Fortifying Textual Integrity: Evolutionary Optimization-powered Watermarking for Tampering Attack Detection in Digital Documents

Roman Shkilev[1], Alevtina Kormiltseva[1], Marina Achaeva[1], Aiziryak Tarasova[2], Marguba Matquliyeva[3]

[1]Candidate of Philological Sciences, Associate Professor of Department of English Philology and Intercultural Communication, Kazan Federal University, Elabuga Institute of KFU, Elabuga, Russia.
[2]Candidate of Philological Sciences, Senior Lecturer of Department of English Philology and Intercultural Communication, Kazan Federal University, Elabuga Institute of KFU, Elabuga, Russia.
[3]PhD in Philological Sciences, Head of the Department of Uzbek and Russian Literature, Urgench State Pedagogical Institute, Urgench, Uzbekistan.
Emails: shkilev.r.e@yandex.ru; kormiltseva.a.l@mail.ru; achaeva.m.s@mail.ru; tarasova.a.n@inbox.ru; matquliyeva.m@mail.ru

Abstract

Digital document helps as the lifeblood of present communication, yet their vulnerability to tampering poses major safety anxieties. Digital text watermarking is an effective mechanism to protect the reliability of text-based data in the digital. Introducing a hidden layer of accountability and safety, allows individuals and organizations to trust the written word and make sure the truth behind all the files. Watermarking model identifies the tampering attack by inspecting the embedded signature for distortions or alterations. Watermarks can able to mechanically classify and repair themselves once tampered with, improving document resilience. Watermarking acts as a powerful tool to detect tampering attacks in digital document. By embedding strong and imperceptible watermarks in document distribution or creation, alterations are recognized by specialized procedure. This study introduces an Evolutionary Optimizer-powered Watermarking for Tampering Attack Detection in Digital Document (EO-WTAD3) model. The main intention of EO-WTAD3 approach is to support textual integrity using the applications of metaheuristic optimizer algorithm based watermarking technique for detecting tampering attacks in digital document. In the EO-WTAD3 method, a digital watermarking method has been proposed for the ownership verification and document copyright protection using data mining concept. Moreover, the EO-WTAD3 technique utilizes the concepts of data mining to define appropriate characteristics from the document for embedding watermarks. Moreover, fractional gorilla troops optimization (FGTO) algorithm can be applied for the assortment of optimal situation of watermarks in the content, ensuring both imperceptibility and strong to tamper. The performance validation of the EO-WTAD3 methodology takes place employing multiple datasets. The extensive result analysis portrayed that the EO-WTAD3 system accomplishes improve solution with other existing approaches with respect distinct aspects.

Keywords: Digital Watermarking; Tampering Attack Detection; Digital Documents; Metaheuristic; Fractional Gorilla Troops Optimization

1. Introduction

Due to wide-ranging growth in the internet and digital communication technologies, the processes of data generation are quickly altering in modern world [1]. Currently, the online digital communication system supports for definitely spreading and storing multimedia files namely video, audio, and image. Nevertheless, the data can be changed for illegitimate usage by intruders at multimedia storage and transmission. Consequently, copyright protection recognition of ownership, and fake detection do not retain data integrity and cause issues with image authentication [2]. In numerous human-centered applications like military communication, medical imaging,

Doi: https://doi.org/10.54216/FPA.140208
Received: July 29, 2023 Revised: November 11, 2023 Accepted: January 13, 2024

remote sensing, and implementation of geographic data systems, illegitimate alteration develops a problem. Digital watermarking (DWM) techniques must be incorporated to overcome these issues. For data security, various methods and approaches are accessible like the detection of tampering, verification of integrity, authentication of content, copyright protection, and access control [3]. To address these problems, steganography and automatic systems of watermarking have been popularly employed. DWM is integrated into digital material in different details namely binary images, video, audio, and text. A fine-grained text watermarking process has been developed dependent upon changing the white spaces and Latin symbols with homoglyph characters [4]. Text is data exchange and easiest mode of communication, taking different challenges when it comes to authentication and copyright protection. Some modifications in text must maintain the value, utility, grammaticality, and meaning of the text. Small documents can be highly complex for protection and authentication as a simple analysis will certainly expose the watermark creating text insecurity [5]. In image, audio, and video watermarking the restrictions of Human Auditory or Human Visual Systems have been utilized for watermark embedding and intrinsic redundancy. It is challenging to determine these restrictions and redundancy in plain text, as text defines sensitivity to some alteration essential to be created for watermark embedding.

Text is simple to reproduce copy and tamper with as related to images, audio, and video [6]. Text has been a specific medium that needs particular authentication and copyright protection solutions. Standard watermarking methods modify the contents of the digital medium to be secured by embedding a watermark. This conventional watermarking method is not applicable to plain text [7]. A particular watermarking technique like zero-watermarking can create the requirement for text. In this research, we proposed an advanced zero-watermarking approach that employs the contents of text itself for its authentication [8]. A zero-watermarking technique does not modify the features of new data however; employs the characters of original information for making original watermark data. Numerous traditional techniques and solutions for text watermarking have been developed and classified into diverse classifications namely structure, format-based and image-based binary images, and linguistic [9]. To embed the watermark data into the text, majority of these results need specific updates or enhancements to the actual text in material digital layout. Zero-watermarking without some modification to the new digital material for embedding the watermark data is an innovative method with clever approaches, which could be utilized [10]. A number of methods are introduced for increasing the capability of coverless data hidden in digital media depending on different algorithms like anime characters, to denote and transfer confidential data employing unchanged natural stego-carriers, and map the connections built among the intrinsic images feature and secret data.

