Computer Systems Science & Engineering
DOI:10.32604/csse.2021.015915
Article

Tech Science Press

A Reliable NLP Scheme for English Text Watermarking Based on Contents Interrelationship

Fahd N. Al-Wesabi[1,2,*], Saleh Alzahrani[3], Fuad Alyarimi[3], Mohammed Abdul[3], Nadhem Nemri[3] and Mohammed M. Almazah[4]

[1]Department of Computer Science, King Khalid University, Muhayel Aseer, Kingdom of Saudi Arabia
[2]Faculty of Computer and IT, Sana'a University, Sana'a, Yemen
[3]Department of Information Systems, King Khalid University, Muhayel Aseer, Kingdom of Saudi Arabia
[4]Department of Mathematics and computer in Ibb University, Yemen and Department of Mathematics, King Khalid University, Muhayel Aseer, Kingdom of Saudi Arabia
[*]Corresponding Author: Fahd N. Al-Wesabi. Email: falwesabi@kku.edu.sa
Received: 01 December 2020; Accepted: 06 January 2021

Abstract: In this paper, a combined approach CAZWNLP (a combined approach of zero-watermarking and natural language processing) has been developed for the tampering detection of English text exchanged through the Internet. The third gram of alphanumeric of the Markov model has been used with text-watermarking technologies to improve the performance and accuracy of tampering detection issues which are limited by the existing works reviewed in the literature of this study. The third-grade level of the Markov model has been used in this method as natural language processing technology to analyze an English text and extract the textual characteristics of the given contexts. Moreover, the extracted features have been utilized as watermark information and then validated with the attacked English text to detect any suspected tampering occurred on it. The embedding mechanism of CAZWNLP method will be achieved logically without effects or modifying the original text document to embed a watermark key. CAZWNLP has been implemented using VS code IDE with PHP. The experimental and simulation results using standard datasets of varying lengths show that the proposed approach can obtain high robustness and better detection accuracy of tampering common random insertion, reorder, and deletion attacks, e.g., Comparison results with baseline approaches also show the advantages of the proposed approach.

Keywords: NLP; text analysis; English text watermarking; robustness; tampering detection

1 Introduction

The reliability and security of text information shared over the Internet is the most exciting and demanding area for the scientific community. In communication technologies, authentication of content, and honesty of automated text verification with different language formats are of great significance. Numerous applications such as electronic banking, electronic commerce, etc. impose most challenges during contents transfer via the internet. In terms of content, structure, grammar, and semantics, much of the multimedia exchanged via the Internet is in form of textual which is very susceptible to online transmission. During the transfer process, malicious attackers can temper such digital content and thus the changed count [1].

For information security, many algorithms and techniques are available, such as content authentication, verification of integrity, detection of tampering, identification of owners, access control, and copyright protection.

To overcome these issues, digital watermarking (DWM) is a technique that can be used to hide the various data, for example; binary images, text, audio, and video with embedding them in digital content as watermark information [2,3].

A fine-grain process for document watermarking is suggested based on the substitution of homoglyph characters of white spaces and Latin symbols [4].

Several conventional methods and solutions for text watermarking were proposed [5] and categorized into different classes, such as linguistic, structure, zero watermarks, and format-based methods [6]. To insert the watermark information into the document, most of these methods need improvement to plain text material. Zero-watermarking without any alteration to the original digital material to embed the watermark information is a recent technology used with intelligent methods and algorithms. In addition, the contents of a given digital background can be used in this process to produce the watermark key [1,6–8].

Restricted research has centered on the appropriate solutions to verify the credibility of critical digital media online [9–11]. In the research community, digital text tampering detection and authentication have received great attention. Also, research in the field of text watermarking has concentrated on copyright protection in the last decade, but less interest and attention has been paid to integrity verification, identification of tampering, and authentication of content due to the existence of text content based on the natural language [12].

Proposing the most appropriate approaches for various formats and content, especially in English and Arabic languages, is the most common challenge in this area [13,14]. Therefore, authentication of content, verification of honesty, and detection of tampering of sensitive text is a major problem in different applications and needs the required solutions.

Some instances of such sensitive digital text content are Arabic Holy-Qur'an, eChecks, and online marking of exams. Different Arabic alphabet characteristics such as diacritics, letter extraction, and symbols of Arabic supplementary that make it easy to alter the key text material meaning by creating basic changes such as modifying diacritic arrangements [11,15]. The most popular soft computing and Natural-Language Processing (NLP) technique is involved for HMM text analysis.

In this paper, the authors present a reliable approach known as CAZWNLP for tampering detection of English text transmitted via the internet. The proposed approach is based on the third grade of alphanumeric mechanism based on the Markov model. In CAZWNLP, a combined model of NLP and English text watermarking technologies. In this approach, NLP used for text analysis to obtain the textual characteristics of the given English contents and generate watermark data. The plain English text will not be affected by the embedding process of the generated watermark key because the embedding will be logically without changes or modifications of the original text. The embedded watermark key will be used later to check the status of the received English text and to determine if it is authentic or not.

The major objective of CAZWNLP approach is to achieve high accuracy of tampering detection that occurred in English text during transmission via Internet, which has gained great importance and needs more security and protection via the Internet.

The rest of the paper has five more sections. Section 2 provides a related work. Section 3 presents CAZWNLP. Section 4 describes the implementation, simulation, and experimental. Section 5 describes the comparison and result discussion, and Section 6 has the conclusion of the article.

