INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH & DEVELOPMENT

ISSN: 2278 – 0211 (Online)

Use Of Textual Compression In Steganography And Cryptography

Dr.Kishori Lal Bansal
Associate Professor, Himachal Pradesh University,
Department of Computer Science, Himachal Pradesh University, Shimla, India
Amardeep Singh
Research Scholar M.Tech,
Department of Computer Science, Himachal Pradesh University, Shimla, India

Abstract:

The recent research and development in the digital multimedia technologies has offered a number of facilities in the transmission, reproduction and manipulation of data.The core idea of using textual compression in steganography and cryptography. So we don't have to compromise with quality of digital watermarking. A encrypted text can affects the picture quality of digital watermarking. Use of textual compression and encryption affects the digital watermarking, but the affects is very small almost negligible. The idea of present scheme is to hide a text or message in a watermark with fractal parameters, Experimental results show that the encrypted document is successfully hidden and the visual quality of digital watermarking is excellent.

Keywords:*Cryptography, Digital watermarking, Steganography, Textual compression.*

1.Introduction

Digital Watermarking started back in 1979, but it was not until 1990 that it gained popularity. No one person is credited with founding or inventing the digital watermark Still in its growth stages today, and with cases like Napster, it is showing more and more reason to have digital watermarking.

Digital watermarking is the process of embedding information into a digital signal which may be used to verify its authenticity or the identity of its owners, in the same manner as paper bearing a watermark for visible identification. In digital watermarking, the signal may be audio, pictures, or video. If the signal is copied, then the information also is carried in the copy. A signal may carry several different watermarks at the same time.

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. The image on the right has a visible watermark. When a television broadcaster adds its logo to the corner of transmitted video; this also is a 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). The watermark may be intended for widespread use and thus, is made easy to retrieve or, it may be a form of steganography, where a party communicates a secret message embedded in the digital signal. In either case, as in visible watermarking, the objective is to attach ownership or other descriptive information to the signal in a way that is difficult to remove. It also is possible to use hidden embedded information as a means of covert communication between individuals.

1.1.Steganography

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 [1].

1.2.Cryptography

Cryptography is the art of protecting information by encrypting it into an unreadable format, called cipher text. Only those who possess a secret key can decrypt the message into plain text. Encrypted messages can sometimes be broken by cryptanalysis, also called code breaking, although modern cryptography techniques are virtually unbreakable.

Steganography is an art of writing message and recipient knows the existence of the message, where as in cryptography message itself is not disguised, but the content obscured and any one see that both parties are communication in secrets [2].

2.Our Approach

Main aim of this research is to compress the text. So that it acquire less space. For experiment we have selected the simple text and compress it by using the remove line width setting method [3]. Original text that we have considered is given below:

2.1. Original text:

2.1.1. Java Language

JAVA is a general purpose object-oriented programming language developed by SUN Microsystems of USA in 1991.Originally called Oak by James Gosling, one of the inventors of the language ,Java was designed for the development of software for consumer electronic devices like TVs, VCRs, toasters and such other electronic machines. The Java team which included Patrick Naughton discovered that the existing languages like C and C++ had limitations in terms of both reliability and portability.

(Font size-12, Font Face- Times New Roman)

Procedure:

- To reduce or remove the line width applying the paragraph marker.
- Replacing the two paragraph markers with a special character ~(a tilde)
- Replacing the single paragraph marker with a space
- Next step is to replacing the special character ~ (a tilde) with single paragraph marker rather than two, to get the section heading back.

2.2.Compress Text:

2.2.1.Java Language

JAVA is a general purpose object-oriented programming language developed by SUN Microsystems of USA in 1991.Originally called Oak by James Gosling, one of the inventors of the language ,Java was designed for the development of software for consumer electronic devices like TVs, VCRs, toasters and such other electronic machines. The Java team which included Patrick Naughton discovered that the existing languages like C and C++ had limitations in terms of both reliability and portability

Next Step:

Encryption of the message or text for encryption of original text. I have selected the MD5 algorithm.

MD5 algorithm – Digest algorithm is a widely used cryptographic hash function that produces a 128 bit (16 bytes) hash value.[4]

It is used commonly in user authentication and MD5 checksum of data integrity.

MD5 algorithm efficiently and effectively helps in reducing the length of the text.

2.3.Encrypted text:

d16fbbde8a8564c502c46330686c00f1 [5]

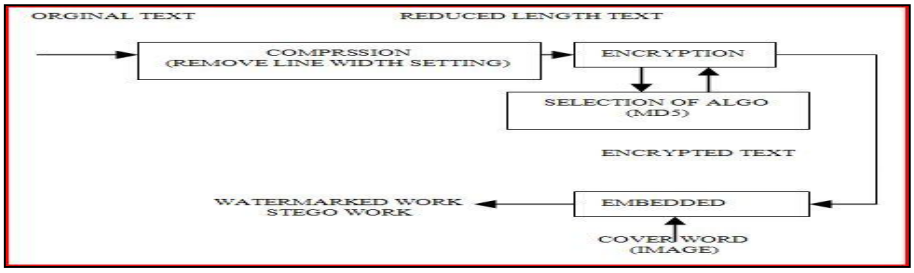

Figure 1: Proposed diagram using compression. (Digital Watermarking)

I have observed that the MS Word is unable to tell the size of text. It tells about the size of the page rather the size of text. MS Paint easily tells us the size of the text

Size of Text			
	Original Text	**Compressed Text**	**Encrypted Text**
MS Office	23.5kb	23.5kb	23.5kb
MS Paint	20.6kb	19.7kb	3.17kb

Table 1: Memory size

Word file extension is .doc

Paint file extension is .JPG

Next step:

Embedding the text on an image by using Picture Title.Msi software

Size of an image: 113kb

Dimensions: 576×461

After using the software the size of watermark image is:

Software	Simple Text+Image	Compressed Text+Image	Encrypted Text+Image
Picture Title .msi	45.1 kb	45.0 kb	43.1 kb

Table 2: Memory size

Embedding the text on an image by using mspaint

After using the software the size of watermark image is

Software	Simple Text+Image	Compressed Text+Image	Encrypted Text+Image
Windows MS Paint	65.2 kb	65.1 kb	53.1 kb

Table 3: Memory size

3. Conclusion

This work has represented a new access for data hiding in document images. The methods or techniques identify the text is invisible in the document images. The technique doesn't affect the quality of the image a lot. Image is slightly altered from its original image. The given message can not easily understandable or readable and the text compression helps us to reduce the size of text as well as the watermarked image size.

Future work may be concentrated on the size of the digital text and selection of encryption algorithm that reduces the encrypted cipher text. So we would get the best results.

4. Reference

1. Digital Watermarking and steganograph by Ingemar J Cox, Matterhew L Miller, Jeffrey A Bloom, Jessica Fridrich , Ton kalker Book second edition.
2. http://www.differencebetween.com
3. http://www.wellsj.com/library/smallwriting.shtml
4. http://en.wikipedia.org/wiki/MD5
5. http://md5decryption.com/