This study develops an Evolutionary Optimization-powered Watermarking for Tampering Attack Detection in Digital Documents (EO-WTAD3) technique. In the EO-WTAD3 technique, a digital watermarking approach has been developed for document copyright protection and ownership verification using data mining concepts. In addition, the EO-WTAD3 technique utilizes the concepts of data mining to determine appropriate characteristics from the document for embedding watermarks. Moreover, fractional gorilla troops optimization (FGTO) algorithm can be applied for the selection of optimum placement of watermarks in the content, ensuring both imperceptibility and strong to tamper. The performance validation of the EO-WTAD3 approach takes place using multiple datasets.

2. Related Works

Al-Wesabi et al. [11] introduced an innovative Coyote Optimizer Algorithm with Watermarking-based Content Authentication and Tampering Detection (COAW-CATD) method for English text. This technique developed a zero-watermarking (ZWM) method for creating watermarks dependent upon the textual contents. The produced watermarks could be removed to promise the verification of the text. Besides, the COA has been employed for enhancing the assignment of the watermarks in the contents. In [12], human visual model based modified LSB replacement technique was employed to propose an image watermarking method. A saliency map was designed as well a watermark has been adaptably inserted into the cover image pixels to achieve good visual photo by raised pay load. The hardware implementation could be established utilizing Virtex6 FPGA board (xc6vlx760).

In [13], an effective text-based watermarking technique was developed. Both removing and embedding of the watermark have been logically applied and could not be modified in the digital text. It was accomplished through the third stage and alpha numeric approach of the Markov technique for example, a text analysis method to analyse the contents for achieving their features that should be deliberated as the digital watermark. In [14], a speech watermarking-based tamper identification and recovery technique was developed. The authentication and recovery watermarks have been inserted into the original speech utilizing misalign and align embedding approaches, correspondingly. Especially, the misaligned embedding scheme that allocates the recovery watermarks repetitively and extensively will avoid speech segmentation as well as simultaneously its recovery watermarks in tampered that considerably improvise the tolerable tamper rate (TTR) of the developed technique.

Doi: https://doi.org/10.54216/FPA.140208
Received: July 29, 2023 Revised: November 11, 2023 Accepted: January 13, 2024

In [15], a novel audio fake detection method was introduced. This method could be utilized in edge devices for recognizing intruders and tampering with audio information. The designed model was employed through a recent mel-frequency cepstral coefficient feature. In the meantime, a Gaussian mixture system could be further implemented for validating and training the developed technique. Alghamdi et al. [16] projected to utilize BC technology—as reliable third party—including watermarking to offer resources of rights security of relational databases. This architecture integrated the flexibility of the watermarking method and robustness of BC technology. The developed method works with non-numeric features of relational datasets as well as does not objective only choose tuples or parts (subset) in the databases for watermark embedding distinct majority of the present approaches.

In [17], an innovative DL-based technique was examined for embedding unnoticeable watermarks. The main insight controlling the framework model was the requirement for correlating the sizes of these watermarks with the dimensions of receptive fields (RF). This version creates the watermarks highly strong but also allows to produce as an improved maintenance of image quality. Banerjee et al. [18] intended to design an innovative Deep End-to-End architected for Text Watermark Detection (TWD). This method utilizes the U-Net3+ framework to improve inferior-quality text without impacting higher-quality text. This method also implements Stacked Hourglass Encoded Fourier Contour Embedding Network (SFCENet) by providing the outcome of U-Net3+ architecture as input. Additionally, the developed method incorporates improvement and identification systems as an end-wise model to identify multiple categories of text in video images.

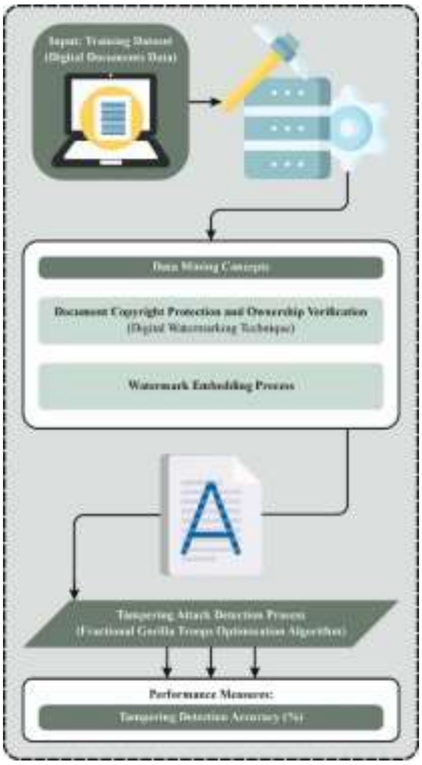
Input: Training Dataset
(Digital Documents Data)
Data Mining Concepts
Document Copyright Protection and Ownership Verification
(Digital Watermarking Technique)
Watermark Embedding Process
Tampering Attack Detection Process
(Fractional Gorilla Troops Optimization Algorithm)
Performance Measures:
Tampering Detection Accuracy (%)

Figure 1: Overall flow of EO-WTAD3 system

3. The Proposed Model

The objective of Data mining (DM) is to extract valuable data from the information. MS-Word document incorporates a group of objects, where all the objects have several properties and methods that allow users to manipulate and interact with them. MS-Word document has various attributes where watermark information is stored, and it could not affect the entire document. The major problem is to determine appropriate properties that is integrate huge sizes of confidential messages. In this work, the watermark is embedded into various attributes of MS-Word document. The presented model is imperceptible, strong, and integrates huge embedded capacity. The watermarked documents are stored or shared via the cloud after embedding the watermark. The accessibility and authentication of original documents are possible through smart gadgets on IoT. Fig. 1 represents the entire flow of EO-WTAD3 algorithm.

