ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 5, Issue 5, May 2017

Image Authentication Using Cryptography and Steganography in Network Security

Deepak Shailendra Singh[1] , Prof. Mrunali Metri[2]

PG Student, Dept.of MCA, NCRD's Sterling Institute of Management Studies, Navi Mumbai, India[1]

Assistant Professor, Dept. of MCA, NCRD's Sterling Institute of Management Studies, Navi Mumbai, India[2]

ABSTRACT: In this paper, a new approach of information security is discussed .two level data security in Network system .Using Cryptography and Steganography. Blowfish and List significant Bit (LSB) are used for data security in Network System Confidential .information is encrypted by BLOWFISH algorithm, and then encrypted data hide into image and Message by LSB algorithm .For more security we used Finger image of authorized person to hide encrypted data.The keys required for BLOWFISH algorithm is generated from same Finger image.In the result of project contain memory utilization, processing time for encryption data and decryption data etc. In this project gives more secure for embedded systems .

KEYWORDS: network security,Blowfish,Cryptography,Steganography ,embedded system,list significant bit.

I. INTRODUCTION

Cryptography and Steganography both algorithm can use to totally change the information in order to cipher or hide their existence respectively.These techniques have a lot of application in computer science and other related fields[1]. They are used to protect our gmail message etc.Cryptography scrambles a information so it cannot be understood means no none able to read any message ; the Steganography hides the information so it cannot be seen.A Stegnography System thus hidden content in unremarkable cover so as not to arouse an suspicion .For example it is possible to embedded a text inside an image .

One such and new technique, an algorithm called Blowfish, is perfect for use in the embedded systems for hiding data. we have very secure methods for both cryptography and Steganography – AES(Advanced Encrytion Standard) algorithm is a very secure method and technique for cryptography and the Steganography methods is good for use Least significant bit, are highly secured[2].Using Cryptography and Steganography methods are used for data security over the network The aim and objective of this project describe a lot method using crytography and steganography together using images and message processing System able to perform at the same time

Finger is considered to be the most trusted and unique feature of the person. Because finger is unique for each people Hence this project proposes a data encryption technique using Finger biometric. Finger images are taking from Finger biometric database.

II.LITERATURE REVIEW

KamaleshB.Waskar,UttamL.Bombale(Electronics and Teleomm.., Bharati College of Engineering, Kolhapur, India)
Rahul Yadav(Department of Computer Science, SRM University, NCR Campus, Ghaziabad, Uttar Pradesh, India)
:=> After reviewing all papers I come to main point related to my field very small work has been added. in field of making secure communication between two parties third party not able to take data. This review has helped me greatly in identifying our problem for proposed project work, which has been discussed . this paper I am using biometric

DOI: 10.15680/IJIRCCE.2017. 0505325

system . For example finger image is unique for human body. Third party people not able to hack the data easily . Because hackers cannot hack their biometric features . Finger Biometric Cryptography for Identity particular Document”, this paper present generate a unique and secure key from finger template. The finger images are processed to produce finger template or code to be utilized for the encryption and decryption tasks. Same like message system sender send the message to the receiver by using encryted format . Third party people not understand that message.

III.PROBLEM DEFINATION

“Finger Biometric Cryptography for Identity Document”,. AES is a symmetric-key algorithm, meaning the same key is used for both encrypting and decrypting the identity data.
The New Approaches for Secured Image Using Steganography Techniques and Type Conversions” This paper give information about Cryptography and Sreganography Network Security.[1]

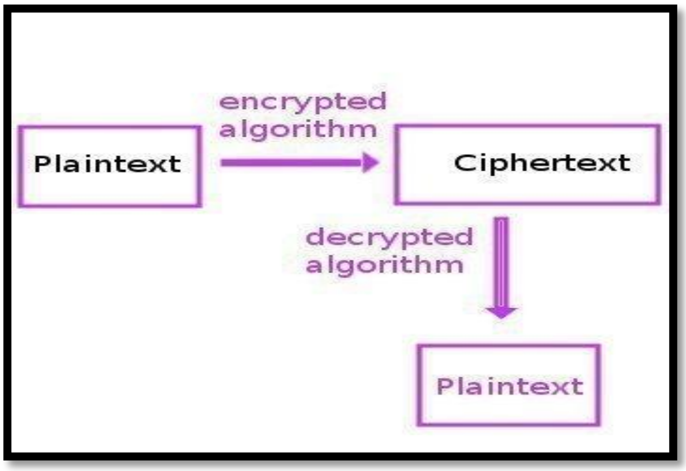
This paper introduces two way provide security wherein cryptography and Steganography are combined to encrypt the data as well as to hide the encrypted data in another medium so the fact that a message being sent is concealed.

