Multimedia Tools and Applications (2020) 79:341–354
https://doi.org/10.1007/s11042-019-08084-0

Enhancing fragility of zero-based text watermarking utilizing effective characters list

Tanzila Saba[1] · Morteza Bashardoost[2] · Hoshang Kolivand[3] · Mohd Shafry Mohd Rahim[2] · Amjad Rehman[4] · Muhammad Attique Khan[5]

Received: 28 December 2018 / Revised: 19 July 2019 / Accepted: 2 August 2019 /
Published online: 15 August 2019

Abstract

Text is an important medium used for sharing information worldwide. For a text document, digital watermarking is an efficient way for copyright protection, authentication, tamper proofing, to name but a few. In this paper, a zero-based watermarking approach is proposed for document authentication and tamper detection. To enhance the fragility of watermark, the proposed text watermarking approach can be comfortably utilized – based on the Effective Characters List (ECL) for watermark generation. The ECL method is generated for English text zero-watermarking by maintaining the contents of the original document and constructing the watermark by formulating the smooth transition between the selected characters in the documents. The evaluation of the proposed watermarking approach is based on three famous watermarking attacks including deletion, insertion, and reordering with an accuracy of 80.76%, 80.36%, and 88.1%, respectively. For a fair evaluation, a comparison is put forth with a recent zero-based watermarking method - clearly showing that the proposed method outperforms existing with greater accuracy.

Keywords Watermarking · Authentication · Tamper detection · Zero-based watermarking · Fragility · Effective characters list

✉ Amjad Rehman
rkamjad@gmail.com

Tanzila Saba
drtsaba@gmail.com

[1] College of Computer and Information Sciences, Prince Sultan University, Riyadh 11586, Saudi Arabia

[2] Media Centre, Institute of Human Centred, University Industry Research Laboratory (UIRL), Universiti Teknologi Malaysia UTM, Skudai, Johor, Malaysia

[3] Department of Computer Science, Liverpool John Moores University, Liverpool L3 3AF, UK

[4] College of Computer and Information Sciences, Imam Mohammad Ibn Saud Islamic University, Riyadh, Saudi Arabia

[5] Department of Computer Science and Engineering, HITEC University, Museum Road, Taxila, Pakistan

1 Introduction

Digital watermarking is an efficient technique utilized for copyright protection, authentication, tamper-proofing, etc. [3, 5, 20, 23]. When the digital watermarking is used for authentication purpose, it would be utilized to identify the original property from fake ones. The robust watermark is ineffective when the text watermarking method is used for authentication purpose [9, 29]. In fact, the opposite side of robustness, which is fragility, should be considered in the development of watermarking methods for authentication purposes [17].

Texts is an important medium that it is used widely to transfer information. Plain text is the main part of many kinds of information and most of the digital contents such as newspapers, books, and legal documents are in the form of text [21]. The malicious attackers are mostly active to modify these text documents and can lead to a fatal decision. The previous attempts on text watermarking can be categorized into four main classes include image-based approach, syntactic-based approach, semantic-based approach, and zero-based approach [20, 35]. Zero text watermarking techniques are content features dependent that is mostly used for authentication purposes [33]. The prominent idea of the zero-based watermarking system is to create the watermark based on some features of documents and store generated watermark in a safe place e.g. Certifying Authority (CA), instead of modifying contents and appearance of the original document [32]. A lot of techniques are introduced in the literature for copyright protection and tamper detection of text documents and some of them gives a very strong solution against crucial problems. The text watermarking methods such as formate, content, and image-based approach has many limitations for tempering detection. These methods are not suitable for all types of tampering attacks.

1.1 Motivation

The two primary reasons based on which the ECL method is adopted are a) fragility and b) watermark size. Both are, although, quite staunch to each other - when the size of watermark decreases, the fragility also decreases and vice versa. Therefore, a robust method is required which maintains the original contents and improve the performance.

1.2 Problem statement

In the digital watermarking, the general problems exist such as: a) robust sufficient to confront attacks while remaining indistinguishable by the human eye, b) the text document is visible for all persons whereas it should be visible only authorized person. These are the key security reasons and limitations for any watermarking approach. In this work, we consider the problem of digital contents which are changes after encryption, therefore through watermarking. We also consider the problem of the number of character selection for watermark generation. The increase in the character list decreased the overall system accuracy.

1.3 Contributions

In this paper, we propose a new zero-based watermarking approach for digital documents, which utilizes the Effective Characters List (ECL) to produce the watermark. Our major contributions are the following:

A new method is proposed for text watermarking through an Effective Characters List (ECL). The proposed ECL method is generated for English text zero-watermarking which maintains the contents of the original document and constructs the watermark by formulating the transition between the selected characters in the documents. Later, through Effectiveness Ratio (ER) determines how many characters are selected for the watermark generation. A group of characters is selected through ER value which referred to as ECL. Further, a 2-D Markov Matrix is utilized to examine the position of ECL members in the document.

2 Related work

The previous attempts towards text watermarking have been categorized by many kinds of literature based on the watermark embedding procedure [2, 3, 9]. There exists several zero text watermarking approaches that are utilized for document authentication and tamper detection [5, 6, 9, 27].

