iJRASET
International Journal For Research in Applied Science and Engineering Technology

# INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

**Volume:** 5 **Issue:** III **Month of publication:** March 2017

**DOI:** http://doi.org/10.22214/ijraset.2017.3026

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

Volume 5 Issue III, March 2017
ISSN: 2321-9653
International Journal for Research in Applied Science & Engineering Technology (IJRASET)

# A Review on Security of Data Using PGP Algorithm along with Steganography

Vikas Kumar Ratre[1], Utkarsh Kumar Jha[2], Washim Akhtar[3], Miss. Roshni Rathour[4]
[1,2,3]Student( 7th Sem-CSE), [4] Assistant Professor , Dept. Of CSE
New Govt. Engineering College, Raipur, Chhattisgarh, India

***Abstract:*** ***Now a day due to rapid increase in number of internet user's data security is one of the prime concerns of internetwork communication. Several techniques have been evolved to prevent data from unauthorized access. Two fundamental types of security measures used frequently now days are "Cryptography" and "Steganography" .This project make use of both methods to achieve high security for transmission of data in internetwork communication. This project provide data security by using encryption method PGP and then concealing encrypted data into digital information using robust & secure LSB steganography method to provide high level security.***
***Keywords****: Include at least 5 keywords or phrases*

## I. INTRODUCTION

Information security is based on three principles Confidentiality, Integrity and Availability of the communication channel. This trio is termed as CIA of information network security. Where "Confidentiality" refers to hiding of sensitive information from any unauthorized person, "Integrity" refers to the insured data and "Availability of the communication channel" signifies the availability of information as when needed by the concerned user.

To achieve this, most of the information networks make use of security tools such as "cryptography" and "Steganography". The word Steganography is originated from two Greek words "steganos" meaning "concealed or protected" and "graphein" meaning "writing". Steganography is a process of "embedding information such as image, audio, video or file within another information as file, image, audio, video". Whereas Cryptography was taken from two Greek words "kryptos" meaning "hidden or secret" and "graphein" meaning "writing". Although "Steganography" is said to be the broad study of Cryptography, they both share different objectives. Here goal of "Cryptography" is to "convert information into unreadable form for such that no third party can read" and "Steganography" is referred to as "Hiding of sensitive information into some other information such that the presence of information is completely invisible or unnoticeable". Today steganography is commonly used on computers with digital data being the carriers and networks being the high speed delivery channels.

Combination of both cryptography and steganography result in a better security mechanism which enhances privacy in a communication over a network.

## II. IMAGE STEGANOGRAPHY

It's the most common type of steganography in which data is hidden inside an image so that it looks just like an ordinary image for the man in the middle .In this process a random picture is chosen by the sender and by using certain algorithm secret message is integrated into this image and then it is passed to the receiver and at the receivers end message is extracted by the receiver

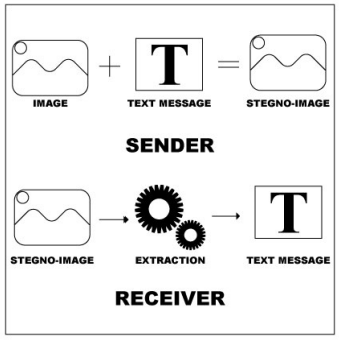



Fig: working of steganography

Volume 5 Issue III, March 2017
ISSN: 2321-9653
International Journal for Research in Applied Science & Engineering Technology (IJRASET)

## III. SECURE LSB ALGORITHM

The best known "Steganography" method that is based on spatial domain is the LSB(least significant bit).This method replaces the list significant bit of a data unit(pixel in this case) to hide the data. List significant bit method uses the last bit of each pixel of the cover image to hide the information i.e. last bit of each pixel color is replaced with the relative bits of the information to be stored in the cover-image. This method has been implemented in several aspects to improve the algorithm. One of the aspects is to hide the information in last bit of any singe color among the three (i.e. red, green and blue) of the pixel of provided cover image.

This paper proposes an improved version of this selective LSB algorithm to improve the robustness of data hidden in the sego-image by designing an algorithm the filters the selection of pixel of the cover-image to hide information. This algorithm will generate a linear equation that will produce output a set of selected pixel, this pixel set will then be used to store data in each of them as serialized. The biggest disadvantage of this method is that it will limit the size of data that can be hidden inside the cover image. To overcome this problem this Robust Selection LSB algorithm will use the 3 least significant bits of the selected pixel of a destined color. This will generate large payload capacity to hide larger data. The strength of this method is its robustness that is very resistant to attacks. .

