We are IntechOpen, the world's leading publisher of Open Access books
Built by scientists, for scientists

6,900
Open access books available

186,000
International authors and editors

200M
Downloads

154
Countries delivered to

Our authors are among the

TOP 1%
most cited scientists

12.2%
Contributors from top 500 universities

CLARIVATE ANALYTICS
BOOK CITATION INDEX
INDEXED

WEB OF SCIENCE™

Selection of our books indexed in the Book Citation Index
in Web of Science™ Core Collection (BKCI)

Interested in publishing with us?
Contact book.department@intechopen.com

Chapter

Perspective Chapter: Text Watermark Analysis – Concept, Technique, and Applications

Preethi Nanjundan and Jossy P. George

Abstract

Watermarking is a modern technology in which identifying information is embedded in a data carrier. It is not easy to notice without affecting data usage. A text watermark is an approach to inserting a watermark into text documents. This is an extremely complex undertaking, especially given the scarcity of research in this area. This process has proven to be very complex, especially since there has only been a limited amount of research done in this field. Conducting an in-depth analysis, analysis, and implementation of the evaluation, is essential for its success. The overall aim of this chapter is to develop an understanding of the theory, methods, and applications of text watermarking, with a focus on procedures for defining, embedding, and extracting watermarks, as well as requirements, approaches, and linguistic implications. Detailed examination of the new classification of text watermarks is provided in this chapter as are the integration process and related issues of attacks and language applicability. Research challenges in open and forward-looking research are also explored, with emphasis on information integrity, information accessibility, originality preservation, information security, and sensitive data protection. The topics include sensing, document conversion, cryptographic applications, and language flexibility.

Keywords: information protection, information security, text analysis, text watermarking, watermarking

1. Introduction

Recent years have seen a dramatic increase in communication via telephone, video, and the Internet. Companies and individuals still exchange paper copies of important documents. The development of a reliable method for authenticating hardcopy documents remains a critical task [1].

In this chapter, we present an innovative method for authenticating documents either electronic or printed documents may be affected combining these methods with traditional ones is recommended In addition to what was mentioned previously. This system is similar to the one proposed in [2], but Noise in the channel is taken into account during the detection process. This is the result of they have a much lower perceptual impact than digital sensors. The binary code of documents

is protected by signatures. The system proposed here protects visual content. As a comparison, digital watermarking schemes are capable of transmitting hidden messages [3]. The proposed system classifies documents based on authenticity or nonauthenticity. A major advantage of this system is that it does not require a database. In this case, the information to be compared will be stored. As a result, the proposed method is suitable for this purpose. Self-authentication using text (TSA) is the name given to this technology. In addition, special considerations have been taken. When using a consumer scanner, only a consumer scanner is required. There is a consideration for a printed document. TSA is not relied upon. There are two ways to modify each character: either by modifying the function or by changing the character itself. This can be achieved with very little perceptual impact using text watermarking using techniques [4–6], or visibly, we can increase robustness.

Information on the internet is among the most common information found in today's world. The digital format is having both positive and negative effects on the modern world. The advancement of technologies, medical science, and astronomy are examples. The misuse of these technologies also has a number of negative aspects, such as protecting copyright and manipulating data. As a result of advanced technologies such as the world wide web and high-speed computer networks, unauthorized copying, redistribution, and storing of digital contents has been carried out in many ways. In order to prevent unauthorized copies of digital content, digital content security is crucial [7]. The Internet of Things (IoT) and cloud computing have experienced extensive government and research support at the global level [8]. There are numerous data formats supported by cloud computing, including video, audio, images, and text. However, establishing responsibility and protecting the content are challenging tasks. The data that enables smart cities to function is crucial for sustaining the data infrastructure and enabling the delivery of digital content to citizens. **Figure 1** illustrates this architecture. All data storage, processing, and analysis take place at a central location. Using digital watermarking, you can protect and verify the ownership of digital content. With the right technology, you can embed secret messages in digital content without compromising valuable information. Ownership identification will then be made possible with this information. The different types of digital watermarking are watermarking in text, photos or images, audio, and videos. These three types of watermarking have been the subject of most research. Text watermarks are becoming increasingly popular due to the large number of text documents currently being produced and shared [9].

Figure 1.
Smart cities are built according to certain architecture.

