Integrated Digital Signature Based Watermarking Technology for Securing Online Electronic Documents

Sinan Q. Salih [1,*], Ravi Sekhar [2,*], Jamal Fadhil Tawfeq [3], Amer Ibrahim [4], Pritesh Shah [5], Ahmed Dheyaa Radhi [6]

[1] Department of Medical Instrumentation Technical Engineering ,Technical College of Engineering, Al-Bayan University, Baghdad, Iraq
[2,5] Symbiosis Institute of Technology (SIT) Pune Campus, Symbiosis International (Deemed University) (SIU), Pune, 412115, Maharashtra, India.
[3] Department of Medical Instrumentation Technical Engineering, Medical Technical College, Al-Farahidi University, Baghdad, Iraq.
[4] College of computer and information technology, American university in the emirates.
[6] College of Pharmacy, University of Al-Ameed, Karbala PO Box 198, Iraq

Emails: Sinan.salih@albayan.edu.iq; ravi.sekhar@sitpune.edu.in; jamaltawfeq55@gmail.com; amer.ibrahim@aue.ae; pritesh.shah@sitpune.edu.in; ahmosawi@alameed.edu.iq

Abstract

Even though the transmission and processing speeds of electronic documents have been vastly enhanced, electronic document information may be revealed, counterfeited, tampered with, or otherwise compromised. To maintain corporate success in the marketplace, network security should be essential to the protection of electronic documents. As a result, there is a rising demand for authentication and verification procedures for a variety of important documents, including those used in banking, government, and other transactions as well as certificates and other academic credentials. In recent years, there has been a fast growth of digital watermarking technology, which involves embedding invisible or hidden digital signatures into data without compromising the data's authenticity. Hence, in this paper, we utilize the watermarking technology in the encrypted data using dynamic wavelet transform algorithm to make a document more protected. Now the protected data is sent to cloud database for storage. Integrated digital signature algorithm (SHA-256 + DSA) is proposed in this research to generate digital signature for each document. When recipients download the data, the data is verified for its integrity after extracting the digital signature and encrypted data. This strategy improves record security. We also compare the suggested technique to standard practices and assess its performance based on a variety of indicators to demonstrate its effectiveness.

Keywords: Online electronic documents; watermarking technology; digital signature; dynamic wavelet transform algorithm; integrated digital signature algorithm (SHA-256+DSA)

1. Introduction

On a digital platform, organizations need information systems that make it simpler for them to manage the documents produced as part of their operations [1]. The introduction of electronic document management systems was assisted by the advancement of information and communication technology, which made it easier to move documents to digital platforms [2]. Information technology and the use of information system applications are increasingly required for firms to succeed. Systems for managing electronic documents (E-docs) are already widespread in a variety of enterprises. The digitization of documents utilizing computer systems and technology is made possible by an electronic document management system (EDMS) to satisfy business demands [3]. This makes it simple for many organizations employing an extensive EDMS to handle all information generated both internally

Doi: https://doi.org/10.54216/FPA.140111
Received: June 16, 2023 Revised: September 14, 2023 Accepted: November 17, 2023

and externally. Therefore, this approach still performs better than institutions that provide services using conventional ways of information management in terms of production/service and efficiency. Institutions use EDMS to store documents securely and enhance operational procedures [4]. Many advantages of EDMS include increased production/service and efficiency, less mistakes, higher service quality, and lower communication costs. However, even if EDMS has numerous advantages for its consumers, it has also made it crucial to implement the new technical framework. Every institution must successfully install an EDMS since these programs expedite business operations and make users' lives easier. The research community has been interested in the possible advantages of electronic documents, such as administration of personal or organizational information, online client access, and easier exchange of organizational data as depicted in figure 1.

