A Zero-Watermarking algorithm on multiple occurrences of letters for text tampering detection

Sukhpreet Kaur
Masters of Technology
Chandigarh Engineering College, Landran
Mohali, India
preet.sukh7@yahoo.com

Geetanjali babbar
Associate Professor, Masters of Technology
Chandigarh Engineering College, Landran
Mohali, India
ergeetanjalibabbar@yahoo.co.in

***Abstract*— Electronic publishing has gained importance with the widespread use of Internet. It involves transmission of digital data in bulk from one place to another. It brings various threats to the data in form of illegal copying, redistribution of copyright contents and forgery. Watermarking provides authentication and copyright protection to the multimedia contents over the Internet. This paper presents a zero- watermarking technique that uses multiple occurrences of letters in a word for generation of watermark. This work will help in tampering detection in the text documents.**

Keywords- ***multiple letters; tamper detection; text documents; text watermarking.***

I. INTRODUCTION

Digital watermarking is a branch of information hiding in which digital data with some hidden information is transmitted over the Internet. It is a technique, which refers to embedding of digital signal into the digital data. The digital signal is also called watermark and consists of information like owner’s name logo or signature etc. It is an identification code that embeds in the data permanently. It provides the copyright protection of the property of owner. Digital watermarking is classified in different categories that are based on the type of data to be watermarked [1]. These are Image watermarking, audio watermarking, video watermarking and Text watermarking.

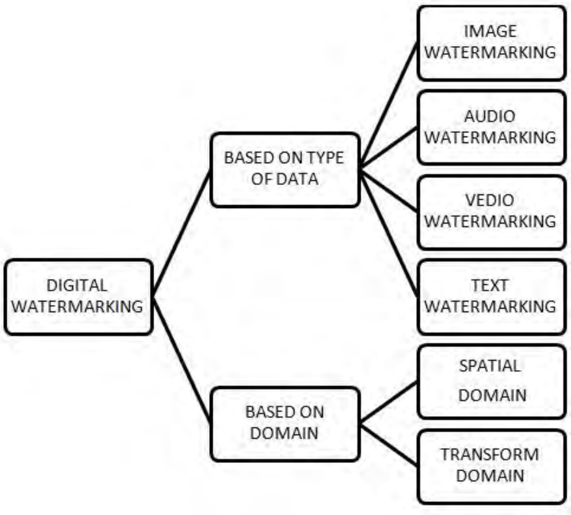


Figure 1. Classification of watermarking

Many day-to-day sources produce digital data like photographs and medical scans in the form of digital images, articles and journals in the form of digital text, sequence of still images in the form of digital videos and music and voices in the form of digital audio. All these forms of data need protection from threats. Watermarking techniques can be divided based on processing domain [2] are:

1. Spatial domain techniques
2. Transform domain techniques

In spatial domain techniques the watermark is directly embedded in the pixel value and there will be a minor change in the intensity of the pixel. Examples of such techniques are LSB based technique, correlation based watermarking technique and CDMA based technique [3].

In transform domain techniques transform coefficients are modified for embedding watermark. These methods are also called frequency domain techniques as these techniques involve the alteration in frequency value from original. Examples of such techniques are DFT, DCT and DWT based watermarking techniques.

An effective watermark has several properties that vary with the applications. Some of the properties are robustness, imperceptibility, security and capacity. It is quite impossible to make such watermarking system, which excels at all these properties. Robustness and security are of major concern.

Robustness can be defined as an ability to resist the modification of the host data due to either processing or other operations that devise to render watermark undetectable. On the other hand security can be defined as an ability of watermark to survive against different types of attacks. These attacks can destroy the communication of information conveyed by watermark such as ownership information [4].