Bashardoost et al., [9] proposed replacement attack that focused to identify word's location in the documents. The proposed text watermarking attack is specifically effective on watermarking approaches that exploit words' transition in the document. Shubah et al. [25] introduced a discrete fractional Fourier transform approach for image watermarking. The original image is converted into frequency components and embedded a binary watermark using a quantization based method. Finally, watermark bits are extracted through adaptive thresholding method. The experiments are conducted on various standard images and achieve significant performance. Ahmed et al. [1] introduced a DCT and DWT based image watermarking approach which initially processed the original image into three respective channels such as red, green, and blue. The DWT and DCT are performed separately on each channel which later embedded through several numbers of color bands. The experimental process is performed on several images such as rotating, filtering, and a few more. The results reveal that the introduced method outperforms for linear and nonlinear attacks. Bin et al. [14] introduced a semi-fragile watermarking approach for image restoration and authentication. The introduced method outperforms to locate temper contents. Ferdinando et al. [13] implemented fuzzy relation equations for image watermarking tamper detection. The makes block-based comparisons and achieved better performance on the presented approach.

Fang et al. [12] introduced a self-embedding approach for watermarking in hierarchical reformation. From each image, the binary bits are obtained and individually interleaved. Later, the interleaved data is segmented into a number of blocks. Finally, the segmented data is combined through LSB layer for authentication. The results reveal that the presented method works well as compare to relative existing techniques. Nassaradin et al. [4] presented a watermarking approach for text protection from malicious attacks. They introduced an Unicode based approach and tested under different various attacks and showed improved capacity as compared to existing methods. Aditi et al. [34] introduced a multiple watermark algorithm for healthcare applications. They used DWT, DCT, and SVD features which are later improved through a neural network (NN). The NN removes the noise factors of the watermarked document and showed significant improvement. Al-wesabi et al. [7] proposed an English text zero-based watermarking algorithm that works based on probabilistic patterns. The authors also developed a content authentication zero-based watermarking method [16] based on word mechanism order one of Markov model. The zero-based concept employed for image watermarking [36]. Later, few zero-based methods [7, 18] were presented for Chinese text watermarking. Jalil et al. [19] developed a method that works based on the occurrence frequency of non-vowel ASCII characters and words. In another attempt [26], the authors used text constituents, double letters and the most frequently used words in English text to generate the zero-based watermark. The Genetic algorithm-based optimization is performed in this work. Mali, et al. [28] introduced an algorithm, which is based on English grammatical words besides a suitable encryption method. An English zero-based watermarking approach based on word mechanism order two of the Markov model is introduced by Vasantrao et al. [10]. Subsequently, Ghilan et al. [15] presented an intelligent zero-based text watermarking approach based on probabilistic patterns. In this approach, the letter-based Markov model of order three (LNMZW3) was constructed to generate the watermark based on the interrelationship of contents. Ba-Alwi et al. [8], also developed the ADV-LNMZW3 method, which is an extension for the LNMZW3 algorithm. A hybrid approach based on zero-watermarking and digital-signature-like manipulations were presented by Tayan et al. [31] for sensitive text documents in order to achieve content originality and integrity verification. Tayan et al. [30] suggested an adaptive zero-watermarking technique for authentication of highly-sensitive documents, such as Quran, which is based on a spread-spectrum approach that embeds one-watermark bit per set, with a parameterized set-size. One of the most prominent properties of zero-based text watermarking methods is fragility and watermark size. Halab et al. [22] described a semi-fragile watermarking approach through multiple features extraction. The cany edge detector is utilized for extraction of original samples the watermark is combined for more security improvement. Chaun et al. [24] presented a self-embedding watermarking approach which significantly handles the problem of tempering revival.

The existing zero-based watermarking approaches that are presented for authentication of documents are unable to improve both fragility and watermark size simultaneously. This means, either the generated watermarks are large in size, or the watermark is not fragile enough to detect and calculate the tampering attacks. Therefore, it is essential to propose new methods which can handle these listed problems.

3 ECL zero-based watermarking: Proposed methodology

The zero-based watermarking methods generate fragile watermarks based on the position of particular document elements. In fact, fragility is the main feature of watermarking algorithms that are used for authentication purpose. Besides fragility, the size of the generated watermark is the other important property of zero-based methods. Two essential properties of zero-based watermarking methods, which are fragility and watermark size contradict each other. It means when the watermark size decreases the fragility of the method also reduces and on the other side, by increasing the fragility of technique the size of generated watermark increases.

Therefore, we introduce an improved English text zero-watermarking technique based on the position of the most frequent characters of a document called ECL watermarking. The ECL watermarking algorithm maintains the contents of the original document and constructs the watermark by formulating the transition between the selected characters in the document. The generated watermark is stored in the Certifying Authority in order to prove the ingenuity of the document in the future. The main flow of the propose method is shown in Fig. 1.

Similar to other common watermarking algorithms, ECL watermarking method has also two separate phases that are watermark generation and watermark re-generation. The main purpose of the first phase is to generate the watermark for the original document and save it in an authentic place. Whereas, the aim of the second phase is to generate the watermark for the received document and check its originality.