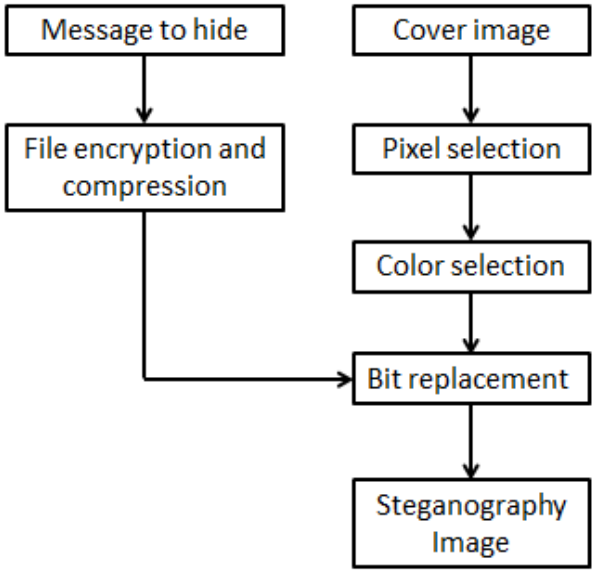



Fig. 1: LSB algorithm

### *A. Architectural Design of Robust Selective LSB Algorithm.*

This architectural design possesses the following steps:
Randomization algorithm for pixel selection.
Hiding image in only in single color.

### *B. Randomization Algorithm for Pixel Selection*

In this algorithm each end i.e. sender and receiver both have a password oriented stego-key that will generate pseudo-random number. This random number will be used as an input for the linear equation to generate set of selected pixel.

### *C. Randomization Algorithm for Pixel Selection*

LSB algorithm for information hiding is achieved by hiding one bit of information in least significant bit of each color of pixel, resulting in leap difference of 65793 colors in the scale of color between original pixel color and newer pixel color.

The more efficient way to introduce less distortion would be by replacing the 3 bits of a single color from the pixel, i.e. for example if a message say "111" is to be hidden inside a pixel with value 11001101 10100011 10011011 (R G B) and the selected color is blue then, the final pixel value will be given as:

11001101 10100011 10011011
11001101 10100011 10011111.

Here the colour leap from the original colour is only 1 .This statistics shows that this method provides lesser distortion in colour of pixel.

## IV. ASYMMETRIC KEY CRYPTOGRAPHY

In this type of cryptography we have two keys one is known as public key which is used by receiver to encrypt message and another key is known as private key used by receiver to decrypt the message encrypted using public key
RSA algorithm is a kind of asymmetric key cryptography

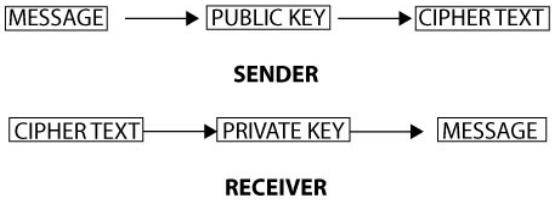



Fig. 3: Asymmetric key cryptography

## V. PRETTY GOOD PRIVACY

It is an encryption program created by Philip Zimmermann in 1991 used to provide privacy as well as authentication; it's based on public key cryptography.
Encryption of message can be time consuming so PGP uses a better algorithm In which firstly we encrypt message using short key which takes less time as compared to encryption via receivers public key and then after encrypting message using a shorter key we encrypt that short key using receivers public key then the message and the encrypted short key is sent to the receiver and at the receivers end decryption of shorter key is done via his private key and the whole message is decrypted using the shorter key derived in previous step thus we can say that it's a combination of conventional cryptography as well as public key cryptography
Uses RSA, DSS or Diffie Hellman for public key encryption, CAST128 IDEA or 3DES for symmetric key encryption and SHA-I for hash coding and ZIP compssion strategy is used for compression

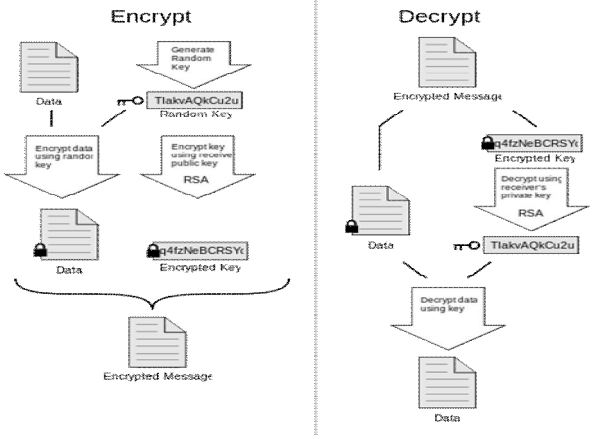



Fig 4: PGP algorithm working

## VI. CONCLUSION

Steganography is a science of hiding data inside another type of carrier and cryptography adds security as well as authenticity to the message so by combining these two methodologies we can achieve elite security and use of PGP along with the LSB provides ease of hiding data along an aid to overcome drawbacks of LSB steganography and this method aims at causing least alteration in resultant image and due to compression mechanism in PGP help us in achieving this.

