International Journal of Engineering Research and Science & Technology

ISSN : 2319-5991
Vol. 1, No. 2
April 2015

2nd National Conference on "Recent Advances in Science Engineering & Technologies" RASET 2015

Organized by

Department of EEE, Jay Shriram College of Technology, Tirupur, Tamil Nadu, India.

www.ijerst.com

Email: editorijerst@gmail.com or editor@ijerst.com

International Journal of Engineering Research and Science & Technology

ISSN 2319-5991 www.ijerst.com
Special Issue, Vol. 1, No. 2, April 2015
2nd National Conference on "Recent Advances in Science, Engineering&Technologies" RASET-2015

Research Paper

DATA SECURITY USING APPLICATION HIDING CRYPTOSYSTEM AND STEGANOGRAPHY

R Ramachandaran[1]*, A Ezra Sathiya Vasagam[1], S Jayakumar[1] and C Magesh Kumar[1]

*Corresponding Author: **R Ramachandaran** ✉ ramachandaranr@gmail.com

Communication which takes place between two peers in the form of text, is usually encrypted by a key which can be either symmetric or asymmetric. Hacker tries to obtain the key by cryptanalysis, thereby obtaining the text. The proposed system places the encrypted text inside an application along with a steganographically hidden image which contains the key and the application is hidden by another application. This is sent to the receiver. The receiver opens the outer application and decrypts the key in the steganographically hidden image. Now the original application, which contains the encrypted text, opens. The cipher text received will be decrypted by the receiver. The last two characters indicate the code of the encryption algorithm used. The receiver has to identify the algorithm and decrypt the cipher text using the same. Now the receiver obtains the plain text. The proposed system improves the security of communication. The system is implemented using more than one cryptographic algorithm, this helps in providing security to the data in case of any unauthorized access of data passing through network. As the security enhancements are provided using the steganography user key retrieval and application hiding techniques, the data security is achieved in higher level.

INTRODUCTION

Steganography and Cryptography are two popular ways of sending vital information in a secret way. Steganography hides the existence of the message and the Cryptography distorts the message itself. There are many cryptography techniques available; among them AES is one of the most powerful techniques. In Steganography, we have various techniques in different domains like spatial domain, frequency domain etc. to hide the message. Steganography is the art and science of hiding communication; a steganographic system thus embeds hidden content in unremarkable cover media so as not to arouse an eavesdropper's suspicion. In the past, people used hidden tattoos or invisible ink to convey steganographic content. Today, computer and network technologies provide easy-to-use communication channels for steganography. 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). The embedding process

[1] Department of Information Technology, SNS College of Technology-Coimbatore, Tamilnadu, India.

creates a stego medium by replacing these redundant bits with data from the hidden message. Modern steganography's goal is to keep the presence of the message undetectable from an unauthorized access. In this project we are developing a system where we develop a new technique in which Cryptography and Steganography are used as integrated part along with newly developed enhanced security module.

INTRODUCTION ABOUT CRYPTOGRAPHY

Cryptography is a method of storing and transmitting data in a particular form so that only those for whom it is intended can read and process it. The term is most often associated with scrambling plaintext (ordinary text, sometimes referred to as clear text) into cipher text (a process called encryption), then back again (known as decryption). Cryptography is a method of storing and transmitting data in a particular form so that only those for whom it is intended can read and process it. Cryptography is closely related to the disciplines of cryptology and cryptanalysis. Cryptography includes techniques such as microdots, merging words with images, and other ways to hide information in storage or transit. However, in today's computer-centric world, cryptography is most often associated with scrambling plaintext (ordinary text, sometimes referred to as clear text) into cipher text (a process called encryption), then back again (known as decryption). Procedures and protocols that meet some or all of the above criteria are known as cryptosystems. Cryptosystems are often thought to refer only to mathematical procedures and computer programs; however, they also include the regulation of human behavior, such as choosing hard-to-guess passwords, logging off unused systems, and not discussing sensitive procedures with outsiders.

The word is derived from the Greek kryptos, meaning hidden. The origin of cryptography is usually dated from about 2000 BC, with the Egyptian practice of hieroglyphics. These consisted of complex pictograms, the full meaning of which was only known to an elite few. The first known use of a modern cipher was by Julius Caesar (100 BC to 44 BC), who did not trust his messengers when communicating with his governors and officers. For this reason, he created a system in which each character in his messages was replaced by a character three positions ahead of it in the Roman alphabet.In recent times, cryptography has turned into a battleground of some of the world's best mathematicians and computer scientists. The ability to securely store and transfer sensitive information has proved a critical factor in success in war and business.Because governments do not wish certain entities in and out of their countries to have access to ways to receive and send hidden information that may be a threat to national interests, cryptography has been subject to various restrictions in many countries, ranging from limitations of the usage and export of software to the public dissemination of mathematical concepts that could be used to develop cryptosystems. However, the Internet has allowed the spread of powerful programs and, more importantly, the underlying techniques of cryptography, so that today many of the most advanced cryptosystems and ideas are now in the public domain.

