Integration of Crayfish Optimization with Watermarking Scheme for Automated Tampering Text Detection

Hanan T. Halawani[1,*]

[1]Department of Computer Science, College of Computer Science and Information Systems, Najran University, Najran, 61441, Saudi Arabia

Email: Hthalawani@nu.edu.sa

Abstract

Digital text document serves as the essence of existing communication but still pose major safety concerns on their vulnerability to tampering. Digital text watermarking acts as a powerful tool to secure the reliability of textual data. Presenting a hidden layer of safety and accountability enables organizations and individuals to make sure of the truth behind each file and trust the written word. Watermarking detects tampering by checking the embedded signature for changes or distortions. The Watermark model is capable of mechanically repairing and classifying themselves once tampered with, enhancing document resilience. Watermarking is an effective mechanism to identify tampering attacks in digital documents. The specialized process of embedding imperceptible and strong watermarks in document creation or distribution detects alterations. This study proposes the Crayfish Optimization with a Watermarking Scheme for Automated Tampering Text Detection (CFOWS-ATTD) technique. The major purpose of the CFOWS-ATTD technique is to accomplish the security of English text using content authentication and tampering detection. In the CFOWS-ATTD technique, two-stage processes are involved. Moreover, the CFOWS-ATTD technique generates a watermark from the text document and performs extraction to verify text authenticity. Furthermore, the CFO approach optimally places the watermark to ensure it remains robust and imperceptible to tampering. The experimentation of the CFOWS-ATTD approach is performed under the ELST, ESST, EHMST, and EMST datasets. The results implied that the CFOWS-ATTD approach obtains optimum performance over other techniques.

Keywords: Digital Watermarking; Tampering Text Detection; Crayfish Optimization; Text Authentication; Embedding

1. Introduction

Securing and verifying shared text online is a growing challenge for researchers [1]. In communicational technologies, automated text verification of trustworthiness and authentication of contents from various formats and languages become of major importance [2]. Various applications like e-commerce and e-banking render data transmitted through the internet to be more complex. Digital watermarking is a main method that is deployed in the authentication and security of images [3]. During the methods, a watermark is inserted at the protection media with the help of redundancy. Accordingly, to the embedding, the hidden image contents become altered which commonly misrepresents the visual quality of the hidden images [4]. Natural images comprise space that is more redundant and it could be employed for watermark embedding. It will be caused an alteration in the watermark images and cannot be observed by human being's eyes. By comparison, to natural images, document images are a reasonably confined redundancy [5]. Therefore, smaller modifications in the document image will be simply identified. During the image documents, it will be comprised of efficiently embedding the digital watermark.

DOI: https://doi.org/10.54216/JCIM.170203
Received: April 02, 2025 Revised: June 24, 2025 Accepted: August 13, 2025

Watermarking techniques can be used in document images, but they are highly prone to distortions from the embedding process [6]. Document image watermarking has several problems and complexities because of such parameters.

Various standard approaches and solutions aimed at text watermarking is presented and categorized as various classifications like structure, linguistic, and images [7]. Embedding watermark data in documents often requires modifications or additions to the original digital text content. There is no modification of zero watermarking for embedding the watermark information will be an advanced approach with smart techniques that will be employed [8]. Numerous methods were developed to increase the proficiency of open information concealed in digital media reliant on diverse methods such as the anime aspect, for signifying and transferring confidential information, and to map the correlation built amongst the complex image features and private data. Limited exploration has concentrated on the proper performance for verifying the reliability of important digital media [9]. Digital text verification and the recognition of fraud in studies gain significant consideration. Also, text watermarking analysis has numerous studies focused on copyright security recently nevertheless, decreased consideration will be compensated by identification of tampering, content and integrity verification because of the presence of text content dependent upon Natural language processing (NLP) [10].

This study proposes the Crayfish Optimization with a Watermarking Scheme for Automated Tampering Text Detection (CFOWS-ATTD) technique. The major purpose of the CFOWS-ATTD technique is to accomplish the security of English text using content authentication and tampering detection. In the CFOWS-ATTD technique, two-stage processes are involved. Moreover, the CFOWS-ATTD technique generates a watermark from the text document and performs extraction to verify text authenticity. Furthermore, the CFO approach optimally places the watermark to ensure it remains robust and imperceptible to tampering. The experimentation of the CFOWS-ATTD approach is performed under the ELST, ESST, EHMST, and EMST datasets.

