Arab J. Nucl. Sci. Appl., Vol. 52, 3, 126-133 (2019)

Arab Journal of Nuclear Sciences and Applications

ISSN 1110-0451 ***Web site: ajnsa.journals.ekb.eg*** **(ESNSA)**

A Tamper Proofing Text Watermarking Shift Algorithm for Copyright Protection

Amira Eid[(1)], Ahmed A. Emran[(2)] , Ahmed Y. Morsy[(2)]
[(1)]Computer and Electrical Engineering Department, Higher Technological Institute, 10th of Ramadan City, Egypt
[(2)]Department of Electrical Engineering, Al-Azhar University, Cairo-11371, Egypt

Received 16th Dec 2018
Accepted 26hMay 2019

Watermarking has proved its great reliability and flexibility for property rights protection and tamper detection of diverse forms of online distributed data. Among the different mediums in which watermarking technology is used, text watermarking represents the most challenging issue due to the distinctive nature of its various formats. Plain text is widely used for transferring information on the internet. Despite this, there is a lack of used plain text watermarking techniques, so obviously it is necessary to focus on that point and pay it more attention. In this paper a blind text watermarking approach is proposed for copyright protection and tamper detection of plain text by inter-word spacing (depending on a secret binary number and a key word) and text fingerprint through using MD5 hash function. Simulation results proved the success of our approach in detecting any tiny content tampering and due to the secret key, and the fingerprint of watermarked text, copyright protection are accomplished efficiently. This approach is a combination of several steps which work cooperatively to reach the desired goals.

Keywords: Text watermarking, Copy-right protection, Tamper detection, Hash function, Plain text

Introduction

In the era of the enormous proliferation of information technology, the role of 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 effectual sciences that offer solution to immunize transmitted data. Unfortunately, its role is limited to protection only during transmission process, once decryption is performed, the information becomes vulnerable to attack [1] and this is not appropriate to protect information circulating through the giant network.

To provide the required protection, digital watermarking is used. It based on 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 and doesn't block the 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.

Corresponding author: amira.eid@hti.edu.eg
DOI: 10.21608/ajnsa.2019.6694.1156

Therefore watermarking is widely applied in multiple mediums for ownership verification, data authentication and fingerprinting.
In this paper, a novel plain text watermarking approach is proposed. This approach provides both copyright protection and tamper detection.
The rest of the paper is organized as follows: section 2 contains an overview on text watermarking. The proposed approach is presented in section 3. In section 4 the simulation results are presented. Finally, the paper is concluded in section 5.

Text Watermarking Overview

The general watermarking concept, which involves three phases, is shown in Figure(1).
Those phases start with watermark generating and embedding which can be achieved by numerous algorithms, followed by the phase of potential attack, where the attacker delete, add or alter the digital content or tries to destroy the watermark. The last step, known as watermark detection, comes where the watermark is extracted from the data and compared to the original one in order to clarify any intentional or accidental attack. The extracted watermark is also used to resolve any dispute on data ownership [2].

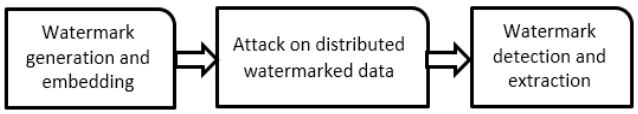

Figure (1): Watermarking Phases

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

1) Robustness: The watermark data is still detectable, although several forms of attack were applied on it and this is appropriate for ownership protection.
2) Imperceptibility: The original host data and the watermarked data cannot be distinguished.
3) Security: Keeping the watermark protected from illegal detection, such attribute is accomplished using cryptographic keys.
4) Capacity: The watermark should have a satisfactory amount of information.

Trade-offs between these requirements is 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 mediums 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 document to conceal 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 area that could provide new solutions for security problems threatening text entity such as all possible kinds of text manipulation like deletion, addition, forgery, alteration , text document property counterfeiting. These problems lead to serious situations especially if the text contains important and sensitive information where many represent critical issues to data owner.
Text watermarking could be exploited in two major applications: ownership verification and text authentication. Ownership verification or the so called copyright protection is executed by using a robust watermark which is 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 which 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 divided 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, stroke feature [5] and pixel levels. Image-based method is not appropriate for various cases as in text messages or blogs and is not robust to attacks.
2. Natural language method: The watermark is inserted using semantic processing [6], syntactic transformations or synonym permutation. 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 differs from other techniques as no alterations in the original document take place to perform the watermarking process, rather the text structure is used to extrapolate the watermark. An algorithm for content authentication of plain text document is presented by Jalil et al. [7]. A hashed watermark, which depends on HTML language structural features, is embedded in a web page [8]. Approaches for text authentication which use Markov model (chain) have been offered by other researchers [9, 10]. These algorithms couldn't succeed with all sorts of text, whilst it's limited to alphabetical documents, namely it is 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. Rizzo, et al [11] has proposed a blind algorithm for short text authentication using Unicode symbols alternatively to ensure content preservation. Researchers suggested [12],[13] and [14] 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.