## VII. ACKNOWLEDGMENT

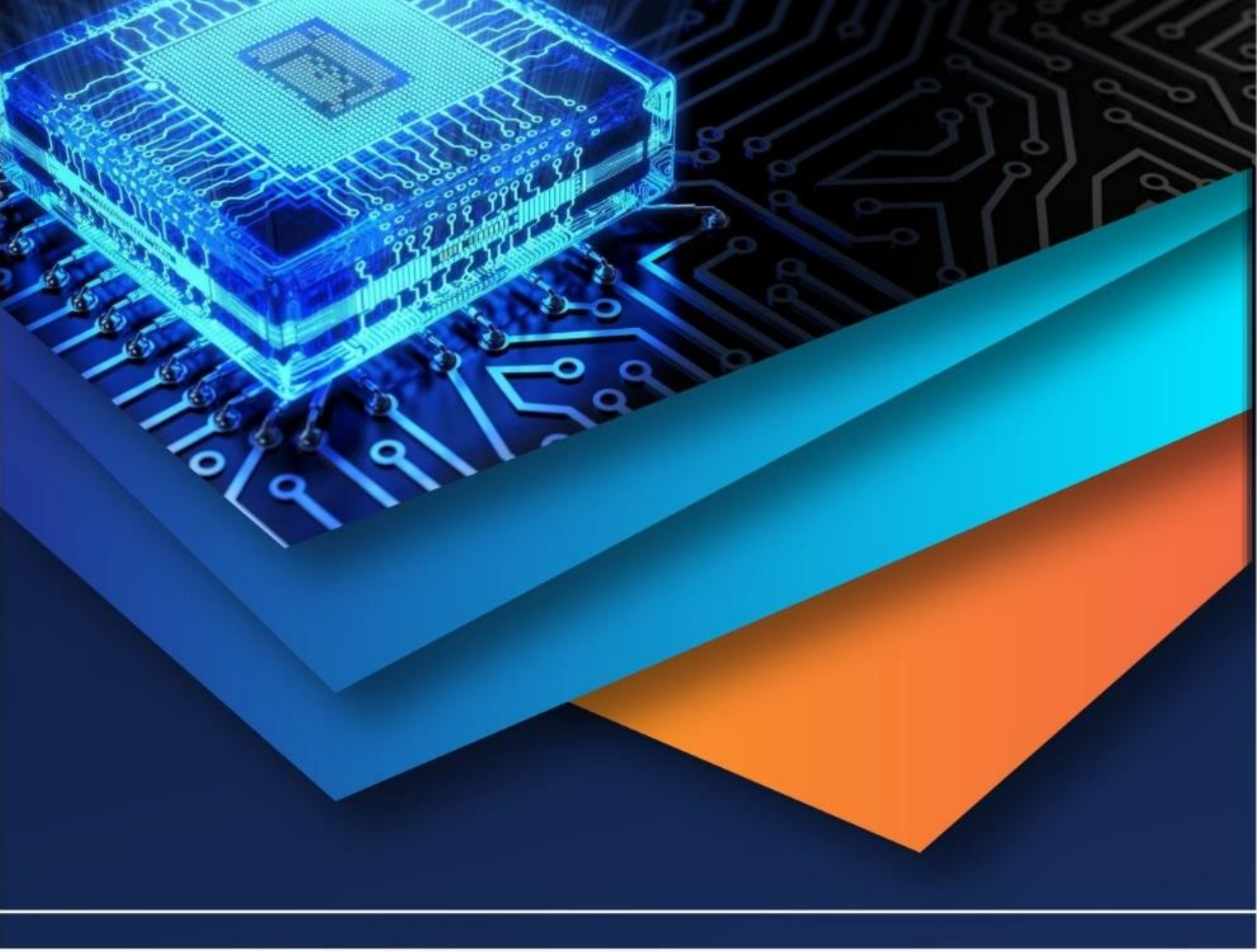
This work was carried out during may 2016 to march 2017 at the former Govt. Engineering College, Sejbahar, Raipur, at the Department of Computer Science and Engineering. I owe my deepest gratitude to my supervisor Professor in CSE Department, Miss. Roshni Rathour. Without her continuous optimism concerning this work, enthusiasm, encouragement and support this study would hardly have been completed. I also express my warmest gratitude to my colleagues Utkarsh Jha and Washim Akhtar who

suggested this topic to me. I am deeply grateful to Professor Dr. R.H.Talwekar, Head of the Department of Comp. Science and Engineering, for making it possible to carry out this work in their departments

## REFERENCES

[1] Champakamala .B.S, Padmini.K, Radhika on "Least Significant Bit algorithm for image steganography"
[2] Sarita Poonia, Mamtesh Nokhwal, Ajay Shankar on "A Secure Image Based Steganography and Cryptography with Watermarking"-2013
[3] Amandeep Kaur, Rupinder Kaur, Navdeep Kumar on "A Review on Image Steganography Techniques"-2015
[4] D. Atkins, W. Stallings P. Zimmermann on "PGP Message Exchange Formats"-1996
[5] Venkata Sai Manoj on paper "CRYPTOGRAPHY AND STEGANOGRAPHY"
[6] T. Morkel , J.H.P. Eloff , M.S. Olivier on "an overview to image steganography"-200
[7] A Cheddad, J Condell, K Curran, P Mc Kevitt on "Digital image steganography: Survey and analysis of current methods
[8] Ashitosh S. Thorat, Prof. Dr. G. U. Kharat on "STEGANOGRAPHY BASED NAVIGATION OF MISSILE"
[9] Mr. Vikas Tyagi on "Data Hiding in Image using least significant bit with cryptography"



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

# INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY