International Journal of Advanced Research in

Computer Science Engineering and Information Technology

Volume: 2 Issue: 3 08-Apr-2014,ISSN_NO: 2321-3337

CREATING AN IMAGE USING ENCRYPTED SENSITIVE WORDS

Reshmi.R.V

Student, Dept. of Information Technology, CSI College Of Engineering, India

ABSTRACT--*Data hiding is one of the most better data and communication protection by hiding information into a media carrier technology called as stegnography. The actual information is not maintained in its original format is known as cryptography. In our daily life we are sending message through email, mobiles, social medias etc… But sometimes the unauthorized person (hackers) will easily hack our secret message. Now days it's very difficult to send a secret message from sender to receiver. To provide the solution to this problem this paper provides a high security for sending the secret message from sender to receiver. This paper shows the method of creating an image using encrypted sensitive words. Mainly two methods are used in this "*Stegnography, Cryptography*". This application mainly used in defense, business, etc… for sending secret message more securely.*

Keywords—Stegnography, Cryptography, Encryption.

1. INTRODUCTION

Currently, Internet and digital media are getting more and more popular. So, requirement of secure transmission of data also increased. Various good techniques are proposed and already taken into practice.

Data Hiding is the process of secretly embedding information inside a data source without changing its perceptual quality. Data Hiding is the art and science of writing hidden messages in such a way that no one apart from the sender and intended recipient even realizes there is a hidden message. Generally, in Data Hiding, the actual information is not maintained in its original format and thereby it is converted into an alternative equivalent multimedia file like image, video or audio which in turn is being hidden within another object. This apparent message is sent through the network to the recipient, where the actual message is separated from it. The requirements of any data hiding system can be categorized into security, capacity and robustness. All these factors are inversely proportional to each other so called data hiding dilemma. The focus of this paper aims at maximizing the first two factors of data hiding i.e. security and capacity coupled with alteration detection. The proposed scheme shows the method of creating an image using encrypted sensitive words.

2. SYSTEM ANALYSIS

2.1 EXISTING SYSTEM:

Now a days, several methods are used for communicating secret messages for defense purposes or in order to ensure the privacy of communication between two parties. So, information is hidden in away that prevent its defection.

Techniques to hide valuable information with in seemingly harmless messages have been widely used for centuries. The actual information is not maintained in its original format is known as cryptography Typically, there we have to use the appropriate when encryption is not available. In this , new cover mediums for hiding the data in communication are constantly being proposed, from the classical image files (such as bmp, gif and jpg formats) and from audio files(i.e. wav and mp3),text and html documents, emails disguised as spam, TCP/IP packets, executables programs, DNA strands etc..Some of the methods used for privacy communication are the use of invisible links; convert channels are some of the existing systems that are used to convey the messages. Audio and video files have massive levels of imperceptible noise. Changing tone bits and the pause duration between notes are great places to hide. Data hiding techniques for written text change spacing and the placement individual characters. Even large hard drivers on PCs can be used to hide the data. File system like FAT or NTFS allocated blocks for storage. Most of the time these blocks have unused space where secret messages can be stored.

2.1.1 ADVANTAGE OF EXISTING SYSTEM

- The user can Record the Voice and encrypt the message in to that wave file.
- It supports Watermarking methods to Encode.

2.1.2 DISADVANTAGE OF EXISTING SYSTEM:

- Non Provision of encryption Key.
- Length of is Limited to 500.
- Consume much time to encode and decode.

2.2 PROPOSED SYSTEM

In this paper we are "**CREATING AN IMAGE USING ENCRYPTED SENSITIVE WORDS"**. For the hacker it's very difficult to find the message. The proposed system is more users friendly and flexible. Data can be used in any form. More accurate result is produced . Fast and secure accesses to data are possible. Compression option is used because large amount of data to be send.

2.2.1 ADVANTAGE OF PROPOSED SYSTEM

- Save Time and Money.
- Reduce the Response Time.

- Easy to Use.
- Flexible and Stable.

- That it can be used to secretly transmit messages without the fact of the transmission being discovered .
- The Secret Message contains a picture.

3. MAIN FEATURES:

Steps:

a) Type the secret message, Encrypt the message by using asymmetric RSA algorithm
b) Select an image.
c) Now the computer have to draw an image using encrypted sensitive words(figure-1), By using pixel mapping method.
d) By using the decryption key the receiver extract the secret message from
The sensitive word image.

Figure-1

- This is an example of the image with sensitive words. This image is full of words.
- For the first time viewer, this is just an image. The person will not recognize the words used to draw this image.

After coloring the image it is like (figure-2)

- So it is very difficult to recognize the words used to create that image.

- This is an Innovative and efficient technology to hind the secret message by creating an image.