Cryptography :

Cryptography concerns with keeping communication private. It scrambles a message or plain text into cipher text, so it cannot be understood. This process is called Encryption and again convert it into a plain text at the receiver hand, the reverse process is called Decryption

What is ciphertext :

Ciphertext is encrypted **text**. Plaintext is what you have before encryption, and **ciphertext** is the encrypted result. Cipher text is known as encrypted data or encoded information because it contains a form of the original plaintext that is unreadable by a human or computer without the proper cipher to decrypt it.



- **NOTATION:**

Notation for relating plaintext, ciphertext, and key
C=Ek(P),
Where, C is cipher P is plaintext, K is key.
P = DK(C) represents of decryption of C to get the plaintext again.
So,DK **(Ek (P)) = P**

Steganography:

Steganography hides the existence of a message (information). So it cannot be seen easily. Data can be hidden in a popular object that will not attract any attention like images, audio or video objects which can be represented in binary format(1 or 0), and at the receiver hand this hidden information can be extracted, from the image or any other object in which information is hidden.

There are a main approaches to hide the data in these objects, these are:- LSB (Least Significant Bit)
Some important to note that while cryptography is necessary or more efficient and provide for secure communications no one able to catch proper information , it is not able to itself sufficient for crytography . There are some specific and unique security requirements for cryptography, including Authentication properly.

Proposed Technique AES algorithm for Cryptography:

Advanced Encryption Standard is a symmetric encryption **algorithm**. This algorithm support in both hardware and software, therefore this algorithm very useful in cryptography and supports a block length of 128 bits and key lengths of 128, 192, and 256 bits

Advantages of Using AES Algorithm

- AES is more secure
- AES is faster in both hardware and software.

OBJECTIVE & SCOPE

Combine both techniques i.e. CRYPTOGRAPHY and STEGANOGRAPHY and an extra security module to get a very highly secure system for data hiding . So that if any intruder extracted the data, it will be encrypted.

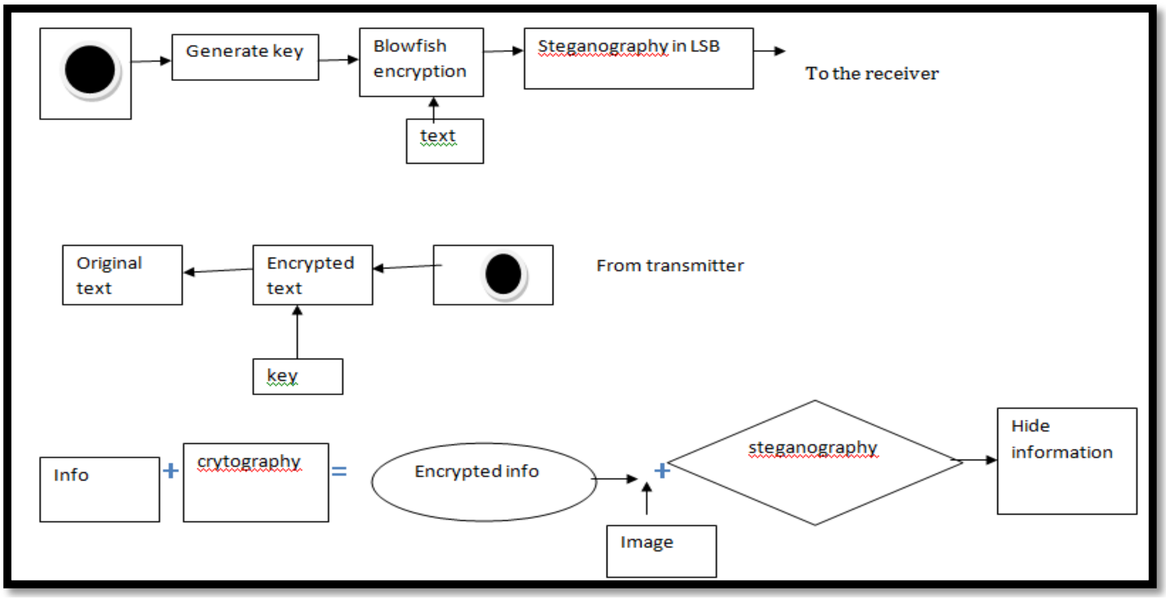
IV.METHODOLOGY

There are many different encryption and decryption algorithms Now a days . are being proposed to provide security to such data.