II. TEXT WATERMARKING

Text watermarking is the classification of digital watermarking. Text watermarking is the process of embedding a watermark into the text documents. It generally provides authentication and copyright protection of the document. Text travels commonly over the Internet in the form of books, newspapers, articles and legal documents. As these are the form of plain text so it requires security from the copyright violators. Text watermarking can be used for copy prevention, tamper detection and finger printing. Text watermarking should embed unique watermark that remains present in the document even after tampering attacks. Different types of attacks [5] on the watermark are:

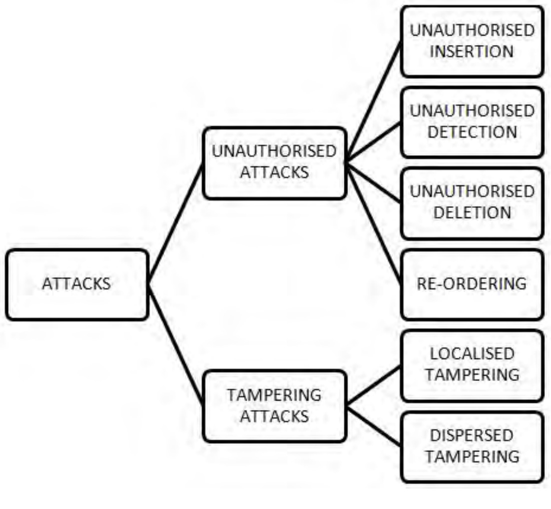


Figure 2. Types of attacks

A. *Unauthorized attacks*

1) *Unauthorized insertion:* This attack involves the addition of words and sentences to the text document to make it look different. An attacker sometimes inserts some text to the original text to add some additional information. When an attacker wants to give some false information for some personal use or to harm other in some way. Example of such attack can be modification in the legal documents. Incorporating a certifying authority in the watermarking architectures can avoid such attacks. These authorities' timestamps the contents in the name of author with current date and time and this timestamp is used to identify the author who registered the content first.
2) *Unauthorized detection:* Unauthorized detection can threaten the security of the watermark present in the document. In some applications, the ability to detect should be restricted.

3) *Unauthorized deletion:* Deletion attack is defined as random deletion of words and sentences from the original text. This attack is made to hide the identity of the owner of the text document by deleting ownership information from the document. Security against unauthorized deletion is required in all watermarking applications. It is more important to secure the watermark that is being embedded in the text document for its protection. The watermark should still survive if the attacker performs a number of alterations in text. Watermark should be detectable by the extraction algorithm.
4) *Reordering:* In text, the words and sentences are reordered or shuffled to destroy the watermark or to make it look different. Certain words are replaced with other words or phrases; merely change in place of words can damage the text document. This attack generally destroys the writing style and meaning of the text.

B. Tampering attacks

Tampering attack is the combination of insertion, deletion and reordering of the text. Tampering can be made at any random location in the text document. Tampering can be done in two ways: localized tampering and dispersed tampering.

1) *Localized:* localized tampering refers to insertion or deletion of words or sentences at a single location in the text. The location can be in the beginning, at the end or anywhere depending upon the attacker's intention of use.
2) *Dispersed:* Dispersed tampering refers to insertion or deletion of sentences and words at multiple locations in the original text. This kind of attack generally occurs in research plagiarism and literary writings.

III. Text Watermarking Approaches

A. Image based approach

In this approach the source of the watermark is the image of the text. Some text watermarking methods utilizing image of text were proposed. These methods [6] are:

1) *Line shifting:* In text document, lines are slightly moved up or down as a watermark to put little difference for human eyes to detect. Odd lines are use at the time of decoding as a reference.
2) *Word Shifting*: A line is made by number of words. So that even group of words is moved left or right as a watermark. In this inter-word spaces are used to embed watermark. Odd group of words is used as reference to calculate the distance at the time of decoding.
3) *Feature coding*: Feature of any specific character is tampered in the document to encode watermark bits in the text. Then it is detected by comparing with original document and watermarked document.

B. *Syntactic approach*

To insert watermark, this approach applies syntactic transformations on text document. A sentence has different syntactic structure [7]. Natural watermarking scheme use syntactic structure of text for watermarking process where syntactic tree is built and to embed the watermark, different transformations to embed the watermark bits are applied.

