MESSAGE SECURITY USING PGP WITH TWO STAGE STEGANOGRAPHY

Pronab Kumar Adhikari
Assistant Professor, Ajay Kumar Garg Engineering College, Ghaziabad, UP, India
adhikaripronab@akgec.ac.in

Abstract- **Communicating confidential information is a matter of concern in information technology as with the rapid growth of communication technologies it also continues to create challenges for information security. When communication is taking place in between parties that are within the same private network, the threats to the information security are significantly low. But now a day, in the modern globalized world where it is not always possible to stay within the same private network. In such scenario where the communicating parsons are spatially separate, the security of confidential information cannot depend only on the current technologies, and additional security mechanisms should be implemented. Internet is one of the most commonly used public infrastructures utilized for communication between two geographically separated remote users. E-mail is mostly used on internet platform for information sharing. However, being a public platform internet is the most vulnerable to security breaches; this is one major disadvantage of using internet for using email services. There are two techniques that are used for E Mail security. First is PGP and second is S/MIME. The research work emphasis on PGP only. PGP is a service that provides five types of services to give the security on emails. They are as: Authentication, Confidentiality, Compression, E Mail Compatibility and Segmentation. The research work concentrates on Authentication and Confidentiality services. There were some security issues in above services of existing PGP. This research work improves these services. We are using symmetric key and two stage secure steganography**

Keywords: *Information Security, Cryptography, Steganography, PGP, Watermarking, LSB*

I. INTRODUCTION

Now a day Computer and Internet have significant role in our daily life. They handle all types of transaction, confidential information, data and files etc. Hence it is very important to provide security to a computerized information system in order to attain the applicable objectives of maintaining the confidentiality, availability and integrity of information system resources (includes software, hardware, firmware, and data.) [1]. Security of confidential information cannot depend only on the current technologies, and additional security mechanisms should be implemented. Cryptography and Steganography are two technological solution to provide securities to confidential messages over an unsecure channel. Cryptography was introduced as technological solution which hides the confidential data in an unreadable format to be communicated over an insecure physical channel such that an unauthorized person finds it unable to read whereas Steganography is the technology of hiding a message in such a way that the presence of the hidden message is unknown to any eavesdropper.

When our concern is to provide security to email, Pretty Good Privacy is a program that is intended to help to make electronic mail more secure. It does this by using sophisticated techniques known as public key encryption. It is a strong encryption mechanism that protects emails by scrambling them such that it cannot be read by anyone without having the key. It also allows one to digitally “sign” the messages so that it can be verified that a message was actually sent. PGP is largely based on asymmetric encryption. In asymmetric encryption every user has two keys: one is public key and the other is private key that must be kept secret [3]. The privacy of the asymmetric key used is crucial for secure use of PGP. If an attacker gets PGP symmetric key, he can read a single message. But anyhow if attacker breaks the PGP asymmetric key all encrypted documents or messages of the past, present and future may be compromised. Therefore, it is of utmost importance for the PGP users to select a crypto algorithm that is proven to be strong, secure and immune to cryptanalysis.

II. LITERATURE SURVEY

INFORMATION SECURITY:

Generally, security means the quality or state of being secure and to be safe from danger. Security can be categorized into different layers depending on the type of content intended to be secured:

- **Personal security:** It is characterized as the security of those people who are formally approved to access private data about the organization and its activities.
- **Physical security:** It defines all the requisites that are needed to protect the data or objects physically from an unauthorized intrusion.
- **Operational security**: It mainly concerned about the assurance of the data identified with a specific task from the series of exercises.
- **Communication security:** The correspondence’s security incorporates the security issues with respect to

organizations communication media, technology and content.

- **Network security:** The network security is responsible for safeguarding the information regarding the networking components, connections and contents.
- **Information security:** Information security is defined as the protection of information along with the systems and hardware that use, store, and transmit that information. Information security can be defined as measures adopted to prevent the unauthorized access or modification of data or capabilities.

III. SECURITY THREATS AND ATTACKS

1. **Interruption**: Hackers can interrupt the data before reaching the destination.
2. **Interception**: Hacker can gain access to email traffic and other data transfers.
3. **Modification:** Altering or replacing of valid data that is needed to send to the destination.
4. **Fabrication:** Hacker or unauthorized person inserts the unauthorized objects by adding records to the file, insertion of spam messages etc.

