IEEE Access
Multidisciplinary ⋮ Rapid Review ⋮ Open Access Journal

Received 17 June 2023, accepted 17 July 2023, date of publication 20 July 2023, date of current version 17 August 2023.

Digital Object Identifier 10.1109/ACCESS.2023.3297263

RESEARCH ARTICLE

Heuristic Optimization Algorithm Based Watermarking on Content Authentication and Tampering Detection for English Text

FAHD N. AL-WESABI[1], **FADWA ALROWAIS**[2], **HEBA G. MOHAMED**[3], **MESFER AL DUHAYYIM**[4], **ANWER MUSTAFA HILAL**[5], **AND ABDELWAHED MOTWAKEL**[5]

[1]Department of Computer Science, College of Science and Art at Mahayil, King Khalid University, Abha 62529, Saudi Arabia
[2]Department of Computer Sciences, College of Computer and Information Sciences, Princess Nourah bint Abdulrahman University, Riyadh 11671, Saudi Arabia
[3]Department of Electrical Engineering, College of Engineering, Princess Nourah bint Abdulrahman University, Riyadh 11671, Saudi Arabia
[4]Department of Computer Science, College of Sciences and Humanities-Aflaj, Prince Sattam bin Abdulaziz University, Al-Kharj 16278, Saudi Arabia
[5]Department of Computer and Self Development, Preparatory Year Deanship, Prince Sattam bin Abdulaziz University, Al-Kharj 16278, Saudi Arabia

Corresponding author: Mesfer Al Duhayyim (m.alduhayyim@psau.edu.sa)

This work was supported by the Deanship of Scientific Research at Princess Nourah bint Abdulrahman University, through the Research Groups Program, under Grant RGP-1443-0048.

ABSTRACT Text information is a natural language dependent, which enhances reliability and security of text data exchanged through Internet networks and is becoming main concern for researchers. Content authentication, Tampering detection, and integrity verification of digital content are considered challenges in the information and communication exchange area through the Internet. Watermarking algorithms emerge as a potential method for achieving this with text. In simple words, text watermarking is embedding imperceptible text messages within the content that serve as unique signatures or identifiers. The text message has data regarding the content creator, copyright data, or other metadata utilized for authentication purposes. Therefore, this study presents a new Coyote Optimization Algorithm with Watermarking-based Content Authentication and Tampering Detection (COAW-CATD) technique for English text. The presented COAW-CATD technique aims to secure the English text via content authentication and tampering recognition. To accomplish this, the presented COAW-CATD technique designs a zero-watermarking (ZWM) approach to produce watermarks depending on the textual content. The generated watermark can be extracted to assure the authentication of the text document. Moreover, the COA can be utilized to optimize the placement of the watermarks in the content to ensure that it is imperceptible and robust to tampering. The experimental outcomes of the COAW-CATD algorithm are tested utilizing a series of simulations and the comparative study reported its superior performance with improved tampering detection accuracy of 95.93%.

INDEX TERMS Watermarking algorithm, content authentication, tampering detection, Coyote optimization algorithm, security.

I. INTRODUCTION

As e-commerce, internet, and other effective communication technology use increases, digital media content's authentication and copyright protection are of utmost significance [1]. Many digital contents are in text, like eBooks, email, short messaging systems/services (SMS), chats, e-commerce, news, and websites. Malicious attackers may temper these text documents, and the modified data can result in transaction disputes and fatal and wrong decisions. Tamper detection and Content authentication of digital image, video, and audio, has attracted more researchers' interest [2]. Currently, tamper detection, copyright protection, and content authentication of textual documents draw attention of researchers [3]. Likewise, over the past, the study on text watermarking techniques primarily concerned with disputes

The associate editor coordinating the review of this manuscript and approving it for publication was Pedro R. M. Inácio.

of copyright protection gave lesser interest to tamper detection, integrity verification, and content authentication [4]. Different approaches were designed for tamper detection, copyright authentication, and protection for digital textual files.

Digital Watermarking (DWM) methods are the dominant solutions to many issues [5]. The digital watermarking methods become solution to breaches of content authentication, tampering identification, and copyright protection of digital media. The authors have devised different watermarking methods for video, images, and audio. However, watermarking methods for text still need to be improved [6]. Conventional text watermarking approaches for text authentication and tampering detection, like image-based, format-based, and content-based, have many limitations [7]. It is not appropriate under arbitrary tampering attacks on each kind of text. They have to utilize certain modifications or transformations on content of the text file to embed watermark data within the original text file that, resulted in value degradation, text capability, meaning, and quality.

Various conventional text watermarking approaches and solutions were designed and categorized into binary image-based, structure-based, format-based, and linguistic-based [8]. Many solutions require certain transformations or modifications on digital text content to embed watermark data within text. Zero watermarking refers to a recent approach that was utilized with intelligent methods deprived of alteration on actual digital content for embedding the watermark data [9]. The difficulties involve evolving suitable approaches to hide data in the delicate text data without any alteration of it. Few studies have concentrated on needed applicable results for integrity authentication of delicate online digital media [10]. Tampering detection and Authentication of digital text have attained more interest among researchers. At the same time, the optimal placement of watermarks in the content can be considered as the NP hard problem, which can be resolved by metaheuristic optimization algorithms.

