ACCEPTED FROM OPEN CALL

Data Aggregation and Privacy Preserving Using Computational Intelligence

Umair Khadam, Muhammad Munwar Iqbal, Sohail Jabbar, and Syed Aziz Shah

Abstract

In today's smart world, the privacy protection of data is an important issue. Data is distributed, reproduced, and disclosed with extensive use of communication technologies. Many non-traditional challenges arise with the rapid increase of IoT devices for system design and implementation. However, security and privacy are the main issues in IoT. With advanced technologies, an illegal copy of the content can easily be generated and shared. Therefore, it is crucial for users to protect and secure their data. In the said perspective, an efficient third-generation watermarking technique is proposed, which works on the computational intelligence model to insert a large amount of robust watermark and make an extra effort to hide more information than first and second-generation techniques. The Advanced Encryption Standard (AES) encryption algorithm is employed to guarantee secure communication, which has a significantly less computational cost. The proposed technique evaluated parameters including security, robustness, imperceptibility, and capacity. The results of the proposed technique are compared to existing text watermarking methods, which illustrates it is secure, robust, imperceptible, and inserts a large amount of watermark information through computational intelligence.

Introduction

In the modern world, advanced technologies such as IoT make our daily life easy in many things. The development of IoT applications is emerging continuously and brings us economic benefits and unprecedented efficiency and accuracy. These technologies help us to share our data globally. On the other hand, it creates problems for original data owners and publishers. Data aggregation presents various security concerns, including data privacy, authentication, integrity, and several different attacks. Data aggregation helps to increase robustness and data accuracy.

Digital content requires full protection against illegal copying [1]. Steganography, cryptography, and watermarking techniques are used to solve copyright issues. Steganography was used at the end of the 15th century, and Herodotus used it back to 440 BC. Histiaeus found his most trusted worker, and shaved his head. They composed a secret message on him, waited until his hair grew, and then conveyed the message by sending him to his partners. At the receiver end, his head was re-shaved to reveal the message. Demaratus composed a note on the wooden surface of the wax composition tablet and then covered it with wax. Orange juice can also be used as an invisible ink for writing a secret message [2].

Cryptography is an art of protecting information by transformation through encryption in an unreadable format. Commonly, data that can be understood and read without any special measures is called clear text or plain text. The method of plain text conversion is called encryption. A secret key is used for encryption of text and data. Only the person who has a decryption key can extract the message. The reverse process of encryption is called decryption or verification. With the development of advanced technologies and widespread use of the Internet, the importance of security has increased. However, modern techniques of cryptography are almost unbreakable. In the past, cryptography techniques were used to protect confidential data, email messages, SMS, passwords, and credit card information.

Umair Khadam is with the University of Kotli Azad Jammu and Kashmir, Pakistan.

Muhammad Munwar Iqbal is with the University of Engineering and Technology Taxila, Pakistan.

Sohail Jabbar and Syed Aziz Shah are with Manchester Metropolitan University, UK.

Digital Object Identifier: 10.1109/IOTM.0001.2000010

In the recent decade, digital text has been the most common means of communication via the Internet. Websites, articles, books, newspapers, and legal document's major components are in simple plain text. Therefore, it is necessary to protect the text from copyright violations. Various techniques have been proposed in the past for audio, video, and images. However, these techniques are insufficient and ineffective for plain text. The process of embedding and extracting or verifying a watermark from a text document that uniquely identifies the copyright or original owner of the document or text is called a text watermark. Fragile watermarking provides secure data aggregation.

