

# Hybrid Cryptographic Approach for Integrating Information

DWARSALA MOHIT REDDY  
*Student, Department of Civil Engineering  
Amrita Vishwa Vidyapeetham, Coimbatore*

---

## Abstract

In today's world, data transport plays a crucial function. There is a possibility of data theft while the data is being sent. To keep data theft secure, we shall employ the cryptography principles. Data transfer refers to the exchange of data from sender to receiver over a communication channel. Through various ways, cryptography is used to offer data security. If we use further approaches to the plain text and it becomes cipher text, we can simply state that the plain text was much protected. To produce the key in this suggested technique, the Local Binary Pattern methods employed. Row Column Transposition Encryption and decryption are accomplished through the use of cipher techniques and even bit swapping.

**Keywords:** Encryption, Decryption, Local Binary Pattern, Even Bit Swapping and Row Column Transposition Cipher

---

Date of Submission: 10-08-2023

Date of acceptance: 25-08-2023

---

## I. INTRODUCTION

Cryptography is a broad idea for guaranteeing data security. Cryptography offers several strategies for maintaining data security. Every approach has an algorithm. Encryption and decryption will be possible using these techniques. Encryption and Decryption in cryptography are performed either bit by bit as well as block by block. If the encryption is done block by block, it is referred to as a block cipher. If the encryption is done bit by bit, this is known as a stream cipher. Cryptography consists primarily of four terms. These terms are Encryption, Decryption, Plaintext, and Cipher text.

Encryption: The process of turning plain text to encrypted text is known as encryption.

Decryption: The process of transforming encrypted text to plain text is known as decryption.

Plain text refers to legible text. Cipher text is illegible text. Cryptography may be classified into three categories. They have every algorithm in cryptography will fall under one of these three strategies

- ❖ Secret key cryptography
- ❖ Public key cryptography
- ❖ Hash functions

## II. LITERATURE REVIEW

By the usage of large amount of internet for transmitting the data it is essential to provide the security as intruders are coming with various kinds of hacking techniques. And the usage of social media is increasing rapidly. With the help of social media people are sharing their personal information from person to person via internet. Therefore, the intruders can find more ways to steal the information so it is essential to provide the security for the information.

## III. PROPOSED METHOD

The suggested approach makes use of the Local Binary Pattern (LBP), Even Bit Swapping, and Row Columnar Transposition Technique. Key generation is carried out using LBP. Even bit switching and the Row Column Transposition approach are utilized for encryption and decryption.

**Local Binary Pattern:** - The 3x3 matrix that makes up LBP has nine boxes in total. In order to produce the key, first enter the nine binary values of each letter in a word into a box. Then proceed with the Instructions below.

## IV. ALGORITHM FOR KEY GENERATION

**Step 1:** In 3\*3 matrix, center element is considered as  $x_c$  and the remaining elements are  $x_0, x_1, x_2, x_3, x_4, x_5, x_6,$  and  $x_7$ . Where the ASCII values of each element in a word can also be denoted as  $x_0, x_1, x_2, x_3, x_4, x_5, x_6,$  and  $x_7$ .

**Step2:** Evaluate each ASCII value with as  $x_c$

**Step3:** If  $x_i > x_c$ , then  $x_i$  value should be replaced with 1. (where  $i$  from 0-7)

**Step 4:** If not, substitute 0 for the value of  $x_i$

**Step5:** Write the values of the 3x3 matrix clockwise

**Step6:** Whatever we choose to be important in Step5 is the key

Finally, we obtain an eight-bit binary integer for use in the system we propose

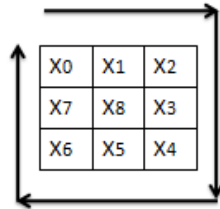


Fig-1: Local Binary Pattern

**Even Bit Swapping:** -Swapping often refers to transferring values from one object to another. The Even Bit Switching operates in a similar manner, swapping the values of every second pair of successive eight-bit numbers.

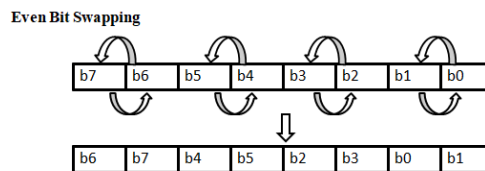


Fig-2: Even Bit Swapping

**Row Column Transposition Algorithm: -**

It is one of the best Transposition Symmetric Encryption algorithms. It contains writing plain text in row wise after that reading cipher text ascending order in column wise.