2. Literature Survey

Alohali et al. [11] developed an Evolutionary Optimizer-based Watermarking for Tamper Attack Detection in Digital Documentation (EO-WTAD3) approach. The proposed approach integrates these concepts, while the fractional gorilla troop's optimizer (FGTO) model is applied to determine optimal conditions. Jana et al. [12] utilized the absolute moment block truncation coding (AMBTC) and fuzzy logic (FL) methods. Using a similarity matrix, blocks are classified by pixel similarity; smooth blocks use mean values for retrieval, while complex blocks apply AMBTC for better detail preservation. Sahu et al. [13] projected an effective two image-based reversible fragile watermarking scheme (DI-RFWS) technique. The pixel modification approach is used for acquiring the dual watermarked images (WIs). Palani and Loganathan [14] introduced an innovative Conventional Attention Network (CoAtNet) method. A 2-stage embedding is also developed. The turtle shell data hiding (TSDH) model executed the main embedding, and another stage of embedding could be performed by the DWT-SVD conversion.

In [15], a tamper identification and self-recovery watermarking method dependent upon texture degree and cross embedding was developed. Primarily, distribute the medical images; produce a dual authentication watermark in the region of interest (RoI); estimate texture complexities reliant on 4D features; create various recovery watermarking by implementing the compression-aware technology. In conclusion, find the tampered blocks at the ROI are dependent upon a 3 stages tamper recognition approach comprising pixel-level, multi-direction subband, and block-level -level. Rhayma et al. [16] projected an innovative technique employing CNN. The method utilizes perceptual hash function (PHF). In addition, a pseudo-random map is produced. This CNN is employed and more compared with the original hash value. In [17], the smart-fragile model on soft computation and digital watermarker (SFASCDW) method is developed. A 1st level-order alphanumeric method is reliant on the hidden Markov with digital zero-watermarking methods. In [18], a region-based flexible medical image watermark method was developed. The method has RoI tamper identification and retrieval proficiencies. The authentication information was embedded by applying the prediction-error developmental method.

3. The Proposed Model

In this study, the CFOWS-ATTD technique is presented. The major purpose of the CFOWS-ATTD technique is to accomplish the security of the English text using content authentication and tampering detection. Fig. 1 exhibits the entire flow of the CFOWS-ATTD model.

DOI: https://doi.org/10.54216/JCIM.170203
Received: April 02, 2025 Revised: June 24, 2025 Accepted: August 13, 2025

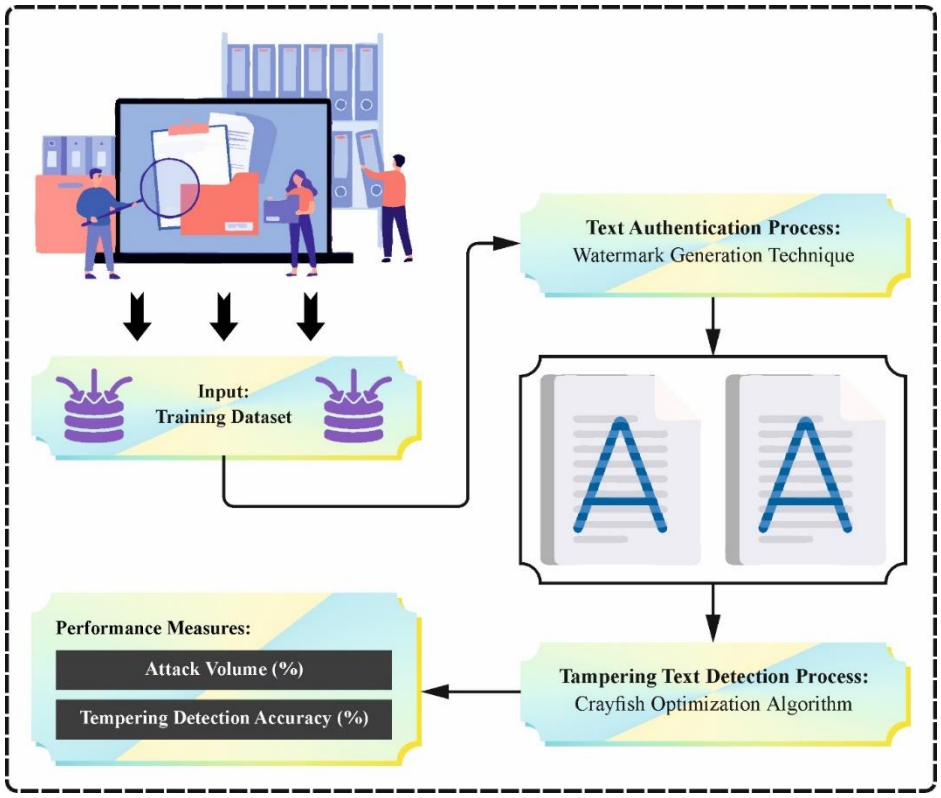

Figure 1. Overall process of CFOWS-ATTD technique

A. Watermarking Scheme

This section considers the watermark data that is embedded in the document [11]. The secret information is encrypted AES using 256 bits; Encryption is employed to safeguard the messages and is carried in the second phase, then the watermarks are created. The encrypted text is changed into binary and then number. It splits the number into 4 equal portions and hoards them into $(a, b, c, and\ d)$ variables. The length (L) is calculated and then zeroes is added at an early stage. Logarithm Base-10 is used for minimizing the variable values (a, b, c, d).

