Volume 3, Issue 12, December 2013 ISSN: 2277 128X

International Journal of Advanced Research in Computer Science and Software Engineering

Research Paper

Available online at: www.ijarcsse.com

Stegno PGP with Enhance Security

Suni Awasthi[1]
M.Tech, Computer Science and Engg.
Kanpur Institute of Technology,
Kanpur, India

Praveen Tripathi[2]
Assitt. Prof.,CSE Deptt
Kanpur Institute of Technology
Kanpur, India

Akhilesh Kosta[3]
Assitt. Prof., CSE Deptt.
Kanpur Institute of Technology
Kanpur, India

Abstract - In recent years cryptography become very popular science. It is the procedure, process and method of making and using secret writing as codes or ciphers. Steganography is an art and science of hiding information within other information. "Steganography" is a Greek origin word which means "hidden writing". Steganography word is classified into two parts: Steganos which means "secret or covered" (where you want to hide the secret messages) and the graphic which means "writing" (text). PGP (Pretty Good Privacy) is a data encryption program created by Phil Zimmermann in 199. PGP has grown to become a de facto standard for encrypting e-mail and is widely used by home users, corporate and government offices worldwide. It uses public key cryptography to encrypt and decrypt files and messages so only those who are intended to read a message can read it [1]. In existing PGP system, Asymmetric Encryption is used due to which there may be chance of attack in data transmission. We proposed a new scheme StegnoPGP with Enhance Security to overcome such attacks. In this research paper, we introduce the concept of two stage secure stegenography in PGP.

Keywords: Steganography, Cryptography, PGP, Watermarking, LSB.

I. INTRODUCTION

In the Steganography system scenario, before the hiding process, the sender must select the appropriate message carrier (i.e image, video, audio, text) and select the effective secret messages as well as the robust password (which suppose to be known by the receiver). The effective and appropriate Steganography algorithm must be selected that able to encode the message in more secure technique. Then the sender may send the Stego file by email or chatting, or by other modern techniques. The Stego file is the carried message with the secret information. After receiving the message by the receiver, he can decode it using the extracting algorithm and the same password used by the sender [2].

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 software that enables us to protect our email and files by scrambling them so others cannot read them. It also allows you to digitally "sign" the messages in a way that allows others to verify that a message was actually sent.PGP is largely based on asymmetric encryption. In asymmetric encryption every user has a pair of keys: one is public and the other is private and must be kept secret [3]. The strength of the asymmetric key used is crucial to the secure use of PGP. If an attacker can break a PGP symmetric key they will be able to read a single message. However, if an attacker is able to break the PGP asymmetric key all encrypted documents or messages of the past, present and future may be compromised. Therefore it is very important that the public key algorithm PGP users select is proven to be strong, secure and immune to cryptanalysis.

II. LITERATURE SURVEY

The word cryptography comes from the Greek words κρυπτο (hidden or secret) and γραφη (writing). It is the art of secret writing. The basic service provided by cryptography is the ability to send information between participants in a way that prevents others from reading it. It includes the protocols, algorithms and strategies to securely and consistently prevent or delay unauthorized access to sensitive information and enable verifiability of every component in a communication.

Goals of Cryptography: Generally there are four main goals. They are as -

i. **Confidentiality**: Only an authorized recipient should be able to extract the contents of the message from its encrypted form. Resulting from steps to hide, stop or delay free access to the encrypted information.
ii. **Integrity**: The recipient should be able to determine if the message has been altered.
iii. **Authentication**: The recipient should be able to verify from the message, the identity of the sender, the origin or the path it traveled or combinations so to validate claims from emitter or to validated the recipient expectations.
iv. **Non-repudiation**: The emitter should not be able to deny sending the message.

PGP

PGP uses a cryptographically strong hash function on the plaintext the user is signing. This generates a fixed-length data item known as a message digest. Then PGP uses the digest and the private key to create the "signature." PGP transmits the signature and the plaintext together. Upon receipt of the message, the recipient uses PGP to recompute the digest,

thus verifying the signature. PGP can encrypt the plaintext or not; signing plaintext is useful if some of the recipients are not interested in or capable of verifying the Signature [3].