Digital watermarking has been used in the past for ownership verification and authentication. A secret message called a "watermark" is inserted into the original content. That is further used for verification of copyrights. Many watermarking techniques have been applied to images, audio, and video, but limited techniques are available for text. Recently text watermarking has received much attention because text documents are the dominant part of every private and public organization. The protection of digital texts has been seriously ignored in the past. Although it is part of the articles, newspapers, eBooks, legal documents, and magazines [3], digital watermarking can be used in many real-world applications. Authorized documents that include certificates, business plans, articles, poems, books, and corporate documents can be protected through watermarking [4]. Digital watermarking consists of two parts. The first part is called watermarking embedding, the second part is called extraction. In the first phase, watermark information (secret information) is embedded in digital content without disturbing the imperceptibility. It means that watermark information cannot be seen by human eyes. After embedding the watermark, digital content is made publicly available. It is also called watermarked content. The second phase is called the watermark extraction or verification process. In this phase, the watermarked content is used as input, where the watermark is extracted and compared with the original watermark [5].

Computational Intelligence is a well known paradigm that is currently gaining popularity in information hiding. Due to its ability to improve the complex problem, such as Genetic Algorithms, Artificial Neural Network (ANN), and Evolutionary Computing. Swarm intelligence algorithms also include Ant

Colony Optimization and Swarm Optimization. Digital watermarking based on computational intelligence is a very hot topic for researchers. Computational intelligence is a sub-branch of Artificial Intelligence (AI). In digital watermarking, computational intelligence is applied to enhance the performance of data privacy.

The applications of watermarking can be used for authentication, copyright protection, copy control, tamper detection, and forgery detection. Both paper and electronic copies of text documents are part of all public or private organizations. Therefore, the protection of these documents is a challenging task in the current domain of the Internet of Things (IoT). Limited techniques are available for ownership verification and copyright protection in IoT [6].

Authentication: The plain text in articles and newspapers highlighted various problems with authentication. Watermarking is a verification tool to authenticate the integrity of the plain text. If the watermark information is perceived, then it is a genuine document. Otherwise, the text has been tampered and cannot be authenticated. To detect any tampering, the authentication mechanism can be used for a text document. If tampering is identified, then the document cannot be considered as original or legal. A watermark is embedded into the original content that evaluates the authentication. If the content is altered or changed, then it is considered as not valid or authentic.

Copyright Protection: Copyright protection is one of the most important applications of digital watermarking. Watermarking is also used in the protection of digital content, like e-books, web content, research papers, poetry, and other documents. The author inserts a watermark in the document for copyright, and this watermark is extracted in the future from the given document to prove ownership. An attacker can use different kinds of methods to manipulate the intellectual property of digital content, which includes text rephrasing, image cropping, modification in audio, and video segmentation. Digital watermarking is very helpful to settle the copyright issues in court.

Tamper Detection: Tamper detection is another application of digital watermarking, which is used to prevent unauthorized modification of digital content. Tamper detection is a challenging task in digital watermarking. Many text documents are available for users to read online, and these documents can be confronted with a series of attacks such as copying, unauthorized access, and redistribution. Tamper detection can detect and recover the tampered region from the digital content.

Copy Control: Watermarking can be used to prevent the illegal copying of digital content. Publishers are looking for more consistent ways to control the copying of their important documents. Likewise, they want their important documents to be available on the Internet for revenue generation. The watermark is also applied here to provide access control and stop illegal copying. In watermarking copy control limits the users from make further copies; only authorized users can make copies.

Forgery Detection: Text document reproduction and plagiarism are serious issues, and it is rapidly growing. Text watermarking is applied here to embedding a watermark in the original document before publishing online. Almost every private and public organization deals with text documents on a daily basis, and digital text watermarking can be applied here to control the forgery detection problem.

Researchers generally count three parameters while developing the watermarking system. However, digital text watermarking evaluation criteria can be classified into security, capacity, robustness, imperceptibility, and computational cost.

Robustness: The watermark contents are attacks in different ways before retrieving. The formatting attacks can damage or alter the original content. After applying different formatting attacks, the watermark remaining in the original content is a key issue while designing a system. Robustness means watermark information still survived after tampering. When a technique of watermarking is being designed, it is essential to include consideration of the future application and the equivalent number of attacks that are possible.

