International Journal of Hybrid Information Technology
Vol.11, No.3 (2018), pp.13-22
http://dx.doi.org/10.21742/ijhit.2018.11.3.03

A Tamper Proofing Text Watermarking Shift Algorithm for Copyright Protection

A. Eid[1], A. Emran[2], and A. Yahya[3]

[1]Department of Computer and Electrical Engineering, Higher Technological Institute, 10th of Ramadan City, Al-sharkia, Egypt
[2,3]Department of Electrical Engineering, Al-Azhar University, Nasr City, Cairo-11371, Egypt
amira.eid@hti.edu.eg

Abstract

Watermarking has proved its great reliability and flexibility for data protection and tamper detection. Among the different media in which watermarking technology is used, text watermarking represents the most challenging issue due to the different nature of various formats. Plain text is widely used for transferring information on the internet. There is a lack of used plain text watermarking techniques, so obviously it's necessary to focus on that point. In this paper, a novel text watermarking approach is proposed for copyright protection and tamper detection of plain text by inter-word spacing (depending on a secret key) and text fingerprint. This approach is a combination of several steps which work cooperatively. Simulation results manifest a promising performance accomplished by our approach in authentication and tampering detection fields.

Keywords: *Text watermarking, Copyright protection, Tamper detection, Authentication, Hash function, Word shift, Plain text*

1. Introduction

In the era of the enormous proliferation of information technology, the role of the Internet is reflected in providing multimedia resources and exchanging various forms of data such as audio, video, image and text. Sharing this massive amount of information on the Internet makes them more susceptible to illegal use such as forgery, manipulation, counterfeiting and fraud. So protecting the distributed digital content from malicious users acquires the attention of researchers.

Cryptography is one of the most effective sciences that offer a solution to immunize transmitted data. Unfortunately, its role is limited to protection only during the transmission process, once decryption is performed, the information becomes vulnerable to attack [1] and this isn't appropriate to protect information circulating through the giant network.

To provide the required protection, digital watermarking is used. It is based on the insertion of a certain watermark which might be a text or an image in the intended digital data (host medium) that could have various forms (text, video, audio, image). When the watermarked data is distributed or sent to a specified destination, the watermark remains within its host medium

Article history:
Received (February 26, 2018), Review Result (March 30, 2018), Accepted (April 19, 2018)

Print ISSN: 1738-9968 eISSN: 2652-2233 IJHIT

and doesn’t block access to the watermarked data or prevent to get benefit from it. So it’s obvious that digital watermarking is exploited by the original owner of distributed content to be a strong indication of the host medium manipulation. Therefore, watermarking is widely applied in multiple mediums for ownership verification, data authentication and fingerprinting.

In this paper, we propose a novel plain text watermarking approach that provides both copyright protection and tamper detection.

The rest of the paper is organized as follows: Section 2 contains an overview of text watermarking. The proposed approach is presented in section 3. In section 4 the simulation results are provided. Later, the paper is concluded in the last section.

2. Text watermarking overview

The general watermarking concept which involves three phases is shown in [figure1].

Watermark generating and embedding which can be achieved by numerous algorithms, potential attack where the attacker delete, add or alter the digital content and there is also a possibility of trying to destroy the watermark and then comes the last step that known as watermark detection, where the watermark is extracted from the data and compared to the original one to clarify any intentional or accidental attack. The extracted watermark is also used to resolve any dispute on data ownership [2].

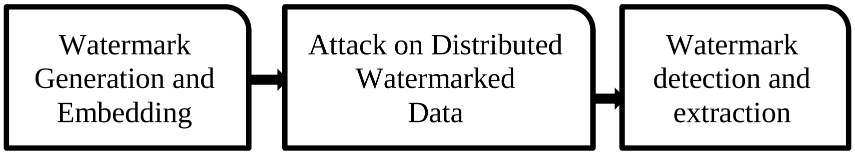

Watermark Generation and Embedding
Attack on Distributed Watermarked Data
Watermark detection and extraction

Figure 1. Watermarking Phases

To reach the desired goals of watermarking implementation, the watermark could be characterized by the following essential features:

Robustness: The host medium is still detectable, although several forms of attack were applied on it and this is appropriate for ownership protection.