2. Technology associated with digital watermarking

The digital watermarking process involves embedding identification information into a data carrier in a way that makes it difficult for third parties to detect, and without it adversely affecting the data. These technologies are often used to protect multimedia data as well as databases and text files. The dynamics and randomness of data make embedded watermarks quite different from those embedded in text files or databases. Data with redundant information and acceptable precision errors are prerequisites to machine learning. Taking into account the range of error tolerance within the database, Boney et al. embedded watermarking in the least important position [10, 11]. Sion et al. proposed a mathematical model based on the statistical property of an array of data (**Figure 2**).

To prevent an attacker from destroying the watermark, attribute data are embedded within it [12, 13]. Furthermore, fingerprints from databases are embedded into watermarking as a means of identifying the information owners and objects distributed [14]. This enables leakers to be identified. Watermarks without secret keys can also be verified using independent component analysis [15]. A number of references are provided for further information [16, 17]. When a fragile watermark is embedded in the tables of databases, data items will be detected in time [18, 19].

Text watermarking uses many generations of methods, which can be categorized into three kinds. There are two types of watermarking: one is based on fine-tuning the document structure, hoping that line spacing will differ from word spacing, and the other is based on subtle differences between line spacing and word spacing. As another type of watermarking, there is text content watermarking, which is based on modifying the content of the text, such as adding white spaces, amending punctuation, etc. Third, watermarking is based on semantic understanding, which can achieve changes by the replacement of synonyms or the transformation of sentences, for instance. Despite the fact that most watermarking studies here focus on static data sets, Big Data's peculiarities, such as high-speed data generation and updating, are not sufficiently addressed (**Figure 3**).
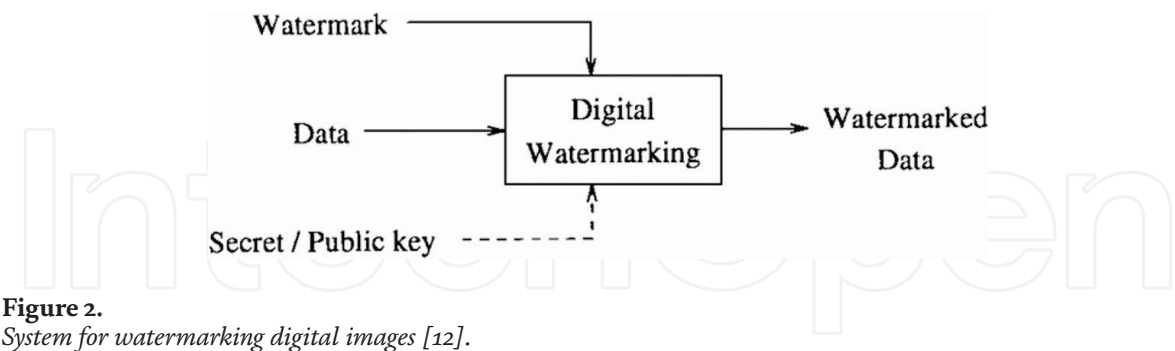

Figure 2.
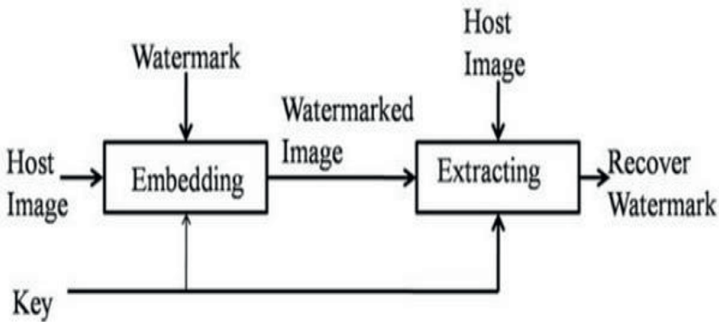*System for watermarking digital images [12].*

Figure 3.
Watermarking system with a digital signature [20].

3. Analyzing watermarks in text

A digital watermark (digital intellectual property) identifies its owner or originator by providing a unique numerical code. Tracking digital media usage online is done and warnings are sent when unauthorized access or use is possible. A digital watermark is an important part of digital rights management (DRM). A kind of marker is hidden within digital media, such as audio, video, or images, allowing us to determine who owns the copyright to them. By tracking copyright infringement on social media, this technique determines whether a note is authentic in banking. Watermarking is an extremely effective method of securing digital documents in addition to its ability to address distortion, replication, unauthorized access, and security breaches.

There are several ways to classify digital watermarking techniques.

3.1 Durability

Digital watermarks that are fragile can no longer be detected if they are altered even slightly. Tamper-proofing is a common method of protecting digital watermarks. Watermarks are commonly used to describe visible changes to a work instead of generalized barcodes.