PROBLEM STATEMENT

In any cryptosystem application the sender sends

the data to the receiver via network on encrypting the data using a cryptographic algorithm and the same algorithm is used by the receiver for the purpose of decrypting the received text. The key and the algorithm must be shared before the communication process starts between the sender and receiver. The unauthorized person or the hacker may try to hack the key of this cryptographic communication. When the key is known to the unauthorized person, the it becomes easy to get all the information passed through the communication.

EXISTING SYSTEM

The Cryptography and Steganography used for securing data transfer using images as cover objects for Steganography and key for the Cryptography.The data hiding using Cryptography and Steganography , the system works as in Cryptography it uses AES Algorithm to encrypt the data and a part of the message is hidden in DCT of an image; remaining part of the message is used to generate two secret keys which make this system highly secured.

Disadvantage of existing system

- No application hiding is done.
- Only one cryptographic algorithm is used.

PROPOSED SYSTEM

The proposed system consists of an application which is used for hiding the cryptosystem application. The sender sends the cryptosystem application along with the steganographically hidden image which contains the encoded secret key. The system has more than one cryptographic algorithm for encryption and decryption, from which the users can choose one or two algorithms according to theirs need. The application can be unhidden in the receiver side using the key retrieved by decrypting the steganographically hidden image. The last two characters of the encrypted text are used to identify the type of encryption algorithm used.

Advantage of proposed system

- Very secure, hard to detect.
- Application hiding is done.
- More than one cryptographic algorithm can be chosen by the user.

PROJECT DESCRIPTION

Overview of the project

Communication which takes place between two peers in the form of text, is usually encrypted by a key which can be either symmetric or asymmetric. Hacker tries to obtain the key by cryptanalysis, thereby obtaining the text. The proposed system places the encrypted text inside an application along with a steganographically hidden image which contains the key and the application is hidden by another application. This is sent to the receiver. The receiver opens the outer application and decrypts the key in the steganographically hidden image. Now the original application, which contains the encrypted text, opens. The cipher text received will be decrypted by the receiver. The last two characters indicate the code of the encryption algorithm used. The receiver has to identify the algorithm and decrypt the cipher text using the same. Now the receiver obtains the plain text. The proposed system improves the security of communication.

List of modules

§ Data Owner Message Sharing

§ Encryption and Confinement

§ User key Retrieval

§ Decryption

MODULE DESCRIPTION

DATA OWNER MESSAGE SHARING

The data owner sends the messages using the cryptosystem application to another user through the network. The data owner sends the key which is used for retrieving the information during the decryption process by using the technique of Steganography.

ENCRYPTION AND CONFINEMENT

The confinement process helps to prevent the cryptographic system from unauthorized or illegal usage. The encryption process may be carried out using one or more algorithms that are used in the system. The encrypted text also contains an indication for specifying the algorithm used for encrypting the plain text. So that, the receiver will use the same algorithm for decrypting the text received by him, in order to get the original message.

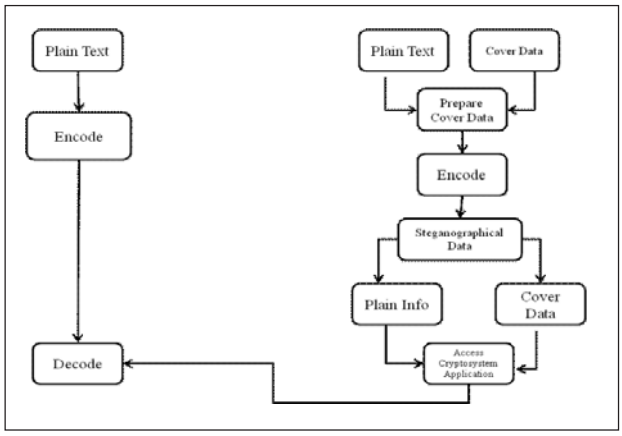
USER KEY RETREIVAL

The receiver receives the data from the network along with a steganographically hidden image. The key which is hidden using the steganography can be retrieved using the steganography application. This can be done only by a authorized user of the cryptosystem. The key which is retrieved by the process of steganography is used for the purpose of unhidding the application that is used as a cover application for the cryptosystem application.

DECRYPTION

Using the cryptosystem application along with the key used for encryption the decryption operation can be done by the receiver to receive the original message that was sent by the sender.

DATA FLOW DIAGRAM



CONCLUSION

In this work, the confidentiality is brought to the sender that even though the unauthorized user or the hacker tries to attack the message passed via network and the key is retrieved by the hacker, it is hard to retrieve the message that was sent by the user. As more than one cryptographic algorithm is used is also provides additional security to the data processed.

