ISSN: 2633-4828 Vol. 6 No.1, January, 2024

International Journal of Applied Engineering & Technology

A RESILIENT DIGITAL WATERMARKING APPROACH FOR DIGITAL IMAGES USING PROBABILISTIC NEURAL SYSTEM

Dr Lakshmana Rao Battarusetty[1], S.V.Chiranjeevi[2], A Venkateswarlu[3], Mutyalaiah Paricherla[4], M Sujana[5] and P Chandrakala[6]

[1]Associate Professor, Department of CSE, NBKRIST, A.P, India

[2, 3,4,5,6] Assistant Professor, Department of CSE, NBKRIST, A.P, India

ABSTRACT

The Digital data and information can be distributed more easily due to the rapid expansion in the use of individual computers, the internet, and digital multimedia technologies. The accessibility of a widespread assortment of image processing tools, however, makes it easier for such data to be used improperly. Digital data can be easily copied, deleted, or modified by unauthorized users or attackers. The prevalence of unauthorized alteration and replication of digital data prompts the development of new methods for safeguarding the IPR of digital information. Watermarking has emerged as a key technique for achieving authentication and copyright protection. All the spatial and frequency domains of host data may incorporate a digital watermark. The present article presents a hybridized technique that syndicates discrete wavelet transformation and singular value decomposition.

Index Terms Digital Image Watermarking, DWT, Intellectual Property Right, Multimedia Security, Hybridized Digital Watermarking, Robust Watermarking, Singular Value Decomposition (SVD)

1. INTRODUCTION

Information obscuring techniques are one of numerous approaches that academics have presented in the literature to address the problem of unlawful data change and reproduction. cryptography, Steganography and watermarking are the three classes into which information concealment techniques fall. Out of the three approaches mentioned, watermarking has been demonstrated to be a more effective way to conceal data. This is the case that steganography conceals information so that only the intended recipient is aware of its existence. Before being transmitted, data in cryptography is transformed into an encrypted code. This is caused by the restriction that requires the user's encryption key in order to interpret the communication.

In the 13th century, watermarks were initially used in Italy as identification marks incorporated into paper products. In 1992, A Tirkel and Ch Osborne introduced the phrase "digital watermarking." Digital watermarking remains the act of adding a watermark—a piece of text, image, or logo—inside of the source digital data—an audio file, an image, or a video—without significantly compromising the host data's visual quality. A digital signature, a randomly generated pattern, a binary logo, or certain biometric characteristics can all be used as watermarks. Digital watermarking's primary purpose is to provide copyright protection and authentication. Robust watermarking is incorporated into applications that require copyright protection, while fragile watermarking is employed in applications that require copyright authentication. While fragile watermarks disappear when subjected to certain targeted or unintentional attacks, robust watermarks display the sustainability characteristic in original information even after projected or unintentional attacks [14]. In the watermarking process, the two most important steps are extracting the watermark from the created image and integrating the watermarked image into the cover image.

The watermark to be embedded and the host data in which the watermark will be implanted are the two inputs used in the watermark embedding process. Throughout the extraction process, a detector is employed to recover the watermark from the received data and determine if it is there or not [1-2]. This document is designed as surveys: Section 2 provides a quick explanation of the key appearances of digital watermarking and the fundamental structure of the system. Section 3 reviews an outline of the latest the FD based watermarking algorithms. In section 4, DWT - SVD based watermarking was extensively introduced. In the current research, the

effectiveness of the implanted procedure has been weighed in terms of SSIM, MSE and PSNR. The performance of the approach is demonstrated by the simulation consequences provided in Section 5. Section 6 then brings the article to a conclusion.

2. Elements and the overall structure of a digital watermark

2.1 Elements of the digital watermark

The following section discusses the key components of the general watermarking system.

a. Payload

It is a fundamental feature of all digital watermarking schemes. The phrase "data payload" signifies the quantity of the bits that a digital watermark encrypts in a certain amount of time. An M-bit watermarking system, for illustration, is a watermark that may encode M bits in a unit of time [4]. Numerous applications need different types of data payloads [4].

b. Robustness

The resilience of a watermarking approach is the ability of an implanted watermark to resist geometric attacks and image processing. A few examples of Spatial filtering, copying, cropping, scaling, translation, compression, and rotating are some examples of these attacks; they can occur accidentally or intentionally [3–4].