All of these algorithms depend on a user’s key which he uses as the key for encryption. But these keys may be hicker, hike only feature or data of a person that hicker cannot hick their biometric features, hence this proposed project consider finger image of a user to generate secrete key for encryption.

For security, only encryption may not be enough, hence proposed project include combination of both cryptography and Steganography. The encrypted data hide into the image(finger image) and then image is transmitted in the network.

- Block Diagram
-



Generated key from finger image, we have taken only finger part of hand of person for more security.
Key length is 128 bits. Using Blowfish algorithm for encryption, the confidential information is encrypted.

Cryptography =Text + Key
This encrypted text then hides into every pixel of finger image.
Steganography =Text + Image
finger image is transmitted to receiver side, hidden data removed from image and using same encrypted key, original data recovered from encrypted text

- **Image Definition**

To a computer, an image is a collection of numbers that areas of the image .
Most images on the internet consists of a rectangular map of the image's pixels (represented as bits) where each pixel is located and its color . That color represented by RGB format These pixels are displayed horizontally row by row.[1]
An image is a picture that has been created or copied and stored in electronic form. An image can be described in terms of vector graphics or raster graphics. An image stored in raster form is sometimes called a bitmap.

Least Significant Bit

There are Many advantages of using LSB as a steganographic method.
Least Significant Bit (LSB) is a simple to implement steganography.Because LSB is a part of all steganographic methods, it embeds the data into the cover so that it cannot be detected by a casual observer. steganography is to make use of LSB of picture's pixel information. This technique works best when the file is longer than the message file and if image is grayscale. When applying LSB techniques to each and every byte of a 24 bit image,three bits can be encoded into each pixel.
-> 24-bit color: each and every pixel can have one in 2^24 colors, and also these are represented as different quantities of three basic colors: red , green , blue ,(RGB) given by 8 bits (256 values) each.
->8-bit color: every pixel can have one in 256 (2^8) colors, chosen from a palette, or a table of colors.

Least Significant Bit (LSB)-Based Substitution

- 240(Information) can be hidden in the first eight bytes of three pixels in a 24 bit image.
- PIXELS

(00100111 11101001 11001000)
(00100111 11001000 11101001)
(11001000 00100111 11101001)
240: 011110000 (in binary)

- Result

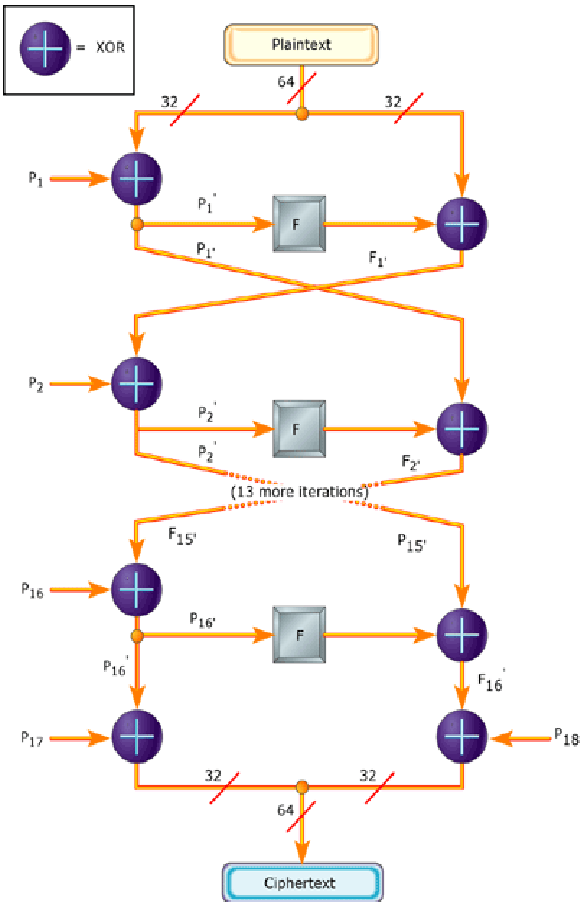
(00100110 1110100111001001)
(00100111 11001001 11101000)
(11001000 00100110 11101000)

