Zero-Text Watermarking Method for Embedded of Watermark Originality
Fahad Sabah\textsuperscript{1,*} and Saleem Butt\textsuperscript{2}

Received: 03 March 2020; Accepted: 11 June 2020; Published: 21 Sep 2020

Abstract: In this era of technology, the ways to share information among people are completely changed. Technology made it fast to connect with people and share their views within second by using different social sites. The need for hours is how to secure data in a more precise form that can survive by any unauthorized users' raids such as copy, changing, insertion, and deletion of data. These types of attacks destroyed the originality of data. Data may be in any contents shape audio, video, and text but text contents are most difficult to survive from unauthorized access and use. As the content of the text is sharing in soft form over different social sites so the chances of attacks are increasing and the value of the text is difficult to maintain. The purposed solution of securing information or text from unauthorized attacks is text watermarking. Watermarking is the most host topic due to increasing attacks and as the technology is growing. To secure confidential information is one of the necessities of this era for preserving the originality and authentication of contents. In recent years different techniques of text watermarking are using for the security purposes of text. Different techniques and algorithms are used but the main requirements of text watermarking are not successfully achieved. These techniques may not give full access to attackers but the value of the text is degraded. This thesis presents a more enhanced technique to maintain the originality of the text.

Keywords: Information protection, information security, text watermarking, watermark.

1 Introduction

Nowadays, most of the users have free access to make use of text contents such as research papers, journals, and books, confidential documents which should be secure and online reports. Due to open and free access to text illegal attacks like duplication, deletion, insertion, and restructure are at the same time increasing. Text may be confidential like your password, documents of any organization and research papers, books, and news that should be secure. Therefore integrity, originality, and the accuracy of text documents is the basic need of everyone. [1][2]

Watermarking is a way of hiding and securing information. The basic procedure of watermarking is to embed a watermark with simple text on the sender side by generating a keyword and extract this watermark on the receiver side by using this secret keyword. The watermarking technique preserves text integrity, text originality, the accuracy of the text, and makes it possible to share text easily and within seconds Audio, video, software, and confidential documents have become a serious issue due to malicious attacks that

\textsuperscript{1}Beijing University of Technology, Beijing, 101300, China
\textsuperscript{2}Bedfordshire University, Bedfordshire, MK45, England
\textsuperscript{*}Corresponding Author: Fahad Sabah. Email: fahad.sabah@hotmail.com

This work is licensed under a Creative Commons Attribution 4.0 International License, which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.
destroy the originality and value of the text. Watermark insertion into these digital contents is one of the most important ways for securing these types of contents, for copyright protection and proof authenticity. The majority of watermarking methods insert small numbers of bits into the content being watermarked. This Chapter presents the basic requirements of the watermarking, basic architecture of text watermarking, problem statement, aim, scopes and significant, different kinds of attacks, applications of text watermarking, aims, and objectives of this research.

1.1 Main Requirements of Watermarking

The basic requirements of watermarking are imperceptibility, robustness, capacity and security which makes this method successful.

Imperceptibility: The ability of a watermark which shows no difference in original text and watermark text easily. It is achieved when the generated watermark looks like the original text. No one can differentiate between original text and watermark.

Robustness: A watermark should be strong enough that it can survive any unauthorized attacks. Due to effortless access to text malicious attacks can easily destroy the value and meaning of the text. Attackers can use documents for illegal purposes [3].

Capacity: Capacity is the highest amount of watermark which is used to hide information in a watermarked document over a definite period. Capacity should not be too much and too low because high capacity increases the visibility of the watermark key and too low may cause to break the watermark. [4]

Security: Security is the potential in the watermarking to resist any illegal changes in the watermarked document. Security makes it, Tamper Proofing, Text Content Authentication, and Forgery Detection [5].