This study presents a new Coyote Optimization Algorithm with Watermarking-based Content Authentication and Tampering Detection (COAW-CATD) technique for English Text. The proposed COAW-CATD technique designs a zero-watermarking (ZWM) approach to produce watermarks depending on the textual content. The generated watermark can be extracted to ensure the authentication of the text document. Moreover, the COA can be utilized to optimize the placement of the watermarks in the content to ensure that it is imperceptible and robust to tampering. The experimental outcomes of the COAW-CATD approach are tested utilizing a series of simulations. In short, the major contributions of the study is listed as follows.

- A new COAW-CATD technique comprising ZWM watermarking and COA based optimization is presented for English text. To the best of our knowledge, the COAW-CATD technique never existed in the literature.
- Proposed model aims to ensure the authenticity and integrity of the text and provide a means for detecting tampering or unauthorized modifications.
- Employ ZWM technique for watermark generation based on textual data, which helps to accomplish text authenticity.
- Present COA based approach for the optimal placement of watermarks in the content.
- Validate the performance of the proposed model on four distinct textual dataset.

II. RELATED WORKS

Alamgeer et al. [11] developed a text zero-watermarking system called SFASCDW, abbreviated as (The smart-Fragile algorithm related to Soft Computing and Digital Watermarking) for tampering detection and content authentication of English text. Depending on hidden Markov method, a first-level order of alphanumeric system is compiled with digital zero watermarking algorithms to enhance watermark strength of presented method. Singh and Sharma [12] devised a tamper identification approach for document imageries utilizing zero watermarking concepts. The inputted document imagery was transformed using the execution of lifting wavelet transform to acquire their sub bands. Such sub bands were sub-classifies into non-overlapping blocks of similar sizes. Attributes of all blocks were mined to create zero watermarks. In [13], the authors presented a compiled technique CAZWNLP for detecting tampering with English text interchanged over the Internet. The third-grade level of Markov method was utilized in this technique as NLP technology to examine an English text and textual features of the presented contents.

Qi et al. [14] introduce a content authentication approach for printed fields depending on text watermarking approach resisting print-and-scan attacks. Initially, depending on the Logistic chaotic map method, an authentication watermark signal series relevant to content of text file was generated. In [15], the authors presented a three-dimensional text image watermarking model depending upon multilayer overlapping of extracted two-dimensional information, and a particular method is accordingly realized by means of embedding, extracting and overlapping of multiple watermarks in sequence. In [16], the authors presented a unique, robust database-watermarking algorithm. The author has established theoretically and confirmed the method performance concerning fewer data distortion and robustness.

Thabit et al. [17] modelled the Color and (CSNTSteg) Spacing Normalization stego approach for resolving the low invisibility and capacity issues in text steganography. The presented method has 2 stages: the pre-embedding phase that attains higher capability RGB as coding and character spacing. It is devised to raise the usable characters and number of bits per location. Li et al. [18] propose a practical and advanced invisible digital watermarking method for PPT fields. The author also can expand new methods from various angles and make reasonable use of the unique elements in PPT for embedding watermarks, which assures the watermark's security and enhance the robustness of the watermark.

Most of the existing watermarking techniques have mainly concentrated on different kinds of data, like images, audio, or video. As a result, there might be a lack of widespread research specifically addressing watermarking for English text authentication and tampering detection. The research gap may lie in the development of watermarking algorithms that can withstand different types of attacks specifically for English text, ensuring both robustness and security. In addition, existing works have the limitations in terms of computational complexity, processing time, or scalability to large-scale text documents. Therefore, this article explore these practical considerations and propose solutions to make the COAW-CATD technique efficient and applicable in real-world scenarios.

III. THE PROPOSED MODEL

This study introduced a novel COAW-CATD approach to authenticate content and detect tampering with English text data. The presented COAW-CATD technique aims to secure the English text via content authentication and tampering recognition. The presented COAW-CATD technique employed the ZWM approach to producing watermarks to accomplish this. Furthermore, the COA can be utilized to optimize the placement of the watermarks in the content to ensure that it is imperceptible and robust to tampering. Fig. 1 illustrates the workflow of the COAW-CATD approach.

A. WATERMARK GENERATION PROCESS

The presented model exploits the content of text to protect it. Based on the author's choice, a keyword from the text can be chosen and based on the length of proceeding, and a watermark is generated and resulting word length, to and from the keyword occurrences in text. It refers to a zero-watermarking system because watermark is not embedded in the text; instead, it can be created with the help of the text characteristics. The watermarking method includes two phases: (1) extraction algorithm and (2) embedding algorithm.

To prove ownership, can do extraction through a Certifying Authority (CA) and Watermark embedding. A trustworthy CA is basic prerequisite; then original copyright owner registers their watermark. When the text or content ownership is questioned, the trusted third party can act as a decision authority. The process that embeds watermarks in text is named as embedding system.