Doi: https://doi.org/10.54216/FPA.140208
Received: July 29, 2023 Revised: November 11, 2023 Accepted: January 13, 2024

A. Watermark Embedding

This part discusses how watermark data is embedded from the document [19]. The confidential messages are encrypt AES model utilizing 256 bits; Encryption is used to protect the message. The encrypted messages are brought to the next stage, but the watermark can be produced. The encrypted messages are changed into binary and then numbers. It is used to split the numbers into 4 equivalent parts and hoard them into number of variables (a, b, c, d). The length (L) of numbers is evaluated and later zeroes are added at the beginning. Logarithm Base 10 is utilized to decrease the variable values (a, b, c, d).

The logarithm of "x" is the exponent to another number that is set, Base "b" must be increased for "x" number.

$$ln(x) = log_e(x) \tag{1}$$

$$e = \lim_{n}(1 + n)^n \tag{2}$$

By increasing the base "b" to the logarithm "y", the inverse of logarithm otherwise known as anti-logarithm is evaluated.

$$x = log^{(-1)}(y) = b^y \tag{3}$$

Next, the new document is taken as input, and DM has been used to define appropriate properties from MS-Word document. The application class and document class are the two different classes of MS-Word documents. Application class property is modified by the VB (Visual Basic) for embedding watermarks, and it could not disturb the document. The distinct characteristics of MS-Word documents were applicable for 2 major causes. At first, son MS-Word mutual command will not impact the watermark data. Next, a massive number of data are stored without affecting the entire document.

The watermark data is divided into equivalent groups embedded in this property and later the second level embedding begins. MS-Word document margins from the layout are directed in second level embedding. The values of margin bottom, top, right, and left are altered and exchanged with 4 variables correspondingly. The watermarked document is created in Portable Document Format (PDF), and when the document format is changed during the verification process, then the document margin cannot be modified and remains unchanged. Once MS-Word document is converted into PDF to Word Document, the Layout and Margins of the text could not be modified. The MS-Word file has been changed into PDF after embedding watermark and shared or stored using the cloud.

B. Watermark Placement using FGTO Algorithm

The FGTO algorithm can be applied for the selection of optimal location of watermarks in the text to confirm that it is invisible and strong to tamper. This section explains and discusses FGTO method, which combines fractional concepts together with GTO method [20]. GTO is a metaheuristic system derived from the social intelligence and collective lifestyle of gorillas. Generally, gorilla survives in a group, known as troop that consists of adult female and male gorillas known as silverback. GTO primarily consists of initialize, global, and local exploitation stages. This technique attains higher accuracy in real applications, but still, it fails to improve the performance while reducing the overall process consumption. This approach attained lesser information loss and better computational performance. Hence, FC model is integrated with GTO technique to enhance performance of the system. The process of FGTO algorithm is given below,

1. Initialization

Assume L gorillas in R^{th} dimension space and the position of v^{th} gorilla in search range is given by,

$$P_v = \{P_{v,1}, P_{v,2}, \dots\dots, P_{v,B}\}; v = 1,2,3, \dots., A \tag{4}$$

Later, initialized process of gorilla population has been represented as follows,

$$P_{A\times B =} rand(A, B) \times (I - N) + N \tag{5}$$

Where I implies upper boundary and N specifies lower boundary. $rand(A, B)$ denotes matrix with A rows and B columns where each component is random number within [0,1].

2. Computation of fitness function

The fitness value can be measured by MSE with difference among classified output and target outcome from DCNN as,

Doi: https://doi.org/10.54216/FPA.140208
Received: July 29, 2023 Revised: November 11, 2023 Accepted: January 13, 2024

$$\omega = \frac{1}{\mathrm{k}} \sum_{\varpi=1}^{k} (M_k^* - M_k)^2 \tag{6}$$

WhereM_k signifies infers generated output from DCNN, ω defines the fitness function (FF), k represents total count of training instances, and M_k^* denotes target result.

3. Exploration phase

The gorillas move to different surroundings and leave their groups. Now, every individual is called a candidate solution and better performance in optimizer process is regarded as silverback. The updating location can be performed by accurately simulating the behavior of migration such as shifting to other groups, migration towards unidentified locations, and migration around familiar positions.

$$TP(w+1) =$$

$$\begin{cases} (I — N) \times y_2 + N & ; y1 < 0 \\ (y_3 - Z) \times P_M(w) + I \times C \times P(w) & ; y_1 \geq 05 \\ P(w) - I \times \Big(I \times \big(P(w) - P_T(w)\big) + y_4 \times \big(P(w) - P_T(w)\big)\Big) & ; \ y_1 < 0.5 \end{cases} \tag{7}$$

where $P(w)$ denotes the existing location vector of individual, W indicates the existing iteration, y_1, y_2, y_3 and y_4 are random numbers within [0,1], $TP(w + I)$ represents candidate site of search agent in successive iterations, $P_M(w)$ and $P_I(w)$ is an arbitrarily selected gorilla location in existing population, the constant C denotes row vector in problem measurement where element value is randomly created within [-Z, Z],

$$Z = [\cos(2 \times y_5) + 1] \times \left[1 - \frac{r}{G}\right] \tag{8}$$

In Eq. (8), cos is cosine function, G is maximal iteration, and y_5 denotes the random number within [0, 1].

$$I = Z \times X \tag{9}$$

In Eq. (9), X is the random number within [-1,1].

