IMAGE STEGANOGRAPHY USING ADAPTIVE B45 ALGORITHM COMBINED WITH PRE-PROCESSING BY TWOFISH ENCRYPTION

Anil Hingmire [1] | Sunil Ojha [1] | Chetan Jain [1] | Komal Thombare [1]

[1] Department of Computer Engineering, University of Mumbai, Mumbai, India.

ABSTRACT

Security is one of the main issues when there is a question of transmitting highly confidential data to various locations over the internet. This paper presents an approach to create a secure system to provide optimal security during the transmission over an insecure channel. Cryptography and steganography alone cannot be used for transmission of data because each has their own weaknesses. But with the proposed system, both the technologies are used together to create a near impossible way for third parties to breach the system and gain confidential data. The system uses latest TwoFish algorithm for encryption while a new approach to perform the steganography is used i.e. Adaptive B45 steganography technique.

KEYWORDS: cryptography, steganography, TwoFish.

I. INTRODUCTION

Steganography is an art and science of writing messages in such a way that no one apart from the sender and intended receiver, suspects the existence of message, a form of security through obscurity. Essentially, the information-hiding process in a steganographic system starts by identifying a cover medium's redundant bits (those that can be modified without destroying that medium's integrity).. Cryptography is the practice and study of techniques for secure communication in the presence of third parties. These two techniques have drawbacks of their own, but when implemented together they cover each others drawback. Cryptography makes the data into an unrecognized format while steganography hides the presence of data. The combination of these two technologies creates a very secure way of transmitting data between users. The end goal of this system is to create a secure way to transmit data. Steganography and cryptography has been evolving over the last decade, as the designers are developing algorithms with more complex strategies while others are trying to detect and decode them.

Even though both methods provide security, a study is made to combine both Cryptography and Steganography methods into one system for better confidentiality and security. Combining these two methods together for the purpose of developing a system that will improve the confidentiality and security of the message is however, the goal of this system.

The power of steganography is in hiding the secret message by hiding its existence in a non-secret file. In that sense, steganography is different from cryptography, which involves making the content of the secret message unreadable while not preventing non-intended observers from learning about its existence. The success of steganography technique depends entirely on the ability to hide the message such that an observer would not suspect its existence; the greatest effort must go into ensuring that the message is invisible unless one knows what to look for. The way in which this is done will differ for the specific media that are used to hide the information. In each case, the value of a steganography approach can be measured by how much information can be concealed in a carrier before it becomes detectable, each technique can thus be thought of in terms of its capacity for information hiding [7].

II. ADAPTIVE IMAGE STEGANOGRAPHY COMBINED WITH TWOFISH ENCRYPTION

A. TwoFish Encryption

TwoFish is a block cipher of 128-bit that accepts a key of variable length of 128, 192 or 256 bits. This algorithm provides high level of security and scalability. This cryptographic algorithm is made up of Feistel network which includes the element of diffusion in the algorithm. It also contains fixed 4-by-4 MDS(Maximum Distance Separable) matrix which includes the element of confusion in the algorithm.

B. Adaptive B45 Steganography

LSB steganography is the most widely used technique for steganography. In this technique, the least significant bit of the cover image pixels are replaced by the data to be encoded. In B45 steganography we analyze the bit no 4 and bit no 5 to embed the bits at place no 3, 2 and 1. The process will carry on using the following technique:

BIT 5	BIT 4	BIT (3, 2, 1)
0	X	1
1	0	2
1	1	3

C. Key sharing using RSA

The main objective of implementing RSA algorithm is to secure the private key used for TwoFish algorithm between the users. The RSA is a public key cryptographic algorithm that is used to help ensure data communication security. It is simply based on two main cryptographic processes. First, using a public key it converts an input data called the Plain-text into an unrecognizable encrypted output called Cipher-text (Encrypted Plain-text), such that it is impossible to recover the original Plain-text without the encryption password in a reasonable amount of time. Second, using a private key, the RSA then converts the unrecognizable data back to its original form Decryption process. Today it is used in web browsers, email programs, mobile phones, virtual private networks and secure shells. Until recently, the use of RSA was very much restricted by patent and export laws. However, the patent has now expired and US export laws have been relaxed. The purpose of RSA is to develop an algorithm in which it is impossible to determine the private key. This algorithm is based on one-way function. As the name implies, the function is only one-way i.e. given some input values it is relatively easy to compute the result. However, it is extremely difficult, nearly impossible to determine the input values given the result.

