Experimental Study of Word-Shift Text Watermarking Technique

Ms. Monika Patel[#1], Mrs. Priti Srinivas Sajja[*2]

#Asst. Professor,
Computer Science Dept,
Natubhai V. Patel College of Pure and Applied Sciences, V.V. Nagar

`monimpatel@yahoo.co.uk`

*Professor,
Post Graduate Department of Computer Science,
Saradar Patel University
`priti@pritisajja. info`

ABSTRACT

The rapid expansion of the Internet in the past years has rapidly increased the availability of digital data such as audio, images, text and videos to the public. Thus, the problem of protecting multimedia information becomes more and more important. As a solution, Digital Watermarking is the most common and possibly strongest technique for protecting digital data. Digital watermarking is the process of embedding information into a digital signal. The signal may be audio, pictures, Text or video. The embedded information is known as a watermark that can be extracted or detected.

With the wide spread use of the Internet in our society, the distribution and access of information is greatly facilitated. However, without methods which prevent or discourage illicit redistribution and reproduction of information content, copyright can be easily infringed. Text watermarking is widely believed to be a valid solution to the problem and this paper presents the study of new method of word shift text watermarking technique. In this technique, the locations of words are vertically shifted to encode the document. So the encoded document cannot be accessed by any other unauthorized person.

Keywords
Digital watermarking, Watermark, Text Watermarking, Word-shift

I.   INTRODUCTION

Digital watermarking is a method to assert an intellectual copyright in the electronic world. Digital watermarking is the process of embedding information into a digital signal in a way that is difficult to remove. The signal may be audio, pictures or video. The embedded information is known as a watermark that can be extracted or detected [1].

Digital watermarking has become an active and important area of research. There are two types of watermarking techniques are available. In visible watermarking the information is visible in the picture. Typically, the information is text or a logo which identifies the owner of the media. Visible watermarks are easy to create in your photo editor. You can either type in the word SAMPLE or © Photographer's Name on the image itself.

In invisible watermarking, information is added as digital data to audio, picture or video but it cannot be perceive. The watermark, usually a personal Identification Number, is digitally embedded within the image. While these watermarks can be defeated, they offer proof of your ownership if they ever turn up in a publication without your permission.

A. *The working principle of watermarking*

A watermarking system is made up of a watermark embedding system and a watermark recovery system. The system also has a key which could be either a public or a
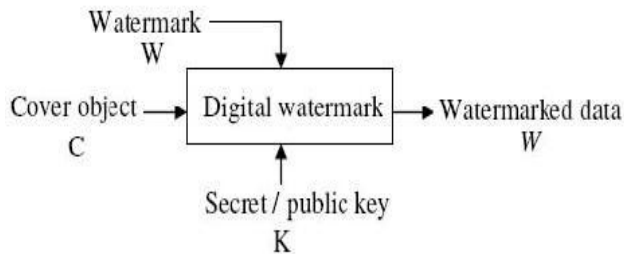

Fig 1: Digital Watermarking - Embedding Process

For the embedding process the inputs are the watermark, cover object and the secret or the public key. The watermark used can be text, numbers or an image. The resulting final data received is the watermarked data W.

B. *Types of digital watermarking*

secret key. The key is used to enforce security, which is prevention of unauthorized parties from manipulating or recovering the watermark. The embedding and recovery processes of watermarking are shown in figure 1 and figure 2 [2].