In the last stage of exploration, the fitness rate of new candidate $TP(w + I)$ solution can be evaluated. If the fitness is better than prior performance then original values are altered with newest solution. In the meantime, optimal performance has been selected as silverback P_{sb}.

$$TP(w+1) = (y_3 - Z) \times P_M(w) + I \times C \times P(w) \tag{10}$$

Now, the $TP(w + I) = P(w + I)$, thus Eq. (10), can be written as,

$$P(w+1) = P_M(w)(y_3 - Z) \times P_M(w) + I \times C \times P(w) \tag{11}$$

Subtract $P(w)$ on both sides in Eq. (11),

$$P(w+1) - P(w) = P_M(w)(y_3 - Z) \times P_M(w) + I \times C \times P(w) - P(w) \tag{12}$$

Apply the concept of FC in above expression,

$$Y^{\alpha}[P(w+1)] = P_M(w)(y_3 - Z) \times P(w) + (I \times C - 1) \tag{13}$$

$$P(w+1) - \alpha P(W) - \frac{1}{2}\alpha P(w-1) - \frac{1}{6}(1-\alpha)P(w-2) -$$

$$\frac{1}{24}\alpha(1-\alpha)(2-\alpha)P(w-3) = P_M(w)(y_3 - Z) + P(w)(1 \times C - 1) \tag{14}$$

$$P(w+1) = P_M(w)(y_3 - Z) + P(w)(I \times C - 1) + \alpha P(VV) +$$

$$\frac{1}{2}\alpha P(w-1) + \frac{1}{6}(1-\alpha)P(w-2) + \frac{1}{24}\alpha(1-\alpha)(2-\alpha)P(w-3) \tag{15}$$

$$P(w+1) = P_M(w)(y_3 - Z) + P(w)[(I \times C - 1) + \alpha] + P(\mathcal{V}V) +$$

Doi: https://doi.org/10.54216/FPA.140208
Received: July 29, 2023 Revised: November 11, 2023 Accepted: January 13, 2024

$$\frac{1}{2}\alpha P(w-1)+\frac{1}{6}(1-\alpha)P(w-2)+\frac{1}{24}\alpha(1-\alpha)(2-\alpha)P(w-3) \tag{16}$$

Where, $P(w+1)$ is position of solution in $(w+1)^{th}$ iteration, $P(w-1)$ specifies location of performance in $(w-1)^{th}$ iteration, $P(w-2)$ represents position of outcome in $(w-2)^{th}$ iteration, and $P(w-3)$ implies location of performance in $(w-3)^{th}$ iteration.

4. Exploitation stage

The silverback has powerful and healthy, while other males are still young. Generally, they follow each choice of silverback while finding different food resources and faithfully helping silverback gorillas. The silverback develops older and deceases together with young black back in troops might get comprised into malicious fights with other male gorillas for mating through leadership and adult females. These 2 features of silverback and competing for adult female gorillas have been intended in exploitation phase. The term 0 is regarded to control the shift amongst them. If the rate of Z is higher than 0, then the 1st method has been preferred. This stage is formulated by,

$$TP(w+1)=I\times G\times[P(w)-P_{sb}]+P(w) \tag{17}$$

In Eq. (17), $P(w)$ implies existing location vector and P_{sb} refers optimum solution,

$$G=\left(\left|\sum_{v=1}^{A}P_v\left(\frac{w}{A}\right)\right|^{2^I}\right)^{\frac{1}{2^{\mathrm{I}}}} \tag{18}$$

In Eq. (18), $P_v(w)$ implies location vector of gorilla in existing iteration and A denotes population size.

The gorilla location was upgraded, if $Z<0$, it defines that last method is chosen.

$$TP(w+1)=P_{sb}-(P_{sb}\times K-P(w)\times K)\times N \tag{19}$$

In Eq. (19), the term K and N are evaluated as follows,

$$K=2\times y_6-1 \tag{20}$$

$$N=\delta\times P \tag{21}$$

$$P=\begin{cases}A_1\ y_7\geq 0.5\\ A_2\ y_7<0.5\end{cases} \tag{22}$$

Where, $P(w)$ denotes existing location, K symbolizes impact force, y_6 indicates random integer from 0 to 1, N imitates violence intensity, y_7 indicates random value within [0,1], and δ denotes constant. Fig. 2 illustrates the flowchart of FGTO.