Digital watermarks, for example, are semi-fragile, which means they resist benign changes but become unrecognizable after malignant changes. The detection of malignant transformations often requires watermarks with semi-fragile properties. The robustness of a watermark depends on how well it resists various types of transformations. Strong watermarks can carry both copying and access control information when used in copy protection applications.

3.2 Perception

The term "imperceptible watermarks" refers to those that are virtually indistinguishable from the original signal.

The observable type of watermark is one that can be felt (e.g., network logos, content bugs, code symbols, images that appear opaque). Occasionally, videos and pictures may have transparent/translucent portions for the convenience of the consumer, but these portions degrade the view and degrade the quality of the video.

A perceptual watermarking is not the same as watermarking that uses human perception limitations to appear indistinguishable.

3.3 Availability

In general, digital watermarking schemes can be divided into two main categories based on the length of the embedded message:

- A zero-bit message is conceptually sent, and the system is designed to detect whether a watermark is present or absent. Zero-bit or presence watermarking schemes are commonly used for this type of watermark.

- Messages are n-bit-long streams modulated by or and contain watermarks. Watermarking schemes of this type are usually called multiple-bit watermarking or non-zero-bit watermarking.

3.4 A method of embedding

The term spread spectrum watermarking refers to digital watermarking methods that are created by modifying signals. Watermarks using spread-spectrum technology may be moderately robust, but they also have poor information capacities as a result of host interference.

Quantization is a type of digital watermarking when the signal is obtained through quantization. The fact that host interference is rejected makes quantization watermarks highly informative despite their low robustness.

A watermark of this type embeds an amplitude modulated signal into an additive modulus, similar to a spread spectrum, but integrated within the spatial domain.

3.5 Examining different watermarking algorithms

3.5.1 Requirements

Watermarking digitally can be applied to a variety of different applications, including:

• The importance of protecting your intellectual property

• Watermarked content can be tracked (different recipients receive different watermarks).

• Monitoring broadcasts (sometimes international agencies watermark their video on television news broadcasts)

• A process for obtaining video authentication

• Screen casting and video editing programs should be purchased in order to get rid of the software.

• Identification cards: their security

• Determining if fraud or tampering has taken place.

• Managing social media content

4. Digital watermarking: A life-cycle

A watermarks encrypt information in an audio signal; however, the term is also used in some contexts to distinguish between watermarked and cover signals. The process of embedding the watermark in a host signal is known as encoding the watermark in a host signal. A watermarking process consists of three steps: embedding, attacking, and detecting. Embedding can create a watermarked signal by using an algorithm to take the host and the data.

In general, watermarked digital signals are transmitted or stored to another party. This signal is then modified by another individual. Modifying the digital watermark may be used by a third party to remove the watermark, which may not even be malicious. Copyright protection applications may be affected by this attack. The images or videos can be modified in a variety of ways, such as by lossy compression (which reduces the resolution), cropping, or intentionally adding noise.
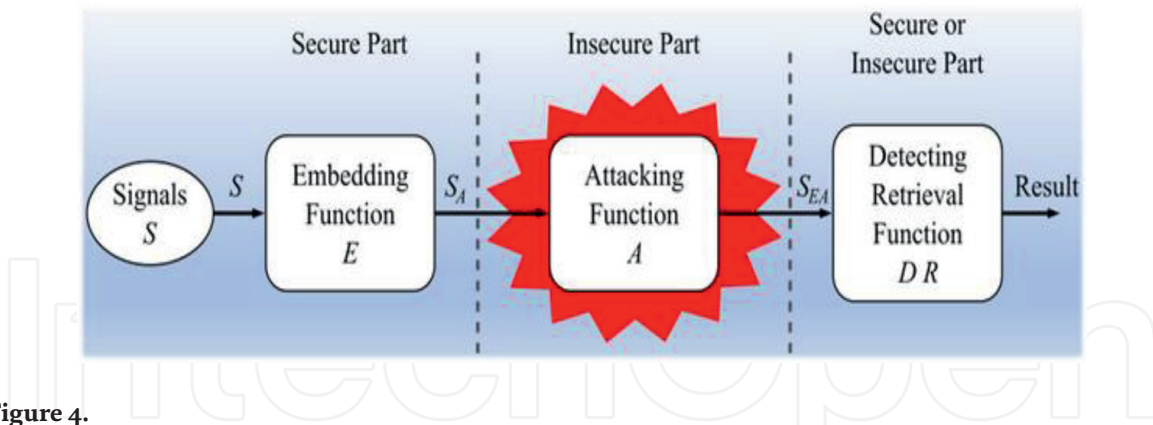
Figure 4.
Life-cycle phases of a digital watermark: embedding, attacking, detecting, and retrieving [21].