c. Security

Preferably, the watermark should be kept hidden and indiscernible to outsiders. The watermark's capacity to remain undetected by unauthorized parties is referred to as its security. The watermark's security determines how resistant it is to attacks [2, 5].

a. Imperceptibility

The imperceptibility of an image is a measure of the extent to which it’s content and the watermarked image is identical [2-4]. The fundamental prerequisite for every watermarking technique is perceived transparency. Every digital watermarking application involves inserting a watermark onto the cover image, which alters the host image's perceived quality. It is always preferred that a watermark be added to a message image in a way that prevents the image's perceived quality from gradually declining.

b. Cost

In the present instance, "cost" refers to the computational expense of the comprehensive watermarking method, which includes both watermark extraction and picture embedding.

c. fragility

If a watermark may be easily altered by unauthorized individuals, it is considered fragile. The smallest attempt to alter a delicate watermark renders it undetectable. Applications that require copyright protection use this type of watermark [14].

2.2 Digital Watermarking: A Broad Overview

There are two fundamental procedures in the digital watermarking technique:

- ✓ Integrating information to be employed as a watermark on the host image
- ✓ The removal of the watermark present in the watermarked cover image.

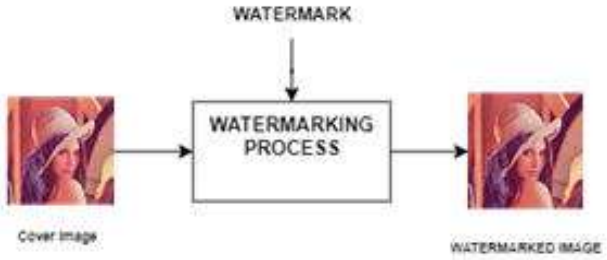


Fig.1. Demonstrates the universal structure of the digital watermarking process.

The visual appearance of the cover message and the message to be watermarked or encoded in the host image are the two primary parameters of the embedder unit. A randomly generated sequence, a digital signature, particulars extracted from the host image, biometric characteristics, a bit combination, a logo, or a few words appended to the host communication image may all be employed as a watermark message [2-3, 9]. After that, the watermarked image is sent or captured. The extractor unit, which looks for a watermark, can be used to retrieve the implanted message from the watermarked cover image.

3. Synopsis of transform domain watermarking

In the DCT area, I.J. Cox et al. (1997) suggested an algorithm for non-blind image watermarking [1]. This involves implanting the watermark into an image's most significant magnitude DCT principles. Because these DCT coefficients can withstand a variety of image processing attacks, the simulation result demonstrates great robustness. However, the provided approach is not suitable for numerous scenarios since it is not blind. Two DCT domain approaches that embed one or more watermarks have been suggested by Wen-Nung Liet al. (2000) [6]. The watermark has their roots in the internal band in order to strike a balance between durability and visible quality. The robustness of each technique has been demonstrated in contradiction of a range of non - geometric and geometric attacks. A wavelet-based approach was proposed by M. Barni et al. (2001) [7]. The features of the HVS (Human Visual System) have been taken into consideration by the writers. Masking of each of the cells has been performed by taking each subband's value of brightness and texture into account. The authors' watermark comprises of an adaptively inserted pseudorandom pattern to DWT sub band coefficients. The proposed system's imitation result demonstrates that this technique offers a watermarking system that is extremely resilient to innumerable digital image processing attacks. By using a significant wide variety of LWT coefficients, V.S. Vermaet al. (2013) [8] presented an incredibly undetectable and trustworthy watermarking technique. The approach involves shifting the blocks of the CH3 subband, after which a watermark is implanted into the furthermost significant coefficient of the scrambled subblock. This algorithm has been placed to the proof by imposing multiple attacks and simulating the algorithm. The results of the simulation demonstrate that the system is both highly resilient to forced image processing attacks and remarkably imperceptible.

