IOSR Journal of Computer Science (IOSR-JCE)
e-ISSN: 2278-0661, p-ISSN: 2278-8727
PP 43-46
www.iosrjournals.org

Efficient TIMG Algorithm for Secure Transmission of Data

Sujeet More[1], Mohammed Mujeeb Arab[2]
Asst. Prof, Dept of Computer Science
Shaikh College of Engg and Technology, Belgaum
[1]sujeetmore7@gmail.com
[2]mujeeb017@gmail.com

Abstract--- *Cryptography is the process where an individual or message sending by party to other individual such that only the authorize party will get the scrambled message, which will be unscrambled to get the original message. In the public network hacking is the biggest problem. Many existing encryption algorithms like DES, 3DES, AES, and RC6 have been used to protect different-different types of attacks to eavesdrop or prevent the data to be communicating to the end-user safely. In this paper, a new encryption algorithm for transfer of data is proposed to achieve the different goals of security i.e., Integrity, Availability, and Confidentiality. This new TIMG algorithm is based on combination of two algorithms. The results show better efficiency compared to different existing algorithms.*

Keywords--- *Decryption, Encryption, Key generation, Pixel, Security, TIMG Algorithm.*

I. INTRODUCTION

The people have to be assured that the information to be read by only the sender and receiver. The basic need to provide security is using cryptography. In our work we are combining neural network and cryptography. Cryptography is often seen as an art something other understand but this is need. These of course need not the case at all. Cryptography is security engineering technique where it is used mathematics. It provides us with the tools that underlie most modern security approaches. It is the key driven technique for protecting information. Cryptography is the science of writing in secret code and is an ancient art. There are a number of security concerns in a dynamic and agile context; especially data confidentiality is regarded as on of the most fundamental issues. There are various cryptosystem dominating the area of information security and one of them is symmetric key algorithm. In this symmetric key algorithm, same secret key is used for encryption & decryption which is only known by sender and receiver of exchanged message and keep confidential to other irrelevant entities.

At present various encryption algorithms have been proposed & widely used such as DES, IDEA, RSA, AES etc. Most of which are used for text & binary data. The secrecy of the message will be protected well when key is kept confidential. Since wireless devices is equipped with battery as their power supply, they have limited computational capabilities and one of them main concern is energy saving. But it cannot be achieved if the encryption & decryption is applied on the complete message. As a result an efficient pixel encryption algorithm is the potential solution to save power for wireless devices and at the same time to sufficiently protect the data. In this article we mainly study how to encrypt pixels, as it is selective approach to conserve time of data transmission and energy of network.

Through applying this method our proposed scheme enhances the features of pixel encryption and avoiding the relevance between different messages. Thus we present the solution for the issue of applying traditional symmetric key algorithm along with pixel encryption for data protection in dynamic environment, such as MANET, WANET etc. The paper is divided in five sections. Section 1 presents introduction about cryptography, Section 2 presents proposed work, Section 3 presents implementation algorithm Section 4 presents results and Section 5 presents conclusion and future work.

II. PROPOSED WORK

Using cryptography the hackers can know that there is some data is transferring. So that, they can modify the data during the message transfer. In order to overcome this we are proposing a model. In our model we are using a combined technique. Using combined technique we can hide the original message in a hidden format. So that the hacker even cannot expect that there some message present in it. Firstly we embed original data into an image using TIMG algorithm. This message is transferred in network. At destination we retrieve the data from image. At stream case if hackers try to get the data, it becomes tedious job to encrypt the message.

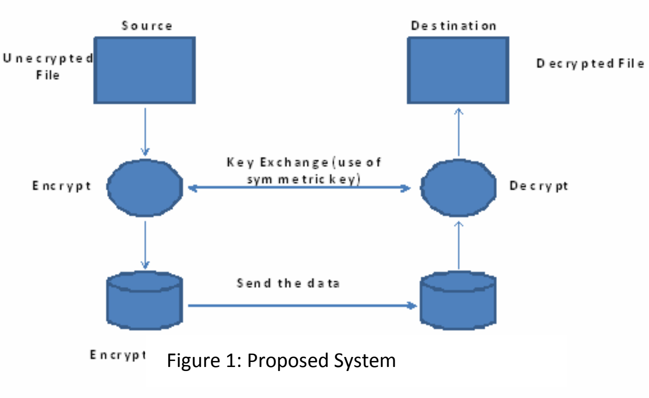
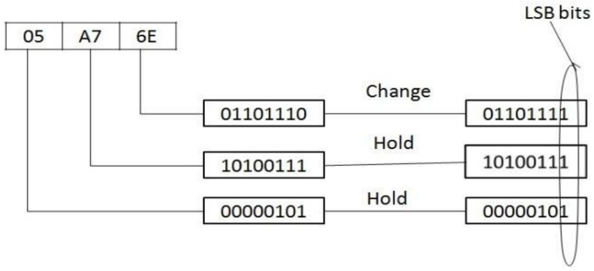