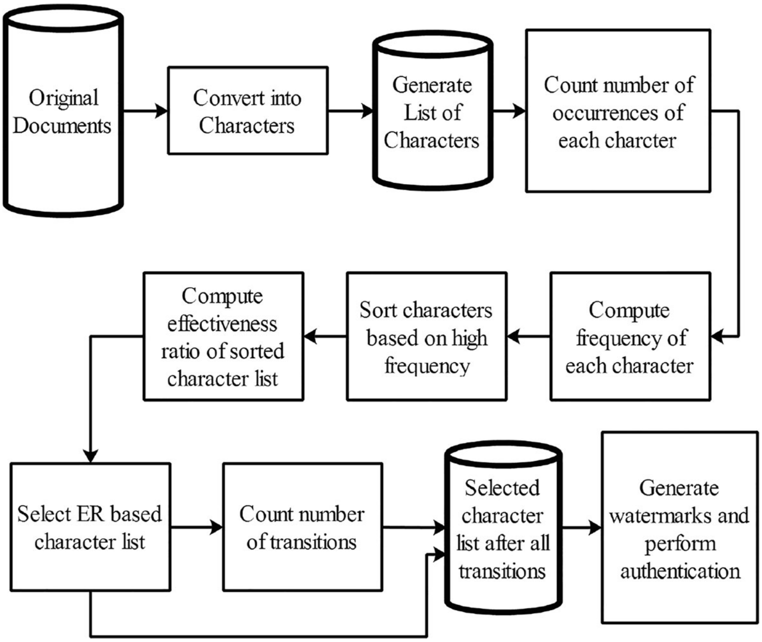
Original Documents
Convert into Characters
Generate List of Characters
Count number of occurrences of each charcter
Compute frequency of each character
Sort characters based on high frequency
Compute effectiveness ratio of sorted character list
Select ER based character list
Count number of transitions
Selected character list after all transitions
Generate watermarks and perform authentication

Fig. 1 Detailed flow of proposed watermarking generation system

3.1 Watermark generation algorithm

Characters are the smallest part of the text structure. The proposed method uses the characters of a document in the process of watermark generation. After converting all the characters to the small cases, the distinct list of all characters of the document is prepared. This list usually includes letters, digits, punctuations, special characters, or any other character that appeared in the document.

When the list of characters is created, the document is processed to count the number of occurrence for each character in the list. Subsequently, the list of characters is sorted in descending order based on the number of occurrences. It means the characters which appeared more frequently in the document, place on the top of the list.

Afterward, the Effectiveness Ratio (ER) determines how many characters should be selected for the watermark generation. The ER is calculated as follows:

$$\mathrm{ER} = \frac{\sum_{i=1}^{n} \mathrm{O}(\mathrm{c_i})}{\mathrm{Count}(\mathrm{Document\ Characters})} \tag{1}$$

Where the value of ER is between zero and one. The notation $\mathrm{O}(\mathrm{c_i})$ represents the number of occurrence of an i$^{\mathrm{th}}$ character in the sorted unique characters, n denotes the total number of characters. The higher values of ER lead to selecting more items from the top of the characters list. By determining the value of ER a group of characters is selected which is referred to as Effective Characters List (ECL). In fact, the effectiveness ratio specifies how many characters need to be in the ECL. ECL is a collection of characters that are selected from the top of sorted unique characters (UCs) and the total number of occurrence of these characters equals to ER percent of document's length. Mathematically, it is described as follows:

$$\mathrm{ECL} = \{\mathrm{c} \mid \mathrm{c} \in \mathrm{UC_s} \& \sum \mathrm{O(c)} = \mathrm{ER} \times \mathrm{Count(Nc)}\} \tag{2}$$

Where, *Nc* denotes total number of characters in the document, c denotes the subset of character list *C*. In order to investigate the relative position of ECL members in the document, a 2D array is utilized, which is called the Markov Matrix. The size of Markov matrix [11] is square and also known as stochaitic matrix. Equation (3) illustrates the Markov matrix:

$$\mathrm{M} = \left\{ \left| \begin{array}{ccccc} * & c_1 & c_2 & .. & c_n \\ c_1 & t_{11} & t_{12} & .. & t_{1n} \\ c_2 & t_{21} & t_{22} & .. & t_{2n} \\ .. & .. & .. & .. & \\ c_n & t_{n1} & t_{n2} & .. & t_{nn} \end{array} \right| \begin{bmatrix} P \\ P_1 \\ P_2 \\ . \\ P_n \end{bmatrix} \mid n = \mathrm{Size\ (ECL)} \right\} \tag{3}$$

Where, c_i refers to an element of ECL, t_{ij} denotes number of immediate appearance of c_j after ci in the document, * denotes the transition point, and P_i shows the transition pattern of each ECL element. The sum of each row in the given matrix is 1 and none of the ECL elements are negative. İts explains that all ECL elements are nonnegative.

The watermark is composed of three sections in the proposed ECL watermarking method. It starts with three digits that represent the ECL length, then followed by ECL members and has the concatenation of all transition patterns at the end. The formation of the generated watermark is illustrated in Eq. (4).

$$\mathrm{WM} = \mathrm{Concatenation(Padding(Size(ECL), 3), ECL, Concatenation(Pi))} \tag{4}$$

Where, WM denotes the generated watermarks which are obtained after concatenation of ECL size, ECL members, and a number of transition patterns (Pi). The entire process of watermark generation is also summarized in Algorithm 1.

