integer value x on the close interval [0-255], so required only a few term for encoding.

$L_{(12)}$ = 199,123,76,47,29,18,11,7,4,3,2,1

$C_{(6)}$ = 132,42,14,5,2,1

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 -

$CL = C_{(6)} \cup L_{(12)}$

= { 199,132,123,76,47,42,29,18,14,11,7,5,4,3,2,1}

Here we get 16 bit representation and 16 virtual planes.

E.g. 120 is represented as 0001010000000010

3. Modified Stegano Graphic Algorithm using Catalan-Lucas Series

3.1 Embedding Algorithm

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 Red, Green and Blue component[5] of the cover image as C_r, C_g and C_b.

3. Apply Catalan-Lucas series algorithm (CL series algorithm using Zeckendrof's Theorem) 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 text file which is to be embedded say Payload.

6. Convert each character of the payload into its ASCII equivalent which forms a 1-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 middle-level bit planes $(C_{r5} \ldots\ldots C_{r10})$ and the result is stored in the lower-level bit planes $(C_{r11} \ldots\ldots C_{r16})$ for C_r.

b) Similarly, next six planes of $PL(P7 \ldots . P12)$ are X-ORed with $(C_{g5} \ldots\ldots C_{g10})$ and the result is stored in $(C_{g11} \ldots\ldots C_{g16})$ for C_g.

c) Last four planes of $PL(P13 \ldots . P16)$ are X-ORed with $(C_{b9} \ldots\ldots C_{b12})$ and the result is stored in $(C_{b13} \ldots\ldots C_{b16})$ for C_b.

10. Construction of Stego Image:

a) R, G and B components of the required image are constructed using bit planes $(C_{r1} \ldots\ldots C_{r4})$, $(C_{r5} \ldots\ldots C_{r10})$ with no change and the modified lower-level bit planes $(C_{r11} \ldots\ldots C_{r16}) = K1$, $(C_{g11} \ldots\ldots C_{g16}) = K2$ 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 and summing up the place values.

11. Send the stego image and the stego keys $K1, K2, K3$ so formed to the receiver.

3.2. Extraction Algorithm

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

1. Read an RGB stego image

2. Separate the R, G and B[5] component of the stego image as 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 extracted 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 by **summing up the place values.**

9. The payload is obtained from the stego image.

3.3. An Algorithm for Converting a Decimal Number into a 16-bit Binary Number using Zeckendrof's Theorem

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 or equal 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 $n = 0$.

4. Steganography Model

A pictorial representation of the Steganography model is depicted in the following figure.

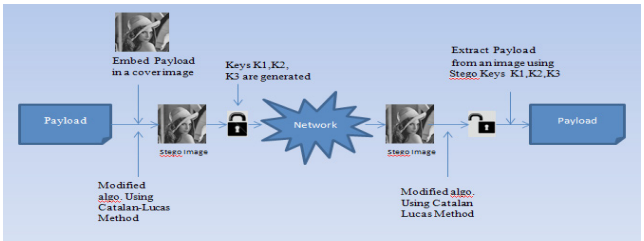

Figure 1. Steganography Model.

The execution steps of the model are as follows:

A Sender Side

1) Read the payload file.

2) Read the cover image.

3) Apply embedding module of the Modified steganographic algorithm using Catalan-Lucas series to embed the payload into an innocent image to get the Stego image.

4) Three keys are generated while embedding.

5) Can Pass the Stego image over the network in an insecure channel.

6) Pass the Stego keys to the receiver over the network on a secure channel.

A Receiver Side

1) Accept the Stego Image.

2) Accept the Stego Keys.

3) Apply extraction module of the Modified Steganographic Algorithm using Catalan-Lucas Series to extract payload from the stego image with the help of Stego Keys. Following figures explain the different states of the model:

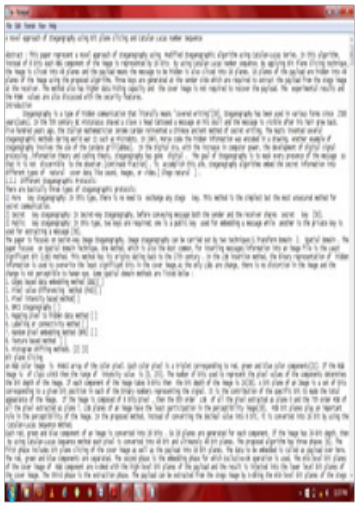

Figure 2. Payload File (118 KB).

