Volume : 3 | Issue : 5 | May 2014 • ISSN No 2277 - 8179

Research Paper

Steganography Using SDS Algorithm

Engineering

KEYWORDS : Steganography, Sieving, Shuffling, Random shares.

SONA.N.M S4 M tech CSE, NSS College of Engineering, Palakkad

USHA.K Asst.Proffessor, Dept.of CSE, NSS College of Engineering, Palakkad

ABSTRACT

Steganography is the process of hiding information inside images, audio, or video. The proposed system is Steganography using SDS Algorithm. The main purpose of this system is to reduce the computational cost, computational complexity and also avoid the attackers or eavesdroppers by applying SDS algorithm in Steganography. In this scheme first we convert the text to bit format. And the image is also converted into bits. These bit planes are created based on the RGB values in each bit. Then create a new bit plane by combining the bits of text and image (i.e., hiding text data within images) and then apply SDS algorithm (Sieving, Division, and Shuffling) in order to provide more security to user data. Exactly it provides triple security to the data.

INTRODUCTION

Steganography or Stego as it is often referred to in the IT community, literally means, "Covered writing" which is derived from the Greek language [1]. Steganography is defined by Markus Kahn as follows, [2] "Steganography is the art and science of communicating in a way which hides the existence of the communication. In contrast to Cryptography, where the enemy is allowed to detect, intercept and modify messages without being able to violate certain security premises guaranteed by a cryptosystem, the goal of Steganography is to hide messages inside other harmless messages in a way that does not allow any enemy to even detect that there is a second message present". In a digital world, Steganography and Cryptography are both intended to protect information from unwanted parties. Both Steganography and Cryptography are excellent means by which to accomplish this but neither technology alone is perfect and both can be broken. It is for this reason that most experts would suggest using both to add multiple layers of security. Steganography can be used in a large amount of data formats in the digital world of today. The most popular data formats used are .bmp, .doc, .gif, .jpeg, .mp3, .txt and .wav. Mainly because of their popularity on the Internet and the ease of use of the steganographic tools that use these data formats. These formats are also popular because of the relative ease by which redundant or noisy data can be removed from them and replaced with a hidden message. Steganographic technologies are a very important part of the future of Internet security and privacy on open systems such as the Internet. Steganographic research is primarily driven by the lack of strength in the cryptographic systems on their own and the desire to have complete secrecy in an open-systems environment.

Steganography can be used to hide important data inside another file so that only the parties intended to get the message even knows a secret message exists. To add multiple layers of Security it is a good practice to use Cryptography and Steganography together. The innocent files can be referred to as cover text, cover image, or cover audio as appropriate. After embedding the secret message it is referred to as stego-medium. A stego-key is used to control the hiding process so as to restrict detection and/or recovery of the embedded data. While cryptography is about protecting the content of messages (their meaning), steganography is about hiding the message so that intermediate persons cannot see the message.

EXISTING SYSTEM

In the existing project [3], we use fingerprints images instead of images that contain faces or natural scenes, because fingerprint image offer us the abilities to change the finger print into another valid fingerprint without affecting the degree and clarity of the fingerprint's pixels. This would make it difficult for the adversary to detect the confidential message, because he would assume it is just another fingerprint. When embedding confidential information in images that contain faces, people, animals or natural scenes, the quality of these images will decrease, also the noise and the degrees of colors will be different than the original image. This makes it easier to adversary to observe the noise and quality of the image.

The system is working in two steps in general, the first is hiding the message, at the beginning, and the sender will write or upload his /her secret message to be hidden. Then the system will get two fingerprint images: one is the receiver's fingerprint image, and the second one is a random fingerprint image. After that the system will convert it to bitmap type to conduct the mathematical process on it. The system will compare between the two images and subtract one from the other to generate a new fingerprint image which is called different fingerprint image, The system will extract from the different fingerprint image the positions that are not equal to zero, that means the differences positions. After that the message will be prepared to the inserting process by converting it from string type to bit type. The message will be inserted into the least significant bit of these extracted positions of the random fingerprint image. The second step is unhide the message, the receiver will get the fingerprint image that hides the message from the sender via email, an instant messaging file transfer, media storage devices, or by any way they prefer. Then he/she will upload the fingerprint image that hides the message, and his/her ID into the system, the system will get his/her fingerprint image from the user fingerprint image database and compares it with the fingerprint image that hides the message to get the difference positions that hide the message, then gets the message bits from the difference positions least significant bits. Finally, it converts the bits into string and displays it to the receiver.

