Indonesian Journal of Electrical Engineering and Computer Science
Vol. 41, No. 1, January 2026, pp. 344~356
ISSN: 2502-4752, DOI: 10.11591/ijeecs.v41.i1.pp344-356

Invisible watermarking as an additional forensic feature of e-meterai

H. A. Danang Rimbawa[1], Sirojul Alam[1], Joko W. Saputro[1], Teddy Mantoro[2]
[1]Cyber Defense Engineering, Faculty of Defense Science and Technology, The Republic of Indonesia Defense University, Bogor, Indonesia
[2]School of Computer Science, Nusaputra University, Sukabumi, Indonesia

Article Info

Article history:

Received May 31, 2024
Revised Aug 23, 2025
Accepted Dec 13, 2025

Keywords:

DFT
E-meterai
Forensic
SIFT
watermarking

ABSTRACT

The e-meterai is an official digital product of the Indonesian government issued by the Directorate General of Taxation (DGT). Its usage has become increasingly widespread as conventional documentation transitions to digital formats, serving the same function as its printed counterpart. This product features a quick-response code embedded with unique Indonesian codes and offers overt, covert, and forensic features. This study aims to experiment with adding a forensic feature in the form of an invisible watermark. We employed two watermark embedding techniques, discrete Fourier transform (DFT) and scale-invariant feature transform (SIFT), to determine which is more suitable for this application. After embedding the watermark, we also simulate various attacks including gaussian noise, salt and pepper noise, averaging filter, rotation, translation, and speckle noise. For each attack, we calculated with normalized-cross correlation (NCC) values, obtaining 0.863 and 0.976 for the gaussian noise attack, 0.929 and 0.984 for the salt and pepper attack, 0.975 and 0.984 for the averaging filter attack, 0.173 and 0.097 for rotation attacks, 0.172 and 0.032 for translation attack, and 0.972 and 0.996 for speckle noise attack, using DFT and SIFT techniques, respectively.

Corresponding Author:

Sirojul Alam
Cyber Defense Engineering, Faculty of Defense Sciences and Technology
The Republic of Indonesia Defense University
Bogor, Indonesia
Email: sirojul.alam@tp.idu.ac.id

1. INTRODUCTION

The advancement of the digital world has increasingly highlighted the importance of security and authenticity of visual content. Digital images are extensively utilized across social media, news outlets, scientific documentation, creative industry, and professional documents. With the rise in digital image usage, challenges related to copyright, forgery, and manipulation have also surged. Consequently, watermarking technology is being viewed as a viable solution due to its diverse techniques and applications.

Recent years have seen significant progress in the research of invisible watermarking. Researchers have developed numerous algorithms aimed at enhancing the robustness of watermarks against various attacks, including compression, cropping, and pixel manipulation. These advancements ensure that watermarks remain intact and detectable even after undergoing such alterations, thereby preserving the integrity of the visual content. These watermarking algorithms focus on embedding watermarks efficiently without compromising the quality of the images. This balance is crucial as it allows for the protection of digital content while maintaining its usability and aesthetic value. As a result, invisible watermarking has

become a pivotal area of study in addressing the growing concerns over digital image security and authenticity in an increasingly digital-dependent world. A range of studies have explored the use of invisible watermarking as a solution for image manipulation, such as those proposed by [1], [2]. Both proposed watermarking schemes aim to enhance image quality while protecting against tampering, specifically for medical images and artworks. Different techniques were employed by Lv [3], who used watermarking to compare deepfake images, making manipulated images easier to detect. Another method introduced by Wen *et al.* [4] is known as tree-ring watermarking, which can produce strong invisible watermarks.

Invisible watermarking safeguards digital content by embedding imperceptible markers within the content itself, making it challenging for unauthorized users to detect and remove the watermark [5], [6]. Techniques such as discrete wavelet transform (DWT) and singular value decomposition (SVD) are commonly employed to ensure the robustness, imperceptibility, and capacity requirements of the watermark, thereby enhancing its effectiveness in protecting intellectual property and preventing copyright infringements [7]. Watermarking systems utilize methods such as the Arnold transform, chaotic maps, and secret signal injection to further enhance security and deter the illegal distribution of digital data [8], [9].

Another longstanding technique used for watermarking is the discrete cosine transform (DCT). This technique offers unique advantages compared to other methods. DCT-based watermarking allows for embedding watermarks into the frequency coefficients of images, enhancing robustness against least significant bit (LSB) attacks and reducing execution time [10], [11]. DCT is widely used in watermarking in the frequency domain and enables the insertion of watermarks in different color spaces, with red-green-blue (RGB) being preferable for DCT in color images and binary for the discrete Fourier transform (DFT) technique [12], [13]. DCT-based watermarking methods can achieve high-speed performance and low computational cost through novel techniques, making them compatible with various embedding ratios and compression scenarios while maintaining high quality and efficiency [6].

DFT is also a method employed to embed secure data within images. Research has explored the use of DCT for watermarking, showing promising results in terms of capacity and imperceptibility [14]. A study on hybrid watermarking schemes combining DWT and SVD demonstrated increased imperceptibility and robustness, especially in the protection of medical images [15]. Another innovative approach involves a fuzzy equilibrium optimization (FEO) technique using DWT for watermark embedding, achieving high robustness against security attacks and significantly improving the peak signal-to-noise ratio (PSNR) values [16]. A novel algorithm combining log-polar transform (LPT) and DCT for medical image watermarking showcased the lossless embedding of patient information while maintaining image quality robustness [17].