The watermark embedding process needs original text file as input, and the copyright owner or original author chooses keyword. The keyword must be a word with occurrence frequency in text. A watermark can be produced as output. Then, this watermark can be registered with CA, with author name, keyword, current time and date, and original text document. The algorithm proceeds as follows:

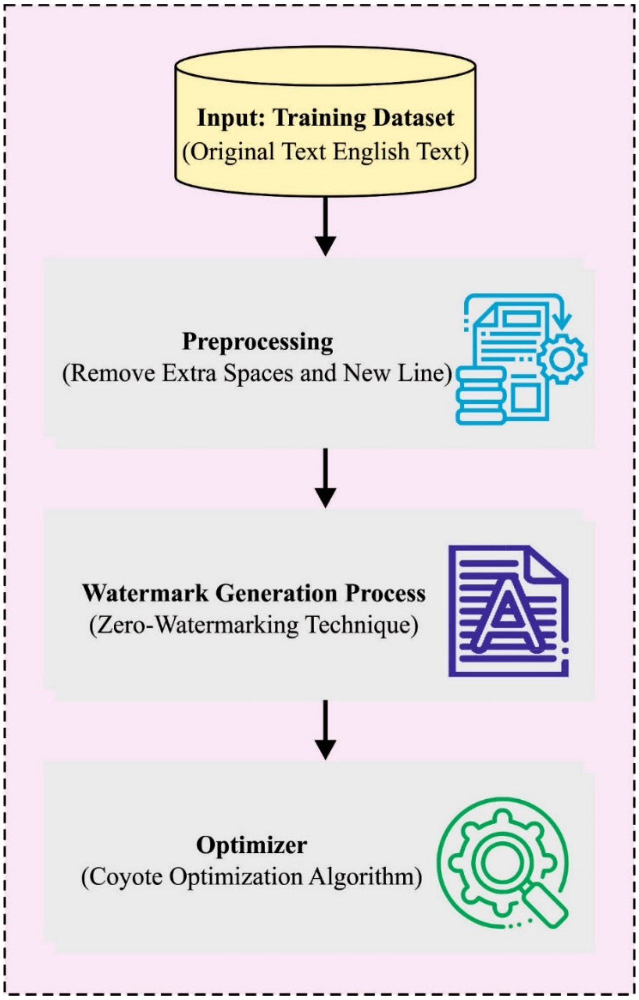
Input: Training Dataset
(Original Text English Text)
Preprocessing
(Remove Extra Spaces and New Line)
Watermark Generation Process
(Zero-Watermarking Technique)
Optimizer
(Coyote Optimization Algorithm)

FIGURE 1. Workflow of COAW-CATD approach.

Algorithm 1 Embedding Process

```
Read $T_O$.
Count frequency of every word in $T_O$.
Choose $KW$ according to frequent occurrence
$KWCOUNT$ = Overall occurrence of $KW$ in text $T_o$
for $i = 1$ to $KWCOUNT$, repeat steps 6 to 8.
$WM[j]$ = length (P)
$WM[j+1]$ = length (N)
$i = i + 1$ and $j = j + 1$
Output $WM$
```

N_i = Next word' of $i - th$ occurrence of KW, T_O = *Original* text; KW = *keyword*; WM = *Watermark*; P_i = Proceeding word' of $i - th$ occurrence of KW; $KWCOUNT$ = keyword count.

The original text (T) can be first attained from author, and frequent occurrence of all the words in text is examined. The author can choose a keyword, which is typically a word with maximal occurrence count in text. A numeric watermark is created, and the next and proceeding word length for each occurrence of keyword in text can be analysed. Then, this can be registered by CA with current date and time.

B. COA BASED WATERMARK PLACEMENT

In this work, the COA can be utilized to optimise the placement of the watermarks in the content to ensure that it is imperceptible and robust to tampering. COA is a population-based technique drawn motivation from coyote behavior where the population can be divided into $N_p \in \wedge p$ packs with $N_c \in N^*$ coyotes each. Initially, consider that the number of individuals in all the packs is fixed [19]. Thus, the population number can be attained by multiplying N_p and N_c. For simplicity purpose, individual coyote is not effectuated in COA. The method of the COA proposed depends on social condition of the coyotes. Fig. 2 illustrates the flowchart of COA. Social condition refers to objective function values; all coyotes represent a solution candidate. Thus, the social condition of c^{th} coyote at p^{th} pack is given as follows:

$$soc_c^{p,t} = \vec{x} = (x_1, x_2, \cdots, x_D) \tag{1}$$

It has been proved that coyote is adapted to the environmental condition $fit_c^{p,t} \in R$.

COA begin with the coyote population initialization. Similar to other random techniques, initial social condition of every coyote was randomly set. It allocates random value in search space for j^{th} dimension of c^{th} coyote at p^{th} pack as follows.

$$soc_{c,j}^{p,t} = lb_j + r_j \cdot \left(ub_j - lb_j\right) \tag{2}$$

In Eq. (2), D denotes the dimension of search space r_j shows the random integer within [0, 1], and lb_j and ub_j represent lower and upper boundaries of j^{th} dimension control parameter. Then, coyote adaptation towards existing social conditions was evaluated.

$$fit_c^{p,t} = f\left(soc_c^{p,t}\right) \tag{3}$$

At first, the coyote was divided into N_p packs. But in few instances, the coyote leaves the pack and joins another pack or becomes lone wolf. If coyote is discarded from the pack, was relevant to the amount of coyotes in pack, and occurrence probability can be evaluated by Eq. (4):

$$P_e = 0.005 \cdot N_c^2 \tag{4}$$

This method assists in diversifying interaction amongst each coyote in the COA, showing cultural interchange across the population. The alpha of p^{th} pack at t^{th} instant of time can be represented as follows.

$$alphd^{p,t}t = \{soc_c^{p,t} | arg_{c=\{1,2,\ldots,N_c\}} minf\left(soc_c^{p,t}\right) \tag{5}$$

Since the coyote shows some group intelligence, COA hypothesizes that coyote can share social conditions and has specific information exchange ability, which is favorable to development and maintenance of population. Thereby, COA connects each data from the coyotes, determined by the cultural trend in the group, and its equation can be given as follows.

