A SECURE DATA COMMUNICATION SYSTEM USING STEGANOGRAPHY WITH ENCRYPTED SECRET MESSAGE INSIDE IMAGE MEDIA

ISSN(Online): 2581-5296

A SECURE DATA COMMUNICATION SYSTEM USING STEGANOGRAPHY WITH ENCRYPTED SECRET MESSAGE INSIDE IMAGE MEDIA

Bharti Sharma[1], Surbhi Maheshwari[2]

ABSTRACT

Secure data communication is the most important area of research now-a-days.Internet is a public network that is used to transfer data from one place to another place and people want secure communication channel over the internet therefore the information should not be changed during transmission.In this research paper, secure data communication is provided by steganography with cryptography. Basically Steganography is an art of hiding data in some other media. On the other hand, Cryptography is used to encrypt text data into cipher text. I use encrypted secret message using cryptography after that the encrypted message is hidden inside an image media using steganography. This two phase security algorithm preventing from unauthorized access and enable verifiability of data in a communication. This paper discusses how secure data communication is achieved with the help of security algorithms.

KEYWORDS: Steganography, LSB, Cryptography, RSA, Image media.

INTRODUCTION

Information security actually starts with the emergence of first main frame computer. But with the introduction of information security many viruses and code breakers were also developed that breaks the security channel and damage the important information. To overcome these issues, firstly physical controls were needed to limit the access of unauthorized persons to susceptible areas. Later on department of defense's Advance research project agency (ARPA) in 1960's started to examine the viability of disused network

Communications in between 1970 and 1980 ARPANET become popular but with the popularity some security issues were also raised, like there are no procedures for identification and authorization of the system while dial – up connection. In 1990's computer networks become more common because of communication which results in the emergence of internet. Internet bought millions of computer into communication with each other, where many Pc's were unsecured. Security is a quality of being secure; it can be physical, personal, communication or network security therefore security is the need of our modern world.

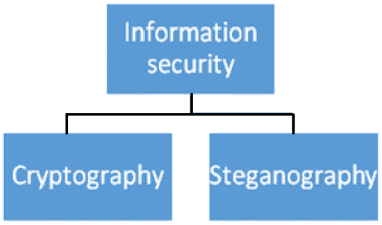

Fig: 1 Information Security Algorithms

1. Assistant Professor at Vivekananda Global University, Jaipur, India,
E-mail Address: bhartisharmavit@gmail.com

2. Assistant Professor at Maharishi Arvind Institute of Science and Management, Jaipur, India

E-mail Address: subhi.kabra@gmail.com

Cryptography

Cryptography is an art of hiding and verification. It provides security and preventing from unauthorized access to sensitive data and enable verifiability of data in a communication. The word cryptography is derived from the Greek words: "crypto" and "Graphien", which mean is "hidden writing".

Steganography

Basically Steganography is an art of hiding secret information in some other media. The information can be in the form of a text, an image, a video or an audio which is to be hidden using any cover medium like image, text, audio or video.

IMAGE STEGANOGRAPHY

Image steganography is a process in which image is used as a cover media to hide secrete information within it. This technique is used because it provides better security to the data than other technologies of steganography. A human can't able to see the hidden information within an image. It prevents secrete data from unauthorized access.

Hiding information within cover image required several elements like:-

1. **Cover Image:** That will hold the secret message
2. **Secret message:** Those we want to hide within the cover medium
3. **Steganography Technique:** By using the technique we will perform the hiding operation.
4. **Stego key:** That we can use to hide or unhide the secret message.

The image steganography method is the best method among all the other steganography methods. The humans are unable to view stego image by naked eye but they usually leave behind some type of fingerprint or statistical hint that they have been modified. It is those discrepancies which an analysis tool may be able to detect. Since some techniques and their effects are commonly known, a statistical analysis of an image can be performed to check for the hidden messages in it.

DESIGN AND METHDOLOGY

The main objective of this purposed technique is to provide security system for secret information during the communication process. The proposed system consists two main phase: first secure text file is converted from plain text to cipher text using strong RSA algorithm and then XOR operation is done over the cipher text so that intruders can't able to recover hidden message. In the second phase encrypted message is embedded into an image using LSB algorithm. The confidential information is retrieved from the image that holds secret message by applying decryption process on stego-image. The proposed system is analyzed using peak-signal to noise ratio (PSNR).

The stego-image is in high quality if PSNR value is high; it means stego-image is equal to original image. If PSNR is high then intruders are unable to detect the confidential information. If in any case the cipher text got revealed from the input image, the middle person other than receiver can't access the information as it is in encrypted form.