Doi: https://doi.org/10.54216/FPA.140208
Received: July 29, 2023 Revised: November 11, 2023 Accepted: January 13, 2024

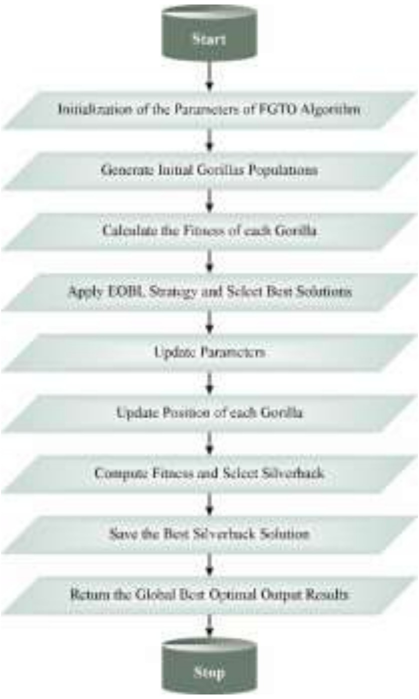
Start
Initialization of the Parameters of FGTO Algorithm
Generate Initial Gorillas Populations
Calculate the Fitness of each Gorilla
Apply EOBL Strategy and Select Best Solutions
Update Parameters
Update Position of each Gorilla
Compute Fitness and Select Silverback
Save the Best Silverback Solution
Return the Global Best Optimal Output Results
Stop

Figure 2: Flowchart of FGTO

5. Evaluating solution possibility

The FF can be estimated by Eq. (6) to obtain optimum solution, if the newest solution is obtained then the ideal solution, and then replaced with oldest solution.

6. Termination

The abovementioned steps are repeated until the terminating criteria are met.

C. Watermark Extraction

The inverse method of watermark embedding is watermark extraction. The watermark verification or extraction method removes the secret data (watermark) in the watermarked document. The PDF document has been kept on the cloud as input and converted into MS-Word. During an initial phase, the value is gained from special property, and anti-log is used for retrieving the actual value. These 4 temporary variables can be utilized for storing the value. Later, concatenate them into separate variables “M”. They can automatically identify the bottom, top, right, and left margins of document layout and store them into variables $("T","B","L","R")$. Anti-log has been used for retrieving the real value and concatenates them into ‘‘D”. These “M” and “D” variables concatenate, and the result is generated as number string. Further, the number string can be changed into Binary and later reverted into character. The AES utilizing 256 bit is applied to encryption was used for the cover message decryption. A similar Key has been utilized for decrypting the text that provides confidential information viz., hidden in the document.

4. Performance Validation

In this part, the experimental results of the EO-WTAD3 technique are verified employing four datasets [21], such as [ELST, 2018], [ESST, 179], [EHMST, 559], and [EMST, 421]. This dataset contains all English characters, numbers, spaces, and symbols. Experiments have been directed with different dataset sizes and types of frequency attacks.

In Table 1 and Fig. 3, the results of the EO-WTAD3 technique is examined in terms of recognition accuracy (DA). The results imply that the EO-WTAD3 technique reaches improved performance with increased DA values. With attack volume of 5%, the EO-WTAD3 technique accomplishes improved DA of 96.65%, 93.69%, and 81.54% under insertion, deletion, and reorder attacks. Additionally, with attack volume of 10%, the EO-WTAD3 model achieves enhanced DA of 92.73%, 86.44%, and 67.43% below insertion, deletion, and reorder attacks. Along with that, with attack volume of 20%, the EO-WTAD3 methodology accomplishes enhanced DA of 84.71%, 74.96%, and 48.31% under insertion, deletion, and reorder attacks. At last, with attack volume of 50%, the EO-WTAD3 model attains upgraded DA of 67.47%, 44.16%, and 23.93% below insertion, deletion, and reorder attacks.

Doi: https://doi.org/10.54216/FPA.140208
Received: July 29, 2023 Revised: November 11, 2023 Accepted: January 13, 2024

Table 1: Classifier result of EO-WTAD3 technique under various attack volumes

Attack Volume (%)	Insertion	Deletion	Reorder
5	96.65	93.69	81.54
10	92.73	86.44	67.43
20	84.71	74.96	48.31
50	67.47	44.16	23.93

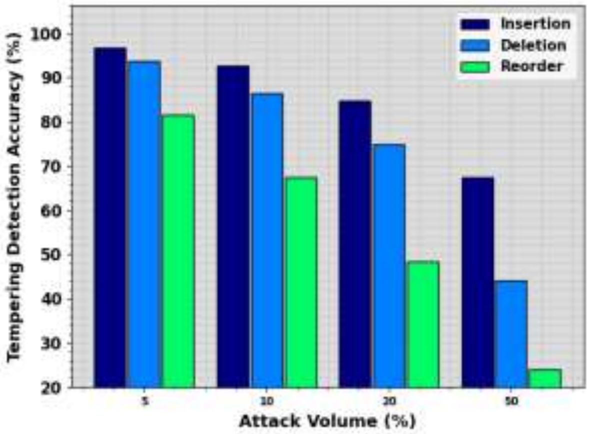

Figure 3: Classifier result of EO-WTAD3 technique under various attack volumes

Table 2 and Fig. 4 represents a comparison study of the EO-WTAD3 technique with current models under varying datasets [11]. The results indicate that the EO-WTAD3 technique obtains enhanced DA values under all datasets. It is noticed that the NLPZWA and ZWAFWMMM models offer least DA values. Besides, the HTAZWA and COAW-CATO models accomplished slightly boosted DA values. However, the EO-WTAD3 technique gains enhanced performance with improved DA of 76.70%, 79.99%, 76.83%, and 77.23% under datasets 1-4, respectively.