1.2 Basic Architecture of Text Watermarking

Watermarking is a technique used to preserve the secret message behind a cover medium in such a means that a common man can’t imagine the message with a bare eye and understand it just like a common cover medium. By keeping this purpose in mind these steps are used in any text watermarking architecture:

1. Implement the different text watermarking techniques on the original text (Embedding Watermark).
2. It should be survivable when a watermarked document shares on the communication channel.
3. Extract the watermark on the receiver side only if the watermark key is available then the receiver can use the document otherwise receiver is not allowed to change text or use text.[6]

Three main types of text watermarking are Blind, Semi Blind, and Non-blind which are based on the information required to detect the embedded data.
Problem Statement

With the massive use of the internet to maintain the integrity and originality of text is the most difficult task. Everyone has internet access so the protection of text from unauthorized users which can misuse the information. It is not an easy task because it requires coding knowledge and most important such techniques which will help out to achieve maximum requirements of text watermarking like imperceptibility (not visible), security, robustness, and capacity.

This system can prove fruitful for different text security purposes like text integrity, confidentiality, preserving, and originality of text more effectively without the interference of unauthorized attacks. This will help in making our text more secure.

Application Domain:

These are major fields in which text watermarking techniques are using:

- Digital Copyright Protection (Proof of Ownership): To preserve the document [8]
- Access Control (Copy Control)
- Tamper Proofing:
- Text Content Authentication:
- Forgery Detection (Prevention: To detect the changes which destroy the originality of the text. This research aims to study the existing methods of text watermarking and design an effective text securing system that is no longer allowed to use the text by unauthorized users. On social network platforms, the owners will only the persons who can use, share, or manipulate text, and through this security of text becomes possible. Implement the different text watermarking techniques by studying and enhancing the previous experiences of text watermarking.
- Study and analysis of text watermarking.
- Selection of text watermarking technique
- Study and Analysis of text watermarking process.
- Selection of the best classifier for enhancing text watermarking.

The main significance of this research is to achieve imperceptibility and robustness of the text watermarking process by using the genetics Algorithm which is most rarely used than other techniques. The most important part of this study is that it prevents illegal changes and circulation of the text. Although there are various ways to the text authentication and preserve the originality, the used method in thesis presents an enhanced technique to protect the text for originality and authorization of the document.
3 Background and Literature Review

3.1 Types of Attacks

Watermarking faces severe types of attacks which may result in the modification, duplication, and fake insertion of text. The types of attacks for text are described below:

3.1.1 Formatting-Based Attacks

Variation and modification in
- Font color
- Copying and pasting
- Printing
- Spaces between words

3.1.2 Content-Based Attacks

- Insertion attack by inserting several fake words in the watermarked document caused to destroy the originality watermarked the document
- Local addition attack: Only one word or sentence is inserted randomly in the text content.
- Dispersed addition attack: When several words and sentences are inserted randomly in the text content.

3.1.3 Deletion attack

Deleting the original content of the document is included in deletion attacks. These attacks may cause of destroying the value of the text.

3.1.4 Reordering attack:

The arrangement of words is changed without destroying the meaning of the text. The text is changed by shifting the words, paragraph, and sentence without shifting their meaning, for example by altering the prepositions, the tenses, active in passive, and passive inactive, and other syntax fundamentals. [9]

3.1.5 Synonym replacement attack:

Certain word is replaced by the same word that has the same meaning; in that way, it does not modify the meaning and originality of the text.

3.2 LITERATURE REVIEW

Work on text watermarking began in 1997 where lots of text watermarking technique was proposed for authorization and copyright protection. After that researchers gain interest in text watermark approaches like structural based watermarking, linguistic-based watermarking, analyzed since then lots of other modern methods have been proposed [1].