IV. CRYPTOGRAPHY

The word cryptography is derived from two Greek words which mean “secret writing”. It is the process of scrambling the original text by rearranging and substituting the original text, arranging it in a seemingly unreadable format for others. It provides an effective way to protect the information that is transmitting through the network communication paths. It is responsible for sending the messages secretly and securely to the destination [2].

Cryptographic Algorithms: There are many cryptographic algorithms available which differ on their type of encryption. Based on the type of encryption standards the algorithms are grouped into two types:

Symmetric encryption algorithm: The symmetric encryption algorithm generally uses the same key for encryption and decryption. The security level for this type of encryption will depend on the length of the key.

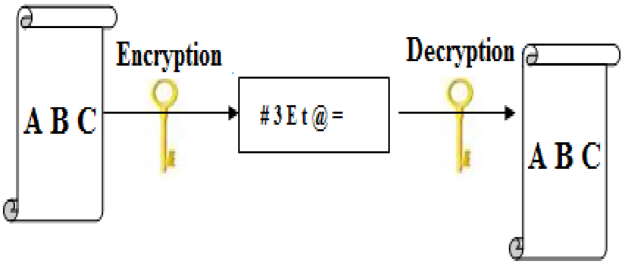


Figure 1-Symmetric Encyryption.

The different symmetric encryption algorithms are-

1. Data Encryption Standard,
2. Advanced Encryption Standard

ii. Asymmetric encryption algorithm: In asymmetric encryption, the encryption and decryption will be done by two different keys.

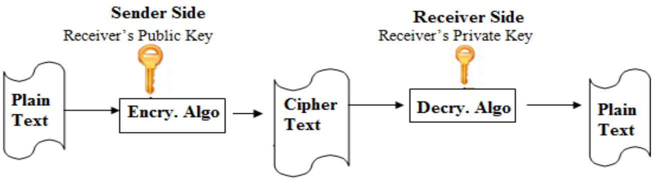


Figure 2-Asymmetric Encyryption.

E-MAIL SECURITY

The protection of email from unauthorized access and inspection is known as electronic privacy. There are two mechanisms for E Mail Security as PGP and S/MIME.

Pretty Good Privacy (PGP: It is a data encryption and decryption that provides cryptographic privacy and authentication for E Mail communication. PGP is often used for signing, encrypting, and decrypting texts, e-mails, files, directories, and whole disk partitions and to increase the security of e-mail communications. It was created by Phil Zimmermann in 1991 [3]. PGP uses a cryptographically strong hash function on the plaintext that user is signing. This generates a fixed- length data item known as a message digest. (Again, any change to the information results in a totally different digest). Then PGP uses the digest and the private key to create the signature. It transmits the signature and the plaintext together. Upon receipt of the message, the recipient uses PGP to recompute the digest, thus verifying the signature.

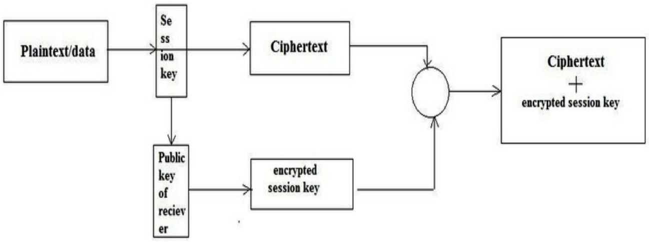


Figure 3-PGP Encryption Working

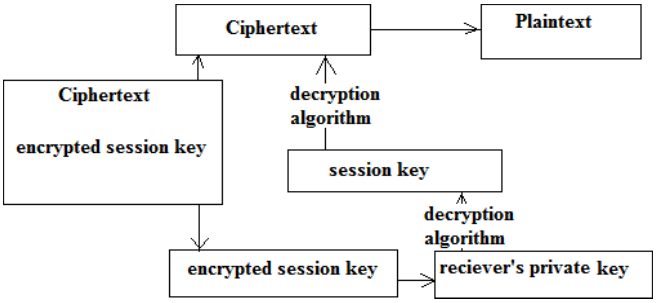


Figure 4-PGP Decryption Working

STEGANOGRAPHY

Steganography is the technology of hiding a message in such a way that the presence of the hidden message is unknown. The presence of the hidden message is known only to the recipient of the message. In steganography the messages that need to be hiding can be injected into other digital file that is called as cover file. In other words, purpose of steganography can be explained as “the aim of steganography is to go incognito i.e. if no attention is drawn to the hidden message then steganography has achieved its goal”.