The combination of DFT and SVD in watermarking schemes ensures increased performance in terms of visual distortion and robustness [18]. DFT-based methods provide imperceptibility and increased security compared to classical techniques, making them highly robust against unauthorized detection [11]. DFT is commonly used in conjunction with other transforms like DWT to enhance watermarking quality, imperceptibility, and robustness, proving to be a valuable tool in digital image authentication and copyright protection [18]-[20]. Several popular watermark applications [19] can be seen in the following Figure 1.

Figure 1. Watermark application trends

According to Figure 1, the implementation of digital watermarking has become extensive, such as in broadcast monitoring, authentication, legacy systems, usage control, medical application, copyright protection, ownership identification, and copy control. These all applications underscore the broad range of capabilities that digital watermarking technology provides across different sectors.

A notable application of digital watermarking is in copyright protection, where it is used to embed watermarks in digital content to establish ownership and prevent unauthorized use or distribution. In the medical field, digital watermarks securely embed patient information or medical records within images or documents, aiding in the accurate tracking and verification of medical data [20]. Track and trace copy control embeds unique identifiers or codes in digital content to trace its origin and monitor its distribution, helping to against piracy and ensure accountability within content distribution networks. Usage control involves regulating and managing access and usage rights of digital content through embedded watermarks. Content authentication ensures the verification of authenticity and integrity.

Another technique to consider in watermark engineering is scale-invariant feature transform (SIFT). These image watermarking techniques are not explicitly discussed in the provided research articles. However, various advanced watermarking methods are provided, such as additive watermarking on sparse coefficients using basis pursuit [21], deep learning-based watermark extraction using convolutional generative adversarial neural networks [22], local watermarking based on histogram shifting for robustness against attacks [23], LSB embedding with canny edge detection for enhanced security [24], and invisible watermarking using DCT for secure data transfer [14]. These techniques focus on aspects like robustness, security, capacity, and resistance attacks, showcasing the diverse approaches employed in digital image watermarking to address different challenges in protecting multimedia data.

The SIFT technique offers several advantages in the realm of multimedia security. SIFT descriptors encode local information around key points, providing affine invariance without the need for viewpoint simulations [25]. When combined with watermarking techniques, such as singular decomposition value (SVD) and all-phase biorthogonal transform (APBT), SIFT-based watermarking algorithms demonstrate strong robustness against various attacks, including JPEG compression, gaussian blurring, subsampling, and resizing [26]-[28]. The fusion of SIFT with watermarking methods enhances the security aspects of digital images, ensuring authenticity, integrity, and copyright protection. Additionally, SIFT's ability to extract feature points with high invariance to rotation, compression, and scaling contributes to the overall effectiveness and reliability of SIFT-based image watermarking schemes.

SIFT also enhances copyright protection by providing robustness and security against various attacks. By utilizing deep learning techniques like convolutional generative adversarial neural networks [22], researchers have developed novel algorithms that embed watermarks imperceptibly into images, ensuring copyright information remains intact even after potential alterations or attacks. The use of encryption algorithms like Arnold transform [29], and cryptographic keys [30] further strengthens the security of the watermarking process. The application of end-to-end document image watermarking schemes using deep neural networks [26] and compressed domain-based digital video watermarking algorithms [27] showcases advancements in ensuring the robustness and imperceptibility of watermarks, thereby enhancing copyright protection for multimedia content. SIFT involves utilizing a feature detector to select local areas for embedding, applying the stationary wavelet transform (SWT) for denoising, and employing histogram shifting for embedding the watermark into denoised local areas [23]. It also involves altering image pixels in the spatial domain to incorporate the watermark by quantizing the block-wise invariant maximum singular value without performing an SVD transform [28].

The e-meterai or what we can call it electronic seal, serves as an official digital seal designed to verify the authenticity of electronic documents, similar to the role of a physical seal on paper documents [31]. This seal offers legal assurance and confidence that the document has not been altered and remains valid. The function of an electronic seal includes validating the date, and the issuing authority, and ensuring the integrity and authenticity of the data within the document. Figure 2 is the sample of e-meterai officially issued by the Directorate General of Taxation (DGT) of the Republic of Indonesia with its features.

The e-meterai used in Indonesia appears as a quick response (QR) code with distinctive Indonesian imagery. This digital seal features the iconic '*Garuda Pancasila*', along with textual elements such as '*Meterai Elektronik'*, the numerical '10000', '*Sepuluh Ribu Rupiah*', and a unique code that varies for each seal. This combination of visual and textual components not only authenticates documents but also maintains their legal integrity, akin to traditional physical seals on paper documents.

