

Secured data transmission by using local binary pattern and even bit swapping

B. Susheel kumar¹, G. Sarvani²,

Yogi Vemana University, Kadapa,

Sri Vivekananda degree & PG college for women, Kadapa,

Submitted: 15-01-2021

Revised: 27-01-2021

Accepted: 31-01-2021

ABSTRACT: In the current scenario the exchange of data has been represented in the many aspects of the cryptography. The information exchange system consists of sender, receiver and a communication channel. Providing high quality security for the data that has been transmitted through the internet is the major aim of the cryptography. If it takes the large amount of time to get the cipher text then it is said to be secured. Several kinds of algorithms are proposed in the field of cryptography to secure the information. In this proposed method Local binary pattern method is used to generate the key and even bit swapping is used at the encryption and decryption.

KEYWORDS: Encryption, Decryption, Local Binary Pattern, Even bit swapping

I.INTRODUCTION

Cryptography plays a key role in providing security for the data with the help of secure encryption and decryption algorithms. Cryptography means converting the information from known form to the unknown form. Now a days there are various kinds of algorithms are provided for security integrity and robustness of the information that is being exchanging from the sender to the receive via the internet.

In the field of Cryptography all the encryption algorithms are comes under either the substitution or transposition approaches. Every element of the plain text is switch by the another element in the substitution approach where as in the transposition approach the plain text is reshuffled.

If all the plain text is encrypted in succession then such process is known as Block cipher. If the plain text is encrypted element by element then such process is known as Stream cipher algorithm.

Cryptography uses single key or one pair of keys to encrypt and decrypt the data. The symmetric key algorithm uses only one key at both the sender and receiver side. So that it is also called as secret or single key algorithm. On the other hand Asymmetric key algorithm uses one pair

of keys at the time of encryption and decryption. Private key at the sender side and public key at the receiver side. Private and Public are the two keys that are used in the asymmetric algorithm.

Symmetric key algorithm:

The symmetric key encryption algorithm uses single key for both the encryption and decryption. The sender and receiver must use same key. Various types of encryption processes are available in symmetric key algorithm.

The two major kinds are substitution and transposition approaches. Caesar cipher, Play fair cipher, Hill cipher, Mono-alphabetic cipher are the example techniques of substitution approach. And the Row transposition technique and Rail fence technique falls under the transposition approach.

II.BACKGROUND STUDY

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 proposed method works by using Local Binary Pattern and Even Bit swapping. LBP is used to generate the key and it consists of 3X3 table. LBP utilizes the bit position and then generate the decimal value.

Local Binary pattern for key generation

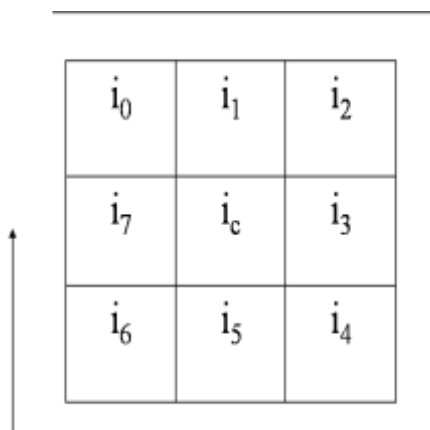


Fig 1. Local Binary Pattern

Formula to calculate the LBP is as follows

$$S = \sum (i_n - i_c) 2^n$$

Where i_c = central value

i_n = neighbour value

- If S is greater than or equal to one then the neighbour value is substituted by 1
- If S value is less than zero then the neighbour value is substituted by 0
- Then write down the values from i_0 to i_7

A. Encryption Algorithm

Step 1: Read the plain text

Step 2: Consider the ASCII codes of the plain text characters.

Step 3: Transform the ASCII code into binary value

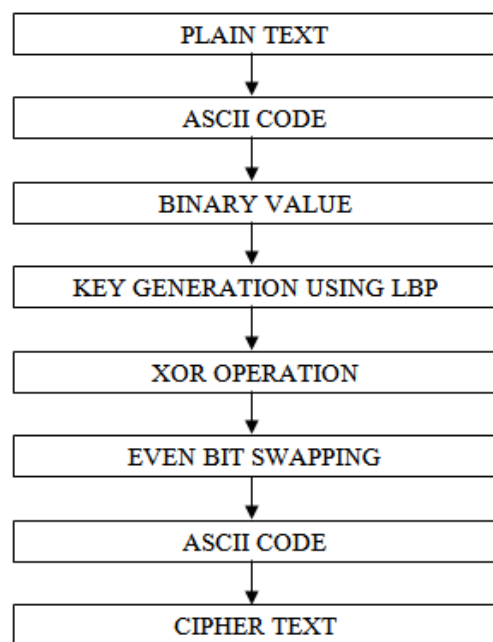
Step 4: Now generate the key by using the LBP

Step 5: After generating the key perform XOR operation with the each of the plain text character binary values.