Algorithm 1. Watermark Generation Algorithm

```
Step 1:Input: $\mathbf{I(x,y)} \leftarrow$ original documents
Step 2: Output: $\mathbf{WM(x,y)} \leftarrow$ Watermark generation
Step 3: For i ← 1: N
        - Remove the spaces and Control characters
        - Compute ER value through $ER = \frac{\sum_{i=1}^{n} O(c_i)}{Count(Nc)}$    // where Nc
          denotes total number of characters in the document
        - Create ECL as $\{c \mid c \in UC_s \& \sum O(c) = ER \times Count(Nc)\}$
Step 4:Generate a Markov matrix using ECL members by Eq. (3)
Step 5:Initiate matrix with zero values as $M \leftarrow zeros[]$
Step 6:FORj ← 1: M                                  // j is each element in ECL
        - Count the number of transition to every state
        - Store the value in Markov matrix
        END                              // Inner loop
Step 7:Generate the pattern based on transitions
Step 8:Construct the watermark base on the generated patterns and ECL
END                              // Outer loop
Step 9:$WM \leftarrow$ Watermarks              //Store the watermark
Step 10:$CA \leftarrow$Certifying Authority     //Document info in the CA
```

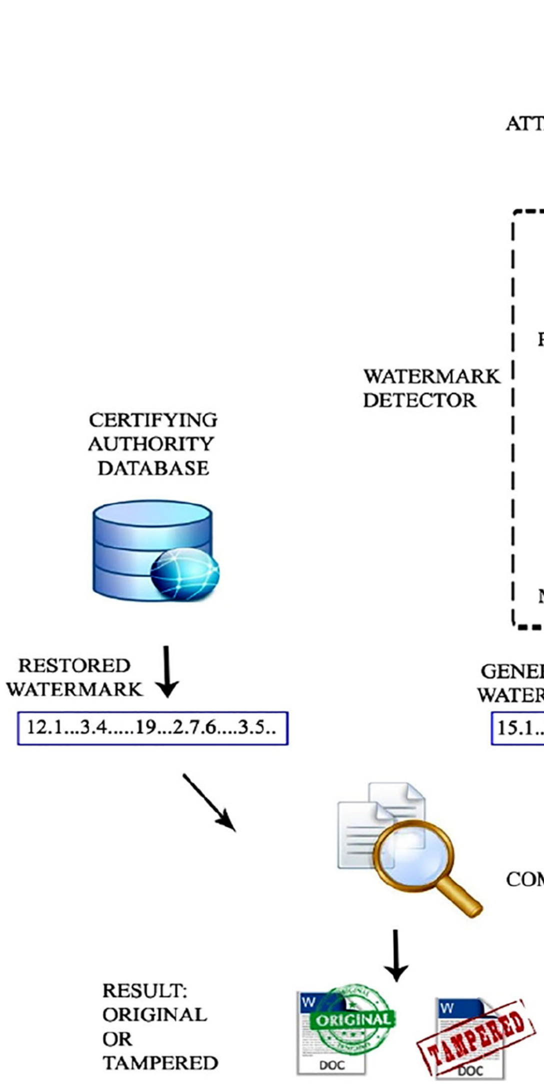

Fig. 2 Watermark regeneration process in ECL watermarking method

3.2 Watermark regeneration and tamper detection

In this phase, which is performing by certifying authority, the genuinely of a given document is examined. This process composed of two steps, which are watermark regeneration and tampering calculation. The first step determines the originality of a document, while the second step estimates the size of tampering attack.

In the first step, the received document is pre-processed and the ECL is produced. Then the Markov matrix is constructed to generate the transition patterns. Afterward, the watermark is produced in the same format that is explained for the original document. Finally, the document is marked as original, if the generated watermark and the retrieved watermark from CA are identical. Figure 2 illustrates the architecture diagram of this process:

The detection algorithm, which is the second step of this phase, computes the distortion rate and temperament percentage. The Pattern Matching Rate (PMR) shows the degree of similarity between the original and attacked watermark. The PMR itself is the average of all State Weights (SW). Moreover, each SW is measured by Eq. (5):

$$S_W(i) = \left| \frac{PMR_s(i) * \text{Transition Frequency}(i)}{\text{Total Number of transitions}} \right| \tag{5}$$

Where, PMR_S denotes the calculated Pattern Matching Rate for one state. The PMR_S and PMR_T are measured by Eq. (6) and (7). PMR_T refers to Pattern Matching Rate that is measured for a certain transition. Also, WMP_O and WMP_A represent the original and attacked watermarking pattern matrices.

$$PMR_S(i) = \left| \frac{\sum_{i=1}^{n} (PMR_T(i, j))}{\text{Total state pattern count}} \right| \tag{6}$$

$$PMR_T(i, j) = \left| \frac{WMP_O(i, j) - |(WMP_O(i, j) - WMP_A(i, j))|}{WMP_O(i, j)} \right| \tag{7}$$

4 Experimental results

The evaluation is performed in two different aspects such as tamper detection & calculation and watermark size. The documents that are used in the experiment are five variable size texts from the Reuters' corpus (volume 1) dataset. Small and large volumes of the most popular attacks of text watermarking, namely deletion, insertion and reordering are applied on the original documents for text alteration. Furthermore, the watermark is generated for the different value of the ER in order to investigate the balance between watermark-size and tamper detection accuracy.

