STM JOURNALS

Research & Reviews:
Discrete Mathematical Structures

ISSN: 2394-1979
Volume 11, Issue 3, 2024
September–December
DOI Journal: 10.37591/RRDMS

https://journals.stmjournals.com/rrdms

Research RRDMS

Encoding-Decoding Algorithm Using the Catalan Transform of Weighted Tribonacci Sequence

Girma Wondale Gelagay[1], Zerfie Teshome Yigzie[2], Bahar Kuloğlu[3,*]

Abstract

In order to improve information security, this paper presents a unique algorithm for encoding and decoding messages utilizing the Catalan Transform of a Weighted Tribonacci Sequence. Utilizing the Catalan and Tribonacci sequences, the methodology combines the concepts of number theory and combinatorics to create an effective encryption and decryption process. First, an array is created by mapping each character in the plaintext message to its corresponding ASCII value. The ASCII-weighted Tribonacci sequence is then obtained by first generating a similar Tribonacci sequence. The weighted Tribonacci sequence is encrypted by performing the Catalan transform, which results in an encrypted message array. In order to recover the plaintext, the decryption method uses the inverse Catalan transform to recreate the original ASCII values. The algorithm's use is demonstrated by encrypting and decrypting the message "CODING" as an example. The method's mathematical rigor is demonstrated by the computational steps that generate Catalan numbers, Tribonacci numbers, and their transformations. By changing the k-value, the algorithm's versatility can be extended to k-Fibonacci sequences, providing more complexity and security. By fusing the structural characteristics of the Tribonacci and Catalan sequences, the method offers a fresh take on encryption methods. Results indicate that the suggested technique can improve secure communication in a number of applications, especially in settings where strong data security is required.

Keywords: Catalan transform, inverse Catalan transform, Tribonacci sequence, weighted Tribonacci sequence

INTRODUCTION

Owing to the growing demand for networking services, enhancing the performance and security of information systems has become crucial [1]. Encryption, which relies on coding and decoding theories, has led to the development of numerous algorithms that utilize different number systems. For example, Kuloglu et al. developed encryption and decryption algorithms using Pell and Jacobsthal numbers [2]. In contrast, others have employed approaches such as the Stakhov-Cassini formula for Fibonacci matrices [3], Prasad's Lucas P-numbers [4], and Sangeetha and Anupreethi's centered hexagonal numbers [5]. In addition, Kuloglu and Ozkan explored Fibonacci polynomials and matrices for cryptographic purposes [6, 7].

***Author for Correspondence**
Bahar Kuloğlu
E-mail: bkuloglu@sivas.edu.tr

[1]Assistant Professor, Department of Engineering Basic Sciences, Sivas University of Science and Technology, Sivas, Türkiye
[2,3]Assistant Professor, Department of Mathematics, Debre Tabor University, Ethiopia

Received Date: December 19, 2024
Accepted Date: December 30, 2024
Published Date: January 10, 2025

Citation: Girma Wondale Gelagay, Zerfie Teshome Yigzie, Bahar Kuloğlu. Encoding-Decoding Algorithm Using the Catalan Transform of Weighted Tribonacci Sequence. Research & Reviews: Discrete Mathematical Structures. 2024; 11(3): 12–16p.

Classical Fibonacci numbers, the Pell equation, and Tribonacci numbers have become prominent research topics. Transformations of these number systems, such as the Laplace transform, wavelet transform, and integral transform, have been effectively applied to encode and decode messages. For instance, Mudiyanselage and Ekanayake [8, 9, 10] employed the Laplace transform for message encryption and decryption, whereas Parthasarathy

and Srinivasan [11] utilized the wavelet transform to create efficient cryptographic techniques. Similarly, Mansour et al. developed encryption algorithms using the SEE integral transform, and Barry [12] explored the Catalan transform and its inverse in text encryption.

