Secure Transmission of Compound Information Using Image Steganography

Lalitha.G
Department of ECE,
K L University
Guntur, Andhra Pradesh

Ashish Jain
Department of ECE,
K L University
Guntur, Andhra Pradesh

U. Raja
Department of ECE,
K L University
Guntur, Andhra Pradesh

Abstract— The security of information handled in real time transmission reception like internet is of paramount consideration, as this information may be confidential. And also, the parameter in concern now-a-days is size as it makes large amount of data to be at a single place. This paper proposes a technique for the simultaneous transmission of multiple data securely. We took an advantage of less space required for storing an image than that of a wav file. The proposed technique brings down the required channel capacity to transfer secret data in real time systems besides improving robustness

Keywords- ***Steganography, cryptography, RSA, Stego-image***

I. INTRODUCTION

The word steganography is derived from the Greek words “*stegos*” meaning “cover” and “*grafia*” meaning “writing” [1] defining it as “covered writing”. In image steganography the information is hidden exclusively in images. Since the rise of the Internet one of the most important factors of information technology and communication has been the security of information.

Cryptography (from Greek kryptós, "hidden", and gráphein, "to write") is, traditionally, the study of means of converting information from its normal, comprehensible form into an incomprehensible format, rendering it unreadable without secret knowledge, the art of encryption. The art of protecting information (plain text) by transforming it (encrypting it) into an unreadable format is called cipher text.

Steganography differs from cryptography in the sense that where cryptography focuses on keeping the contents of a message secret, steganography focuses on keeping the existence of a message secret [2]. Steganography and cryptography are both ways to protect information from unwanted parties but neither technology alone is perfect and can be compromised. Once the presence of hidden information is revealed or even suspected, the purpose of steganography is partly defeated [2]. The strength of steganography can thus be amplified by combining it with cryptography.

A successful attack on a steganographic system consists of an adversary observing that there is information hidden inside a file, while a successful attack on a watermarking or fingerprinting system would not be to detect the mark, but to remove it [3]. Research in steganography has mainly been driven by a lack of strength in cryptographic systems. Many governments have created laws to either limit the strength of a cryptographic system or to prohibit it altogether [4], forcing people to study other methods of secure information transfer

Image Compression: When working with larger images of greater bit depth, the images tend to become too large to transmit over a standard Internet connection. In order to display an image in a reasonable amount of time, techniques must be incorporated to reduce the image’s file size.

Compression plays a very important role in choosing which steganographic algorithm to use. Lossy compression techniques result in smaller image file sizes, but it increases the possibility that the embedded message may be partly lost due to the fact that excess image data will be removed. Lossless compression though, keeps the original digital image intact without the chance of lost, although is does not compress the image to such a small file size. An example of an image format that uses the lossy compression technique is JPEG (Joint Photographic Experts Group). The most popular image formats that use lossless compression is GIF (Graphical Interchange Format) and 8-bit BMP (a Microsoft Windows bitmap file)

II. THE PROPOSED TECHNIQUE

Fig.1 below shows the block diagram of the proposed technique’s transmission side setup. The input messages can be in any digital form, of course all the forms, and are often treated as a bit stream. For the *image input*, first, the secret image is compressed using wavlet compression. It is then encrypted using public key algorithm – RSA. Of all the public-key algorithms proposed over the years, RSA is by far the easiest to understand and implement. It is also the most popular, named after the three inventors – Ron Rivest, Adi Shamir and Leonard Adleman. RSA gets its security from the difficulty of factoring large numbers. The public and private keys are functions of a pair of large (100 to 200 digits or even larger) prime numbers. Recovering the plaintext from the public key and the ciphertext is conjectured to be equivalent to factoring the product of the two primes.

For an *audio input*, the procedure said above is same except that before doing so, we need to convert it to an image to have an advantage of reduced size.

For a text input, it is simply converted to an image by some mathematical manipulation. Thus, at each stage we get an output image as 1,2,3. Now, all these images are hidden in a single large image. Choosing an appropriate size for embedding saves the space and thus increases the embedding capacity. The encryption at each stage provides more security for the hidden information. The algorithms at various stages are as follows:

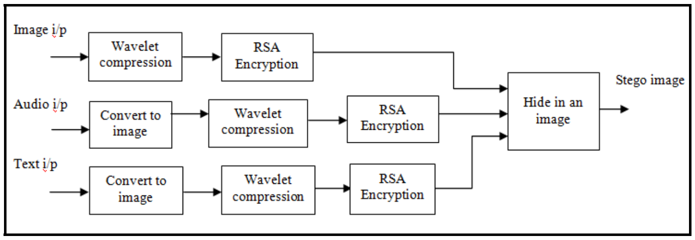

Fig.1: Transmission setup

A. Wavelet compression:

Basically, the wavelet compression scheme consists of three operations, which are the transform, quantization and entropy encoding operations.

