Data Embedded Security System Using Stenography

Mayuresh bathe1,Vipul bhilare2,Abhishek gole3,Prasad mumbarkar[4]
Electronics and telecommunication Department
KCCEMSR, Thane , India

[1]mayuresh_bathe@yahoo.com ; [2]vbhilare11@gmail.com ;[3]abhi97737@gmail.com[4]mumbarkar465@gmail.com

Abstract - Steganography is the technique of hiding confidential information within any media. Steganography is often confused with cryptography because the two are similar in the way that they both are used to protect confidential information. The difference between the two is in the appearance in the processed output; the output of steganography operation is not apparently visible but in cryptography the output is scrambled so that it can draw attention. Steganalysis is process to detect of presence of steganography. In this project we have tried to elucidate the different approaches towards implementation of steganography using 'multimedia' file such as static images audio and video.

Totally secure steganography systems are those systems whose messages cannot be identified as steganographic messages with any rational means better than random guessing. This fact was stated by Christian Cachin in an information theoretic model for Steganography.

I. INTRODUCTION

Steganography in the last few years has gained a wider audience due in part to the suspicion that the technology may have been used by terrorists to communicate plans for upcoming attacks. While those claims have never been formally substantiated, the technology has certainly been the topic of widespread discussion among the IT community and has provided the benefit of helping more people understand steganography and how it can be used today to conceal information. This report discusses the concepts behind steganography by exploring firstly what it is and how it has been used throughout history. This is followed by technical discussions on how it works and what methods are used to embed information in digital carriers. This report explores the relationship with cryptography and how the two technologies differ. Modern day uses of steganography are then briefly discussed followed by details on how it can be detected through the use of steganalysis. Finally, the conclusion presents 'The Right Way' to use steganography as a means of concealing information and the pitfalls to be wary of by outlining key points to consider when using steganography[1].

Encryption and steganography are the preferred techniques for protecting the transmitted data, as a result, there are various encryption systems to encrypt and decrypt image data, and it can be argued that there is no single encryption algorithm satisfies the different image types. Data exchange is a good example of an application that uses encryption to maintain data confidentiality between the sender and the receiver. In this project, steganography is used to hide information to perform encryption. Steganography techniques are getting significantly more sophisticated and have been widely used. The Steganography techniques are the perfect supplement for encryption that allows a user to hide large amounts of information within an image. Thus, it is often used in conjunction with cryptography so that the information is doubly protected; first it is encrypted and then hidden so that an adversary has to first find the hidden information before decryption take place. The problem with cryptography is that the encrypted message is obvious. This means that anyone who observes an encrypted message in transit can reasonably assume that the sender of the message does not want it to be read by casual observers. This makes it possible to deduce the valuable information. Thus, if the sensitive information will be transmitted over unsecured channel such as the internet, steganography technique can be used to provide an additional protection on a secret message. When hiding information inside images the LSB (Least Significant Bit) method is usually used. While the cryptography tries to convert an image to another one that is hard to understand, steganography involves hiding information so it appears that no information is hidden at all. Therefore, the person will not attempt to decrypt the information. For example, an alteration of the least significant digit for the color value of some pixels in an image will not affect the quality of the image and thus, enabling a message to be sent within an image using these bits. In our project, steganography technique will be used to send the secret information along with an encrypted image. A number of horizontal and vertical blocks at the sender side will be generated, and then mixed with the encrypted image before transmitting it to the receiver. The receiver will need this information to reconstruct the same secret transformation table after extracting the secret information from the encrypted image. Instead of sending the whole secret transformation table, which is usually big, only the secret information is sent. In this approach, the binary representation of the hidden data is used to overwrite the LSB of each byte within the encrypted image randomly. This method will be expected to spread hidden information within encrypted image data randomly based on the secret key before transmission. The values of the correlation and entropy before and after the insertion process are expected to be the same. 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[8].

II. CHOICE OF CARRIER

So, what digital format should you choose to conceal your private message? Steganography can be used in just about any type of file. Here we will only discuss in detail methods used in images, audio and video.

Some of the discussed methods can be used in all three but we will be concentrating on more common methods in each.

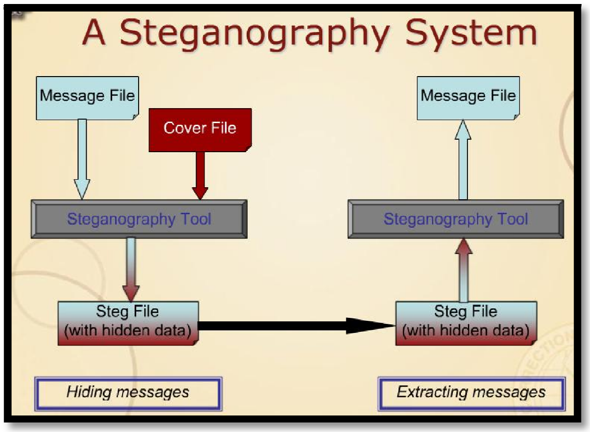
Images

Least Significant Bit

Here we will only specifically discuss its relevance to image files. "To a computer, an image is an array of numbers that represent light intensities at various points, or pixels". An image size of 640 by 480 pixels, utilizing 256 colours (8 bits per pixel) is fairly common and would containaround 300 kilobits of data. Digital images are usually in either 24-bit or 8-bit per pixel formats. 24-bit images are sometimes known as true colour images.

