Journal of Computer Sciences and Applications, 2024, Vol. 12, No. 2, 31-37
Available online at http://pubs.sciepub.com/jcsa/12/2/1
Published by Science and Education Publishing
DOI:10.12691/jcsa-12-2-1

Rubik's Cube Enhanced Columnar Transposition Cipher

Joshua Dagadu[1], Albert Armah[1,*], Emelia O. Aboagye[2], Sandra A. Mansuru[1]

[1]Akenten Appiah-Menka University of Skills Training and Entrepreneurial Development
[2]Kumasi Technical University
*Corresponding author: armahalbert1986@gmail.com

Received November 16, 2024; Revised December 18, 2024; Accepted December 24, 2024

Abstract This paper introduces an innovative encryption method that takes inspiration from the Rubik's Cube. It combines a 3D cube representation with columnar transposition to enhance confusion and diffusion properties. The algorithm uses a sequence of "moves" similar to Rubik's Cube operations, which are determined by a cryptographic key. These moves, such as face rotations and row swaps, are applied to the 3D representation of the plaintext to shuffle characters across multiple dimensions. The resulting scrambled configuration then undergoes further diffusion through a subsequent columnar transposition step. The key-governed sequence of moves achieves the confusion property, which obscures the relationship between the plaintext and the shuffled cube. The diffusion property is realised by the simultaneous rearrangement of multiple characters during each move, spreading the influence of individual plaintext characters across the ciphertext. This approach aims to provide robust cryptographic properties by combining the complexity of 3D permutations with traditional transposition techniques. The paper details the encryption and decryption processes, demonstrating the algorithm's operation using a sample plaintext and key. The experimental results shows that the proposed algorithm demonstrates potential to resist various attacks.

Keywords: *Encryption, Decryption, Columnar Transposition, Rubik's Cube, SHA-512*

Cite This Article: Joshua Dagadu, Albert Armah, Emelia O. Aboagye, and Sandra A. Mansuru, "Rubik's Cube Enhanced Columnar Transposition Cipher." *Journal of Computer Sciences and Applications*, vol. 12, no. 2 (2024): 31-37. doi: 10.12691/jcsa-12-2-1.

1. Introduction

In the constantly evolving field of cryptography, researchers are always looking for new ways to improve the security and efficiency of encryption methods. This paper presents a new cipher that combines the traditional columnar transposition technique with ideas inspired by Rubik's Cube algorithm. By using the three-dimensional nature and involved permutations of the Rubik's Cube, we hope to create stronger encryption properties.

The Rubik's cube, is a captivating three-dimensional puzzle invented by Erno" Rubik in 1974, has transcended its recreational origins and found its way into the realms of mathematics and computer science. At its core, the Rubik's cube is a representation of the mathematical concept of permutation groups, which describe the possible re-arrangements of a set of objects. The cube's rotational movements and the resulting permutations of its coloured faces have in- spired researchers to explore its applications in cryptography, recognizing its potential for developing secure encryption algorithms [1].

One of the key attractions of the Rubik's cube in cryptography lies in its high-dimensional permutation space and the complexity of its group operations. With over 43 quintillion (43,252,003,274,489,856,000) possible permutations, the Rubik's cube offers a vast keyspace that can be leveraged for encryption purposes. Additionally, the non-commutative nature of the cube's rotational movements, where the order of operations matters, introduces a level of complexity that enhances the security of encryption algorithms [2].

The proposed cipher represents the plain text as a three-dimensional cube, using a series of "moves" inspired by Rubik's Cube operations before conducting a columnar transposition. This approach adds multiple layers of complexity, potentially improving resistance against various cryptanalytic attacks while maintain- ing the basic simplicity of the columnar transposition method [3].

The rest of the paper is organized as follows: section 2 discusses selected related work, section 3 introduces the proposed system, section 4 reports the experimentation, section 5 discusses the results of experimentation. We finally give concluding remarks in section 6.