Step 6: Now perform the even bit swapping for the resultant bits.

Step 7: Write the ASCII code for the resultant values

Step 8: Cipher text.



Flow chart of encryption process

B. Decryption Algorithm:

Step 1: Read the cipher text

Step 2: Write the ASCII codes for the given cipher text characters

Step 3: Now transform the ASCII codes into binary values.

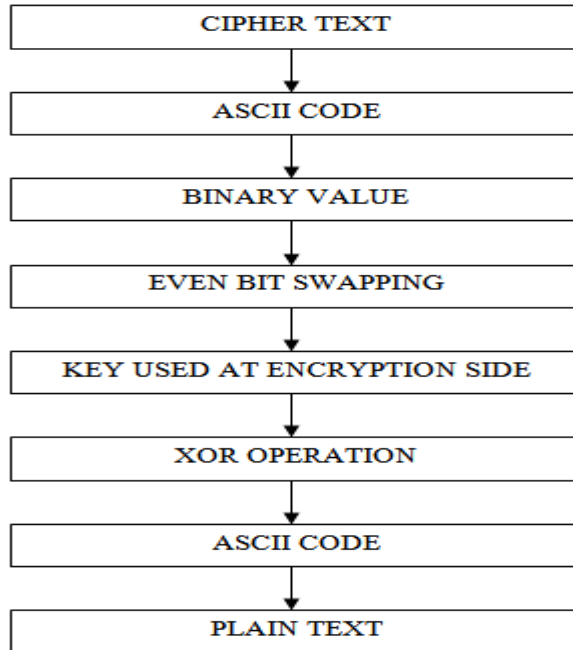
Step 4: Now perform even bit swapping for the above bits

Step 5: Consider the key that is generated at the time of encryption

Step 6: Perform the XOR operation with resultant bits obtained by performing the even bit swapping

Step 7: Transform the resultant bits into ASCII codes

Step 8: Plain text



Flow chart of decryption process

IV.RESULT TABLE

PLAIN TEXT	ASCII CODE	BINARY VALUES 1	KEY GENERATE D BY USING LBP 2	XOR OPERATION 1&2	EVEN BIT SWAPPING	ASCII CODE	CIPHER TEXT
E	69	01000101	11111111	10111010	01110101	117	U
D	68	01000100		10111011	01110111	113	Q
U	85	01010101		10101010	01010101	85	U
C	67	01000011		10111100	01111100	124	
A	65	01000001		10111110	01111101	125	}
T	84	01010100		10101011	01010111	87	W
I	73	01001001		10110110	01111001	121	Y
O	79	01001111		10110000	01110000	112	P
N	78	01001110		10110001	01110010	114	R

Encryption Table

CIPHER TEXT	ASCII CODE	BINARY VALUES	EVEN BIT SWAPPING	KEY USED AT ENCRYPTION	XOR OPERATION	ASCII CODE	PLAIN TEXT
u	117	01110101	10111010	11111111	01000101	69	E
q	113	01110111	10111011		01000100	68	D
U	85	01010101	10101010		01010101	85	U
	124	01111100	10111110		01000011	67	C
}	125	01111101	10111110		01000001	65	A
W	87	01010111	10101011		01010100	84	T
y	121	01111001	10110110		01001001	73	I
p	112	01110000	10110000		01001111	79	O
r	114	01110010	10110001		01001110	78	N

Decryption table

V.CONCLUSION:

The key generation plays an key role in the encrypting and decrypting the data. The proposed method encrypt and decrypt text using the dynamic key generated by the Local Binary Pattern, even bit swapping. By using this proposed method we can protect our confidential information from eavesdropping. The even bit swapping gives high security in non secure environment and we can prevent replay attacks from intruders.

REFERENCES:

- [1]. William Stallings, "Cryptography and Network Security: Principles and Practices", 4th Edition, Prentice Hall, 2006, page numbers 30-39.
- [2]. Hans Delfs and Helmut Knebl, "Introduction to Cryptography: Principles and Applications", Springer, first edition, 2002, page numbers 11- 14.
- [3]. Pradeep Kumar Reddy. R, Dr. Nagaraju .C "Text Encryption Through Level Based Privacy using DNA Steganography", International Journal of Engineering Trends and Technology in Computer Science (2278-6856), Volume 3, Issue 3, May- June 2014.
- [4]. Dániza C. Morales Berrios, "A Parallel Bit Reversal Algorithm and It's CILK Implementation," Computing Research Conference (CRC 1999), University of Puerto Rico, Mayagüez Campus, 1999.



**International Journal of Advances in
Engineering and Management**
ISSN: 2395-5252



IJAEM

Volume: 03

Issue: 01

DOI: 10.35629/5252

www.ijaem.net

Email id: ijaem.paper@gmail.com