TRANSMISSION OF CRYPTIC TEXT USING ROTATIONAL VISUAL CRYPTOGRAPHY

P. R. Sushma Priya[1], P. Vijaya Bharati[2]

[1]student, [2]Asst.Prof.,Department of CSE, Vignan's Institute of Engineering for Women, Visakhapatnam, Andhra Pradesh, India, ***sushmapriya_pr3135@yahoo.co.in, pvijayabharati@gmail.com***

Abstract

Today security is an important thing when we need to transmit data from one location to another safely. In this paper we are proposing an empirical model of secure data transmission technique with a hybrid approach of Cryptography, Stegnography and rotational analysis. In the initial phase, data is encrypted with DES algorithm with the help of Session key which is generated by the Diffie-Hellman Key exchange Algorithm. In the second phase Cipher Data is hidden into the cover image's LSB to form the stego image, by considering security as the optimal security parameter. In the third phase, the Stego image is rotated with specific angle. At the receiver end, the image is de-rotated and the cipher information from the LSB is retrieved and the cipher information is decrypted with session key. This scheme achieves lossless recovery and is difficult to decrypt by the attackers.

Keywords: *Cryptography, Stegnography, Visual Cryptography, DES, Diffie-Hellman Algorithm, Session Key*

----------***----------

1. INTRODUCTION

Cryptography is the method that allows information to be sent in a secure form in such a way that the only receiver is able to retrieve the information. Now-a-days, cryptography has many commercial applications. It provides high level of privacy for individuals and groups. However, the main purpose of the cryptography is not only to provide confidentiality but also provide solutions for other problems like: data integrity, authentication, non-repudiation. Presently continuous researches on the new cryptographic algorithms are going on. However, it is very difficult to find out the specific algorithm they must consider various factors like: security, the features of algorithm, the time complexity and space complexity.

Visual Cryptography (VC) is a new technique of cryptographic scheme, which can decrypt encrypted images without any mathematical computations but with the help of Human Visual System (HVS). Visual cryptography scheme has many applications like secret sharing scheme, Copyright protection, Halftoning process and Watermarking. There are various schemes of Visual Cryptography. Visual Cryptography scheme can also be used for authentication and identification process (visual authentication and identification)[11].

Steganography is the art and science of invisible communication. This is accomplished through hiding information in other information, thus hiding the existence of the communicated information. The word steganography is derived from the Greek words "stegos" meaning "cover" and "grafia" meaning "writing" , defining it as "covered writing". In image steganography the information is hidden exclusively in images [8].

The main feature of the encryption/decryption process implementation is the generation of the encryption key. Our hybrid approach achieves the optimal security during the transmission of data over the network. Due to three levels of security, cipher text cannot be decrypted and the time required to break the cipher to plain is more.

Our approach follows the conversion of plain text to cipher text, hiding the cipher information in the image pixels and rotating the image with the required or specific angle to prevent the unauthorized access over the network [5].

The main difference between Cryptography and stegnography is, Cryptography is a process of converting a plain text to cipher text where as Stegnography is a process of hiding the data into the cover medias [3]. Image rotation enhances our security feature by integrating with our previous stegnography because of the noise factors we regularized our approach to few specific angles of rotation of pixels in the image.

2. RELATED WORK

As our initial research starts with the different types of attacks, mainly classified as Active attacks (Interruption, modification, fabrication) and passive attacks(Interception) during the transmission of data, Cryptography introduced to convert the formatted text to unformatted text through the various cryptographic algorithms[1][2].

Now-a-days hackers and attackers are also very familiar with cryptanalysis(cracking of ciphers or unformatted texts),so cryptography may not resolve the problem of security, later stegnography is introduced for hiding the data into the image, which is a simple implementation issue and human eye undetectable changes are seen. In this process we consider these two parameters i.e., cover image and the message are embedded and form the stego image. Even though various cryptography and stegnographic approaches are developed, security is still an importantant research issue in the field of network security [6][7].

Here we are introducing a new approach that uses image rotational analysis along with the cryptographic and Stegongraphic techniques.

In the traditional process of visual cryptography, data can be added to the Cover image to convert it into stego image and the stego image can be divided into number of shares, to retrieve the data, we need to combine the shares, there is a noise issue during the data retrieval. In our approach there is no issue of noise during the stego image conversion or during image rotation.