Fig 2: Digital Watermarking - Extracting process

The inputs during the decoding process are the watermark or the original data, the watermarked data and the secret or the public key. The output is the recovered watermark W.
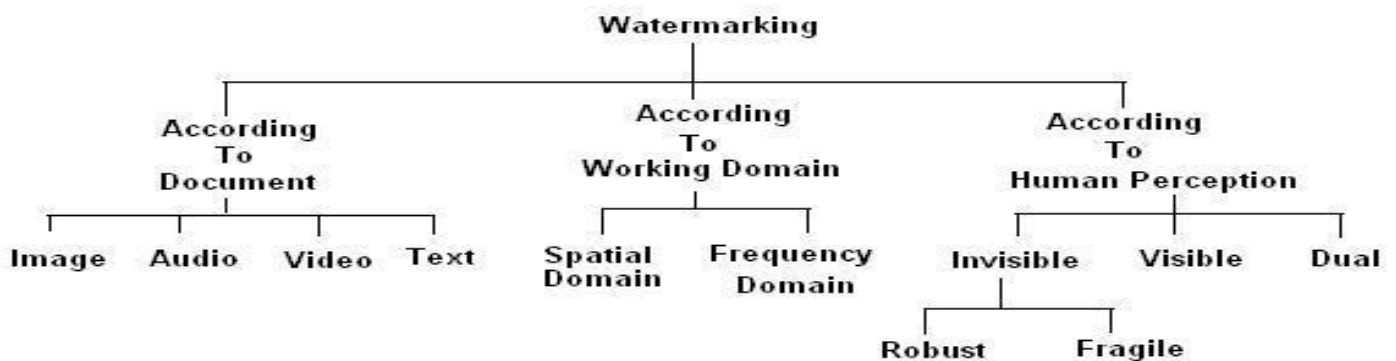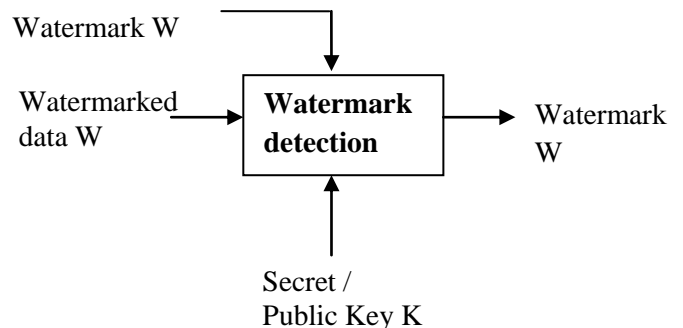

Fig 3: Types of Digital Watermarking

II.   PROPOSED TEXT WATERMARKING MODEL

The proposed a new text watermarking method uses of the distinct character of a text document like space or any

other special characters. The proposed text watermarking model is shown in below figure 4.
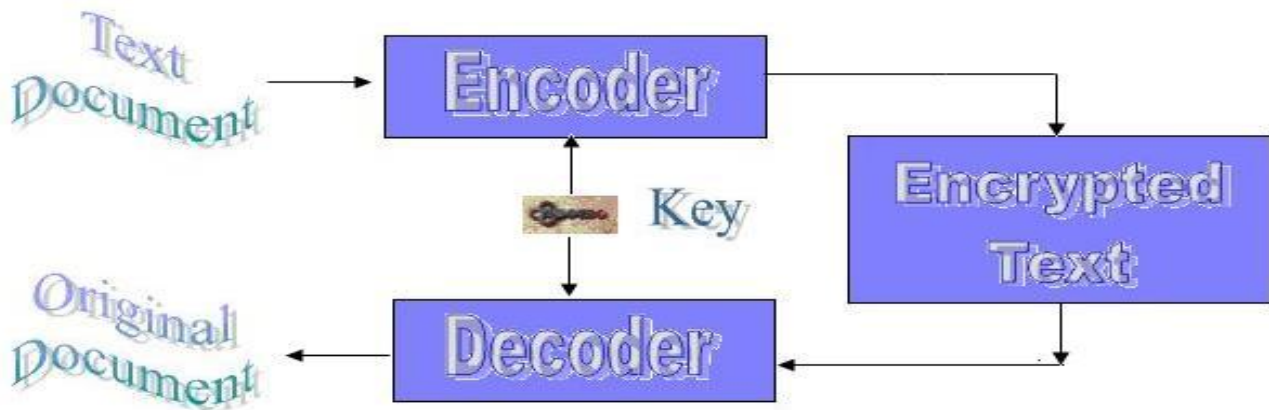
Fig 4: Proposed Text Watermarking Model

In Word-Shift technique each line is first divided into groups of words. Each group has a sufficient number of characters. Then, each even position group is swapped with odd position group. After swapping encryption key is given to the encrypted file. If user wants to decrypt encrypted file then he or she has to know the key. The unique key is given for each encrypted file.

III.   ENCODING AND DECODING ALGORITHM FOR WORD-SHIFT

A. Encoding

Encoding process for Word-Shift technique contains following steps.