Proposed Algorithm

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

The majority of used text watermarking techniques employs only one watermarking algorithm to achieve one of these goals, copyright protection or tamper detection. For more strength in facing malicious users, the present approach combines the two procedures to attain both copyright protection and tamper detection. First of all, 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 to the text, the watermark is extracted.

Before embarking on watermarking phases including insertion and extraction procedures, a brief description of MD5 function is initially provided.

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:

1) The generated hash has a fixed length regardless of the input message length.
2) Each message has a unique invariable hash value.
3) Ease of computation.
4) Irreversible "original message can't be obtained from its hash value".
5) 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:

Watermark embedding

The watermark WM insertion into the text to be watermarked using embedding algorithm is illustrated in Figure(2). Initially, the most occurring word MOW in the text is obtained in addition to the number of occurrence NOO. Afterward 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" shift the KW to left and for digit "0" leave the KW unchanged. Thus a watermarked document WD1 is produced. Thereafter, get the message digest of the marked text HV.

During the embedding process, calculating HV ensures detection of any defect in the text basic content besides, clarifying intruders' attempts to destroy the watermark.

The MOW, SK and HV are registered at a certifying authority (CA) as a reliable institution which is resorted at any dispute.

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 is to get the hash value HV_E of doubted watermarked content WD2 which in turn is compared to HV. Based on this comparison, it can be revealed whether or not there is a tampering. The second action is using WD2 to obtain the most occurring word MOW_E which is later employed as a keyword KW_E. Subsequently, the secret key SK_E is extracted via tracking the existence of a space after KW_E. The matching between the KW_E and KW and between SK_E and SK achieves the goal of our algorithm in terms of copyright protection. The extraction process is minutely elucidated in Figure(3).

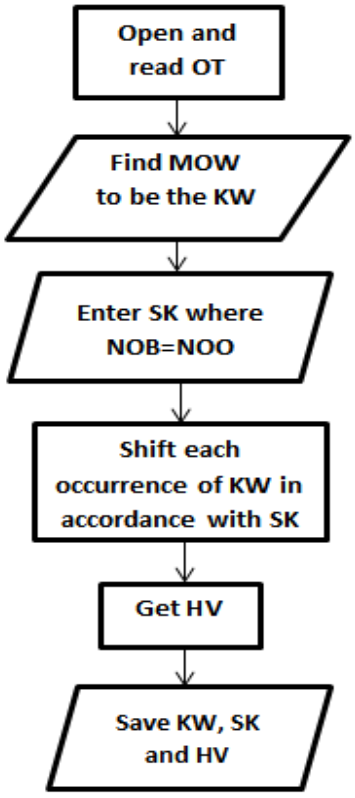

Figure (2): Embedding process sequences

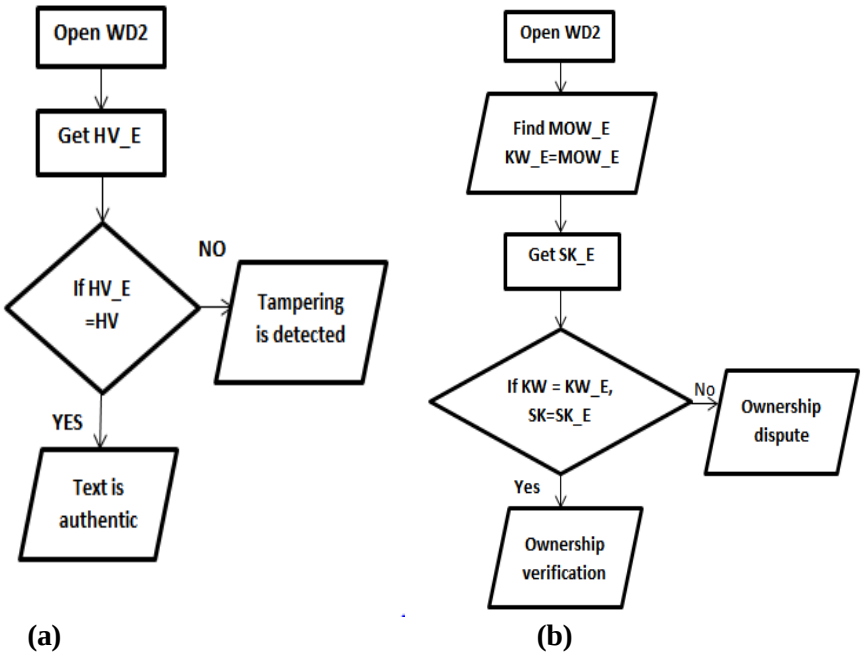

Figure (3): Workflow for extraction process; (a) Tampering detection and (b) Ownership verification