Figure 1: Proposed System

In computer terminology the ASCII value are used for each of the alphabet or anything, which intern is converted to its binary value while processing. Each pixel holds a bit value which can be encrypted/ decrypted, so using this concept we proposed an algorithm to encrypt and decrypt the messages.



The simplest approach to hiding data within an image file is called least significant bit (LSB) insertion. In the LSB insertion method we can take a binary representation of hidden data and overwrite the LSB of each byte within the cover image. In a computer, images are represented as arrays of values. These values are represented by three colors R (Red), G (Green), and B (Blue), where value of each color described a pixel. Each pixel is combination of three components (R, G, and B). For example, suppose one can hide a message in three pixels of an image (24-bit colors). Suppose the original three pixels are:

(10010101 00001101 11001001)
(10010110 00001111 11001010)
(10011111 00010000 11001011)

A TIMG algorithm could hide the letter "A" which has a position 65 into ASCII character set and have a binary representation "001000001", by altering the set of 9 bits over the LSB of the 9 bytes above; we get the following three pixels (where bits in bold have been changed):

(1001010**0** 0000110**0** 11001001)
(10010110 0000111**0** 11001010)
(1001111**0** 00010000 11001011)

We have successfully hidden 9 bits but at a cost of changing only 4 bits or roughly 50%of the LSB.

III. IMPLEMENTATION ALGORITHM

1. Embedding phase

Embedding secret text message in image will have following steps:
Step 1: Read the message.

Step 2: Read the pixel from Original image.
Step 3: Break the pixel into RGB color component.
Step 4: One LSB bit of first color component replace by one bit of message.
Step 5: Do the same process for next seven bit.

2. Text Encryption Algorithm

Step 1: Generate the ASCII value of the letter.
Step 2: Generate the corresponding binary value of it. [Binary value should be 8 digits e.g. for decimal 32 binary number should be 00100000].
Step 3: Reverse the 8 digit's binary number.
Step 4: Take a 4 digits divisor (>=1000) as the Key.
Step 5: Divide the reversed number with the divisor.
Step 6: Store the remainder in first 3 digits & quotient in next 5 digits (remainder and quotient wouldn't be more than 3 digits and 5 digits long respectively. If any of these are less then 3 and 5 digits respectively we need to add required number of 0s (zeros) in the left hand side. So, this would be the cipher text i.e. encrypted text. Now store the remainder in first 3 digits & quotient in next 5 digits.

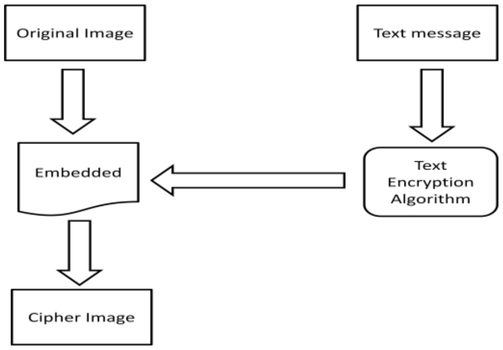


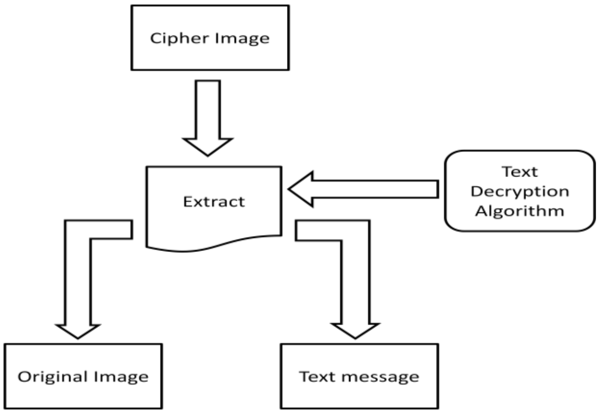
Figure 2: Embedding Phase

3. Extraction phase

Extraction of text message from embedded image will have following steps:
Step I: Read the pixel from Cipher image.
Step II: Break the pixel into color component.
Step III: Extract bit from the color component to make character.
Step IV: Obtain the plain text.