1) Read Text file.
2) Divide the text file into words.
3) Swap the odd position word with even position word.
4) Enter encryption key.
5) Save encrypted text into database.

B. Decoding

Decoding process for Word-Shift technique contains following steps.

1) Read Encrypted text file.
2) Enter the key for decryption. It must be same as encryption key.
3) Swap the odd position word with even position word.
4) Convert the words into lines.
5) Save the original file.

IV.   DATABASE USED FOR TEXT WATERMARKING SYSTEM

TABLE 1
Text Watermarking Database

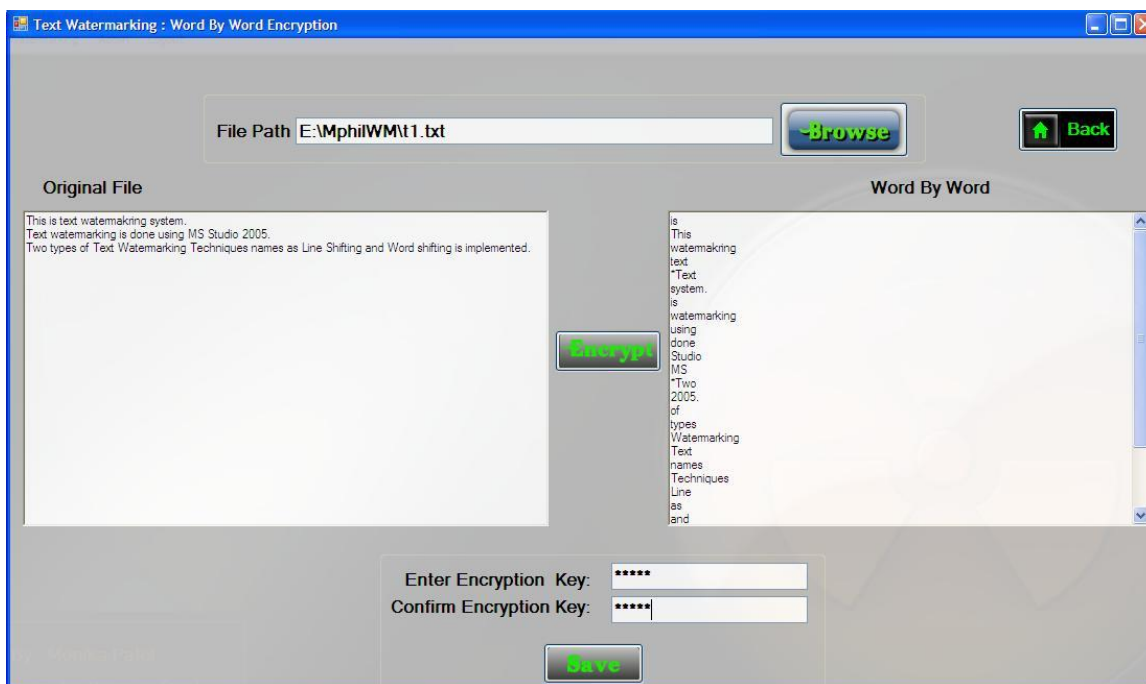| Field Name	Field Type	Field Size	Constraint	Description
Fno	Int	4	-	File no which is auto generated
Fname	Nvarchar	10	-	File name
Skey	Nvarchar	5	Primary Key	Key
Ofc	Ntext	16	-	Original file content
Efc	Ntext	16	-	Encrypted file content

