IFERP
connecting engineers... developing research

ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)
Vol 4, Issue 10, October 2017

Hiding of text in a 3D image using steganography

[1] Ms. Chandraleka, [2] Ankita Singh [3] Astha Mehta
[1] Guide, [2][3] Student
[1][2][3] Department of Information Technology,
SRM University, Ramapuram.

***Abstract* - Steganography is the science of hiding data. It is the practice of concealing messages within other non-secret text, images or audio. The word steganography is derived from the greek word “ stegos ” meaning “ cover ” and “ grafia ” meaning “ writing ” defining it as covered writing. Steganography involves hiding information in such a manner that the third party is unaware about the existence of the data. Here, we are using RSA Algorithm in the 1st least significant (LSB Technique) and last 4 significant bits (Modulus 4 bit technique) of the pixel of image. In the RSA algorithm, the third party cannot identify the hidden information easily and even if the third party is able to access the encrypted data, no confidential information will be revealed. In the case of LSB, the data is hidden in the last 4 least significant bits of pixels of images which can’t be detected.MD5 hash algorithm is used to maintain data integrity. Use of hash algorithm provides data integrity. At the receiver’ s end, receiver first get data from image, decrypt it and then find message using the same algorithm and compare it with original message. If the message digest matches with the original message then the data is not tempered and accepted. Therefore, we have applied encryption using RSA and MD5 hash algorithm.**

***Keywords:*--- Data integrity, LSB technique, MD5 Hash Algorithm, Modulus 4 bit algorithm, RSA Algorithm, Steganography.**

INTRODUCTION

Steganography can also be called invisible communication. It is a manner of hiding communication. This can be done by hiding the information in some other data, in a manner that the existence of the information is unknown. The word steganography is derived from the greek word “stegos” meaning “cover” and “grafia” meaning “writing” thereby meaning covered writing . In image steganography the communication is hidden under an image.

The use of steganography can be traced back to the 440BC.Histiaeus sent a message to his vassal, Aristagoras, by shaving the head of his most trusted servant, “marking” the message onto his scalp, then sending him on his way once his hair had regrown, with the instruction. Another instance in history where steganography was used was by Demaratus, who sent a warning about a forthcoming attack to Greece by writing it directly on the wooden backing of a wax tablet before applying its beewax surface. Nowadays, steganography is usually used digitally(to hide digitalised messages in order to hide confidential information).

Steganography is usually confused with Cryptography.

Cryptography is a technique of hiding information when using untrusted third party medium(either apps or website), while Steganography is technique of composing hidden messages so that only the sender and the receiver know about the message. In Steganography, only the sender and the receiver know about the existence of the message, whereas in cryptography the existence of the encrypted message is visible to the everyone. Due to this Steganography removes the unwanted attention. Crytographic methods try to protect the content of a message, while steganography uses the methods that would hide both the message as well as the content. It is based on keys and applying keyed transformation to data and the data changes to encrypted data so that with the key one can reverse the transformation(or check authenticity).On the other hand, Steganography is method to modify text or other form of information transforming the source to a target file which encodes a message but without knowing the key the image looks like a normal image.

Water marking and finger printing are two other technologies that are closely related to steganography. These technologies are used for the protection of intellectual property and therefore, the algorithms have different requirements.

Steganography is usually used to improve the security of the data using the cryptographic system. Sometimes, the cryptographic is found insufficient and therefore steganography is used to improve the security of the system.

Steganography is modern printers, including Hewlett-Packard and Xerox. These printer add tiny yellow dots to each page. The barely visible dots contain encoded printer serial numbers and date and time stamps. This technique of steganography is also by intelligence services to interact and pass messages among each other.

1.Overview

This used to explain steganography.This can be done in a series of ways:

1.1.Steganography concepts

Steganography is an concept linked with the covering of sensitive data under a layer of another data which can be of any form such as audio ,image or even data itself in a manner that the third party does not know about the existence of the image .The use steganography can be traced back in history to a lot events. Usually, used to transmitted information of very sensitive kind from one place to another in a number of forms. Nowadays, steganography is usually practiced in its digital form. There are many steganographic techniques that can be used to achieve information security.