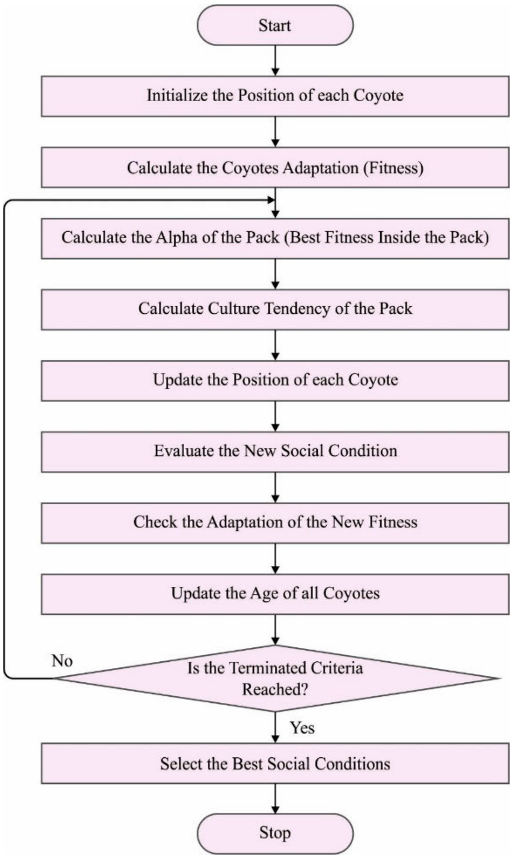
Start
Initialize the Position of each Coyote
Calculate the Coyotes Adaptation (Fitness)
Calculate the Alpha of the Pack (Best Fitness Inside the Pack)
Calculate Culture Tendency of the Pack
Update the Position of each Coyote
Evaluate the New Social Condition
Check the Adaptation of the New Fitness
Update the Age of all Coyotes
No
Is the Terminated Criteria Reached?
Yes
Select the Best Social Conditions
Stop

FIGURE 2. Flowchart of COA [20].

$$cult_j^{p,t} = \begin{cases} O_{\frac{N_C+1}{2}j}^{p,t}, & N_c isodd \\ \dfrac{o_{\frac{N_C}{2},j}^{p,t} + O_{\frac{N_C+1}{2},j}^{p,t}}{2}, & otherwise \end{cases} \tag{6}$$

In Eq. (6), $O^{p,t}$ signifies ranked social condition of every coyote of p^{th} pack at t^{th} instant of time for every j in the interval [1, D]. COA consider births and deaths of coyotes and calculates the age (in years), which can be represented as $age_c^{pt} \in N$. Birth of new coyote was relevant to parental social condition (arbitrarily chosen) and ecological influence that can be represented as follows:

$$pup_J^{p,t} = \begin{cases} soc_{r_1 i}^{p,t}, & rnd_j < P_s orj = j_1 \\ soc_{r_2 j}^{p,t}, & rnd_j \geq P_s + P_a orj = j_2 \\ R_j, & otherwise \end{cases} \tag{7}$$

In Eq. (7), P_s represent the scattering probability; r_1 and r_2 denote random coyote individuals at p^{th} pack;R_j implies the random integer in the range of control variable of j^{th} dimension; $j_1 andj_2$ shows the two random dimensions of the problems; rnd_j shows the random integer produced with uniform probability within [0, 1]; P_a indicates the association probability. Association and Scattering probabilities control diversity of social conditions in offspring coyotes. P_s and P_a are shown below:

$$P_s = 1/D$$
$$P_a = \frac{1-P_s}{2} \tag{8}$$

where P_a contain a similar effect on both parents, COA considers that every coyote was impacted by alpha (δ_1) and population (δ_2). The previous one signifies cultural differences among alpha Coyote and random coyote cr_1, whereas next one signifies difference between pack the and cultural tendency of random Coyote cr_2. Random coyote was carefully chosen by uniform distribution as follows.

$$\delta_1 = alpha^{p,t} - soc_{cr_1}^{p,t}$$
$$\delta_2 = cult^{p,t} - soc_{cr_2}^{p,t} \tag{9}$$

Therefore, alpha and pack effects updated the new social conditions of coyotes.

$$new\_soc_c^{p,t} = soc_c^{p,t} + r_1 \cdot \delta_1 + r_2 \cdot \delta_2 \tag{10}$$

In Eq. (10), r_1 and r_2 denote the weight of alpha and pack influence correspondingly. They were uniformly distributed random numbers from the [0, 1] interval. Then the subsequent equitation is used for evaluating the newest social condition.

$$new - fit_c^{p,t} = f\left(new\_soc_c^{p,t}\right) \tag{11}$$

Coyotes' cognitive capabilities define whether new social condition was superior to an older one:

$$soc_c^{p,t+1} = \begin{cases} new\_soc_c^{p,t}, & new\_fit_c^{p,t} < fit_c^{p,t} \\ soc_c^{p,t}, & otherwise \end{cases} \tag{12}$$

Lastly, the social condition of coyotes are better suited for environment were designated as global optimum solution to presented problems.