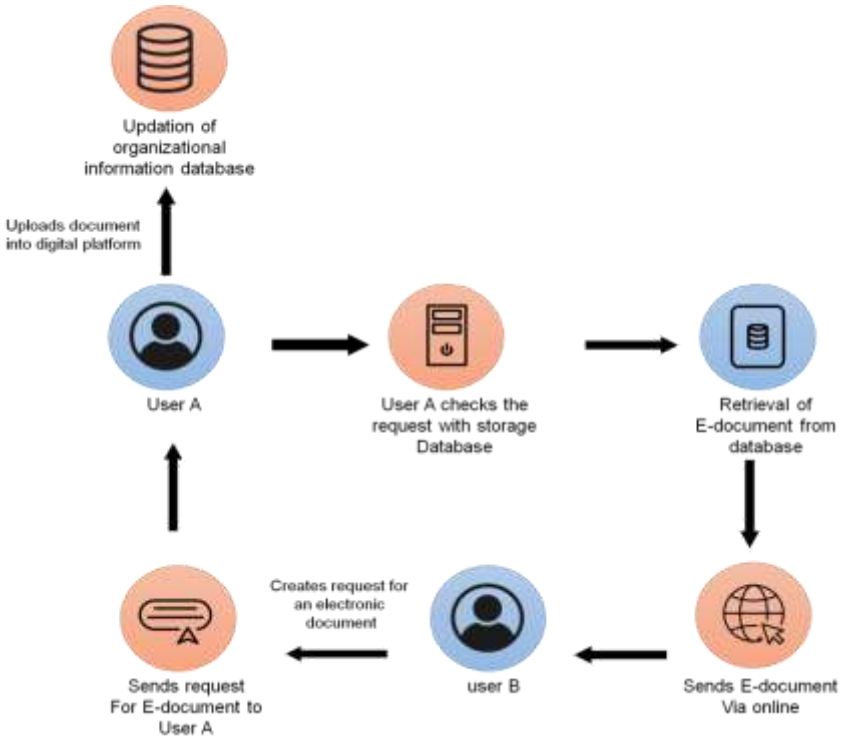


Figure 1: Exchange of electronic document between two users

Electronic documents are transmitted and accessed through the network [5]. This digital advantage also poses a risk since adjustments or modifications are not always visible to the data owner. E-documents in public channels are susceptible to malicious assaults, raising issues with information security as depicted in figure 2. Attacks against E-documents can take many different forms, such as replay attacks (transmission of valid data is maliciously delayed or repeated), man-in-the-middle attacks (where an attacker intervenes in a conversation between two users, giving the impression that a normal information exchange is taking place), and impersonation attacks (where an attacker poses as a legitimate sender to mislead the recipient into clicking on a malicious link, compromise attacks (accessing or modifying the original data context, and Masquerade attack(gaining unauthorized access to information by using fake identity). These cyber-security attacks raise concerns about the accuracy of electronic documents. The privacy and security of electronic documents are difficult to maintain in the modern digital age. The substantial attention in information security has been focused on the different aspects like confidentiality, data availability, and integrity. Research on strategies to ensure the reliability of electronic documents is being carried out in various professional sectors. Digitally signing electronic documents is now one of the options that are most often offered. To prove the integrity and validity of electronic documents, encryption and the digital signature are increasingly used. It may be possible to use this method to guarantee the accuracy of electronic records.

Doi: https://doi.org/10.54216/FPA.140111
Received: June 16, 2023 Revised: September 14, 2023 Accepted: November 17, 2023

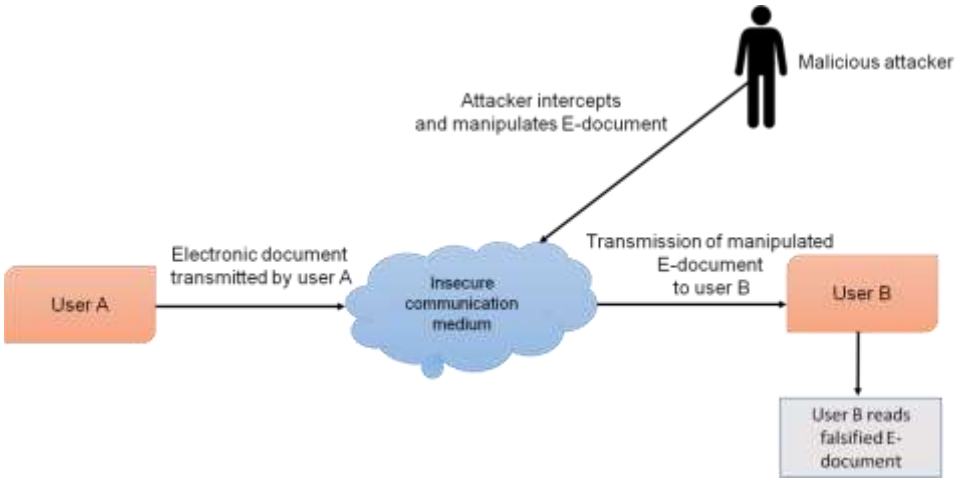


Figure 2: Insecure transmission of electronic documents between two users

2. Related works

The study [6] suggests a method of encrypting digital images inside electronic documents. The primary notion is that by adding digital watermarks to the images in this document, the authorship of the electronic document may be safeguarded. The paper considers three cases utilizing the suggested methodology: complete copies of electronic documents, copies of images within the document, and copies of text. It is shown that authorship confirmation can be effectively done in all three scenarios. Watermarking is a kind of steganography used by both electronic and paper document users. The only thing a watermark can provide is that the document is legitimately owned, not that it can't be used or altered in any way. Numerous people employ the steganographic technique of watermarking on both digital and paper materials. Adding a watermark to a document does not protect it from being copied or altered in any way; it just proves that the owner is legitimate. To increase the security of the owner's documents, a digital watermark might be established. Watermarking involves concealing a label by introducing datum bits into the image segment using a technique called "Singular Value Decomposition (SVD)". Videos, images, texts, and sounds are all examples of watermark domains. Utilizing the technique of SVD, numerical watermarking applications may be created [7].