The American Standard Code for Information Interchange (ASCII) presents a standard-coded character set for information interchange among information processing systems, communication systems, and associated equipment. The following Table 1 is an ASCII representation of the English alphabet [13, 14]. Building on this foundation, we propose a coding-decoding algorithm based on the Catalan transform of the weighted Tribonacci sequence.

This paper is organized into three sections. Section 1 introduces the topic, reviews the relevant literature on encryption algorithms, and establishes the perseverance of the paper. In Section 2, we present background information that helps us to understand the research context and provide the main discussion of encryption and decryption algorithms using the weighted Catalan transform with an illustrative example.

MAIN RESULTS

For any positive real number k, the k-Fibonacci sequence, that is, $\{F_{k,n}\}_{n\in N}$is defined recurrently by

$$F_{k,n+1} = kF_{k,n} + F_{k,n-1}$$

for $n \geq 1$with initial conditions $F_{k,0} = 0$ and $F_{k,1} = 1$ [15].

Kilic [16] defined the Tribonacci sequence for$n > 1$

$$T_{n+1} = T_n + T_{n-1} + T_{n-2}$$

Where $T_0 = 0, T_1 = 1,$ and , $T_2 = 1$

The first few Tribonacci numbers are $T = \{0,1,1,2,4,7,13,24,44,81,149, \dots\}$

Renault defined "For integers $a$and$b$, we define the (a, b) −Fibonacci sequence F as the sequence with initial conditions $F_0 = 0,\ F_1 = 1$, that satisfies the general second-order linear recurrence relation $F_n = aF_{n-1} + bF_{n-2}$" [9], [17].

From Renault's definition, we assume that the integers are equal. Therefore, (a, a) −Fibonacci sequence becomes, $F_n = aF_{n-1} + aF_{n-2} = a)$ a. Again, consider the ASCII code of the English alphabet instead of the coefficient integer a and the Tribonacci sequence instead of the (a, a) −Fibonacci sequence. Renault's definition is then extended to the weighted Tribonacci sequence, which is generated by

$$W_n = A_n(T_{n-1} + T_{n-2} + T_{n-3}) = A_nT_n$$

Where A_n is the ASCII code of the $(n + 1)^{th}$ alphabet in a message and T_n is the Tribonacci term.

Thus, the Catalan numbers, with the general term $C(n)$, are described by [12]

$$C(n) = \frac{1}{n+1}\binom{2n}{n}$$

Table 1. ASCII code of English alphabets.

A	B	C	D	E	F	G	H	I	J	K	P
65	66	67	68	69	70	71	72	73	74	75	80
Q	R	S	T	U	V	W	X	Y	Z	Q	R
81	82	83	84	85	86	87	88	89	90	81	82

The Catalan Sequence is then $C = \{1,1,2,5,14,42,132, \dots\}$

Catalan transform is typically defined by the formula [10]:

$$B_n = \sum_{i=0}^{n} \frac{i}{2n-i} \binom{2n-i}{n-i} T_i$$

which is equivalent to:

$$B_n = \sum_{i=0}^{n} C_i T_i$$

where C_i is the i^{th} Catalan number and $T_i$is the $i^{th} k$-Fibonacci number.

Note that we call the transform B_n Catalan transform of a Tribonacci sequence whenever the sequence $T_i$is the Tribonacci sequence.

Encoding-Decoding Algorithm

Encryption

The sender encrypts his/her message by applying the Catalan transform to the weighted Tribonacci sequence.

- *Step 1:* Map the characters of the message to their ASCII codes and form an array.