2 Related Work

Natural language is the foundation of approaches to linguistic text watermarking. The mechanism of those methods embedding the watermark is based on changes applied to the semantic and syntactic essence of plain text [1].

To enhance the capability and imperceptibility of Arabic text, A method of text watermarking is suggested room dependent on the accessible words [16]. In this method, any word-space is used to mask the Boolean bit 0 or 1 that physically modifies the original text. A text steganography technique was proposed to hide information in the Arabic language [17]. The step of this approach considers Harakat's existence in Arabic diacritics such as Kasra, and Damma as well as reverses Fatha to cover the message.

A Kashida-marks invisible method of watermarking [18], based on the features of frequent recurrence of document security and authentication characters, was proposed. The method is based on a predetermined watermark key with a Kashida placed for a bit 1 and a bit omitted. The method of steganography of the text was proposed to use Kashida extensions depend on the characters 'moon' and 'sun' to write digital contents of the Arabic language [19]. Also, the method Kashida characters are seen alongside characters from Arabic to decide which hidden secret bits are kept by specific characters. In this form, four instances are included in the kashida characters: moon characters representing '00'; sun characters representing '01'; sun characters representing '10'; and moon characters representing '11'.

A text steganographic approach [20] based on multilingual Unicode characters has been suggested to cover details in English scripts for the use of the English Unicode alphabet in other languages. Thirteen letters of the English alphabet have been chosen for this approach. It is important to embed dual bits in a timeframe used ASCII code for embedding 00. However, multilingual ones were used by Unicode to embed between 01, and 10, as well as 11. The algorithm of text watermarking is used to secure textual contents from malicious attacks according to Unicode extended characters [21]. The algorithm requires three main steps, the development, incorporation, and extraction of watermarks. The addition of watermarks is focused on the development of predefined coding tables, while scrambling strategies are often used in generation and removal, the watermarking key is safe.

The substitution attack method focused on preserving the position of words in the text document has been proposed [22]. This method depends on manipulating word transitions in the text document. Authentication of Chinese text documents based on the combination of the properties of sentences, text-based watermarking approaches have been suggested [23,24]. The proposed method is presented as follows: firstly, a text of the Chinese language is split into a group of sentences, and for each word, the code of a semantic has been obtained. The distribution of semantic codes influences sentence entropy. The distribution of semantic codes influences sentence entropy.

A zero-watermarking method has been proposed to preserve the privacy of a person who relies on the Hurst exponent and the nullity of the frames [25]. For watermark embedding, the two steps are determined to evaluate the unvoiced frames. The process of the proposed approach bases on integrating an individual's identity without notifying any distortion in the signals of medical expression.

A zero-watermarking method was proposed to resolve the security issues of text-documents of the English language, such as verification of content and copyright protection [26]. A zero-watermarking approach has been suggested based on the authentication Markov-model of the content of English text [27,28]. In this approach, to extract the safe watermark information, the probability characteristics of the text of English are involved and stored to confirm the validity of the attacked text-document. The approach provides security against popular text attacks with a watermark distortion rate if, for all known attacks, it is greater than one. For the defense of English text by copyright, based on the present rate of ASCII non-vowel letters and terms, the conventional watermark approach [29] has been suggested.

3 The Proposed Approach

This paper proposes a model consisted of the combination of NLP and English text watermarking technologies. The method proposed in this paper is called CAZWNLP (a combined approach of zero-watermarking and natural language processing). In CAZWNLP, authors utilize the third grade of alphanumeric of the Markov model as NLP technique to procced text analyze, obtain the textual regentship, and extract the characteristics of the given English text.

The main contributions of our approach, CAZWNLP can be summarized as unlike the existing work in terms of watermark embedding mechanism, external watermark data, limitations on size or nature of the English contents. The CAZWNLP method addressed all of these issues by using integrated techniques which no need to use extra information as a watermark key, no effects or modification needed on the original text, and no limitations on size and nature of the given text, no limitations also in the tampering positions, type or volume of the attack.

The following subsections explain in detail two phases that should perform in CAZWNLP. The first process is called the watermark generation and embedding phase; however, the second phase is watermark extraction and detection.

3.1 Watermark Generation and Embedding Phase

Three steps should be performed in this phase: pre-processing, generating watermark, and embedding watermark as illustrated in Fig. 1.

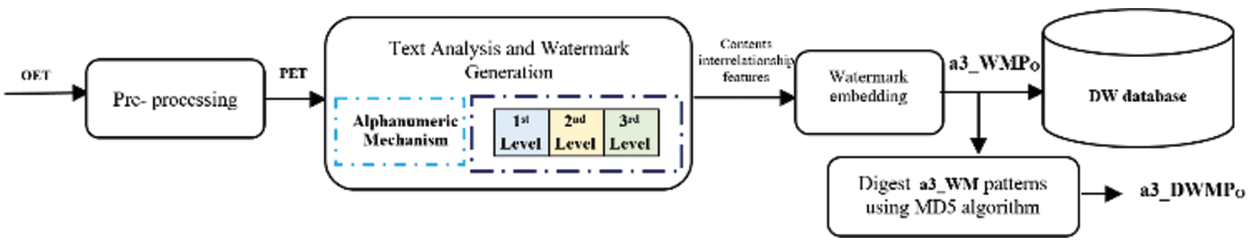

Figure 1: CAZWNLP English text-watermark steps

3.1.1 Pre-Processing Step

The pre-processing of the original English text is one of the key steps in both generating and extracting watermark for many proposes such as the present the given text in a small letter case, remove any extra newlines or spaces. The original English text (OET) is required as input to run this procedure.