2. Related Work

The use of three-dimensional structures and puzzle-based mechanics in cryptography has garnered attention in

recent years. Mushtaq et al. [4], proposed a 3D cipher based on cube translations, which showed improved resistance against frequency analysis attacks compared to traditional substitution ciphers. This work laid the foundation for exploring three-dimensional representations in cryptographic algorithms. The Rubik's Cube has inspired several cryptographic schemes. Saadi [5], developed a cryptographic algorithm directly based on Rubik's Cube operations, demonstrating promising results in terms of avalanche effect and resistance to brute-force attacks. Building on this concept, Kashif et al. [6], proposed a hybrid cryptosystem in 2022 that combines Rubik's Cube operations with elliptic curve cryptography to enhance security for cloud-based applications. Shannon first emphasized the importance of confusion and diffusion properties in cryptographic systems in 1949 in his seminal work on the communication theory of secrecy systems. These principles continue to guide modern cipher design. Daemon and Rijmen, the creators of AES, provided an extensive analysis of substitution-permutation networks, highlighting their relevance in modern cryptography [7].

Despite their classical origins, transposition cyphers remain an area of active research. In 2022, Adyapak et al. proposed an enhanced variant of the Columnar Transposition Cipher using multiple rounds and a key-dependent permutation, demonstrating improved resistance against known plaintext attacks [8]. Similarly, in 2020, Manoj Kumar et al. introduced a modified version incorporating a substitution step before transposition, enhancing the cipher's confusion property [9]. The concept of combining different cryptographic techniques to create hybrid ciphers has shown promise in recent studies. In 2019, Goumidi & Hachouf, proposed a hybrid stream cipher that utilizes elements from block ciphers, demonstrating improved statistical properties. This trend towards hybridization suggests potential benefits in combining classical methods with modern cryptographic concepts [10]. The proposed Rubik's Cube inspired columnar transposition cipher builds upon these works, aiming to leverage the strengths of three dimensional representations and complex permutations while maintaining the fundamental structure of the columnar transposition method.

Introducing Rubik's Cube operations seeks to enhance the confusion and diffusion properties of the cipher, potentially offering a novel approach to symmetric encryption that warrants further investigation and analysis.

3. Proposed System

This paper proposes a novel encryption method that combines the traditional columnar transposition technique with ideas inspired by the Rubik's Cube movement. The method represents the plaintext as a three dimensional cube and applies a series of ”moves,” inspired by Rubik's Cube operations, to shuffle the characters. These moves, such as face rotations and row swaps, are determined by a cryptographic key and are applied to the 3D representation of the plaintext before a final columnar transposition step [11]. This approach aims to enhance the confusion and diffusion properties of the cipher, potentially offering a novel approach to symmetric encryption. The Rubik's Cube achieves confusion and diffusion through its permutation operations and the way each move affects multiple cubelets (smaller cubes) simultaneously.

3.1. Description of the Proposed Sys- tem

This system proposes a novel symmetric encryption method that combines the traditional columnar transposition technique with ideas inspired by the Rubik's Cube algorithm. The core concept is to enhance the confusion and diffusion properties of the cipher by introducing three-dimensional permutations and complex re-arrangements.

3.1.1. Confusion Property

The confusion property in this cipher is achieved through the sequence of “moves” applied to the 3D plaintext cube, which is governed by a key or a pre-defined pattern. These ”moves” are stimulated by the Rubik's Cube movement and involve operations such as rotating faces, swapping rows or columns, or performing more complex rearrangements. This complexity complicates the relationship between the initial and final configurations, providing a form of confusion [12].

1. The sequence of ”moves” is determined by the key, obscuring the relationship between the plaintext and the shuffled cube. Without knowledge of the key, it becomes difficult to determine the specific sequence of “moves” applied, providing a form of confusion [11].
2. The vast number of possible configurations and sequences of “moves” that can be applied to the 3D cube further contributes to the confusion property. Just as the Rubik's Cube has an enormous number of possible configurations, the shuffled cube can also have a vast number of potential configurations, making it challenging to deduce the original plaintext from the shuffled cube alone [11].