The article [8] introduces a new approach to dual watermarking by combining the "Discrete Wavelet Transform (DWT)", "Singular Value Decomposition (SVD)", and "Set Partitioning In Hierarchical Tree (SPIHT)" structure. The approach employs a second-level DWT to decompose the host image into a variety of frequency components. Then, we apply the SVD transformation to the selected wavelet subcomponent. Both the logo watermark and the signature watermark are encrypted using Arnold transform and hamming code, respectively, prior to embedding. As a last step, we use an embedding technique to include both encoded watermarks into the host image after its transformation. Regarding the safety of electronic documents, article [9] suggests a watermarking method based on a combination of encryption and compression. This method provides a useful resource for safeguarding sensitive information, enforcing intellectual property rights, and maximising the efficiency of the system's compression capabilities. Using data mining, the study [10] offer a digital watermarking method for safeguarding intellectual property in documents and establishing authorship. Data mining methods are used to extract useful information from the document, which is then used to insert a watermark. The suggested technique safeguards text documents on both the traditional computer model and the more modern cloud-based model against infringement. Twenty unique text documents are utilised to conduct many attacks, including formatting, insertion, and deletion, in order to evaluate the suggested method.

The study [11] suggest a safe electronic health record (EHR) program based on essential element crypto algorithm and smart contract innovation to ensure privacy, verification, authenticity of medical information, and allow fine-grained security controls. Blockchain transactions provide extra details about the sender and receiver and are broadcast openly on the blockchain network. Everyone has a public address on the blockchain that powers bitcoin, and anybody can see the money they have previously put there. Users cannot remain anonymous on the network in this manner. The article [12] provide a lightweight privacy-preserving ring signature system (LPPRS) that is appropriate for anonymous transactions by genuine users while maintaining user anonymity and authenticity. On the one hand, a minimal digital signature ensures that data hasn't been changed, as if it were sealed with a tamper-proof seal that would be compromised if the data's contents were changed.

Doi: https://doi.org/10.54216/FPA.140111
Received: June 16, 2023 Revised: September 14, 2023 Accepted: November 17, 2023

By effectively managing the medical resources, IoT, when integrated with a cloud server, enhances patients' quality of life while reducing time and expense. Sensitive patient information is often compromised, however, because of the existence of malevolent individuals. The paper [13] presents a highly secure approach for medical IoT devices utilizing "Lamport Merkle Digital Signature (LMDS)" that is motivated and driven by these criteria. The study [14] suggested a system that incorporates a blockchain-based scheme that maintains confidentiality and privacy (CP), and it functions in two stages simultaneously. Elliptic curve cryptography (ECC)-based digital signature architecture is used in the first step. A two-step authentication structure is then suggested in the second phase to protect the ecosystem from potential attack points. To guarantee the validity, non-forgery, non-reuse, inalterability, and irrevocability of electronic documents, the study [15-20] introduced a cryptography based on elliptic curves to enhance document security systems through the digital signature.

3. Proposed methodology

This section discusses in detail about the integrated digital signature based watermarking technology for securing online electronic documents. When a sender uploads a document digitally, digital signature is generated for the document and the data in the document is encrypted. Watermarking of encrypted data is performed by Dynamic Wavelet Transform based document watermarking scheme. The digital signature is embedded into the watermarked document to obtain digitally signed E-document. This protected data is sent to cloud database for storage. When recipient sends a request for an electronic document to the user. When the legitimate recipient downloads the data, the data is verified for its integrity after extracting the digital signature and encrypted data. If the data is authenticated by the recipient, the data is then decrypted using the keys provided for recipient. After decryption, recipient reads the original data. Figure 3 shows the suggested security architecture for safeguarding online electronic documents.