The "x" defines the exponent to alternative no. of sets, base "b" should be higher for the "x" number.

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

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

The anti-logarithm is calculated by raising the base "b" to the power of the logarithm "y".

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

Then, the new documents are considered as input, and DM defines suitable properties from the MS Word file. There are two diverse classes of MS Word documents namely application and document classes. Visual Basic (VB) modifies the application class to embed the watermark without affecting the document. MS Word features are ideal as common commands don't disrupt the watermark, and large data can be stored without altering document content.

The watermark information is broken down into equal groups and begins, the 2nd stage of embedding. MS Word file margins are focused in 2nd stage embedding. The margin-left, top, bottom and right values are exchanged and altered with 4 variables. The watermarked documents are generated in PDF, which remains unchanged and cannot be modified while the file format will be modified during the verification procedure. The text's layout and margins must be alternated once the word is converted to PDF. After embedding the watermark, the MS Word file must be altered to PDF and hoarded or shared via the cloud.

DOI: https://doi.org/10.54216/JCIM.170203
Received: April 02, 2025 Revised: June 24, 2025 Accepted: August 13, 2025

The extraction method or watermark verification erases the watermark (secret data) in the watermarked file. The PDF files are inputs and changed to MS Word. Initially, the values were derived from specific properties, and anti-log was utilized for the real value retrieval. These provisional four variables are used for saving the value. Next, combined with variable "M". They automatically detect document margins and store them in the variables ($"T","B","L", and\ "R"$) variables. Anti-log retrieves the actual values and concatenates them into‘ "D". The variables "M" and "D" are concatenated, and then the outcome is created as a number. Furthermore, the no. of sequence should be altered from the Binary and then reversed to the character. The AES using 256 bit will be employed for encryption is employed for text decrypting. The Key is utilized for the message decryption that provides sensitive data i.e., hidden in the document.

B. CFO based Watermark Placement Approach

The hunting of crayfish, heat evading, and competition behaviours [19] stimulates CFO. To imitate the features of swarm intellect, the population of crayfish X is definite as the preliminary phase, X_i denotes ith crayfish location, which signifies the candidate solution $X_i = \{X_{i,1}, X_{i,2}, \cdots, X_{i,\mathrm{dim}}\}$, which gets the fitness value over the objective function $f(\cdot)$.The CFO must follow the below-mentioned heuristic instructions:

The CFO progress and exploration stage is guided by the temperature; if it becomes too high, the CFO goes into the behavior of competitive or heat evading; or else if it is appropriate, the CFO goes into the behavior of foraging;

In the behavior of summering, the population of crayfish upgrades the outcome by separate and burrow position;

During the behavior of foraging, food as the optimum outcome is attained by the existing and optimum value of fitness. CFO employs cosine and sine to pretend the crayfish food distribution behavior. Food consumption is completely defined by temperature.

Search Optimizer Strategy

(1) Initialization

The CFO is set with an arbitrary even distribution plan and the data method was mentioned below:

$$X_{i,j} = lb_j + \left(ub_j - lb_j\right) \times rand \tag{4}$$

Here, $X_{i,j}$ signifies the jth position data of the ith crayfish, $rand$ depicts an arbitrary number in $[0\ and\ 1]$ and lb_j and ub_jspecifies the lower and upper bounds of jth dimension, correspondingly.

(2) Describing temperature and food consumption

Temperature alterations influence behaviour of crayfish, which results in diverse activity phases. If it exceeds 30°C, they look for cooler locations, while optimal temperatures trigger foraging behavior. Crayfish nourishing is finest at 15^oC, 30^oC, and 25^oC. The CFO formulation is created below:

$$p = C_1 \times \left(\frac{1}{\sqrt{2\times\pi}\times\sigma} \times \exp\left(-\frac{(temp-\mu)^2}{2\sigma^2}\right)\right) \tag{5}$$

$$temp = rand \times 15 + 20 \tag{6}$$

Amongst them, crayfish consumption is almost generally dispersed, $temp$ signifies the temperature where the crayfish with stay, μ denotes the modified temperature, σ and C_1 are mostly employed to switch the consumption of crayfish at dissimilar temperatures.