A detection algorithm is used to find a watermark in an attacked signal (also known as extraction). Even a transmission that was unaltered can still contain the watermark. Even robust digital watermarking applications should correctly extract watermarks despite strong changes. The extraction algorithm should fail whenever the signal is modified in fragile digital watermarking (**Figure 4**).

5. Watermarking text using digital technology

Watermarking has been a vital research area since 1991 when the concept of text digital watermarking was introduced. As the internet grows and communication spreads globally, a variety of text watermarking techniques have been proposed with the passage of time. Images-based and linguistic-based systems, as well as structural-based and hybrid approaches, are all available [22, 23].
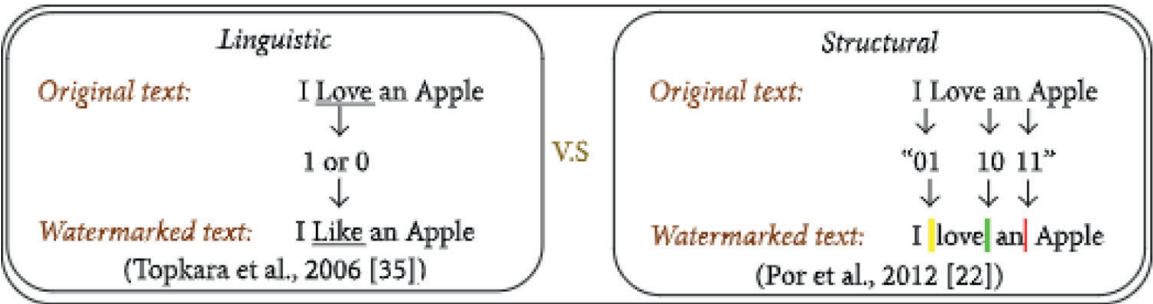
A. Methodologies based on images

The cover text is viewed as an image and embedded with a watermark according to the image-based approach described in [24]. The watermarked logos and images are converted into text strings and the data is generated. Watermarks serve as both a means of verifying ownership and preventing copyright infringement. In spite of the fact that optical character recognition (OCR) is considered safe for formatting attacks, it has limited applicability due to the fact that it ruins hidden information [25]. A technique described by Rizzo et al. [24] encrypts a short piece of text with a hidden watermark while preserving its content strictly. Images cannot be altered in either their content or appearance when converted from the text. Watermarking with blind watermarks helps protect content and ensure visibility. According to the authors of the study, a zero watermarking hybrid approach was used in their study [26, 27]. Watermarks are created by converting images into watermarks and embedding them on book covers. The disadvantage of this technology is that keys generated by certified authorities (CAs) must be stored in a large amount of storage space. In their [28] work, Thongkor and Amornraksa describe the process of watermarking scanned and printed documents with spatial information. For embedding the watermark, the image is composed of white and blue components. To determine whether the proposed technique is efficient, a variety of scanning resolutions, printing materials, and quality levels are analyzed.

B. An interdisciplinary approach to linguistics

The semantic and syntactic approach relies on techniques that emphasize semantics that is used to embed the watermark without altering the meaning of the texts. The idea is to conceal data by using a semantic approach, which replaces words with their synonyms. By using this method, grammatical alternations are used for embedding watermarks without changing the meaning of the original text. The watermarking process involves several language parts, such as verbs, adverbs, nouns, pronouns, adjectives, prepositions, acronyms, and conjunctions. In **Figure 5**, structural and linguistic approaches are compared. Based on integrating Chinese text features, Liu et al. [28] propose a method. Each word has been translated. In addition to measuring entropy, weight is also calculated using entropy. This method does well when considering formatting attacks. An approach to resolving this issue has been proposed by Yingjie et al. [30]. A Watermarking technique based on prose characteristics. Using representative words, one can generate keywords, core verb sets, and proportional features for adjectives. Watermarks are embedded by using verbs, adjectives, nouns, and adverbs. The reposed technique does not embed watermarks well.
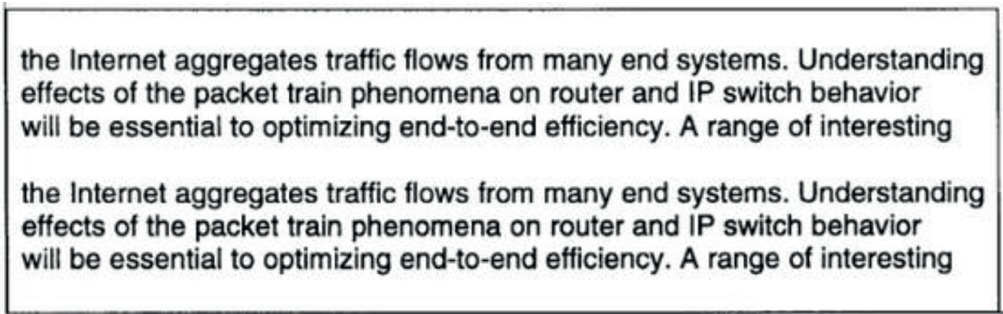
C. Approaches based on structural analysis