Plaint Text: encryption proces

Keyword: 4 2 1 3

4	2	1	3
e	n	c	r
y	p	t	i
o	n	p	r
o	c	e	s

Print the characters from 1 2 3 4

Cipher Text : c t p e n p n c r i r s e y o o

Fig-3: Row Column Transposition

The message is written out in row wise pattern and then read out again column by column, and the columns are chosen in ascending order. Finally, to assign the text in left to right order. Now it the cipher text.

Example: - Plaint text is encryption process

Key: - 4 2 1 3

Cipher Text is ctpenpncrirs eyoo

#### IV. ENCRYPTION ALGORITHM & FLOW CHART

Step1: - Read simple plain text

Step2: - Convert it into ASCII code

Step3: - Read corresponding binary value of

given ASCII code

Step4: - Produce the session key using LBP

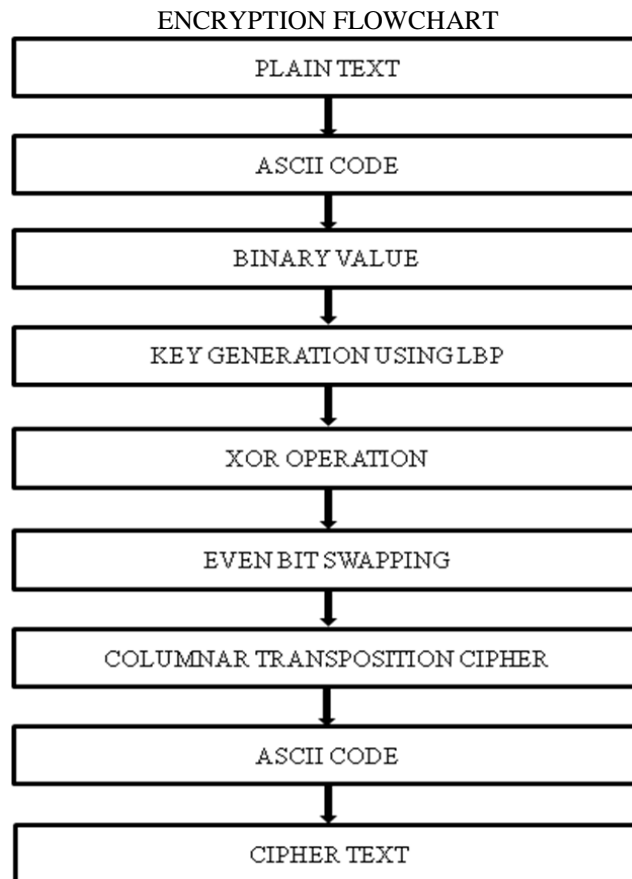
Step5: - Perform XOR operation on binary value with LBP generated key

Step6: - Compute Even bit swapping on resultant XOR operation

Step7: - Apply Row Columnar Transposition Cipher on result of Step-6

Step8: - Generate ASCII code of Row Columnar transposition Cipher

Step9: - The resultant text is a Cipher text



**VI. DECRYPTION ALGORITHM & FLOW CHART Step1: - Read cipher text**

Step2: - Convert cipher text into ASCII Code

Step3: - Generate binary values of each given ASCII code

Step4: - Apply Row Columnar Transposition Cipher on binary values

Step5: - Perform Even bit swapping result of Row Columnar Transposition Cipher algorithm

Step6: - Generate key using LBP technique

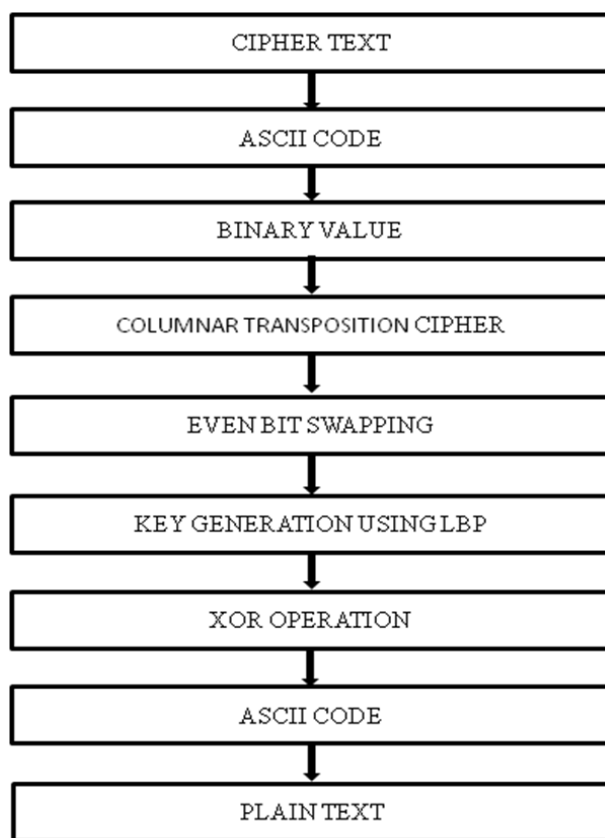
Step7: - Apply XOR operation using secret key and even bit swapping