3.1.2 Watermark Generation Step

Two procedures should be performed in this step are build the Markov matrix and set up the states and transitions of the given English text, text analyzing, and generating the watermark.

- *Set up the Markov matrix* to represent the initial step to run this procedure of CAZWNLP method. In this procedure every triple of unique alphanumeric should be represented as a unique state, and every unique alphanumeric should be represented as a transition in the Markov matrix.

The procedure of the pre-processing and set up the Markov matrix is represented by the pseudocode as shown in Algorithm 1.

Algorithm 1: The procedure of the pre-processing and set up the Markov matrix using CAZWNLP

```
PROCEDURE Prep_Building_MM (OET)

Input: original English text (OET)
Output: Markov matrix with zeros initial value
BEGIN
// perform pre-processing process
for each alphanumeric in OET
        // remove new lines and spaces letters
        PET ← trim ("space" or "newLine")
        // convert letter case from capital to small letters
          PET ← LowerCharacter(alphanumeric)
// Build list of non values text alphanumerics
a3_mm = { }
for each alphanumeric in PET
      if alphanumeric not in a3_mm
            a3_mm ← a3_mm U {alphanumeric}
      for ps = 1 to a3_mm.length – 3
            for ns = 1 to a3_mm.length
                  a3_mm[ps][ns] = 0
return a3_mm
```

where,

OET: is the original English text, PET: is a pre-processed English text, a3_mm: states and transitions matrix, ps: refers to the current state, ns: refers to next state.

The length of $a3\_\mathrm{mm}[i][j]$ matrix of CAZWNLP is dynamic in which the number of states is equal to the total number of unique triples of alphanumeric in given English text. However, the number of transitions is fixed which is equal to the total number of English characters, integer numbers from 0 to 9, and special symbols.

- *Text analyzing and generating the watermarking procedure:* this procedure is performed to analyzing the given English text and obtain the contents relationships in order to use them to generate the watermark. This process is computed by Eq. (1).

$$a3\_mm[ps][ns] = \sum\nolimits_{i,j=1}^{n-3} \mathrm{transtions}[i][j] \tag{1}$$

where n: is the total number of states.

To demonstrate the working mechanism of the proposed CAZWNLP, the authors use the following sample of English text.

> "The quick brown fox jumps over the brown fox whoo is show jumps over the brown fox who is dead."

When using the third grade of the alphanumeric Markov model, each unique triple sequence of alphanumeric is represented as a state. Text analysis is achieved to find the inter characteristics for both current and next states. Fig. 2 below shows the available transitions and analysis results of the above sample of English text.

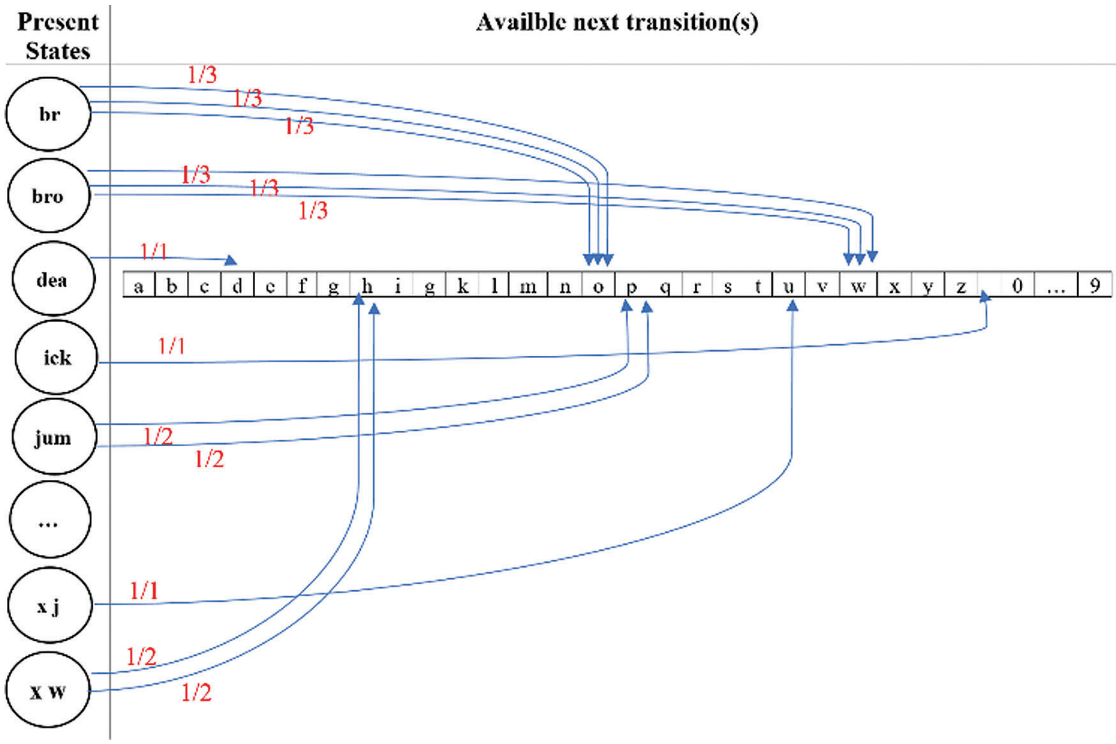

Figure 2: Representing states and their transitions of sample text using CAZWNLP

Authors assume "br" is a present state, and the available next transition(s) are 'o', 'o', and 'o'. I observe that three transitions available in the given English text sample.

