Nanotechnology Perceptions
ISSN 1660-6795
www.nano-ntp.com

An Analysis Of Blockchain-Based Hybrid Watermarking Techniques

M. Subashini[1] , P.V Ravindranath[2]

[1] School of Computer Studies, Bharathiar University, India
*E-Mail: subaphd1217@gmail.com **
[2] School of Computer Studies, Bharathiar University, India
E-Mail: ravindranath@rvsgroup.com

One kind of information masking used to stop illegal replication and distribution of multimedia data is digital watermarking, which masks important information in the original work. In a variety of ways, placing digital security watermarks to vital files may prevent loss of information, misuse, and unlicensed sharing. It is necessary to maintain the trade-off between imperceptibility, robustness, ability, and security while building an efficient and reliable digital image watermarking system. This study provides an analytical evaluation of the digital image watermarking using hybrid methods that are currently in use. After a quick examination of the literature, the levels of complexity of various existing hybrid approaches are compared. These approaches' limits and relevance are also discussed. Finally, the shortcomings of current approaches are summarized and closed the paper by suggesting future research possibilities.

Keywords Discrete Cosine Transform, Discrete Fourier Transform, Discrete Wavelet Transform, singular value decomposition, Blockchain.

1.INTRODUCTION

Every day, multimedia technology advances. As a result, the digital image can be easily changed, duplicated, copied, and circulated via communications across local networks and the Internet at a low cost and with immediate delivery without a decrease in quality. Images that are provided on the Internet are especially susceptible to such malicious attacks.

Digital watermarking can be used to prevent unauthorized data reuse as well as to protect copyright. The practice of adding a piece of information known as a watermark onto digital data by its owner is known as digital watermarking. Watermarks are classified into Visible Watermarks, Invisible Watermarks, Public Watermarks, and Fragile Watermarks [1]. First the digital watermark is embedded to the cover image. A threat arises when the transmitted media gets altered and this is known as a watermarking system attack. Protection is the process of extracting a watermark from a noisy signal that may have undergone media manipulation (JPEG compression, rotation, cropping, and noise addition).Watermarks can be visible or invisible. Visible watermarks, also known as transparent watermarks, are semi-transparent marks that are placed on the original image that show who owns the digital property. Invisible watermarks are also known as hidden or covert watermarks. As the name implies, these watermarks are invisible to the naked human sight. Various techniques based on either the spatial or transform domains, or both, have been proposed in recent years. The spatial domain defines the image as pixels.The watermark is embedded in the spatial domain by modifying the intensity and color value of specific preferred pixels.Transform coefficients are modified in the transform domain. The three most often used transformations are Discrete Wavelet Transform (DWT), Discrete Fourier Transform (DFT), and Discrete Cosine Transform (DCT).The hybrid technique combines two or three transformations while balancing imperceptibility, robustness, capacity, and security.

This research's contributions are

(i) The most relevant hybrid approach trends have been provided.
(ii) The limits of hybrid digital image watermarking approaches have been identified.
(iii) The issues that future learners must address have been highlighted.

2. LITERATURE REVIEW

A modified Pigeon method has been used in the Discrete Cosine Transform (DCT) based watermarking method to determine the optimal region in which to embed the watermark [2].This method requires minimal complexity for both embedding and extracting, is extremely imperceptible after the watermark is embedded, and is very resistant to various attacks.After that, inverse DCT is applied to obtain the watermarked image.In the other piece of work, the gradient is computed for each non-overlapping block that makes up a digital image [3]. Next, non-maximum suppression is used after convolution masks have been applied to determine the gradient's direction and magnitude. Lastly, using LSB, the watermark is embedded into the hysteresis step. Additionally, the chaotic substitution box scrambles the watermark signal to add an additional layer of security. The proposed method demonstrates high robustness against geometrical attacks and image processing. The other study proposes to use wavelet transforms along with convolutional neural networks (CNNs) to embed and extract watermarks by creating a watermarking network [4]. Maintaining performance, the network only consists of 11 layers; it is independent of the host picture resolution and can handle any kind of watermark. Two metrics are used to assess performance: the degree of similarity between the original and extracted watermarks, as well as the degree of similarity between the watermarked and host images.Consequently, the total BER has decreased. In order to embed information for the greyscale photographs, an invisible watermarking technique was presented in the next study [5]. This technique used a linear modulation algorithm to insert a stego-text into the least significant bit (LSB) of the Discrete Cosine Transformation (DCT) coefficient. when 1 bit/block is implanted, it is imperceptible. The other research suggests a deep neural network-based end-to-end document picture watermarking method [6]. The watermark is specifically intended to be embedded and extracted using an encoder and a decoder. To resemble the several types of attacks that could occur in real life, a noise layer is included. The embedding alteration on characters is limited by a text-sensitive loss algorithm. A method for adjusting the embedding strength is suggested in order to enhance the watermarked image's quality while maintaining minimal extraction accuracy loss. Next, using the principle of compression resistance, a strong embedding domain with theoretical basis and best invisibility is built [7]. Then, to maintain and enhance smooth parts and avoid changes visual quality, the embedding channel is chosen using the strong abstraction of an image and strong measurement. Based on this, a suggested approach is provided by combining STC codes with error-correcting to achieve message embedding at a minimal price while enhancing extraction accuracy. The suggested coding parameters to enhance message extraction integrity are then provided after the parameters have been discussed and chosen. Although these methods have numerous benefits, it is advised to utilize hybrid transformation methods because many attacks are not detected by a single transformation method.