Table 2: Comparative analysis of EO-WTAD3 technique with recent models under varying datasets

Dataset	ZWAFWMMM	NLPZWA	HTAZWA	COAW-CATO	EO-WTAD3
Dataset 1	70.23	67.75	71.51	74.94	76.70
Dataset 2	69.12	63.59	73.91	78.32	79.99
Dataset 3	65.23	55.62	67.39	75.33	76.83
Dataset 4	61.70	51.39	69.25	75.52	77.23

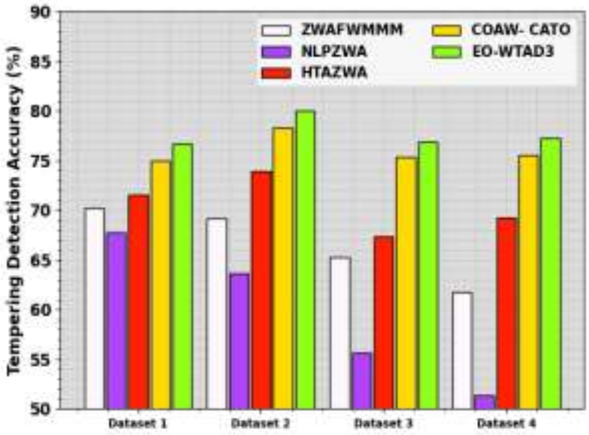

Figure 4: Comparative analysis of EO-WTAD3 technique under varying datasets

Doi: https://doi.org/10.54216/FPA.140208
Received: July 29, 2023 Revised: November 11, 2023 Accepted: January 13, 2024

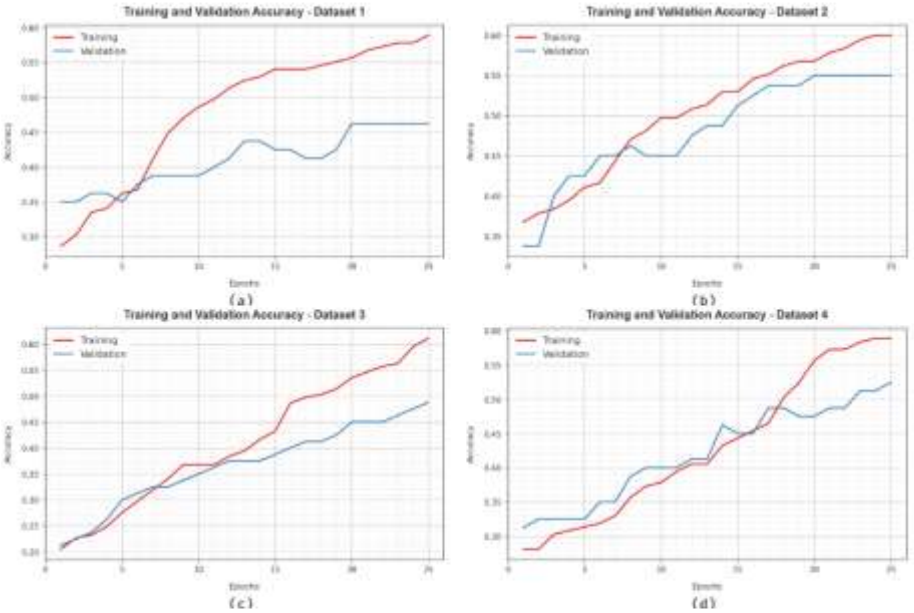

Figure 5: $Accu_y$ curve of EO-WTAD3 technique under varying datasets

The $accu_y$ curves for training (TR) and validation (VL) exposed in Fig. 5 for the EO-WTAD3 technique under varying datasets provide valuable visions into its performance below numerous epochs. Particularly, there is a reliable development in both TR and TS $accu_y$ with growing epochs, representing the model's ability in learning and identifying patterns from the both TR and TS data. The upward trend in TS $accu_y$ highlights the model's flexibility to the TR dataset and its capability to create precise forecasts on unseen data, emphasizing robust generalized abilities.

Fig. 6 offers a complete summary of the TR and TS loss values for the EO-WTAD3 model below varying datasets. The TR loss steadily decreases as the model enhances its loads to decrease classification errors on both datasets. The loss curves obviously clarify the model's alignment with the TR data, highlighting its ability to capture designs professionally in both datasets. Noteworthy is the continuous modification of parameters in the EO-WTAD3 technique, aimed at minimalizing differences amongst predictions and actual TR labels.

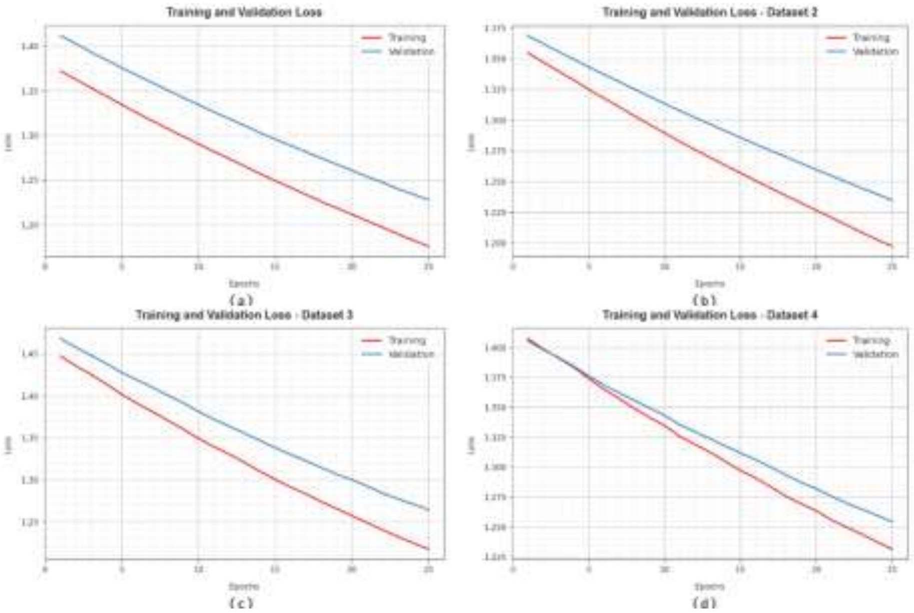

Figure 6: Loss curve of EO-WTAD3 technique under varying datasets

Doi: https://doi.org/10.54216/FPA.140208
Received: July 29, 2023 Revised: November 11, 2023 Accepted: January 13, 2024