Step1: First, wavelet transform is used to analyze the non-stationary phenomena that are often found in two-dimensional digital images.

Step 2: Then, scalar quantization is applied to remove the redundancies in the images with no visible loss under normal viewing.

Step 3: Finally, entropy encoder is used to compress the image in an efficient way where a large reduction of image size occurs. To reconstruct the compressed image, the operations are reversed.

B. RSA algorithm:

Step.1: To generate the two keys, choose two random large prime numbers, p and q. For maximum security, choose p and q of equal length. Compute the product:

$n = pq$ ----- *(1)*

Step.2: Then randomly choose the encryption key, e, such that e and $(p - 1)(q - 1)$ are relatively prime.

Step.3: Finally, use the extended Euclidean algorithm to compute the decryption key, d, such that
$ed = 1 \bmod (p - 1)(q - 1)$

In other words, $d = e-1 \bmod ((p - 1)(q - 1))$ ---------(2)

Note that d and n are also relatively prime. The numbers e and n are the public key; the number d is the private key. The two primes, p and q, are no longer needed. They should be discarded, but never revealed.

Step.4: The encryption formula is simply

ci = (mi^e) mod n -----------(3)

Step.5: To decrypt a message, take each encrypted block ci and compute

mi = (ci^d) mod n ----------*(4)*

thus, public key: n,e, private key: d, ciphertext:c, decoded message:m.

C. Algorithm for sound to image conversion:

Step.1: Compute the size of wav file and save it

Step.2: Choose the required image size to be converted and modify the data accordingly such that the wav data (usually <1) is converted to a value in the range [0,255]

Step.3: Save the converted data as an image with some extension .bmp, .jpg or some other required format.

D. Algorithm for Text to image conversion:

Text data can be converted to image by a simple mathematical manipulation using Matlab.

III. RESULTS AND DISCUSSION

In the proposed technique, we are transmitting image, audio & text files simultaneously. Thus, we have outputs at each stage of input file.

- If we consider the *secret image stage*, the results are as follows:

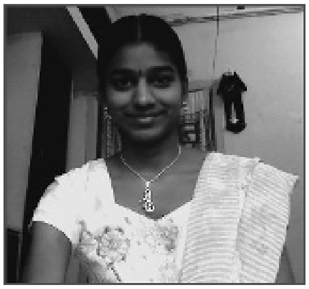

Fig 2: Secret image

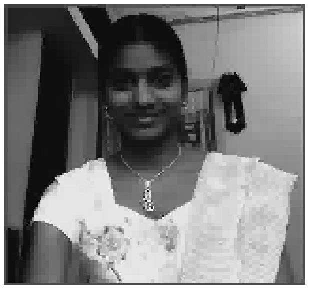

Fig 3: Wavelet compressed image

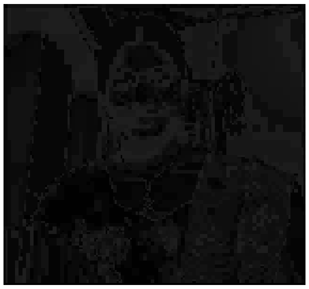

Fig 4: RSA Encrypted image

- If we consider the *secret audio stage*, the results are as follows:

The secret audio file consider here is of size 275 KB and the corresponding converted image is of size 39.7 KB, thus the size is reduced by the process of conversion.