The structural-based approach changes the structure of the text to embed the watermark. This technique makes use of some layout features (e.g., spaces in between words and spaces in between lines), and format (e.g., color, font, and height of text) for generating watermark [10]. The method changes the position of words and sentences upwards direction from its original place or downwards direction from its original place to embed watermark was first presented by Brassil [11], [12]. It may consist of a line shift algorithm in which changes the complete text line position upward direction or downward direction, a word shift algorithm that changes the position of letters [12][13]

Linguistic based watermarking a natural language-based method, used language syntax or grammar, like changes of verbs, nouns, prepositions of sentences, spellings of a word, the structure of sentences, rules of grammar, etc. to insert watermark in the text. This technique is used related to words or sentence structure.
so; it means this technique is language-dependent. Therefore on the text like poetry, it can’t apply. Due to language dependency, it has limited applicability and destroys the value and meaning of the text.

Jalil et al. 2010 [2, 10, 26] proposed a zero text watermarking technique that is also used to resolve the issues of both linguistic and structural techniques. The key point of using this technique is it does not change the originality and meaning of the text. Zero text watermarking now using in different modern text watermarking techniques. This technique chooses a word as the key point then generates a watermark by using the back and next word length of the selected word (key point).

\[
\text{Keyword} = \text{“is”}
\]

![Figure 3: Zero Text Watermarking Technique [10]](image)

Another proposed embedding method uses the frequency of occurrence of preposition and double letters in the text document to generate a watermark based on the frequency of words in the English language. It offers robust copyright protection of documents and secures its against addition, deletion, and rearranging attacks. [14][25]

In 2019 they proposed a novel text watermarking method by using an image as a watermark. This method converts watermark into the text to generate a watermark key and the most frequent occurrence of double letters in the text is also used to make a robust watermark. This proposed approach was successful to preserve the integrity and value of the text. [16]

R. A. Alotaibi et al. (2017) presented two methods that were high imperceptible, have good capacity, and high robustness. These methods used spaces between words and at the end of lines and between sentences can’t be noticed by a reader easily. No doubt these methods are imperceptible, robust again copy and pasting attacks, and have good capacity ratio but vulnerable to retyping attacks. [17]

Stefano Giovanni Rizzo et al. 2017 [18] presented a method that used watermarking for most sharable content on social media which is such a small text like Facebook messages. This research paper clearly defines that text watermarking which is not suitable for social media text securing and hiding information for a small piece of text like image watermarking, syntactic/semantic watermarking, and zero watermarking. This research purposed some other techniques in place of watermarking such as Whitesteg and Unispach to hide information on social media for small text.

Tayan et al. (2017) presented a summary that shows the results of work which is done to preserve the integrity, originality, and authenticity of online Arabic language contents. Limitations and drawbacks are also discussed which will help out to researchers for presenting a better approach to preserve the integrity and originality of Arabic text. [25]

Nurul Shamimi Kamaruddin et al. 2018 [19] have discussed the issues and challenges like copyright protection (proof of ownership), access control (copy control), tamper-proofing text content authentication, forgery detection, and preserving the integrity of the text. This paper also discussed the watermarking
structure, proposed techniques, approaches, and languages which are helpful to achieve the main requirements of watermarking and used methods in detail.

Ali A. Alwanet al. 2018 [5] presented an in-depth overview of different challenges, issues, and different proposed methods that are published from 2013 to 2018. This paper shows that a few of these methods' main concern is text quality, while others are dealing with the main requirements of text watermarking like imperceptibility, authenticity, and security.

Alotaibi et al. 2018 [6, 13, 14, 23] used an enhanced method of watermarking based on open word space for securing Arabic text. This method used to different techniques like spaces between words is used to generate watermark and to achieve maximum imperceptibility and robustness. The study shows that the proposed methods have the highest capacity to achieve the main requirements of watermarking such as robustness and imperceptibility.