Table 3 and Fig. 7 signifies a contrast research of the EO-WTAD3 model with current methods below dissimilar kinds of attacks. The outcomes designate that the EO-WTAD3 methodology gets improved DA values below all attacks. It is observed that the ZWAFWMMM and HNLPZWA techniques provide least DA values. Also, the HTAZWA and COAW-CATO methodologies proficient slightly increased DA values. But, the EO-WTAD3 approach gains higher performance with better DA of 97.78%, 85.19%, and 66.94% under insertion, deletion, and reorder, correspondingly.

Table 3: Comparative analysis of EO-WTAD3 technique with recent models under varying attacks

Different types of attacks	ZWAFWMMM	HNLPZWA	HTAZWA	COAW-CATD	EO-WTAD3
Insertion	79.86	70.77	81.69	90.16	91.78
Deletion	66.02	56.55	71.54	83.56	85.19
Reorder	45.77	35.74	52.06	65.39	66.94

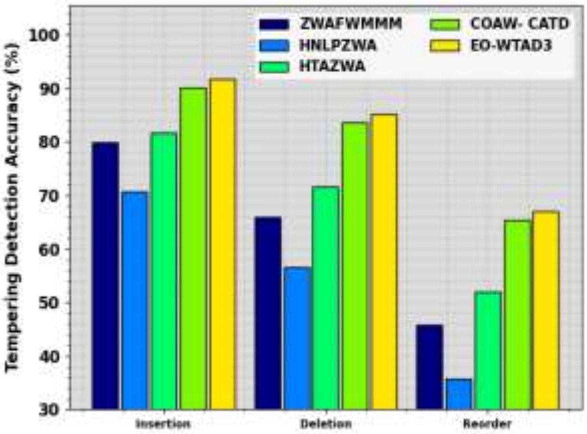

Figure 7: Comparative analysis of EO-WTAD3 technique under varying attacks

Table 4 and Fig. 8 denotes a comparison study of the EO-WTAD3 model with current models below varying attack volumes. The consequences designate that the EO-WTAD3 approach attains boosted DA values under all attack volumes. It is perceived that the ZWAFWMMM and HNLPZWA models provide minimum DA values. Moreover, the HTAZWA and COAW-CATO models accomplished slightly boosted DA values. However, the EO-WTAD3 method gains greater performance with enhanced DA of 98.49%, 93.97%, 83.45%, and 62.38% under attack volume of 5-50%, separately.

Table 4: Comparative analysis of EO-WTAD3 technique with recent models under varying attack volumes

Attack volume (%)	ZWAFWMMM	HNLPZWA	HTAZWA	COAW-CATD	EO-WTAD3
5	82.24	80.86	90.86	96.69	98.49
10	72.53	71.27	81.99	92.40	93.97
20	58.51	54.96	67.70	81.74	83.45
50	33.81	10.99	45.81	60.83	62.38

Doi: https://doi.org/10.54216/FPA.140208
Received: July 29, 2023 Revised: November 11, 2023 Accepted: January 13, 2024

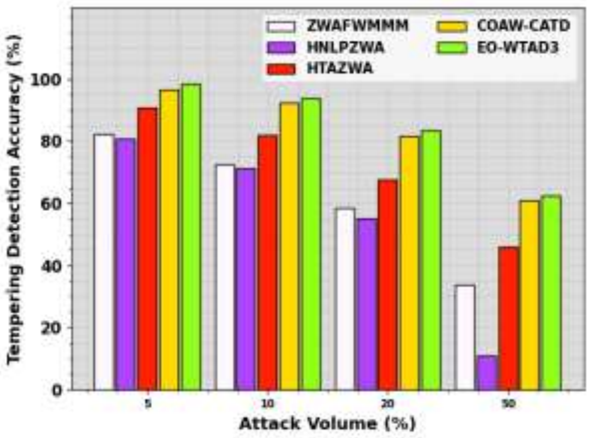

Figure 8: Comparative analysis of EO-WTAD3 technique under varying attack volumes

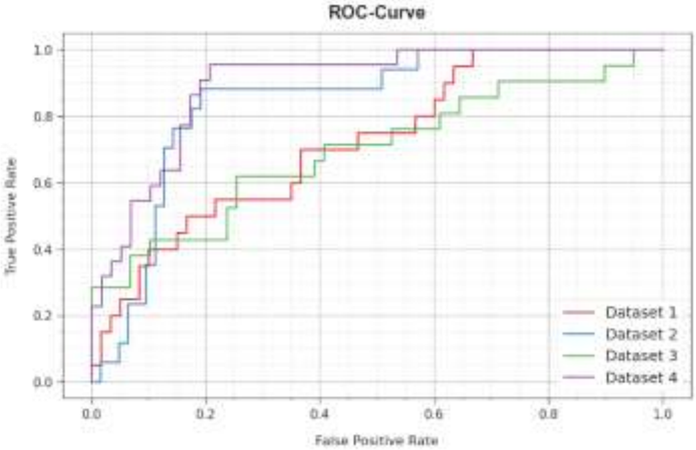

Figure 9: ROC curve of EO-WTAD3 technique under varying datasets

Furthermore, in Fig. 9, we present ROC curves generated by the EO-WTAD3 model under varying datasets, representing its ability in distinguishing amongst class labels. These curves provide valuable visions into how the trade-off between TPR and FPR differs through diverse classification epochs and thresholds. The results underline the model's accurate classification performance below several class labels, highlighting its efficiency in addressing varied classification tasks.