Imperceptibility: The original host data and the watermarked data can’t be distinguished.

Security: Keeping the watermark protected from illegal detection, such attribute is accomplished using cryptographic keys.

Capacity: The watermark should have a satisfactory amount of information.

Trade-offs between these requirements are based on the application requirements.

Researchers have categorized watermarking according to the host medium into four classes: audio watermarking, video watermarking, image watermarking and text watermarking.

The online extensive dissemination of textual documents as a basic means of sending and sharing information makes them more prone to misuse and illegal exploitation by malicious users. Because of the dominance of plain text on the routes of daily communications between individuals, institutions and even governments, it became necessary to give greater priority to text watermarking as a promising solution to the challenges facing published text. Text watermarking has enabled publishers to track, secure, authenticate and verify ownership of their distributed text.

For the last decade most research teams have drawn their attention to audio, video and image domains which have analogous techniques and concepts that are inappropriate to be utilized for the text. Text watermarking procedures are completely dissimilar to the aforementioned medium's techniques [3]. Audio, video and image have sufficient redundancy exploited to embed the watermark so imperceptibility is accomplished. Such redundancy should be excavated within text documents to conceal the watermark. For setting up an algorithm for text watermarking, we can make good use of multiple features in text such as text format, word frequency, letter count, word synonym and acronym, style, grammar, text structure, etc. [4].

Text watermarking is a remarkable research spot that could provide new solutions for security problems threatening text entity such as all possible kinds of text manipulation like deletion, addition, forgery and alteration, also text document property counterfeiting. These problems lead to serious situations, especially if the text contains important and sensitive information and expose the data owner to a critical issue.

Text watermarking could be exploited in two major applications: ownership verification and text authentication. Ownership verification or so-called copyright protection is executed by using a robust watermark which prepared to resist any kind of attack trying to destroy or delete the watermark. Text authentication or tamper detection can be accomplished using a fragile watermark that is designed for detecting even tenuous changes in the watermarked document [3].

Diverse techniques are innovated for watermarking text and could be sorted based on watermark nature or the type of text and how to deal with it.

Depending on embedding mode, the most common techniques are split into four classes:

(1) Image-based approach, The text document is used as an image in which there are three levels for the watermark to be embedded, character [6][7][8], stroke feature [9][10][11][12] and pixel levels [5][13]. The image-based method isn’t appropriate for various cases as in text messages or blogs and isn’t robust to attacks.

(2) Natural language method the watermark is inserted using semantic processing [14][15][16][17], syntactic transformations or synonym permutation[18],[19].This approach provides a high level of robustness but depends on language and not suitable for unchangeable text content such as official documents and poetry.

(3) Structured-dependent algorithms differ from other techniques as no alterations in the original document take place to perform watermarking process, rather the text structure is used to extrapolate the watermark. Jalil et al. presented multiple algorithms for ownership verification and content authentication of plain text documents [6][20][21][22][23][24]. Approaches that use the Markov model (chain) are offered in [25][26]. These algorithms couldn’t succeed with all sorts of text, whilst it’s limited to alphabetical documents, namely, it’s not suitable for financial or mathematical documents.

(4) Format-dependent watermarking which focuses on spacing, text style and text layout. watermarks concerning to spaces have already been mentioned in image-dependent watermarks but the pivotal difference here that the text isn’t treated as an image and this is more suitable and practical for text in all respects. Fura and Liu [27] proposed a copyright protection scheme based on word shift and a secret key, Levenshtein distance specifies where to embed watermark bits. This one can’t resist all kinds of attacks. Researchers suggested [28],[29] and [30] for Arabic text, the first employs kashida as a watermark cover,the second benefitted from dotted and un-pointed letters to insert a pseudo space in words according to a key and the third is related to the anterior but applying different spaces, these algorithms can’t be applied on all languages text.