Umair Khadam et al. 2019 presented a digital watermarking technique for text document protection using data mining analysis. This proposed technique provides copyright protection to text documents on local and cloud computing environments. Several models have been proposed for text watermarking, but still need such models that are applicable for the cloud, IoT devices, and smart cities. [7]

4 Proposed Work

The previous algorithms or methods such as semantic syntactic watermarking algorithms which used in past for simple text mostly embed a watermark in the original text file itself which causes to change text quality, sense of sentence and significance degradation. We purpose a zero-text watermarking method in which robustness of a document is specially kept in mind. For this purpose, this method mainly focused that due to embedding of watermark originality of host document is not altered. So, for this purpose the characteristics of text are used to make a watermark.

A. Embedding Algorithm

Embedding algorithm embeds the watermark in the original text for securing information from unauthorized attacks. For embedding watermark main requirement of embedding algorithm original text file as input and for generating watermark keyword is selected that totally depends on the choice of the original author/copyright owner. Keyword that author chooses must have high frequency of occurrence in the original text. The algorithm follows these steps in sequence as follows:

The original text contents (Tc) first of all gain from the author and occurrence frequency of each word in text is analyzed. Selection of Keywords is totally based on author’s choice typical words having high occurrence count in text. The proceeding and next word length for all occurrences of keyword in text is analyzed and a numeric watermark is generated. The generated watermark is afterward registered with the certifying authority by using current date and time.

B. Extraction Algorithm

Extraction algorithm is used for the extraction of the watermark. The proposed extraction algorithm used the received text and keyword as input. The text’s content may be affected by attacker or not. The watermark is generated from this received text by using the extraction algorithm and afterward, it is matched with the original watermark registered with the Certifying Authority. Author name, current date and time is also recorded with the Certifying Authority. Registration of multiple watermark may cause conflicts, Certifying Authority can be resolved this issue by keeping record of time and date. The author having former registration entry will be regarded as the original author.

The extraction algorithm is as follows:

1. Read Tc or Ta, W-M and K-W.
2. Count frequency of K-W in given text.
3. K-WCount= Total occurrence count of K-W in text
4. for K=1 to K-WCount, repeat step 5 to 7.
5. EW-M [L] = length (P_k)
6. EW-M [L+1] = length (N_k)
7. k=k+1 and l=l+1
8. if (EW-M not equals W-M) 
   Tamper = YES
9. Output EW-M.

Tc= Original text content; Ta= Attacked text; K-W=keyword; K-WCount= keyword count ; EW-M= Extracted Watermark; P_k= ‘Proceeding word’ of the kth occurrence of keyword (K-W); N_k= ‘Next word’ of the kth occurrence of keyword (K-W)

Figure 4: Block diagram of proposed methodology
IMPLEMENTATION

We used 10 samples of variable size text document as an input from the data set which is used for results. These text which is used as input collected from different web pages-books, and newspapers etc. Tampering like adding/insertion and removing/deletion of words and complete sentences was done by many times different and randomly choose places in input text.

Table 1: Original and Attacked Text Samples with Insertion and Deletion Ratios

<table>
<thead>
<tr>
<th>Sample No.</th>
<th>'and' WC&lt;sub&gt;O&lt;/sub&gt;</th>
<th>'and' WC&lt;sub&gt;A&lt;/sub&gt;</th>
<th>Tamper Detection</th>
<th>WAR</th>
</tr>
</thead>
<tbody>
<tr>
<td>1: [SST2]</td>
<td>12</td>
<td>10</td>
<td>Yes</td>
<td>0.1538</td>
</tr>
<tr>
<td>2: [SST4]</td>
<td>8</td>
<td>6</td>
<td>Yes</td>
<td>0.4736</td>
</tr>
<tr>
<td>3: [MST2]</td>
<td>8</td>
<td>7</td>
<td>Yes</td>
<td>0.2941</td>
</tr>
<tr>
<td>4: [MST4]</td>
<td>59</td>
<td>55</td>
<td>Yes</td>
<td>0.1935</td>
</tr>
<tr>
<td>5: [MST5]</td>
<td>19</td>
<td>13</td>
<td>Yes</td>
<td>0.3333</td>
</tr>
<tr>
<td>6: [LST1]</td>
<td>257</td>
<td>264</td>
<td>Yes</td>
<td>0.1248</td>
</tr>
<tr>
<td>7: [LST3]</td>
<td>45</td>
<td>51</td>
<td>Yes</td>
<td>0.4190</td>
</tr>
<tr>
<td>8: [LST5]</td>
<td>286</td>
<td>299</td>
<td>Yes</td>
<td>0.1868</td>
</tr>
<tr>
<td>9: [VLST3]</td>
<td>858</td>
<td>915</td>
<td>Yes</td>
<td>0.1717</td>
</tr>
<tr>
<td>10: [VLST5]</td>
<td>1031</td>
<td>1053</td>
<td>Yes</td>
<td>0.1326</td>
</tr>
</tbody>
</table>