These results shown that the EO-WTAD3 technique reaches better performance over other models on tampering attack detection on digital text documents.

5. Conclusion

In this study, we have established an innovative EO-WTAD3 technique. The EO-WTAD3 technique aims to fortify textual integrity via the application of metaheuristic optimization algorithm based watermarking approach for the detection of tampering attacks in digital documents. In the EO-WTAD3 technique, a digital watermarking model has been projected for document copyright security and ownership verification employing data mining models. Besides, the EO-WTAD3 technique uses the thoughts of data mining in order to describe the suitable features from the document for embedding watermarks. Furthermore, FGTO procedure can be employed for the selection of optimum placement of watermarks in the content, safeguarding both imperceptibility and strong to tamper. The performance validation of the EO-WTAD3 model takes place by employing manifold datasets. An extensive outcome analysis depicted that the EO-WTAD3 model attains improved solution with other current approaches with respect dissimilar features.

Funding: “This research received no external funding”

Conflicts of Interest: “The authors declare no conflict of interest.”

Doi: https://doi.org/10.54216/FPA.140208
Received: July 29, 2023 Revised: November 11, 2023 Accepted: January 13, 2024

References

[1] Smarandache, F., Neutrosophic set a generalization of the intuitionistic fuzzy sets. Inter. J. Pure Appl. Math., 24, 287 – 297, 2005.

[2] 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.

[3] 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.

[4] 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.

[5] 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.

[6] 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.

[7] 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.

[8] 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.

[9] 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.

[10] 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.

[11] Qu, C., Liu, C., Liu, Y., Chen, X., Peng, D., Guo, F. and Jin, L., 2023. Towards Robust Tampered Text Detection in Document Image: New Dataset and New Solution. In Proceedings of the IEEE/CVF Conference on Computer Vision and Pattern Recognition (pp. 5937-5946).

[12] Al-Wesabi, F.N., Alrowais, F., Mohamed, H.G., Al Duhayyim, M., Hilal, A.M. and Motwakel, A., 2023. Heuristic Optimization Algorithm Based Watermarking on Content Authentication and Tampering Detection for English Text. IEEE Access.

[13] Sinha Roy, S., Basu, A., Chattopadhyay, A. and Kamal, R., 2021. Hardware execution of a saliency map based digital image watermarking framework. Multimedia Tools and Applications, 80(18), pp.27245-27258.

[14] Mustafa Hilal, A., Al-Wesabi, F.N., Alamgeer, M., Hamza, M., Mahzari, M. and Almekhlafi, M.A., 2022. An Optimal Text Watermarking Method for Sensitive Detecting of Illegal Tampering Attacks. Computers, Materials & Continua, 70(3).

[15] Wang, S., Yuan, W., Zhang, Z. and Wang, L., 2023. Speech watermarking based tamper detection and recovery scheme with high tolerable tamper rate. Multimedia Tools and Applications, pp.1-19.

[16] Mubeen, Z., Afzal, M., Ali, Z., Khan, S. and Imran, M., 2021. Detection of impostor and tampered segments in audio by using an intelligent system. Computers & Electrical Engineering, 91, p.107122.

[17] Alghamdi, A.S., Naz, S., Saeed, A., Al Solami, E., Kamran, M. and Alkatheiri, M.S., 2022. A novel database watermarking technique using blockchain as trusted third party. Computers, Material and Continua (CMC), 70(1), pp.1585-1601.

[18] Semyonov, N., Puzis, R., Shabtai, A. and Katz, G., 2023. ReMark: Receptive Field based Spatial WaterMark Embedding Optimization using Deep Network. arXiv preprint arXiv:2305.06786.

[19] Banerjee, A., Shivakumara, P., Acharya, P., Pal, U. and Canet, J.L., 2022, August. TWD: A New Deep E2E Model for Text Watermark/Caption and Scene Text Detection in Video. In 2022 26th International Conference on Pattern Recognition (ICPR) (pp. 1492-1498). IEEE.

[20] Khadam, U., Iqbal, M.M., Azam, M.A., Khalid, S., Rho, S. and Chilamkurti, N., 2019. Digital watermarking technique for text document protection using data mining analysis. IEEE Access, 7, pp.64955-64965.

[21] Mali, S.D. and Agilandeeswari, L., 2023. Non-redundant shift-invariant complex wavelet transform and fractional gorilla troops optimization-based deep convolutional neural network for video watermarking. Journal of King Saud University-Computer and Information Sciences, 35(8), p.101688.

[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.

Doi: https://doi.org/10.54216/FPA.140208
Received: July 29, 2023 Revised: November 11, 2023 Accepted: January 13, 2024