3. Proposed algorithm

Ensuring the integrity of electronic content, especially online messages, widespread scientific articles and vital documents has occupied an utmost solicitude. The plain text represents a large proportion of web scripts, therefore our approach is associated with plain text.

The majority of used text watermarking techniques employ only one watermarking algorithm to achieve one of these goals, authentication, copyright protection, or tamper detection. For more strength in facing malicious users, our approach combines two procedures to attain both copyright protection and tamper detection. First of all, we get the hash value of the raw text, then the most occurring word in the plain text is obtained which in turn is used as a keyword (KW) in the second step where this KW is shifted according to a secret key, then the whole text is hashed using MD5 function. When there is doubt or dispute concerned with the text, the watermark is extracted.

Before embarking on watermarking phases including insertion and extraction procedures, we first provide a brief description of the MD5 function.

3.1. MD5 hash function

Hashing is a mathematical operation that transmutes a message having any length to a fixed length string which is called a hash value. Message digest (MD5) is a sort of these functions. The exemplary lineaments of a hash function:

The generated hash has a fixed length regardless of input message length.

Each message has a unique invariable hash value.

Ease of computation.

Irreversible “original message can’t be obtained from its hash value”.

Any slight change in the message changes its hash value.

Hashing is used as a fingerprint for message authentication, integrity check and detecting manipulation.

Generally, the watermarking process has two main phases:

3.2. Watermark embedding

The watermark (WM) insertion into the text to be watermarked using an embedding algorithm. This is illustrated in figure 2. The hash value of Original Text (OT) is obtained (HV1) using the MD5 hash function, afterward, the Most Occurring Word (MOW) in the text is obtained in addition to the Number of Occurrences (NOO). A binary number Secret Key (SK) is generated which in turn enhances watermark security, taking into account that Number of Bits(NOB) equals NOO. Considering the MOW to be a keyword (KW), then compare each KW with the corresponding binary digit in the secret key. For digit “1” shifts the KW to left and for the digit “0” leaves the KW unchanged. Thus a Watermarked Document (WD1) is produced. Thereafter, get the message digest of the marked text (HV2).

During the embedding process, calculating HV1 ensures detection of any defect in the text's basic content, besides obtaining HV2 to clarify intruders’ attempts to destroy the watermark.

The MOW, SK, HV1 and HV2 are registered at a Certifying Authority (CA) as a reliable institution that is resorted at any dispute.

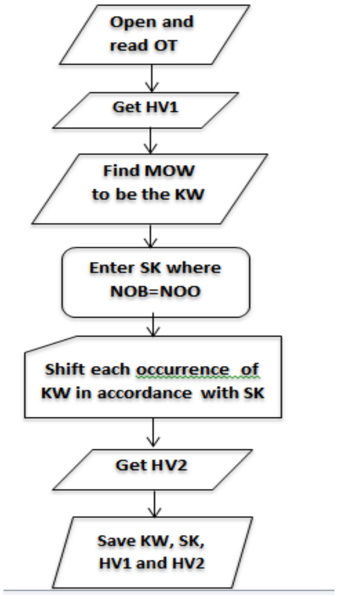


Figure 2. Embedding process sequences

3.3. Watermark extraction

A step implemented by the original owner to verify the authenticity of published Watermarked Documents (WD2) and to detect any possible attack. The watermark is also extracted from watermarked text to prove ownership through the supervision of the certifying authority.

In our method as a first step WM is eliminated to get the raw text (UT), then its hash value is obtained (HV1_E) which in turn is compared to HV1. The second action is to obtain the hash value of watermarked content (HV2_E) and the extracted secret key (SK_E). The matching ratio between the extracted watermark and the original one indicates whether there is manipulation and defines its location. The extraction process is minutely elucidated in figure 3.

4. Simulation results and scheme evaluation

Simulation experiments were performed on multiple English text documents with different lengths (short text ST, medium text MT and long text LT) and proved its efficiency in revealing all kinds of attacks threatening text documents.

