Research and Reviews: Discreate Mathematical Structures

Vol: 11, Issue: 3, Year: 2024, ISSN(e): 2394 –1979

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

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

1, * Assistant Professor, Department of Engineering Basic Sciences, Sivas University of Science and Technology, Sivas, Türkiye

Email: bkuloglu@sivas.edu.tr or bahar_kuloglu@hotmail.com

Research Paper

Received Date: 19 December 2024

Accepted Date:30 December 2025

Published Date:10 January 2025

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. 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 several applications, especially in settings where strong data security is required.

Keywords: Catalan Transform, Inverse Catalan Transform, Tribonacci Sequence, Weighted Tribonacci Sequence

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

1. INTRODUCTION

Due 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 developed numerous algorithms utilizing 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], Sangeetha and Anupreethi's centered hexadecagonal numbers [5]. Additionally, Kuloglu and Ozkan explored Fibonacci polynomials and matrices for cryptographic purposes [6,7].

Classical Fibonacci numbers, the Pell equation, and Tribonacci numbers have become prominent research interests. 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, while 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.

American Standard Code for Information Interchange (ASCII) presents the standard coded character set for information interchange among information processing systems, communication systems, and associated equipment. The following table is an ASCII representation of the English alphabet [13,14].

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

Table 1: ASCII code of English alphabets

Building on this foundation, we propose a coding-decoding algorithm based on the

Catalan transforms the weighted Tribonacci sequence.

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

2. MAIN RESULTS

For any positive real number k, the k-Fibonacci sequence, say $\{F_{k,n}\}_{n\in N}$ 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 $(a, b)-$Fibonaccisequence 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, let us assume the integers are equal. So, $(a, a)-$Fibonacci sequence becomes, $F_n = aF_{n-1} + aF_{n-2} = a$). Again, consider the American Standard Code for Information Interchange (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:

$$W_n = A_n(T| \quad |n-1 + T_{n-2} + T_{n-3}) = A_n T_n$$

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]

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

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.

2.1 Encoding-Decoding Algorithm

Encryption

The sender will encrypt his message by applying the Catalan transform to the weighted Tribonacci sequence.

Step 1: Map the characters of the message to their ASCII code 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 $W_{n=A_nT_n}$ 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 to decrypt 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 he has received.

For a better understanding of the above steps, let's examine the following example:

Example

Suppose the sender wants to send the message "CODING".

Encryption

The sender will encrypt his message by applying the Catalan transform to the weighted Tribonacci sequence.

During the encryption and decryption process, we use the Catalan and Tribonacci number sequences which are given by:

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

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

Step 1: Construct the ASCII code table for "CODING".

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

Table 2: ASCII code of the characters

Thus, $A = \{67,79,68,73,78,71\}$

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

$$W_0 = A_0 = 67 \qquad W_3 = A_3T_3 = 73 * 2 = 146$$

$$W_1 = A_1T_1 = 79 * 1 = 79 \qquad W_4 = A_4T_4 = 78 * 4 = 312$$

$$W_2 = A_2T_2 = 68 * 1 = 68 \qquad W_5 = A_4T_4 = 71 * 7 = 497$$

Hence the ASCII-weighted Tribonacci sequence becomes:

$W = \{67,79,68,146,312,497\}$

Step 4: Finally find the Catalan transform B_n of $T$by:

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

$$B_0 = C_0 W_0 = 1 * 67 = 67$$

$$B_1 = C_0 W_0 + C_1 W_1 = 67 + 1 * 79 = 146$$

$$B_2 = (C| \quad |0W_0 + C_1 W_1) + C_2 W_2 = 146 + 2 * 68 = 282$$

$$B_3 = (C_0 W_0 + C_1 W_1 + C_2 W_2) + C_3 W_3 = 282 + 5 * 146 = 1012$$

$$B_4 = (C| \quad |0W_0 + C_1 W_1 + C_2 W_2 + C_3 W_3) + C_4 W_4 = 1012 + 14 * 312 = 5380$$

$$B_5 = (C| \quad |0W_0 + C_1 W_1 + C_2 W_2 + C_3 W_3) + C_4 W_4 = 5380 + 42 * 497 = 26254$$

