A Novel Strategy to Enhance Security through Retro Bit Method

Mr.Sundar
Asst.Prof, Department of Computer Science and Engineering,Velammal Engineering College, Surapet, Chennai.
Arul Mozhi Varman. G.
Department of Computer Science and Engineering,Velammal Engineering College, Surapet, Chennai.
TVishaal. B
Department of Computer Science and Engineering,Velammal Engineering College, Surapet, Chennai.

ABSTRACT

The existing method in majority of cryptography methods uses LSB method.In that method the least significant bits in the end will be eliminated and the Encrypted message will be placed in that removed place and the LSB method willhave large pixel expansion while used in steganography.So, the process becomes complicated and the process has been in existence for a long time and it is also very prone to attacks,so we provide a new method for Encryption.This method we have used is called retro bit method, it doesn't work based on LSB method and this will be the first method to perform this kind of Encryption technique based on t9 keyboard.The alphabets will be mapped on to the position of the numbers on the keyboard and will be scrambled across it according to the key provided.The main strength of this technique lies in the key.The key generated by the sender will be secretly sent to the receiver and it is also efficient enough.

Keywords - **LSB(Least Significant Bit),T9 keyboard.**

I. INTRODUCTION

Cryptography, or the art and science of Encrypting sensitive information, was once exclusive to the realms of government, academia, and the military. However, with recent technological advancements, cryptography has begun to permeate all facets of everyday life.Everything from your smartphone to your banking relies heavily on cryptography to keep your information safe and your livelihood secure. The existing method in majority of cryptographymethodsuses LSB method.In that method the least significant bits in the end will be eliminated and the Encrypted message will be placed in that removed place and the LSB method will be having large pixel expansion while used in steganography.In the system we proposed we will Encrypt message into a new method we named as Retro Bit Method.The project's aim is that to change the existing Encryption technique to be more efficient. It follows the T9 keyboard in older phones and maps the messages into its positions accordingly to the alphabets.If the Encryption method is successful, this can also be further developed to use on an Image and other medias.

II. MOTIVATION

2.1 Enhance Security system

LSB is the one that eliminates the least bit zeros and replace it with Encrypted message is more complicated , outdated and it is also prone to attackers.There are situations where So the process becomes complicated and the process has been in existence for a long time and it is also very prone to attacks,so we provide a new method for Encryption.this will be the first method to perform this kind of Encryption technique based on t9 keyboard.Thus, this system developed in this paper provides the necessary solution for this problem.

III. ALGORITHM

Step1: Get the text to be encrypted from the user

Step2: Initiate the numeric digits present in the T9 keyboard
to the respective letters in the text

Step3: Swap the assigned numeric digits by the respective
opposite digit after one digit

Step4: Convert the swapped numeric digits into letters in the
T9 keyboard respectively

Step5: Put the alphabets in matrix form from one to twenty
five eliminating the least used letter

Step6: Map the matrix to another identical 5X5 matrix
containing digits one to twenty-five

Step7: Take the Coordinates of the digits in the alphabetical
matrix corresponding to the letters in the Message
matrix.

Step8: Get a public key from the user and modulo it with the
predefined private key

Step9: Take the modulus value and retrieve the every
corresponding value in the array position followed by
the remaining values

Step10:The encrypted message is obtained

IV. PROPOSED SYSTEM

In the system we proposed we will Encrypt message into a new method we named as Retro Bit Method.Retro bit method follows the T9 keyboard in older phones and maps the messages into its positions accordingly to the alphabets.If the Encryption method is successful, this can also be further developed to use on an Image and other medias. This method can to change the Existing Encryption technique to be more efficient.

V. TECHNOLOGIES USED

Python is used to achieve integrated learning and develop skills for producing high quality software applicable to research and design of advanced level projects. Python is an interpreted and multipurpose high-level programming language created by Guido Van Rossim. During the last years it has become one the most used languages for software development. Python can be used in various operating systems and platforms, such as Windows, Mac OS X, Linux, smartphones, and embedded systems.

VI. SYSTEM OPERATIONALDESCRIPTION

Our system is depicted in Figure 11.