The approach has been evaluated through watermark transparency, tamper detection ability and robustness availability points of view.

4.1. Watermark transparency

[Figures (4-1)] and [Figure (4-2)] illustrates an original text sample and its marked version beside the hash value of each one. The human eye can hardly observe the two versions differences because the horizontal spacing is only executed in case when a binary one is available in SK. Showing the watermarked content to a group of observers, the results illustrate a good level of imperceptibility.

4.2. Tamper detection ability

Exposing the three referred different lengths texts to various forms of attacks with different volumes. Deleting or adding some words or phrases to text structure, text reordering and word replacement attacks are applied at random positions with 10%, 20%

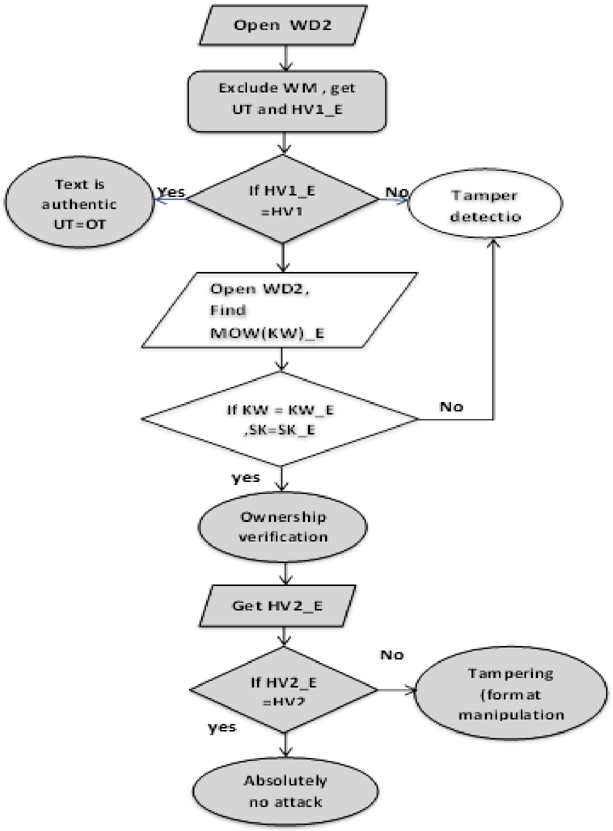
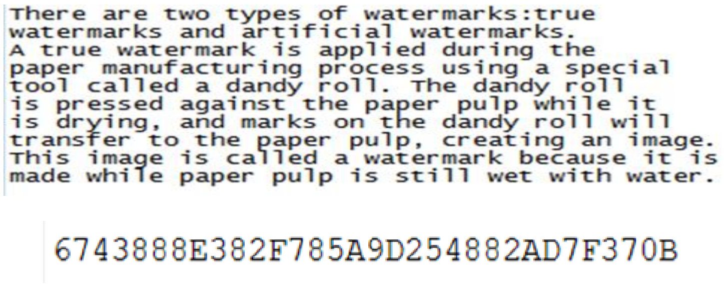
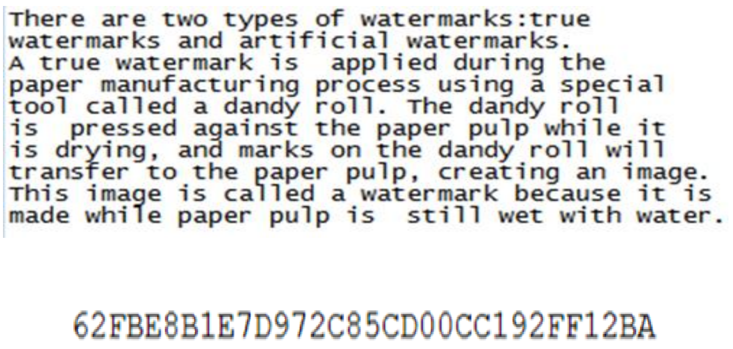