The pseudocode of the procedure of the text analyzing and watermark generating based on the third grade of alphanumeric Markov model presented in Algorithm 2 and proceeds as illustrated in Fig. 3.

Algorithm 2: Text analyzing and watermark generating using CAZWNLP

```
PROCEDURE ETA_WM_generation(PAT)

Input: PET, IMM
Output: FM
BEGIN
Prep_Building_MM (PET)
pa = first_trip_alpha(PET)
pd2 = PET – [pa] // begin with 2nd triple of alphanumeric
fm = a3_mm
for each a in pd2
        fm[pa][ca] = fm[pa][a] + 1
        pa = ca
return fm
```

where pa: previous triple of alphanumeric, ca: current triple of alphanumeric.

The extracted characteristics of the given English text of non-zero values will be concatenated in decimal form to generate the original watermark key WMP_O, as provided in Eq. (2) and Fig. 4.

States	Transitions																																																											
	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z	0	1	2	3	4	5	6	7	8	9		'	"	,	;	:	?	!	/	\	@	$	&	%	*	+	-	=	>	<	(	)	[	]	DWM patterns
‘ br’	0	0	0	0	0	0	0	0	0	0	0	0	0	0	3	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	3
‘bro’	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	3	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	3
‘dea’	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1
‘ick’	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1
‘jum’	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	2	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	2
… … …	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	
‘x j’	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1
‘x w’	0	0	0	0	0	0	0	2	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	2

Figure 3: Text analyzing and watermark generating of the given English text using CAZWNLP

3 –3–1–1–2– … –1– 2

Figure 4: The generated watermark key WMP_O using CAZWNLP

$$a3\_WMP_O \;\&= \; a3\_mm[ps]\,[ns] \tag{2}$$

3.1.3 Watermark Embedding Step

In the CAZWNLP technique, the embedding of zero watermarks will be done logically by identifying all non-zero values in the Markov chain matrix without needing to modify the original text. The generated WMP_O is stored in WM database with other related information of the given English text document.

3.2 Watermark Extracting and Detecting Phase

Two core procedures are involved in this phase: extracting the watermark and detecting the watermark. $a3\_EWM_A$ will be obtained from the attacked text (PET_A) and matched with $a3\_WMP_O$ by detection algorithm. The working mechanism of this phase is illustrated in Fig. 5.

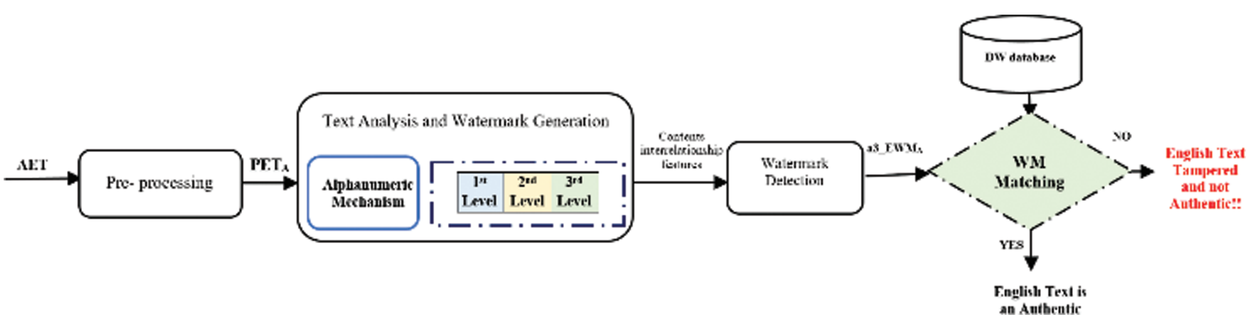

Figure 5: Extracting and detecting watermark phase using CAZWNLP

3.2.1 Procedure of Extracting Watermark

PET_A is the major input for this procedure. However, the output is $a3\_WMP_A$. The technical details of this procedure are formulated in pseudocode as illustrated in Algorithm 3.

Algorithm 3: Extracting the watermarking procedure based CAZWNLP

PROCEDURE WM_extraction(PET_A)

- Input: pre-processed text (PET_A)
- Output: attacked watermark patterns ($a3\_WMP_A$).
- BEGIN
- ETA_WM_generation (PET_A)
- **for** ps = 1 **to** a3_arrList'.Length - 3,
    - **for** ns = 1 **to** a3_arrList'.Length,
    - **if** a3_mm[ps][ns] != 0,
    - $a3\_WMP_A$ &= a3_mm[ps] [ns],
- **return** $a3\_WMP_A$

where, PET_A: pre-processed attacked English text, $a3\_WMP_A$: attacked watermark patterns.