The number of occurrences of words having same keyword “and”, “of”, and “in” was examined in the original and attacked text selected text. These keywords were selected because of frequent occurrences of word length in all text taken as input. Watermark Accuracy Rate (WAR) and Watermark Distortion Rate (WDR) are calculated by using the following formulas:

WAR = Number of characters correctly detected / Number of watermark characters

WDR = 1 – WAR
Table 2: Accuracy of Extracted Watermark with Keyword "and"

<table>
<thead>
<tr>
<th>Sample No.</th>
<th>Original Text</th>
<th>Attack</th>
<th>Attack Text</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>WC</td>
<td>Insertion</td>
<td>Deletion</td>
</tr>
<tr>
<td>1: [SST2]</td>
<td>421</td>
<td>26%</td>
<td>25%</td>
</tr>
<tr>
<td>2: [SST4]</td>
<td>179</td>
<td>44%</td>
<td>54%</td>
</tr>
<tr>
<td>3: [MST2]</td>
<td>559</td>
<td>49%</td>
<td>25%</td>
</tr>
<tr>
<td>4: [MST4]</td>
<td>2018</td>
<td>14%</td>
<td>12%</td>
</tr>
<tr>
<td>5: [MST5]</td>
<td>469</td>
<td>57%</td>
<td>53%</td>
</tr>
<tr>
<td>6: [LST1]</td>
<td>7993</td>
<td>9%</td>
<td>6%</td>
</tr>
<tr>
<td>7: [LST3]</td>
<td>1824</td>
<td>26%</td>
<td>16%</td>
</tr>
<tr>
<td>8: [LST5]</td>
<td>16076</td>
<td>9%</td>
<td>5%</td>
</tr>
<tr>
<td>9: [VLST3]</td>
<td>51800</td>
<td>11%</td>
<td>7%</td>
</tr>
<tr>
<td>10: [VLST5]</td>
<td>67214</td>
<td>7%</td>
<td>5%</td>
</tr>
</tbody>
</table>

Results show that our algorithm always detects altering, misusing, and updating of text even when the altering, misusing, and updating volume is low. Firstly, the best ability of the proposed watermark is no one can easily detect a difference in original text and watermark text. By using this algorithm-generated watermark look like the original text. No one can differentiate between original text and watermark. This algorithm maintains the integrity and does not change or degrade text and destroy the value and meaning of the text. Attackers can use documents for illegal purposes. Robustness is the second important key ability of our generated watermark respectively. WC0 and WCA show the keyword count in original and attacked text respectively.

Figure 4: Simulation results
CONCLUSION

Results show that our algorithm always detects altering, misusing, and updating of text even when the altering, misusing, and updating volume is low. Firstly, the best ability of the proposed watermark is no one can easily detect a difference in original text and watermark text. By using this algorithm-generated watermark look like the original text. No one can differentiate between original text and watermark. This algorithm maintains the integrity and does not change or degrade text and destroy the value and meaning of the text. Attackers can use documents for illegal purposes. Robustness is the second important key ability of our generated watermark.

References