The security features of electronic seals can generally be categorized into three levels: overt, covert, and forensic. Overt features are security elements easily identifiable by the naked eye, such as the image of the '*Garuda Pancasila'* and other visible markings. Covert features, in contrast, require specialized tools for verification, such as scanners and signature panels in PDF reader applications. Forensic features can only be examined by authorized entities such as Peruri Indonesia, the system authority, which may include audit logs,

cryptography, and code generators [32]. Together, these three levels of security ensure integrity and authenticity, providing multi-layered protection against tampering and unauthorized access. Forensic features in images refer to unique characteristics or traces that can be analyzed to detect forgeries or manipulations. These features are crucial in image forensics for distinguishing between authentic and doctored content. Various techniques such as copy-move forgery detection using algorithms such as SLIC, SIFT, and FLANN [33], machine learning approach [34], and universal detectors with transferable forensic feature (TFF) like color as a critical feature are employed [35].

As digital technology continues to advance, the need to improve the authentication and security features of electronic seals becomes more critical, surpassing the traditional dependence solely on serial numbers as differentiation. To address this requirement, we add a new forensic feature in e-meterai: an invisible watermark. The addition of this watermark is implemented using two different techniques: DFT and SIFT. The objective is to evaluate which technique performs the best and then adopt the most suitable one for use. Unlike the overt feature, this watermark functions unobtrusively, ensuring it does not interfere with the primary features of the e-meterai. By incorporating an invisible watermark, we aim to enhance the integrity and authenticity of electronic documents, offering an additional layer of protection against counterfeiting and modification.

Figure 2. E-meterai

2. METHOD

In the field of watermarking, the DFT and SIFT techniques each have their unique advantages. DFT offers robustness and security by utilizing SVD and encryption with chaotic maps, ensuring imperceptibility and increased performance [21]. SIFT is known for its robustness to various image transformations and distortions, making it a valuable tool for image feature extraction and matching.

The image we used is an original e-meterai with a size of 709×709 pixels, serving as the host image to embed the watermark. We also use the logo of the DGT of the Republic of Indonesia as the watermark image, which has the same size as the host image, 709×709 pixels. Figures 3 and 4 show the host image and the watermark image used.

Figure 3. Host image

Figure 4. Watermark image

Figure 3 shows the e-meterai as the host image, and Figure 4 depicts the DGT logo as the watermark image. Both images are created with the same dimension to ensure the watermark is evenly spread across the host image. This approach allows the watermark to be better distributed, making it difficult to remove without damaging the host image.

If the watermark image is smaller than the host image, it would only be embedded in certain parts of the host image, such as in the corners or areas with high texture to conceal it. We then processed both images using DFT and SIFT techniques. The steps of the DFT technique can be seen in Figure 5.

The DFT is a mathematical technique used to convert spatial domain data into frequency domain data [36]. DFT can be utilized to embed a watermark into an image by modifying its frequency components. As shown in Figure 5, before we apply the DFT we ensure that the host image and watermark image are in the correct format and size. We load a grayscale version of the host and watermark image. Grayscale images are preferred as they simplify the processing and are sufficient for many watermarking applications. We also ensure the size of the watermark image, and if the images are too large, we resize them to fit within the host image. We apply DFT to the host image to transform it from the spatial domain to the frequency domain. In this step, we compute the DFT of the host image using the fast Fourier transform (FFT) algorithm. This operation results in a complex-valued frequency spectrum, then we shift the zero-frequency component to the center of the spectrum for easier manipulation and visualization.

When embedding the watermark, we select frequency coefficients from the transformed host image. Mid-frequency components are chosen to balance robustness and imperceptibility. We then embed the watermark by adding pixel values of the watermark to these selected coefficients. This step can be performed by scaling the watermark and adding it to the chosen frequency coefficients. Next, we apply the inverse DFT to revert the frequency domain data to the spatial domain. We use inverse FFT on the modified frequency spectrum to obtain the watermarked image in the spatial domain. Afterward, we save the image with the embedded watermark. Subsequently, we simulate attacks on the watermarked image. These attacks involve image manipulation that disrupts the watermark. Some of the attacks performed include noising, salt and pepper, averaging filter, rotation, and translation. We then extract the watermark from the attacked image to observe the effect of these attacks. The purpose of these attacks is to examine the robustness of the watermark, which we measure using the normalized cross-correlation (NCC) value.

In the initial steps of SIFT technique as shown in Figure 6, we observe similarities with our approach using the DFT technique. This is because these initial steps are standard procedures in watermarking applications. The difference lies in the watermark embedding process. SIFT first detects key points, which are chosen for their robustness against image transformations. The watermark is embedded by modifying the intensity values of pixels at the detected key points.