Simulation results and scheme evaluation

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

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

Watermark transparency

Figures (4-1 and 4-2) illustrate an original text sample and its marked version besides 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 a binary one is available in SK. Showing the watermarked content to a group of observers, the results illustrate an excellent level of imperceptibility.

Tamper detection capability

Three referred different lengths texts were exposed to various forms of attacks with different volumes. Deleting, adding some words or phrases to text structure and text reordering attacks are applied at random positions with 10%, 20% and 40% volumes of attack. Experiments results showed that any attack is detected efficiently, no matter how small the tampering is. During the embedding process, calculating HV ensures the detection of any defect in the text basic content besides clarifying intruders' attempts to destroy the watermark. Specific statistics of each text type and attack volume are illustrated in table 1.

```
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): Watermarked Text Sample and Its MD5 Digest

Table1. Text Documents and Attacks Statistics

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

Copyright protection ability

The copyright protection process enables the legal text owner, who generated and embedded the watermark, to guarantee his ownership. So, the watermark shouldn't be detected by intruders and this is accomplished by a robust watermark. For non-blind watermarking algorithms, this robustness is guaranteed by the imperative availability of the original text to extract the watermark. But for our blind proposed scheme, using a secret key and a keyword provide a high level of security as it's only possessed by the author besides having the hash value of watermarked text also increased robustness, that's why any illegal attempt for snatching ownership fails.

Robustness availability

Ownership verification demands a robust watermark which cannot be easily destroyed.

For our algorithm robustness evaluation, different forms of attacks were applied to measure the accuracy of extracted watermark. Figs. (5, 6) and 7) show the measured accuracy of the extracted watermark from different text samples after being exposed to different levels of deletion, insertion and reordering attacks respectively. A large amount of words and sentences was piled up to attack all text document samples. It should be borne in mind that the attack location is random in the three samples but the attack volume is maintained as shown in Table (1).

Regarding the results, it can be noticed that for deletion attack, all text samples achieve a convergent level of extracted watermark accuracy. The most accurate extracted watermark is provided by the three samples at 10%, 20% and 40% insertion attack. For reordering the attack, the accuracy of watermark is the best for MT. For 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, attack size and where the attack occurs within the text. So it is clear that the size of the text does not play a large role in determining the extracted watermark accuracy and the evidence is the results shown by MT.

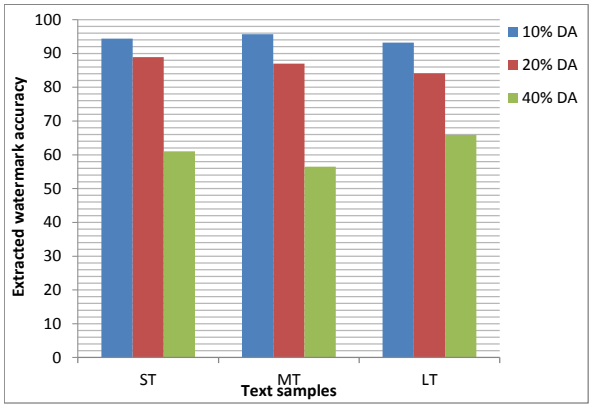

Figure (5): Accuracy for 10%, 20% 40% deletion attack "DA" on each text sample

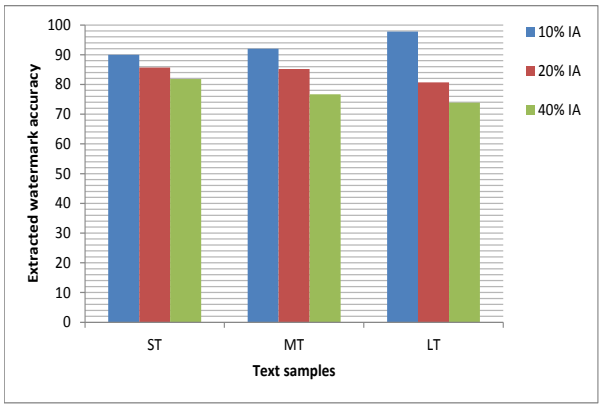

Figure (6): Accuracy for 10%, 20% and 40% insertion attack "IA" on each text sample

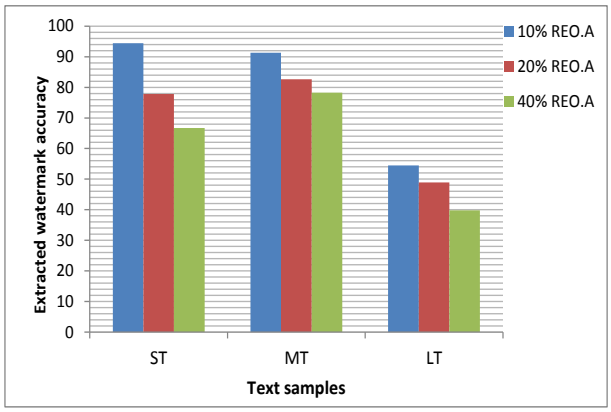

Figure (7): Accuracy for 10%, 20% and 40% reordering attack "REO.A" on each text sample

System comparison