C. *Semantic approach*

Text constitutes verbs, nouns, objectives, prepositions, word spelling, synonyms, acronyms, sentence structure, and grammar rules and so on. Such semantic contents of text are used to insert watermark [7]. The methods come under this category are:

1) *Synonyms or acronyms substitution*: Specific words are selected then replaced by its synonyms or acronyms in the text document such that the meaning of that document remains same. Then resultant document is watermarked one. Example: a phrase like "This is great news" replaced by "it is a good news" or "This is awesome news" [8].
2) *Noun verb based technique*: in this technique, nouns and verbs in the sentence are parsed using grammar parser and semantic network.
3) *Text pruning and grafting*: The algorithm is based on text meaning representation strings [9].

D. *Some other approaches*

There are more approaches to text watermarking these are given below:

1) *Technique based on not important content*: some change in the expression will not change the meaning of the document, so this is used as watermark [10].

2) *Font size and font coding*: In font size, coding character 0.5 in watermarked document increases font size otherwise keep document as it is. In font coding, Microsoft word has many types of fonts some of them are almost same means that the difference between them is not identified easily. Such fonts are used for watermarking. [11].
3) *Key based*: There is an object-based environment in which each text string is considered as different object. Each object has properties and attributes. So by using key, watermark is generated and embedded based on properties of object [12].
4) *DWTC*: This technique is dual watermarking technique that is based on web documents. Watermark embedded into web document. This technique highly improves invisibleness and robustness [13].

IV. Proposed Algorithm

Text watermarking approaches aims at embedding watermark information into the protective information like text. The information is used for tamper detection and copyright protection. A zero watermarking approach was proposed in which the host data is not altered to embed watermark, rather the characteristics of host text are used to generate a watermark. To generate a watermark, the contents of text document are utilized. This watermark pattern is later matched with the pattern generated by tampered document to identify any tampering. The watermark generation and extraction process is illustrated in fig.3. Watermark is used in the extraction algorithm later to detect tampering in the text document. The contents of text are utilized to protect it. An attacker will always try to tamper document in such a way that the document looks different but the meaning remains same. The attacker modifies the text and change the place of different words like nouns and verbs but cannot avoid them to make a sentence. Tampering can be passivation, clefting, topicalization or re-phrasing [14]. All these tampering do not alter the nouns, adjectives or proverbs that usually contain more than 4 letters.

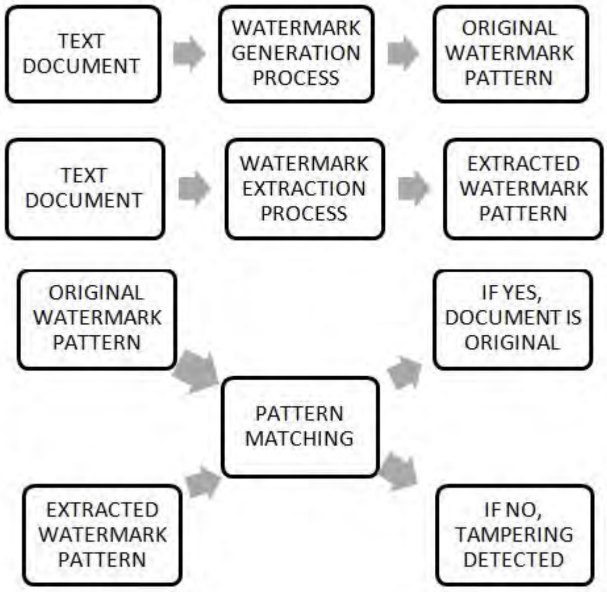
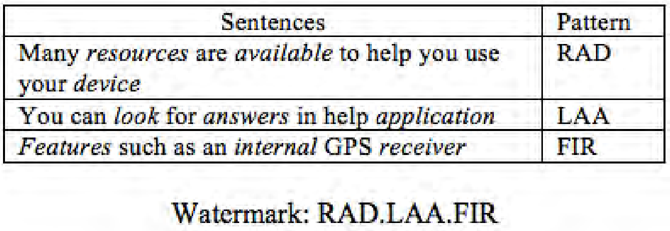