V.   WORKING OF SYSTEM

Fig 5: Result of Word by Word Text Watermarking of Encryption Process

From the above screen when user clicks on Browse button then selected text file will appear in the original file text box control. After this when user clicks on Encrypt button then selected text file will be encrypted word by word and result will appear in the Word by Word text box control. Now user has to input encryption key and confirmation of encryption key. When user clicks on Save button then keys are stored in the database file.
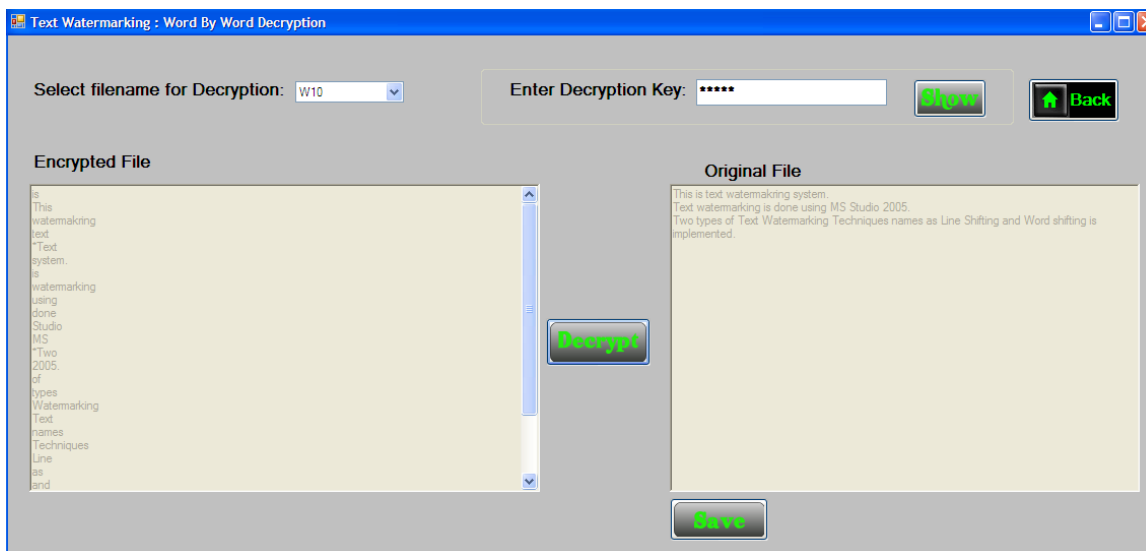

Fig 6: Result of Word by Word Text Watermarking of Decryption Process

For decryption, user has to select encrypted filename from the given drop down box. As well as user has to input valid decryption key. If encryption key and decryption key both are not same then user cannot access the content.

If encryption and decryption key both are same and user clicks on Show button then encrypted file will appear in the text box control. Now when user clicks on Decrypt button then decryption is done and original file will appear in respective control. By clicking on Save button user can also save the file.

VI.   CONCLUSION

This paper presents analytical study of Word Shift Text Watermarking method using Microsoft Visual Studio 2005 with C# language. This method works with text files only. In future, text watermarking is also implemented for word documents. As well as feature coding method can be implemented for text watermarking.

I.   REFERENCES

- http://en.wikipedia.org[1]
- Navneet Kumar Mandhani, "Watermarking Using Digital Sequences", MS thesis, Andhra University, August 2004.[2]
- J. Brassil, S. Low, N. Maxemchuk, and L. O'Gorman, "Electrical Marking and Identification Techniques to Discourage Document Copying*"*, *IEEE Journal on Selected Areas in Communications*, vol.13, no. 8, pp. 1495-1504, October 1995.[3]
- J. Brassil, L. O'Gorman, *"*Watermarking Document Images with Bounding Box Expansion*"*, in Anderson [1], pp. 227-235.[4]
- S. Katzenbeisser, F. A.P. Petitcolas, Eds. "Information Hiding Techniques for Steganography and Digital Watermarking", Boston, Artech House, 2000.[5]
- S. H. Low, N.F. Maxemchuk, *"*Performance Comparison of Two Text Marking Methods*"*, in special issue [5], pp. 561-572.[6]
- S. H. Low, N.F. Maxemchuk, J.T. Brassil, and L.O'Gorman, *"*Document Marking and Identification Using Both Line and Word Shifting*"*, *Proc. Infoncom'95*, Boston, MA, April 1995, pp. 853-860.[7]
- S. H. Low, N.F. Maxemchuk, A.M. Lapone, "Document Identification for Copyright Protection Using Centroid Detection", *IEEE Transactions on Communications*, vol. 46, no. 3, pp. 372-383, March 1998.[8]
- Professional C# 2005 by Christian Nagel, Bill Evjen, Jay Glynn, Morgan Skinner, Karli Watson, Allen Jones, Wrox Publication.[9]