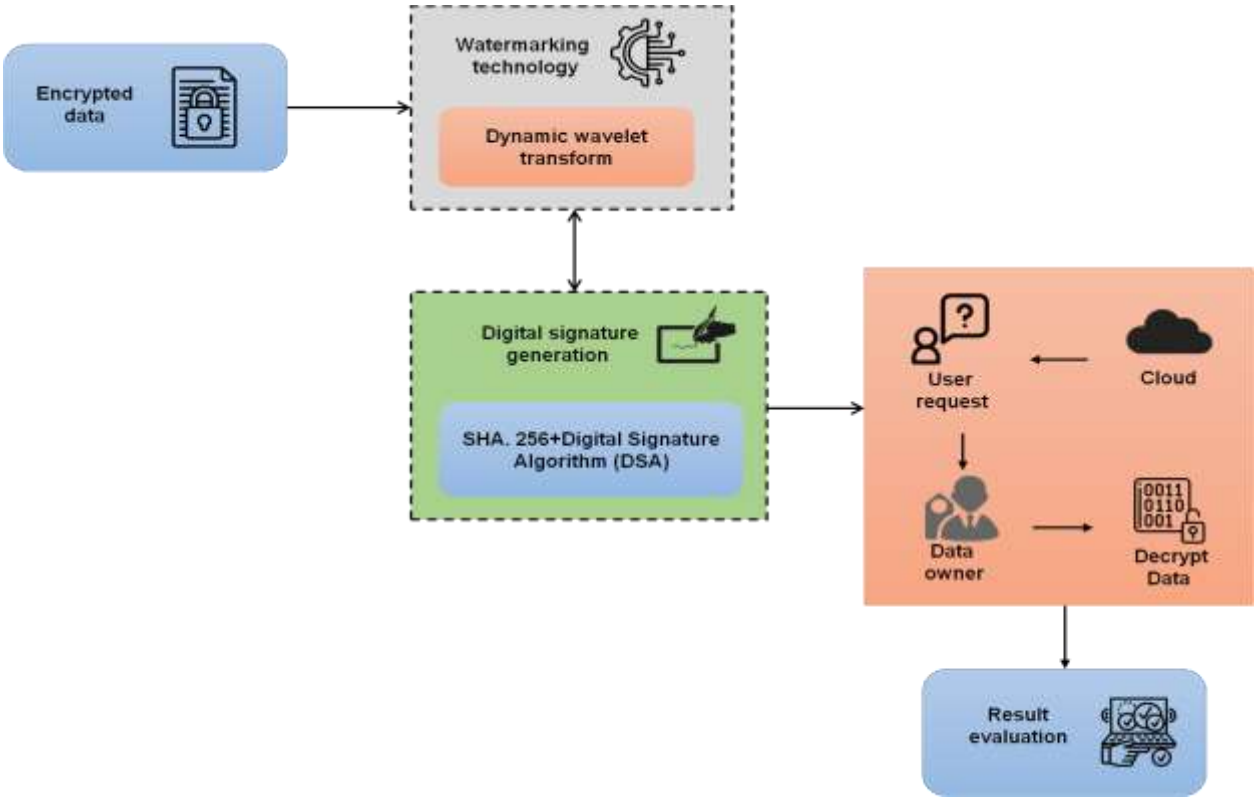


Figure 3: Flow of the methodology

A. SHA-256 Integrated Digital signature Algorithm (SHA-256+DSA)

The digital signature is assigned to each document uploaded by the user into the online platform. With the use of a digital signature, you may verify that the signed data has not been altered. A digital signature is a sort of electronic signature that may be used for any kind of electronic transaction. The digital signature process and outcomes are very different from other electronic signatures. Due to these variations, digital signatures are more useful for legal purposes. For signing and verifying, these require for the use of two keys, one private and one public. Signatures are produced and distributed by certifying authorities, a trustworthy entity that can be verified. The use of a cryptographic technique known as a digital signature can verify a significant number of these items. The digital

Doi: https://doi.org/10.54216/FPA.140111
Received: June 16, 2023 Revised: September 14, 2023 Accepted: November 17, 2023

signature of a document is an individual piece of data that is derived from both the document and the signer's private key. In most cases, a hash function and a private signing function are used to build it (with the signer's private key being used for encryption). Traditional digital signature techniques have the drawback that their signatures are as lengthy as or longer than the communications they are meant to authenticate. This becomes a serious problem when the messages are huge. Utilizing cryptographic hash functions in digital signature creation is one approach to addressing this issue. For signing, the sender selects pseudorandom number which should be less than the length of the text. A document's content, which might be of any length, is fed into a hash function, which in turn generates a message digest of a predetermined length. Any function that converts a sequence of bytes into a string of a certain length is considered a hash function. In this case, we hash the electronic document using SHA-256, which generates a 256-bit hash result.

B. Watermarking of Encrypted E-document by Dynamic Wavelet Transform based Document Watermarking scheme

After E-document encryption, encrypted E-document is sent to watermarking stage. Here The encrypted E-document in transformed into wavelet domain by decomposition of document by discrete wavelet transformation. The original encrypted document's watermark location is determined using the pseudo-random number. The resulting number serves as the sub-watermarking band's location. The random number is adjusted by multiplying it by the sub-size bands to make it suit the band's size. Calculate the mean value of the specified pixel in the document image for the nearby symbols. Algorithm 1 explains the process of proposed methodology.