Although existing system provide more security to user data, it have some disadvantages. They are the following:

- The processing time required is much higher.
- More computations or processing are take place.
- Both the sender and receiver needs a punching machine thus the cost will be higher.
- It provides single security only.

PROPOSED SYSTEM

In the proposed system we are introducing a new concept,ie Steganography using SDS Algorithm[3],[4]. The main purpose of this system is to reduce the computational cost, computational complexity and also avoid the attackers or eavesdroppers by applying SDS algorithm in Steganography. In this scheme first we convert the text in to bits. The image is also converted into bits. Then create a new bit plane by combining the bits of text and image and then apply SDS algorithm in order to provide more security to user data. Exactly it provides triple security to the data.

SYSTEM OVERVIEW

The main processes involved in this system are as follows: we have exactly two inputs to the system; they are the text file

Volume : 3 | Issue : 5 | May 2014 • ISSN No 2277 - 8179

which we want to send and image file in which we want to hide the text. Based on the loaded image we create a bitmap. And the text (including text file name and content) file is read as bytes. In order to reduce the complexity we are converting both bytes into Boolean value. Hiding of text message is takes place in two steps. In the first step we hide the file name (including its path) inside the image and in the second step we hide the file content inside the image [5]. Mainly three bitmaps are used here; they are input bitmap which is the bitmap of loaded image, changed bitmap created during the encryption process and the decrypted bitmap generated after decryption. After hiding text file data in image we apply SDS algorithm to provide more security [6]. SDS Algorithm means Sieving, Division and Shuffling.

Figure 1: Overview of the System

SDS involves splitting an image into multiple shares [4]. The shares so generated reveal no information about the original secret image. In order to retrieve the secret image we need all the shares. The proposed technique is implemented with the SDS algorithm and involves three steps. In step one (Sieving) the secret image is split into its primary colors. In step two (Division) these split images are randomly divided. In step three (Shuffling) these divided shares are then shuffled each within itself. Finally these shuffled shares are combined to generate the desired random shares.

In order to represent colored images or datas we can use, additive and subtractive color models. In the RGB or the additive model, the three primary colors i.e. Red, Green, Blue are mixed to generate the desired colors. Example: The colors as visible on the computer monitor. Similarly when using the CMY or the subtractive model, the colors are represented by the degree of the light reflected by the colored objects. In this scheme Cyan (C) Magenta (M) and Yellow (Y) pigments are used to produce the desired range of colors. This model is extensively used in printers.

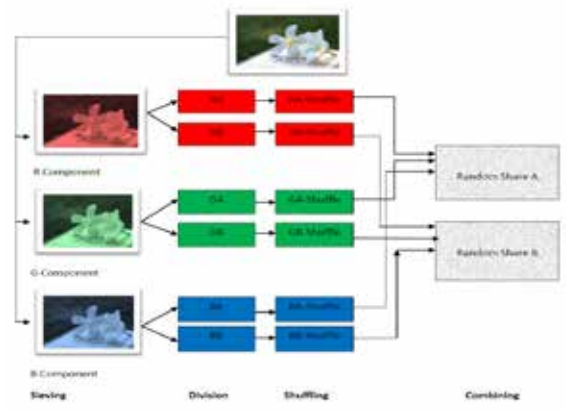

Figure 2: Concept of SDS Algorithm

The scheme implemented using the SDS (Sieve, Division, Shuffle) algorithm involves the following three steps:

Sieving : Sieving involves filtering the combined RGB components into individual R, G and B components (refer Figure 2). The granularity of the sieve depends the range of values that R/G/B component may take individually. To make the process computationally inexpensive, sieving uses the XOR operator.