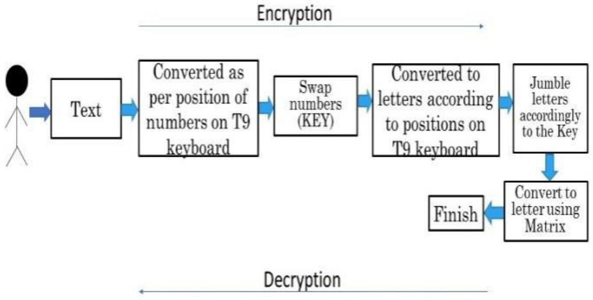
Encryption
Text
Converted as per position of numbers on T9 keyboard
Swap numbers (KEY)
Converted to letters according to positions on T9 keyboard
Jumble letters accordingly to the Key
Convert to letter using Matrix
Finish
Decryption

Fig 11: Block Diagram.

Retro Bit method follows the T9 keyboard in older phones which maps the letters in the messages to be Encrypted into the keys of the T9 keyboard respectively. The mapped text will be converted into digits according to the numbers present in the standard T9 keyboards. The message which has been mapped into the T9 keyboard and converted into digits will be buffered aside,Then the numbers will be swapped accordingly to the default positions in it. The swapped letters will be swapped accordingly a method known as Jump over five method which involves the digits jumping over the number five and then plotting the number on it. For number 5 it will be swapped to the number 0 and for other digits it will be swapped according the next number jumping over a digit. Then the converted letters will be again plotted to the positions on the T9 keyboard. After that the Encrypted text will be then jumbled according tothe text. After that the letters will be converted accordingly to the Matrix form. From the Matrix form all the alphabetical letters will be plotted to the all the Twenty-Five Empty positions. Then from the Twenty-Five positions the coordinates will be noted then the taking the coordinates into account new Encrypted Text will be noted down. Now the Encrypted Text will be jumbled in a random form. From the Jumbled Text the numbers will assigned from zero to twenty-five numbers to get the Desired Result.

VII. CONCLUSION & FUTURE WORK

The Retro bit method is a light weight method to process the Encryption method.This will be future in future in future as it is Light weight and it can be Multiplied N-number of times.The process is Light Weighted so it can be easily used in mobile phones and other hand-held devices as it will not consume much processor power.This can further be multiplied any number of times due to its flexibility in Concept.This method can also be used to map pixels on to an Image and the whole process and can be easily implemented on to an Image.

VIII. ACKNOWLEDGEMENT

The authors thank the department of Computer Science and Engineering for providing grant to conduct this research work.

REFERENCES

[1] Color image steganography using Sha-512 and losslesscompression. *Article in international journal of imaging and robotics.*

[2] Bailey k, Currank (2006) *an evaluation of image-based steganography methods. Multimer tools appl* 30:55-88

[3] Muhammad k, ahead j, Rehman nu Jan z, Qureshi rj (2015) a secure cyclic steganographic technique for color images using randomization technical journal uet Taxila, Pakistan 19(3):57-64

[4] *Critical analysis of cryptography and steganography- IEEEpublication*.

[5] *A survey on image cryptography using lightweight Encryption algorithm- IEEE publication.*

[6] *Color image steganography using LSB multi-bit embedding process- IEEE publication.*

[7] W. Stallings, Cryptography and Network SecurityPrinciples and Practice, E NJ: Prentice-Hall, 2016

[8] Ali Al-Haj, GheithAbandah, Noor Hussein, "Crypto-based algorithms for secured medical image transmission", *IET Information Security*, vol. 9, no. 6, pp. 365-373, Nov. 2015.

[9] Tan, C. Ng, X. Xu, C. Poh, L. Yong, K. Sheah, "Security protection of DICOM medical images using dual-layer reversible watermarking with tamper detection capability", *Journal of Digital Imaging*, vol. 24, no. 3, pp. 528-540, 2011.

[10] X. Zhang, "Separable reversible data hiding in encrypted image", *IEEE Trans. Inf. For. Security*, vol. 7, no. 2, pp. 826-832, 2012.

[11] X. Guo, T. Zhuang, "A region-based lossless watermarking scheme for enhancing security of medical data", *Journal of Digital Imaging*, vol. 22, no. 1, pp. 53-64, 2009.