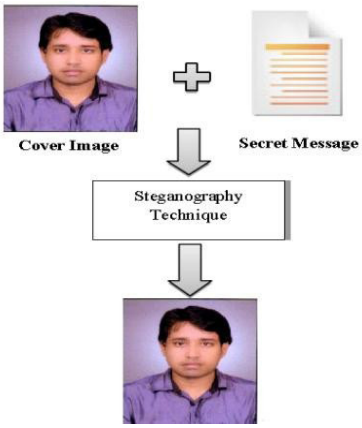


Figure 5-Implementing Steganography

V. PROPOSED WORK

There were some security issues in the existing PGP. We use public key cryptography in PGP for encryption and decryption. For this RSA Algorithm is used. As we know that both the keys of public key method are dependent on each other. The public key of each user is known to all other users in the network. So, there may be the chance in which any opponent can try to find the private key of the sender depending on its known public key. This problem of existing PGP is eliminated in our proposed research work. Now we’ll use symmetric key instead of asymmetric key. The sender will generate a unique key for each user in the network. This unique key is provided to the receiver by using two level secure stereography. This two-level stereography is achieved by following manner: the secret key is hiding behind an image and further this image is password protected and the password is again hidden behind an image to provide two stage secure stenography. Both the images are then sent to the receiver.

This research work includes:

1. To improve Authentication
2. To improve Confidentiality
3. To improve the Compression
4. To implement with e-mail

The first two improvements are done by using symmetric key cryptography and two stage steganography. The compression part is improved by improving the conventional LZ78 Algorithm. The improvement is achieved by converting the concatenate message (original message + encrypted hashed message) into radix 16 format.

VI. IMPLEMENTATION

Implementation of Proposed Algorithm We use LSB algorithm. LSB is the most popular Steganography technique. It hides the secret message in the RGB image based on it its binary coding. LSB algorithm is used to hide the secret messages by using algorithm LSB makes the changes in the image resolution quite clear as well as it is easy to attack [7]. In LSB steganography, the least significant bits of the cover media’s digital data are used to conceal the message. The simplest of the LSB steganography techniques is LSB replacement. LSB replacement steganography changes the last bit of each of the pixel values to reflect the message that needs to be hidden. Consider an 8- bit grayscale bitmap image where each pixel is stored as a byte representing a gray scale color value. Suppose the first eight pixels of the original image have the following gray color values:

01010010
01001010
10010111
11001100
11010101
01010111
00100110
01000011

To hide the letter Z whose binary value of ASCII code is 10110101, we would replace the LSBs of these pixels to have the following new values:

01010011
01001010
10010111
11001101
11010100
01010111
00100110
01000011

Note that, on average, only half the LSBs need to change. The difference between the cover (i.e. original) image and the stego image will be hardly noticeable to the human eye. However, one of its major limitations is small size of data which can be embedded in such type of images using only LSB. LSB is extremely vulnerable to attacks. LSB techniques implemented to 24-bit formats for the color image are difficult to detect contrary to 8-bit format.

VII. RESULT

We implemented proposed work in C# using .NET. Here we are using SHA – 1 for message authentication. Two

Stage secure steganography is used with PGP to provide authentication, confidentiality and compression services. The implementation is shown in figures.