Step8: - Generate ASCII code from result of XOR operation

Step 9: Read the plain text from the given

ASCII code

DECRYPTION FLOWCHART:



VI. RESULT TABLE

Table-I: - Encryption Table

Plain Text	Ascii Code	Binary Values	Key Generated Using LBP	X-Or Operation	Even Bit Swapping	Row Column Transposition Algorithm	Ascii Code	Encrypted Data
P	80	01010000	11111111	10101111	01011111	00000000	0	NUL
R	82	01010010		10101101	01011110	01111111	127	DEL
I	73	01001001		10110110	01111001	11111111	255	ÿ
N	78	01001110		10110001	01110010	11111101	253	ÿ
C	67	01000011		10111100	01111100	11000011	195	Ã
I	73	01001001		10110110	01111001	11011110	222	Þ
P	80	01010000		10101111	01011111	10011011	155	¸
L	76	01001100		10110011	01110011	00101011	43	+
E	69	01000101		01110101	01110101	01001111	79	o

**Table-II: - Decryption Table**

Encrypted Data	Ascii Code	Binary Values	Row Column Transposition Encrypted Algorithm	Even Bit Swapping	Key Generated Using LBP	X-Or Operation	Ascii Code	Plain Text
NUL	0	00000000	01011111	10101111	11111111	01010000	80	P
DEL	127	01111111	01011110	10101101		01010010	82	R
ÿ	255	11111111	01111001	10110110		01001001	73	I
ý	253	11111101	01110010	10110001		01001110	78	N
Ã	195	11000011	01111100	10111100		01000011	67	C
þ	222	11011110	01111001	10110110		01001001	73	I
›	155	10011011	01011111	10101111		01010000	80	P
+	43	00101011	01110011	10110011		01001100	76	L
O	79	01001111	01110101	01110101		01000101	69	E

### VII. CONCLUSION

In this proposed methodology, encryption and decryption area accomplished using the Row Column Transposition method with even bit shifting. Using these two methods will make the data highly private. The data is transformed into secure data using these two methods. The Local Binary Pattern approach, which is utilized for encryption and decryption, is employed to produce the dynamic key. Utilizing these three methods will make the data more secure, preventing data theft.

### REFERENCES

- [1]. He, H., Wu, D., & Zhao, D. (2019). Local binary pattern with six intersection points: Redefining texture description. *Pattern Recognition Letters*, 126, 118-123.
- [2]. Fischer, J., & Welschenbach, M. (2017). Columnar transposition cipher with variable key length. In *International Conference on Smart Card Research and Advanced Applications* (pp. 188-202). Springer.
- [3]. Baggili, I., & Marrington, A. (2011). Forensic analysis of columnar transposition cipher using index of coincidence and letter frequency. In *International Conference on Digital Forensics and Cyber Crime* (pp. 123-136). Springer.
- [4]. Balasubramanian, S., & Rengarajan, V. (2008). New bit permutation techniques for encryption. In *2008 IEEE Region 10 and the Third international Conference on Industrial and Information Systems* (pp. 1-6). IEEE
- [5]. Chakraborty, M., Roy, S., Datta, D., & Bandyopadhyay, S. (2013). A new approach for data encryption using columnar transposition cipher. *Procedia Technology*, 10, 481-487.
- [6]. Ullah, K., Yang, X., & Niaz, I. A. (2018). Cryptanalysis of bit-level permutation-based image encryption scheme. *Optics and Laser Technology*, 102, 171-177.
- [7]. Alqarni, A., Khalil, I., & Jantan, A. (2017). A bit-level image encryption using a chaotic key stream. *Multimedia Tools and Applications*, 76(13), 14761-14788