International Journal of Engineering Sciences Paradigms and Researches, Vol. 02, Issue 01, December 2012
ISSN (Online): 2319-6564
www.ijesonline.com

Data Security Management Using Message Encoding and Covert Communication

Dr. Grima Dhingra[1], Ms. Sumity[2]

[1]A. P., Deptt. of Physics, MDU, Rohtak
grimadhingra@gmail.com

[2]Deptt. of Physics, MDU, Rohtak

Abstract

Secure data exchange between two parties over the internet is one of the major issues. In this paper approach is used to provide the security to key exchange over internet by implementing all the security methods collectively. The complete procedure is divided in different stages and these all stages are used sequentially to make a true method of data key security. These methods include: key Encoding, key Compression and key Steganography. In first phase the message encoding method is used to generate the 128 bit key which is thus compress in next phase so as to reduce its length. This form is such smaller one that can be used bit by bit in out next phase. The final phase includes the phenomenon of hiding the encoded compressed data in an image through Steganography. To perform this Steganography the task in again divided in sub stages. At first we have to find the areas from the image that have higher density, thus we have to compare each pixel with all its surrounding pixels. As each pixel is in touch of 8 surrounding pixels, we have to find pixels that have maximum no. of different pixel around it. As we get some areas the next work is to find the bit pattern of that pixel. Next work is to replace the LSB (least significant bit) of each such pixel by the bit that we get in term of compressed bit pattern. This process is repeated for all pixels obtained from the compressed key. Finally we get the image with data behind it.

Keywords: *Encryption, Compression, Steganography, Least Significant Bit, pixel.*

1. Introduction

With the huge growth of computer networks and the latest advances in digital technologies, a huge amount of digital data is being exchanged over various types of networks. Thus security is the biggest issue so as to prevent the data from unauthorized access. A major part of this information is confidential and private which leads to an increase demand of various strong encoding and steganographic techniques. As a result there are various encryption algorithms and it can be argued that there is no single encryption algorithm satisfies different image types.

Steganography or covert communication means covered or secret writing, is art of hiding information. While cryptography provides privacy, steganography is intended to provide secrecy. If a sender uses cryptography, and send a coded pile of gibberish that only the web site can decipher. Though your code may be unbreakable, any hacker can look and see you've sent a message. For true secrecy, you don't want anyone to know you're sending a message at all. In essence, it "camouflages" a message to hide its existence and make it seem "invisible" thus concealing the fact that a message is being sent altogether. Thus, an encrypted message may draw suspicion while an invisible message will not.

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 secret message present. While performing the data hiding techniques certain specifications are assumed such as degradation of cover data must be kept to a minimum, and the hidden data must be made as immune as possible to possible attack from manipulation of the cover data. Thus in the proposed technique described in the paper the message called plain text is encoded to cipher text by encryption and after that encrypted key obtained is compressed so as to provide the sort of smaller form of data and then steganography is applied by finding the pixel in dense area of image and replacing the LSB of pixel with required bit pattern.

Thus, it will be used to reduce the chance of the encrypted image being detected and then enhance the security level of the encrypted images. Furthermore, this information will be used to enable the receiver to reconstruct the same secret transformation table after extracting hidden data and hence the original image can be reproduced by the inverse of the transformation, decompression and encryption processes.

2. Problem Statement

The main issue discussed here is the development of a better technique that uses not only one method for security of data but the combination of all methods such as cryptography, compression and steganography. While dealing with cryptography for sending data through insecure media like internet an intruder always knows about the presence of information in the message and may apply various means to retrieve the information while in combination of the techniques the message is encoded first and then this encoded message is covered in image so that if intruder intercepts it then it is unaware of the presence of any useful data. Thus major challenge is to define a method that surly and effectively hides the message into cover media like image. However the most important factor is type of cover image selected to hide the message.

2.1 Issues in Image Steganogrphy

In essence, image steganography is about exploiting the limited powers of the human visual system (HVS). Within reason, any plain text, cipher text, other images, or anything that can be embedded in a bit stream can be hidden in an image. To a computer, an image is an array of numbers that represent light intensities at various points, or pixels. These pixels make up the image's raster data. An image size of 640 by 480 pixels, utilizing 256 colors (3 bytes per pixel) is fairly common. Such an image would contain around 300 kilobits of data. Digital images are typically stored in either 24-bit or 8-bit per pixel files. 24-bit images are sometimes known as true color images. Obviously, a 24-bit image provides more space for hiding information; however, 24-bit images are generally large and not that common. A 24-bit image 1024 pixels wide by 768 pixels high would have a size in excess of 2 megabytes. As such large files would attract attention were they to be transmitted across a network or the Internet, image compression is desirable.

Alternatively, 8-bit color images can be used to hide information. In 8-bit color images, (such as GIF files), each pixel is represented as a single byte. Each pixel merely points to a color index table, or palette, with 256 possible colors. The pixel's value, then, is between 0 and 255. The image software merely needs to paint the indicated color on the screen at the selected pixel position. If using an 8-bit image as the cover-image, many steganography experts recommend using images featuring 256 shades of gray as the palette, for reasons that will become apparent. Grey-scale images are preferred because the shades change gradually from byte to byte. This increases the image's ability to hide information. When dealing with 8-bit images, the steganographers will need to consider the image as well as the palette. Obviously, an image with large areas of solid color is a poor choice, as variances created by embedded data might be noticeable. Once a suitable cover image has been selected, an image encoding technique needs to be chosen.