A 24-bit image is easier to hide messages in due to the extra bytes of information. However, because of these extra bytes, it would also be larger than an 8-bit image and the transfer of large images across the Internet can raise suspicion in certain circumstances. Therefore sometimes 8-bit images are chosen as the carrier object with a preference for grey-scale images because the colour transitions from one to another are barely noticeable i.e. changing the LSB is barely noticeable.

III. BASIC ARCHITECTURE



Masking

Image compression can often have an effect on the integrity of the hidden message. There are two types of image compression:

•Lossy – JPEG (Joint Photographic Experts Group) uses this format and offers the highest compression ratio.

•Lossless – BMP (Microsoft Bitmap) and GIF (Graphics Interchange Format) are two formats that provide a higher quality but less compression and therefore are easier carriers to hide messages within.

A simple conversion from a GIF or BMP format to a lossy compression format such as JPEG can destroy the hidden information in the image. Masking or filtering techniques are more effective than LSB when using JPEG images. "By covering, or masking a faint but perceptible signal with another to make the first non-perceptible, we exploit the fact that the human visual system cannot detect slight changes in certain temporal domains of the image". This quote comes back to the fact that human perception does not notice minute changes in colour. However, this form of message hiding is more closely related to watermarking than Steganography although the concept is the same.

Audio

The human ear is extremely sensitive to changes in audio patterns but is not so sensitive to differential sounds i.e. loud sounds tend to mask quiet sounds especially those of the same frequency.

When concealing a secret message in an audio file, one must consider the transmission medium that the file willtravel. Will it be strictly digital? i.e. computer to computer or will it pass over an analog medium such as a home stereo or even over the air to amicrophone? Some methods are more robust to manipulation and noise than others and the transmission medium must be taken into account when choosing a steganographic method. Audio steganography is a classic example of "finding and making use of "natural uncertainty" (e.g. noise)".

Video

Steganography in video generally uses the Discrete Cosine Transformmethod of manipulation. A good example for this method could be video conferencing as described by Westfeld and Wolf. Video conferencingrequires a high frame rate which often places great stress on digitalnetworks. To overcome this problem, it uses differential lossy compression which means that only the differences in each successive still frame are transmitted across the wire. This method essentially eliminates the issue of image comparison to determine differences which can lead to the discovery of the use of Steganography.

IV. DISCRETE COSINE TRANSFORM (DCT)

Embedding messages in an image is seen as an effective way to hide secretdata. However, image compression will destroy the integrity of the hiddenmessage rendering it unrecoverable. The following method explains howsome modern programs overcome this issue:DCT works by using quantization on the least important parts of the image inrespect to the human visual capabilities. Quantization means for example thevalue 5.7489763 can be rounded up to the value 6 and therefore berepresented by a lot less number of bits. Of course, doing this to each andevery value would produce a noticeable distortion in the image. However, thehuman eye under normal conditions does not detect high frequencies inimages so this allows DCT to make larger modifications to these frequencieswith little noticeable image distortion. DCT works by dividing the image upinto smaller areas and performing the quantization on the frequencies thathumans do not normally detect. This is the lossy compression stage. Anysecret message is then injected at this point. The image will then be'lossless compressed' which will not have any impact on the integrity of thesecret message.

V. CONCLUSION

Steganography is one of the less known branches of cryptography. While most cryptography applications work on securing a message so only the sender and receiver can understand it, steganography hides a message so only the sender and receiver know it's there. While everyone may see the public data, they won't know the secret message is present. The secret message can truly be hidden in plain sight.

A new steganography approach for data hiding is proposed. This approach uses the Least Significant Bits (LSB) insertion to hide data within encrypted image data. The binary representation of the hidden data is used to overwrite the LSB of each byte within the encrypted image randomly. Experimental results show that the correlation and entropy values of the encrypted image before the insertion are similar to the values of correlation and entropy after the insertion. Since the correlation and entropy have not changed, the method offers a good concealment for data in the encrypted image, and reduces the chance of the encrypted image being detected. The hidden data will be used to enable the receiver to reconstruct the same secret transformation table after extracting it and hence the original image can be reproduced by the inverse of the transformation and encryption processes.

REFERENCES

[1]. Kipper, Greg "Investigator's Guide to Steganography" Auerbach Publications,
2004

[2]. Fridrich, Goljan, Du. "Reliable Detection of LSB Steganography in Color and
Grayscale Images"
http://www.ws.binghamton.edu/fridrich/Research/acmwrkshp_version.pdf

[3]. Zollner, Federrath, Klimant, Pfitzmann, Piotraschke, Westfeld, Wicke, Wolf.
"Modelling the security of steganographic systems" Paper presented at the 2nd
Workshop on Information Hiding – April 1998, Portland.