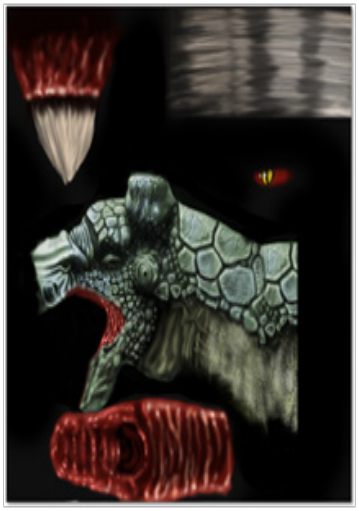

Figure 3. Cover Image(768 KB).

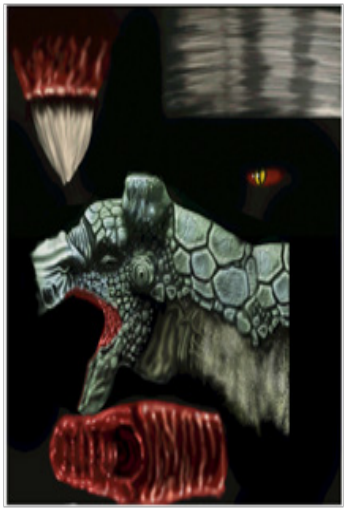

Figure 4. Stego Image (PSNR 41.66).

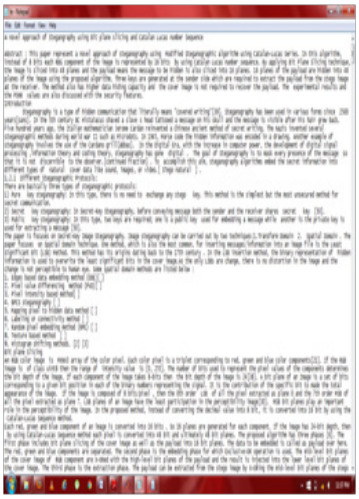

Figure 5. Extracted Payload File

5. Performance Measure

The size of the file successfully encrypted and decrypted depends on the cover image dimensions (row × column). The length of the message in a file to be encrypted must be less than or equal to the image size (row × column). Depending on the image size the computation efforts are increases. PSNR is often expressed on a logarithmic scale in decibels dB which works as countermeasures for Data Hiding. PSNR value greater than or equal to 30dB is hard to detect by the human eyes[3]. PSNR value below 30 dB indicates a fairly low quality. The PSNR values of the stego images are given in the table below.

The selection of the cover image depends on the payload. More the payload, bigger image is required for embedding the payload which increases the computation efforts.

6. Conclusion

A modified stegano graphic algorithm using Catalan-Lucas series presents in this paper provides high security by generating three keys K1, K2 and K3. So unless the hacker knows all the keys, extraction is not possible. Every time the key generated is payload dependent. If the key compromised, it is not useful for another payload (message). It provides very high hiding capacity of 16 bits/pixel. The number of characters of a secret message to be embedded must be less than or equal to the image size (row × column). BMP images with variant intensity are most suitable for this work. It works for JPEG and

Table 1. Observations about the payload, cover image size, PSNR and Time

Payload File	Size of payload (KB)	No. of Characters in a file	Size of cover Image (KB)	No. of pixels of a cover image	Size of stego image (KB)	PSNR (Db)	Time for generating the stego image (seconds)	Time for Extraction (seconds)
texts.txt	14.3	14662	121	41616	121	38.64	22.01	24.72
exp.txt	48	49575	148	50544	148	39.1	28	35
texts.txt	14.3	14662	192	65536	192	39.74	31.33	36.53
x.txt	87	89126	768	262144	768	41.00	105	135
My.txt	118	121394	768	262144	768	41.66	108	139
Myd.txt	125	128499	768	262144	768	40.33	112	146

Table 2. Comparison of the payload size and cover image

Sr. No	Size of Payload file	Size Cover image	PSNR of the Stego image (dB)
1.	35.7 KB	Leena.bmp(192KB)	40.00
2.	54.7 KB	Leena.bmp(192KB)	46.66
3.	68.1 KB	Leena.bmp(192 KB) Can't fit into this image	----------
4	87.0 KB	Leena.bmp(192 KB) Can't fit into this image	----------
5.	112 KB	Leena.bmp(192 KB) Can't fit into this image	----------
6.	68.1 KB	Head4.bmp(768 KB)	40.66
7.	87.0 KB	Head4.bmp(768 KB)	41.00
8.	112 KB	Head4.bmp(768 KB)	41.00

PNG images also with acceptable PSNR but the size of the image gets change. There is no need of a cover image to recover the payload.