Those techniques incorporate the essential bits of an In-Text, including its structure and characteristics. Watermarks may be used, for example, as identifiers for documents when they are incorporated into a line. Although this method resolves the problem of document ownership authentication for some types of text documents, it is not applicable to all types of documents. There will be no possibility of hidden information being revealed if there are spaces between words, lines, and paragraphs. The following **Figure 6** illustrates this. The first three lines in **Figure 6** are shifted downward so that the middle line is facing downward. To enhance the textual features preserved by this approach, we also used natural language processing (NLP) techniques and resources. As part of their Arabic watermarking technique, Taha et al. [29] propose the use of Kashida extension characters and extra small whitespaces. This approach does not resist formatting attacks as a result of removing the spaces between words. Ba-Alwi et al. [32] developed a new approach to watermarking zero text based on probabilistic models. A watermark is created by measuring the spacing between characters. In comparison with similar techniques, this method is more robust and performs better in reordering attacks. Zhang et al. [33] proposes a method for encrypting watermarking

Figure 5.
The comparative analysis of linguistics and structuration [29].

the Internet aggregates traffic flows from many end systems. Understanding effects of the packet train phenomena on router and IP switch behavior will be essential to optimizing end-to-end efficiency. A range of interesting

the Internet aggregates traffic flows from many end systems. Understanding effects of the packet train phenomena on router and IP switch behavior will be essential to optimizing end-to-end efficiency. A range of interesting

Figure 6.
*An illustration of line-shift coding [31].*

information with the Caesar cipher using the user key, then making and packing plain text messages from the encrypted messages. Tests have been performed to prove that the system is undetectable. Whitespace-based approaches are low embedding capable and vulnerable to formatting attacks, according to Liang and Iranmanesh [34]. This method has the disadvantage of requiring a large number of blank spaces to conceal the secret message. By applying the modern technology of information security, Usmonov et al. [35] proposed a technique for protecting data transmitted between logical, physical, and virtual components of IoT systems. A secure online health application is based on the integration of IoT, Big Data, and Cloud convergence, as designed by Suciu et al. [36]. Cloud View Exalead's infrastructure-level information can be used for online and enterprise-based search applications. An approach using Font-Code by Xiao et al. [37, 38] embeds watermarks into font glyphs rather than changing the actual text. This algorithm has the advantage of being robust and imperceptible, but it only works with one font family and is relatively small in capacity. In order to detect the message, a large font size is required, depending on the OCR library.

D. Methodologies that combine the best of both worlds

To combine the benefits of different text watermarking techniques, a hybrid approach has been developed. The hybrid approach is considered robust and can be applied to wide-text documents [39]. Elrefaei and Alotaibi [31] proposed a method for handling Arabic text using pseudo-space. This method recovers watermarked letters from strings of connected letters. The proposed method is unnoticeable and robust when used in a formatted document; however, it is not robust when used in a document with retyping. By Hamdan and Hamarsheh [39, 40], Hamdan and Hamarsheh present a new way of hiding text messages in text using Omega network structures. The authors of this study [41, 42] suggested that fragile watermarks be used to safeguard data integrity in the IoT.
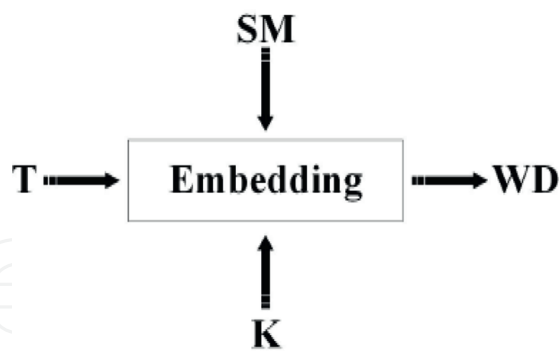
6. The process of watermarking embedding and extraction