(3) Summering behavior (exploration)

If the temperature is higher than 30^oC, This leads to crayfish adopting behavior of summering, with burrow positions is formulated below:

$$X_{shade} = \frac{X_G + X_L}{2} \tag{7}$$

Here, X_G and X_L signify an optimal solution for present iteration and population, respectively. The crayfish opposition fight has no burrow so they can openly arrive it for summering shown in Eq. (8):

$$X_{i,j}^{t+1} = X_{i,j}^{t} + C_2 \times rand \times \left(X_{shade} - X_{i,j}^{t}\right) \tag{8}$$

DOI: https://doi.org/10.54216/JCIM.170203
Received: April 02, 2025 Revised: June 24, 2025 Accepted: August 13, 2025

Whereas t and $t+1$ signifies the existing and subsequent iteration number, and C_2 is a condensed parameter:

If $Q \leq (C_3+1)/2$, the crayfish wants to transfer to the nutrition and consume promptly:

$$C_2 = 2 - \frac{t}{T} \tag{9}$$

Whereas, T symbolizes the highest iterations number. In the behavior of summering, the reason for the crayfish to tactic the cave like the method of optimum result and guarantee the CFO for quick convergence.

(4) Competitive behavior (exploration)

If the $temp > 30$ and $rand \geq 0.5$, other crayfishes are involved by struggling with others, they capture the opportunity to tactic an optimum solution that is accurately demonstrated below:

$$X_{i,j}^{t+1} = X_{i,j}^{t} - X_{z,j}^{t} + X_{shade} \tag{10}$$

Whereas z signifies a randomly generated crayfish, intended as:

$$z = round\big(rand \times (N-1)\big) + 1 \tag{11}$$

In this stage, crayfish contest with all to alter their place data by accidental crayfish locations. Employing the alteration process, the CFO exploration range upsurges and behavior is improved.

(5) Foraging behavior

If $temp \leq 30$, crayfish are appropriate to go searching. In this phase, after noticing the nutrition, the searching behavior process is definite by considering the food dimension. The X_{food} is normally definite as the optimum outcome X_G. The food size is definite as below:

$$Q = C_3 \times rand \times \left(\frac{fitness_j}{fitness_{food}}\right) \tag{12}$$

Where C_3 signifies the factor of food that signifies the biggest food and normally seizes the value of 3; $fitness_j$ and $fitness_{food}$ indicate adaptation value of the ith crayfish and position of the foods, correspondingly.

When $Q > (C_3+1)/2$, the nutrition is too big and the crayfish wants to utilize the 1st tore foot to split the nutrition, the calculation will be given:

$$X_{food} = \exp\left(-\frac{1}{Q}\right) \times X_{food} \tag{13}$$

Once the food is cut and made into small, the crayfish employs the 2nd and 3rd nails to take the food and consume it. To pretend the food range procedure, the CFO utilizes cosine and sine functions to pretend the procedure, the exact foraging model is as below:

$$X_{i,j}^{t+1} = X_{i,j}^{t} + X_{food} \times p \times \big(\cos(2 \times \pi \times rand) - \sin(2 \times \pi \times rand)\big) \tag{14}$$

$$X_{i,j}^{t+1} = \big(X_{i,j}^{t} - X_{food}\big) \times p + p \times rand \times X_{i,j}^{t} \tag{15}$$

During the phase of foraging, crayfish feed utilizing dissimilar feeding models dependent upon the size of food. If the dimension is appropriate for crayfish to consume, it will select to tactic the nutrition. Or else, if the food is too huge, crayfish are initially reduced into small pieces and consumed. Over the behavior of foraging, the CFO considers the best solution, growing the exploitation ability and hastening the performance of convergence. Fig. 2 indicates the CFO flowchart.

DOI: https://doi.org/10.54216/JCIM.170203
Received: April 02, 2025 Revised: June 24, 2025 Accepted: August 13, 2025