  $A = \{a_0, a_1, a_2, \dots\}$
- *Step 2:* Generate a Tribonacci sequence:

  $T_{m+1} = T_m + T_{m-1} + T_{m-2}$
- *Step 3:* Generate the weighted Tribonacci sequence W_n by $W_{n=A_n T_n}$for $n > 0$ and $W_0 = A_0$.
- *Step 4:* Find the Catalan transform B_n of W_n by:

  $B_n = \sum_{i=0}^{n} C_i W_i$

The receiver will get an encrypted message $B = \{b_n\}$

Decryption

Applying the inverse Catalan transform is mandatory for decrypting a message encrypted by the Catalan transform.

$$A_n = \frac{1}{C_n T_n} \left(B_n - \sum_{i=0}^{n-1} C_i W_i\right)$$

After obtaining all the A_is and looking back at the ASCII table, the receiver can understand the meaning of the message that he has received.

For a better understanding of the above steps 1 to 4, we examine the following example.
Example:
Suppose the sender wants to send the message “CODING”.

Encryption

The sender encrypts his/her message by applying the Catalan transform to the weighted Tribonacci sequence.

During the encryption and decryption processes, we use the Catalan and Tribonacci number sequences, which are given by (Table 2)

$C = \{1,1,2,5,14,42,132, \dots\}$

$T = \{0,1,1,2,4,7,13,24,44,81, \dots\}$

Table 2. ASCII code of the characters.

C	O	D	I	N	G
67	79	68	73	78	71

Step 1: Construct the ASCII code table for "CODING".
Thus, $A = \{67,79,68,73,78,71\}$

Step 2: Generate the ASCII-weighted Tribonacci sequence $W_{n=A_nT_n}$

$W_0 = A_0 = 67$
$W_1 = A_1T_1 = 79 * 1 = 79$
$W_2 = A_2T_2 = 68 * 1 = 68$
$W_3 = A_3T_3 = 73 * 2 = 146$
$W_4 = A_4T_4 = 78 * 4 = 312$
$W_5 = A_4T_4 = 71 * 7 = 497$

Hence the ASCII-weighted Tribonacci sequence becomes:
$W = \{67,79,68,146,312,497\}$

Step 3 and 4: Finally find the Catalan transform B_n of T by:
$B_n = \sum_{i=0}^{n} C_iW_i$
$B_0 = C_0W_0 = 1 * 67 = 67$
$B_1 = C_0W_0 + C_1W_1 = 67 + 1 * 79 = 146$
$B_2 = (C_0W_0 + C_1W_1) + C_2W_2 = 146 + 2 * 68 = 282$
$B_3 = (C_0W_0 + C_1W_1 + C_2W_2) + C_3W_3 = 282 + 5 * 146 = 1012$
$B_4 = (C_0W_0 + C_1W_1 + C_2W_2 + C_3W_3) + C_4W_4 = 1012 + 14 * 312 = 5380$
$B_5 = (C_0W_0 + C_1W_1 + C_2W_2 + C_3W_3) + C_4W_4 = 5380 + 42 * 497 = 26254$

Therefore, the receiver obtains $B = \{67,146,282,1012,5380,26254\}$ instead of the plain text "CODING."

Decryption

The receiver can decrypt it by using the inverse Catalan transform.

$A_n = \frac{1}{C_nT_n}\left(B_n - \sum_{i=0}^{n-1} C_iW_i\right)$
$A_0 = W_0 = 67$
$A_1 = \frac{1}{C_1T_1}(B_1 - C_0W_0) = 146 - 67 = 79$
$A_2 = \frac{1}{C_2T_2}\left(B_2 - (C_0W_0 + C_1W_1)\right) = \frac{1}{2}\left(282 - (67 + 79)\right) = 68$
$A_3 = \frac{1}{C_3T_3}$
$A_4 = \frac{1}{C_4T_4}$
$A_5 = \frac{1}{C_5T_5}$

From Table 1, we get that $A = \{67,79,68,73,78,71\}$ is "CODING".