Imperceptibility: Imperceptibly is the primary and fundamental requirement, which means that the watermark is securely embedded into the document objects. The watermark information could not feel the audience, or the watermark should not affect the original text. The watermarked and original information should be similar, and the content should be perceptually equal. The quality of the content is also important while designing an imperceptible watermarking technique. After embedding the watermark information, the quality of the content should not degrade.

Capacity: Capacity indicates that the maximum bits of watermark information can be stored in the host document. If a technique can hold large hiding capacity without affecting the visibility, then it is considered. Typically, the capacity of any watermarking technique should be high. However, different applications have various capacity constraints. For example, comparing images and text, images have many features that could be modified for watermarking, while on the other hand, text has limited features that can be altered. It is a challenging task to hide a large amount of watermark information in text.

Security and Computational Cost: Security is also very important while designing a watermarking system. It states that the information of the author (watermark) is hidden from unauthorized users; they do not have access to detect the watermark. The watermark still existing and the payload still remaining covered is the definition of security. Unapproved and unauthorized parties are not capable of identifying the author's information. Text watermarking techniques are computationally less complex while designing for plain text. More computation power is required for text documents that occupy many pages. Authentication guarantees to the aggregator that the received data is valid. Privacy preservation means that the privacy of data is not disturbed during system communications and operations. In data integrity, the aggregator should detect malicious operations. Our main contributions in this research are listed as:

•An efficient third-generation watermarking technique based on coding is proposed for data privacy in IoT.

•We propose a computational intelligence model that makes an extra effort to hide more information.

•The proposed model can be applied to enhance the performance of data privacy and security. It also protects plain text and sensitive text documents against unauthorized access.

•The proposed technique is imperceptible, with the PSNR at 33.65 and the SIM percentage at 99.42. The length of the secret message is improved from 1576 bits to 9952 bits.

Theoretical Backgound

Text digital watermarking is an emerging field of research that was initially started in 1991. In the past, numerous techniques have been suggested for digital content authentication and copyright protection.

Line-Shift Coding: In the Line Shift Coding technique, the lines of text are shifted a few degrees vertically. For example, some text lines are turned up and down 1/300 inch for inserting watermark information. The proposed method is applicable to text documents.

Word-Shift Coding: In word shift coding, the locations of words in text lines are shifted horizontally. Both line and word shift coding methods are not robust. Optical Character Recognizer (OCR) can remove the spacing between the words and lines, and then the watermark information is also ruined.

Feature Coding: In the feature coding method, some features of the text are modified for watermarking. This method is applied to a bitmap image of a document [7]. Text features are inspected from the bitmap image, and those features are changed for embedding watermark information. A method is recommended in [8], based on quadtree partition that is