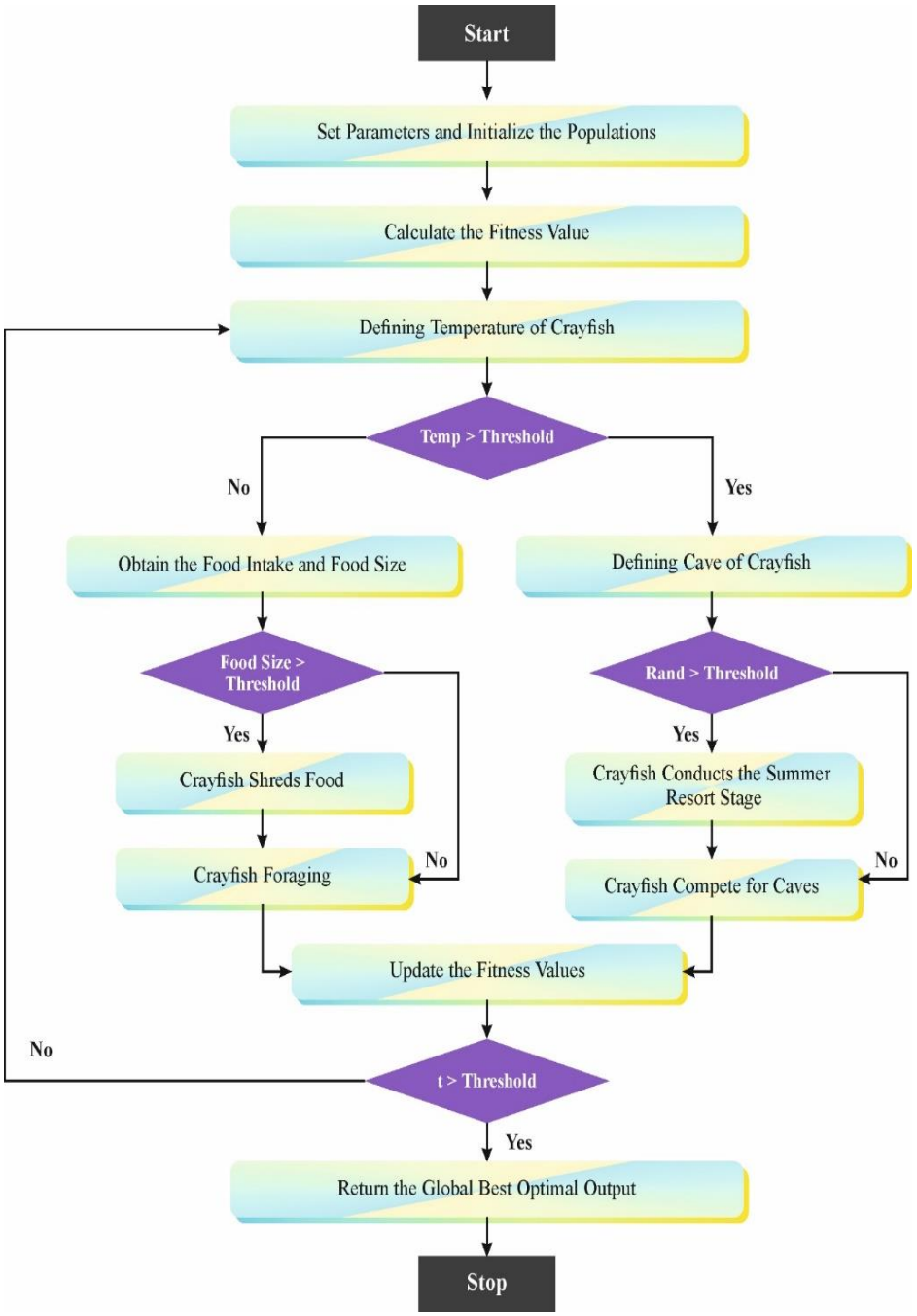

Figure 2. Flowchart of CFO technique

4. Result Analysis

The performance evaluation of the CFOWS-ATTD method is performed by utilizing four datasets [ELST, 2018], [ESST, 179], [EHMST, 559], and [EMST, 421] [20]. The given datasets encompass all English characters, spaces, numbers, and symbols. Table 1 and Fig. 3 represent an overall tampering detection accuracy (TDA) outcome of the CFOWS-ATTD method with varying attack volumes and types. The results depict that the CFOWS-ATTD approach gets enriched TDA values. With 5% attack volumes, the CFOWS-ATTD method attains a TDA of 95.23%, 92.06%, and 80.07% under insertion, deletion, and reorder attacks correspondingly. In addition, based on 5% attack volumes, the CFOWS-ATTD method gets TDA of 95.23%, 92.06%, and 80.07% on insertion, deletion, and reorder attacks respectively. Next, based on 5% attack volumes, the CFOWS-ATTD approach obtains a TDA of 95.23%, 92.06%, and 80.07% under insertion, deletion, and reorder attacks.

DOI: https://doi.org/10.54216/JCIM.170203
Received: April 02, 2025 Revised: June 24, 2025 Accepted: August 13, 2025

Table 1: TDA outcomes of CFOWS-ATTD method on varying attack volumes and types

Attack Volume (%)	*Insertion*	*Deletion*	*Reorder*
5	95.23	92.06	80.07
10	91.21	84.90	66.07
20	83.32	73.48	46.76
50	66.00	42.72	22.34