TEXT DOCUMENT
WATERMARK GENERATION PROCESS
ORIGINAL WATERMARK PATTERN
TEXT DOCUMENT
WATERMARK EXTRACTION PROCESS
EXTRACTED WATERMARK PATTERN
ORIGINAL WATERMARK PATTERN
IF YES, DOCUMENT IS ORIGINAL
PATTERN MATCHING
EXTRACTED WATERMARK PATTERN
IF NO, TAMPERING DETECTED

Figure 3. Watermark Generation and Extraction Processes

In this proposed algorithm, words having multiple occurrences of letters are identified and the initial alphabets of those words are used to generate watermark patterns. These patterns are concatenated to form a watermark. This process is illustrated in fig.4, where a watermark is generated based on text contents.



Sentences	Pattern
Many *resources* are *available* to help you use your *device*	RAD
You can *look* for *answers* in help *application*	LAA
Features such as an *internal* GPS *receiver*	FIR

Watermark: RAD.LAA.FIR

Figure 4. Watermark Generation

It is called zero-watermarking algorithm because watermark is not actually embedded in the text document itself rather than that contents of text are used to generate it. Watermarking process involves two stages:

- Embedding algorithm
- Extraction algorithm

There is a Certifying Authority (CA) that performs watermarking embedding and extraction for detecting tampering and to prove ownership. This authority registers the owner's watermark and uses it to prove ownership whenever the situation demands.

A. Embedding Algorithm

The algorithm which embeds the watermark in the text is called embedding algorithm. The input to this algorithm is the original text document and a watermark is generated as output by this algorithm. The certifying authority registers that watermark along with the original document, author name, date and time. T1 is the original text document that is taken from owner. In that document, we will take some sentences and in each sentence the length of each word is analyzed. After that every single letter is compared and words with multiple occurrences of letters are analyzed and initial letter of words are combined to generate watermark patterns. All combined patterns are concatenated to generate the watermark. This watermark is then registered to the authority. The algorithm is given following:

```
1)  Read text file T1
2)  NOS = Total number of sentences in T1
3)  for i=1 to NOS, repeat step 4 to 15
4)  NOW=Number of words in ith sentence
5)  for j=1 to NOW, repeat steps 6 to 15
6)  LOW= Length of jth word
7)  For k=1 to LOW repeat steps 8 to 15
8)  SA= letter for comparison/search (kth letter)
9)  Repeat-Count=0;
10) for m= 1 to word-length, repeat steps 11 to 13
11) current-letter= mth letter of word
12) if (SA= current-letter)
    repeat-count= repeat-count+1;
13) m=m+1
14) if (repeat-count>1)
    word(k)= initial letter of kth word
    break internal for;
15) k=k+1
16) j=j+1
17) i=i+1
18) Output W (watermark)
```

B. Extraction Algorithm

The algorithm, which extracts the watermark from the text, is called the extraction algorithm. Text document is taken as input in the extraction algorithm and extracted watermark will be the output. This text document can be the attacked on or not. This text document is used to generate watermark pattern. This watermark pattern is compared with the patterns of original watermark.