Algorithm 1: Dynamic Wavelet Transform

```
At sender side
Begin
input: Watermark pdf (secret information), cover pdf
output: Encrypted information and Watermarked information
begin
begin enhanced DES
        x=read('cover.pdf')
begin image transformation
        imshow (x);
        y=save current figure
end
        encrypt y using EDES
        return encrypted y
end
begin RSA
        x1=read('watermark.pdf')
begin image transformation
        imshow (x1);
        y1=save current figure
end
        encrypt y1 using RSA
return encrypted y1
end
begin watermarking
        z = Load encrypted y;
        z1=Load encrypted y1;
        Split z and z1 into blocks
for each block in z and z1
        W= (z_b || z1_b);
end
        save gcf as pdf or .png image
end
        At receiver side
Begin
input: Watermarked pdf
output: decrypted cover and water mark pdf
begin de-watermarking
        Load watermarked data
                L=length(W);
```


Doi: https://doi.org/10.54216/FPA.140111
Received: June 16, 2023 Revised: September 14, 2023 Accepted: November 17, 2023

```
        While(i<L)
        for j=1:8
                index=(i-1)+j;
                b=W(index);
                if (b==1)
        bitchar=set(bitchar,j);
end
                if (bitchar==255)
                flag =1;
else
                b_index=(i-1)/8+1;
                bitword(b_index)=char(bitchar);
end
                return encrypted cover;
                return encrypted watermark;
begin
        begin enhanced DES
                x=read(‘ encrypted cover)
        begin image transformation
                imshow (x);
        y=save current figure as cover.jpg;
end
        decrypt y using EDES
return decrypted y
end
begin RSA
        x1=read(‘encrypted watermark)
begin image transformation
        imshow (x1);
        y1=save current figure
end
decrypt y1 using RSA
return decrypted y1
end
end
```

The watermark generated for the encrypted E-document is embedded into encrypted document to form watermarked E-document. After watermarking, digital signature is embedded into watermarked E-document to obtain digitally signed E-document. The framework for digital watermarking is depicted in figure 4.

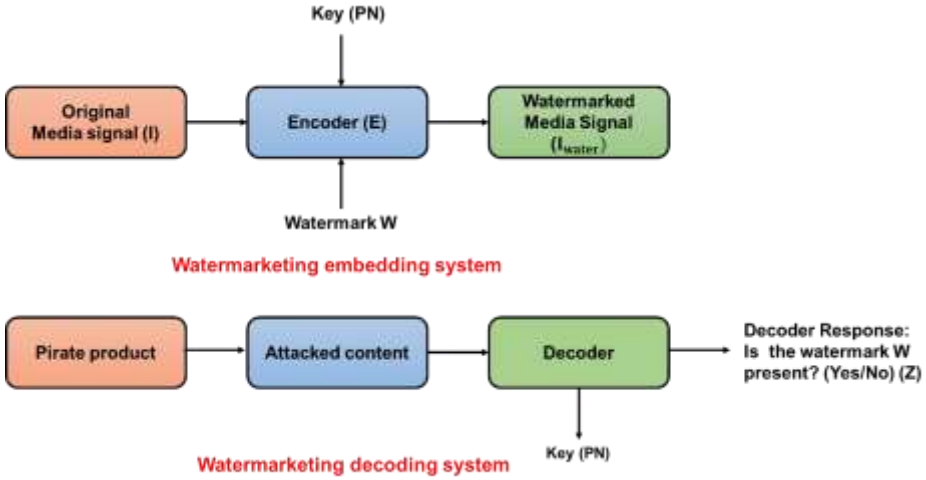


Figure 4: Framework of Digital watermarking

4. Result and Discussion

To watermark a digital image, watermark data must first be embedded into a multimedia output, where it may later be extracted or recognized by the watermarked result. These methods ensure the image is coherent, genuine, and

Doi: https://doi.org/10.54216/FPA.140111
Received: June 16, 2023 Revised: September 14, 2023 Accepted: November 17, 2023

unaltered. The ideal size for cover files is 256 pixels wide by 256 pixels high. Due to the availability of the original cover image at the time of detection, non-blind watermarking techniques are more reliable than blind watermarking methods. The original cover image is seen in figure 5a. The process of gently modifying a piece of data to incorporate metadata is known as watermarking. The watermarking image is shown in figure 5b. A watermarked image is embedded into the original picture during the watermark embedding process. The embedding of the watermark and the extracted cover image is shown in figure 5c and 5d.