D Singh et al. [9] demonstrated a reliable and intuitively imperceptible copyright protection technique. To accomplish encryption, novelists have additionally included the Arnold Cat Map technique and DCT. The most prevalent security issues that arise utilizing SVD are detection of false positives and unauthorized reading, which the authors have addressed. According on their comprehensive evaluation, the authors have demonstrated that their suggested approach is simultaneously secure and undetectable against various signal processing threats. A perceptually invisible image watermarking system based on DWT-SVD was presented by Falgun N. Thakkar et al. (2017) [11] with the objective of employing it for medicinal purposes. Through the decomposition of the medical image and the application of DWT to the region of passion, numerous frequency sub bands are investigated in the following method. After that, ROI's low frequency sub-band LL is subjected to Block-SVD. To assess the methodology they employed, the novelists examined CT and X-ray scans. A watermarked image with great imperceptibility is produced by the described approach. The authors have also tested the method's robustness by showcasing multiple checkmark assaults. According to the research, this approach is quite resistant to the simulated attacks.

4. DWT - based Digital Watermark using SVD

Comparing Discrete Wavelet Transform to other approaches including Discrete Fourier transform and Discrete Cosine Transform has demonstrated that DWT offers superior robustness and discernible transparency [15]. The DWT technique alienates the image under evaluation into four frequency subbands. One 1-Dimentional transformation is applied over the rows of the picture array to split the image in half vertically, and these two 1-Dimentional transformations can be interpreted as the two 1-Dimentional transformations that comprise the 2-Dimentional DWT. The image array's columns are divided in half horizontally using a second 1-Dimentional transformation process. LL (low-low), LH (low-high), HL (high-low), and HH (high-high) are the four frequency sub bands that make up the image. By recommending 2-D DWT once more, one can further subdivide any of the sub bands. Image decomposition processes using 2-D DWT and I level are shown in Figs. 2 and 3, respectively [10].

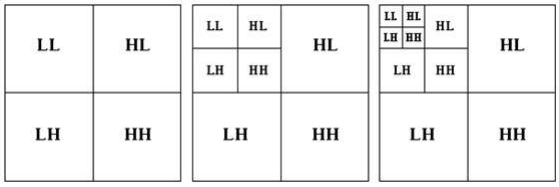


Fig.2. DWT decomposition methodology

Matrix transformation is one way to understand Singular Value Decomposition (SVD). This transformation acquires 3 matrices, U, S, and V, by first breaking down a M x N sized picture into a 2-D M x N matrix and then applying SVD over this M x N matrix [13, 14]. The the factorization of the image A into three SVD matrices is illustrated in Fig. 4 as follows:

$$\mathbf{A = USV^T}$$

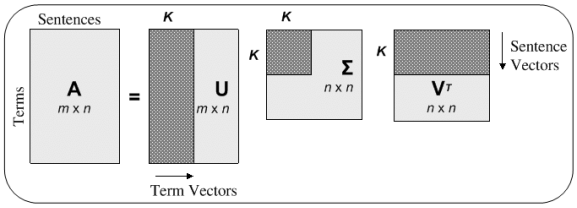


Fig. 3 SVD process's matrix division

The present research presents the resilient DWT-SVD algorithm implementation. Five distinct input photos and one watermarked image are taken into consideration for the comparative analysis. To smooth overall analogies, the values of MSE, PSNR and SSIM are determined.

Fig. 5. Demonstrates the block diagram for the watermarking implementation of DWT-SVD.

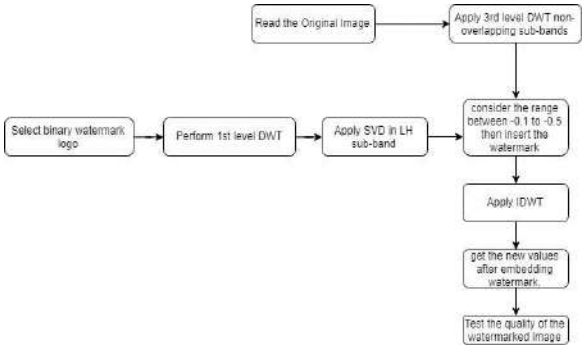


Fig.5. Watermark embedding procedure using proposed method

In the recommended method, the input image is first read and then applied using the DWT 3rd level of decomposition. In a similar way, the original watermark image to be added into the query image is chosen using the DWT 1st level of decomposition. The watermarked image's LH band, which is injected into the requested image and contains values in the range of -0.1 to -0.5, was subjected to the SVD technique. The original image, which is used for the watermark insert, was then recovered using the inverse DWT concept. Several experiments have been conducted to evaluate the original image preservation quality once the original image has been reconstructed following the insertion of a watermark.