Watermarking is used to discourage illegal copying and prevent digital assets from being distributed [43]. The **Figure** 7 below shows an implementation of text digital watermarking. Watermarking is a two-step process that involves embedding and removing the watermark. The document contains a piece of information called a watermark. There are three steps involved in embedding a watermark. Developing
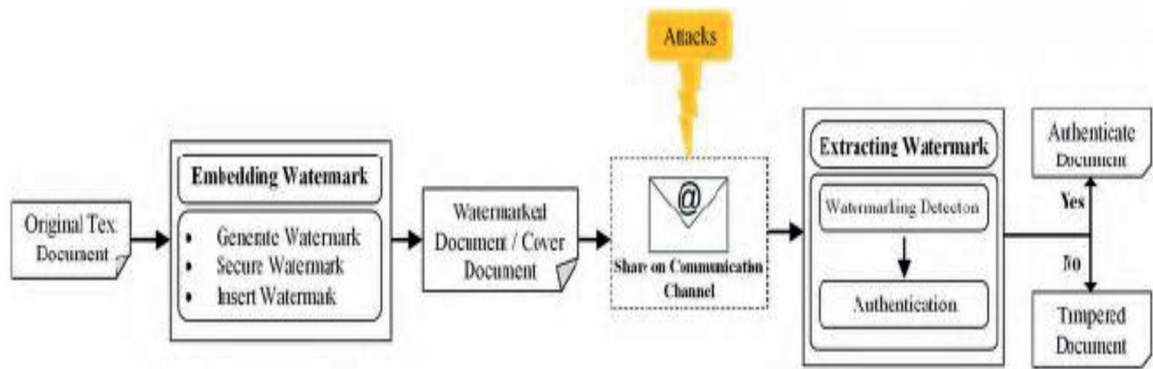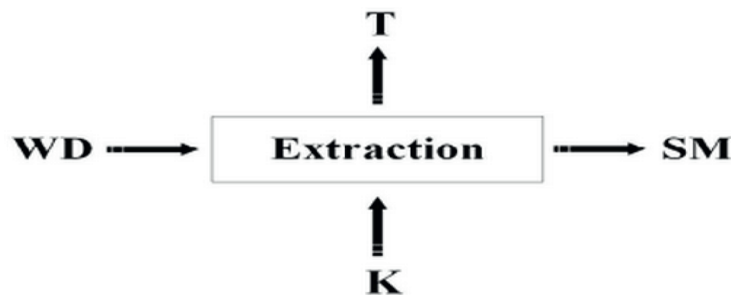
Figure 7.
An overview of digital text watermarking [42].

a watermark first requires that you include information about its owner, such as the author and publisher. Watermark security is the transformation of a watermark into a binary string or group. The last option is to insert a watermark in a document without having it affect the whole document. **Figure 7** illustrates the process for embedding a watermark. This is accomplished by representing "SM" for the secret message, "T" for the original document, "WD" for a watermarked document and "K" for the key. Watermarked documents can be shared via e-mail, websites, and social media channels. The process of extracting or verifying watermarks reverses watermark embedding. **Figure 6** illustrates how watermarks are extracted by entering the key and the watermarked document and detecting the secret message (**Figures 8** and **9**).

Figure 8.
The process of embedding watermarks [44].

Figure 9.
Process of extracting watermarks [44].

7. Conclusion

Text watermarking provides copyright protection. Generally, this is the most reliable and affordable way, especially for regular users. The algorithm, however, cannot be conquered by a computer hacker. A text document's cost can be kept low to improve watermark protection by preventing them from being attacked. In order to authenticate the digital contents of smart cities, and efficient watermarking algorithm is proposed. A comparison between the proposed technique and previous methods is done in order to evaluate its imperceptibility, security, robustness, and capability. There are many different approaches to this problem, but we also need a method that can be applied to smart cities, IoT devices, and the cloud. Experiments have shown that the proposed algorithm is highly imperceptible and achieves a 95.99 similarity factor. Despite being very robust, this algorithm can detect watermarks with high accuracy despite attacks such as cutting, copying, and pasting, font size, color, and alignment. By comparison, the proposed algorithm is more efficient than previous techniques. This method gives the same results in the cloud computing environment for securing text documents in smart cities. A future extension of the proposed solution could cover the copyright protection of print documents.