3.2.2 Procedure for Detecting Watermark

$a3\_WMP_A$ and $a3\_WMP_O$ are the core two inputs to run this procedure, while the output is the notification status of English text, which can be authentic or tampered. This procedure is achieved in two sub-steps:

- *Primary detecting* is performed to matching both $a3\_WMP_O$ and $a3\_WMP_A$. If both appear identical, then the status of the transferred English text is authentic. Otherwise, the transferred text has been tampered, and then it continues to the next step.
- *Secondary detecting* is achieved by detecting the authenticity of all transitions of every state of the generated watermark data as given by Eqs. (3 and 4).

$$a3\_PMR_T(i,j) = \left| \frac{a3\_WMP_O[i][j] - \left(a3\_WMP_O[i][j] - a3\_WMP_A[i][j]\right)}{a3\_WMP_O[i][j]} \right|, \quad \textit{for all } i,\ j \textit{ states and transitions} \tag{3}$$

where,

- $a3\_PMR_T$: represents tampering detection accuracy rate value in transition level, ($0 < a3\_PMR_T <= 1$)

$$ea3\_PMR_S(i) = \left| \frac{\sum_{j=1}^{n} (a3\_PMR_T(i,j))}{Total\ StatePatternCount(i)} \right| \textit{for all } i \tag{4}$$

where,

- $a3\_PMR_S$: value of tampering detection accuracy rate in state level, ($0 < a3\_PMR_S <= 100$).

After the tampering detection accuracy value of each state has been obtained; the next step is to produce the values of each stored state in the Markov matrix as shown in Eq. (5).

$$a3\_Sw = \left| \frac{a3\_PMR_S(i) \ * \ \text{Transitions frequency}(i)}{\text{total number of transitions}} \right| \tag{5}$$

Where,

- $a3\_PMR_S$: is the total matching value in the i^{th} state level.

The values if a3_PMR of PET_A and OET_P are obtained by Eq. (6).

$$a3\_PMR = \left| \frac{\sum_{i=1}^{n} a3\_PMRS(i)}{N} \right| \quad (6)$$

The destroyed rate of the watermark refers to the weight of the tampering that occurred on the attacked contents, which is represented by a3_WDR, and obtained by Eq. (7).

$$a3\_WDR = 1 - \ a3\_PMR * 100 \quad (7)$$

The watermark detecting procedure is presented formally using pseudocode as shown in Algorithm 4.

Algorithm 4: Detecting the watermarking procedure based CAZWNLP

PROCEDURE WM_detection (a3_WMP_O, a3_WMP_A)

- Input: pre-processed text (a3_WMP_O, a3_WMP_A)
- Output: a3_PMR, a3_WDR
- BEGIN
- ATA_WM_generation (a3_WMP_O)
- *WM_extraction* (WMP_A)
    - **IF** a3_WMP_A = a3_WMP_O
        - Print "English document is authentic and no tampering occurred"
        - a3_PMR = 100
    - Else
        - Print "English document is not authentic and tampering occurred"
    - **for** i = 1 **to** a3_arrList'.Length - 3,
        - **for** j = 1 **to** a3_arrList'.Length
            - IF a3_WMP_O[i][j] != 0
                - pattern Count +=1
                - $a3\_PMR_T(i,j) = \left|\frac{a3\_WMP_O[i][j] - (a3\_WMP_O[i][j] - a3\_WMP_A[i][j])}{a3\_WMP_O[i][j]}\right|$
                - transPMRTotal += a3_PMR_T
            - Else
                - IF a3_WMP_A[i][j] != 0
                - patternCount += a3_WMP_A[i][j]
    - $a3\_PMR_S(i) = \left|\frac{\sum_{j=1}^{n}(a3\_PMR_T(i,j))}{Total\ StatePatternCount(i)}\right|$
    - $sWeight = \frac{a3\_PMR_S(i) * Transitions\ frequency(i)}{total\ no\ of\ transitions}$
- a3_SW += stateWeight
- $a3\_PMR = \frac{\sum_{i=1}^{n}(a3\_SW) * Total\ number\ of\ transitions}{Total\ number\ of\ transitions} * 100$
- a3_WDR = 1 – a3_PMR * 100

return a3_PMR, a3_WDR

where, a3_SW refers to the weight value of states correctly matched., and a3_WDR refers to the value of watermark distortion rate ($0 < a3\_WDR_S <= 100$).

The results of the watermark extracting and detecting procedures are illustrated in Fig. 6.

States	Original WM patterns	Extracted WM patterns	Destroyed WM patterns	Primary matching rate	Primary matching rate of transition level $PMR_T(i,j)$		Primary matching rate of transition level $PMR_S(i,j)$
					TP1	TP2	
‘ br’	3	2	2	-	0.6667	-	0.6667
‘bro’	3	2	2	-	0.6667	-	0.6667
‘dea’	1	1	1	1	-	-	1
‘ick’	1	1	1	1	-	-	1
‘jum’	2	2	2	1	-	-	1
… … …	… … …	… … …	… … …	… … …	… … …	… … …	… … …
‘x j’	1	1	1	1	-	-	1
‘x w’	2	1	1	-	0.5	-	0.5
Robustness (PMR) =							58.0006 / 72 = 0.8056

Figure 6: Results of watermark extracting and detecting procedures using CAZWNLP

4 Implementation and Simulation

A variety of experiments and simulations are conducted to test the performance of CAZWNLP. This section outlines an implementation environment, and typical scenarios of experimentation, and a discussion of outcomes. A self-developed program has been developed for CAZWNLP technique using PHP VS Code IDE programming environment.