This method provides two stage security to the text data with the help of security algorithms. And quality of stego-image is also improved therefore attackers unable to detect hidden information inside an image.

The RSA Algorithm

The text message is encrypted and decrypted using RSA algorithm. The RSA algorithm is developed by Ron Rivest, Adi Shamir and Leonard Adelman at MIT in 1978. This algorithm consist three steps: Key Generation, Encryption, Decryption.

Key-Generation Algorithm

1 First generate two Random prime numbers p and q, of approximately equal size such that their product n= pq is of the required bit length. Ex: 1024 bit

2 Then calculate n= p x q, it is a key length which is expressed in bits.

3 Calculate Euler's totient function φ (n) = (p - 1) x (q - 1).

4 Calculate e based on the following conditions:

- $1 < e < \varphi(n)$
- GCD (e, φ (n)) = 1 that is e and φ (n) are co-prime.
- Also ensure that e must have a short bit-length and small Hamming weight.

5 At the last step, find d by using the following relation:

- (e x d) mod n=1, private key (d, n) and public key (e, n).

The LSB Technique

Least Significant bit is the most widely used method for secret data hiding in any digital media like text, image, audio /video. With the use of LSB, last bit of an image replaced with bit of secret message. One can use 8 or 24 bit image to hide information for hiding large amount of data 24 bit images are appropriate. However LSB is an easy and helpful for the user but at the time of transmitting data on the network, it can be detected by an attacker. There are numerous versions of LSB include Edge based LSB, Random based LSB and Enhanced based LSB and soon. This kind of embedding leads to an addition of a noise of 0:5p on average in the pixels of the image where p is the embedding rate in bits/pixel. The secret information is hidden inside the cover image such that it cannot be seen by the human visual system (HVS). An algorithm to embed secret message into cover image using LSB technique is:

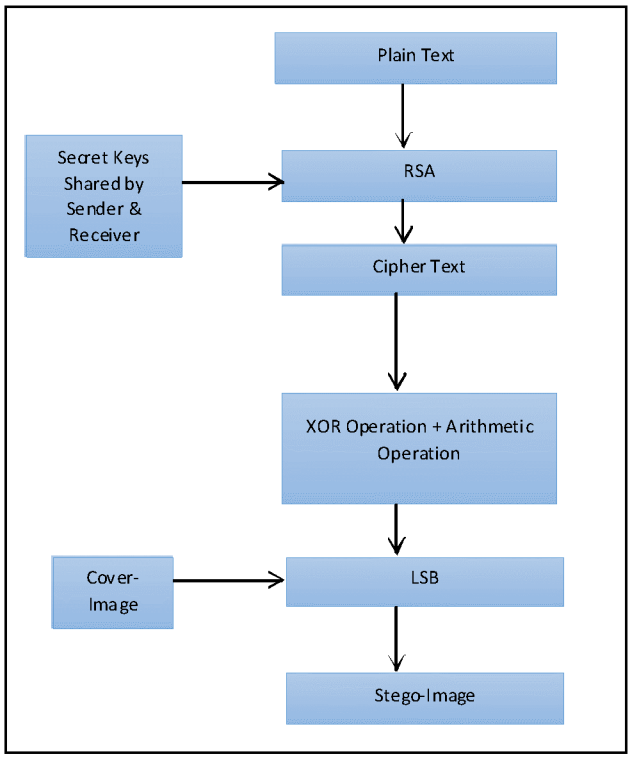

Fig: 2 Architecture for Embedding the Secret Message into the Cover Image

EXPERIMENTS AND RESULTS

Results are simulated on MATLAB version 8.5.0.197613(R2015a) on windows8 platform.

Cover Images and Stego Images

Fig: 3(a) cover image of a bird

Fig: 3(b) stego image of a bird

Fig: 4(a)cover image of Lenna

Fig: 4(b) stego image of Lenna

CONCLUSION AND FUTURE SCOPE

Steganography indeed is still in its developing stages, and a lot of research work is going on to increase the security, capacity, and robustness of the information systems.This paper proposed a highly secured data hiding approach using the combination of security algorithms.