C. WATERMARK EXTRACTION PROCESS

The process that extracts the watermark from the text is named extraction algorithm. The presented approach inputs the keyword and plain text [21]. The text might be un-attacked or attacked. The watermark was produced from the text through the extraction method, and later; the original watermark registered was compared with CA. Also, the author's name, current time and date with *CA* are recorded. Numerous watermark registration conflicts with CA are resolved by maintaining record of time and date. The author with past registration entries can be considered an original author.

Text documents can be named authentic text without tampering, and these algorithms can precisely identify the watermark in the absence of attack on text. The watermark is distorted in the existence of tampering attack with text. Tampering could be deletion, insertion, re-ordering or paraphrasing of sentences and words in text. The extraction approach is given below:

EWM = Extracted Watermark; T_O = *Original* text; T_A =Attacked text; *KW* = *keyword*; P_i = Proceeding word' of $i-th$ occurrence of *KW*; N_i = 'Next word' of *ith* occurrence of *KW*; *KWCOUNT* =keyword count.

Algorithm 2 Extraction Process

```
Read $T_O$ or p$T_A$, $KW$ and $WM$.
Count occurrence of $KW$ in specified text.
$KWCOUNT$ = Total occurrence of $KW$ in tex
for $i = 1$ to $KWCOUNT$, repeat steps 5 to 7.
$EWM[j]$ = length (P)
$EWM[j+1]$ = length (N)
$i = i + 1$ and $j = j + 1$
if $EWM$( does not equal $WM$)
$Tamper = YES$
Output $EWM$.
```

TABLE 1. TDA analysis of COAW-CATD approach with distinct volumes of attacks.

Attack Volume (%)	Insertion	Deletion	Reorder
5	95.06	91.91	79.91
10	91.06	84.72	65.90
20	83.14	73.31	46.59
50	65.82	42.54	22.16

IV. RESULTS AND DISCUSSION

In this section, the experimental outcomes of the COAW-CATD method are tested using four datasets [22], namely [ELST, 2018], [ESST, 179], [EHMST, 559], and [EMST, 421]. This dataset includes all English characters, numbers, spaces, and symbols. Experiments have been conducted with distinct dataset size and various kinds of frequency attacks.

Table 1 and Fig. 3 report the overall tampering detection accuracy (TDA) results of the COAW-CATD technique under different attacks. The figure indicates that COAW-CATD technique attains increasing TDA values under all volumes. For example, with attack volume of 5%, the COAW-CATD technique achieves TDA of 95.06%, 91.91%, and 79.97% under insertion, deletion, and reorder attacks. Meanwhile, with attack volume of 10%, the COAW-CATD method achieves TDA of 91.06%, 84.72%, and 65.90% under insertion, deletion, and reorder attacks. Moreover, with attack volume of 20%, the COAW-CATD approach gains TDA of 83.14%, 73.31%, and 46.59% under insertion, deletion, and reorder attacks. Finally, with attack volume of 50%, the COAW-CATD method achieves TDA of 65.82%, 42.54%, and 22.16% under insertion, deletion, and reorder attacks.

In Table 2 and Fig. 4, the comparative outcomes of the COAW-CATD method are given under varying datasets with existing methods [22], [23] such as hybrid text analysis and zero-watermarking approach (HTAZWA), Zero-Watermarking Approach based on Fourth level order of Word Mechanism of Markov Model (ZWAFWMMM), an intelligent hybrid of natural language processing and

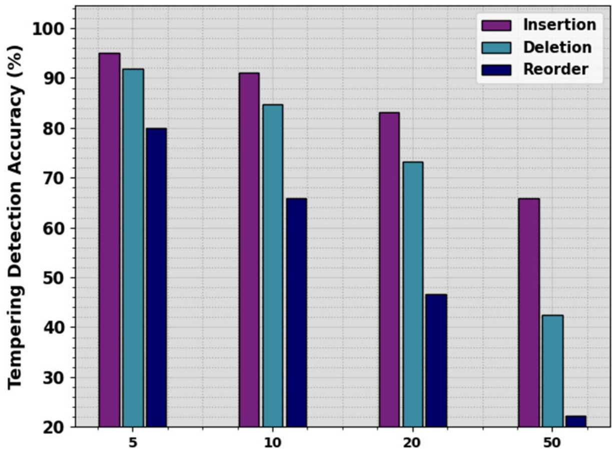

FIGURE 3. TDA analysis of COAW-CATD approach with distinct volumes of attacks.

TABLE 2. TDA analysis of COAW-CATD approach with other systems under distinct datasets [22], [23].