4. Text Decryption Algorithm

Step 1: Multiply last 5 digits of the cipher text by the Key.
Step 2: Add first 3 digits of the cipher text with the result produced in the previous step.
Step 3: If the result produced in the previous step i.e. step 2 is not an 8-bit number we need to make it an 8- bit number.
Step 4: Reverse the number to get the original text i.e. the plain text.



IV. RESULTS

Figure 3: Extraction Phase

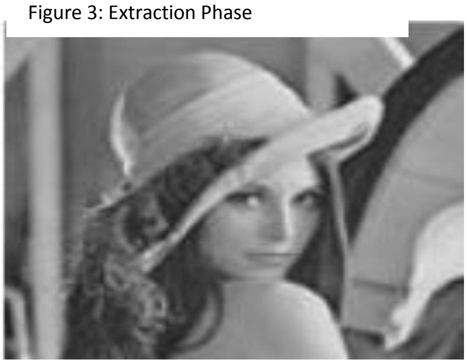


Figure 4: Original Image of "Lena:

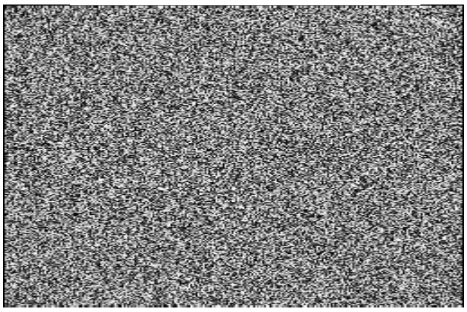


Figure 5: Encrypted Image

V. CONCLUSION

Cryptography is used to achieve few goals like Confidentiality, Data integrity, Authentication etc. of the send data. Now in order to achieve these goals various cryptographic algorithms are developed by various people. For a very minimal amount of data those algorithms wouldn't be cost effective since those are not designed for small amount of data. The aim of this work was to design and implement a new (TIMG) algorithm to address these issue so that we don't have to apply complex algorithms (which are not cost-effective) to encrypt a small amount of data.

In future we would like to concentrate of more secured technique for text encryption for video encryption in real time, so that wireless networks gain a high efficiency in security issues.

REFERENCE

[1] A.Cheddad, J. Condell, K. Curran, P.M. Kevitt,"Digital image steganography: Survey and analysis of current methods", Elsevier Journal Signal Processing, vol. 90, Issue3, pp. 727–752, March 2010.

[2] Data Hiding and Retrieval : Asoke Nath, Sankar Das, Amlan Chakraborty, published in IEEE Proceedings of International Conference on Computational Intelligence and Communication Networks(CICN 2010) held from 26-28 NOV' 2010 at Bhopal.

[3] Advanced Steganography Algorithm using encrypted secret message: Joyshree Nath and Asoke Nath, International Journal of Computer Science and Applications, Vol-2, No. 3, Page- 19-24, Mar (2010).

[4] New Steganography algorithm using encrypted secret message: Joyshree Nath, Meheboob Alam Mallik, Saima Ghosh and Asoke Nath : Proceedings of Worldcomp 2011 held at Las Vegas (USA), 18-21 Jul, 2011.

[5] W. N. Lie and L. C. Chang." Data hiding in images with adaptive number of least significant bits based on the human visual system." Proc. ICIP '99, 1:286–290, 1999.

[6] S .K. Moon and R.S. Kawitkar, "Data Security using Data Hiding," International Conference on Computational Intelligence and Multimedia Applications, vol. 4, pp. 247- 251, 2007.

[7] X. Yi, C. Tan, C. Siew, S. Rahman,"Fast encryption for multimedia," IEEE Transactions on Consumer Electronics, Feb. 2001, Vol. 47, No. 1, pp. 101 – 107.