How PGP works

PGP combines some of the best features of both conventional and public key cryptography. PGP is a hybrid cryptosystem. When a user encrypts plaintext with PGP, PGP first compresses the plaintext. Data compression saves modem transmission time and disk space and, more importantly, strengthens cryptographic security. Most cryptanalysis techniques exploit patterns found in the plaintext to crack the cipher. Compression reduces these patterns in the plaintext, thereby greatly enhancing resistance to cryptanalysis [1].

PGP then creates a session key, which is a one-time-only secret key. This key is a random number generated from the random movements of your mouse and the keystrokes you type. This session key works with a very secure, fast conventional encryption algorithm to encrypt the plaintext; the result is ciphertext. Once the data is encrypted, the session key is then encrypted to the recipient's public key. This public key-encrypted session key is transmitted along with the ciphertext to the recipient

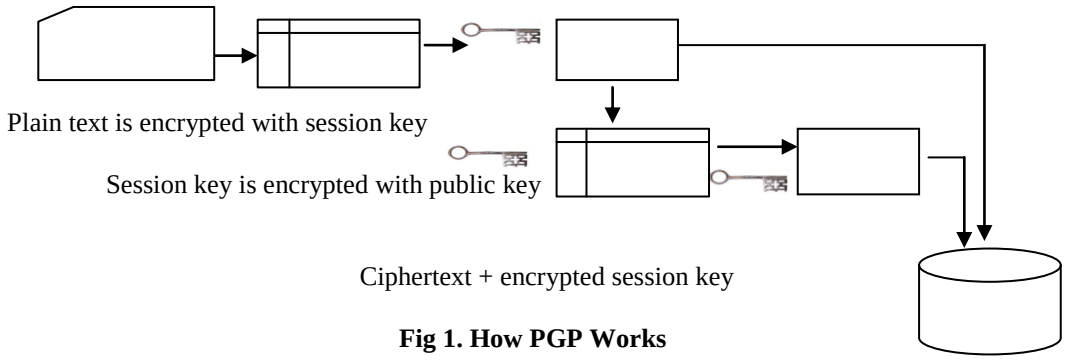

Fig 1. How PGP Works

STEGANOGRAPHY

The term "steganography" derives from the Greek for "covered writing" which is a good representation of the central idea of steganography. The end goal of steganography is to hide data in a digital object so that it cannot be detected through observation (or even complex analysis). It is the art and science of writing hidden messages in such a way that no one, apart from the sender and intended recipient, suspects the existence of the message, a form of security through obscurity [4].

Steganography and cryptography both are used for the purpose of sending the data securely [5]. Steganography supports different types of digital formats that are used for hiding the data .These files are known as carriers [6]. The main file formats that are used for steganography are Text, images, audio, video and protocol.

III. 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.

Our proposed research work includes:

1. To improve Authentication
2. To improve Confidentiality
3. To improve the compression

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.

IV. 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. Figure 2 presents an example about pixel values and shows the secret message. 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].

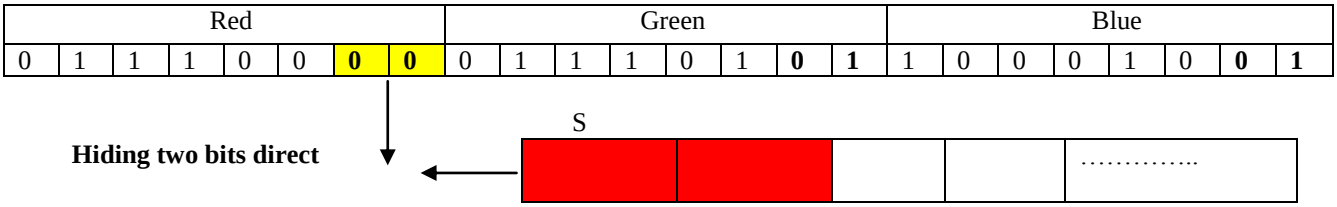

Fig 2. Least Significant Bit Hiding Technique

Proposed Algorithm

Inputs: RGB image, secret message and the password.
Output: Stego image.
Begin

scan the image row by row and encode it in binary.
encode the secret message in binary.
check the size of the image and the size of the secret message.
start sub-iteration 1:
choose one pixel of the image randomly.
divide the image into three parts (Red, Green and Blue parts).
hide two by two bits of the secret message in each part of the pixel in the two least significant bits.
set the image with the new values.
end sub-iteration 1.
set the image with the new values and save it.