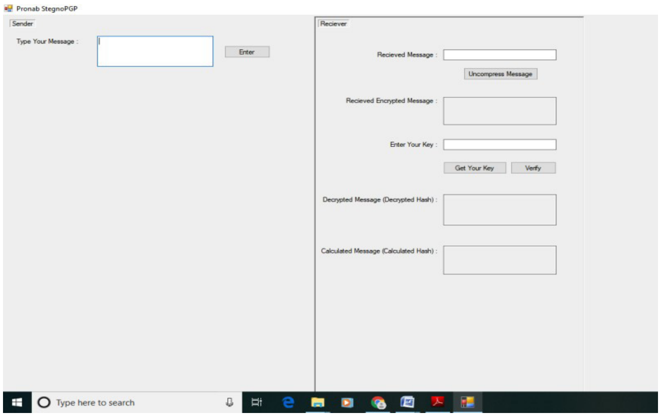
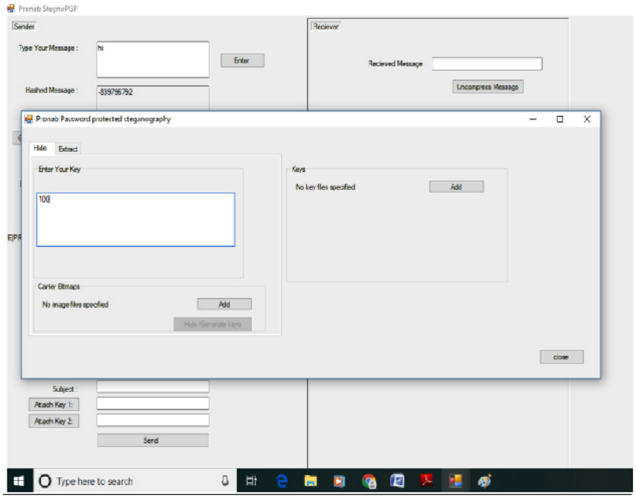


Figure 6-Initial View of the Application



Type Your Message : hi

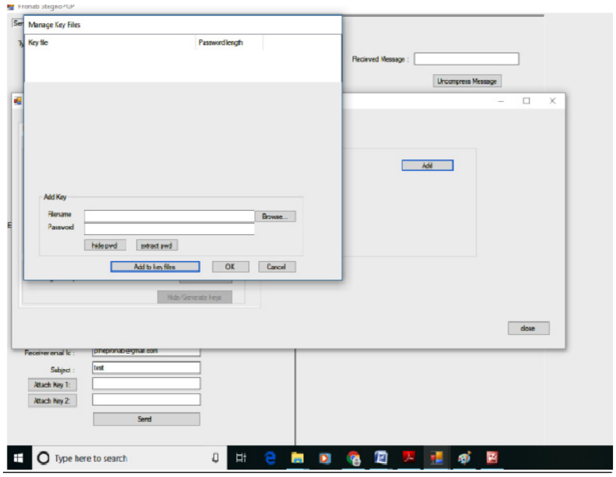
Hashed Message : -839796792

100

No key files specified

No image files specified

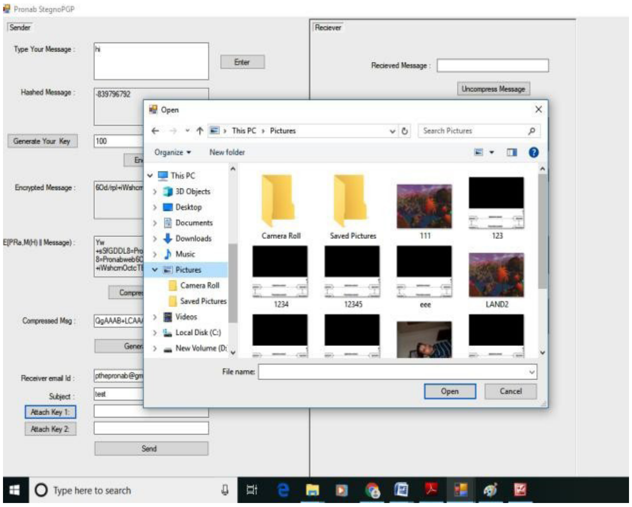
Figure 7-Stage-One Steganography (Hiding secret key with the image file)



Receiver email Id : pthepronab@gmail.com

Subject : test

Figure 8-Stage-Two Steganography (Password key hiding in another image)