Dataset	ZWAFWMMM	NLPZWA	HTAZWA	COAW-CATD
Dataset 1	68.68	66.16	69.94	73.41
Dataset 2	67.42	62.06	72.15	76.56
Dataset 3	63.63	53.86	65.84	73.72
Dataset 4	60.17	49.76	67.73	73.72

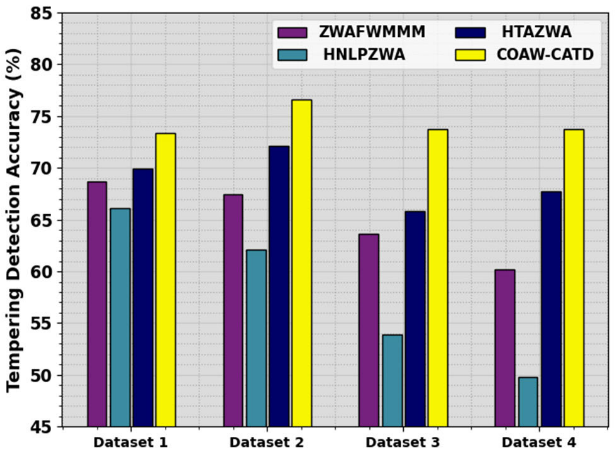

FIGURE 4. TDA analysis of COAW-CATD approach under distinct datasets.

TABLE 3. TDA analysis of COAW-CATD method with other systems under distinct types of attacks [22], [23].

Different types of attacks	ZWAFWMMM	HNLPZWA	HTAZWA	COAW-CATD
Insertion	78.10	69.21	79.95	89.57
Deletion	64.40	54.77	69.95	81.80
Reorder	44.04	34.04	50.33	63.66

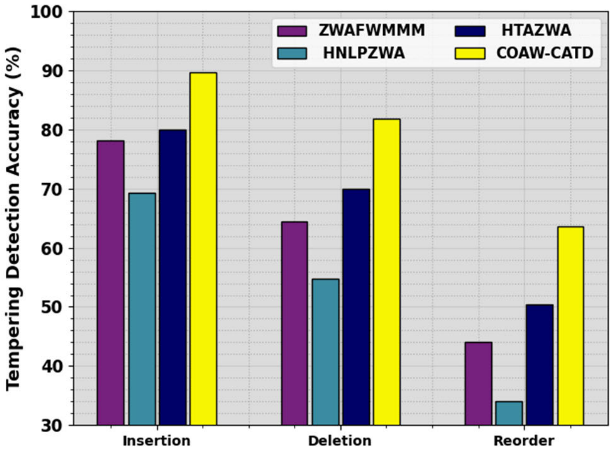

FIGURE 5. TDA analysis of COAW-CATD approach under distinct volumes of attacks.

zero-watermarking approach (HNLPZWA). The figure indicate the better performance of the COAW-CATD method under all datasets. For example, with dataset-1, the COAW-CATD approach accomplishes higher TDA of 73.41% while the ZWAFWMMM, HNLPZWA, and HTAZWA techniques obtain lower TDA of 68.68%, 66.16%, and 69.94% respectively. Simultaneously, with dataset-2, the COAW-CATD approach accomplishes higher TDA of 76.56% while the ZWAFWMMM, HNLPZWA, and HTAZWA techniques obtain lower TDA of 67.42%, 62.06%, and 72.15% correspondingly. Concurrently, with dataset-3, the COAW-CATD technique establishes higher TDA of 73.72% while the ZWAFWMMM, HNLPZWA, and HTAZWA techniques acquire lower TDA of 63.63%, 53.86%, and 65.84% correspondingly. At last, with dataset-4, the COAW-CATD technique establishes higher TDA of 73.72% while the ZWAFWMMM, HNLPZWA, and HTAZWA techniques reach lower TDA of 60.17%, 49.76%, and 67.73% respectively.

In Table 3 and Fig. 5, the comparative outcomes of the COAW-CATD method are given under different attacks. The figure indicates the better performance of the COAW-CATD technique under types of attacks. For example, with Insertion, the COAW-CATD method accomplishes higher TDA of 89.57% while the ZWAFWMMM, HNLPZWA, and HTAZWA techniques acquire lower TDA of 78.10%, 69.21%, and 79.95% respectively. Simultaneously, with Deletion, the COAW-CATD technique accomplishes higher TDA of 81.80% while the ZWAFWMMM, HNLPZWA, and HTAZWA methods obtain lower TDA of 64.40%, 54.77%, and 69.95% correspondingly. Simultaneously, with Reorder, the COAW-CATD method accomplishes higher TDA of 63.66% while the ZWAFWMMM, HNLPZWA, and HTAZWA techniques obtain lower TDA of 44.04%, 34.04%, and 50.33% correspondingly.

TABLE 4. TDA analysis of COAW-CATD approach with other systems under distinct attack volumes [22], [23].

