Transmitting Cryptographic data through Steganography

Maria Akhtar Mufti[1], Aihab Khan[2], Malik Sikandar Hayat Khiyal[3] and Asim Munir[4]

[1] *Software Engineering, Fatima Jinnah Women University, Rawalpindi, Pakistan*

[2] *Software Engineering, Army Public College of Management and Sciences, Rawalpindi, Pakistan*

[3] *Computer Science, Iqra University, Rawalpindi, Pakistan*

[4] *Computer Science, International Islamic University Islamabad, Pakistan*

Abstract

Computers are being used worldwide. The internet connects the world as one. Cybercrime is a huge issue which can be resolved by some approaches. In this paper an approach is introduced to ensure the security of data. Steganography and cryptography are merged together in order to obtain a secure and reliable way of transmitting data. In this paper an encrypted image is transmitted using steganography to thwart attackers. Noise is introduced to the image at sender end and is reduced at receiving end. In this way a clear image is received instead of a corrupted image.

Keywords: *Steganography, Cryptography, Stego-image, Secret Key, Cover Medium, Transmission Noise.*

1.Introduction

Information is no longer safe, even on computers. Attackers are always on the standby to steal private and confidential information and misuse it. Attackers can misuse the stolen information as blackmail or selling it to rivaling parties, etc. As computers and the internet are being used worldwide many fear for the safety of their information. Security has become a necessity and in order to achieve it multiple steganography and encryption techniques are available. By using these techniques one can be ensured of the confidentiality, authentication, privacy and integrity of their information. Information can be of any type; may it be in the form of text, image, audio or video. Security is ensured of all types of information.

The need for having a security means at hand to prevent unwanted access to confidential information is a huge aspect today. Almost all work is done using computers. Almost all organizations use computers and the internet to do their work. Information is being transferred over the internet every millisecond. There is no doubt that the computer is a magnificent creation and it has proven to help man a lot but every pro has its con. Whereas computer is a pro in the sense helping mankind it is also used as a con by man in doing illegal actions called cybercrime [1]. Similarly the internet is also a pro in the sense that it brings the world together and keeps us connected but it is a con as well as it has also caused a boom in cybercrime. Cybercriminals steal important data and misuse it to attain their own benefit regardless of any consequences that their actions may hold. Hence it is necessary to have a prevention method at hand to ensure the safety of information. By having such a method, the integrity, authentication, confidentiality and credibility of information are maintained.

The only solution to prevent cybercrime and to ensure the security of information is to have a method of prevention at hand. Here cryptography, steganography and compression will be used side by side in order to achieve security of information (secret images). The Steganography is an ancient art. Steganography is the art of hiding secret information so that its existence is concealed. Cryptography and steganography differ from one another as; cryptography is the art of masking the content of the message whereas steganography is the art of masking the existence of the message. Cryptography renders the message unintelligible to outsiders by various transformations or substitutions of the text whereas steganography conceals the very existence of the message. Cryptography provides *privacy* whereas steganography

provides *secrecy*. The technique proposed will benefit mankind. It will ensure that confidential data is safe and secure and keep the owner of the data assured that their data is safe [5].

The secret message is encrypted and then embedded within the cover image in such a way that the secret message cannot be detected. The merits achieved will be the authentication of the stego image and its sender, the confidentiality will be attained between wanted parties only, the integrity of the secret message will remain intact and the unwanted parties will not be able to know of the mere existence of the secret message. If steganography fails and the stego image is ceased by an unwanted party then the encryption of the message will thwart off the approaches of said unwanted third party. The demerits of this approach are that all kinds of attacks may not be thwarted and testing to check compatibility of this approach with attacks will be considered as future work.

This approach will be used to maintain the security of secret images when they are transported over the internet. The security will be maintained by not letting any unwanted party eavesdrop or steal the secret image. The secret image may be a blueprint of a new skyscraper, atomic bomb, etc. Security is a main issue in today's world. The purposed approach ensures that the security is not breached. Spies can send important information back to governments in order to stop terrorist attacks. This approach benefits mankind.

2. Review Stage

Steganography and cryptography are not something new; both of them have been around since before WW-1. Over the years both steganography and cryptography have evolved and now they both are being used together to ensure the secrecy and privacy of information. Some previous works that are related to the problem domain are discussed below.