An article attaches secret information to cover images while presenting a novel non-blind watermarking algorithm that makes use of the benefits of DFT, DCT, and SVD transforms [8]. The Fourier domain carrier picture is first broken down into four frequency sub images using onion peel decomposition (OPD), which is applied after DFT in the procedure. After applying DCT to the frequency bands, the plan arranges them zigzag to create four distinct frequency arrays. The watermarked image is created by embedding four copies of the watermark's singular value contents with the carrier image's singular value contents in the DFT domain during the last step of the embedding process. As a result, even in cases when potential attacks severely alter the watermarked images, high-quality watermarked images are nevertheless produced. The following study on a robust watermarking technique combines singular value decomposition (SVD), discrete wavelet transforms (DWT), and discrete cosine transform (DCT) [9]. The objective of this approach is to add an undetectable image watermark on a medical image. DCT and SVD are used to transform the cover medical image after it has been split up into the third level of DWT coefficients. The watermark image goes through the same process. The watermark's singular value is appended to the high-frequency sub bands' singular value in the cover image's third level DWT.An analytical analysis of the current hybrid digital image watermarking techniques was offered in the other publication [10]. The coefficients of transforms can be changed using discrete Fourier transforms (DFT), discrete wavelet transforms (DWT), or discrete cosine transforms (DCT). The hybrid method maintains a trade-off between imperceptibility, robustness, capacity, and security by combining any two or three transformations. According to the above synopsis, hybrid domain digital image watermarking techniques offer more security and are more reliable. They also offer greater imperceptibility. They are not without restrictions, though. HE + GN, HE + SPN, GN + JPEG compression, SPN + JPEG compression, and LPGF + SPN are examples of combination attacks that they cannot resist. Improved security against these combined attacks is offered by the more recent introduction of blockchain-based authentication and machine learning.

It is proposed to create a novel combination of blockchain-based encryption and invisible image watermarking [11]. The discrete wavelet transform (DWT) coefficient's edge detection (ED) is used to implement the watermarking. The L level DWT transform is used for decomposing the medical image to produce multi-resolution coefficients.When embedding a watermark, edge coefficient and difference of dilation are applied to improve robustness.For medical images, a blockchain-based hash technique is used to encrypt the watermarked image. While decryption is accomplished at the decoding end, the image is rebuilt.The hybrid watermarking approach and encryption are combined in the other study to protect 3D multiresolution meshes [12]. The three components of the new crypto-watermarking system are as follows: in the first step, known as watermark preparation, the copyright information associated with the logo is encrypted using the RSA algorithm, and a convolutional encoder is then used to encode the encrypted logo. The next phase, known as mesh preparation, is breaking down the 3D multiresolution mesh using the wavelet transform to produce a wavelet coefficient vector. The third and last step, known as hybrid watermarking, involves inserting an encrypted logo and RSA keys into the mesh's spatial and multiresolution presentations.Watermark data is securely stored on blockchain, which also offers timingstamp verification for several watermarks to verify the order of creation [14]. The watermark information in an image can be verified without the primary image by using the perceptual hash function to obtain a hash value derived from the picture's structural data. To increase the robustness and magnitude of digital watermarking, QR code images are created by utilizing QR code with copyright information and image hash as watermark images; IPFS is used for storing and distributing watermarked images decentralized from a central server. This approach can improve the copyright protection capabilities of digital watermarking technology.a blockchain-watermarking system that successfully integrates blockchain, multimedia watermarking, compressed sensing, and Interplanetary File System (IPFS) technologies to protect the integrity, privacy and availability of compact sensed images [15]. The blockchain guarantees the watermark's security. Compressive sensing hides the original content of images, and the encrypted domain is where watermarking is performed. The blockchain watermark may identify and locate the modified area on the compressive sensed images.