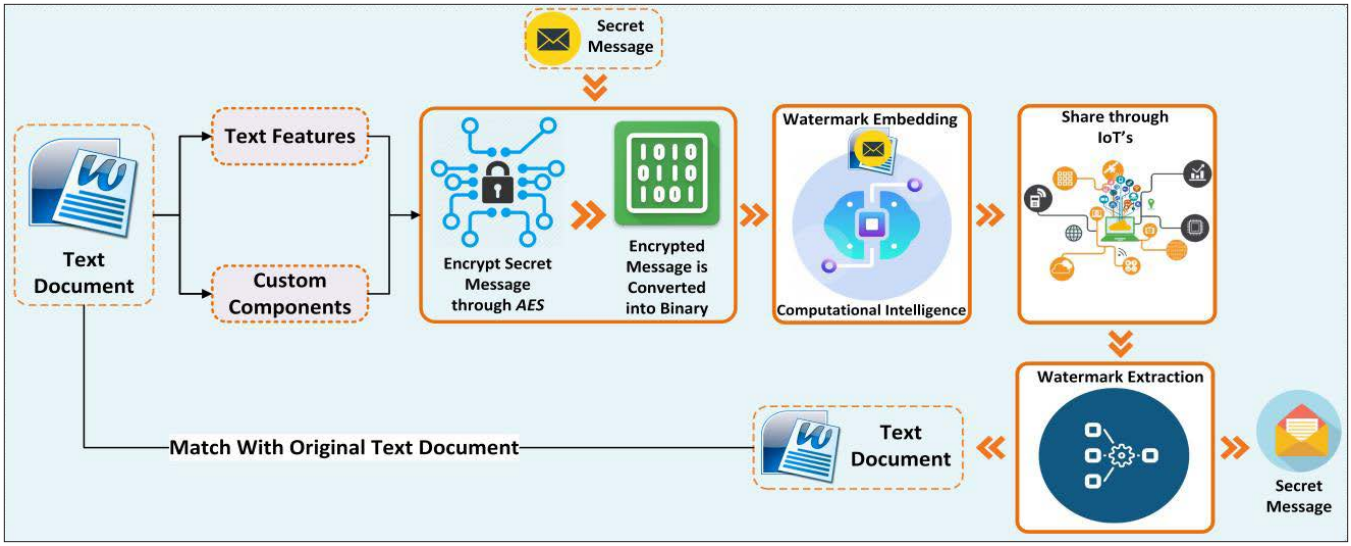

FIGURE 1. Proposed model for text watermarking.

applied for hiding data. The proposed algorithm compresses the extracted parts then converts them into binary string bits. Zero behind the numbers is ignored, and after that converting them into decimal values. The proposed technique is not robust and is inefficient in calculating the halftone image. A technique is introduced in [9] that reversed the border points of each character by using Fourier descriptors. The visual perception characteristics and nonsignificant graphical aspects are used for watermarking.

A text watermarking technique for Bangali and non-Roman alphabets is proposed in [10]. Special features of Bangali characters are represented through multiple options that are used for watermarking. The proposed technique is only applicable to the Bangali language and non-Roman alphabets. An algorithm is proposed in [11] which is based on the RGB (Red Green Blue) of the font color. The suggested method is imperceptible but cannot resist against formatting attacks. KF Rafat *et al*. [2] introduced a text watermarking scheme that exploits the flexibility of specific property attributes of a Microsoft Word document. An information hiding technique for Portable Document Format (PDF) is based on the justified text introduced in [12]. First, the secret message is compressed by Huffman coding. Some unique lines of PDF files are chosen to conceal the information. The embedding operation takes place by replacing the added spaces with the regular spaces of the host rules. Alghamdi *et al*. [13] presented a text steganography technique for the Arabic language. Markov Chain (MC) is implemented for encoder and decoder combined with Huffman Coding. The upper and lower bounds are also computed for the stego-text. The proposed technique is format-independent and less robust against attacks. Long *et al*. [14] proposed a coverless technique based on web text by which a large number of web pages are used to conceal the secret message. The mature search engines are applied to obtain the secret information that is associated with web pages. Motwani *et al*. [15] proposed a novel 3D multimedia approach to overcome the current challenges using Artificial Neural Networks (ANN). The proposed method uses an artificial neural network to select the vertices according to the geometry of the ring of vertices, which surrounds it and gives good results (visually and analytically) for different types of surface 3D models.

A security sensing strategy based on IoT policy is presented in [16]. The IoT policy rules and reporting history are used for data collection, which ensures the trustworthiness of the data and the IoT devices. Zhang *et al*. [17] proposed a scheme for data integrity in IoT that is based on fragile watermarking. The perception layer is used for data protection which contains thousands of sensor nodes. The proposed technique is lightweight and based on a random position strategy. The existing text watermarking techniques are not applicable for IoT nor considered as secure.

Proposed Technique

Our proposed solution is presented in this section as shown in Figure 1. The features of the text are used for embedding a watermark. In the first step, the text document is given as input to the system. Computational intelligence is applied to find the suitable features and components from the text document. In the second step, a secret message is taken as input. Advanced Encryption Standard (AES) is applied to the secret message for encryption. After encryption, the secret message is transformed into a binary string then into numbers. The intelligent agents embed the secret message into text documents imperceptibly. The novelty of this research is that we use the computational intelligence model to solve the optimization issues and insert high-density information. Computational intelligence techniques are explored to insert a higher amount of watermark. The goal of this research was to develop a system with the help of computational intelligence, that is robust and secure.