In 2009, Mamoun [2] proposed a steganographic technique of embedding a digital color image into a color image. This requires the use of uncompressed 24-bit windows format bitmap image. The major characteristic of this algorithm is the ability of embedding a large digital image into a small digital image and vice versa. This method allows for embedding a text message into a cover image and produces a high degree of security and privacy. This method also includes a password in the stego image, so that no one can extract the secret image except for those who know the password. The limitation of this technique is that it solely based on steganography and does not involve encryption, hence does not give privacy if steganography fails.

Another solution proposed to hide data within a digital image is combining a complete complementary (CC) spreading sequences and nested scalar quantization (NSQ). The source image is encrypted before it is embedded. Investigations were done on the effect of CC sequence length on the performance for both non-blind and blind hiding, and show that there is a noticeable improvement in performance with increase in code length for blind data hiding, whereas the effect is negligible for non-blind data-hiding. [3].The weaknesses this approach showed was its lack of robustness and compression. Also no testing was done to check whether the attacks will prevail or not.

The development of network technique is making research on the information security more important. An approach proposed to solve this problem has been introduced. First, to make the encryption system strong, the secret message is encrypted through the combination of a new gray value substitution operation and position permutation. Secondly, the processed secret message is hidden in the cover image. The experimental result shows a high security level and better image quality [4].

3. Framework Overview

The system block diagram, shown in Figure 1, depicts the working of the system.

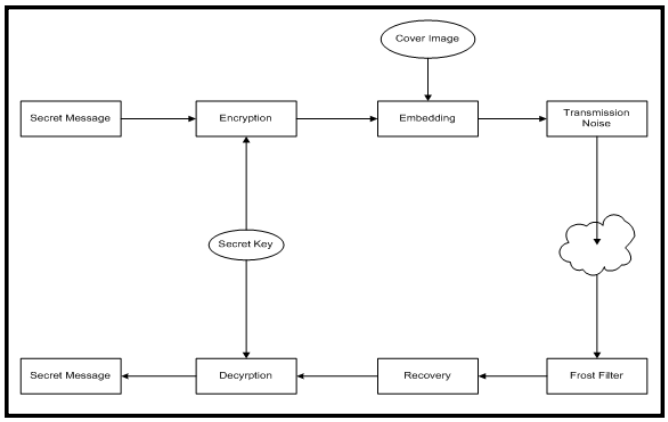

Figure 1: Block Diagram of System

The main focus is to hide data in a digital image before transmitting the image across the internet/transmission network. Then recover the hidden data from the digital image. The system focuses on two users; one is the sender and the other is the receiver. The sender is the user who sends the message and the receiver is the user that the message is addressed to. The system provides secrecy, integrity and privacy to both the data and the two users. The purpose of hiding data in digital images is done to thwart off attackers and not to arouse suspicions. A filter is introduced to remove any transmission noise that the stego-image attains after transmission. Only when the noise is removed from the sego-image will the receiver be able to acquire the plain-text of the secret message. The encoded secret message cannot be retrieved to its exact

form until noise is removed from the stego-image. The noise distortion causes the encrypted message to be distorted. This distortion must be removed or else the system fails.

4. Technique

This technique is fulfilled in two phases:

- Sender side
- Receiver side

In first phase, a Pre-defined cryptography key that is known by both sender and receiver only acts as one of the inputs of the encryption phase. The second input is the secret message that the sender wants to send the receiver. The sender will use both the secret key and the secret message in order to encrypt the message. The secret message is now in the cipher-text form.

After the encryption phase the sender will select a cover-medium. Using the cover-medium and the cipher-text of secret message, the sender will apply steganography. The resultant produced by steganography is the stego-image.

Both encryption and steganography have been done successfully. So, transmit the image.

In the second phase, the receiver shall receive a distorted stego-image. First and foremost the stego-image has to be filtered in order to remove and restore the pixels of the stego-image so that the embedded cipher-text is not altered. After filtration, the embedded cipher-text is recovered from the stego-image. The recovery process is the mirror image of the embedding process.

Now decrypt the cipher-text to attain the plain-text of the secret message.

5. Experimental Results

First is the encryption of the message, Figure 2. In the encryption phase a plain-text of 15 characters is converted into the cipher-text.

```
plaintext =

this is a test!

ciphertext =

}8r1u\x5rYSM?Uy
```

Figure 2: Encryption

Taking the image of a baby as the cover-medium and the cipher-text as the secret message, steganography is conducted and the following results are obtained.