Figure 3. Workflow for extraction process


```
There are two types of watermarks:true
watermarks and artificial watermarks.
A true watermark is applied during the
paper manufacturing process using a special
tool called a dandy roll. The dandy roll
is pressed against the paper pulp while it
is drying, and marks on the dandy roll will
transfer to the paper pulp, creating an image.
This image is called a watermark because it is
made while paper pulp is still wet with water.
```

```
6743888E382F785A9D254882AD7F370B
```

Figure 4-1. Original text sample and its md5 digest, the kw is “is” which repeats 6 times in this text sample



```
There are two types of watermarks:true
watermarks and artificial watermarks.
A true watermark is  applied during the
paper manufacturing process using a special
tool called a dandy roll. The dandy roll
is  pressed against the paper pulp while it
is drying, and marks on the dandy roll will
transfer to the paper pulp, creating an image.
This image is called a watermark because it is
made while paper pulp is  still wet with water.
```

62FBE8B1E7D972C85CD00CC192FF12BA

Figure 4-2. The watermarked text sample and its md5 digest

And 40% volumes of attack. Experiments results showed up that any attack is detected efficiently, no matter how small the tampering is. During the embedding process, calculating HV1 ensures detection of any defect in the text's basic content, besides obtaining HV2 to clarify intruders' attempts to destroy the watermark. Specific statistics of each text type and attack volume are illustrated in [Table 1].

Table1. Text documents and attacks statistics

Text type	Word count	Character count	MOW "KW"	NOO	Type and volume of attack			
					Deletion	Reordering	Insertion	Replace
ST	210	1230	the	18	10%	10%	10%	10%
MT	513	3134	the	23	20%	20%	20%	20%
LT	1528	9389	the	88	40%	40%	40%	40%

4.3. Robustness availability

Ownership verification demands a robust watermark that can't easily be destroyed. Using a secret key provides a high level of security as it's only possessed by the author, that's why any illegal attempt for snatching ownership fails.

To evaluate our algorithm robustness, different forms of attacks were applied while measuring the accuracy of watermarking extraction. [Figures 5], [Figures 6] and [Figures 7] showing the measured accuracy of the extracted watermark from different text samples after being exposed to different levels of deletion, insertion and deleting attacks respectively. A large number of words and sentences was piled up to attack all text document samples. Regarding the results, it can be noticed that for deletion attacks, all text samples achieve a convergent level of extracted watermark accuracy.

The best accurate extracted watermark is provided by the three samples at 10%, 20% and 40% insertion attack. For reordering attacks, the accuracy of the watermark is the best for MT. For the LT sample it can be noticed that the extracted watermark is more sensitive towards reordering attack. The proposed algorithm provides a great ability to reveal any tamper and introduce a satisfactory level of robustness depending on attack type and size.

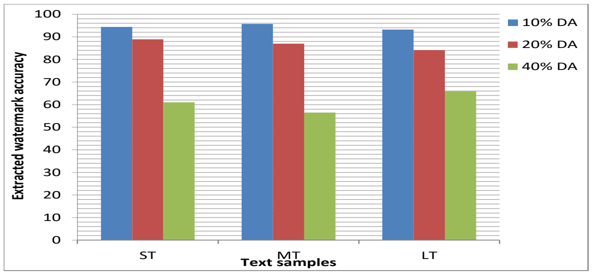


Figure 5. Accuracy for 10%, 20% 40% deletion attack “DA” on each text sample

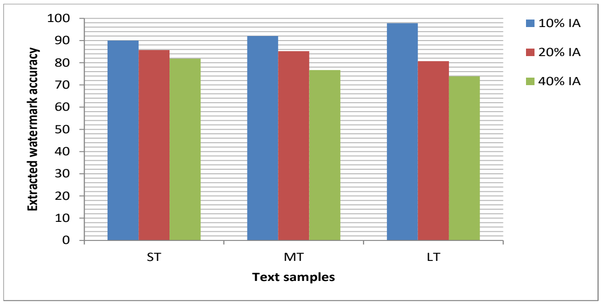


Figure 6. Accuracy for 10%, 20% and 40% insertion attack “IA” on each text sample