CONCLUSION

In this study, we ensured message security using the Catalan Transform of a Weighted Tribonacci Sequence. This Catalan transform coding-decoding algorithm can also be applied to any value of $k$of

the k −Fibonacci sequence, which can increase the computational complexity of the coding-decoding process by intensifying the k-value of the k-Fibonacci sequence. Complexity is also dependent on the string length of the message. Moreover, a greater degree of variability is introduced by increasing the k-value, thereby strengthening the resistance of encryption to possible attacks. Owing to its flexibility, the system can be scaled to meet varying security requirements, making it appropriate for a wide range of applications. Sequence computations are also directly impacted by string length selection, which introduces another level of complexity. This method uses the k-Fibonacci sequence and Catalan transformations to construct a dynamic framework for secure communication, which strikes a compromise between advanced cryptographic resilience and computational effort.

Financial Sources

This research did not receive any specific grants from funding agencies in the public, commercial, or not-for-profit sectors.

REFERENCES

1. Amalraj AJ, Jose JR. A survey paper on cryptography techniques. Int J Comput Sci Mob Comput. 2016;5:55–9.
2. Eser E, Kuloglu B, Özkan E. An encoding-decoding algorithm based on Fermat and Mersenne numbers. Appl Math E – Notes. 2024;24:274–82.
3. Stakhov AP. Fibonacci matrices, a generalization of the 'Cassini formula', and a new coding theory. Chaos Solitons Fractals. 2006;30:56–66. DOI: 10.1016/j.chaos.2005.12.054.
4. Prasad B. Coding theory on Lucas p numbers. Discrete Math Algor Appl. 2016;8:1650074. DOI: 10.1142/S1793830916500749.
5. Sangeetha V, Anupreethi T, Somanath M. Cryptographic application of elliptic curve generated through centered hexadecagonal numbers. Indian J Sci Technol. 2024;17:2074–8. DOI: 10.17485/IJST/v17i20.1183.
6. Kuloğlu B. Creating a new coding and decoding algorithm based on violin notes. Res Rev Discrete Math Struct. 2023;10(3):25–30.
7. Kuloglu B, Ozkan E. Matrix representation of (d, k) – Fibonacci polynomials. Bull Transilvania Univ Brasov Ser III. 2024;III:185–200. DOI: 10.31926/but.mif.2024.4.66.2.11.
8. Samarasinghe Mudiyanselage TR, Ekanayake EMUSB. Cryptography algorithm using Laplace transformation. Int J Integr Sci. 2024;3:1053–66. DOI: 10.55927/ijis.v3i9.10486.
9. Raghunandan KR, Shetty R, Aithal G. Key generation and security analysis of text cryptography using cubic power of Pell's equation. 2017 International Conference on Intelligent Computing, Instrumentation and Control Technologies (ICICICT), Kerala, India. 2017. p. 1496–500. DOI: 10.1109/ICICICT1.2017.8342791.
10. Deveci O, Shannon A. On the complex-type Catalan transform of the k-fibonacci numbers. J Integer Seq. 2022;25:1352–67.
11. Parthasarathy MB, Srinivasan B. Increased security in image cryptography using wavelet transforms. Indian J Sci Technol. 2015;8:1–8. DOI: 10.17485/ijst/2015/v8i12/62433.
12. Barry P. A Catalan transform and related transformations on integer sequences. J Integer Seq. 2005;8(8):1–24.
13. American Standard Code for Information Interchange, ASA X3.4-1963, American Standards Association, June 17, 1963.
14. Tan B, Wen ZY. Some properties of the Tribonacci sequence. Eur J Comb. 2007;28:1703–19. DOI: 10.1016/j.ejc.2006.07.007.
15. Falcon S. Catalan transform of the κ-fibonacci sequence. Commun Korean Math Soc. 2013;28:827–32. DOI: 10.4134/CKMS.2013.28.4.827.
16. Kılıç E. Tribonacci sequences with certain indices and their sums. Ars Combin. 2008;86:13–22.
17. Renault M. The period, rank, and order of the (a, b)-fibonacci sequence mod m. Math Mag. 2013;86:372–80. DOI: 10.4169/math.mag.86.5.372.