Under varying attack volume	ZWAFWMMM	HNLPZWA	HTAZWA	COAW-CATD
5	80.58	79.08	89.19	95.93
10	70.84	69.72	80.20	90.69
20	56.98	53.24	65.97	80.20
50	32.27	9.42	44.25	59.23

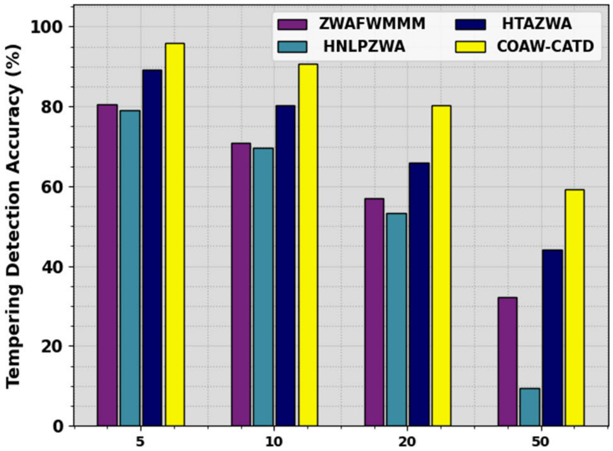

FIGURE 6. TDA analysis of COAW-CATD approach under distinct attack volumes.

In Table 4 and Fig. 6, the comparative outcomes of the COAW-CATD method are given under varying attack volumes. The outcomes indicate the better performance of the COAW-CATD approach under all attack volumes. For example, with attack volume of 5%, the COAW-CATD technique accomplishes higher TDA of 95.93% while the ZWAFWMMM, HNLPZWA, and HTAZWA techniques obtain lower TDA of 80.58%, 79.08%, and 89.19% respectively. Simultaneously, with attack volume of 10%, the COAW-CATD technique has higher TDA of 90.69%, while the ZWAFWMMM, HNLPZWA, and HTAZWA techniques obtain lower TDA of 70.84%, 69.72%, and 80.20% correspondingly.

Concurrently, with attack volume of 20%, the COAW-CATD technique accomplishes higher TDA of 80.20% while the ZWAFWMMM, HNLPZWA, and HTAZWA techniques obtain lower TDA of 56.98%, 53.24%, and 65.97% correspondingly. Eventually, with attack volume of 50%, the COAW-CATD technique accomplishes higher TDA of 59.23% while the ZWAFWMMM, HNLPZWA, and HTAZWA techniques obtain lower TDA of 32.27%, 9.42%, and 44.25% correspondingly.

Finally, a detailed ROC analysis of the proposed model is presented under four datasets, as shown in Fig. 7. The results indicate that the proposed model reaches improved ROC values under all datasets. Therefore, the proposed model can be applied for accomplishing content authenticity and tampering detection process.

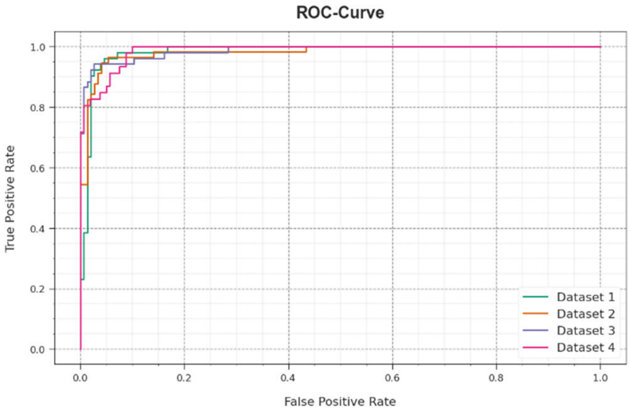

FIGURE 7. ROC analysis of COAW-CATD approach under distinct datasets.

V. CONCLUSION

In this study, we have introduced a novel COAW-CATD method to authenticate content and detect tampering with English text data. The presented COAW-CATD technique aims to secure the English text via content authentication and tampering recognition process. To accomplish this, the presented COAW-CATD technique employed the ZWM approach to producing watermarks depending upon the textual content. The generated watermark can be extracted to assure the authentication of the text document. Furthermore, the COA can be utilized to optimize the placement of the watermarks in the content to ensure that it is imperceptible and robust to tampering. The experimental outcomes of the COAW-CATD technique are tested with the sequence of simulations. The comparison study reported that the COAW-CATD technique shows improved performance over its recent method. In the future, the performance of the COAW-CATD approach will be boosted by the use of image watermarking system. Besides, the proposed model can be extended to the content authentication on different languages. Moreover, the computational time complexity of the proposed model can be examined in the future.

ACKNOWLEDGMENT

This work was supported by the Deanship of Scientific Research at Princess Nourah bint Abdulrahman University, through the Research Groups Program, under Grant RGP-1443-0048.

REFERENCES

[1] G. O. Young, "Synthetic structure of industrial plastics," in *Plastics*, vol. 3, 2nd ed., J. Peters, Ed. New York, NY, USA: McGraw-Hill, 1964, pp. 15–64.

[2] S. K. Das and M. Z. Rahman, "A secured compression technique based on encoding for sharing electronic patient data in slow-speed networks," *Heliyon*, vol. 8, no. 10, Oct. 2022, Art. no. e10788.

[3] M. L. P. Gort, M. Olliaro, A. Cortesi, and C. F. Uribe, "Semantic-driven watermarking of relational textual databases," *Expert Syst. Appl.*, vol. 167, Apr. 2021, Art. no. 114013.

[4] U. Khadam, M. M. Iqbal, M. Alruily, M. A. Al Ghamdi, M. Ramzan, and S. H. Almotiri, "Text data security and privacy in the Internet of Things: Threats, challenges, and future directions," *Wireless Commun. Mobile Comput.*, vol. 2020, pp. 1–15, Feb. 2020.