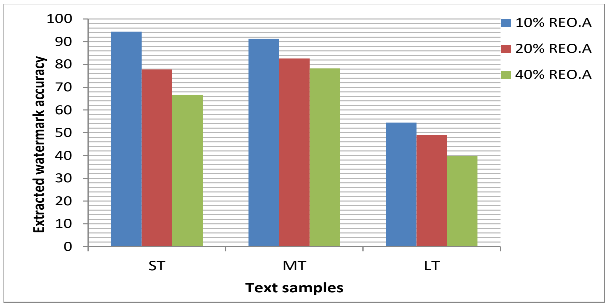


Figure 7. Accuracy for 10%, 20% and 40% reordering attack “REO.A” on each text sample

Acknowledgments

In this paper, we propose a watermarking scheme for plain text documents. Unlike the majority of other approaches that consider the text as an image while the watermark is embedded by modifying its pixels, our algorithm treats the text as an explicit text document with exploiting script format to embed the watermark directly. Multiple strategies are combined to achieve security, tamper detection and authentication goals.

References

[1] X. Zhou, W. Zhao, Z. Wang, and L. Pan, “Security theory and attack analysis for text watermarking,” Proceedings of the 2009 International Conference on E-Business and Information System Security., May 23-24, Wuhan, IEEE, pp.1-6, **(2009)**

[2] N.A. Al-Maweri and R. Ali, "State-of-the-art in techniques of text digital watermarking challenges and limitations," Journal of computer sciences., pp.62-80, **(2016)**

[3] Q. Chen, Y. Zhang, and L. Zhou, "Word text watermarking for ip protection and tamper localization," IEEE, pp.3595-3598, **(2011)**

[4] Z. Jalil and A. M. Mirza, "A review of digital watermarking techniques for text documents," Proceedings of the 2009 International Conference on Information and Multimedia Technology., IEEE, pp.230-234, **(2009)**

[5] Y. W. Kim and Il-Seok Oh, "Watermarking text document images using edge direction histograms," Elsevier, pp.1243-1251, **(2004)**

[6] J. T. Brassil, S. Low, N. F. Maxemchuk, and L. O'Gorman, "Electronic Marking and Identification Techniques to Discourage Document Copying" IEEE Journal on Selected Areas in Communications., vol.13, no.8, October, pp.1495-1504, **(1995)**

[7] J. T. Brassil, S. Low, N. Maxemchuk, and L. O. 'Gorman, "Hiding information in document images," In Proceedings of the 29th Annual Conference on Information Sciences and Systems. Baltimore, Maryland. 22-24 March, pp.482-489, **(1995)**

[8] D. Huang and H. Yan, "Inter-word distance changes represented by sine waves for watermarking text images," IEEE Trans. Circuits and Systems for Video Technology., Vol.11, No.12, December, pp.1237-1245, **(2001)**

[9] J. T. Brassil, S. Low, and N. F. Maxemchuk, "Copyright protection for the electronic distribution of text documents," Proceedings of the IEEE., vol.87, no.7, July, pp.1181-1196, **(1999)**

[10] T. Amano, "A feature calibration method for watermarking of document images," IBM Research., Tokyo Research Laboratory., pp.1-4.

[11] M. A. Al-Ahmad and A. E. Al-duwaikh, "A New Fragile Digital Watermarking Technique for a PDF Digital Holy Quran," proceedings of the 2013 International Conference on Advanced Computer Science Applications and Technologies., IEEE, pp.250-253, **(2013)**

[12] R. Olanrewaju, F. Fajingbesi and N. Ishak, "Watermarking in protecting and validating the integrity of digital information: a case study of the holy scripture," proceedings of the 2016 6th International Conference on Information and Communication Technology for The Muslim World., IEEE, pp.222-227, **(2016)**

[13] A. K. Bhattacharjya and H. Ancin, "Data embedding in text for a copier system," IEEE, pp.245 -249, **(1999)**

[14] J. Chen, F. Yang, H. Ma, and Q. Lu, "Text watermarking algorithm based on semantic role labeling," IEEE, pp.117-120, **(2016)**

[15] X. Sun and A. J. Asiimwe, "Noun-verb based technique of text watermarking using recursive decent semantic net parsers".

