Reducing Data Traffic in Digital Watermarking Process

[1]Anita Chauahn, [2] Sahil Dalwal, [3] Anuj Verma
[1]Research Scholar M.tech, [2]Assistant Professor, [3]Assistant Professor
Department of Computer Science
Bells Institute of Management and Technology, Shimla, India

***Abstract* - A digital watermark is a kind of marker covertly embedded in a noise-tolerant signal such as audio or image data. It is typically used to identify ownership of the copyright of such signal. The central proposal of using textual compression is steganography and cryptography. So we don't have to negotiate the quality of digital watermarking. Use of textual compression and encryption affects the digital watermarking. Main aim of this research is to compress the text, which is used as a watermark so that it acquires less space, also to add the security to the image by using the best encryption algorithm. Experimental results show that the visual worth of digital watermarking is excellent and security has also been provided.**

***IndexTerms*- Cryptography, Digital Watermarking, Encryption, Steganography**

I. INTRODUCTION

Digital watermarking is the act of hiding a message related to a digital signal (i.e. an image, song, and video) within the signal itself. It is a concept closely related to steganography, in that they both hide a message inside a digital signal. However, what separates them is their goal. Watermarking tries to hide a message related to the actual content of the digital signal, while in steganography the digital signal has no relation to the message, and it is merely used as a cover to hide its existence. Watermarking has been around for several centuries, in the form of watermarks found initially in plain paper and subsequently in paper bills.[1] The hiding process has to be such that the modifications of the media are imperceptible. For images, this means that the modifications of the pixel values have to be invisible. Furthermore, the watermark must be either robust or fragile, depending on the application. By "robust", we mean the capability of the watermark to resist manipulations of the media, such as lossy compression (where compressing data and then decompressing it retrieves data that may well be different from the original, but is close enough to be useful in some way), scaling, and cropping, among others. [2]

In visible digital watermarking, the information is visible in the picture or video. Typically, the information is text or a logo, which identifies the owner of the media. When a television broadcaster adds its logo to the corner of transmitted video; this is called visible watermark.

In invisible digital watermarking, information is added as digital data to audio, picture, or video, but it cannot be perceived as such (although it may be possible to detect that some amount of information is hidden in the signal).

A. Steganography

Steganography derives from the Greek word steganos meaning covered writing. Steganography is the practice of concealing a file, message, image, or video within another file, message, image, or video [3]. Steganography is about concealing their very existence. Steganography sometimes is used when encryption is not permitted. Or, more commonly, steganography is used to supplement encryption. An encrypted file may still hide information using steganography, so even if the encrypted file is deciphered, the hidden message is not seen.[4]

There are a large number of steganographic methods that most of us are familiar with (especially if you watch a lot of spy movies!), ranging from invisible ink and microdots to secreting a hidden message in the second letter of each word of a large body of text and spread spectrum radio communication. With computers and networks, there are many other ways of hiding information, such as:

- Covert channels (e.g., Loki and some distributed denial-of-service tools use the Internet Control Message Protocol, or ICMP, as the communications channel between the "bad guy" and a compromised system)
- Hidden text within Web pages
- Hiding files in "plain sight" (e.g., what better place to "hide" a file than with an important sounding name in the c:\winnt\system32 directory?)
- Null ciphers (e.g., using the first letter of each word to form a hidden message in an otherwise innocuous text)

Steganography today, however, is significantly more sophisticated than the examples above suggest, allowing a user to hide large amounts of information within image and audio files. These forms of steganography often are 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 information (an often difficult task in and of itself) and then decrypt it. [5]

B. Cryptography

The art of protecting information is by transforming it (encrypting it) into an unreadable format, called cipher text. Only those who possess a secret key can decipher (or decrypt) the message into plain text. Encrypted messages can sometimes be broken by cryptanalysis, also called codebreaking, although modern cryptography techniques are virtually unbreakable. [6]

The difference between steganography and cryptography is that in cryptography, one can tell that a message has been encrypted, but he cannot decode the message without knowing the proper key. In steganography, the message itself may not be difficult to decode, but most people would not detect the presence of the message. When combined, steganography and cryptography can provide two levels of security. Computer programs exist which encrypt a message using cryptography, and hide the encryption within an image using steganography.