Data aggregation is applied to the documents to aggregate the same types of documents. The watermark information is in the form of the decimal embedded into the original document with the help of the Glyph Codebook. The Glyph Codebook is constructed using Microsoft Word font families, a lookup table constructed with a series of perturbed glyphs for the commonly used font of each character. The construction codebook aims to satisfy similar perceptually of glyph perturbation. It means the differences with the original fonts should hardly be perceptible to our eyes.

Embedding Watermark: The text document is loaded and finds the text indexes on the basis of decimal numbers. Spaces, commas, and full stop are removed from the original text. The first number is taken from the decimal array and finds that character on the basis of the decimal index. We always increase one in decimal numbers to handle the zero. To locate the lines from the text, the document is used to find the indexes of text.

The Original and Modified text looks the same and is not detectable to human eyes. The glyphs of characters are replaced in the Modified Version, which can be highlighted in Figure 2. A secret message or watermark is encrypted through a key in the first step, then converted into binary. The watermark, which is already in binary, is further transformed into a decimal number array. For example, we have a number array like [760127508....]. We add 1 to each number to handle the

zero. The spaces, commas, and full stop are removed from the plain text. The first number in the array is chosen, which is 7, after adding 1, the 8th position character is replaced with its glyph. The next number is selected from the number array, and after adding 1 it became 7 after adding the current number into the last value. The character at the 15th index is replaced with its glyph. This whole process is repeated until the completion of the array, and a watermarked document is generated at the end.

Extraction of Watermark: The reverse process of watermark embedding is called extraction or verification. The watermarked document is given as input and the extraction algorithm extracts the secret message and authenticates the document. Spaces, comma's and full stop are removed from the watermarked document. Perturbed glyphs are identified then return the indexes of perturbed glyphs. An array is used to store the indexes and subtract 1 from each index. The decimal array is converted to binary and then into characters. The encrypted message is decrypted using AES. On the basis of the secret message, the document is verified

Materials and Methods

In this section, the results of our proposed system are analyzed on the basis of digital watermarking evaluation criteria, which can be categorized into imperceptibility, capacity, and robustness. Robustness is a critical factor in digital watermarks, and it indicates that after applying various attacks, either 100 percent watermark information is restored or not. The brute force attacks (BFAs) are applied to the proposed technique to check the robustness through various kinds of attacks. These attacks include content and format-based attacks.

The Relative Letter Frequency Attack (RLFA) of the embedded message is calculated and then matches with the standard English relative letter frequency. The entire process is recurring for each character again and again for robustness assurance. This attack can be applied to all 26 English characters like 26 x 26 possible matches. In the letter extraction attack (LEA), the embedded watermark information is extracted by performing this attack. The probability of single letter extraction is analyzed in experiments using LEA. The brute force attacks are applied to the proposed technique to check the robustness through various kinds of attacks. These attacks include content and format-based attacks.

Imperceptibility belongs to the primary watermarking factor that means the watermark is invisible to human eyes. The audience could not feel the watermark information, and it could not affect the original contents of the document. Peak Signal to Noise Ratio (PSNR) and Similarity Percentage (SIM) are measured, respectively, to ensure the imperceptibility. The PSNR and SIM percentage on four categories of text samples, Short Size Text (SST), Medium Size Text (MST), and Large Size Text (LST) with ten experiments are examined. The highest PSNR value achieved with the proposed algorithm against SST is 33.73, and the SIM percentage is 99.20 percent. The PSNR against MST is 33.65, and the SIM percentage is 99.30 percent.