5. EXPERIMENTAL RESULTS

Robustness against geometric attacks and image processing is demonstrated by experimental evidence. Images of Cell, Circuit, Cameraman, MRI, and Pout are used as input host samples, and each host image has a watermark applied by Lena. MATLAB R2017b version 9.3.0.713579 was used to simulate the model on a Windows 10 personal computer. Figure 6 exhibits the original images in addition to the image which has been watermarked, while Figure 7 displays the comparable watermarked images.

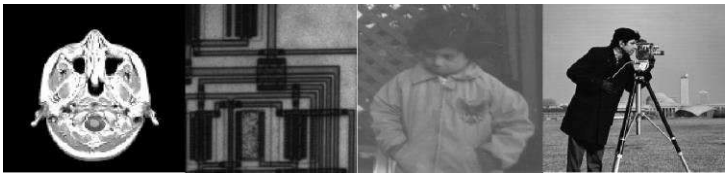
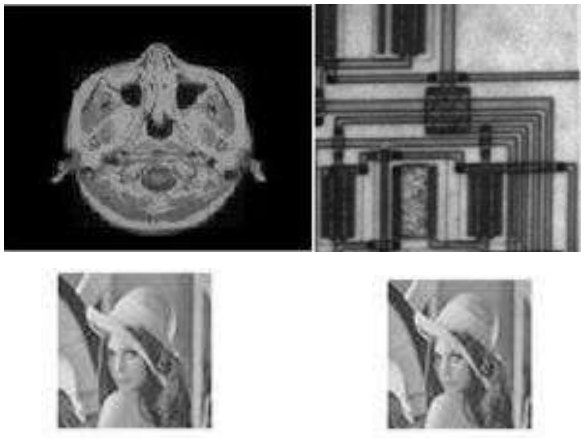


Figure 6(a) shows the original MRI images; (b) shows the original Circuit images; (c) shows the original Pout photos; (d) shows the original Cameraman images.

Fig. 6 (e). Cell **Fig. 6** (f). Lena as watermark



7(a). Watermarked Images of MRI 7(b). Watermarked Images of Circuit

7 (c) . Pout Watermarked Images 7 (d) . Photographs of the cameraman with watermarks 7 (e) . Circuit Images with Watermarks

Calculations of MSE, PSNR, and SSIM have been performed made in mandate to measure the robustness of the established algorithm. Whereas

$$\text{MSE} = \frac{1}{n}\sum_{i=1}^{n}(Y_i - \hat{Y}_i)^2$$

Y- Observed Values

MSE- Mean Square Error

$\hat{Y}$ -Predicted Values

n- Number of Data Points

$$PSNR = 10\log_{10}\frac{255^2}{MSE}\text{dB}$$

$$\text{SSIM}(\mathbf{x},\mathbf{y}) = \frac{(2\mu_x\mu_y + C_1)(2\sigma_{xy} + C_2)}{\left(\mu_x^2 + \mu_y^2 + C_1\right)\left(\sigma_x^2 + \sigma_y^2 + C_2\right)}.$$

The MSE simulation outcomes are listed in Fig.8, while the PSNR and SSIM values are reported in Fig.9 and Fig.10, respectively. These tables' first column displays the outcomes of an attack-free watermarking system, while the remaining columns show the values obtained after applying different attacks, such as rotation, blurring, sharpening, resizing, Gaussian-noise, cropping, salt and pepper- noise.

Fig.8. compares the obtained MSE principles for several images, both with and without assaults.