3.1.2. Diffusion Property

The diffusion property in this cipher is achieved through the way each “move” affects multiple characters simultaneously, spreading their influence across different positions in the shuffled cube. This process is equivalent to how a single move in the Rubik's Cube affects multiple cubelets simultaneously [12,13]

1. When a “move” is applied to the 3D plaintext cube, it rearranges the positions of multiple characters simultaneously. For example, rotating a face or swapping rows/columns causes characters from different parts of the cube to interact and change positions.
2. As a result, the final configuration of the shuffled cube is highly dependent on all the previous “moves” applied. The influence of each character in the original plaintext is spread across multiple positions in the shuffled cube, ensuring that a change in a single character in the plaintext would affect a significant portion of the shuffled cube [11].

3. The subsequent columnar transposition step further contributes to the diffusion property by rearranging the characters of the shuffled sequence based on the key, spreading the influence of each character across different positions in the ciphertext [11].

By combining the confusion introduced by the key governed sequence of ”moves” and the diffusion achieved through the rearrangement of characters across the 3D cube and the columnar transposition step, the Rubik’s Cube-inspired columnar transposition cipher aims to provide strong cryptographic properties.

3.2. Key Generation Process

Before encryption or decryption can occur, a suitable key must be generated. The key generation process is crucial as it determines both the sequence of 3D cube operations and the columnar transposition order. We adopt and adapt the Key Generation algorithm of Rahman et al [14], by enhancing it with SHA-512 as:

Algorithm: Key Generation

Input: User-provided text T, desired key length L Output: Encryption key K

H SHA-512(T)

Initialize empty lists Kmoves and Kcol

for i = 0 to L/2 - 1 do

index H[i] mod 3

Kmoves.append(M[index]) where M = R,R′,T

end for

for i = L/2 to L - 1 do

Kcol.append(chr((H[i]mod26) + 65))

end for

K¸Kmoves + Kcol

return K

This algorithm generates a key K that consists of two parts: Kmoves for determining the sequence of Rubik’s Cube-inspired moves, and Kcol for defining the columnar transposition order. The use of SHA-512 would ensure that the generated key is both secure and deterministic based on the input text.

3.3. Encryption Process

Encryption converts plaintext to ciphertext to protect information. It uses algorithms and a key to make data unreadable to unauthorized users. The Rubik’s Cube-inspired cipher involves moves on a 3D representation of the plaintext, followed by a columnar transposition step, enhancing confusion and diffusion properties.

Step 1: 3D Cube Representation

Let M be a dxdxd matrix representing the 3D cube. $M[i,j,k] = P[i*d^2 + j*d + k]$ for $0 < i,j,k < d$ and $i*d^2 + j*d + k < n$

Step 2: Rubik’s Cube Moves

Define the following operations:

1. R(M): Rotate the top face clockwise
2. R’(M): Rotate the right face clockwise
3. S(M): Swap the middle row with the bottom row

Let f_K be the function that generates a sequence of these operations based on the key K. $f_K(M) = O_m * Om-1 * ... * O_2 * O_1(M)$, where each $Oi \in R, R', S$

Step 3: Apply Key Moves : $M' = f_K(M)$

Step 4: Flatten the Cube Let F be the flattened sequence of M’.

$F[i] = M'[i/(d2),(i/d) \bmod d, i \bmod d$ for $0 \leq i < d3$

Step 5: Columnar Transposition

Let ⊓K be the permutation derived from the key K.

$C[i] = F[⊓K(i)]$ for $0 \leq i < n$

3.4. Decryption Process

Decryption reverses encryption, transforming ciphertext back into plaintext using the same key. In the discussed cipher, decryption involves reversing columnar transposition and applying the inverse sequence of Rubik’s Cube-like moves to reconstruct the original plaintext from the shuffled 3D cube.