Original	Text documents are almost part of every organization, which are in the form of both paper and electronic documents such as soft degrees, birth certificated, banking documents, financial statements and legal documents. The challenge is to define a method which authenticates such documents and reliable.
Modified	Text documents are almost part of every organization, which are in the form of both paper and electronic documents such as soft degrees, birth certificated, banking documents, financial statements and legal documents. The challenge is to define a method which authenticates such documents and reliable.

FIGURE 2. Changed glyphs.

Pakistan, officially the Islamic Republic of Pakistan is a country in South Asia. It is the world's sixth most populous country with a population exceeding 212,742,631 people. In area, it is the 33rd largest country, spanning 881,913 square kilometres (340,509 square miles). Pakistan has a 1,046-kilometre (650-mile) coastline along the Arabian Sea and Gulf of Oman in the south and is bordered by India to the east, Afghanistan to the west, Iran to the southwest, and China in the far northeast. It is separated narrowly from Tajikistan by Afghanistan's Wakhan Corridor in the northwest and shares a maritime border with Oman.

FIGURE 3. The actual change in the watermarked document.

When considering LST, then PSNR is 33.78, and the SIM is 99.42 percent.

The Indexes in the document are highlighted and then replaced with character glyphs that are based on decimals of a secret message for watermarking. The changes in the watermarked document are exposed to indexes as present in Figure 3.

The embedding capacity is an essential aspect of the text watermarking evolution criteria. The embedding capacity indicates the number of watermarking bits concealed in the host content. Existing techniques can only hide a few characters in the host content. In the capacity analysis, twenty different text documents are used in the experiments. Figure 4 demonstrates the comparison of the proposed technique with existing methods. Twenty watermarked documents are compared with original documents. The ratio of the proposed system is improved as compared with existing techniques. Only two documents that are not matched with the original documents are shown in the proposed technique. The capacity ratio of existing method 1 is 20 percent. Method 2 can improve slightly, which is 30 percent and increases in method 3 by 40 percent. The capacity ratio of the proposed system is 80 percent. The robustness and imperceptibility of the proposed system are also improved as compared to the existing three methods.

The length of the watermark is calculated, including characters and words as shown in Figure 5. The proposed system can store 9952 bits of the secret data. The document has 61 lines, 621 words, and 4058 characters. The proposed method can embed 1244 characters.

Several experiments are done to check the capacity analysis of the proposed system. The embedding capacity of the

Techniques	Content and format-based attacks										
	Insert	Delete	Replace	Copy	Paste	Font Size	Font Color	Font Weight	Paragraph Alignment	Line and Paragraph Spacing	Text Highlight
Existing Method 1	✓	✓	✓	×	×	✓	×	×	×	×	×
Existing Method 2	✓	✓	✓	×	×	✓	✓	✓	×	×	×
Existing Method 3	×	×	×	×	×	✓	✓	✓	✓	×	×
Proposed Method	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓

TABLE 1. The comparison of proposed and existing techniques against content and format-based attacks.

proposed technique is improved. Through the experimental results, our proposed system achieves excellent results against all three parameters. The proposed system can be applied for copyrights and owner authentication of text documents. It can also protect the text documents against illegal use.

Conclusions

In this investigation, a secure data aggregation digital text watermarking technique based on computational intelligence is proposed for the data integrity of IoT. In our daily life, the Internet of Things (IoT) enables many advanced technologies such as smart cities, smart healthcare, and so on. Security has become a bottleneck restricting the further development of IoT. The data aggregation summarizes data and minimizes unnecessary data transfers via the communication channel. The glyphs of characters are used on the basis of character indexes for watermark embedding. The proposed technique can protect sensitive documents and plain text against unauthorized access and is also applicable for IoT. The experimental results prove that the proposed technology is robust, imperceptible, and improves the hiding capacity. The proposed system is imperceptible with PSNR of 33.65, and the SIM percentage is 99.42 percent. The length of the secret message is improved from 1576 to 9952 bits. The proposed system can be applicable to plain text authentication, copyright protection, tamper detection, copy control, forgery detection, and ownership verification. In the future, the PDF file will be investigated for watermarking in the IoT paradigm.