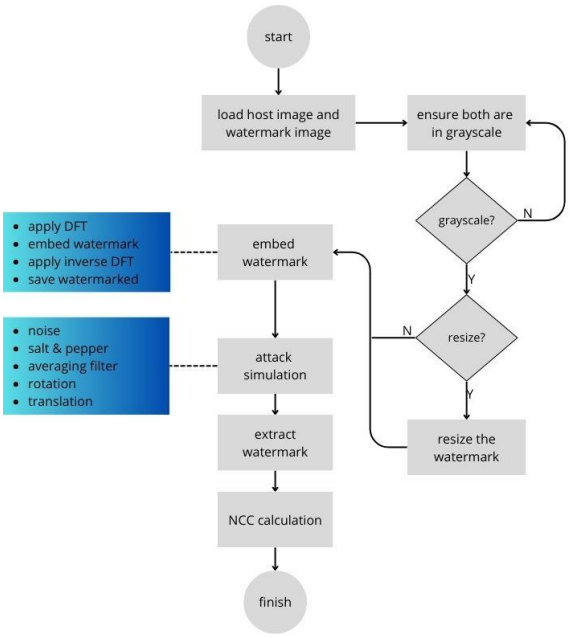

Figure 5. The steps of the DFT technique

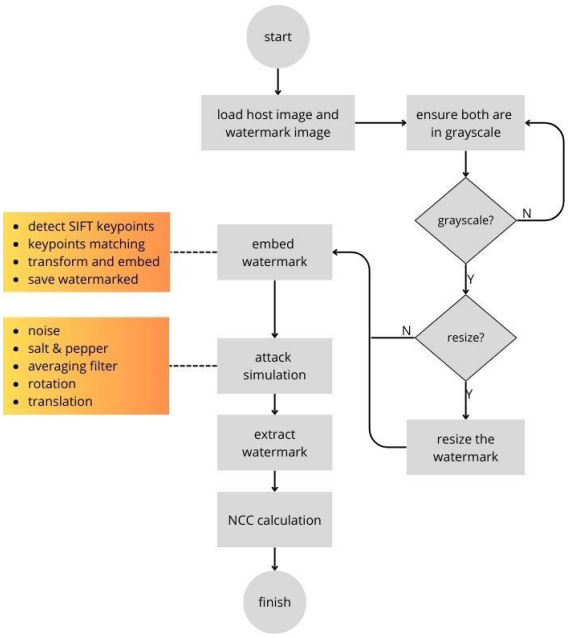

Figure 6. The steps of the SIFT technique

After embedding the watermark, we apply an inverse transformation to obtain the watermarked image, ensuring that it remains in the same domain as the host image. This step is crucial to maintain the practicality and usability of the watermarked image. We also simulate various attacks on the watermarked image, similar to those conducted in the DFT technique, including noise addition, filtering, rotation, and translation. Following these attacks, we extract the watermark from the attacked image and evaluate its robustness using NCC values. This evaluation allows us to assess the effectiveness of the SIFT-based watermarking technique. All of these experimental steps were conducted on Google Colab notebook using Python programming language. For both techniques, we utilize several libraries as illustrated in Figure 7.

```
import cv2
import numpy as np
from numpy.fft import fft2, ifft2, fftshift, ifftshift
import matplotlib.pyplot as plt
```

Figure 7. Library set

In Figure 7, we imported the libraries necessary for our experiments. The *'cv2'* library was utilized for image processing tasks, the *'numpy'* library was employed in the numerical calculation, the *'fft'* module for the DFT technique, and the *'matplotlib'* library for visualizing the experimental results. Following the importation of these libraries, we created a function that embeds a watermark into the host image using the DFT technique, as depicted in Figure 8.

```
def dft_watermarking(host_image, watermark, alpha=0.1):
    dft_image = fft2(host_image)
    dft_image_shifted = fftshift(dft_image)
    watermark_resized = cv2.resize(watermark, (host_image.shape[1], host_image.shape[0]))
    watermarked_dft = dft_image_shifted + alpha * watermark_resized
    watermarked_image = ifft2(ifftshift(watermarked_dft)).real
    return watermarked_image
```

Figure 8. DFT watermarking function

Figure 8 shows the function to embed a watermark into a host image by manipulating the frequency components of the image. By adding a scaled version of the watermark to the DFT of the host image and then transforming it back to the spatial domain, the function achieves a robust watermarking effect. The 'alpha' allows for control over the visibility and strength of the watermark. Unlike DFT, the SIFT technique identifies and matches key points between the host image and the watermark image. The function of SIFT is depicted in the Figure 9.

```
def apply_sift_watermarking(host_image, watermark):
    # Convert images to grayscale
    gray_host = cv2.cvtColor(host_image, cv2.COLOR_BGR2GRAY)
    gray_watermark = cv2.cvtColor(watermark, cv2.COLOR_BGR2GRAY)

    # Initialize SIFT detector
    sift = cv2.SIFT_create()

    # Detect keypoints and descriptors
    kp1, des1 = sift.detectAndCompute(gray_host, None)
    kp2, des2 = sift.detectAndCompute(gray_watermark, None)

    # Use FLANN matcher to match descriptors
    index_params = dict(algorithm=1, trees=5)
    search_params = dict(checks=50)
    flann = cv2.FlannBasedMatcher(index_params, search_params)
    matches = flann.knnMatch(des1, des2, k=2)

    # Store all good matches as per Lowe's ratio test
    good_matches = []
    for m, n in matches:
        if m.distance < 0.7 * n.distance:
            good_matches.append(m)

    # Draw matches
    result = cv2.drawMatches(host_image,
                             kp1, watermark,
                             kp2, good_matches,
                             None, flags=cv2.DrawMatchesFlags_NOT_DRAW_SINGLE_POINTS)
    return result
```