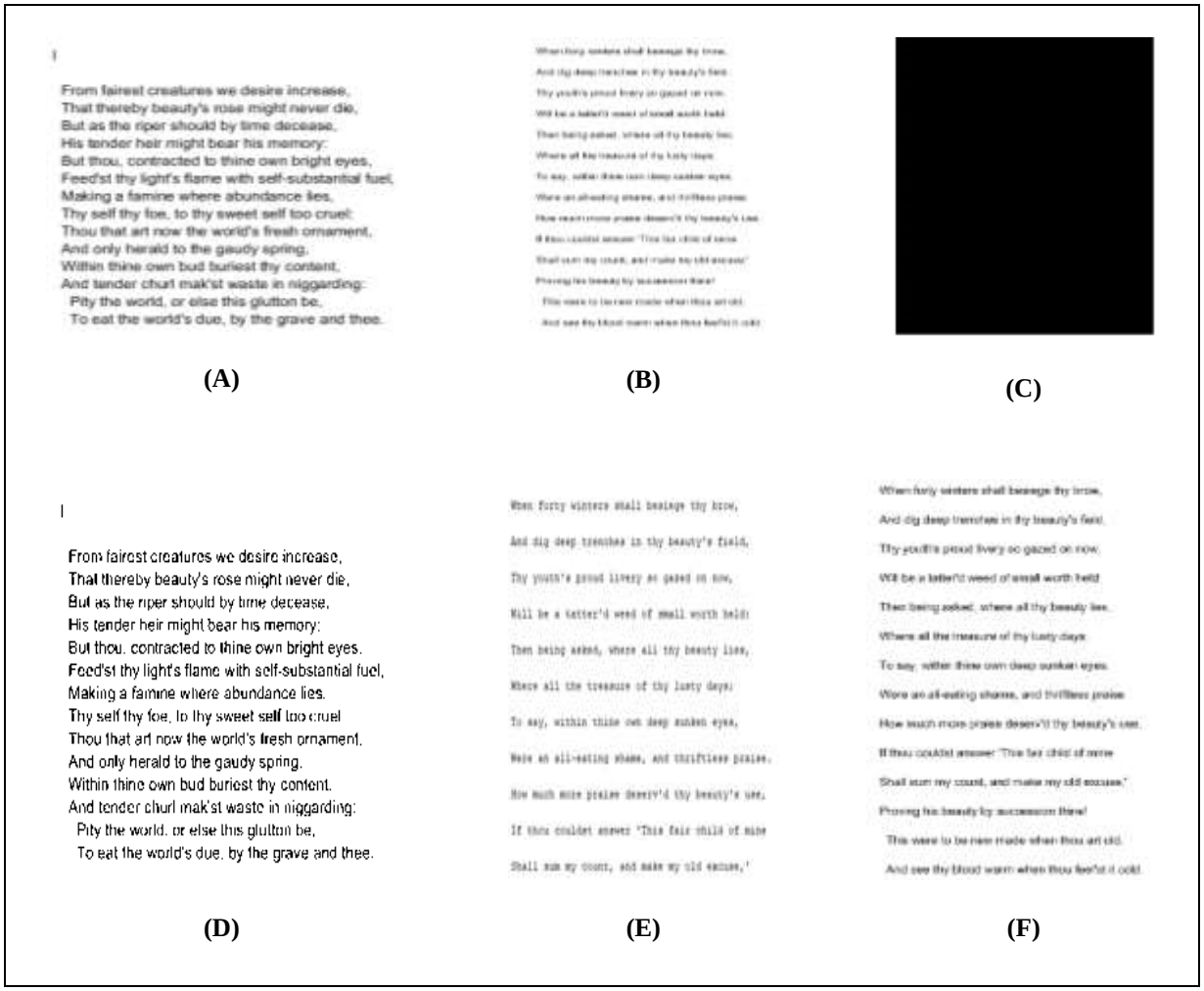


Figure 5: Digital watermarking process

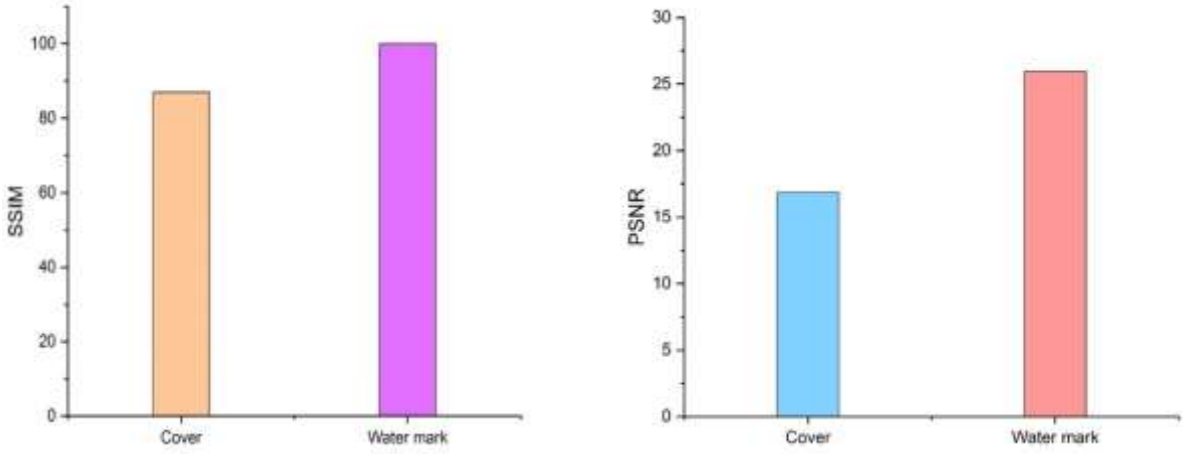
Digital image watermarking is the technique of adding hidden information, or a watermark, to a multimedia output so that it may be later read and used. Figures 3e and 3f show the decrypted water mark image extraction.