Original watermark pattern	Extracted watermark pattern	Pattern matching
RAD	RAD	YES
LAA	ALE	NO
FIR	FIR	YES

Figure 5. Watermark extraction process

If the matching is successful the document is said to be tampered document. The process is shown is fig.5.The extraction algorithm is given following:

```
1)  Read text file T(A) and OW
```

```
2)  NOS = Total number of sentences in T(A)
3)  for i=1 to NOS, repeat step 4 to 15.
4)  NW=Number of words in ith sentence
5)  for j=1 to NW, repeat step 6 to 15
6)  LOW= Length of jth word
7)  For k=1 to LOW repeat steps 8 to 15
8)  SA= letter for comparison/search (kth letter)
9)  Repeat-Count=0;
10) for m= 1 to word-length, repeat steps 11 to 13
11) current-letter= mth letter of word
12) if (SA= current-letter)
    repeat-count= repeat-count+1;
13) m=m+1
14) if (repeat-count>1)
    word(k)= initial letter of kth word
15) k=k+1
16) j=j+1
17) i=i+1
18) if EW = OW (primary match)
      PM(p) = 1
    else
        if EW = OW (secondary match)
          PM(s)= No. of matched secondary patterns/TP
        else
          PR= (NM(p)+NM(s))/TP
```

T(A)=Attacked text file; PM= Pattern matching rate; TP = Total patterns; OW = Original watermark; EW = Extracted watermark; NM = Number of matched patterns

The above algorithm will detect the authentication of text document accurately. This scheme will resist common sentence re-writing and re-ordering attacks. However, the watermark will get destroyed with excess tampering attacks.

V. RESULTS

We use different samples of variable sized text data. These samples are collected from the Internet in the form of eBooks and web pages. We tampered the document by inserting and deleting words and sentences at multiple places in the text. Table I show the sample number, total number of words and total number of patterns in original text and attacked text.

TABLE I. TEXT SAMPLES WITH NUMBER OF PATTERNS

Sample no.	Total number of words	Total number of patterns
1	240	15
2	364	13
3	450	23
4	462	21

Pattern Matching Percentage (PMP) indicates the matching percentage of total number of patterns in original watermark patterns and extracted watermark patterns. Higher the value of PMP, chances of ownership of document increases and tampering is detected in the document. Watermark Distortion Percentage (WDP) is the distortion percentage in the original watermark. WDP indicates that the watermark is being distorted because of the tampering attacks. Text is sensitive to meaning preserving modifications made by the attacker to make it look different or to destroy the writing style of original author. The values of PMP and WDP are shown in table II.

TABLE II. VALUES HAVE PMP AND WDP IN %

Sample no.	Matched patterns	PMP (In %)	WDP (In %)	Tamper detection
1	8	53.3	46.6	Yes
2	6	46.15	53.85	Yes
3	20	86.95	13.04	Yes
4	15	71.42	28.58	Yes

It can be observed in table II that tampering is always detected in every case. This proves that the accuracy of watermark gets affected even with minor tampering and the evident watermark fragility proves that text has been attacked. Fig.6 and Fig.7 show the values of PMP and WDP graphically.

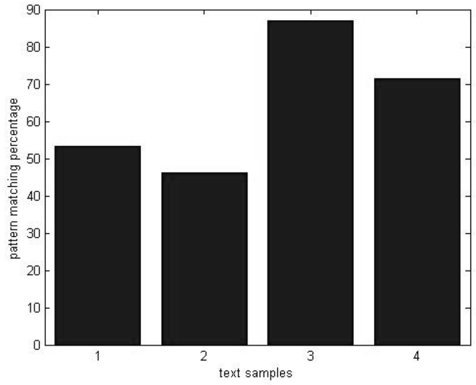


Figure 6. Pattern matching percentage

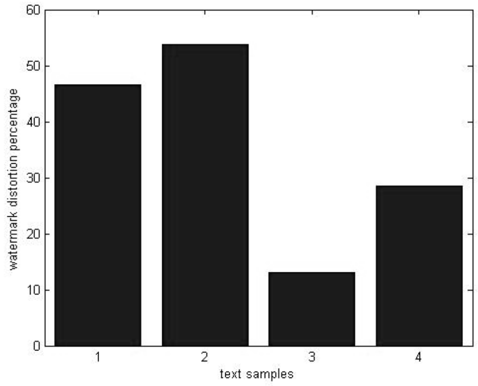


Figure 7. Watermark distortion percentage

VI. CONCLUSION

Text watermarking approaches for tamper detection are less. It is difficult to prove ownership of the tampering text documents. This paper proposes a technique that uses multiple occurrences of letters in a word to generate a watermark and later compare it with the extracted watermark to detect whether the text document is attacked or not. Using double letter words in sentences to generate watermark can extend this work in near future.