Text watermarking is a challenging and a complex research field because text is sensitive to any content change. Despite the widespread use of the text in different means of communication, the development of employed algorithms is slow. Each of these algorithms is often designed to serve a particular language among the many known languages. In addition, each single-language text can be presented in multiple text or document formats.

Therefore, when a new algorithm is being created, it is based on achieving a specific goal in a particular application, so it becomes innovative and not necessarily based on another one.
Table (2) indicates our proposed scheme compared to Rizzo's algorithm [11].

The comparison clearly shows that the proposed scheme has overcome the limitations of the other scheme specially text size, embedding and watermark extraction complexity and this reduced the embedding and extraction time of our algorithm.

Table (3) shows the embedding time, the watermark extraction time from authentic watermarked text and the watermark extraction time from attacked watermarked text for the three text samples.

Table 2: Comparison between the two schemes

	Proposed Scheme	Rizzo's Scheme
Type	Blind algorithm	Blind algorithm
Application	Tampering detection and copyright protection	Authorship verification
Watermark	SK, KW and hash value of watermarked text	Hash value of combined text and password
Embedding	Inserts a space after KW	Replaces spaces and characters with Unicode symbols
Watermark extraction	Direct and easy	Using a predefined symbols mapping "complex"
Text size	Short, medium, long and very long text	Only short text

Table 3: Embedding and extraction time for the 3 samples

Text size	Watermark embedding time in seconds	Watermark extraction time for authentic text in seconds	Average extraction time of attacked text In seconds
ST	0.010741	0.011844	0.011571
MT	0.018455	0.017914	0.017933
LT	0.027400	0.018150	0.018821

Conclusion

In this paper, a blind watermarking scheme for plain text documents is proposed. Unlike the majority of other approaches that consider the text as an image while watermark is embedded by modifying its pixels, the present algorithm treats the text as an explicit text document with exploiting script format to embed the watermark directly. Experimental results have showed that the proposed algorithm is applied efficiently to all text sizes as the space is added after the keyword only when its corresponding bit in the secret binary key is 1 and is not added when the bit is 0. 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, (2009), pp. 1-6.

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., (2016), pp. 62-80.

3-Q. Chen, Y. Zhang and L. Zhou, "Word Text Watermarking for IP Protection and Tamper Localization", IEEE, (2011), pp. 3595-3598.

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, (2009), pp. 230-234.

5- 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, (2016), pp. 222-227.

6-J. Chen, F. Yang , H. Ma and Q. Lu, " Text Watermarking Algorithm Based on Semantic Role Labeling", IEEE, (2016), pp. 117-120.

7-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 (2010), pp. 212-217.

8-M. T. Ahvanooey, H. D. Mazraeh & S. H. Tabasi, "An innovative technique for web text watermarking (AITW) ", Information Security Journal: A Global Perspective, (2016), pp. 1-6.

9-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, April (2014), pp. 25-36.

10-M. Bashardoost, M. Rahim and N. Hadipour, "A novel zero-watermarking scheme for text document authentication", Journal Teknologi (Sciences & Engineering), (2015), pp. 49–56.

11-S. G. Rizzo, F. Bertini and D. Montesi, "Text Authorship Verification through Watermarking", European Intelligence and Security Conference**,** IEEE**, (**2016), pp. 168-171.

12-Y. M. Alginahi , M. N. Kabir and O. Tayan, "An enhanced kashida-based watermarking approach for Arabic text documents", IEEE, (2013), pp. 301-304.

13-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, (2016), pp. 111-116.

14-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.