7. Future Scope

Modified Stegano graphic algorithm using Catalan-Lucas Series fulfilled the requirements of the applications where high data security is important irrespective of the processing cost.

8. References

1. Chakraborty S, Jalal AS, Bhatnagar. An efficient bit plane X-O Ring algorithm for irreversible image steganography, International Journal of Trust Management in computing and communications .2012.
2. Sravana Kumar D, Suneetha C.H ,Chandrasekhar A. Novel Encryption Schemes Based on Catalan Numbers, International Journal of Engineering Research and Applications (IJERA) ISSN: 2248-9622 www.ijera.com 2012 Mar-Apr ;2(2):161–166.
3. Aroukatos N, Manes K, Zimeras S, Georgiakodis D. Technique in Image Steganography using Famous Number Sequence. International Journal of Advanced Computer Science. 2015 Jan.
4. Sandipan D, Ajith A, Bijoy B, Sugata S. Data Hiding Techniques Using Prime and Natural Numbers. Journal of Digital Information Management. 2008 December: 6(6).
5. Kekre H . B, Halarnkar P , Tanuja Sarode . Three novel chaotic polynomials for image encryption using three different MOD operators, Computational Intelligence in Industrial Application. Proceedings of the 2014 Pacific-Asia Workshop on Computer Science in Industrial Application, CIIA, Singapore; Chapter 45, December 8-9.2014.
6. Nikolaos G. Aroukatos_, Kostas Mane, Stelios Zimeras, Social Networks Medical Image Steganography Using Sub-Fibonacci Sequences, mHealth Ecosystems and Social Networks in Healthcare, Chapter 13. Spinger International Publishing ;Switzerland: 2016.

7. Stephen K. Representing Numbers Using Fibonacci Variants, The Mathematics of Various Entertaining Subjects: Research in Recreational Math, Lucas Jennifer Beineke and Jason Rosenhouse, Editor, Chapter 17,2015.
8. Alan Anwer Abdulla , Harin Sellahewa, Sabah A. Jassim . Steganography based on pixel intensity value decomposition. Mobile Multimedia/Image Processing, Security and Applications. 2014
9. Diego De Luca Picione , Federica Battisti , Marco Carli ,Jaakko Astola, Karen Egiazarian. A Fibonacci LSB Data Hiding Technique,14th European Signal Processing Conference (EUSIPCO 2006), Florence, Italy. Sept 2006.
10. Yacoub M , Saoudi A. Recurrent Neural Networks and Fibonacci Numeration System, Proceedings of 1993 International Joint Conference on Neural Networks. 1993
11. Nikolaos Aroukatos, Kostas Manes, Stelios Zimeras, Fotis Georgiakodis. Data Hiding Techniques in Steganography using Fibonacci and Catalan numbers, Ninth International Conference on Information Technology - New Generations.2012.
12. Sandipan D, Ajith A, Sugata S. An LSB Data Hiding Technique Using Natural Numbers, IEEE Third International Conference on Intelligent Information Hiding and Multimedia Signal Processing, IIHMSP 2007, Nov 26–28, Kaohsiung City, Taiwan, IEEE Computer Society press, USA, ISBN 0-7695- 2994-1, 2007.P.473–76,
13. Sandipan D, Ajith A, Sugata S. An LSB Data Hiding Technique Using Prime Numbers, The Third International Symposium on Information Assurance and Security, Manchester, UK, IEEE CS press;2007.
14. Sandeep Rathor, Soumendu Chakraborty, Tripathi S.P, Jalal A. S. A payload distribution method for high capacity image steganography, 2013 4th International Conference on Communication Technology (ICCCT). 2013.
15. The First 200 Lucas numbers and their factors. [updated 2 April 2008]. Avaiable from: http://www.maths.surrey.ac.uk/hosted-sites/R.Knott/Fibonacci/lucas200.html