ACKNOWLEDGMENT

I would like to thank god for giving me strength, my brother Harpreet Singh for helping me in study and my mother for supporting me mentally. I am also grateful to my supervisor Mrs. Geetanjali babbar for her guidance to complete this work.

REFERENCES

[1] M. Chandra, S. Pandey, R. Chaudhary, **“**Digital Watermarking techniques for protecting digital images”, IEEE, 2010.

[2] Rajvant kaur, “Developing a benchmark model for image digital watermarking”, International Journal of Applied Information Systems (IJAIS) – ISSN: 2249-0868 Foundation of Computer Science FCS, New York, USA Volume 3– No.5, July 2012

[3] “Chapter 2 image watermarking literature survey” [online], http://shodhganga.inflibnet.ac.in/bitstream/10603/2413/10/12chapter2.pdf.

[4] Hussain Nyeem, Wageeh Boles, Colin Boyd, “On the robustness and security of digital image watermarking”, International conference on informatics, Electronics and vision, 2012.

[5] Zunera Jalil, “Copyright protection of plain text using digital watermarking”, FAST National University of Computer and Emerging Sciences, September, 2010.

[6] Huijuan Yang, Alex, and C.Kot, "Text document authentication by integrating inter character and word spaces watermarking", IEEE Inter-national Conference on Multimedia and Expo., Vol. 2, pp. 955 – 958, June 26-30, 2004.

[7] Zunera Jalil and Anwar M.Mirza, “A review of digital watermarking techniques for text documents”, IEEE International Conference on Information and Multimedia Technology, pp. 230-234, 2009.

[8] Nighat Mir and Sayed Afaq Hussain, “Web page watermarking: XML files using synonyms and acronyms”, World Academy of Science, Engineering and Technology, Issue 49, Jan 2011.

[9] P. Lu, et al., “An optimized natural language watermarking algorithm based on TMR”, Proc. of the 9th International Conference for Young Computer Scientists, 2009.

[10] Zhichao Yu and Xiaojun liu, “A new digital watermarking scheme based on text”, IEEE Inter-national Conference on Multimedia Information Networking and Security, Vol. 2, pp. 138-140, 2004.

[11] He Lu, Fang Ding Yi, Gui Xiao Lin, Chen Xiao Jiang, XuXinBai, and Liu Jin “A New Chinese Text Digital Watermarking for Copyright Protecting Word Document”, Vol. 3, pp. 435-439, 2009.

[12] Mussarat Abdullah, Quaid Avenue and Fazal Wahab, “Key based text watermarking of E-text documents in an object based environment using Z-Axis for watermark embedding”, World Academy of Science, Engineering and Technology, 2008.

[13] Zhang, “DWTC: A dual watermarking scheme based on threshold cryptography for web document”, International Conference on Computer Application and System Modeling (ICCASM), Vol. 8, pp. v8510 – v8 514, 2010.

[14] Zunera Jalil, Anwar M. Mirza, and Hajira Jabeen, “Word length based zero-watermarking algorithm for tamper detection in text documents”, 2nd International Conference on Computer Engineering and Technology, vol. 6, v6-378 – v6-382, 2010.

AUTHOR’S PROFILE

Sukhpreet Kaur is currently pursuing her Masters of Technology from Chandigarh Engineering College, Landran under Punjab Technical University. She is the student in computer science department since 2011. Her research area is text watermarking.

Geetanjali Babbar received her Masters of Technology degree in computer science from Punjab technical University. She is an Associate Professor in the faculty of Masters of Technology in computer science branch at Chandigarh Engineering College, Landran.