Figure 9. SIFT watermarking function

The function in Figure 9 embeds a watermark into a host image using the SIFT method and provides a visual representation of matching key points between the two images. It starts by converting both images to grayscale, simplifying the process by focusing on intensity value. A SIFT detector object is then created to identify key points and compute descriptors for each image. Using the FLANN-based matcher [37], the function finds correspondences between the two sets of descriptors, optimizing the search for the best matches. Lowe's ratio test is applied to filter out poor matches, ensuring only reliable matches are retained. The function visualizes the matching key points by drawing lines between the matched points in the host image and the watermark image, providing a visual representation of the embedding process. This technique ensures that the watermark is robust and resistant to common image transformations, making it an effective technique for watermark embedding. As described in the experiment steps, we evaluated each watermarking technique by calculating their respective NCC values. The function for calculating the NCC is shown in Figure 10.

```
def calculate_ncc(image1, image2):
    product = np.mean((image1 - image1.mean()) * (image2 - image2.mean()))
    stds = image1.std() * image2.std()
    if stds == 0:
        return 0
    else:
        ncc_value = product / stds
        return ncc_value
```

Figure 10. NCC measurement function

NCC function as declared in Figure 8 effectively assesses the similarity between two images by quantifying the correlation between their pixel intensities, taking into account their mean and standard deviation. Normalized NCC evaluates the resemblance between a template and a section of an image by comparing their pixel values. NCC values, which range between -1 and 1, are critical for determining the accuracy of image correspondence [38]. Recent advancements have bolstered the robustness of NCC by processing images with 'siamese' convolutional networks, optimizing the contrast between NCC values of true and false matches [37]. A high NCC value approaching 1 indicates a strong similarity between the original watermark and the extracted one, suggesting that the watermark can endure certain types of distortions.

3. RESULTS AND DISCUSSION

Watermarks, which typically consist of logos, names, or symbols embedded within digital images, act as unique identifiers. We embedded a watermark image into a host image using both DFT and SIFT techniques and then compared their performance by calculating the NCC values. This comparison is essential to assess the feasibility of applying these techniques to e-meterai products, considering their respective strengths and weaknesses. The result of watermark embedding using both techniques can be seen in Figures 11 and 12.

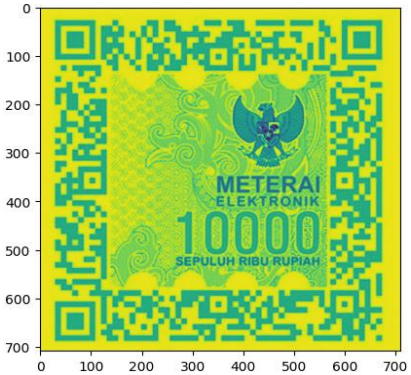

Figure 11. DFT watermarking

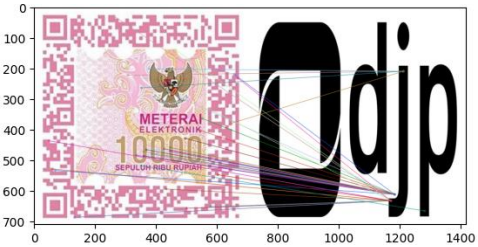

Figure 12. SIFT watermarking

Figure 11 shows the original image after embedding the watermark using the DFT technique, which has not yet been converted to a colored image. Figure 12 displays the result of the SIFT watermarking technique, highlighting the key points within the host image where the watermark was embedded. Both images were then restored to their original forms, now featuring the new forensic capability of an invisible watermark, as illustrated in Figures 13 and 14.

Figure 13. E-meterai with DFT

Figure 14. E-meterai with SIFT

Both images, Figures 13 and 14, appear identical because the forensic features are not visible to the naked eye. This means the feature can only be extracted by authorized personnel if needed. We have conducted attack simulations on the watermarked image, and the results are displayed in the Figures 15 to 26.