1.2 Steganography Techniques

1.2.1.Physical Technique

Modern day steganography entered the world in 1985 with the emergence of personal computers by applying classical steganography to the digital form. Development of this form steganography has been slow , but some kinds of softwares' are still available:

a)Concealing messages within the lowest bits of noisy images or sound files

b)Concealing data within encrypted data or with random data. The message is first encrypted and hidden within data.

c)Mimic functions converts one file to have the statistical profile of another. This can thwart statistical method that help brute-force attacks identify the right solution in ciphertext-only attack.

d)Concealed text in tampered executable files, exploiting redundancy in the targeted instruction set.

e)Pictures in video material(can be played at higher or lower speed)

f)Injecting imperceptible delays to packets sent over the network from the keyboard. Delays in key presses in some applicants can mean a delay in packets, and the delays in the packet can be used to encode data.

g) Changing the order of elements in set.

h) Content-Aware Steganography hides the information in the semantics a human user assigns to a datagram. These systems offer security against a nonhuman warden.

Physical technique can also include social steganography which is used in:

a)Hiding a message in the title and context of a shared video or image.

b)Misspelling names or words that are popular in the media in a given week, to suggest an alternate meaning.

c)Hiding a picture which can be traced by using Paint or any other drawing tool.

1.2.2.Network

All information hiding techniques that maybe used to exchange steganograms in telecommunication networks can be classified under the general term of network steganography. This name was proposed by Krzysztof Szczypiorski in 2003. The first book on network steganography was published in 2016 by Mazurczyk et al. Typical steganographic methods use digital media to hide data, network steganography uses communication protocols' control elements and their intrinsic functionality. As a result, such methods can be harder to detect and eliminate.

Normally, network steganography methods involve modification of the properties of a single network protocol. Such modification can be applied to the PDU(Protocol Data Unit), to the time relations between the exchanged PDUs, or both (hybrid methods).

Network Steganography has two techniques namely,

a)Steganography-the concealment of messages in Voice-over-IP conversations, e.g. the employment of delayed or corrupted packets that would normally be ignored by the receiver, or , alternatively, hiding information in the unused header fields.

b)WLAN Steganography-transmission of steganograms in Wireless ocal Area Networks. A practical example of wlan steganography is the HICCUPS system(Hidden Communication System for Corrupted Networks).

1.2.3.Cyber-physical Systems/Internet of Things

Works on Steganography in 2012 have demonstrated the feasibility of steganography for Cyber-physical systems(CPS)/the Internet of things. Some techniques of IOT steganography is similar to network steganography. Specific techniques hide data in CPS components.

1.2.4. Printed

Digital steganography output can be in the printed document form. A message, the plain text, may be first encrypted to form cypher text. Then, a covertext is modified in a manner so that it can contain the cyphertext, giving the stegotext.

Some modern color laser printers integrate the model, serial number and timestamps on each printout for traceability reasons using a dot-matrix code made of small, yellow dots not recognizable.

1.3. Types of steganography

There are typically two kinds of steganographies mainly, audio and image steganography.

1.3.1. Audio Steganography

Embedding secret message in a digital sound is a more difficult process.Variety of techniques for hiding information in digital audios have established. It is the technique of hiding message in a digital audio .The most common algorithm used for audio steganography is LSB(Least significant bit)because it has low computational complexity and easier implementation.

1.3.2. Image steganography

An bitmap image is a digital image composed of matrix of dots. When viewed at 100% ,each dot corresponds to an individual pixel on the display. For image steganography we will use bitmap images. We can achieve this by embedding the data in the least significant bit of image. We can find least significant bit by the method of ARGB(Transparency, Red, Green, Blue).Under ARGB first eight bits(0-7) of the pixel belong to transparency value. The second eight bits (8-15) represents the red colour, third consists of 16-23 bits for green colour and the last 8 bits 24-31 represent the blue colour. The maximum value for each parameter of ARGB system is 28 i.e. 256. If a change is made to the value at the least significant bit that is ,the bit location 0 for alpha value, 8 for red value, 16 for green value and 24 for blue value the impact is likely to be 0.39%(1/256*100).As the change in original value is low we can use LSB of any or all four ARGB bytes for storing information.