4.1 Experimental and Performance Parameters

A series of experiments and simulation scenarios of CAZWNLP have been performed using various sizes of standard datasets [very small (ESST), small (EMST), medium (EHMST), and large (ELST)]. An experiments and simulation scenarios performed under predefined attacks (insertion, deletion, and reorder) with their volumes (very small (5%), small (10%), mid (20%), and large (50%)] randomly on multiple positions of these datasets. The desired accuracy rate with close to 100%.

4.2 CAZWNLP Simulation and Experiment Findings

To evaluate the accuracy of tampering detection of CAZWNLP, scenarios of many studies are performed as shown in Tab. 1, for all forms of attacks and their volumes.

The results shown in Tab. 2 and Fig. 7 show that little effect is detected with deletion attack in case of the low rate of tampering attack. Though, a high effect has been detected with insertion attack in case of mid-rate of attack. In case of the high rate of attack, a high effect has been detected with insertion and deletion attacks. This means that the CAZWNLP technique provides the best accuracy of tampering detection with both reorder and deletion attacks in all rates of attacks.

Table 1: Assessment detection accuracy of CAZWNLP under all volumes

Attack Volume	Insertion	Deletion	Reorder
5%	94.02	96.41	95.36
10%	88.29	92.49	91.62
20%	80.89	85.86	86.90
s50%	63.54	67.30	80.19

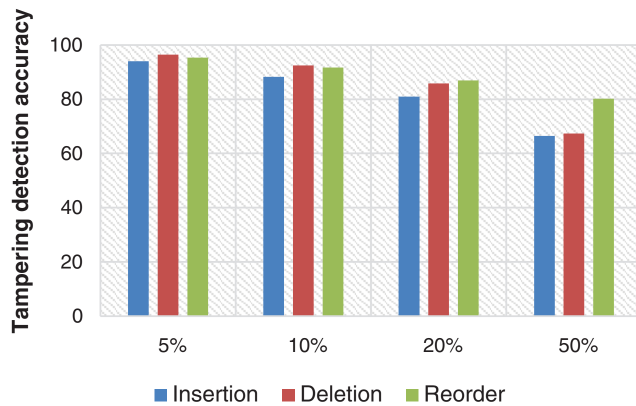

Figure 7: Tampering impact under all attacks of many volumes

5 Comparison and Result Discussion

The accuracy of tampering detection is critically studied, analyzed, and compared between CAZWNLP and baseline methods SAWMWMM presented in [5] and NIATRAATI presented in [30].

5.1 English Text Size-Based Effect Comparison

A comparison of typical sizes of the English datasets in terms of tampering detection accuracy of CAZWNLP with baseline methods SAWMWMM and NIATRAATI have been shown in Tab. 2.

Table 2: Detection accuracy comparison based on English text size

Dataset size	SAWMWMM	NIATRAATI	CAZWNLP
[ESST]	71.33	67.27	84.41
[EMST]	69.93	63.80	84.79
[EHMST]	66.90	59.23	86.55
[ELST]	63.94	54.47	83.76

The results shown in Tab. 2 and Fig. 8 shows how the detection accuracy of CAZWNLP, SAWMWMM and NIATRAATI methods are affected by analyzing the dataset size. In Fig. 8, it can be seen that in all cases of CAZWNLP and baseline SAWMWMM and NIATRAATI methods, the effect of English dataset size in terms of high accuracy are ordered from high to low as ESST, ELST, EMST, and EHMST. This means that the detection accuracy of all methods increased with decreasing size of English text and right reverse.

Generally, the comparative results show that CAZWNLP method outperforms both SAWMWMM and NIATRAATI methods in terms of detection accuracy and general performance with all sizes of English dataset sizes.

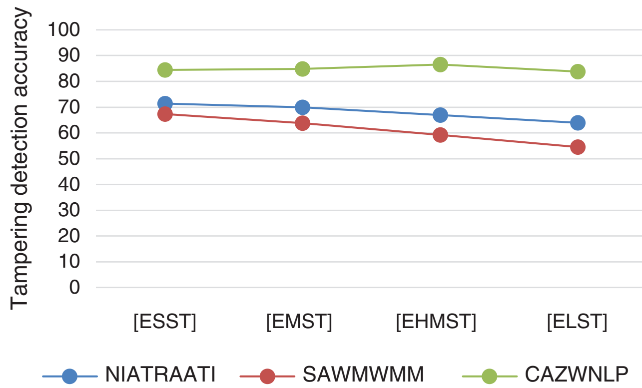

Figure 8: English text size-based comparison of tampering detection accuracy

5.2 Attack Type-Based Effect Comparison

A comparison of typical types of tampering attacks in terms of detection accuracy of CAZWNLP with baseline methods SAWMWMM and NIATRAATI have been shown in Tab. 3.

Table 3: Detection accuracy comparison based on attack type

Method	Insertion	Deletion	Reorder
SAWMWMM	81.00	69.48	56.84
NIATRAATI	80.50	70.45	48.36
CAZWNLP	82.40	85.52	88.52

The results shown in Tab. 3 and Fig. 9 shows that CAZWNLP method outperforms SAWMWMM and NIATRAATI in terms of detection accuracy and general performance in all cases of attacks. This means that CAZWNLP method is suitable and reliable for sensitive tampering detection of all kinds of attacks that can be occurred on English text exchanged through the internet.