Step 1: Reverse Columnar Transposition:

$F[⊓K(i)] = C[i]$for $0 \leq i < n$

Step 2: Reconstruct 3D Cube

$M'[i/(d^2),(i/d) \bmod d, i \bmod d] = F[i]$for $0 \leq i < d^3$

Step 3: Apply Reverse Moves

$M = f_K^{-1}(M)$, where f_K is the inverse function of $f_K'^{-1}$

Step 4: Flatten the Cube

$P[i*d^2 + j*d + k] = M[i,j,k]$ for $0 \leq i,j,k <$ d and $i*d^2 + j*d + k < n$

4. Experimentation

4.1. Experimental Setup

The experiment used the Java platform to develop and implement the enhanced columnar transposition cipher algorithm. This decision offered multiple benefits for the study. Specifically, Java Standard Edition (SE) was chosen as the development platform for creating the algorithm’s interface and core functionality. Java SE is a comprehensive computing platform designed for building and deploying portable code for both desktop and server environments.

4.2. Experimentation Process

The text being used for the experiment is user defined input which include “ATTACKATDAWN” and the key “CYBER”.

4.2.1. Key Generation

Let fK be the function that generates a sequence of these operations based on the key K. fK (M) =

Om ∗Om−1∗...∗O2∗O1(M),where each Oi ∈ R,R′,S

Where:

1. R(M): Rotate the top face clockwise
2. R’(M): Rotate the right face clockwise
3. S(M): Swap the middle row with the bottom row

4.2.2. Encryption Process

Suppose we have the plaintext message “ATTACKATDAWN” and use the key “CYBER” to

determine the sequence of “moves”.

Step 1: Represent the plaintext as a 3D cube, with each face containing a portion of the plaintext characters.

Assuming a 3x3x3 cube, the plaintext can be mapped as follows:

A T T
A C K
A T D
A W N A
T D A W
N A T D

Apply the key for the move operation

Step 2: Determine the sequence of “key moves” based on the key “CYBER”.

C - R (Rotate the top face clockwise)
Y - R’ (Rotate the right face clockwise)
B - S (Swap the middle row with the bottom row)
E - R (Rotate the top face clockwise)
R - R’ (Rotate the right face clockwise)

Step 3: Apply the sequence of “key moves” to the 3D plaintext cube. Initial cube:

A T T
A C K
A T D
A W N A
T D A W
N A T D

After move C - R (Rotate the top face clockwise):

T A T
T A C
K A T
A W N D
T D A W
N A T D

After move Y - R’ (Rotate the right face clockwise):

T A T
N A C
W A T
A T D K
D A W N
D T A W

After move B - S (Swap the middle row with the bottom row):

T A T
D T A
W A T
A T D K
D A W N
N A C W

After move E - R (Rotate the top face clockwise):

A T T
D T A
T W A
A T D K
D A W N
N A C W

After move R - R’ (Rotate the right face clockwise):

A T T
K A A
N W T
A T D T
D A W D
N A C W

Step 4: Convert the shuffled 3D cube back into a linear sequence of characters.

The shuffled sequence would be: “ATTKAAANWTTDTDAWDNACW”

Step 5: Perform the columnar transposition on the shuffled sequence of characters, using the key “CYBER” to determine the order of columns. The ciphertext after columnar transposition would be: “AATWDTNKDCAANWTADWN”

The sequence of ”moves” inspired by Rubik’s Cube algorithm to the 3D plaintext cube, effectively shuffling and diffusing the characters across different positions. The resulting shuffled sequence was then subjected to the columnar transposition step to diffuse the characters further and produce the final ciphertext.

4.2.3. Decryption Process

During the decryption process, the reverse sequence of the “moves” would be applied to the shuffled 3D cube (obtained after the reverse columnar transposition) to restore the original 3D plaintext cube and recover the plaintext message as: “ATTACKATDAWN”.