4.1 Tamper detection and calculation

The first stage of text watermarking methods' evaluation is to check if the modification of the document can be detected. The watermark is generated base on a variable range of effectiveness ratio for each attacked document. All the generated watermarks are compared to correspondent original watermark for the purpose of checking the similarity of watermarks. The degree of similarity of original and tampered documents is presented as Pattern Matching Rate (PMR). The PMR always has a value between 0 and 1, where 0 is the minimum and 1 is the maximum degrees of similarity.

Table 1 Calculated PMR values for documents under 5% of attack

Doc. Name	Word Count	Attack Type	Effectiveness Ratio									
			0.10	0.20	0.30	0.40	0.50	0.60	0.70	0.80	0.90	1.00
[SST1]	179	Ins	0.000	0.889	0.824	0.841	0.862	0.711	0.889	0.907	0.920	0.943
		Del	0.000	0.946	0.957	0.963	0.939	0.960	0.955	0.946	0.956	0.962
		Ord	0.000	0.956	0.954	0.931	0.961	0.936	0.946	0.943	0.949	0.957
[SST2]	421	Ins	1.000	0.971	0.947	0.646	0.940	0.914	0.901	0.905	0.889	0.963
		Del	1.000	0.735	0.833	0.880	0.876	0.906	0.918	0.922	0.933	0.977
		Ord	1.000	0.902	0.909	0.932	0.951	0.958	0.940	0.926	0.921	0.974
[MST1]	469	Ins	1.000	0.965	0.963	0.920	0.924	0.915	0.916	0.818	0.895	0.954
		Del	0.750	0.941	0.896	0.930	0.927	0.937	0.939	0.940	0.944	0.977
		Ord	1.000	0.963	0.854	0.893	0.900	0.909	0.910	0.920	0.931	0.971
[MST2]	559	Ins	1.000	0.250	0.937	0.954	0.958	0.933	0.914	0.925	0.924	0.965
		Del	0.969	0.971	0.971	0.943	0.950	0.950	0.945	0.939	0.945	0.979
		Ord	1.000	0.979	0.837	0.889	0.933	0.939	0.936	0.930	0.932	0.975
[LST1]	2018	Ins	1.000	0.962	0.946	0.943	0.945	0.933	0.921	0.806	0.905	0.952
		Del	0.905	0.939	0.956	0.946	0.952	0.940	0.941	0.943	0.938	0.970
		Ord	0.968	0.959	0.857	0.866	0.893	0.916	0.916	0.915	0.909	0.960

4.1.1 Small-size attack

In this section, the accuracy of tamper detection is investigated for the documents, which have been modified by 5% of various attacks. The calculated PMR values for attacked documents with respect to different Ers, presented in Table 1. 10 different ER ratios are selected such as 0.10 to 1.00, where the 0.10 is an increment of each iteration. The results presented in Table 1 are computed on different Doc documents such as SST1, SST2, MST1, MST2, and LST1. Each document includes a number of words as 179, 421, 469, 559, and 2018. Three types of attacks are performed aginst each document and achieve average PMR rate is more than 92%. From Table 1, the volume of insertion attack is 5% and the desired PMR for this experiment is 0.95.

Table 2 Calculated PMR values for documents under 50% of attack

Doc. Name	Word Count	Attack Type	Effectiveness Ratio									
			0.10	0.20	0.30	0.40	0.50	0.60	0.70	0.80	0.90	1.00
[SST1]	179	Ins	0.500	0.450	0.436	0.319	0.455	0.351	0.377	0.432	0.526	0.800
		Del	0.000	0.896	0.288	0.305	0.475	0.465	0.532	0.568	0.646	0.750
		Ord	0.000	0.718	0.787	0.806	0.792	0.807	0.754	0.735	0.749	0.831
[SST2]	421	Ins	0.300	0.344	0.343	0.365	0.309	0.367	0.313	0.363	0.400	0.800
		Del	0.600	0.638	0.304	0.539	0.458	0.545	0.529	0.536	0.576	0.835
		Ord	0.600	0.591	0.770	0.780	0.813	0.825	0.771	0.742	0.776	0.907
[MST1]	469	Ins	0.000	0.181	0.164	0.283	0.212	0.356	0.369	0.317	0.382	0.805
		Del	0.500	0.796	0.748	0.691	0.480	0.523	0.525	0.516	0.584	0.810
		Ord	1.000	0.642	0.689	0.704	0.741	0.763	0.742	0.717	0.730	0.893
[MST2]	559	Ins	0.781	0.198	0.461	0.472	0.462	0.324	0.338	0.358	0.408	0.811
		Del	0.438	0.109	0.624	0.584	0.563	0.548	0.546	0.528	0.589	0.826
		Ord	0.906	0.685	0.758	0.786	0.821	0.834	0.776	0.772	0.754	0.895
[LST1]	2018	Ins	0.444	0.155	0.400	0.256	0.284	0.323	0.223	0.274	0.340	**0.802**
		Del	0.476	0.448	0.452	0.513	0.508	0.509	0.512	0.504	0.506	**0.817**
		Ord	0.841	0.859	0.814	0.790	0.812	0.843	0.807	0.817	0.785	**0.879**

Regarding the presented PMR values in Table 1, the volume of alteration is estimated precisely for the majority of generated watermarks. The best watermarks are generated when the ER equals 0.60 or more. The worst cases of tamper calculation occurred when the value of ER set to 0.1.