[5] X. Wang and Y. Jin, "A high-capacity text watermarking method based on geometric micro-distortion," in *Proc. 26th Int. Conf. Pattern Recognit. (ICPR)*, Aug. 2022, pp. 1749–1755.

[6] S. Abdelnabi and M. Fritz, "Adversarial watermarking transformer: Towards tracing text provenance with data hiding," in *Proc. IEEE Symp. Secur. Privacy (SP)*, May 2021, pp. 121–140.

[7] N. Mir and M. A. U. Khan, "Copyright protection for online text information: Using watermarking and cryptography," in *Proc. 3rd Int. Conf. Comput. Appl. Inf. Secur. (ICCAIS)*, Mar. 2020, pp. 1–4.

[8] Y. Chou, K. Anggriani, N. Wu, and M. Hwang, "Research on E-book text copyright protection and anti-tampering technology," *Int. J. Netw. Secur.*, vol. 23, no. 5, pp. 739–749, 2021.

[9] A. Banerjee, P. Shivakumara, P. Acharya, U. Pal, and J. L. Canet, "TWD: A new deep E2E model for text watermark/caption and scene text detection in video," in *Proc. 26th Int. Conf. Pattern Recognit. (ICPR)*, Aug. 2022, pp. 1492–1498.

[10] U. Khadam, M. M. Iqbal, S. Saeed, S. H. Dar, A. Ahmad, and M. Ahmad, "Advanced security and privacy technique for digital text in smart grid communications," *Comput. Electr. Eng.*, vol. 93, Jul. 2021, Art. no. 107205.

[11] M. Alamgeer, F. N. Al-Wesabi, H. G. Iskandar, I. Khan, N. Nemri, M. Medani, M. A. Al-Hagery, and A. M. Al-Sharafi, "Smart-fragile authentication scheme for robust detecting of tampering attacks on English text," *Comput., Mater. Continua*, vol. 71, no. 2, pp. 2497–2513, 2022.

[12] B. Singh and M. K. Sharma, "Tamper detection technique for document images using zero watermarking in wavelet domain," *Comput. Electr. Eng.*, vol. 89, Jan. 2021, Art. no. 106925.

[13] F. N. Al-Wesabi, S. Alzahrani, F. Alyarimi, M. Abdul, N. Nemri, and M. M. Almazah, "A reliable NLP scheme for English text watermarking based on contents interrelationship," *Comput. Syst. Sci. Eng.*, vol. 37, no. 3, pp. 297–311, 2021.

[14] W. Qi, W. Guo, T. Zhang, Y. Liu, Z. Guo, and X. Fang, "Robust authentication for paper-based text documents based on text watermarking technology," *Math. Biosci. Eng.*, vol. 16, no. 4, pp. 2233–2249, 2019.

[15] K. Ding, T. Hu, W. Niu, X. Liu, J. He, M. Yin, and X. Zhang, "A novel steganography method for character-level text image based on adversarial attacks," *Sensors*, vol. 22, no. 17, p. 6497, 2022.

[16] Y. Zhang, Z. Wang, Z. Wang, and C. Liu, "A robust and adaptive watermarking technique for relational database," in *Proc. 18th China Annu. Conf. Cyber Secur. (CNCERT)*, Beijing, China. Singapore: Springer, Jan. 2022, pp. 3–26.

[17] R. Thabit, N. I. Udzir, S. M. Yasin, A. Asmawi, and A. A. Gutub, "CSNTSteg: Color spacing normalization text steganography model to improve capacity and invisibility of hidden data," *IEEE Access*, vol. 10, pp. 65439–65458, 2022.

[18] D. Li, Y. Chen, J. Li, L. Cao, U. A. Bhatti, and P. Zhang, "Robust watermarking algorithm for medical images based on accelerated-KAZE discrete cosine transform," *IET Biometrics*, vol. 11, no. 6, pp. 534–546, Nov. 2022.

[19] A. Abaza, R. A. El-Sehiemy, K. Mahmoud, M. Lehtonen, and M. M. Darwish, "Optimal estimation of proton exchange membrane fuel cells parameter based on coyote optimization algorithm," *Appl. Sci.*, vol. 11, no. 5, p. 2052, 2021.

[20] J.-H. Zhu, J.-S. Wang, X.-Y. Zhang, H.-M. Song, and Z.-H. Zhang, "Mathematical distribution coyote optimization algorithm with crossover operator to solve optimal power flow problem of power system," *Alexandria Eng. J.*, vol. 69, pp. 585–612, Apr. 2023.

[21] Z. Jalil, A. M. Mirza, and M. Sabir, "Content based zero-watermarking algorithm for authentication of text documents," 2010, *arXiv:1003.1796*.

[22] F. N. Al-Wesabi, "Text analysis-based watermarking approach for tampering detection of English text," *Comput., Mater. Continua*, vol. 67, no. 3, pp. 3701–3719, 2021.

[23] F. N. Al-Wesabi, H. G. Iskandar, M. Alamgeer, and M. M. Ghilan, "Proposing a high-robust approach for detecting the tampering attacks on English text transmitted via Internet," *Intell. Autom. Soft Comput.*, vol. 26, no. 4, pp. 1267–1283, 2020.