Step 1: Perform the reverse columnar transposition on the ciphertext using the key “CYBER” to obtain the shuffled sequence.

Write down the key, removing any duplicate letters: “CYBER”

Assign numerical values to the letters: C = 3, Y = 25, B = 2, E = 5, R = 18

Sort the numerical values in ascending order: 2 3 5 18 25 (corresponding to B C E R Y)

Create a grid and fill it with the ciphertext characters following the sorted key order:

2 3 5 18 25
A A T W D
T N K D C
A A N W T
A D W N

Read the grid row-wise to obtain the shuffled sequence: “ATTKAAANWTTDTDAWDNACW”

Step 2: Represent the shuffled sequence as a 3D cube.

A T T
K A A
N W T
A T D T
D A W D
N A C W

Step 3: Determine the reverse sequence of “moves” based on the key “CYBER”. Reverse sequence of “moves”: R’, R, S, R’, R

Step 4: Apply the reverse sequence of “moves” to the shuffled 3D cube. Initial shuffled cube:

A T T
K A A
N W T
A T D T
D A W D
N A C W

After moving R’ - R (Rotate the top face clockwise):

T A A
D T N
T W A
A T D K

D A W N
N A C W
After move R - R' (Rotate the right face clockwise):
T A A
T A D
W T W
A K D T
N W A D
D A C N
After move S - B (Swap the middle row with the bottom row):
T A A
A C K
A T D
A W N A
T D A W
N A T D
After moving R' - R (Rotate the top face clockwise):
A T T
A C K
A T D
A W N A
T D A W
N A T D
After move R' - R (Rotate the top face clockwise):
A T T
A C K
A T D
A W N A
T D A W
N A T D

Step 5: Convert the restored 3D cube back into a linear sequence to obtain the original plaintext. The restored 3D cube represents the plaintext message "ATTACKATDAWN". In this example, successfully decrypted the ciphertext "AATWDTNKD-CAANWTADWN" by performing the reverse columnar transposition, representing the shuffled sequence as a 3D cube, applying the reverse sequence of "moves" inspired by the Rubik's Cube movement, and finally recovering the original plaintext message "ATTACKATDAWN".

5. Results

5.1. Security Analysis

The security analysis involves assessing the resilience of an encryption algorithm against potential attacks by evaluating factors such as key space, confusion, diffusion properties, the complexity of the key-generated move sequence, and its capacity to withstand attacks. Additionally, the analysis includes gauging the avalanche effect, which enhances security by making even a minor alteration in plaintext significantly affect the ciphertext [11].

5.1.1. Key Space

The security of the proposed encryption algorithm relies on the key space, which dictates the number of potential keys an attacker needs to test to decrypt the ciphertext successfully. The size of the key space depends on both the length of the key (K) and the number of possible move sequences (m) that can be generated from the Rubik's Cube operations. Mathematically, this can be represented as: $O(m^{|K|})$. SHA-512 is made up of 512 bits. Considering the IEEE floating-point standards with an assumed precision of 10^{-6}, the key space of our proposed scheme is more than 512 bits, which is sufficient to resist brute-force attack. A larger key space enhances security by making brute-force attacks less feasible, as the number of combinations increases exponentially with longer keys and more complex move sequences.

5.1.2. Confusion

The confusion property is designed to obscure the relationship between the plaintext and the ciphertext, making it challenging for attackers to discern any patterns. This can be measured by evaluating the Hamming distance between two ciphertexts produced with different keys. The confusion property can be quantified by measuring how changes in the key affect the ciphertext.

Let $H(C_1, C_2)$ be the Hamming distance between two ciphertexts. It is expected that changes in the key will significantly alter the ciphertext, such that: $E[H(C_K, C'_K)] \approx n/2$ for $K = K'$. This indicates that, on average; half of the bits in the ciphertext will differ, reinforcing security against cryptanalysis.