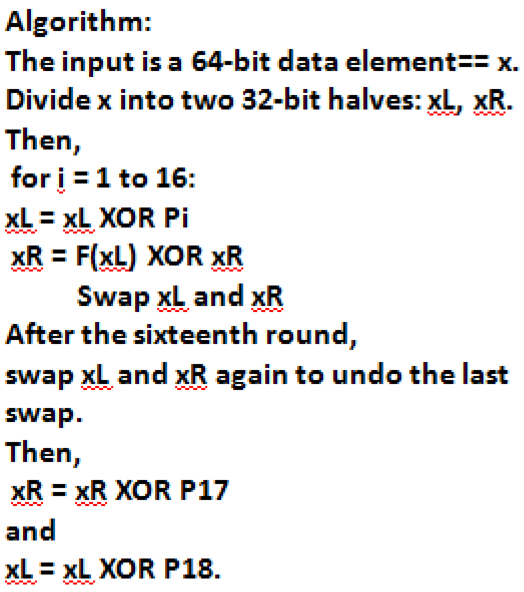
Number 240 is embedded into first eight bytes and only 6 bits are changed. Result contains information (240), in the pixels of the image.

Blowfish

Blowfish is symmetric block cipher can be used to drop-in replace for DES(Data Encryption Standard) or IDEA(International Data Encryption Algorithm) . It take a variable-length key pair, from 32 bits to 448 bits.

Blowfish is a symmetric encryption algorithm, meaning that uses same secret key to both side encrypt and decrypt messages.





```
Algorithm:
The input is a 64-bit data element== x.
Divide x into two 32-bit halves: xL, xR.
Then,
 for i = 1 to 16:
xL = xL XOR Pi
 xR = F(xL) XOR xR
        Swap xL and xR
After the sixteenth round,
swap xL and xR again to undo the last
swap.
Then,
 xR = xR XOR P17
and
xL = xL XOR P18.
```

V.LIMITATIONS & FUTURE SCOPE

Now a day, I often listen a popular term“Hacking”. Hacking is nothing but an unauthorized and unknow people to access of data which can be collected at the time of data transmission.
When transmit the data one place to other place third party member easily get the data. But sender and receiver don't know who can hacking my data.
In future, the most important and efficient use of steganographic techniques will probably be lying in the field of digital watermarking. digital watermarks provide tracking the owners of these materials
digital watermarking software and services that allow webmasters and copyright owners to imbed information within graphics and audio files that can be used to identify the owner's rights to these works
Currently we are using LSB algorithm for steganography and AES for cryptography, in future we can combine cryptography and steganography, by using there other secure algorithms like ECC (Eliptic curve cryptography).

VI.CONCLUSION

In this project we have presented a new system for the combination of cryptography and Steganography using LSB algorithm, and an extra security module.
Steganography, combined with cryptography, is a become too powerful tool which enables people to communicate without possible eavesdroppers even knowing there is a form of communication in the first place.
The main advantage of this Cryptography and Steganography method used for encryption and decryption , AES, is very secure and the LSB Steganography techniques are very hard to detect.
Most confidential finger image of person because finger image is unique for each people consider for Steganography, so when finger image with hidden text is on network, and if hackers hack this image, then it is too difficult to catch the hidden data because finger image is unique identity for person, there is no another same image can be generated or captured. So this is the advantage.

REFERENCES

[1] Pallavi H. Dixit, Kamalesh B. Waskar, Uttam L. Bombale , " Multilevel Network Security Combining Cryptography and Steganography on ARM Platform ".
[2] RAHUL YADAV," MESSAGE SECURITY USING CRYPTOGRAPHY AND LSB ALGORITHM OF STEGANOGRAPHY"
[3] Padmashree G, Venugopala P S ,"Audio Stegnography and Cryptography: Using LSB algorithm at 4th and 5th LSB layers "
[4] Mr . Vikas Tyagi*1, Mr. Atul kumar2, Roshan Patel3, Sachin Tyagi4," IMAGE STEGANOGRAPHY USING LEAST SIGNIFICANT BIT WITH CRYPTOGRAPHY "
[5]Shraddha G. Kokate ,Ranjit R Keole,"Non Repudation protocol in network security"

BIOGRAPHY

Deepak Shailendra Singh is a Post Graduate Student Of Master Of Computer Application Department, College of NCRD's Sterling Institute Of Management Studies, Mumbai University.

Prof.Mrunali Metri is a Assistant Professor in Master Of Computer Application Department, College of NCRD's Sterling Institute Of Management Studies, Mumbai University.

DOI: 10.15680/IJIRCCE.2017. 0505325