The Security

Every popular algorithm can be cracked by various probability based tools of reverse engineering and dark web so in term of security regular changes in algorithm must necessary to enhance security of algorithms and prevent the secure system. It is possible to enhance security of algorithm by adding or removing various mathematical functions so that it is non guessable for hacker. From our proposed method can be seen that the text data is transformed from plain text to cipher text by using RSA algorithms so that an attacker can't able to read the secret text data. But there are various tracking tools available. To enhance the security, I apply XOR operation and some mathematical function on cipher text and also hide the existence of secret text data by using steganography method. Even, if an attacker known that the secret data is hidden inside an image but still can't able to detect the secret text data because it is in encrypted form and they needs private key to access it. It prevents confidential data from unauthorized access. Therefore it improves the security of data.

It enhances the security of text data to the higher level, because the mathematical functions are non-guessable. A human eye can't able to detect secret data because human visual system (HVS) not able to detect the minor changes between cover image and stego image.

Future Scope

This architecture is widely adopted by various cyber security organizations to make secure authentication or authorization mechanism in which they follow various traditional security algorithms with mathematical and logical functions. Using this method they make non guessable background technology which is hack proof through various reverse engineering tools and enhance privacy.

I am adding XOR with traditional security algorithm but we can more enhance the security of algorithm by adding more mathematical functions and creates multilayered secured system, in which every layer contains a random mathematical functions even developer doesn't know about the background technology.

REFERENCES

1. Xinyi Zhou, Wei Gong, WenLong Fu, LianJing Jin, "An Improved Method for LSB Based Color Image steganography Combined with Cryptography", in IEEE Journals, 2016 © 978-1-5090-0806-3 ICIS, June 26-29.
2. Shyam Nandan Kumar, "Review on Network Security and Cryptography", in International Transaction of Electrical and Computer Engineers System, 2015, Vol. 3, No. 1, 1-11 ©Science and Education Publishing ,DOI:10.12691/iteces-3-1-1.
3. Sadaf Bukhari, Muhammad Shoaib Arif, M.R. Anjum, Samia Dilbar, "Enhancing Security of Image by Steganography and Cryptography Technique", in The Sixth International Conference of Innovative Computing Technology (INTECH), 2016, 978-1-5090-2000-3/16©2016 IEEE.
4. Rohit Minni, Kaushal Sultania, Saurabh Mishra, Prof Durai Raj Vincent PM, "An Algorithm to Enhance Security in RSA", in 4th ICCCNT, 2016, IEEE–31661.
5. Rig Das, Thamrichon Tuithung, "A Novel steganography Method for Image Based on Huffman Encoding", in IEEE Journals, 2012, 978-1-4577-0748-3/12© 2012 IEEE.
6. Anjali Tiwari, Seema Rani Yadav, N.K. Mittal, "A Review on Different Image Steganography Techniques", in International Journal of Engineering and Innovative Technology (IJEIT), Volume 3, Issue7, January 2014, ISSN: 2277-3754, ISO 9001:2008 Certified
7. Rupali Jain, Jaishree Boaddh, "Advances in Digital Image Steganography", in 1st International Conference on Innovation and Challenges in Cyber Security (ICICCS2016), 978-1-5090-2084-3/16©2016 IEEE.
8. G.S.Sravanthi, B.Sunitha Devi, S.M.Riyazoddin & M.Janga Reddy, "A Spatial Domain Image Steganography Technique Based on Plane Bit Substitution Method", in Global Journal of Computer Science and Technology Graphics & Vision, Volume 12 Issue 15 Version 1.0 Year 2012, ISSN: 0975-4172.
9. K.Thangadurai and G.Sudha Devi, "An analysis of LSB Based Image Steganography Techniques", in International Conference on Computer Communication and Informatics (ICCCI), Jan 03-05, 2014, 978-1-4799-2352©2014 IEEE.
10. Hamad A. Al-Korbi, Ali Al-Ataby, Majid A. Al-Taee, Waleed Al-Nuaimy, "High-Capacity Image Steganography Based on Haar DWT for Hiding Miscellaneous Data", IEEE Jordan Conference on Applied Electrical Engineering and Computing Technologies, 978-1-4799-7431 3, 2013.
11. Sanchit Mahajan, "Improved Copyright Image Protection using Steganography Technique", International Journal of Innovative Research in Computer and Communication Engineering, Vol. 4, Issue 2, February 2016.
12. Kshetrimayum Jenita Devi of Department of Computer Science and Engineering National Institute of Technology-Rourkela Odisha, "A Secure Image Steganography Using LSB Technique and Pseudo Random Encoding Technique", 2013, pg. No. 6-7.
13. Navneet Kaur, Sunny Behal, "A Survey on various types of Steganography and Analysis of Hiding Techniques", in International Journal of Engineering Trends and Technology, Volume 11 Number 8 - May 2014, ISSN: 2231-5381.

❑ ❑ ❑