Algorithm:

1. Choose two large prime numbers P and Q.

2. Calculate N=P*Q.

3. Select the public key e (encryption key) such that it is not a factor of (P-1) and (Q-1).

4. Select the private key d (decryption key) such that the following equation is true:

   $(d*e) \bmod (P-1)*(Q-1)=1$

5. For encryption , calculate the cipher text

   $CT=PT^{e} \bmod N$

6. Send CT as the cipher text to receiver.

7. For decryption, calculate the plain text PT from the cipher text CT as follows:

   $PT=CT^{d} \bmod N$

III. PROPOSED SYSTEM

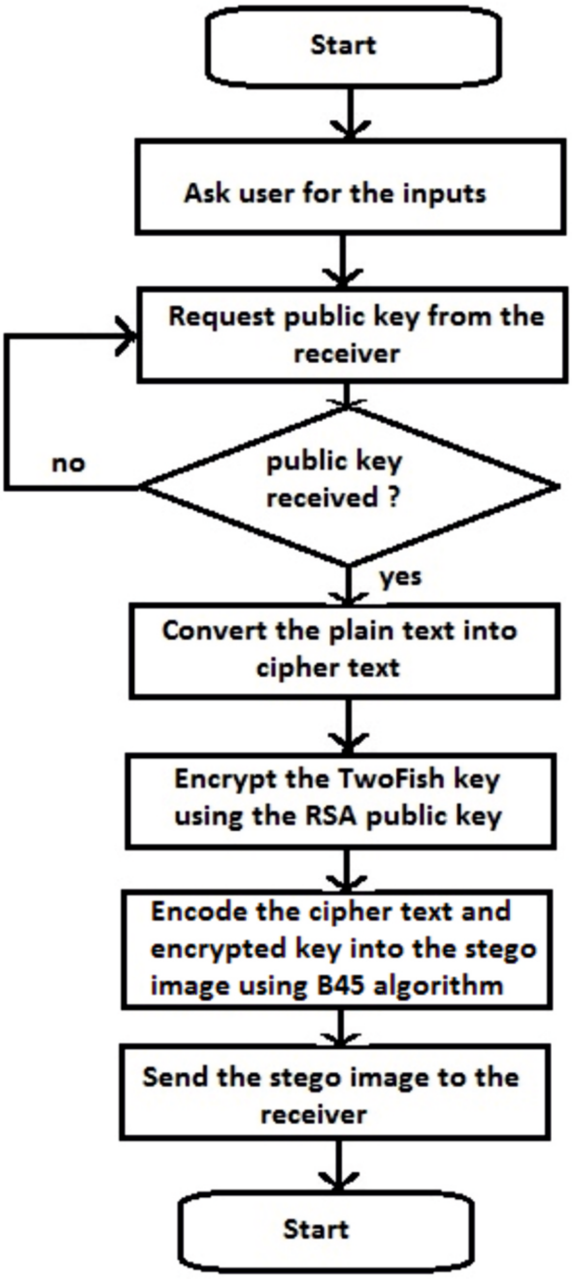
Our system uses the above mentioned algorithms together simultaneously to achieve multiple level of security.

Steps:

A. Sender side:

1. Ask user for plain-text, cover image and private key for TwoFish algorithm.
2. Request public key (RSA) from the receiver.
3. Receive the public key from the user.
4. Encrypt the TwoFish private key using the using the public key received at step 3.
5. Encrypt the plain-text using the TwoFish private key to get the cipher-text.
6. The cipher-text and the encrypted key is then encoded into the cover image using the Adaptive B45 steganography technique.
7. Save and send the cover image generated at step 6 to the intended receiver.