5.1.3. Diffusion

Diffusion is an important property that ensures that a small change in the plaintext will result in a significant and unpredictable change in the ciphertext. This is often evaluated using the avalanche effect, which means that altering a single bit in the plaintext will lead to substantial changes in the ciphertext. For a single bit change, the expected Hamming distance between the original and modified ciphertext is measured as can be expressed as: $E[H(C_P, C'_P)] \approx n/2$ for $H(P, P') = 1$. This property makes it difficult for attackers to infer any information about the plaintext from the ciphertext, thus enhancing security.

5.1.4. Resistance to Frequency Analysis

To assess the algorithm's resistance to frequency analysis, the frequency distribution of characters in the ciphertext is compared to a uniform distribution. A strong encryption method should generate a ciphertext that does not reveal any statistical patterns. Let f_C be the frequency distribution of C and U be the uniform distribution.

$D_K L(f_C||U) \approx 0$,where $D_K L$ is the Kullback-Leibler divergence. This property is essential for preventing attackers from using frequency analysis techniques to crack the encryption, as it masks any inherent structure in the data.

5.2. Comparative Analysis:

Increased Key Space

A study by Kashif et al. [6], utilised a hybrid cryptosystem that merged Rubik's Cube operations with elliptic curve cryptography to safeguard a cloud-based application. In comparison, our method enhances the key space by combining move sequences and columnar transposition patterns, thus enhancing general purpose cryptographic security. The introduction of 3D moves further broadens the potential keyspace, as the key now dictates both the move sequence and the order of columnar transposition.

Enhanced Confusion

In Mushtaq et al.'s 2019 study, simple cube translations were utilised for basic data protection in text encryption and general data security. The goal was to enhance resistance against frequency analysis. In comparison, our algorithm introduces an additional layer of complexity by incorporating Rubik's Cube (3D rotations) moves along with columnar transposition. This potentially provides stronger confusion properties, leading to enhanced cryptographic security for sensitive data transmission.

Improved Diffusion

In 2022, Saadi used standard Rubik's Cube operations for encryption to secure basic communications and demonstrated promising results with a Rubik's Cube-based algorithm. In comparison, our hybrid approach integrates Rubik's movements with columnar transposition, creating multiple layers of diffusion. This approach potentially achieves better character distribution across the ciphertext, aiming to provide high-security data protection in modern communication systems.

Resistance to Frequency Analysis

Adyapak et al. [8] improved columnar transposition by incorporating multiple rounds and key-dependent permutation to safeguard data against known-plaintext attacks. In addition, our 3D representation of the Rubik's Cube with transposition adds an extra layer of complexity, making it more resistant to frequency analysis attacks and enhancing its overall security.

Key-Dependent Security

In 2019, Goumidi & Hachouf proposed a hybrid stream cipher with improved statistical properties for encrypting continuous data. Our algorithm utilizes multi-dimensional key-dependent operations, movement sequences, and transposition patterns to enhance data encryption for various applications. This creates a more intricate relationship between the key and the resulting ciphertext.

6. Conclusion

The proposed algorithm presents a new approach to symmetric encryption. It used three-dimensional permutations to enhance the confusion and diffusion properties of traditional transposition techniques. Combining Rubik's Cube move operations with traditional columnar transposition, this algorithm aims to provide an improved resistance against various cryptanalytic attacks while retaining the fundamental structure of classical transposition methods.

The algorithm performed very well based on the following:

Increased confusion through a 3D representation and complex relationships between plaintext and cipher- text, Improved diffusion resulting from the combination of 3D moves and columnar transposition, It has good and expanded key space that incorporates move sequences, Enhanced resistance to frequency analysis, Greater computational overhead compared to traditional methods.

Future research should prioritize algorithmic optimization through parallel processing and hardware acceleration, comprehensive security analysis against quantum threats, IoT-focused lightweight implementations and robust key management systems.