FUTURE WORK

In the future enhancement of our proposed system, there can be options available for more than two cryptographic algorithms for encrypting the data to be sent. The enhancement can also be brought in terms of using the steganography technique for also the purpose of hiding the data processed in the cryptographic system, instead of using it only for hiding the key.

REFERENCES

1. Abikoye Oluwakemi C, Adewole Kayode S, Oladipupo Ayotunde J (2012), Department of Computer Science , University of Ilorin,

Ilorin "Efficient Data Hiding System using Cryptography and Steganography", *International Journal of Applied Information Systems (IJAIS)* – ISSN: 2249-0868 Foundation of Computer Science FCS, New York, USA Vol. 4, No. 11, December, www.ijais.org

2. Vasumathi Kannaki S, Porkodi K P, Ananthi M, Department of CSE, Info Institute of Engineering, Kovilpalayam, Coimbatore . "SECURE DATA HIDING USING AN INTEGRATION OF CRYPTOGRAPHY AND STEGANOGRAPHY", *Research Journal of Computer Systems Engineering* - RJCSE CCIIT-2013 ISSN: 2230-8563; e-ISSN-2230-8571.

3. Agrawal Jayesh G, Ashwini Gadge B, Dawange Yogesh P, Chaube Neha V, and Achaliya Parag N (2012), "DATA SECURITY USING CRYPTOGRAPHY, STEGANO-GRAPHY AND LAN MESSAGING "(DSCSL), 1st International Conference on Recent Trends in Engineering & Technology, Mar-2012 Special Issue of *International Journal of electronics, Communication & Soft Computing Science & Engineering*, ISSN: 2277-9477.

4. *"Handbook of Applied Cryptography*" by Alfred J Menezes, Paul C van Oorschot and Scott A Vanstone.

5. "Cryptography and Network Security: Principles and Practice", by William Stallings.

6. "A Course in Number Theory and Cryptography", by Neal Koblitz.

7. "Introduction to Cryptography", by Johannes A Buchmann.

8. "Cryptography Theory and Practice", by Doug Stinson.

9. Secure Data Transmission using Stegnography and Encryption Technique, Shamim Ahmed Laskar and Kattamanchi Hemachandran, *International Journal on Cryptography and Information Security (IJCIS)*,Vol. 2, No. 3, September 2012.

10. Novel Security Scheme for Image Steganography using Cryptography Technique, *International Journal of Advanced Research in Computer Science and Software Engineering*, Vol. 2, Issue 4, 2012.

11. Archana S Vaidya, Pooja N More, Rita K Fegade, Madhuri A Bhavsar, Pooja V Raut (2013), "Image Steganography using DWT and Blowfish Algorithms", *IOSR Journal of Computer Engineering* (IOSR-JCE), e-ISSN: 2278-0661, p- ISSN: 2278-8727, Vol. 8, Issue 6 (Jan. - Feb. 2013), pp. 15-19.

12. Firas A Jassim (2013), "A Novel Steganography Algorithm for Hiding Text in Image using Five Modulus Method", *International Journal of Computer Applications* (0975–8887), Vol. 72, No. 17.

13. Patel K and Kauwid Rora K (2013), "Lazy Wavelet Transform Based Steganography in Video", International Conference on Communication Systems and Network Technologies.

14. Qin C, Ying-Hsuan Huang (2013), "An Inpainting-Assisted Reversible Stegano-graphic Scheme Using a Histogram Shifting Mechanism", *IEEE transactions on circuits and systems for video technology*, Vol. 23, No. 7.

15. Sharma V and kumar S (2013), "A new approach to hide text in image using Steganography", *International journal of kumar advanced research in computer science and software engineering,* Vol. 3, Issue 4.

16. Steffy Jenifer K and Yogaraj G (2014), "LSB approach for video Steganography to embed images" *International journal of computer science and information technology,* Vol. 5, No. 1.

17. Kumar A, Sharma R (2013), "A secure image Steganography based on RSA algorithm and Hash-LSB technique", *International journal of kumar advanced research in computer science and software engineering,* Vol. 3, Issue 4, Vol. 3, Issue 7, July 2013.

18. Gupta H and Chaturvedi D (2013), "Video Data Hiding Through LSB Substitution Technique", *Research Inventy: International Journal Of Engineering And Science,* Vol. 2, Issue 10.

19. Debiprashad B and Dasgupta K (2014), "A novel secure image Steganography method based on chaos theory in spatialdomain", *International of security, privacy and trust management (IJSPTM),* Vol. 3, No. 1.

20. Sharp A and Sharif H (2013), "A Video Steganography Attack Using Multi-Dimensional Discrete Spring Transform", *IEEE International Conference on Signal and Image Processing Applications (ICSIPA).*

International Journal of Engineering Research and Science & Technology
Hyderabad, INDIA. Ph: +91-09441351700, 09059645577
E-mail: editorijlerst@gmail.com or editor@ijerst.com
Website: www.ijerst.com