4.1.2 Large-size attack

In the second part of the tamper calculation review, the accuracy of attack measurement is inspected for the documents, which have been amended by 50% of insertion, deletion, and reordering attack. In the same style with the previous section, the cell with a dark background color in Table 2 represents a deficiency of method in document authentication. The results presented in Table 2 are calculated for different ER ratios for five documents. As the volume of attack is 50% in this experiment. Therefore, the anticipated PMR value is 0.5. By comparing the result of this experiment with the previous experiment, the tamper calculation accuracy is dramatically reduced. However, when the ER is set to a value between 0.5 and 0.9, the method provides a better estimation for the size of the attack. On the other hand, the tamper detection accuracy is rather unreliable once the Effectiveness Ratio equals to 0.1.

4.2 Watermark size

Watermark size is the other prominent properties of zero-based text watermarking techniques that refer to the length of the generated watermark for the original document. Indeed, any zero-based text watermarking method that provides a high level of tamper detection should be able to maintain a small size of the generated watermark. Table 3 illustrates the size of generated watermarks for the selected documents based on different values of Effectiveness Ratio. From Table 3, the size of the generated watermark is directly related to the value of the ER. The significant surge in the generated watermark size appears when the ER changes from 0.90 to 1.00. However, the watermark length increases steadily when the ER value soars from 0.10 to 0.90. Furthermore, checking the size of the watermark under an ER value verifies that the length of the generated watermark has a slight growth while the size of document increased. Moreover, we also compute the ER on a new large dataset which includes a total of 3484 documents. The number of words and characters counts is 305,442 and 477,210, respectively. The different values of ER show that watermark size is increased for ratio 0.90 to 1.0.

Table 3 Watermarks size based on different values of effectiveness ratio

Doc. Name	Word Count	Char. Count	Effectiveness Ratio									
			0.10	0.20	0.30	0.40	0.50	0.60	0.70	0.80	0.90	1.00
[SST1]	179	1023	4	22	37	53	105	167	236	364	510	1050
[SST2]	421	2589	6	13	46	71	99	167	247	334	586	2185
[MST1]	469	2712	5	25	40	61	120	197	287	426	766	2226
[MST2]	559	3378	6	13	43	69	134	208	297	450	800	2537
[LST1]	2018	12,897	6	17	52	78	115	203	300	549	924	3403
[Tobacco 3484] 34]	305,442	477,210	37	97	159	278	390	598	852	1304	2902	5126

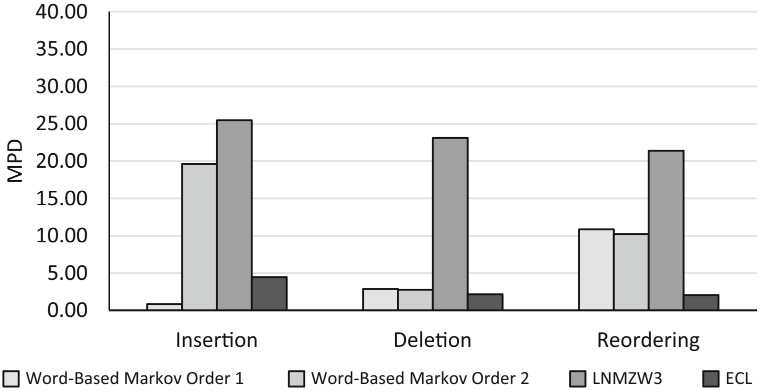

Fig. 3 Mean percentage of deviation(MPD) in tamper calculation for 5% of attack

Comparison and discussion In this section, the proposed ECL based watermarking method is compared with recent zero-based watermarking approaches [8, 10]. The evaluation is performed in two aspects as- tamper detection accuracy and watermark size.

4.2.1 Tamper detection accuracy

As the first part of the evaluation, the mean error of tampered detection accuracy for 5% and 50% of insertion, deletion, and reordering attacks is reviewed. Figure 3 illustrates the mean percentage of deviation in the estimation of attack size when 5% of insertion, deletion, and reordering attacks are applied to original documents. In order to consider the different size of ECL in the experiment, the average attack size for diversity values of ER is referred to as estimated attack size in the proposed ECL method.

The evaluation results show that the proposed watermarking approach provides the minimum tamper calculation error for deletion and reordering attacks. However, the word-based Markov order 1 method offers the best precision of attack size, when the documents are modified by 5% of insertion attack. Nevertheless, the ECL method can measure the volume of insertion attack better than word-based Markov order 2 and LNMZW3 approaches [8]. In another tamper detection evaluation scenario, the documents are altered by 50% of common text watermarking attacks. Figure 4 demonstrates the percentage of error in detecting the size of the attack by the above-mentioned approaches.