Figure 15. DFT gaussian noise attack

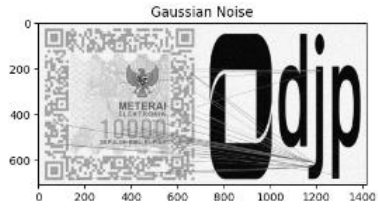

Figure 16. SIFT gaussian noise attack

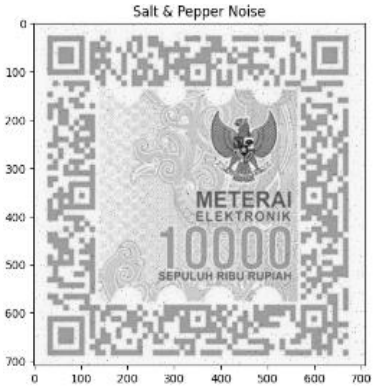

Figure 17. DFT salt and pepper noise attack

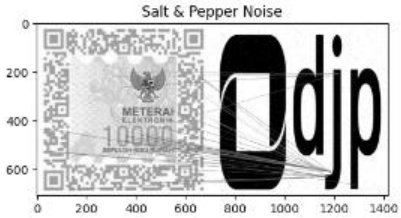

Figure 18. SIFT salt and pepper noise attack

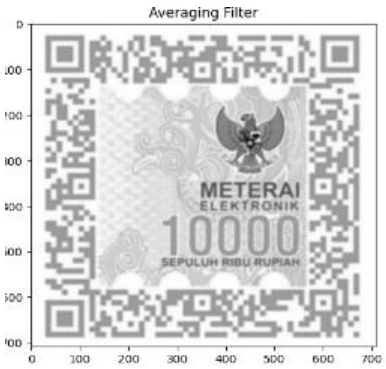

Figure 19. DFT averaging filter attack

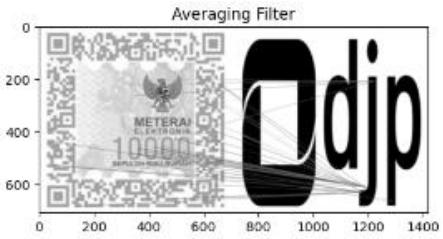

Figure 20. SIFT averaging filter attack

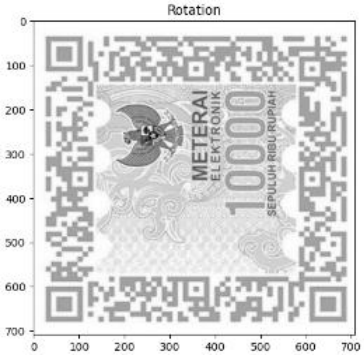

Figure 21. DFT rotation attack

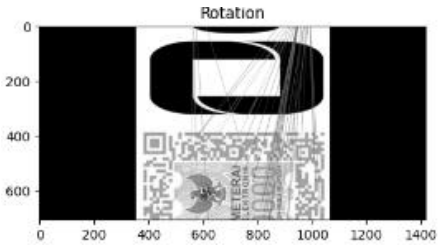

Figure 22. SIFT rotation attack

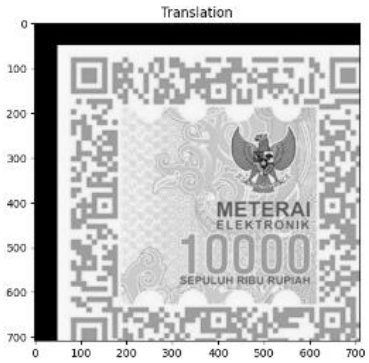

Figure 23. DFT translation attack

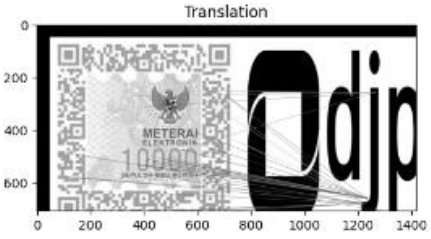

Figure 24. SIFT translation attack

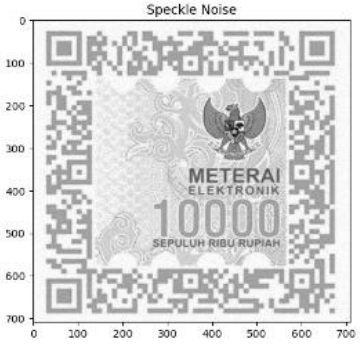

Figure 25. DFT speckle noise attack

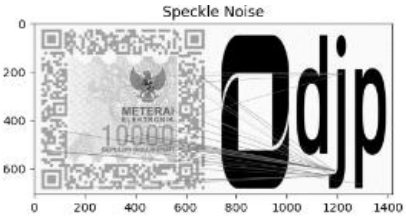

Figure 26. SIFT speckle noise attack

A gaussian noise attack adds random noise throughout the entire image. The uniform nature of gaussian noise can obscure the watermark by introducing random pixel value changes across the images, making it difficult to detect or extract the watermark directly. A salt and pepper noise attack is a common method to test the robustness of image watermarking schemes by introducing impulse noise that affects random pixels, typically setting them to the minimum (salt) or maximum (pepper) values.

An averaging filter attack on a watermarked image involves applying an averaging filter to blur the image. This filter works by replacing each pixel's value with the average value of its neighboring pixels. This attack aims to degrade the image quality to make the watermark less visible or harder to detect. A rotation attack involves rotating the image by a certain angle. The purpose of this attack is to disrupt the alignment of the watermark, making it harder to detect or extract.

A translation attack on a watermarked image involves shifting the entire image by a certain amount in any direction, up, down, left, or right. The purpose of this attack is to move the watermark out of its expected position. The speckle noise attack introduces multiplicative noise into the watermarked image, potentially distorting the watermark by affecting areas of the image differently based on their intensity. It is particularly challenging because it can vary significantly across different parts of the image. When we have conducted the simulation attacks and the results obtained, we then evaluated the watermarking technique by calculating the NCC values for each attack. The NCC values are shown in Table 1.

Table 1. NCC values of each attack

Techniques	Attacks					
	Gaussian noise	Salt and pepper noise	Averaging filter	Rotation	Translation	Speckle noise
DFT	0.863	0.929	0.975	0.173	0.172	0.972
SIFT	0.976	0.984	0.984	0.097	0.032	0.996

The NCC values for DFT and SIFT watermarking techniques provide insights into their robustness against various types of attacks. Based on the NCC values above, SIFT demonstrates superior robustness against various noise attacks and performs slightly better with an averaging filter, and DFT shows better performance in handling rotation attacks. However, both techniques perform poorly on translation attacks. SIFT is well-suited for scenarios where the watermark needs to withstand various noise distortions, and DFT has better resistance to rotation attacks. Both techniques can be applied to e-meterai products and provide good NCC values in several watermark attack tests. The implementation of these techniques in e-meterai products is relatively new and has never been done before, so their potential use is significant, especially as digital technology continues to advance.