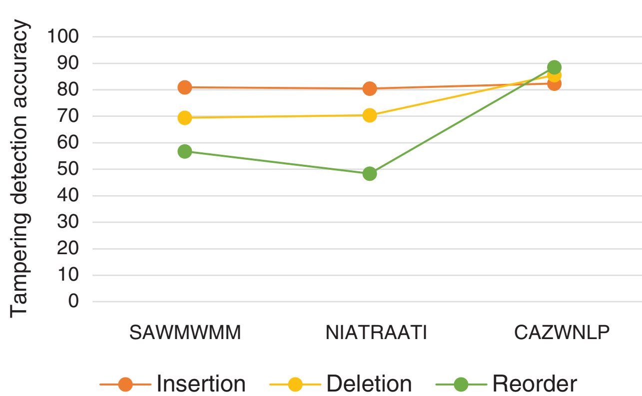

Figure 9: Attack type-based comparison of tampering detection accuracy

5.3 Attack Rate-Based Effect Comparison

A comparison of typical rates of tampering attacks in terms of detection accuracy of CAZWNLP with baseline methods SAWMWMM and NIATRAATI have been shown in Tab. 4.

Table 4: Detection accuracy comparison based on attack rates

Attack volume	SAWMWMM	NIATRAATI	CAZWNLP
5%	82.09	84.98	95.26
10%	72.74	76.21	90.80
20%	57.71	61.46	84.55
50%	13.66	39.57	71.30

The results shown in Tab. 4 and Fig. 10 shows that, if the attack volume increases, the tampering detection accuracy decreases. It seen also, CAZWNLP method outperforms both SAWMWMM and NIATRAATI methods in terms of detection accuracy and general performance in all rates of attacks (low, mid, or high). This means that CAZWNLP method is suitable and reliable for sensitive tampering detection of all volumes of attacks that can be occurred on English text exchanged through the internet.

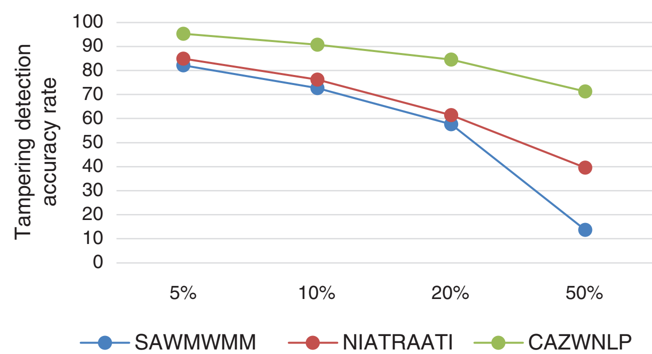

Figure 10: Attack rate-based comparison of tampering detection accuracy

6 Conclusion

CAZWNLP method is proposed in this paper and implemented by the self-developed program in PHP VS code IDE programming environment. Several typical scenarios of experiments and simulations are performed on various typical of English datasets with various rates of tampering attacks. CAZWNLP has been compared with SAWMWMM and NIATRAATI methods. The results of simulation and comparison show that CAZWNLP outperforms SAWMWMM and NIATRAATI methods in terms of detection accuracy and general performance. The results also show that CAZWNLP is suitable and reliable to detect sensitive tampering that can occur on all English contents with real numbers and special characters. For future work, the enhancement of accuracy should be considered for all attack rates and types.

Funding Statement: The authors extend their appreciation to the Deanship of Scientific Research at King Khalid University for funding this work under grant number (R. G. P. 2/55/40 /2019), Received by Fahd N. Al-Wesabi. www.kku.edu.sa

Conflicts of Interest: The authors declare that they have no conflicts of interest to report regarding the present study.

References

[1] F. N. Al-Wesabi, "A smart English text zero-watermarking approach based on third-level order and word mechanism of Markov model," *Computers Materials & Continua*, vol. 65, no. 2, pp. 1137–1156, 2020.

[2] M. Abd-Eldayem, "A proposed security technique based on watermarking and encryption for digital imaging and communications in medicine," *Egyptian Informatics Journal*, vol. 14, no. 1, pp. 1–13, 2013.

[3] F. N. Al-Wesabi, "A hybrid intelligent approach for content authentication and tampering detection of Arabic text transmitted via Internet," *Computers, Materials & Continua*, vol. 66, no. 1, pp. 195–211, 2020.

[4] S. G. Rizzo, F. Bertini and D. Montesi, "Fine-grain watermarking for intellectual property protection," *EURASIP Journal on Information Security*, vol. 10, 2019.

[5] F. N. Al-Wesabi, K. Mahmood and N. Nemri, "A zero watermarking approach for content authentication and tampering detection of Arabic text based on fourth level order and word mechanism of Markov model," *Journal of Information Security and Applications*, vol. 52, pp. 1–15, 2020.

[6] P. Selvama, S. Balachandran, S. Pitchai and R. Jayabal, "Hybrid transform based reversible watermarking technique for medical images in telemedicine applications," *Optik*, vol. 145, pp. 655–671, 2017.

[7] Hurrah N. N., Parah S. A., Loan N. A., Sheikh J. A., Elhoseny M. and Muhammad K., "Dual watermarking framework for privacy protection and content authentication of multimedia," *Future Generation Computer Systems*, vol. 94, pp. 654–673, 2019.

[8] A. Panah, R. Van, T. Sellis and E. Bertino, "On the properties of non-media digital watermarking: a review of state-of-the-art techniques," *IEEE Access*, vol. 4, pp. 2670–2704, 2016.