II. OUR APPROACH

Main aspire of this research is to find the encryption algorithm which compress the text, so that it requires less space and also provide good security. For this we have selected the simple text and compress it by removing line breaks and spaces.

A. Original Text

Like traditional watermarks, digital watermarks are only perceptible under certain conditions, i.e. after using some algorithm, and imperceptible otherwise. If a digital watermark distorts the carrier signal in a way that it becomes perceivable, it is of no use. Traditional Watermarks may be applied to visible media (like images or video), whereas in digital watermarking, the signal may be audio, pictures, video or texts. A signal may carry several different watermarks at the same time.
(Font size-12, Font Face-Times New Roman)

Procedure to compress data [7]

- Remove line breaks.
- Remove spaces.
- Remove extra spaces

B. Compressed Text

Liketraditionalwatermarks,digitalwatermarksareonlyperceptibleundercertainconditions,i.e.afterusingsomealgorithm,andimperceptibleotherwise.Ifadigitalwatermarkdistortsthecarriersignalinawaythatitbecomesperceivable,itisofnouse.TraditionalWatermarksmaybeappliedtovisiblemedia(likeimagesorvideo),whereasindigitalwatermarking,thesignalmaybeaudio,pictures,videoortexts.Asignalmaycaryseveraldifferentwatermarksatthesametime.

C. Selection of Algorithm

I have selected tiger algorithm, for encrypting the text. Tiger is a cryptographic hash function designed by Ross Anderson and Eli Biam which produces hash value of 128/160/192 bits, according to your expectation. Unlike MD5, there are no known effective attacks on the full 24-round Tiger. While MD5 processes its state with 64 simple 32-bit operations per 512-bit block. Tiger updates its state with a total of 144 such operations per 512-bit block, additionally strengthened by large S-box look-ups. [8]
Tiger is faster than SHA-1 and MD5.

D. *Encrypted text*

26110286971e960653a778dfde1267a1[8]

Table 1: Memory size

	Size of Text		
	Original Text	**Compressed Text**	**Encrypted Text**
MS Office	10.3kb	10.0kb	9.8kb
MS Paint	219kb	219kb	197kb

E. Next Step

Embed the text into an image by using the picture Title.msi software and MS Paint software. We used different software because the MS Paint tells the size of the text only whereas MS Word tells the size of the page.

Size of image: 37.7 Kb
Dimensions: 336 x 402

Table 2: Memory size

Software	Simple Text +Image	Compressed Text +Image	Encrypted Text +Image
Picture Title .msi	32.3	32.3	30.1
Windows MS Paint	260	259.8	245

III. Conclusion

This work has represented a new admittance for data hiding in document images. This paper shows that the size of the encrypted text and the image is reduced and it also provides the authentication and security for the image.

Future work can be concentrated upon finding the best encryption algorithm which further reduces the size of the cipher text and also maintains the security issues.

IV. Acknowledgment

It gives me immense pleasure to express my deepest sense of gratitude and sincere thanks to my highly respected and esteemed guide Ms. Sahil Dalwal and HOD Mr. Anuj Verma for their valuable guidance, encouragement and help for completing this work. Their useful suggestions for this whole and cooperative behavior are sincerely acknowledged. I also wish to express my indebtedness to my parents as well as my family member whose blessings and support always helped me to face the challenges ahead.

References

[1].https://www.cl.cam.ac.uk/teaching/0910/R08/work/essayma485-watermarking.pdf
[2].http://www.alpvision.com/watermarking.htm
[3] http://en.wikipedia.org/wiki/Steganography
[4] http://www.webopedia.com/TERM/S/steganography.html
[5] http://www.garykessler.net/library/steganography.html
[6] http://www.webopedia.com/TERM/C/cryptography.html
[7] http://www.unit-conversion.info/texttools/compress/
[8] http://www.unit-conversion.info/texttools/tiger/