Division: Division step involves dividing the R, G and B components into z parts/ shares each.

R → (RA, RB, RC,----------, RZ)

G → (GA, GB, GC, ----------, GZ)

B → (BA, BB, BC, ----------, BZ)

(Refer fig2)

Shuffling: In the randomly divided shares, we perform the shuffle operation. This involves shuffling the elements in the individual shares. The sequence in which the elements within the shares are shuffled depends on the value of one of the other shares generated from the same primary color. In other words RB decides how RA is shuffled, RC decides how RB is shuffled, ---------- RZ decides RZ-1 is shuffled and RA decides how Rz is shuffled. Having carried out the above three operations the generated shares are combined to generate the final z random shares (RS).

RSA _ (RA- shuffle, GA- shuffle and BA- shuffle)

RSB _ (RB- shuffle, GB- shuffle and BB- shuffle)

- - - -

RSZ _ (RZ,- shuffle GZ- shuffle and BZ- shuffle)

The random shares so generated individually convey no information about the secret image, however to recover the original image all the random shares would be required. The generic algorithm for the above described process is as under:

Algorithm
1. Sieving
Input _ Secret Image

Sieve (Secret Image)

Output _(R, G, B components)

2. Division
n = total number of pixels (0 to n-1)

Ri / Gi / Bi = individual values of the ith pixel in

the R, G, B components

z = total number of random shares

x =number of bits representing each primary color

max_val = 2x

Repeat 2 for R, G, B component

2(a) for i = 0 to (n-2)

{ for share k = A to (Z-1)

Rki = Random(0, max_val)

Aggr_Sumi = _ Rki

}

Rzi =(max_val + Ri – (Aggr_Sumi % max_val))

% max_val

3. Shuffle
Repeat for RA-Z, GA-Z and BA-Z (all generated

shares)

for k = A to Z

{ Rk-shuffle = Rk

PtrFirstVac = 1

PtrLastVac = n-1

For i = 1 to (n-1)

{ If (R(k+1)(i-1) is even)

{ R(k-shuffle) PtrFirstVac = Rki

PtrFirstVac ++, i++

}

Else

{ R(A-shuffle) PtrFirstVac = RAi

i++, PtrLastVac --

} } }

4. Combine
For k = A to Z

RSk = (Rk-shuffle XOR Gk-shuffle XOR Bk-shuffle)

Thus at the end of the above process we have Random

shares (RSA ,RSB ---------- RSk).

Another important feature of our proposed system is that it can provide image editing options. Ie, we can edit the image which we selected for hiding the information. Image editing options include crop the image, rotate the image, adding animations etc. And another feature of our proposed system is that it can also hide picture messages which is not present in existing system.

CONCLUSION

In summary, the stegnography system using SDS algorithm is used for supporting information security. And for reducing the computational cost and complexity, by employing a new algorithm which split the secret image (including text data) into multiple images or shares and with minimum computation the original secret image can be retrieved back. The system is used by two users; in which one act as the secret message sender and the other act as the receiver. The proposed system has the following merits (a) The processing time required is much lower (b)Both the sender and receiver needs only this software in their system thus the cost will be lower (c)It provides triple level security.

REFERENCE

[1] Monika Agarwal-"TEXT STEGANOGRAPHIC APPROACHES: A COMPARISON"- International Journal of Network Security & Its Applications (IJNSA), Vol.5, No.1, January 2013. | [2] Wikipedia-Steganography, History. | | [3] Hanan Mahmoud, Aljoharah Al-Dawood , Dhay Yousef AL-Salman." Novel Technique for Steganography in Fingerprints Images: Design and Implementation1". | | [4] Siddharth Malik, Anjali Sardana, Jaya." A Keyless Approach to Image Encryption" | | [5] A. Shamir, "How to share a secret," Commun. ACM, vol. 22, no. 11, pp. 612–613, 1979. | | [6] Arpad Incze, "Pixel sieve method for secret sharing & visual cryptography" RoEduNet IEEE International Conference Proceeding Sibiu 24-26 June 2010, ISSN 2068-1038, p. 89-96 | |