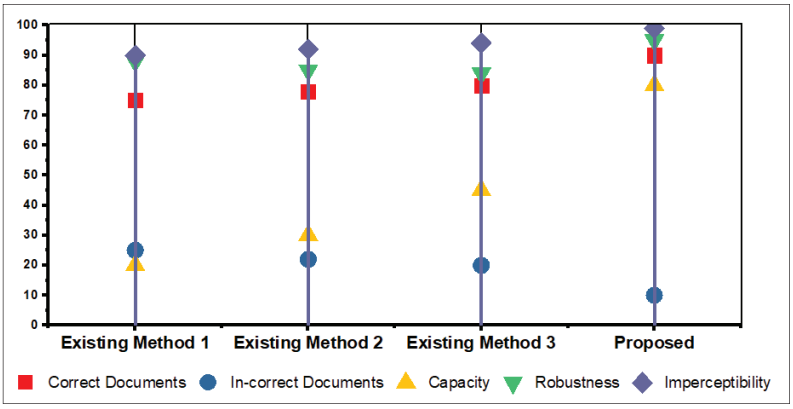

FIGURE 4. The analysis of the proposed system.

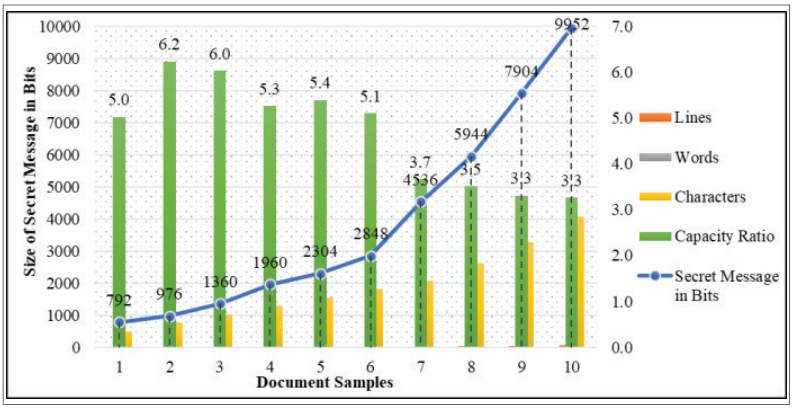

FIGURE 5. The proposed system capacity analysis.

References

[1] M. Zeeshan *et al.*, "A Review Study on Unique Way of Information Hiding: Steganography," *International J. Data Science and Technology*, vol. 3, no. 5, 2017, p. 45.

[2] K. F. Rafat and M. J. Hussain, "Secure Text Steganography for Microsoft Word Document," World Academy of Science, Engineering and Technology, *International Journal of Computer, Electrical, Automation, Control and Information Engineering*, vol. 11, no. 6, 2017, pp. 736–41.

[3] N. S. Kamaruddin *et al.*, "A Review of Text Watermarking: Theory, Methods, and Applications," *IEEE Access*, vol. 6, 2018, pp. 8011–28.

[4] U. Khadam *et al.*, "Digital Watermarking Technique for Text Document Protection Using Data Mining Analysis," *IEEE Access*, vol. 7, 2019, pp. 64955–65.

[5] M. M. Iqbal *et al.*, "A Robust Digital Watermarking Algorithm for Text Document Copyright Protection based on Feature Coding," in *Proc. 15th International Wireless Communications & Mobile Computing Conference (IWCMC)*, 2019.

[6] U. Khadam *et al.*, "Text Data Security and Privacy in the Internet of Things: Threats, Challenges, and Future Directions," *Wireless Commun. and Mobile Computing*. 2020.

[7] M. Ahmad *et al.*, "A Sustainable Solution to Support Data Security in High Bandwidth Health Care Remote Locations by Using TCP CUBIC Mechanism," *IEEE Trans. Sustainable Computing*, vol. 5, no. 2, April-June 2020, pp. 249–59.