3. CONCLUSION

Image authentication is a difficult operation because of Internet traffic. Image enhanced data embedding capacity, data security, robustness and imperceptibility are essential to be ensured. While there are many advantages to techniques such as DCT, DWT, and DFT, such as robustness and imperceptibility, it is advisable to use hybrid transformation methods because many attacks are not detected by a single transformation method. The digital image watermarking using hybrid domain techniques offer enhanced imperceptibility with strong security and are more reliable. Despite these advantages, they are unable to resist the combined attacks. Blockchain technology and machine learning can be applied to solve the challenges of combined attacks in order to overcome this.

REFERENCES

[1] Anuja Dixi, Rahul Dixi, “A Review on Digital Image WatermarkingTechniques”, I.J. Image, Graphics and Signal Processing, vol (4), 56-66, 2017.

[2] MuathAlShaikh, MalekAlzaqebah, Sana Jawarneh, “Robust watermarking based on modified Pigeon algorithm in DCT domain”, Multimedia Tools and Applications (82) 3033–3053, 2022.

[3] Zaid Bin Faheem, Abid Ishaq, Furqan Rustam, Isabel de la Torre Diez, Daniel Gavilanes, Manuel Masias Vergara, Imran Ashraf, “Image Watermarking Using Least Significant Bit and Canny Edge Detection”, National Library of Medicine, 2023.

[4] Alireza Tavakoli, Zahra Honjani, HediehSajedi, “Convolutional Neural Network-Based Image Watermarking using Discrete Wavelet Transform”, International journal of information technology (2021-2029), 2023.

[5] Waleed Alomoush , Osama A. Khashan, Ayat Alrosan, Hani H. Attar, Ammar Almomani, FuadAlhosban and Sharif Naser Makhadmeh, "Digital image watermarking using discrete cosine transformation based linear modulation", Journal of Cloud Computing: Advances, Systems and Applications, 2023.

[6] Sulong Ge, Zhihua Xia, Jianwei Fei, Xingming Sun, and Jian Weng, "A Robust Document Image Watermarking Scheme using Deep Neural Network" JOURNAL OF LATEX CLASS FILES, NO. 9, 2022

[7] Yi Zhang ,Xiangyang Luo , Jinwei Wang , Yanqing Guo, Fenlin Liu, "Image robust adaptive steganography adapted to lossy channelsin open social networks", Information sciences pages (306-326), 2021.

[8] Justin Varghese , Omer Bin Hussain , Saudia Subash and Abdul Razak T, "An effective digital image watermarking scheme incorporating DCT, DFT and SVD transformations, Journal of Engg. Research (113-130), 2023.

[9] Imane Assini1, Abdelmajid Badri, Khadija Safi, Aicha Sahel, Abdennaceur Baghdad, "A Robust Hybrid Watermarking Technique for Securing Medical Image", International Journal of Intelligent engineering * Systems, 2018.

[10] Mahbuba Begum, and Mohammad Shorif Uddin, "Analysis of Digital Image Watermarking Techniques through Hybrid Methods", Hindawi Advances in Multimedia, 2020.

[11] Praveen Kumar Mannepalli, Vineet Richhariya, Susheel Kumar Gupta, Piyush Kumar Shukla, Pushan Kumar Dutta, "Block Chain Based Robust Image Watermarking Using Edge Detection And Wavelet Transform, Research Square, 2021.

[12] Ikbel Sayahi, and Chokri Ben Amar, "Robust and Hybrid Crypto-watermarking Approach for 3DMultiresolution Meshes Security", International Conference on Software Technologies (398-407), 2021.

[13] Himanshu Kumar Singh and Amit Kumar Singh, "Comprehensive review of watermarking techniques in deep-learning environments, Journal of Electronic Imaging, 2023.

[14] Meng Z., Morizumi T., Miyata S., & Kinoshita H., Design Scheme of Copyright Management System Based on Digital Watermarking and Blockchain", IEEE 42nd Annual Computer Software and Applications Conference (COMPSAC), 2018.

[15] Ming Li , Leilei Zeng , Le Zhao, Renlin Yang, Dezhi An , and Haiju Fan, "Blockchain-Watermarking for Compressive Sensed Images", Institute of Electrical and Electronics Engineers, 2021.