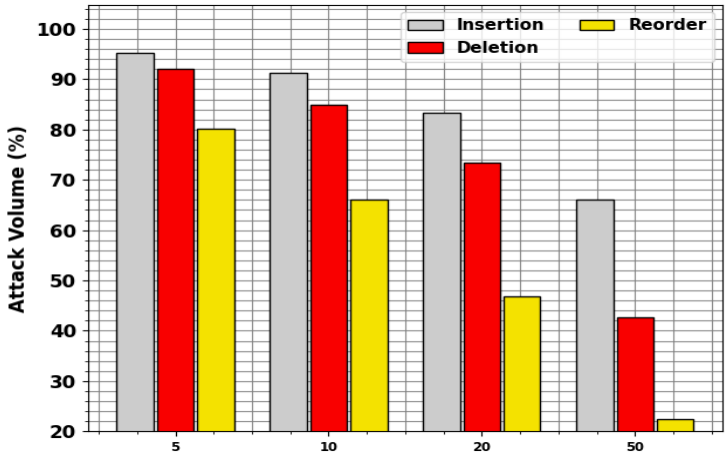

Figure 3. TDA analysis of CFOWS-ATTD model at different attack volumes and types

Table 2 and Fig. 4 depicts the comparative result of the CFOWS-ATTD method on four datasets [21,22]. The results highlighted that the CFOWS-ATTD technique accomplished better performance over other models on all datasets. The ZWAFWMMM and HNLPZWA models obtained worse results with the least TDA values. At the same time, the HTAZWA and COAW-CATD models accomplish to some extent increased TDA values. Nevertheless, the CFOWS-ATTD technique gains improved performance with a maximum TDA of 68.75%, 67.49%, 63.70%, and 60.25% under datasets 1, 2, 3, and 4, correspondingly.

Table 2: TDA outcomes of CFOWS-ATTD technique with recent approaches on four datasets

Tempering Detection Accuracy (%)	*ZWAFWMMM*	*HNLPZWA*	*HTAZWA*	*COAW − CATD*	*CFOWS − ATTD*
Dataset 1	68.75	66.23	70.00	73.49	75.16
Dataset 2	67.49	62.13	72.22	76.62	78.33
Dataset 3	63.70	53.93	65.89	73.80	75.55
Dataset 4	60.25	49.84	67.79	73.79	75.45

DOI: https://doi.org/10.54216/JCIM.170203
Received: April 02, 2025 Revised: June 24, 2025 Accepted: August 13, 2025

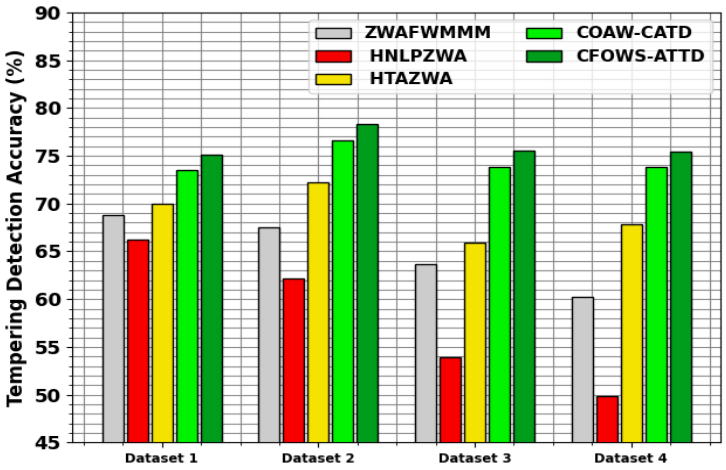

Figure 4. TDA analysis of CFOWS-ATTD technique on four databases

Table 3 and Fig. 5 examines the comparison outcome of the CFOWS-ATTD technique with distinct types of attacks. These experimentation outcomes highlighted that the CFOWS-ATTD method achieved better performance over other methods with distinct categories of attacks. This is noticed that the ZWAFWMMM and HNLPZWA methods obtained poorer outcomes with reduced TDA values. Concurrently, the HTAZWA and COAW-CATD methods have gained moderately improved TDA values. However, the CFOWS-ATTD technique provides increased performance with higher TDA of 91.44%, 83.46%, and 65.48% on insertion, deletion, and reorder, respectively.

Table 3: TDA outputs of CFOWS-ATTD method with existing approaches on distinct types of attacks

Tempering Detection Accuracy (%)	*ZWAFWMMM*	*HNLPZWA*	*HTAZWA*	*COAW − CATD*	*CFOWS − ATTD*
Insertion	78.15	69.27	80.02	89.64	91.44
Deletion	64.48	54.84	70.02	81.86	83.46
Reorder	44.10	34.12	50.40	63.72	65.48