[8] S. H. Soleymani and A. H. Taherinia, "High Capacity Image Data Hiding of Scanned Text Documents Using Improved Quadtree," arXiv preprint arXiv:1803.11286, 2018.

[9] L. Tan *et al.*, "Print-scan Invariant Text Image Watermarking for Hardcopy Document Authentication," *Multimedia Tools and Applications*, 2018, pp. 1–23.

[10] M. Khairullah, "A Novel Steganography Method Using Transliteration of Bengali Text," *J. King Saud University-Computer and Information Sciences*, 2018.

[11] Z. Hongbin *et al.*, "The Application of Multiple Texts Watermarking Algorithm in the Transmission of Power Information Security under the Internet," in *2017 IEEE Conference on Energy Internet and Energy System Integration (EI2)*, 2017.

[12] B. Khosravi *et al.*, "A New Method for PDF Steganography in Justified Texts," *J. Information Security and Applications*, vol. 45, 2019, pp. 61–70.

[13] N. Alghamdi and L. Berriche, "Capacity Investigation of Markov Chain-Based Statistical Text Steganography: Arabic Language Case," in *Proc. 2019 Asia Pacific Information Technology Conference*, 2019, ACM.

[14] Y. Long *et al.*, "Coverless Information Hiding Method Based on Web Text," *IEEE Access*, vol. 7, 2019, pp. 31926–33.

[15] M. C. Motwani *et al.*, "3D Multimedia Protection Using Artificial Neural Network," in *2010 7th IEEE Consumer Communications and Networking Conference*, 2010.

[16] W. Li, H. Song, and F. Zeng, "Policy-based Secure and Trustworthy Sensing for Internet of Things in Smart Cities," *IEEE Internet of Things Journal*, vol. 5, no. 2, 2017, pp. 716–23.

[17] G. Zhang *et al.*, "A New Digital Watermarking Method for Data Integrity Protection in the Perception Layer of IoT," *Security and Communication Networks*, 2017.

Biographies

Umair Khadam received the B.S. degree in computer science from the Department of Computer Science, the University of Azad Jammu and Kashmir, Pakistan, in 2011, and an M.S. degree in computer science from IQRA University Islamabad, Pakistan. He received a Ph.D. degree in computer science from the University of Engineering and Technology Taxila, Pakistan. He is currently a faculty member in the Software Engineering Department at the University of Kotli Azad Jammu and Kashmir, Pakistan. His research interests include digital watermarking, data mining, and the Internet of Things (IoT).

Muhammad Munwar Iqbal is working as an assistant professor in the Department of Computer Science, University of Engineering and Technology Taxila, Pakistan. He is the bearer of HOD responsibilities in computer science. His area of research is the Internet of Things (IoT), information-centric networking, ambient intelligence, wireless sensor, machine learning, databases, data science, data mining, semantic web, social media analysis and artificial intelligence (AI).

Sohail Jabbar received his Ph.D. degree from Bahria University, Islamabad, Pakistan. Currently, he is a postdoctoral fellow with the CfACS IoT Lab, Manchester Metropolitan University. He has served in different academic and managerial positions at National Textile University, COMSATS University Islamabad, and Bahria University in Pakistan. He has authored two book chapters and published more than 100 research articles. He has been engaged in many national and international level projects. He has been a guest editor of special issues in leading journals in his domain. He is performing collaborative research with renowned research centers and institutes around the globe on various issues in the domains of IoT, WSN, and Blockchain.

Syed Aziz Shah is an experienced academic with more than eight years of research and teaching experience in prestigious institutes, including the University of Glasgow, United Kingdom; Xidian University, China; Linkoping University, Sweden; and COMSATS University, Pakistan. He has done extensive research leveraging machine learning/deep learning (supervised and unsupervised) considering various programming tools, including MATLAB, Python, TensorFlow, Python, R, and Scikit. He has more than 20 publications in top ranked, multidisciplinary journals including IEEE and IET.