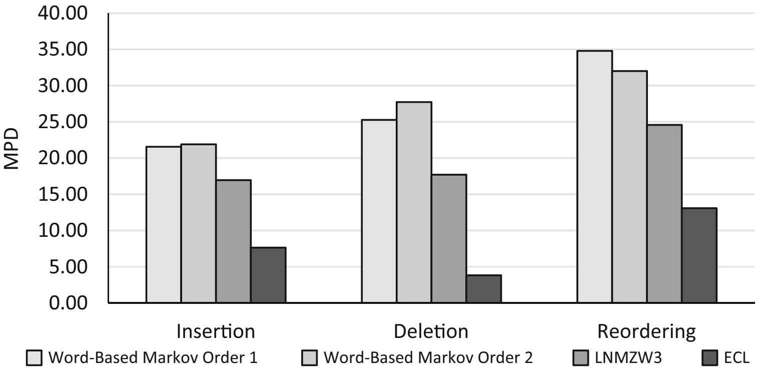

Fig. 4 Mean percentage of deviation(MPD) in tamper calculation for 50% of attack

The overall comparison of tested methods for 50% of attacks proves that the ECL method identifies the attack volume more accurately. Although, the word-based methods perform accurate tamper calculation for the small size of attacks when the size of the attack increases the provided estimation are hardly accurate.

4.2.2 Watermark size

As the second part of the evaluation plan, the length of generated watermarks by using selected methods is analyzed. Table 4 represents the length of the generated watermark for five original documents such as SST1, SST2, MST1, MST2, and LST1. The ECL method's generated watermark sizes as shown when ER is set to 90%, 100%, and the average size of all tested ERs. Based on the provided information in Table 4, the length of the generated watermarks is smaller than the size of the original documents in all methods except LNMZW3. In [7], the generated watermarks for SST1, SST2, MST1, MST2, and LST1 are 327, 765, 899, 1065, 3731, respectively. The size of generated watermarks in the LNMZW3 [8] method is high as compare to word-based methods. The size of generated watermarks in the word-based methods is dependent on the size of the documents and the length of generated watermarks by word base methods is about one-third of the original documents' length. In the proposed ECL method generates small sizes of the watermark when the ER is set to 90% or below. The drawback of the ECL method is when the effectiveness ratio equals 100% where the size of the watermark is comparatively larger than word-based methods. Nevertheless, the ECL method (with ER = 100%) generates smaller watermarks for the large document when it is compared with word-based methods. Additionally, the trend of increasing watermark sizes in ECL method is very slower than word-based methods.

In addition, the comparison with existing techniques is conducted in Table 5. In Table 5, the comparison is conducted through different parameters such as insertion, deletion, and reordering. In addition, the comparison is also conducted based on the average performance. The comparison results described that the proposed technique outperforms as compared to existing one's.

5 Conclusion and future work

In this article, we propose a zero-text watermarking algorithm to ensure the fragility and watermark size. A group of most frequency characters in the document is selected for watermark generation in order to reduce the size of generated watermark while maintaining the fragility of the watermark. The effective characters list (ECL) is exploited to reduce the size

Table 4 Size of generated watermark in evaluated methods

Method	[SST1]	[SST2]	[MST1]	[MST2]	[LST1]
Word-Based Markov Order 1[22]	327	765	899	1065	3731
Word-Based Markov Order 2[30]	349	827	929	1099	4057
LNMZW3 [8]	1458	3078	3665	4095	10,612
ECL (Average all ER)	254	375	415	455	530
ECL (ER = 0.9)	510	586	766	800	829
ECL (ER = 1.0)	1050	2185	2226	2537	3228

Table 5 Comparison with existing techniques

Method	Year	Average Accuracy
[8]	2014	70.34%
[10]	2017	62.068% (Under 10% of attacks) 87.02% (Under 1% of attacks)
Proposed	2018	80.36% (Insertion under 50% of attacks) 80.76% (Deletion under 50% of attacks) 88.1% (Reordering under 50% of attacks)

of the generated watermark. Performance of the proposed ECL watermarking approach is evaluated by applying three types of random dispersed attacks, namely deletion, insertion, and reordering. From results, we conclude that the proposed method significantly reduces the number of generated watermarks. We also conclude that the proposed algorithm always detects any modification size in the tested documents when the effectiveness ratio (ER) is greater than 0.1. On 0.1, not significant performance is achieved. In addition, the ECL method provides the best precision of tampering detection in the majority of test cases. Also, the generated watermarks by the ECL method are the smallest watermarks among the tested approaches.

This method is a few limitations such as: a) it is less accurate to calculate the size of advance replacement attacks compare to the normal replacement attacks. In future work, we will consider this limitation. Moreover, in the future, the fragility of the ECL watermarking approach need to be examined under advanced types of possible attacks.

Acknowledgements “This work is the output of the collaboration of Department of Computer Science, Liverpool John Moores University, Liverpool, UK , University Industry Research Laboratory (UIRL), Universiti Teknologi Malaysia UTM, Skudai, Johor, Malaysia This work was also collaborated, supported by Artificial Intelligence and Data Analytics (AIDA) Lab Prince Sultan University Riyadh Saudi Arabia. Authors are thankful for the support”.