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

Decryption

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

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

$$A_0 = W_0 = 67$$

$$A_1 = \frac{1}{C_1 T_1}(B_1 - C_0 W_0) = 146 - 67 = 79$$

$$A_2 = \frac{1}{C_2 T_2}\big(B_2 - (C_0 W_0 + C_1 W_1)\big) = \frac{1}{2}\big(282 - (67 + 79)\big) = 68$$

$$A_3 = \frac{1}{C_3 T_3}$$

$$A_4 = \frac{1}{C_4 T_4}$$

$$A_5 = \frac{1}{C_5 T_5}$$

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

3. CONCLUSION

In this study, we ensure message security using the Catalan transform of a weighted Tribonacci sequence. This Catalan transform coding-decoding algorithm can also be applied for 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. The complexity is also dependent on the string length of the message. Moreover, a greater degree

of variability is introduced by raising the k-value, strengthening the encryption's resistance to possible attacks. Because of its flexibility, the system may be scaled to meet varying security requirements, making it appropriate for a wide range of applications. The sequence computations are also directly impacted by the string length selection, which introduces even another level of complexity. This method uses the k-Fibonacci sequence and Catalan transformations to construct a dynamic framework for secure communication that strikes a compromise between advanced cryptographic resilience and computational effort.

Financial Sources

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

REFERENCES

1. Amalraj, A. J., & Jose, J. R. (2016). A Survey Paper on Cryptography Techniques. International Journal of Computer Science and Mobile Computing, 5(8), 55-59.
2. Eser, E., Kuloglu, B., & Özkan, E. (2024). An Encoding-Decoding Algorithm Based On Fermat and Mersenne Numbers. Applied Mathematics E-Notes, 24, 274-282.
3. Stakhov, A. P. (2006). Fibonacci matrices, a generalization of the "Cassini formula", and a new coding theory. Chaos, Solitons & Fractals, 30(1), 56-66.
4. Prasad, B. (2016). Coding theory on Lucas p numbers. Discrete Mathematics, Algorithms and Applications, 8(04), 1650074.
5. Sangeetha, V., Anupreethi, T., & Somanath, M. (2024). Cryptographic Application of Elliptic Curve Generated through Centered Hexadecagonal Numbers. Indian Journal of Science and Technology, 17(20), 2074-2078.
6. Kuloğlu, B. (2024). Creating a New Coding and Decoding Algorithm Based on Violin Notes.
7. Kuloglu, B., & Ozkan, E. (2024). Matrix representation of (d, k)-Fibonacci polynomials. Bulletin of the Transilvania University of Brasov. Series III: Mathematics and Computer Science, 185-200.
8. Mudiyanselage, T.R.S., & Ekanayake Emusb. (2024). A Cryptography Algorithm Using Laplace Transformation. International Journal of Integrative Sciences, 3(9), 1053-1066.
9. Raghunandan, K. R., Shetty, R., & Aithal, G. (2017, July). Key Generation and Security Analysis of Text Cryptography using Cubic Power of Pell's Equation. International conference on intelligent computing, instrumentation, and control technologies (ICICICT) (pp. 1496-1500). IEEE.
10. Deveci, O., & Shannon, A. (2022). On the Complex-type Catalan Transform of the k-Fibonacci Numbers. Journal of Integer Sequences, 25(4), 1352-1367.
11. Parthasarathy, M.B., & Srinivasan, B. (2015). Increased Security in Image Cryptography using Wavelet Transforms. Indian Journal of Science and Technology, 8(12), 1-8.
12. Barry, P. (2005). A Catalan Transform and Related Transformations on Integer Sequences. Journal of Integer Sequences, 8.
13. American Standard Code for Information Interchange, ASA X3.4-1963". American Standards Association (ASA). 1963-06-17. Retrieved 2020-06-06.
14. Tan, B., & Wen, Z. Y. (2007). Some Properties of the Tribonacci Sequence. European Journal of Combinatorics, 28(6), 1703-1719.
15. Falcon, S. (2013). Catalan Transform of the κ-Fibonacci Sequence. Communications of the Korean Mathematical Society, 28(4), 827-832.

16. Kilic E. (2008). Tribonacci Sequences with Certain Indices and Their Sums.
17. Renault, M. (2013). The Period, Rank, and Order of the (a, b)-Fibonacci Sequence Mod m. Mathematics Magazine, 86(5), 372–380.