ISSN No:-2456 –2165

Transcribe Sensitive Words into Images

Dr. Firoz Kayum Kajrekar
Asst. Professor, Dept. of CS&IT
SPK Mahavidyalay,
Sawantwadi.

Dr. Chandrashekar Sonawane
Asst. Professor, Dept. of CS&IT,
YCCC College, Sillod.

Abstract— Protection of data by hiding information from unwanted access is one of the better ways into a media carrier technology and is called as steganography. The original information format is changed to other encoded format known as cryptography. Messages or information shared or send through emails, mobiles and other social medias between two known persons are hacked by unauthorized person know as hackers. If message is confidential or of top secret and important than it will be very difficult to send it in the same known format and rely on network security that it is not access by unauthorized person. To provide solution for such and other kind of problem this paper provides a high security method for sending the confidential message from sender to receiver. This paper shows the method of creating an image using encrypted sensitive words. Two methods are used for same one is Steganography and other is Cryptography. These types of applications are mainly used in defense and highly competitive business.

Keywords— Steganography; Cryptography; Hackers; Data Hiding;

I. INTRODUCTION

Secure transmission of data is the need of today with ever increasing use of internet and digital media. Various techniques are put forward and implemented to safeguard the transmission of data through the media.

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.

II. RELATED WORKS

For confidential information sharing or messages for defense purposes or to ensure privacy of communication between two parties, several methods are used to hide information in a way that prevents its defection.

For centuries various techniques are in use to hide valuable information. 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. waved mp3),text and html documents, emails disguised as spam, TCP/IP packets, executable 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, confidential messages can be stored in this blocks having unused space.

A. Advantage of Existing System:

- User can record voice, encrypt message into wave file
- It supports Watermarking methods to Encode

B. Disadvantage of Existing System:

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

ISSN No:-2456 –2165

III. PROPOSED SYSTEM

The proposed system is more users friendly and flexible. In this system we can use data in any format and this create a more accurate result. With this system we can access the data very fast and safe and secure. In the proposed system we can compress the large amount of data to be sent. So, using the proposed system it will be very much difficult for any hackers to encrypt or decode the message.

A. Advantage of Proposed System:

- Save time and money and is easy
- Flexible and stable and reduce the response time
- Message transmitted secretly
- Picture images contains confidential messages

IV. MAIN FEATURES

The confidential messages are encrypted using asymmetric RSA - Rivest Shamir Adliman algorithm. In this feature the sender side selects an image and computer draw this image using encrypted sensitive words using the pixel mapping method. Receiver side uses the decryption keys that extract the confidential and secret message from the sensitive words in image.

The following is the example of the image with sensitive words. This image is full of words. But, the first time viewer think of this as just a simple image, he will not recognize the words used to draw the image.

After coloring the image the image will look as follow and it will be very difficult to recognize the hidden words used while creating this image. This technology is very efficient and innovative to hide the confidential and secrets from the unwanted access.

V. DATA SIZE ESTIMATION

Images are drawn using the data from the source kept for data hiding. The maximum size of data that can be hidden is calculated. The size of the image is 2000 x 1000 and is modified to 2048 x 1024. After calculating still further we get 786,432,000 of characters that can be embedded. 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:

- Each frame consist = 2048 × 1024 = 2, 097, 152 Pixels.
- Each pixel include 3 bytes (We use single bit for encode data hiding) R = 1bit, G = 1 bit and B = 1 bit.
- Each frame = Pixels ×3 = 2, 097, 152 × 3 = 62, 915, 456 bits
- Each frame we can maximum hiding data is 62, 915, 456 bits/8 bits = 786, 432 bytes.
- If this video 3000 frames = 786, 432 × 3000 = 2, 359.296, 000 bytes (1 bytes = 1Character).
- One char of Unicode need 3 byte/1 character of Unicode = 2, 359.296,000 byte/3 =786, 432, 000 char.

A. System Specification

a). Software Specification

- Operating System: Windows 7
- Front End: Microsoft Visual Studio .Net 2010
- Coding Language: C#.Net

b). Hardware Specification

- System: Intel core i7
- Hard Disk: 1 TB
- Monitor: 15" LED Monitor.
- Mouse: Logitech
- Ram: 4 GB
- Keyboard: 110 keys enhanced.