Table 1: Comparative Analysis

	SSIM	**PSNR**	**Size**
Cover	0.8725	16.845	The size is reduced to 5 kb to 49 kb
watermark	1.00	Inf because the size and SSIM is same	The size is remains same for both original and extraction

Extraction of a digital watermark image utilizing structural index similarity (SSIM) and signal-to-noise ratio (PSNR) as parameters. Comparative comparison of the cover and watermark images is shown in Table 1.

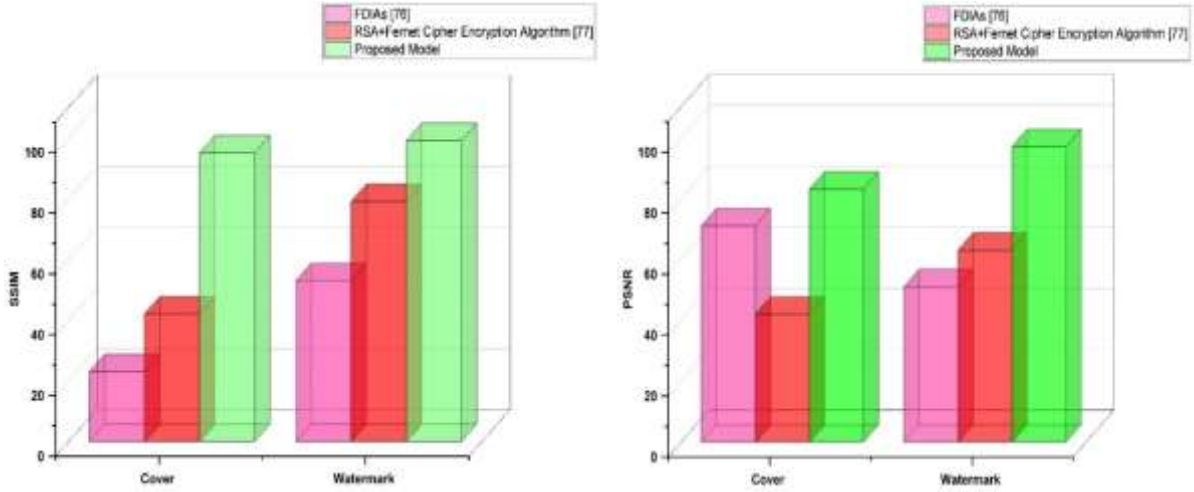
Doi: https://doi.org/10.54216/FPA.140111
Received: June 16, 2023 Revised: September 14, 2023 Accepted: November 17, 2023



(A) **(b)**

Figure 6(a) Comparison of SSIM and b) PSNR

The quality of the compressed or rebuilt image improves with a greater PSNR. The SSIM and PSNR comparison for the cover and watermark picture is depicted in figure 6(a) and figure 6(b). We have compared our suggested strategy with other approaches, including False Data Injection Attacks (FDIAs) and Rivest Sharmir Adleman (RSA) + Fernet Cipher Encryption Algorithm. Figure 7(a) and (b) compares the SSIM to the suggested and existing methods.



(A) (B)

Figure 7(a) Comparison of SSIM and (b) PSNR

5. Conclusion

The unique technique for strong database watermarking that has been suggested is particularly helpful for database copyright protection. It is less likely to be attacked since we are embedding the same watermark twice, and if it is, it will be quite simple to remove the original watermark because it is implanted twice. We can successfully extract one watermark from the two locations. Although it alters numerous characteristics of a tuple in a database, it may be more expensive in terms of data accuracy if we are considering comprehensive copyright protection. Since we are extracting the watermark as well as detecting it in the suggested manner.

References

[1] Rathore, M. S., Poongodi, M., Saurabh, P., Lilhore, U. K., Bourouis, S., Alhakami, W., ... & Hamdi, M. (2022). A novel trust-based security and privacy model for internet of vehicles using encryption and steganography. Computers and Electrical Engineering, 102, 108205.