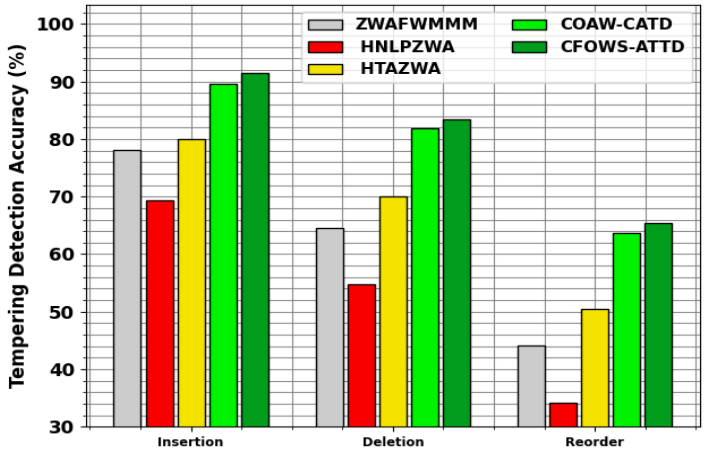

Figure 5. TDA result of CFOWS-ATTD model with existing approaches on distinct types of attacks

Table 4 and Fig. 6 demonstrate a comparative assessment of the CFOWS-ATTD technique on distinct attack volumes. These achieved findings pointed out that the CFOWS-ATTD approach accomplished greater performance over other methods under distinct attack volumes.

DOI: https://doi.org/10.54216/JCIM.170203
Received: April 02, 2025 Revised: June 24, 2025 Accepted: August 13, 2025

Table 4: TDA outcomes of CFOWS-ATTD model with existing techniques under distinct attack volumes

Varying attack volume	*ZWAFWMMM*	*HNLPZWA*	*HTAZWA*	*COAW − CATD*	*CFOWS − ATTD*
5	81.21	79.80	89.79	96.51	98.10
10	71.56	70.56	80.97	91.40	93.20
20	57.62	53.94	66.78	81.00	82.72
50	33.11	9.98	44.84	59.84	61.59

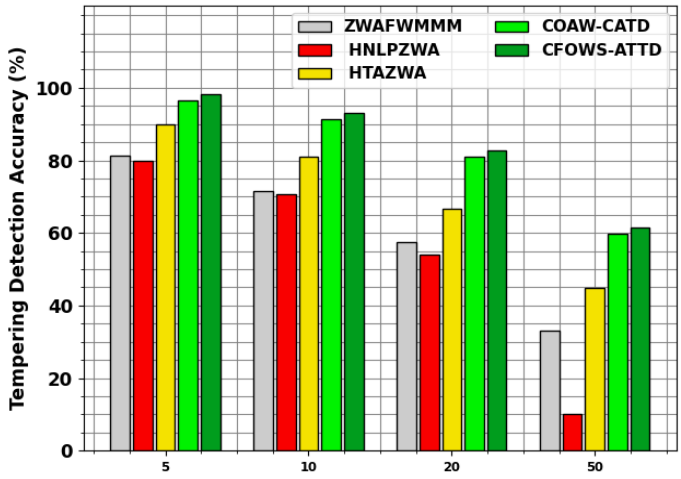

Figure 6. TDA outcomes of the CFOWS-ATTD method at various attack volumes

Next, the HTAZWA and COAW-CATD methods have achieved somewhat improved TDA values. However, the CFOWS-ATTD model gains excellent performance with increased TDA of 98.10%, 93.20%, 82.72%, and 61.59% under attack volumes 5, 10, 20, and 50, respectively.

Fig. 7 demonstrates the ROC curve of the CFOWS-ATTD approach under distinct labels. It provides a clear view of the trade-off between TPR/FPR across various thresholds and epochs. Results demonstrate robust classification performance of the CFOWS-ATTD approach across all classes, effectively handling complex tasks. These findings confirm that the CFOWS-ATTD model outperforms other models in TDA metrics.

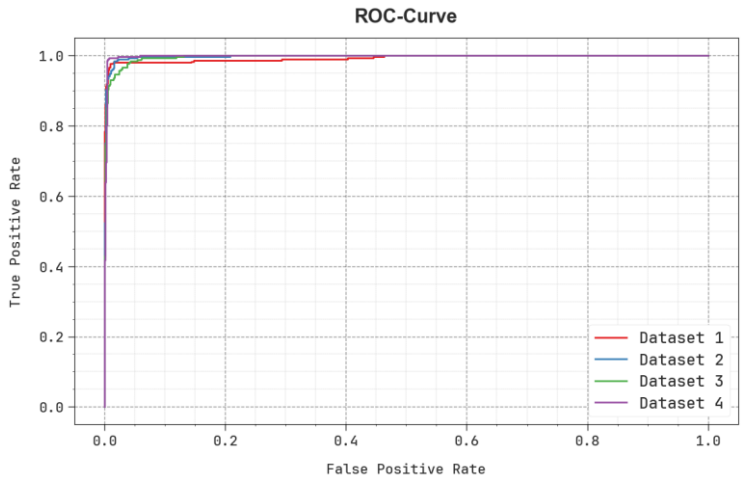

Figure 7. ROC curve of CFOWS-ATTD model

DOI: https://doi.org/10.54216/JCIM.170203
Received: April 02, 2025 Revised: June 24, 2025 Accepted: August 13, 2025