VI. PROJECT DESCRIPTION

A. Problem Definition

The system is for hiding the data in the form of image. In this paper we are creating or printing an image using the sensitive words in a encrypted method. The encryption done by using RSA algorithm which is been more secured, so it will be very difficult to decrypt by the hacker.

B. Overview of the Project

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

C. RSA Algorithm:

RSA is an algorithm used by modern computers to encrypt and decrypt messages. It is an asymmetric cryptographic algorithm. Asymmetric means that there are two different keys. This is also called public key cryptography, because one of them can be given to everyone. The other key must be kept private. It is based on the fact that finding the factors of an integer is hard (the factoring problem). RSA stands for Ron Rivest, Adi Shamir and Leonard Adleman, who first publicly described it in 1978. A user of RSA creates and then publishes the product of two large prime numbers, along with an auxiliary value, as their public key. The prime factors must be kept secret. Anyone can use the public key to encrypt a message, but with currently published methods, if the public key is large enough, only someone with knowledge of the prime factors can feasibly decode the message.

D. How The RSA System works

The RSA algorithm involves four steps: key generation, key distribution, encryption and decryption. A basic principle behind RSA is the observation that it is practical to find three very large positive integers. In addition, for some operations it is convenient that the order of the two exponentiations can be changed and that this relation also implies, RSA involves a public key and a private key. The public key can be known by everyone, and it is used for encrypting messages. The intention is that messages encrypted with the public key can only be decrypted in a reasonable amount of time by using the private key. The public key is represented by the integer's n and e; and, the private key, by the integer d (although n is also used during the decryption process. Thus, it might be considered to be a part of the private key, too), m represents the message.

E. 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.

VII. IMPLEMENTATION STEPS INVOLVE

A. Encryption of Message

The confidential secret message is first encrypt using the asymmetric RSA algorithm. Using an encryption key (e,n), the algorithm firstly 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. Next encrypt the message by raising it to the eth power modulo n. The result is a cipher text message C. To decrypt cipher text 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. To determine appropriate values for e, d, and n following steps can be followed:

- Choose two very large (100+ digit) prime numbers. Denote these numbers as p and q.
- 2.Set n equal to p * q.
- 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))).

B. 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 secures public-key encryption methods. The encrypted words are can't understand by the peoples very easily.

VIII. ARCHITECTURAL DESIGN

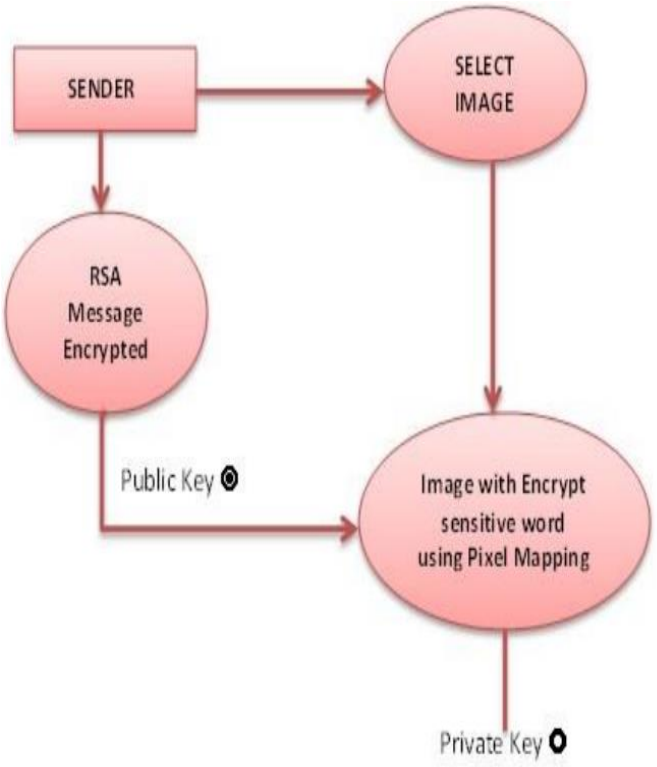

Fig.1 Architectural Design

IX. CONCLUSION

Purpose is 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 correct 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 effect 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, D57068 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