4. CONCLUSION

We have conducted watermark embedding experiments using DFT and SIFT techniques. Both techniques were applied to enhance forensic features in e-meterai products, whose usage is increasingly prevalent in digital documents. From our experiments, we obtained NCC values for each technique, demonstrating that both have strengths in withstanding various image manipulation attacks. Based on the NCC values, the SIFT technique generally offers better robustness against common noise attacks and averaging filters, making it a more suitable choice for applications where the watermark needs to withstand such distortion. However, if the rotation robustness is a critical factor, DFT might be preferred despite its overall lower performance in other areas. The choice of watermarking technique ultimately depends on the product owner. However, considering the advantages, we propose that the DFT technique be given more consideration for use. To address future challenges, advanced research that can be conducted includes the implementation of quantum security in e-meterai products.

ACKNOWLEDGEMENTS

We would like to express our gratitude to The Republic of Indonesia Defense University for their financial support, which made this research possible.

FUNDING INFORMATION

The research presented in this article was fully funded and supported by the Cyber Defense Engineering Study Program, The Republic of Indonesia Defense University. The funding covered the essential resources required for data collection, technical analysis, and the overall execution of the study. The

authors extended their highest appreciation to the institution for its continuous support in advancing cyber defense research and academic excellence.

AUTHOR CONTRIBUTIONS STATEMENT

This journal uses the Contributor Roles Taxonomy (CRediT) to recognize individual author contributions, reduce authorship disputes, and facilitate collaboration.

Name of Author	C	M	So	Va	Fo	I	R	D	O	E	Vi	Su	P	Fu
H. A. Danang Rimbawa	✓	✓		✓	✓				✓	✓	✓	✓	✓	✓
Sirojul Alam	✓	✓	✓	✓		✓	✓	✓	✓	✓	✓			
Joko. W. Saputro			✓	✓	✓	✓		✓		✓		✓	✓	✓
Teddy Mantoro	✓	✓			✓	✓		✓				✓		

C : **C**onceptualization
M : **M**ethodology
So : **So**ftware
Va : **Va**lidation
Fo : **Fo**rmal analysis
I : **I**nvestigation
R : **R**esources
D : **D**ata Curation
O : Writing - **O**riginal Draft
E : Writing - Review & **E**diting
Vi : **Vi**sualization
Su : **Su**pervision
P : **P**roject administration
Fu : **Fu**nding acquisition

CONFLICT OF INTEREST STATEMENT

The authors declare that they have no known competing financial interests, personal relationship, or professional affiliations that could have appeared to influence the work reported in this paper. This research was conducted in the absence of any political, ideological, or academic competing interests that could potentially bias the objectivity of the results and conclusions presented herein.

INFORMED CONSENT

Not applicable. This research does not involve human participants, clinical trials, or the collection of personal identifiable information. All data analyzed in this research were obtained through https://peraturan.bpk.go.id/Details/179718/pmk-no-134pmk032021 and https://peruri.co.id which do not required individual informed consent.

ETHICAL APPROVAL

Ethical approval was not required for this study as it does not involve human subjects, animal experimentation, or the collection of sensitive personal data. The research was conducted in accordance with the institutional guidelines for technical and engineering research at the Republic of Indonesia Defense University, ensuring all simulations and data analysis adhered to professional ethical standards.

DATA AVAILABILITY

The data support the findings of this study were derived from publicly available resources and official platforms, specifically from the Peruri official website (https://peruri.co.id), the Indonesia Audit Board's legal database (https://peraturan.bpk.go.id), and the electronic stamp duty portal (https://e-meterai.co.id).

REFERENCES

[1] A. Soualmi, A. Alti, and L. Laouamer, "An imperceptible watermarking scheme for medical image tamper detection," *International Journal of Information Security and Privacy*, vol. 16, no. 1, pp. 1–18, 2022, doi: 10.4018/IJISP.2022010102.

[2] Y. Luo, T. Zhou, F. Liu, and Z. Cai, "IRWArt: levering watermarking performance for protecting high-quality artwork images," *ACM Web Conference 2023 - Proceedings of the World Wide Web Conference, WWW 2023*, pp. 2340–2348, Apr. 2023, doi: 10.1145/3543507.3583489.

[3] L. Lv, "Smart watermark to defend against deepfake image manipulation," *2021 IEEE 6th International Conference on Computer and Communication Systems, ICCCS 2021*, pp. 380–384, 2021, doi: 10.1109/ICCCS52626.2021.9449287.

[4] Y. Wen, J. Kirchenbauer, J. Geiping, and T. Goldstein, "Tree-ring watermarks: fingerprints for diffusion images that are invisible and robust," 2023, [Online]. Available: http://arxiv.org/abs/2305.20030.

[5] M. M. Laftah, I. I. Hamid, and N. A. Ali, "Video copyright protection," *International Journal of Interactive Mobile Technologies*, vol. 17, no. 8, pp. 135–145, 2023, doi: 10.3991/ijim.v17i08.39339.