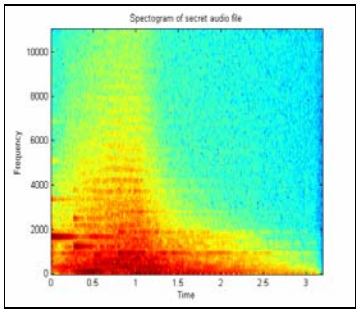

Fig 5: Spectrogram of audio file

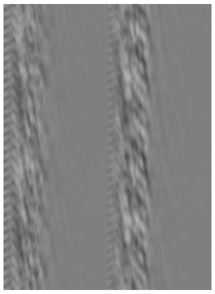

Fig 6: audio→image

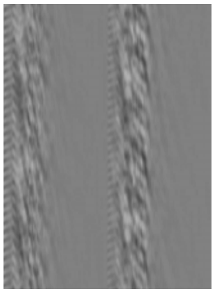

Fig 7: compressed audio Image

Fig 8: Encrypted

- If we consider the *secret text stage*, the results are as follows:

The secret text file consider here is of size 2.15 KB and the corresponding converted image is of size 733 Bytes, thus the size is reduced by the process of conversion.

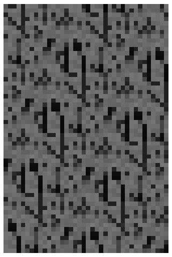

Fig 9: Text → image

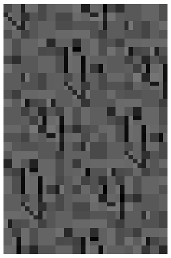

Fig 10: Compressed text image,

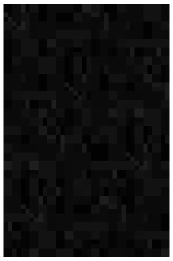

Fig 11: Encrypted image

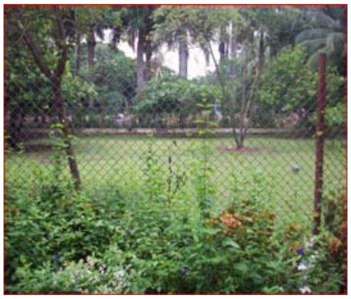

Fig 12: Stego-image

Table 1: Text Vs Converted Image file sizes

S.No	Size of Text file	Size of converted Image file
1.	8.61 KB	3.09 KB
2	4.30 KB	1.08 KB
3	2.15 KB	920 Bytes

Table 2: Audio Vs Converted Image file sizes

S.No	Size of Audio file	Size of converted Image file
1.	275 KB	39.7 KB
2	168 KB	30.7 KB
3	117 KB	19.2 KB

These tables show the results of our algorithm used to convert text to image and audio to image. From these tables, we can say that the conversion of text → image & audio → image brings the advantage of reduced file size. This makes us to send more information at a considerably lesser size.

IV. Conclusion

We proposed a technique for the simultaneous transmission of multiple data securely. The compound information considered in our example is a single audio, single image & a single text file which is transmitted securely by providing security at each stage. Thus the proposed technique brought down the required channel capacity to transfer secret data in real time systems besides improving robustness. We can also transmit multiple audio files or multiple image files or whatever the compound information might be securely at a lesser size compared to that of the size required to transmit each file independently.

References

[1] Moerland, T., “Steganography and Steganalysis”, *Leiden Institute of Advanced Computing Science*, www.liacs.nl/home/tmoerl/privtech.pdf

[2] Wang, H & Wang, S, “Cyber warfare: Steganography vs. Steganalysis”, *Communications of the ACM*, 47:10, October 2004

[3] Anderson, R.J. & Petitcolas, F.A.P., “On the limits of steganography”, *IEEE Journal of selected Areas in Communications*, May 1998

[4] Dunbar, B., “Steganographic techniques and their use in an Open-Systems environment”, *SANS Institute*, January 2002

[5] A. Graps, "An Introduction to Wavelets"**,** *IEEE Computational Sciences and Engineering*, Vol. 2, No. 2, Summer 1995, pp 50-61.

[6] M.L. Hilton, B.D. Jawerth, A. Sengupta, ” Compressing Still and Moving Images with Wavelets„, *Multimedia Systems*, Vol. 2 and No. 3, Apr. 18, 1994

[7] C. Mulcahy, ” Image Compression Using The Haar Wavelet Transform„, *Spelman College Science & Mathematics Journal*, Vol. 1, No 1, Apr. 1997, pp. 22-31.

[8] Tom Davis “RSA Encryption” *http://www.geometer.org/mathcircles* October 10, 2003

[9] Bruice Schneier, Applied Cryptography Protocols, Algorithm and Source Code in C. Second edition. Wiley India edition 2007.

[10] Divakar Roy “Hide_images in a single large image” Copyright (c) 2009.