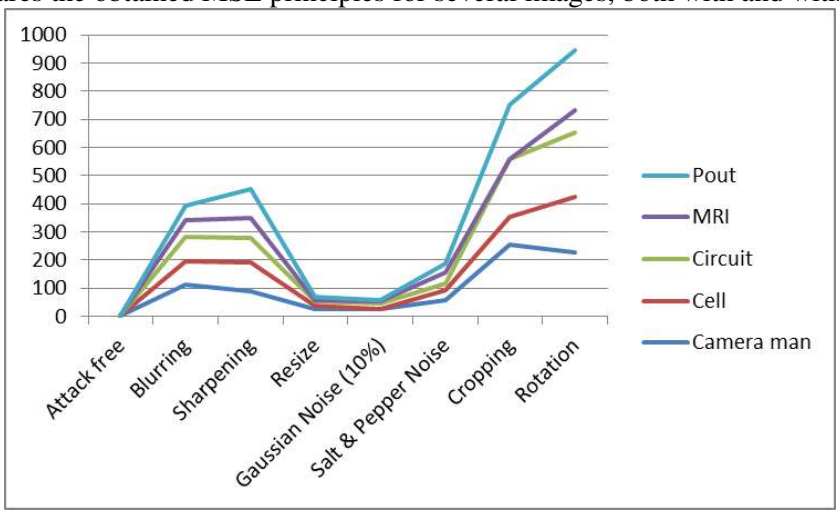
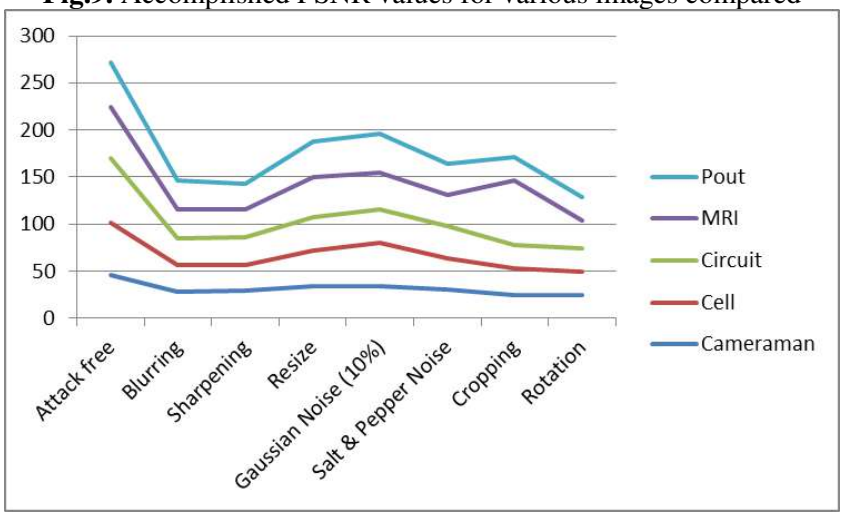
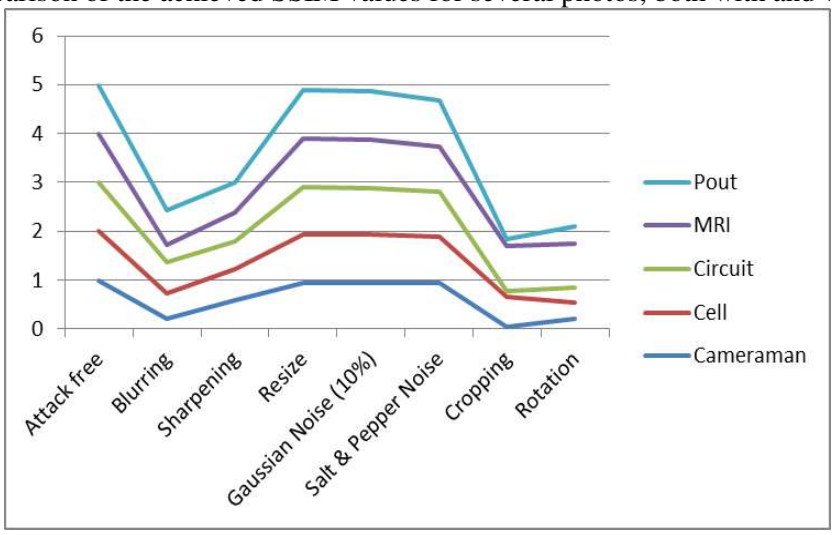


Fig.9. Accomplished PSNR values for various images compared



The values for MSE, PSNR, and SSIM are displayed in the first row of each table when an image is not exposed to any kind of image processing or signal processing attack. The subsequent data of Fig. 8, Fig. 9 and Fig. 10 illustrate the simulated results that were produced after applying attacks like sharpening, resizing, blurring, guassian noise (10%), salt and pepper noise, cropping, and rotation on five different images.

Fig.10 A comparison of the achieved SSIM values for several photos, both with and without attacks.



6. CONCLUSION

The research introduces a strong digital watermarking methodology that combines two transformation methods: SVD and DWT. The watermark is overlaid on the unique values' sub bands in the cover image. Simulation results indicate that this technology can attain great imperceptibility without compromising perceptual quality. Fig.10 presents the experiment findings and shows that there have been notable gains in relations of the imperceptibility. The obtained MSE, PSNR, and SSIM values show that DWT-SVD offers a considerable degree of robustness against various image/signal processing threats.