Figure 3: Original Image

Figure 4: Stego-Image

Figure 5: Transmitted Image

Figure 6: Filtered Image

Figure 3 shows the cover-image selected by the user in its initial and original form. By using the selected cover-medium and the cipher-text "}8r1u\x5rYSM?Uy" steganography is done and a stego-image, Figure 4 is generated. Now that cryptography and steganography both have been successfully completed, the stego-image is transmitted. Figure 5 depicts a noisy stego-image. The noise introduced into the stego-image is the effect of transmission. The image has successfully been transmitted by the sender to the receiver. Before the receiver can perform any further actions on the stego-image, the stego-image must be filtered. Figure 6 shows the filtered stego-image. Noise distortion has been removed from the stego-image.

```
ciphertext =

}8r1u\x5rYSM?Uy

plaintext =

this is a test!
```

Figure 7: Decryption

The receiver now extracts the encrypted message from the stego-image. Lastly, the cipher-text is converted to original plain-text by using decryption. Note that the receiver uses the same key as the sender used for encryption. As shown in Figure 7.

If an attacker were to get a hold of the stego-image and try to get the secret message without knowing the secret key then his tries will be useless.

6. Conclusion

A successful implementation of hiding data in digital images in MATLAB 7.0 environment is achieved. The system is user friendly. The system is reliable as it ensures security of message and hides the very existence of the message within a cover medium. The user can select any image to be his cover medium. The system provides authentication and confidentiality to user. The limitations of the system are that only a message of 15 characters can be encrypted and decrypted. The frost filter successfully removes the noise from stego-image without disrupting the embedded cipher-text.

The future work for this system is to apply an encryption technique that does not limit the characters of the secret message. Another enhancement that could be made is to check the robustness of the system.

References

[1] Parthasarathi Pati, “Cybercrime”, http://www.naavi.org/pati/pati_cybercrimes_dec03.htm
[2] Mamoun Al Rababaa, "Colored Image in Image Hiding", Accepted in the Ubiquitous Computing and Communication Journal (UBICC), 22nd February, 2011.
[3] Qiwen Liu,Chadi Khirallah, Lina Stankovi´c, Vladimir Stankovi´c “Image-In-Image Hiding Using Complete Complementary Sequences”, Accepted at IEEE International Conference 2008, pages 233-246, 14th February 2011.
[4] Mansour Jamzad, Hedieh Sajedi and Zahra Toony, “A High Capacity Image hiding Method based on Fuzzy Image Coding/Decoding”, Accepted at the 14th International CSI, Tehran, pages 511, 21st January 2011.
[5] Hongmei Tang, Cuixia Wu, Gaochan Jin, Peijiao Song, “A New Image Encryption and Steganography Scheme”, Accepted in ICCS 2009, in the International Conference, Hong Kong, China, pages 60, 15th January 2011.
[6] Meenu Kumari, “JPEG Compression Steganography & Cryptography Using Image-Adaptation Technique”, journal of advances in information technology, vol. 1, no. 3, 14th February, 2011.

Maria Akhtar Mufti is a graduate student of Software Engineering from Fatima Jinnah Women University. She Participated in Speed Programming Competition held by Sidra Tabassum, Chair IEEE Student Chapter 09. She is the IT Executive in Celeros Networks Private Limited.

Dr. **Malik Sikandar Hayat Khiyal** is Head of Academic (ES) at APCOMS, Khadim Hussain Road, Lalkurti, Rawalpindi, Pakistan. He received his M.Sc degree from Quaid-e-Azam University, Islamabad. He got first position in the faculty of Natural Science of the University. He was awarded the merit scholarship for Ph.D. He received his Ph.D. degree from UMIST, Manchester, U.K. He developed software of underground flow and advanced fluid dynamic techniques. His areas of interest are Numerical Analysis, Modeling and Simulation, Discrete structure, Data structure, Analysis of Algorithm, Theory of Automata and Theory of Computation. He has more than hundred research publications in National and International Journals and Conference proceedings.

Aihab Khan is an assistant professor of Computing and Technology at Iqra University. His areas of interest are Network Security, Information Security and Databases.

Asim Munir is in the process of completing his Ph.D. He is the Assistant Professor of Computer Science department at International Islamic University, Islamabad. He is a gold medalist in Microsoft Official Curriculum Training – MCSE.