Author details

Preethi Nanjundan* and Jossy P. George
Department of Data Science, Christ University, Pune Lavasa, India

*Address all correspondence to: preethi.n@christuniversity.in

IntechOpen

References

[1] Borges PVK, Mayer J, Izquierdo E. Performance Analysis of text halftone modulation. In: 2007 IEEE International Conference on Image Processing. 2007. pp. III-285–III-288. DOI: 10.1109/ICIP.2007.4379302

[2] Villan R, Voloshynovskiy S, Koval O, Deguillaume F, Pun T. Tamper-proofing of electronic and printed text documents via robust hashing and data-hiding. In: Proceedings of SPIE-IST Electronic Imaging 2007, Security, Steganography, and Watermarking of Multimedia Contents IX, San Jose, USA. 2007

[3] Barni M, Bartolini F. Watermarking Systems Engineering: Enabling Digital Assets Security and Other Applications. New York: Marcel Dekker; 2004

[4] Brassil JT, Low S, Maxemchuk NF. Copyright protection for the electronic distribution of text documents. Proceedings of the IEEE. 1999;**87**(7):1181-1196

[5] Vllan R, Voloshynovskiy S, Koval O, Vila J, Topak E, Deguillaume F, Rytsar Y, Pun T. Text data-hiding for digital and printed documents: Theoretical and practical considerations. In: Proc. of SPIE, Elect. Imaging, USA, 2006

[6] Borges PV, Mayer J. Document watermarking via character luminance modulation. In: IEEE Int'l Conf. on Acoustics, Speech and Signal Processing, May 2006

[7] Zeeshan M, Ullah S, Anayat S, Hussain RG, Nasir N. A review study on unique way of information hiding: Steganography. International Journal of Data Science. 2017;**3**(5):45

[8] Huh S, Cho S, Kim S. Managing IoT devices using blockchain platform. In: Proc. 19th Int. Conf. Adv. Commun. Technol. (ICACT), February 2017. pp. 464-467

[9] Panah AS, Van Schyndel R, Sellis T, Bertino E. On the properties of non-media digital watermarking: A review of state of the art techniques. IEEE Access. 2016;**4**:2670-2704

[10] Boney L, Tewfik AH, Hamdy KH. Digital watermarks for audio signals. In: Proc. EUSIPCO 1996, Trieste, Italy, September 1996

[11] Bors A, Pitas I. Embedding parametric digital signatures in images. In: EUSIPCO-96, Trieste, Italy, September 1996

[12] Sion R, Atallab M, Prabhakar S. On watermarking numeric sets. In: Proceedings of the first international workshop on digital watermarking, Seoul, Korea, November 21-22; 2002

[13] Sion R, Atallah M, Prabhakar S. Right protection for relational data. In: Proceedings of the 2003 ACM SIGMOD international conference on management of data, San Diego, USA, June 10-12; 2003

[14] Guo F, Wang J, Li D. Fingerprinting relational databases. In: Proceedings of the 2006 ACM symposium on applied computing, Dijion, France, April 23-27; 2006

[15] Jiang C, Sun X, Yi Y, et al. Study of database public watermarking based on JADE algorithm. Journal of Simulation. 2006;**18**(7):1781-1785

[16] Zhang Y, Niu X, Zhao D. A method of protecting relational databases copyright with cloud watermark. International

Journal of Information Technology. 2004;**1**(1):206-210

[17] Liu Y, Ma Y, Zhang H, et al. A method for trust management in cloud computing: Data coloring by cloud watermarking. International Journal of Automation and Computing. 2011;**8**(3):280-285

[18] Guo H, Li Y, Liu A, et al. A fragile watermarking scheme for detecting malicious modifications of database relations. Information Sciences. 2006;**176**(10):1350-1378

[19] Khan A, Mirza AM. Genetic perceptual shaping: Utilizing cover image and conceivable attack information during watermark embedding. Information Fusion. 2007;**8**(4):354-365. CiteSeerX 10.1.1.708.9509. DOI: 10.1016/j. inffus.2005.09.007 ISSN 1566-2535. "CPTWG Home Page". cptwg.org. Archived from the original on 2008-02-23

[20] Akter A, Nur-E-Tajnina, Ullah M. Digital image watermarking based on DWT-DCT: Evaluate for a new embedding algorithm. 2014. pp. 1-6. DOI: 10.1109/ICIEV.2014.6850699

[21] Abbas N. Watermarked and noisy images identification based on statistical evaluation parameters. Journal of Zankoy Sulaimani-Part A (JZS-A). 2013;**15**:159. DOI: 10.17656/jzs.10265

[22] Hao Y, Chuang QFL, Rong D. A survey of digital watermarking. Journal of Computer Research and Development. 2005;7:1093-1099