Doi: https://doi.org/10.54216/FPA.140111
Received: June 16, 2023 Revised: September 14, 2023 Accepted: November 17, 2023

[2] Hurrah, N. N., Parah, S. A., Loan, N. A., Sheikh, J. A., Elhoseny, M., & Muhammad, K. (2019). Dual watermarking framework for privacy protection and content authentication of multimedia. Future generation computer Systems, 94, 654-673.
[3] Kiu, M.S., Lai, K.W., Chia, F.C. and Wong, P.F., 2022. Blockchain integration into electronic document management (EDM) system in construction common data environment. Smart and Sustainable Built Environment.
[4] Ali, O., Shrestha, A., Soar, J., & Wamba, S. F. (2018). Cloud computing-enabled healthcare opportunities, issues, and applications: A systematic review. International Journal of Information Management, 43, 146-158.
[5] Dagher, G.G., Mohler, J., Milojkovic, M. and Marella, P.B., 2018. Ancile: Privacy-preserving framework for access control and interoperability of electronic health records using blockchain technology. Sustainable cities and society, 39, pp.283-297.
[6] Melman, O. Evsutin, and A. Shelupanov, "An authorship protection technology for electronic documents based on image watermarking", Technologies, 8(4), p.79, 2020.
[7] S. Sinurat, and E.R. Siagian, "Application of the Concept of Singular Value Decomposition forthe Making of Watermark in Documents", Instal: Jurnal Komputer, 14(01), pp.24-30, 2022.
[8] C. Kumar, A.K. Singh, and P. Kumar, "Dual watermarking: An approach for securing digital documents", Multimedia Tools and Applications, 79(11), pp.7339-7354, 2020.
[9] Krishnamoorthy, S., Dua, A., & Gupta, S. (2023). Role of emerging technologies in future IoT-driven Healthcare 4.0 technologies: A survey, current challenges and future directions. Journal of Ambient Intelligence and Humanized Computing, 14(1), 361-407.
[10] U. Khadam, M.M. Iqbal, M.A. Azam, S. Khalid, S. Rho, and N. Chilamkurti, "Digital watermarking technique for text document protection using data mining analysis", IEEE Access, 7, pp.64955-64965, 2019.
[11] H. Wang, and Y. Song, "Secure cloud-based EHR system using attribute-based cryptosystem and blockchain", Journal of medical systems, 42(8), pp.1-9, 2018.
[12] A.D. Dwivedi, G. Srivastava, S. Dhar, and R. Singh, "A decentralized privacy-preserving healthcare blockchain for IoT", Sensors, 19(2), p.326, 2019.
[13] J.A. Alzubi, "Blockchain-based Lamport Merkle digital signature: authentication tool in IoT healthcare", Computer Communications, 170, pp.200-208, 2021.
[14] H. Ghayvat, S. Pandya, P. Bhattacharya, M. Zuhair, M. Rashid, S. Hakak, and K. Dev, "CP-BDHCA: Blockchain-based Confidentiality-Privacy preserving Big Data scheme for healthcare clouds and applications". IEEE Journal of Biomedical and Health Informatics, 26(5), pp.1937-1948, 2021.
[15] N.J.G. Saho, and E.C. Ezin, "December. Securing document by digital signature through RSA and elliptic curve cryptosystems". In 2019 International Conference on Smart Applications, Communications and Networking (SmartNets) (pp. 1-6). IEEE, 2019.
[16] Salih YK, See OH, Yussof S, Iqbal A, Mohammad Salih SQ. A proactive fuzzy-guided link labeling algorithm based on MIH framework in heterogeneous wireless networks. Wirel Pers Commun. 2014;75(4):2495–511.
[17] Tao H, Salih SQ, Saggi MK, Dodangeh E, Voyant C, Al-Ansari N, et al. A Newly Developed Integrative Bio-Inspired Artificial Intelligence Model for Wind Speed Prediction. IEEE Access [Internet]. 2020;8:83347–58. Available from: https://ieeexplore.ieee.org/document/9078735/
[18] Ali AM, Ngadi MA, Sham R, Al Barazanchi II. Enhanced QoS Routing Protocol for an Unmanned Ground Vehicle, Based on the ACO Approach. Sensors (Basel). 2023;23(3).
[19] Ali AM, Ngadi MA, Al Barazanchi II, JosephNg PS. Intelligent Traffic Model for Unmanned Ground Vehicles Based on DSDV-AODV Protocol. Sensors (Basel). 2023;23(14):1–13.
[20] Al-Barazanchi I, Hashim W, Ahmed Alkahtani A, Rasheed Abdulshaheed H, Muwafaq Gheni H, Murthy A, et al. Remote Monitoring of COVID-19 Patients Using Multisensor Body Area Network Innovative System. Al-Sarem M, editor. Comput Intell Neurosci [Internet]. 2022 Sep 15;2022:1–14. Available from: https://www.hindawi.com/journals/cin/2022/9879259/

Doi: https://doi.org/10.54216/FPA.140111
Received: June 16, 2023 Revised: September 14, 2023 Accepted: November 17, 2023