Type Your Message : hi

Hashed Message : -839796792

100

Encrypted Message : 6Od/ipl+Wshcm

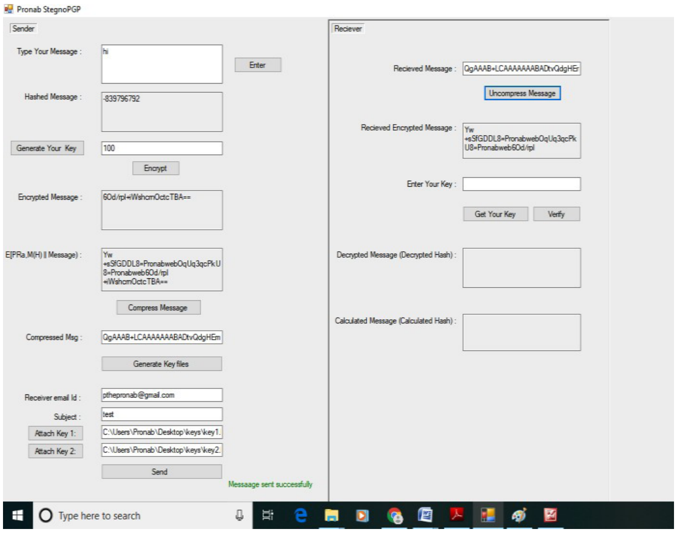
E[PRa,M(H) || Message) : Yw +sSfGDDL8=Pro 8=Pronabweb6O +WshcmOdcT

Compressed Msg : QgAAAB+LCAA

Receiver email Id : pthepronab@gm

Subject : test

Figure 9-key files are attached along with email



Type Your Message : hi

Hashed Message : -839796792

Generate Your Key : 100

Encrypted Message : 6Od/ipl+WshcmOdcTBA==

E[PRa,M(H) || Message) : Yw +sSfGDDL8=PronabwebOqUq3qcPkU 8=Pronabweb6Od/ipl +WshcmOdcTBA==

Compressed Msg : QgAAAB+LCAAAAAAAABADvQdgHEm

Receiver email Id : pthepronab@gmail.com

Subject : test

Attach Key 1: C:\Users\Pronab\Desktop\keys\key1.

Attach Key 2: C:\Users\Pronab\Desktop\keys\key2.

Message sent successfully

Recieved Message : QgAAAB+LCAAAAAAAABADvQdgHEr

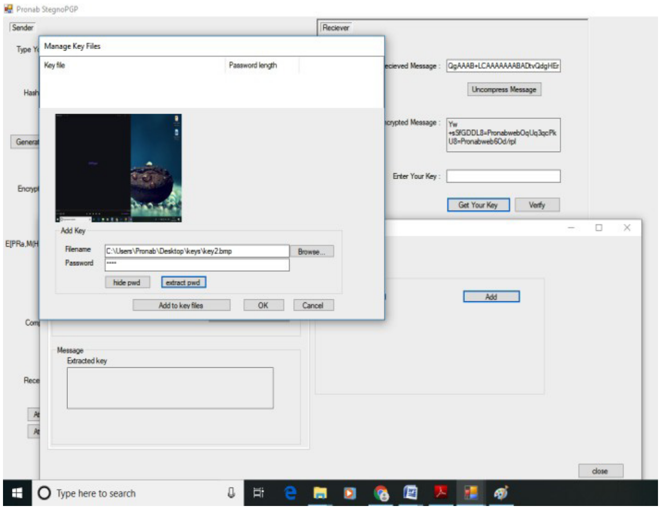
Recieved Encrypted Message : Yw +sSfGDDL8=PronabwebOqUq3qcPk U8=Pronabweb6Od/ipl

Enter Your Key :

Decrypted Message (Decrypted Hash) :

Calculated Message (Calculated Hash) :

Figure 10-Uncompressing message at the Receiver side



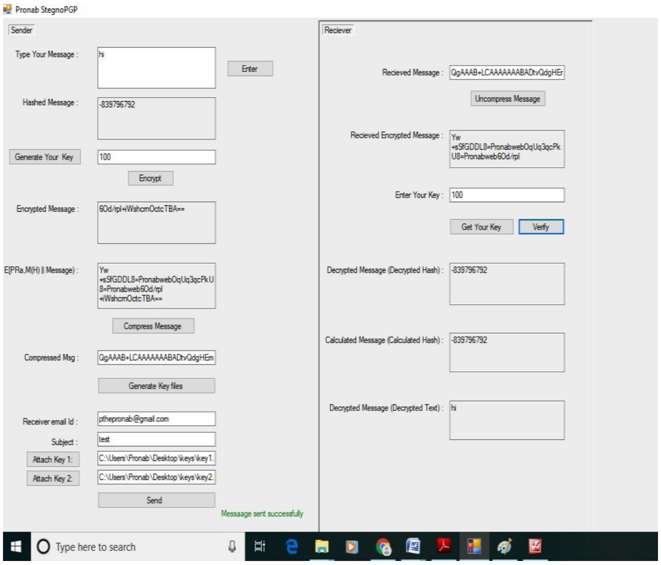
Filename C:\Users\Pronab\Desktop\keys\key2.bmp