3. PROPOSED MODEL

We are proposing a hybrid approach with both cryptography and rotational visual cryptography for secure data transmission over the network. In our approach, initially the sender converts the plain text to cipher text with Data Encryption Standard (DES) algorithm. The reason to choose DES and Diffie-Hellman algorithms in our paper is, DES is most certified algorithm than the many traditional cryptographic algorithms. Implementation of DES is not complex and it is fast in hardware and relatively fast in software. But the DES requires a 56-bit session key for the process of encryption and decryption, which can be achieved by the Diffie-Hellman key exchange protocol. After the session key generation, the sender converts the plain text to cipher text by DES algorithm with the key generated by the key exchange protocol (Diffie-Hellman)[10]. It is one of the most efficient Symmetric key approach. No individual user can create the session key, without using the other half part of the receiver or sender. Diffie-Hellman ephemeral key exchange provides perfect forward secrecy. Computational complexity is low during the key calculations and not much expensive. The cover image is selected and is converted into binary format and the cipher text is embedded into the LSB of the binary format of the image which forms the stego image. The stego image is rotated by some specific angle and is sent to receiver. The reverse process is done at the receiver end. The receiver receives the rotated image and the encrypted angle with the same session key exchanged by Diffie-Hellman key exchange protocol. The entire process is shown in architectural Fig-1.

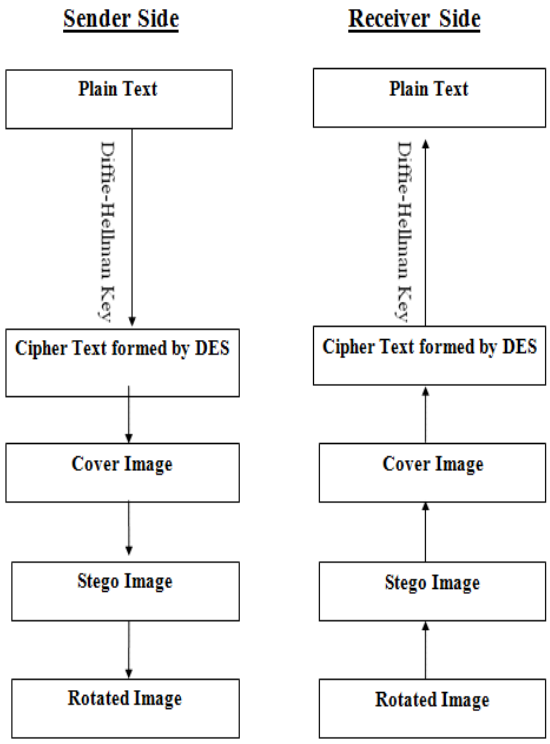

Fig-1: Architecture

4. LSB APPROACH

LSB (Least Significant Bit) substitution is the process of adjusting the least significant bit pixels of the carrier image. It is a simple approach for embedding message and the image. The Least Significant Bit insertion varies according to number of bits in an image. For an 8 bit image, the least significant bit i.e., the 8th bit of each byte of the image is changed with the bit of cipher text. For a 24 bit image, the colors of each component like RGB (red, green and blue) are changed. LSB is effective in using BMP images since the compression in BMP is lossless [4].

5. ROTATIONAL ANALYSIS

Rotational Analysis is a new approach where the image is rotated with an angle instead of sending it directly. In our approach, after hiding the data in the image, it is rotated with a specific angle by the sender and is sent to the receiver. The angle is transmitted in encrypted format using the session key generated by Diffie-Hellman Key Exchange Algorithm. In the reverse process, receiver decrypts the angle and than of 900,1800,2700, de-rotates the image with the same angle, extracts the cipher information from the stego image (i.e., least significant bits of the pixels of image) then converts the cipher information to plain text with the DES algorithm followed by the key generated with Diffie- Hellman Key Exchange.