References

1. Abdulrahman AK, Ozturk S (2019) A novel hybrid DCT and DWT based robust watermarking algorithm for color images. Multimed Tools Appl 78(12):17027–17049
2. Ahmad AM et al (2014) Data hiding based on improved exploiting modification direction method and Huffman coding. J Intell Syst 23(4):451–459
3. Alkawaz MH et al (2016) Concise analysis of current text automation and watermarking approaches. Sec Commun Netw 9(18):6365–6378
4. Al-maweri NAS et al. (2016) Robust digital text watermarking algorithm based on Unicode extended characters. Indian J Sci Technol 9(48)
5. Alotaibi RA, Elrefaei LA (2018) Improved capacity Arabic text watermarking methods based on open word space. J King Saud Univ-Comput Inform Sci 30(2):236–248
6. Alotaibi RA, Elrefaei LA (2018) Text-image watermarking based on integer wavelet transform (IWT) and discrete cosine transform (DCT). Applied Computing and Informatics
7. Al-Wesabi FN, Alshakaf AZ, Vasantrao KU (2012) A zero text watermarking algorithm based on the probabilistic weights for content authentication of text documents. In Proceedings on National Conference on Recent Trends in Computing NCRTC. Citeseer
8. Ba-Alwi FM, Ghilan MM, Al-Wesabi FN (2014) Content authentication of English text via internet using zero watermarking technique and Markov model. Int J Appl Inform Syst (IJAIS) 7(1):25–36

9. Bashardoost M, Rahim MSM, Saba T, Rehman A (2017) Replacement attack: a new zero text watermarking attack, 3D Res , vol. 8(8). doi:https://doi.org/10.1007/s13319-017-0118-y
10. Bashardoost M et al (2017) Replacement attack: a new zero text watermarking attack. 3D Res 8(1):8
11. Blackwell D (1953) Equivalent comparisons of experiments. Ann Math Stat: 265–272
12. Cao F et al (2017) Hierarchical recovery for tampered images based on watermark self-embedding. Displays 46:52–60
13. Di Martino F, Sessa S (2019) Fragile watermarking tamper detection via bilinear fuzzy relation equations. J Ambient Intell Humaniz Comput 10(5):2041–2061
14. Feng B et al. (2019) A novel semi-fragile digital watermarking scheme for scrambled image authentication and restoration. Mobile Networks and Applications: 1–13
15. Ghilan MM, Ba-Alwi FM, Al-Wesabi FN (2014) Combined Markov model and zero watermarking techniques to enhance content authentication of english text documents. Int J Comput Ling Res 5(1):26–42
16. Gutub AA-A, Al-Alwani W, Mahfoodh AB (2010) Improved method of Arabic text steganography using the extension 'Kashida'character. Bahria Univ J Inform Commun Technol 3(1):68–72
17. Hemida O et al. (2018) A restorable fragile watermarking scheme with superior localization for both natural and text images. Multimed Tools Appl: 1–31
18. Husain A (2015) Printed document forgery detection using text reordering and mixing of matrices in zero watermarking, Universiti Teknologi Malaysia
19. Jalil Z et al (2010) Improved zero text watermarking algorithm against meaning preserving attacks. World Acad Sci Eng Technol 46:592–596
20. Kamaruddin NS et al (2018) A review of text watermarking: theory, methods, and applications. IEEE Access 6:8011–8028
21. Krishna GJ, Vadlamani R, Bhattu SN (2018) Key generation for plain text in stream cipher via bi-objective evolutionary computing. Appl Soft Comput
22. Patel HA, Divecha NH (2018) A feature-based semi-fragile watermarking algorithm for digital color image authentication using hybrid transform, Advances in computer and computational sciences, Springer: 455–465
23. Pramoun T, Amornraksa T (2009) Improved image watermarking using pixel averaging and unbiased retrieval. In 2009 9th International Symposium on Communications and Information Technology. IEEE
24. Qin C et al (2018) Non-uniform watermark sharing based on optimal iterative BTC for image tampering recovery. IEEE MultiMedia 25(3):36–48
25. Saxena S et al. (2019) Robust digital image watermarking Scheme based on discrete fractional fourier transform. In AIP Conference Proceedings. AIP Publishing
26. Singh M, Saxena A (2017) Image watermarking using discrete cosine transform [DCT] and genetic algorithm [GA]
27. Sinha S et al (2018) Authentication and tamper detection in tele-medicine using zero watermarking. Procedia Comput Sci 132:557–562
28. Taleby Ahvanooey M et al. (2018) A comparative analysis of information hiding techniques for copyright protection of text documents. Security and Communication Networks 2018
29. Tan L et al. (2018) Print-scan invariant text image watermarking for hardcopy document authentication. Multimed Tools Appl: 1–23
30. Tayan O, Alginahi YM, Kabir MN (2013) An adaptive zero-watermarking approach for text documents protection. In International Conference on Advances in Computer and Information Technology
31. Tayan O, Kabir MN, Alginahi YM (2014) A hybrid digital-signature and zero-watermarking approach for authentication and protection of sensitive electronic documents. Sci World J 2014
32. Walke A et al (2018) Enhanced password processing scheme using visual cryptography and steganography. Int J Recent Innovation Trends Comput Commun 6(4):35–37
33. Wang C et al (2019) Ternary radial harmonic Fourier moments based robust stereo image zero-watermarking algorithm. Inf Sci 470:109–120
34. Zear A, Singh AK, Kumar P (2018) A proposed secure multiple watermarking technique based on DWT, DCT and SVD for application in medicine. Multimed Tools Appl 77(4):4863–4882
35. Zheng W et al. (2018) Robust and high capacity watermarking for image based on DWT-SVD and CNN. In 2018 13th IEEE Conference on Industrial Electronics and Applications (ICIEA), IEEE
36. Zhenjiu X et al (2017) Zero-watermarking based on boost normed singular value decomposition and cellular neural network. J Image Graph 3:002

Publisher's note Springer Nature remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.