End

V. 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.

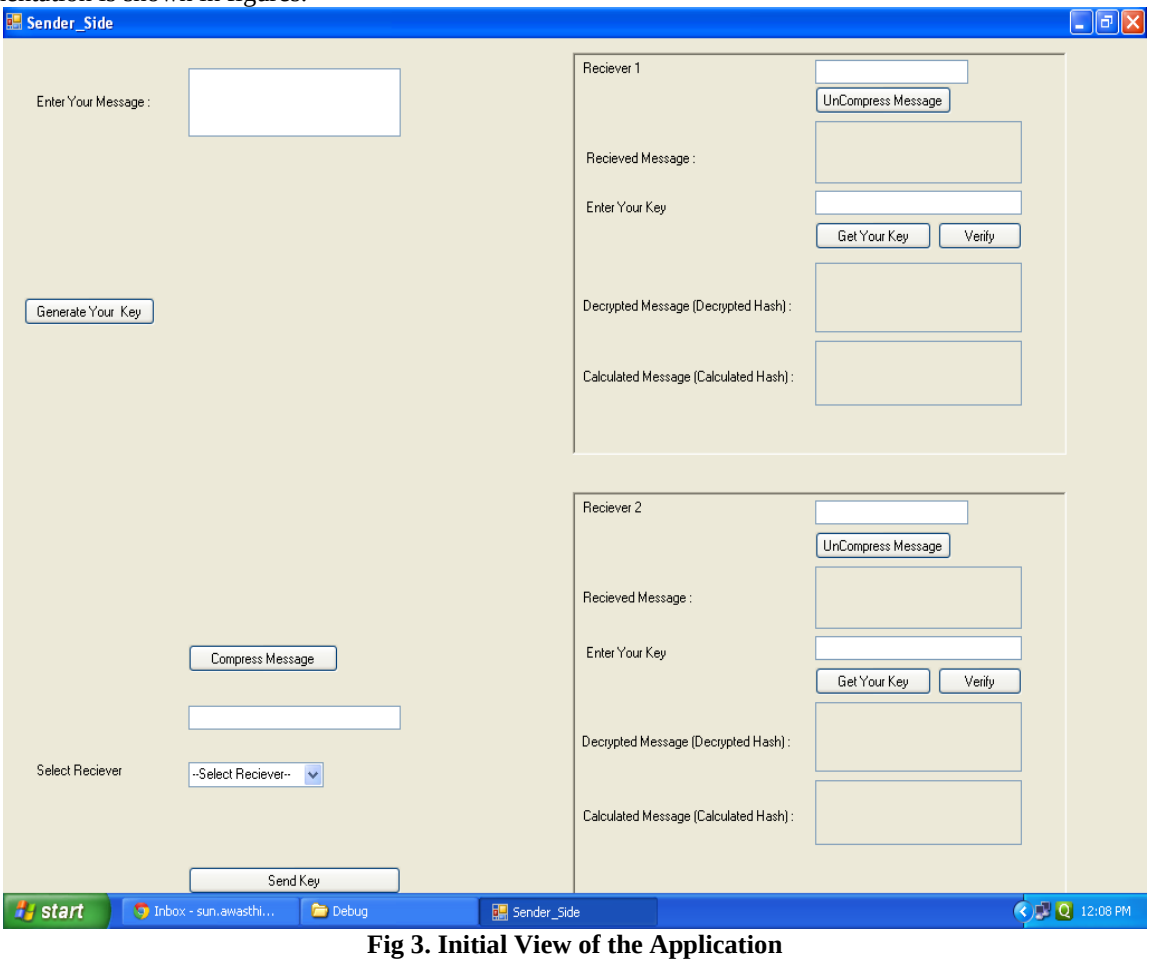

Fig 3. Initial View of the Application

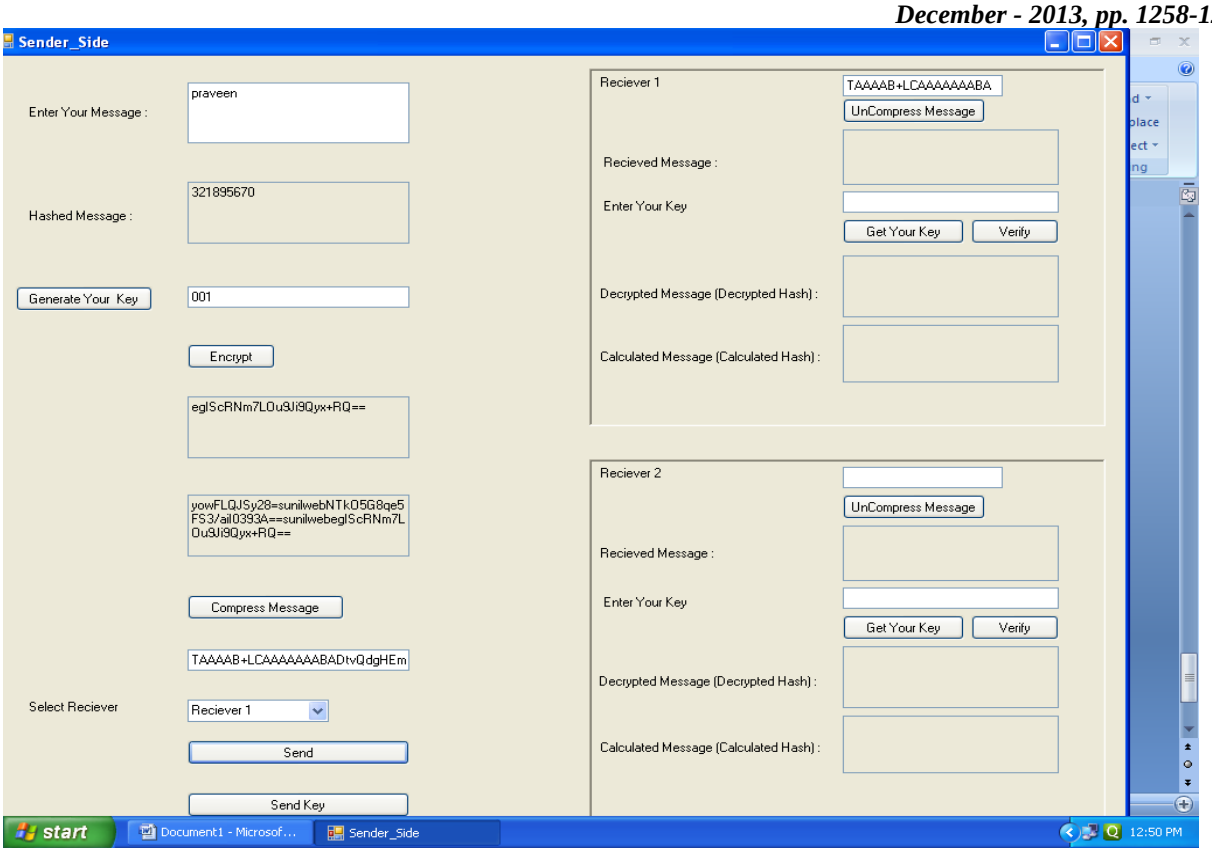

Fig 4. Sending Message to Receiver

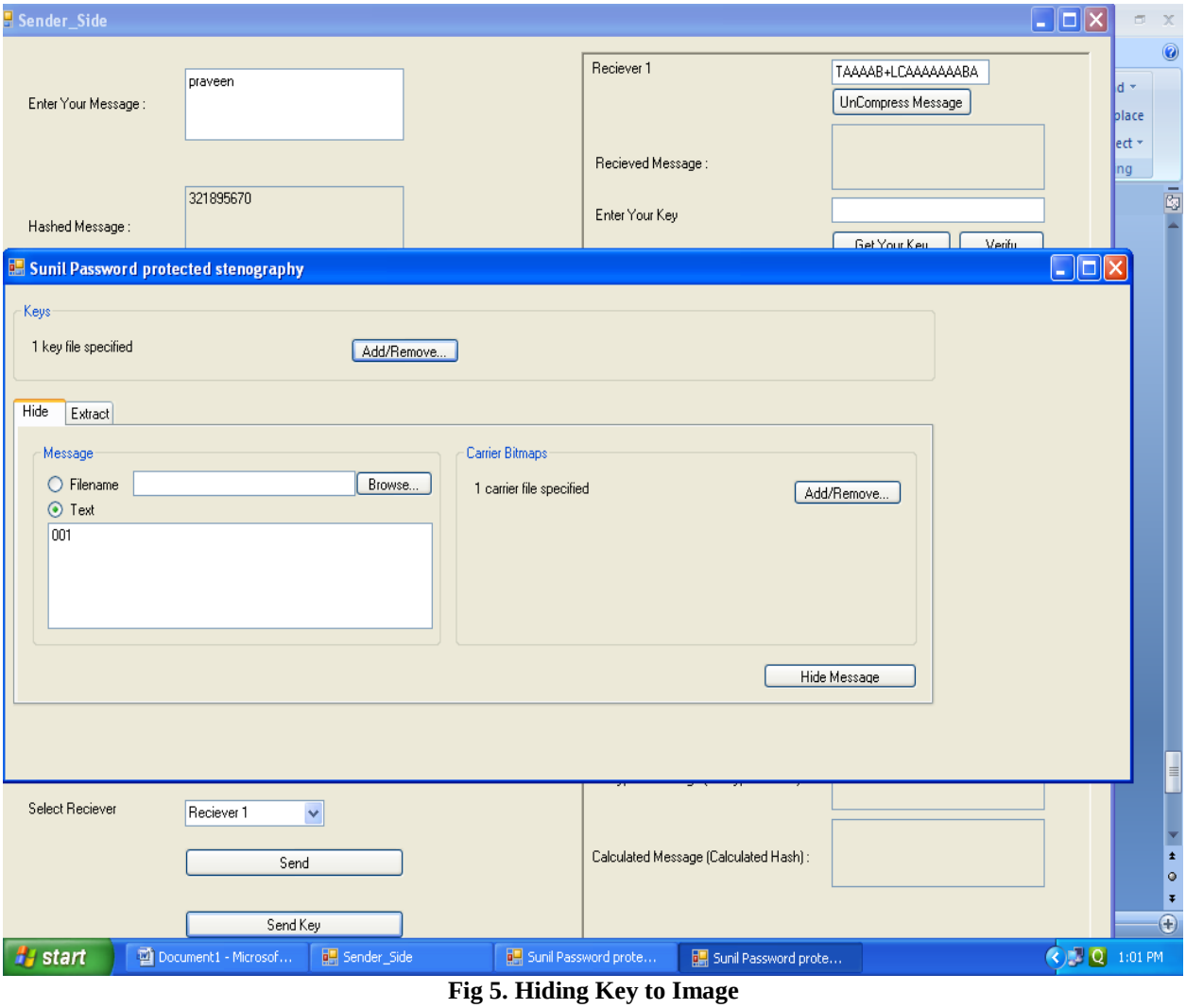

Fig 5. Hiding Key to Image

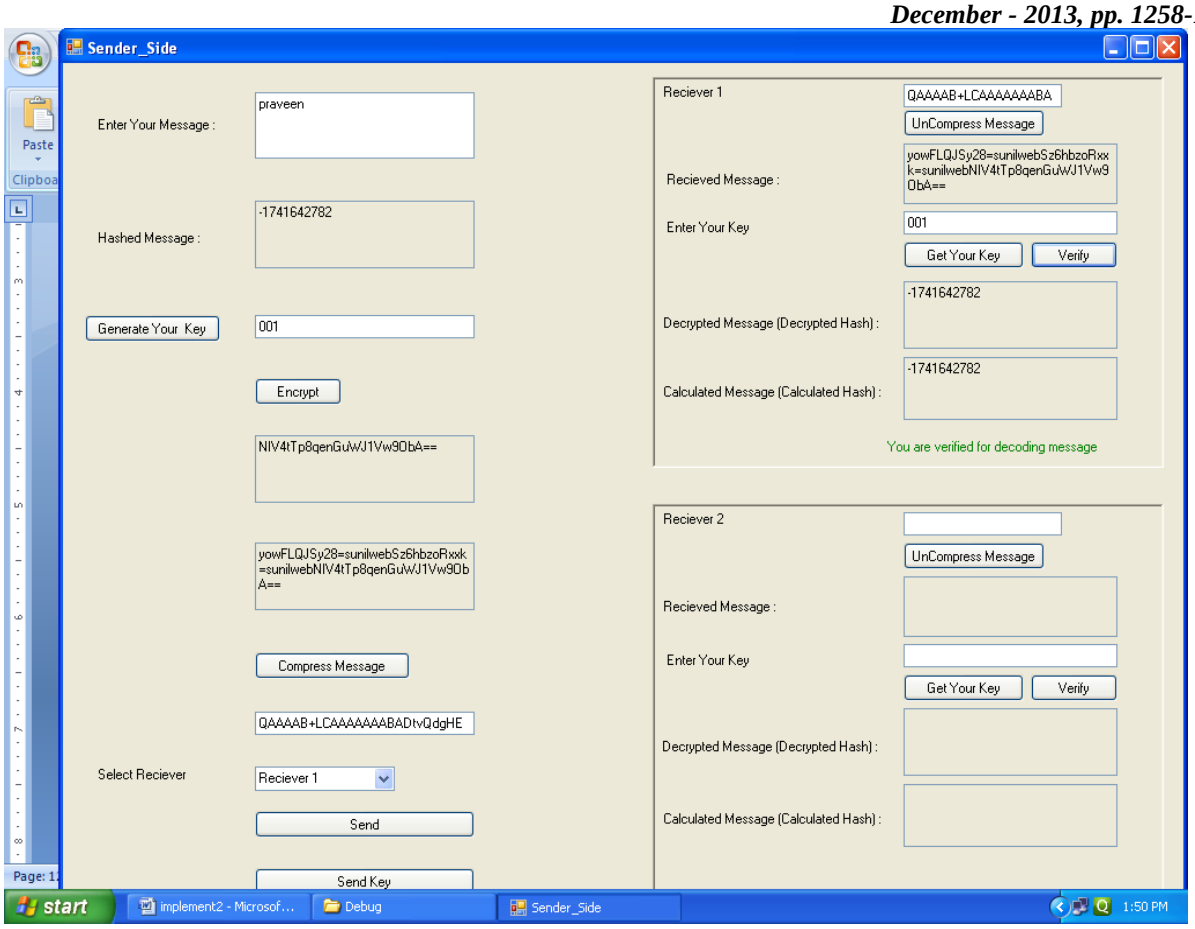

Fig 6. Authentication and Confidentiality verification

VI. CONCLUSIONS

This new approach of PGP provides more security. By changing the architecture