2. RELATED WORK

S-Tools and EzStego are tools that use LSB method for hiding information. These tools, in addition to hiding the information in the LSBs, also do some additional processing to make the hiding less detectable. For example, the EzStego tool arranges the palette to reduce the occurrence of adjacent index colors that contrast too much before it inserts the message. This ensures that there is not to much change in the color of the pixel once the LSB is modified.

3. PROPOSED WORK

Steganography is not the same as cryptography, data hiding techniques in cryptography have been widely used to hide the secret messages for long time. Assuring data security is a big dispute for computer users. Business men, professionals, and home users all have some important data that they want to secure from others. Even though both methods provide protection, adding multiple layers of security is always a good practice to use, so Cryptography and Steganography are combined together. By combining, the data encryption can be done by a software and then embed the cipher text in an image or any other media with the help of stego key. The combination of these two methods will enhance the security of the data embedded. This combined chemistry will satisfy the requirements such as capacity, security and robustness for secure data transmission over an open channel. The proposal will be achieved by using Java and Android. These languages will be used to achieve image steganography.

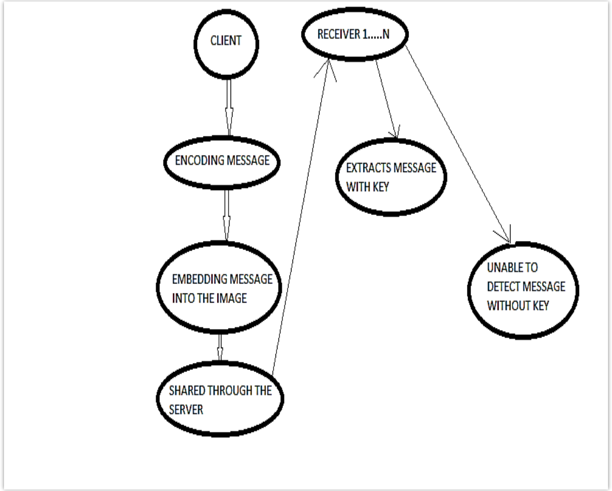
The proposal consists of a messenger app similar to Whatsapp, Messenger. etc which will be created and developed on android studio. The app will permit users to easily interact among each other via simple messages. Or maybe a simpler form can be used by creating a server on PHP to which a number of computers will be connected and will have the ability to interact with each other through the server. The server will have the ability to link all the system and will also act as a link between the computers. Once, the admin uploads data on the server it can be viewed and used by anyone who has access to the server. This technique is usually used in companies, which develop their own intranet to transfer information among the employees.

The next stage of the proposal consists of embedding the message into the image. This is achieved by using Java. The message to be sent is first encoded and then embedded in the image using the above mentioned technique. The secret message can only be viewed by the person who has the access to the key.

So, the message is uploaded on the server and accessed by all the systems connected to the server. The order of the data can randomised to secure the data further. The person who has to access the data has the key and thereby, can view the data or hidden message.

The next stage of the proposal is to decrypted the data from the image using the stegokey and the decoding the message and finally can be viewed by the individual.

In this proposal we will combine steganography and cryptography to increase the data security.


CLIENT
RECEIVER 1.....N
ENCODING MESSAGE
EXTRACTS MESSAGE WITH KEY
EMBEDDING MESSAGE INTO THE IMAGE
UNABLE TO DETECT MESSAGE WITHOUT KEY
SHARED THROUGH THE SERVER

4. REFERENCES

[1].Principles of Steganography by Max Weiss

[2] New generating technique for image steganography by Seifidine Kadry and Sara Nasr

[3] Art of Hiding: An introduction to Steganography by Maninder Singh Rana, Bhupender Singh Sangwan and Jitender Singh Jangir

[4] Wikipedia

[5] Data Hiding Algorithm for Bitmap Images Using Steganography by Mamta Juneja

[6] file:///C:/Users/hp/Downloads/mini%20project.html

[7] Steganography with data integration by Deepali

[8] Steganography Algorithm to hide Secret Message inside an image