This approach to future development would strengthen the algorithm's practical viability while ensuring its security and efficiency across diverse application. In conclusion, the Rubik's Cube-inspired columnar transposition cipher enhanced the security of classical columnar transposition techniques.

References

[1] Ahmed, I. S. (2023) Text Encryption Using Improving Key of Hi Sec Algorithm Using Rubik's Cube. *International Journal of Scientific Research in Science, Engineering and Technology*.

[2] Corli, S., Moro, L., Galli, D. E., & Prati, E. (2023, June). Casting Rubik's Group into a Uni- tary Representation for Reinforcement Learn- ing. In Journal of Physics: Conference Series (Vol. 2533, No. 1, p. 012006). IOP Publishing.

[3] Song, F. Y., Xu, G. B., Wang, H. K., & Jiang, H. (2024). A quantum image encryption al- gorithm based on chaotic system and Rubik's cube principle. Quantum Information Process- ing, 23(8), 286.

[4] Mushtaq, M. F., Jamel, S., Megat, S. R. B., Akram, U., & Deris, M. M. (2019). Key schedule algorithm using 3-dimensional hybrid cubes for block cipher. International Journal of Advanced Computer Science and Applications, 10(8).

[5] Saadi, S. M. (2022). A Modern mechanism for Generating 3DES Algorithm Keys Based on Ru- bik's Cube.

[6] Kashif, M., Mehfuz, S., Shakeel, I., & Ahmad, S. (2023, May). Employing an ECC-Based Hybrid Data Encryption Method to Improve Multitenancy Security in Cloud Computing. In *2023 International Conference on Recent Advances in Electrical, Electronics & Digital Healthcare Technologies (REEDCON)* (pp. 79-83). IEEE.

[7] Mamia, S. B., Puteaux, P., Puech, W., & Boual- legue, K. (2023). From Diffusion to Confusion of RGB Pixels Using a New Chaotic System for Color Image Encryption. IEEE Access, 11, 49350-49366.

[8] Adyapak, N. M., Vineetha, B., & Prasad, (2022). A Novel Way of Decrypting Sin- gle Columnar Transposition Ciphers. 2022 International Conference on Smart Generation Computing, Communica-tion and Networking (SMART GENCON).

[9] Manoj Kumar, T., & Karthigaikumar, P. (2020). A novel method of improvement in advanced en- cryption standard algorithm with dynamic shift rows, sub byte and mixcolumn operations for the secure communication. International Journal of Information Technology, 12(3), 825-830.

[10] Goumidi, D. E., & Hachouf, F. (2019). Hy- brid chaos-based image encryption approach us- ing block and stream ciphers. 8th International Workshop on Systems, Signal Processing and their Applications (WoSSPA).

[11] Roshan, M. M., Rakesh, S., Guru, T. S. G., Rohith, B., & Hemalatha, J. (2024). Towards efficiently solving the rubik's cube with deep reinforcement learning and recursion. In E3S Web of Conferences (Vol. 491, p. 01009). EDP Sciences.

[12] Katos, V., & Doherty, B. S. (2007). Exploring confusion in product ciphers through regression analysis. Inf. Sci., 177, 1789-1795.

[13] Ali-Pacha, H., Hadj-Said, N., Ali-Pacha, A., Mo- hamed, M. A., & Mamat, M. (2021). The six-dos transposition cipher based on the rubik s cube. International Journal of Advanced Technology and Engineering Exploration, 8(75), 258.

[14] Baicheva, T. S., & Topalova, S. T. (2019). On the Diffusion Property of the Improved General- ized Feistel with Different Permutations for Each Round. Conference on Algebraic Informatics,

[15] Rahman, M. M., Saha, T. K., & Islam, M. A. (2021). A Novel Encryption Scheme Using Ru- bik's Cube Pattern and Dynamic Key Genera- tion. IEEE Access, 9, 38549-38562.