Password ****

Recieved Message : QgAAAB+LCAAAAAAAABADvQdgHEr

Recieved Encrypted Message : Yw +sSfGDDL8=PronabwebOqUq3qcPk U8=Pronabweb6Od/ipl

Figure 11-Extracting keys at the receivers' side



Pronab StegnoPGP

Sender

Type Your Message : hi

Hashed Message : -839796792

Generate Your Key : 100

Encrypted Message : 6Od/rpl+iWshcmOctcTBA==

E[PRa,M(H) || Message) : Yw +sSfGDDL8=PronabwebOqUq3qcPkU8=Pronabweb6Od/rpl +iWshcmOctcTBA==

Compressed Msg : QgAAAB+LCAAAAAAABADtvQdgHEm

Receiver email Id : pthepronab@gmail.com

Subject : test

Attach Key 1: C:\Users\Pronab\Desktop\keys\key1.

Attach Key 2: C:\Users\Pronab\Desktop\keys\key2.

Messaage sent successfully

Reciever

Recieved Message : QgAAAB+LCAAAAAAABADtvQdgHEr

Recieved Encrypted Message : Yw +sSfGDDL8=PronabwebOqUq3qcPkU8=Pronabweb6Od/rpl

Enter Your Key : 100

Decrypted Message (Decrypted Hash) : -839796792

Calculated Message (Calculated Hash) : -839796792

Decrypted Message (Decrypted Text) : hi

Figure 12-Authentication and Confidentiaity verification with successful decryption

VIII. CONCLUSIONS

This new approach of PGP provides more security. By changing the architecture of PGP from Asymmetric to Symmetric and using two stages secure stereography to secure the shared key from opponents make the existing PGP more secure. Changing architecture makes PGP more secure because of reducing the chance of finding the original secret key because now there is no concept of private key and public key so intruder can't find private key from public key in any way because there doesn't exists any relation between them. Every receiver knows only its own key which is generated by sender for him. If attacker keen to know key he has to face difficulty because he doesn't know in which image the key which he wants is hidden. And if he gets any chance to get that image a similar type of problem arises again because of hidden key used for getting the original key from image and this key is again hidden in another image and attacker have to find it again which is a very difficult task. So, by changing the architecture of existing PGP makes it simpler and use of stegnography at various levels makes it more secure.

REFERENCES

[1] Johnson, N.F. Jajodia, S. & Duric, Z., 2001. Information hiding: steganography and watermarking – attacks and countermeasures. Kluwer academic publishers.

[2] N Borisov, I Goldberg, E Brewer,"Off-the-record communication, or, why not to use PGP", ACM workshop on Privacy, 2004, dl.acm.org

[3] Domenico Daniele Bloisi , Luca Iocchi ,Image based steganography and cryptography", Conference: VISAPP 2007: Proceedings of the Second International Conference on Computer Vision Theory and Applications, Barcelona, Spain, March 8-11, 2007 - Volume 1

[4] E. Cole, Hiding in Plain Sight: Steganography and the Art of Covert Communication, Indianapolis: Wiley Publishing, 2003.

[5] Grover, D., 2001. Data Watermarking: Steganography and Watermarking of Digital Data. Computer Law & Security Report, 17(2), pp.65-67.

[6] Made Sudarma, Dandy Pramana Hostiadi, "Implementation of Email Security using PGP at Zimbramail Server", IJCSI International Journal of Computer Science Issues, Volume 13, Issue 6, November 2016 ISSN (Print):1694-0814 | ISSN (Online): 1694-0784

ABOUT THE AUTHOR

Pronab Kumr Adhikari B.Tech, M.Tech, (Assistant Professor at AKGEC, India, publish 4 paper in international journal and also member of IEEE, IET, IFERP and research area in computer network.