[16] "Natural language generation with markov chains and grammar" TJHSST Senior Research Project Computer Systems Lab 2009-2010 Sam Zhang June 15, **(2010)**

[17] M. L. Mali, N. N. Patil, and J. B. Patil, "Implementation of text watermarking technique using natural language watermarks," proceedings of the 2013 International Conference on Communication Systems and Network Technologies., IEEE, pp.482-486, **(2013)**

[18] M. J. Atallah and V. Raskin, "Natural language water-marking: design, analysis and a proof of concept implementation," Springer-Verlag Berlin Heidelberg, pp.185-200, **(2001)**

[19] H. M. Meral and B. Sankur, "Natural language watermarking via morphosyntactic alterations," Computer Speech and Language., Elsevier Ltd, pp.107-125, **(2009)**

[20] Z. Jalil and A.M. Mirza, "Text watermarking using combined image-plus-text watermark," Proceedings of the 2nd International Workshop on Education Technology and Computer Science., IEEE Xplore Press, pp.11-14, **(2010)**

[21] Z. JaliI and H. Aziz, "A zero text watermarking algorithm based on non-vowel ASCII characters," proceedings of the 2010 International Conference on Educational and Information Technology., IEEE, pp.503-507, **(2010)**

[22] Z. Jalil and A.M. Mrirza, "An invisible text watermarking algorithm using image watermark," Innovations in Computing Sciences and Software Engineering., Springer, New York, pp.147-152, **(2010)**

[23] Z. Jalil, A. M. Mirza, and M. Sabir, “Content based zero-watermarking algorithm for authentication of text documents,” proceedings of the International Journal of Computer Science and Information Security., vol.7, no.2, February, pp.212-217, **(2010)**

[24] Z. Jalil, A.M. Mrirza, and H. Jabeen, “Word length based zero-watermarking algorithm for tamper detection in text documents,” Proceedings of the 2nd International Conference on Computer Engineering and Technology., Apr. 16-18, IEEE Xplore Press, Chengdu, pp.378- 382, **(2010)**

[25] F. M. Ba-Alwi, M. M. Ghilan, and F. N. Al-Wesabi, “Content authentication of english text via internet using zero watermarking technique and markov model,” International Journal of Applied Information Systems., vol.7, no.1, Aprilpp.25-36, **(2014)**

[26] M. Bashardoost, M. Rahim, and N. Hadipour, “A novel zero-watermarking scheme for text document authentication,” Journal Teknologi (Sciences & Engineering), pp.49–56, **(2015)**

[27] D. Hanyurwimfura, Y. Liu and Z. Liu, “Text format based relational database watermarking for non-numeric data,” proceedings of the 2010 International Conference On Computer Design And Applications, IEEE, pp.312-316, **(2010)**

[28] Y. M. Alginahi, M. N. Kabir, and O. Tayan, “An enhanced kashida-based watermarking approach for Arabic text documents,” IEEE, pp.301-304, **(2013)**

[29] R. A. Alotaibi and L. A. Elrefaei, “Utilizing word space with pointed and un-pointed letters for arabic text watermarking,” proceedings of the 2016 UK Sim-AMSS 18th International Conference on Computer Modeling and Simulation., IEEE, pp.111-116, **(2016)**

[30] R. A. Alotaibi and L. A. Elrefaei, “Improved capacity Arabic text watermarking methods based on open word space,” Journal of King Saud University - Computer and Information Sciences., pp.1-13, **(2017)**