of PGP from Asymmetric to Symmetric and using two stages secure stegenography 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 exist 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 ih want is hidden. And if he get 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]. Caftori, Lal, Rosenberg, Poole. "Tutorial for Beginners to PGP". (Revised April 8, 2001). URL: http:// www.neiu.edu/~ncaftori/PGP.htm - foreword.

[2]. W, Peter. Disappearing Cryptography: Information Hiding: Steganography & Watermarking (second edition). San Francisco: Morgan Kaufmann. 3(1992) 192-213.

[3]. Amirthanjan,R. Akila,R & Deepika chowdavarapu, P., 2010. A Comparative Analysis of Image Steganography, International Journal of Computer Application , 2(3), pp.2-10.

[4]. Talele, K.T. Gandhe, S.T & Keskar, A.A., 2010. Steganography Security Fir Copyright

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

[6]. El-Emam,N.N., 2008. Embedding a large amount of information using high secure neural based steganography algorithm. International Journal of Signal Processig, 4(2), pp.54

[7]. Ali-al, H. Mohammad, A. 2010. Digital Audio Watermarking Based on the Discrete Wavelets Transform and Singular Value Decomposition, European Journal Of Scientific Research , vol 39(1), pp 231-239.

[8]. Ker, A.: Improved detection of LSB steganography in grayscale images. Proc. 6th Information Hiding Workshop. Springer LNCS, vol. 3200, pp. 97-115, 2004.