[23] Kaur M, Mahajan K. An existential review on text watermarking techniques. International Journal of Computers and Applications. 2015;**120**(18):1-4

[24] Rizzo SG, Bertini F, Montesi D. Content-preserving text watermarking through unicode homoglyph substitution. In: Proc. 20th Int. Database Eng. Appl. Symp. 2016. pp. 97-104

[25] Tayan O, Kabir MN, Alginahi YM. A hybrid digital-signature and zero-watermarking approach for authentication and protection of sensitive electronic documents. Scientific World Journal. 2014;**2014**:514652

[26] Thongkor K, Amornraksa T. Digital image watermarking for printed and scanned documents. Proceedings of SPIE. 2017;**10420**:104203O

[27] Ahvanooey MT et al. A comparative analysis of information hiding techniques for copyright protection of text documents. Security and Communication Networks. 2018;**2018**:1-22

[28] Liu Y, Zhu Y, Xin G. A zero-watermarking algorithm based on merging features of sentences for Chinese text. Journal of the Chinese Institute of Engineers. 2015;**38**(3):391-398

[29] Taha A, Hammad AS, Selim MM. A high capacity algorithm for information hiding in Arabic text. Journal of King Saud University - Computer and Information Sciences, to be published

[30] Yingjie M, Huiran L, Tong S, Xiaoyu T. A zero-watermarking scheme for prose writings. In: Proc. Int. Conf. Cyber-Enabled Distrib. Comput. Knowl. Discovery (CyberC), October 2017. pp. 276-282

[31] Alotaibi RA, Elrefaei LA. Improved capacity Arabic text watermarking methods based on open word space. Journal of King Saud University - Computer and Information Sciences. 2018;**30**(2):236-248

[32] Ba-Alwi FM, Ghilan MM, Al-Wesabi FN. Content authentication of english text via Internet using zero

watermarking technique and Markov model. International Journal of Applied Information Systems. 2014;**7**(1):25-36

[33] Zhang Y, Qin H, Kong T. Anovel robust textwatermarking forword document. In: Proc. 3rd Int. Congr. Image Signal Process (CISP), vol. 1, 2010. pp. 38-42

[34] Liang OW, Iranmanesh V. Information hiding using whitespace technique in Microsoft word. In: Proc. 22nd Int. Conf. Virtual Syst. Multimedia (VSMM), October 2016. pp. 1-5

[35] Usmonov B, Evsutin O, Iskhakov A, Shelupanov A, Iskhakova A, Meshcheryakov R. The cybersecurity in development of IoT embedded technologies. In: Proc. Int. Conf. Inf. Sci. Commun Technol. (ICISCT). 2017. pp. 1-4

[36] Suciu G et al. Big data, internet of things and cloud convergence - an architecture for secure E-health applications. Journal of Medical Systems. 2015;**39**(11):141

[37] Xiao C, Zhang C, Zheng C. FontCode: Embedding information in text documents using glyph perturbation. ACM Transactions on Graphics. 2018;**37**(2):15

[38] Jalil Z. Copyright protection of plain text using digital watermarking. FAST Nat. Univ. Comput. Emerg. Sci., Islamabad, Pakistan, Tech. Rep. 1059, 2010

[39] Hamdan AM, Hamarsheh A. AH4S: An algorithm of text in text steganography using the structure of omega network. Security and Communication Networks. 2017;**9**(18):6004-6016

[40] Zhang G, Kou L, Zhang L, Liu C, Da Q, Sun J. A new digital watermarking method for data integrity protection in the perception layer of IoT. Security and Communication Networks. 2017;**2017**:3126010

[41] Topkara M, Riccardi G, Hakkani-Tür D, Atallah MJ. Natural language atermarking: Challenges in building a practical system. Proceedings of SPIE. 2006;**6072**:60720A

[42] Al-Maweri NAS, Ali R, Adnan WAW, Ramli ARB, Ahmad SMSAA. State-of-the-art in techniques of text digital watermarking: Challenges and limitations. Journal of Computational Science. 2016;**12**(2):62-80

[43] Mayer J, Bermudez JCM. Multi-bit informed embedding watermarking with constant robustness. In: IEEE International Conference on Image Processing; 2005. pp. I-669. DOI: 10.1109/ICIP.2005.1529839

[44] Khadam U, Iqbal MM, Azam MA, Khalid S, Rho S, Chilamkurti N. Digital watermarking technique for text document protection using data mining analysis. IEEE Access. 2019;**7**:64955-64965. DOI: 10.1109/ACCESS.2019.2916674