6. EXPERIMENTAL RESULT

Fig-2 shows the plain text , Fig-3 shows the cipher text, Fig-4 shows the binary text, Fig-5 shows the cover image before embedding data into it, Fig-6 shows the stego image (i.e., after data embedding) and Fig-7 shows the rotated image as follows

Fig-2: Plain Text

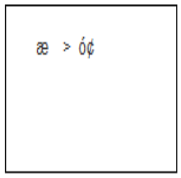

Fig-3: Cipher text

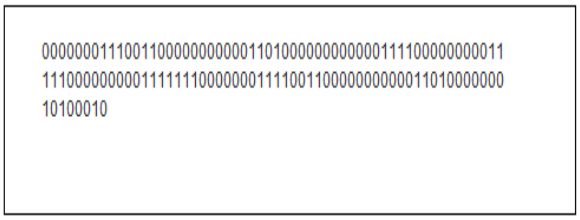

Fig-4: Binary Text

Fig-5: Cover Image

Fig-6: Stego Image

Fig-7: Rotated Image

While in the reverse process, we derotate the image with the specific angle and retrieve the cipher information from the LSBs of the stego image to retrieve the final cover image and plain text.

CONCLUSIONS

We are concluding our research issue with empirical approach of data hiding through rotational visual cryptography. Our experimental result shows an efficient performance results than the traditional approach with hybrid mechanism of cryptography, stegnogrpahy and rotational visual cryptography.

FUTURE SCOPE

- We can enhance our approach by using the advanced cryptographic algorithms like AES, but Computational complexity is the major issue with the advanced algorithms.
- We designed our architecture with some specific static angles, we can enhance our system by providing the flexibility of rotation of image with any angle.
- We can also enhance our approach with elliptic curve key exchange Algorithm for more secure session key generation.

REFERENCES

[1] A. Forouzan.,: " Cryptography and Network Security ", First Edition. McGraw-Hill, (2007), USA.

[2] R Hamamreh., M Farajallah., " Design of a Robust Cryptosystem Algorithm for Non-Invertible Matrices Based on Hill Cipher ". International Journal of Computer Science and Network Security, (2009): Vol (9), pp: 12-21.

[3] J Hoffstein., et al, "An Introduction to Mathematical Cryptography ", First Edition. Springer Science & Business Media, (2008):, Germany.

[4] H.Kenneth, “Elementary Number Theory and Its Applications " Third Edition. Addison-Wesley, (1992): Germany.

[5] M.Lucas, “Thomas Jefferson wheel cipher ", Monticello Research Department, Thomas Jefferson Foundation, Charlottesville, (1995):, VA.

[6] Steganography and steganalysis-Robert Krenn, Internet Publication, March 2004

[7] Steganographic Techniques and their use in an Open-Systems Environment- Bret Dunbar, The Information Security Reading Room, SANS Institute 2002

[8] Steganography Primer - Ruid, Computer Academic underground,2004

[9] Image Compression and Discrete Cosine Transform - Ken Cabeen and Peter Gent,Math 45 College of the Redwoods,1998

[10] Practical Data Hiding in TCP/IP - Kamran Ahsan and Deepa Kundur Multimedia and Security Workshop at ACM Multimedia,
Juan-les-Pins, France, Friday, Dec 6th, 2002

[11] "Rotation Visual Cryptography Using Basic (2, 2) Scheme", International Journal of Computing Science and Communication Technologies, VOL. 3, NO. 2, Jan. 2011. (ISSN 0974-3375) ,1B. Dinesh Reddy, 2V. Valli Kumari, 3KVSVN Raju, 4Y.H. Prassanna Raju 1Vignan Institute of Information Technology.

BIOGRAPHIES

P. R. Sushma Priya received the M.C.A degree from JNTU, Hyderabad in 2007. She is pursuing the M. Tech(Computer Science Engineering) degree from JNTU, Kakinada. She worked as an assistant professor in Vignan's Institute of Engineering, Visakhapatnam, Andhra Pradesh, India.

P. Vijaya Bharati received the M.Sc degree in Computer Science from Gitam University in 2004, Visakhapatnam and the M.Tech degree in Computer Science from Vignan University in 2009. She is pursuing her Ph.D from Gitam University, Visakhapatnam. Presently, she is working as an Assistant Professor in Vignan's Institute of Engineering for Women. Her research interests in areas of Computer Networks, Mobile Computing, DSP, MATLAB, Data Mining, Sensor Networks. She attends so many Workshops and National & International Conferences.