5. Conclusion

In this article, the CFOWS-ATTD technique is presented. In the CFOWS-ATTD technique, two-stage processes are involved. The CFOWS-ATTD technique generates a watermark from the text document and employs an extraction process to verify text authenticity. Moreover, the CFO approach is used for the optimal watermark placement to guarantee that it is robust and imperceptible to tampering. The experimentation of the CFOWS-ATTD approach is performed under the ELST, ESST, EHMST, and EMST datasets. The results implied that the CFOWS-ATTD approach obtains optimum performance over existing models.

Funding: This research received no external funding

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

References

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

[2] Y. Liu, Z. Wang, and H. Zhang, "Robust text watermarking based on semantic analysis and syntactic transformation," *IEEE Trans. Inf. Forensics Security*, vol. 16, pp. 4568-4582, 2021, doi: 10.1109/TIFS.2021.3107462.

[3] 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.

[4] 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.

[5] K. Chen, L. Wang, and X. Li, "A zero-watermarking scheme for Chinese text documents based on stroke modulation," *J. Inf. Secur. Appl.*, vol. 55, p. 102647, 2020, doi: 10.1016/j.jisa.2020.102647.

[6] 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 Gener. Comput. Syst.*, vol. 108, pp. 935-949, 2020.

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

[9] 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.

[10] Qu et al., "Towards robust tampered text detection in document image: New dataset and new solution," in *Proc. IEEE/CVF Conf. Comput. Vis. Pattern Recognit.*, 2023, pp. 5937-5946.

[11] M. A. Alohali et al., "Digital text document watermarking based tampering attack detection via Internet," *Comput. Syst. Sci. Eng.*, vol. 48, no. 3, 2024.

[12] M. Jana, B. Jana, and S. Joardar, "Local feature-based self-embedding fragile watermarking scheme for tampered detection and recovery utilizing AMBTC with fuzzy logic," *J. King Saud Univ.-Comput. Inf. Sci.*, vol. 34, no. 10, pp. 9822-9835, 2022.

[13] K. Sahu, M. Sahu, P. Patro, G. Sahu, and S. R. Nayak, "Dual image-based reversible fragile watermarking scheme for tamper detection and localization," *Pattern Anal. Appl.*, vol. 26, no. 2, pp. 571-590, 2023.

[14] Palani and A. Loganathan, "Semi-blind watermarking using convolutional attention-based turtle shell matrix for tamper detection and recovery of medical images," *Expert Syst. Appl.*, vol. 238, p. 121903, 2024.

[15] H. Shi, K. Yan, J. Geng, and Y. Ren, "A cross-embedding based medical image tamper detection and self-recovery watermarking scheme," *Multimedia Tools Appl.*, pp. 1-42, 2023.

[16] H. Rhayma, R. Ejbali, and H. Hamam, "Auto-authentication watermarking scheme based on CNN and perceptual hash function in the wavelet domain," *Multimedia Tools Appl.*, pp. 1-23, 2024.

[17] M. Alamgeer et al., "Smart-Fragile Authentication Scheme for Robust Detecting of Tampering Attacks on English Text, Comput" *Mater. Continua*, vol. 71, no. 2, 2022.

DOI: https://doi.org/10.54216/JCIM.170203
Received: April 02, 2025 Revised: June 24, 2025 Accepted: August 13, 2025

[18] S. Bhalerao, I. A. Ansari, and A. Kumar, "A reversible medical image watermarking for ROI tamper detection and recovery," *Circuits, Syst., Signal Process.*, vol. 42, no. 11, pp. 6701-6725, 2023.

[19] L. Ma, B. Xie, F. Liu, and L. Ma, "A Method of Applying Virtual Reality Converged Remote Platform Based on Crawfish Optimization Algorithm to Improve ESN Network," *EAI Endorsed Trans. Scalable Inf. Syst.*, vol. 11, no. 3, 2024.

[20] 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.

[21] N. Al-Wesabi et al., "Heuristic Optimization Algorithm Based Watermarking on Content Authentication and Tampering Detection for English Text," *IEEE Access*, 2023.

[22] M. Zhang, R. Yang, and W. Huang, "Digital document protection using optimized watermarking with tamper localization and recovery," *Multimedia Tools Appl.*, vol. 79, no. 35, pp. 25891-25912, 2020, doi: 10.1007/s11042-020-09176-w.

DOI: https://doi.org/10.54216/JCIM.170203
Received: April 02, 2025 Revised: June 24, 2025 Accepted: August 13, 2025