Figure-2

3.1 Data size estimation

Each drown image is taken data source for Data Hiding. First the maximum size of the hiding data is calculated . The size of the image is 2000 ×1000 and modified it to 2048 × 1024. On further calculations we get786,432,000 chars that can be embed. We have followed the following equation mentioned below: (((Width × height) × 3 bits)/8 bits)/3 bytes × 3000 frames = char/video.And the image Bitmap size = 2048 × 1024 Step of calculations the maximum of hiding information:

a. Each frame consist = 2048 × 1024 = 2, 097, 152 Pixels.
b. Each pixel include 3 bytes (One byte we use single bit for encode data hiding) R = 1bit, G = 1 bit and B = 1 bit.
c. Each frame = Pixels ×3 = 2, 097, 152 × 3 = 62, 915, 456 bits
d. Each frame we can maximum hiding data is 62, 915, 456 bits/8 bits = 786, 432 bytes.

e. If this video 3000 frames = 786, 432 × 3000 = 2, 359.296, 000 bytes (1 bytes = 1Character).
f. For 1 Character of Unicode we need 3 bytes/1 character of Unicode = 2,
359.296,000 bytes/3 =786, 432, 000 chars.

4. SYSTEM SPECIFICATION

4.1 SOFTWARE SPECIFICATION:

OPERATING SYSTEM : Windows 7
FRONT END : Microsoft visual studio .Net 2010
CODING LANGUAGE : C#.Net

4.2 HARDWARE SPECIFICATION:

SYSTEM : Intel core i5
HARD DISK : 500GB
MONITOR : 15 VGA colour monitor.
MOUSE : Logitech
RAM : 4 GB
KEYBOARD : 110 keys enhanced.

5. PROJECT DESCRIPTION

5.1 PROBLEM DEFINITION

The problem in the existing system is the data hide behind the Image. In this paper we are drawing or creating an image using encrypted sensitive words. The encryption done by using RSA algorithm which is been more secured, so it will be very difficult to decrypt by the hacker.

5.2 OVERVIEW OF THE PROJECT

In this paper the encryption done by using RSA algorithm and the computer drawing or creating an image using encrypted sensitive words. which is been more secured, so it will be very difficult to decrypt by the hacker.

5.3 RSA ALGORITHM:

RSA is an Internet encryption and authentication system that uses an algorithm developed in 1977 by Ron Rivest, Adi Shamir, and Leonard Adleman. The RSA algorithm is the most commonly used encryption and authentication algorithm and is included as part of the Web browsers from Microsoft and Netscape. It's also part of Lotus Notes, Intuit's Quicken, and many other products. The encryption system is owned by RSA Security. The company licenses the algorithm technologies and also sells development kits. The technologies are part of existing or proposed Web, Internet, and computing standards.

5.3.1 How the RSA System Works

The mathematical details of the algorithm used in obtaining the public and private keys

are available at the RSA Web site. Briefly, the algorithm involves multiplying two large prime numbers (a prime number is a number divisible only by that number and 1) and through additional operations deriving a set of two numbers that constitutes the public key and another set that is the private key. Once the keys have been developed, the original prime numbers are no longer important and can be discarded. Both the public and the private keys are needed for encryption decryption but only the owner of a private key ever needs to know it. Using the RSA system, the private key never needs to be sent across the Internet.

The private key is used to decrypt text that has been encrypted with the public key. Thus, if I send you a message, I can find out your public key (but not your private key) from a central administrator and encrypt a message to you using your public key. When you receive it, you decrypt it with your private key. In addition to encrypting messages (which ensures privacy), you can authenticate yourself to me (so I know that it is really you who sent the message) by using your private key to encrypt a digital certificate. When I receive it, I can use your public key to decrypt it.

5.3.2 Communication using RSA

Cryptographic methods cannot be proven secure. Instead, the only test is to see if someone can figure out how to decipher a message without having direct knowledge of the decryption key. The RSA method's security rests on the fact that it is extremely difficult to factor very large numbers. If 100 digit numbers are used for p and q, the resulting n will be approximately 200 digits. The fastest known factoring algorithm would take far too long for an attacker to ever break the code. Other methods for determining d without factoring n are equally as difficult.

Any cryptographic technique which can resist a concerted attack is regarded as secure. At this point in time, the RSA algorithm is considered secure.

6. IMPLEMENTATION STEPS INVOLVE:

6.1 ENCYPTION OF MESSAGE:

In this paper first encrypt the secret message using asymmetric RSA algorithm.

Using an encryption key (e,n), the algorithm is as follows:

1. Represent the message as an integer between 0 and (n-1). Large messages can be broken up into a number of blocks. Each block would then be represented by an integer in the same range.
2. Encrypt the message by raising it to the eth power modulo n. The result is a ciphertext message C.

3. To decrypt ciphertext message C, raise it to another power *d* modulo *n*

The encryption key (*e*,*n*) is made public. The decryption key (*d*,*n*) is kept private by the user.