ACKNOWLEDGEMENT

The authors have no conflicts of interest to declare. All co-authors have seen and agree with the contents of the manuscript and there is no financial interest to report. We certify that the submission is original work and is not under review at any other publication.

REFERENCES

[1] Cox, Ingemar J., Joe Kilian, F. Thomson Leighton, and Talal Shamoon. "Secure spread spectrum watermarking for multimedia." *IEEEtransactions on image processing* 6, no. 12 (1997): 1673-1687.

[2] Kutter, Martin, and Fabien AP Petitcolas. "Fair benchmark for image watermarking systems." *Security and Watermarking of Multimedia Contents* 3657 (1999): 226-239.

[3] Cox, Ingemar J., and Matt L. Miller. "The first 50 years of electronic watermarking." *EURASIP Journal on Advances in Signal Processing* 2002, no. 2 (2002): 820936.

[4] Cox, I. J., and M. L. Miller. "J. A, Bloom,"Digital watermarking," Chapter 5—Watermarking with Side Information." (2001).

[5] Poonam, S.M. arora, "Digital Watermarking: An Introduction" *International Journal of Applied Research* 3(4), 2017 128-131.

[6] Lie, Wen-Nung, Guo-Shiang Lin, Chih-Liang Wu, and Ta-Chun Wang. "Robust image watermarking on the DCT domain." In *Circuits and Systems, 2000. Proceedings. ISCAS 2000 Geneva. The 2000 IEEE International Symposium on*, vol. 1, pp. 228-231. IEEE, 2000.

[7] Barni, Mauro, Franco Bartolini, and Alessandro Piva. "Improved wavelet-based watermarking through pixel-wise masking." *IEEE transactions on image processing* 10, no. 5 (2001): 783-791.

[8] Verma, Vivek Singh, and Rajib Kumar Jha. "Improved watermarking technique based on significant difference of lifting wavelet coefficients." *Signal, Image and Video Processing* 9, no. 6 (2015): 1443-1450.

[9] Singh, D. and Singh, S.K., 2017. DWT-SVD and DCT based robust and blind watermarking scheme for copyright protection. *Multimedia Tools and Applications*, *76*(11), pp.13001-13024.

[10] Ganic, Emir, and Ahmet M. Eskicioglu. "Robust DWT-SVD domain image watermarking: embedding data in all frequencies." In *Proceedings of the 2004 Workshop on Multimedia and Security*, pp. 166-174. ACM, 2004.

[11] Thakkar, F.N. and Srivastava, V.K., 2017. A blind medical image watermarking: DWT-SVD based robust and secure approach for telemedicine applications. *Multimedia Tools and Applications*, *76*(3), pp.3669-3697.

[12] Bhatnagar, Gaurav, and Balasubramanian Raman. "A new robust reference watermarking scheme based on DWT -SVD." *Computer Standards & Interfaces* 31, no. 5 (2009): 1002-1013.

[13] Sadek, Rowayda A. "SVD based image processing applications: state of the art, contributions and research challenges." *arXiv preprint arXiv:1211.7102* (2012).

[14] Honsinger, Chris. "Digital watermarking." *Journal of Electronic Imaging* 11, no. 3 (2002): 414.

[15] Kang, Xiangui, Jiwu Huang, Yun Q. Shi, and Yan Lin. "A DWT-DFT composite watermarking scheme robust to both affine transform and JPEG compression." *IEEE transactions on circuits and systems for video technology* 13, no. 8 (2003): 776-786.

[16] B Lakshmana Rao "Modeling Automated Image Watermarking Using Meta heuristic based Deep Learning with Wavelet Approach", Sensing and Imaging (Springer), July 2023.

[17] B Lakshmana Rao "Impeccable Watermarking for Digital Images" Jour of Adv Research in Dynamical & Control Systems (Scopus), Vol. 11, No. 8, 2019.

[18] Kumar, R. Prasanna, and Showri Rayalu Bandanadam. "Block chain-based decentralized public auditing for cloud storage with improved EIGAMAL encryption model." International Journal of Information Technology 16.2 (2024): 697-711.