3. Implementation

The proposed technique is divided into phases so the initial input is given as the data to be transmitted and the output obtained is the image with hidden data called as stego image. Thus stages included are:

1. Encoding
2. Compression
3. Embedding

Hence overall function can be represented as:

Output= (key_steganography(key_compresstion(key_cryptography)))

3.1 Encoding

In this stage the message string is converted to the cipher text by the application of 128 bit key and then substitution as well as transposition is applied. Thus the procedure to encrypt the block q of data is:-

```
Encrypt_data(string q)

1. [Generate the bit pattern of message &divide it to group of 128 bits.]
Bit_pattern[]=q;

2. [shift the bits to right to apply transformation]
A1= (q>>1) modulus 127

3. [Again rotate the bit pattern to left]
X1= (q<<2) modulus 127

4. Cipher text=A1*X1+(q>>3)modulus 127
```

3.2 Compression

Now the 128 bit cipher text thus obtained is compressed to reduce the size of message. The compression uses mathematical analysis and formulation so as to convert the 128 bit key to 48 bit. DCT is the most common transformation that is applied to perform compression. It include following steps:

1. Generate the ascii code array of cipher text obtain.

2. Calculate the intensity of occurrence of each code of text.

3. Arrange the values in descending order of no. of occurrences.

4. Assign bit pattern accordingly to each code.

5. Combine all bits to generate compressed data.

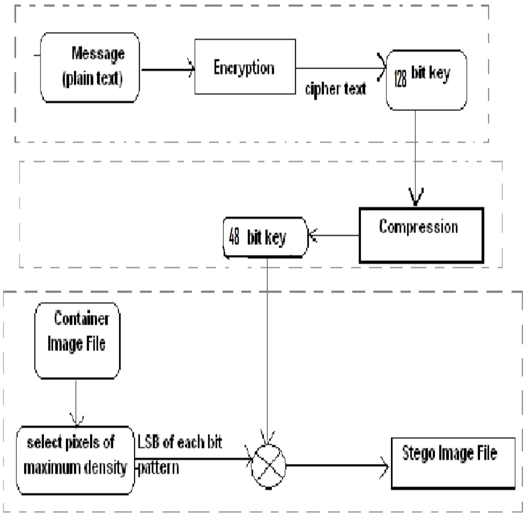

Figure (a) Block Diagram Of Message Encoding and covert communication.

3.3 Embedding

Here we are embedding the encoded text into the image file which will thus send over internet. Container image file is processed so as to find the maximum intensity value pixels.
Now as a pixel is surrounded by maximum eight pixels and most intense pixel will have all eight surrounding pixels of different color values leading to distinction. Thus such pixels are selected and used for replacement. As in 24 bit image the 3 bits are stored in each pixel so for 48 bits we require 16 pixels of different intensity. Thus descending order of intensities is formulated and top 16 pixels are selected to replace their LSB with the encoded key bit pattern.

```
Embed_data(image)
    1. [Find maximum intensity pixels of color image]
       Intensity[]= getpixel( colorvalue (x,y))
    2. [Apply sorting to obtain array values in descending order.]
       Sort(intensity[])
    3. For (pixel=1 to 16 of intensity[]) do
       3.1 Generate bit pattern of pixel.
       3.2 XOR 48 bit key and LSB of pixel.
    4. Return Stego image.
```

4. Conclusion

A steganography method is proposed to embed information within an container image. This method will be expected to spread hidden information within encrypted image data randomly based on the secret key before transmission. Thus, this information appears to be nothing out of the usual and should be available to the receiver safely. However the information can be extracted at receiver's side by again finding high intensity pixels and extraction being performed. The time consumption is less and is easily negotiable. However very small distortion of image can occur after inserting text but effect is negligible. It is the better way to provide security to data transfer over internet.

5. References

[1] A. Sinha, K. Singh, "A technique for image encryption using digital signature," Source: Optics Communications, vol.218, no. 4, 2006, pp.229-234.

[2] A.F. Al-Husainy. Mohammed, "Image Encryption Using Genetic Algorithm," Journal of Information Technology, Vol. 5, No. 3, 2006, PP.516-519.

[3] MAB. Younes, A. Jantan, "Image Encryption Using Block-Based Transformation Algorithm," IAENG International Journal of Computer Science, Vol. 35, Issue. 1, 2008, pp.15-23.

[4] EE. Kisik Chang, J. Changho, L. Sangjin, "High Quality Perceptual Steganographic Techniques," Springer, Vol. 2939, 2004, pp.518-531.

[5] Elke, Fraz, "Steganography preserving statistical properties," proceeding of the 5th internationally Workshop on information Hiding, Noordwijkerhout, The Netherlands, October 2003, LNCS 2578, Springer 2005, pp. 278-294.

[6] G. C. Kessler, "Steganography: Hiding Data within Data," An edited version of this paper with the title "Hiding Data in Data," originally appeared in the April 2002 issue of *Windows & .NET Magazine*. September 2001.

[7] H. El-din H. Ahmed, M. K. Hamdy, and O. S. Farag Allah, "Encryption quality analysis of the RC5 block cipher algorithm for digital images," Optical Engineering, Vol. 45, Issue 10107003.