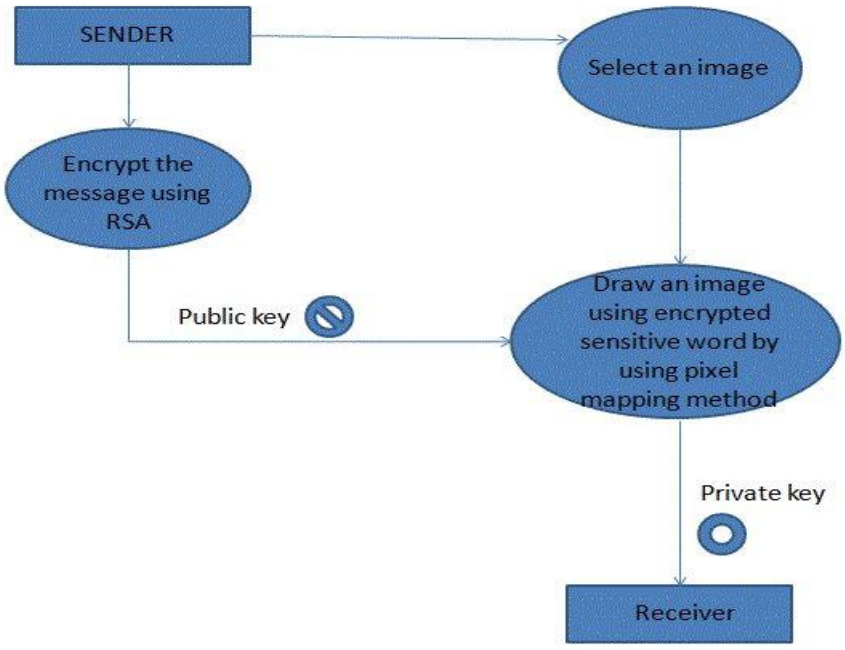
How to Determine Appropriate Values for *e*, *d*, and *n*

1. Choose two very large (100+ digit) prime numbers. Denote these numbers as *p* and *q*.
2. Set *n* equal to *p* * *q*.
3. Choose any large integer, *d*, such that GCD(*d*, ((*p*-1) * (*q*-1))) = 1.
4. Find *e* such that *e* * *d* = 1 (**mod** ((*p*-1) * (*q*-1))).

6.2 CREATING AN IMAGE:

A message, either encrypted or unencrypted, Then using pixel mapping method the system will draw a image using the encrypted sensitive and transmitted over the Internet, a CD or DVD, or any other medium. That is by selecting the pixels from another image and maps the pixel for drawing an encrypted sensitive word. this module is concerned with the creating an image using encrypted sensitive words . Here we are converting the message or plain text in to cipher text format using RSA algorithm. Using RSA the message will be in the cipher text format with the help of public key. The Rivest-Shamir-Adelman (RSA) algorithm is one of the most popular and secure public-key encryption methods. The encrypted words are can't understand by the peoples very easily.

7. ARCHITECTURAL DESIGN:



8. CONCLUSION

In this paper I propose a data hiding technique by creating or drawing an image using encrypted sensitive word. It is a new innovative methodology to hide the data. Main intension is to provide proper protection on data during transmission. For the accuracy of the corrects message output that extract from source we can use a tools for comparison and statistical analysis can be done. Its main advantage is that it is a blind scheme and its affect on image quality or coding efficiency is almost negligible. It is highly configurable, thus it may result in high data capacities. Finally, it can be easily extended, resulting in better robustness, better data security and higher capacity.

REFERENCES

1) Image Steganography and Steganalysis Using Pixel Mapping Method.International Journal of Engineering Research & Technology(IJERT)Vol. 2 Issue 11, November – 2013.
2) Steganography Algorithm to Hide Secret Message inside an Image.
3) Data Hiding in Video Arup Kumar Bhaumik1, Minkyu Choi2, Rosslin J.Robles3, and Maricel O.Balitanas4 International Journal of Database Theory and ApplicationVol. 2, No. 2, June 2009.
4) A Robust Algorithm for Text Detection in Images Julinda Gllavata1, Ralph Ewerth1 and Bernd Freisleben1,2 1SFB/FK 615, University of Siegen, D-57068 Siegen, Germany 2Dept. of Math. & Computer Science, University of Marburg, D-35032 Marburg, Germany juli, ewerth.
5) Image Steganography using DWT and Blowfish Algorithms 1Mrs.Archana S. Vaidya, 2Pooja N. More., 3Rita K. Fegade., 4Madhuri A.Bhavsar., 5Pooja V. Raut. 1Asst. Prof. Department of Computer Engg.GES's R. H. Sapat College of Engineering, Management Studies and Research, Nashik (M.S.), INDIA.

BIOGRAPHY

Ms RESHMI.R.V

CSI COLLEGE OF ENGINEERING

ANNA UNIVERSITY

THE NILGIRIS.