[9] C. Qin, C. Chang and T. Hsu, "Fragile watermarking for image authentication with high-quality recovery capability," *KSII Transactions on Internet and Information Systems*, vol. 7, no. 11, pp. 2941–2956, 2013.

[10] S. Parah, J. Sheikh and G. Bhat, *StegNmark: A Joint Stego-Watermark Approach for Early Tamper Detection*, vol. 660. Switzerland: Springer International Publishing, 427–452, 2017.

[11] S. Hakak, A. Kamsin, O. Tayan, M. Yamani and G. Gilkar, "Approaches for preserving content integrity of sensitive online Arabic content: a survey and research challenges," *Information Processing & Management*, vol. 56, no. 2, pp. 367–380, 2019.

[12] M. Taleby, Q. Li, X. Zhu, M. Alazab and J. Zhang, "A Novel intelligent text watermarking technique for forensic identification of information on social media," *Computers and Security*, vol. 90, pp. 1–14, 2020.

[13] S. Parah, J. Sheikh, J. Akhoon and N. Loan, "Electronic health record hiding in images for smart city applications: a computationally efficient and reversible information hiding technique for secure communication," *Future Generation Computer Systems*, vol. 108, pp. 935–949, 2020.

[14] R. Ahmed and L. Elrefaei, "Arabic text watermarking: a review," *International Journal of Artificial Intelligence & Applications (IJAIA)*, vol. 6, no. 4, pp. 1–16, 2015.

[15] K. Hameed, A. Khan, M. Ahmed and A. G. Reddy, "Towards a formally verified zero watermarking scheme for data integrity in the internet of things based-wireless sensor networks," *ELSEVIER Future Generation Computer Systems*, vol. 167, pp. 1–16, 2018.

[16] R. Alotaibi and L. Elrefaei, "Improved capacity text watermarking methods based on open word space," *Journal of King Saud University – Computer and Information Sciences*, vol. 30, no. 2, pp. 236–248, 2018.

[17] M. Memon and A. Shah, "A novel text steganography technique to Arabic language using reverse fat5th5ta," *Pakistan Journal of Engineering, Technology and Sciences*, vol. 1, no. 2, pp. 106–113, 2015.

[18] Y. Alginahi, M. Kabir and O. Tayan, "An enhanced Kashida-based watermarking approach for increased protection in arabic text-documents based on frequency recurrence of characters," *International Journal of Computer and Electrical Engineering*, vol. 6, no. 5, pp. 381–392, 2014.

[19] A. Shaker, F. Ridzuan and S. Pitchay, "Text steganography using extensions Kashida based on moon and sun letters," *International Journal of Advanced Computer Science and Applications*, vol. 8, no. 8, pp. 286–290, 2017.

[20] A. Rahma, W. Bhaya and D. Al-Nasrawi, “Text steganography based on Unicode of characters in multilingual,” *Journal of Engineering Research and Applications*, vol. 3, no. 4, pp. 1153–1165, 2013.

[21] N. Al-maweri, W. Adnan, A. Rahman, S. Khair and S. Syed, “Robust digital text watermarking algorithm based on Unicode characters,” *Indian Journal of Science and Technology*, vol. 9, no. 48, pp. 1–14, 2016.

[22] M. Bashardoost, M. Rahim, T. Saba and A. Rehman, “Replacement attack: a new zero text watermarking attack,” *3D Research*, vol. 8, no. 1, 2017.

[23] Y. Liu, Y. Zhu and G. Xin, “A zero-watermarking algorithm based on merging features of sentences for Chinese text,” *Journal of the Chinese Institute of Engineers*, vol. 38, no. 3, pp. 391–398, 2015.

[24] P. Zhu, W. Song, A. Li, Y. Zhang and R. Tao, “A text zero-watermarking algorithm based on Chinese phonetic alphabets,” *Wuhan University Journal of Natural Sciences*, vol. 21, no. 4, pp. 277–282, 2016.

[25] Z. Ali, M. Shamim, G. Muhammad and M. Aslam, “New zero-watermarking algorithm using hurst exponent for protection of privacy in telemedicine,” *IEEE Access*, vol. 6, pp. 7930–7940, 2018.

[26] O. Tayan, Y. Alginahi and M. Kabir, “An adaptive zero-watermarking approach for text documents protection,” *International Journal of Image Processing Techniques*, vol. 1, no. 1, pp. 33–36, 2014.

[27] M. Ghilan, F. Ba-Alwi and F. N. Al-Wesabi, “Combined Markov model and zero watermarking to enhance authentication of Arabic text,” *Journal of Computational Linguistics Research*, vol. 5, no. 1, pp. 26–42, 2014.

[28] F. N. Al-Wesabi, A. Alsakaf and K. U. Vasantrao, “A zero text watermarking algorithm based on the probabilistic patterns for content authentication of text documents,” *International Journal of Computer Engineering & Technology*, vol. 4, no. 1, pp. 284–287, 2013.

[29] H. Ahmed and M. Khodher, “Comparison of eight proposed security methods using linguistic steganography text,” *International Journal of Computing and Information Sciences*, vol. 12, no. 2, pp. 243–251, 2016.

[30] F. N. Al-Wesabi, “Proposing high-smart approach for content authentication and tampering detection of Arabic text transmitted via Internet,” *IEICE transactions in Information Systems*, vol. E103, no. 10, pp. 2104–2112, 2020.