B. Flowchart(Sender):

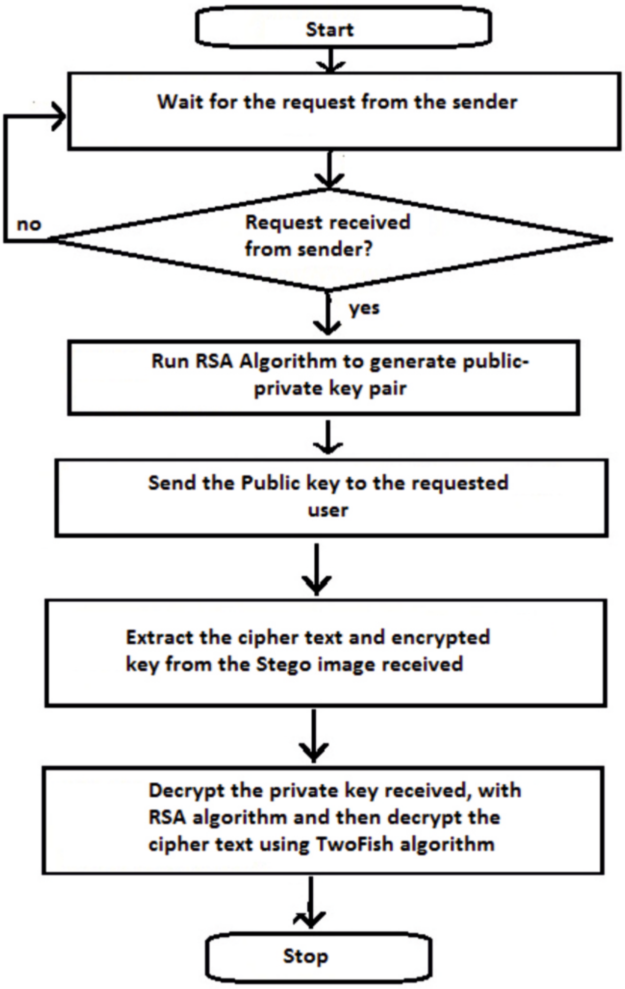


Start
Ask user for the inputs
Request public key from the receiver
public key received ?
no
yes
Convert the plain text into cipher text
Encrypt the TwoFish key using the RSA public key
Encode the cipher text and encrypted key into the stego image using B45 algorithm
Send the stego image to the receiver
Start

C. Receiver side:

1. Look for request from the sender.
2. If received, launch RSA algorithm to generate the public key (E), private key (D).
3. Send the public key to the sender.
4. Receive the stego-image from the sender.
5. Extract the cipher-text and encrypted key from the stego image using Adaptive B45 steganography technique.
6. Compute the TwoFish private key using the RSA algorithm.
7. Decrypt the cipher-text using the TwoFish algorithm.

D. Flowchart (Receiver):



Start
Wait for the request from the sender
Request received from sender?
no
yes
Run RSA Algorithm to generate public-private key pair
Send the Public key to the requested user
Extract the cipher text and encrypted key from the Stego image received
Decrypt the private key received, with RSA algorithm and then decrypt the cipher text using TwoFish algorithm
Stop

Conclusion

Image steganography and cryptography provide a very effective way to conceal and transfer messages securely between two parties. Even though one of the technique gets compromised the other technique provides the necessary confidentiality to the document to be transferred. This application aims to remove the inconsistencies in the stand alone systems of cryptography and steganography. The system is well secured with TwoFish encryption algorithm and the B45 steganography technique.

REFERENCES

1. Bruce Schneier, John Kelseyy, Doug Whitingz, David Wagnerx, Chris Hall, Niels Ferguson, "Twofish: A 128-Bit Block Cipher,", 15 June 1998.
2. https://www.schneier.com/cryptography.
3. Yang Ren-er, Zheng Zhiwei, Tao Shun, Ding Shilei "Image Steganography Combined with DES Encryption Pre-processing", Ningbo University, Ningbo 315211, China.
4. http://www.developeriq.in/articles.
5. Khalil Challita, Hikmat Farhat "Combining Steganography and Cryptography: New Directions", Notre Dame University - Louaize, Lebanon.
6. Yang Ren-er, Zheng Zhiwei, Tao Shun, Ding Shilei, "Image Steganography Combined with DES Encryption Pre-processing", College of Information Science and Engineerin Ningbo University, Ningbo 315211, China.
7. Abikoye Oluwakemi C., Adewole Kayode S., Oladipupo Ayotunde J., "Efficient Data Hiding System using Cryptography and Steganography"
8. Saleh Saraireh, "A Secure Data Communication system using cryptography and steganography," International Journal of Computer Networks & Communications (IJCNC) Vol.5, No.3, May 2013.