[6] Y. Wang, Y. Luo, Z. Wang, and H. Pan, "A hidden dct-based invisible watermarking method for low-cost hardware implementations," *Electronics (Switzerland)*, vol. 10, no. 12, pp. 1–25, 2021, doi: 10.3390/electronics10121465.

[7] X. Zhao, Y. X. Wang, and L. Li, "Protecting language generation models via invisible watermarking," in *Proceedings of Machine Learning Research*, 2023, vol. 202, pp. 42187–42199.

[8] T. Ketipearachchi and M. Wickramasinghe, "Invisible colour image watermarking technique for colour images using DWT and SVD," *International Journal on Advances in ICT for Emerging Regions (ICTer)*, vol. 13, no. 2, pp. 1–16, 2020, doi: 10.4038/icter.v13i2.7214.

[9] K. N. Radakrishnan and H. K. Mammi, "A grid-based invisible watermarking for .Jpeg images using least significant bit," *International Journal of Innovative Computing*, vol. 10, no. 1, pp. 1–6, 2020, doi: 10.11113/ijic.v10n1.235.

[10] S. Nabipour, "Fast BCH coding for optimal robust image watermarking in DCT domain," *arXiv: Multimedia*, 2021.

[11] A. B. Şahin, "A survey of digital image watermarking techniques based on discrete cosine transform," *International Journal of Information Security Science*, vol. 10, no. 3, pp. 99–110, 2021.

[12] K. Hemachandran and B. Justus Rabi, "Performance analysis of discrete cosine transform and discrete wavelet transform for image compression," *Journal of Engineering and Applied Science*, vol. 2, no. 13, pp. 436–440, 2018.

[13] S. Varkeessheeba and V. Magudeeswaran, "Performance evaluation of various discrete cosine transforms," *International Journal of Computer Science and Mobile Applications*, vol. 2, no. 11, pp. 78–86, 2014.

[14] W. Alomoush *et al.*, "Digital image watermarking using discrete cosine transformation based linear modulation," *Journal of Cloud Computing*, vol. 12, no. 1, pp. 1–17, 2023, doi: 10.1186/s13677-023-00468-w.

[15] T. K. Araghi and D. Megías, "Analysis and effectiveness of deeper levels of SVD on performance of hybrid DWT and SVD watermarking," *Multimedia Tools and Applications*, vol. 83, no. 2, pp. 3895–3916, Jan. 2024, doi: 10.1007/s11042-023-15554-z.

[16] S. Bhatia and A. Almutairi, "A robust fuzzy equilibrium optimization-based ROI Selection and DWT-based multi-watermarking model for medical images," *Sustainability (Switzerland)*, vol. 15, no. 7, pp. 1–18, 2023, doi: 10.3390/su15076189.

[17] T. Li, J. Li, J. Liu, M. Huang, Y. W. Chen, and U. A. Bhatti, "Robust watermarking algorithm for medical images based on log-polar transform," *Eurasip Journal on Wireless Communications and Networking*, vol. 2022, no. 1, 2022, doi: 10.1186/s13638-022-02106-6.

[18] M. Begum and M. S. Uddin, "Implementation of secured and robust DFT-based image watermark through hybridization with decomposition algorithm," *SN Computer Science*, vol. 2, no. 3, pp. 1–13, 2021, doi: 10.1007/s42979-021-00608-6.

[19] A. Ray and S. Roy, "Recent trends in image watermarking techniques for copyright protection: a survey," *International Journal of Multimedia Information Retrieval*, vol. 9, no. 4, pp. 249–270, 2020, doi: 10.1007/s13735-020-00197-9.

[20] S. Gull and S. A. Parah, "Advances in medical image watermarking: a state of the art review, " *Multimedia Tools and Applications*, vol. 83, no. 1, pp. 1407-1447, 2024, doi: 10.1007/s11042-023-15396-9.

[21] S. Maity, "Image watermarking on degraded compressed sensing measurements," *Journal of Mechanics of Continua and Mathematical Sciences*, vol. 18, no. 4, pp. 10–22, 2023, doi: 10.26782/jmcms.2023.04.00002.

[22] C. Annadurai, I. Nelson, K. N. Devi, R. Manikandan, and A. H. Gandomi, "Image watermarking based data hiding by discrete wavelet transform quantization model with convolutional generative adversarial architectures," *Applied Sciences (Switzerland)*, vol. 13, no. 2, 2023, doi: 10.3390/app13020804.

[23] Z. Jiang, C.-M. Pun, X.-C. Yuan, and T. Liu, "Robust digital watermarking method based on adaptive feature area extraction and local histogram shifting," *arXiv:Computer Science*, pp. 1–28, 2023, doi: https://doi.org/10.48550/arXiv.2302.03837.

[24] Z. Bin Faheem *et al.*, "Image watermarking using least significant bit and canny edge detection," *Sensors*, vol. 23, no. 3, pp. 1–15, 2023, doi: 10.3390/s23031210.

[25] A. F. Eldaoushy, M. I. Desouky, S. A. El-Dolil, A. S. El-Fishawy, and F. E. A. El-Samie, "Efficient hybrid digital image watermarking," *Journal of Optics (India)*, vol. 52, no. 4, pp. 2224–2238, 2023, doi: 10.1007/s12596-023-01144-7.

[26] P. V. Sanivarapu, K. N. V. P. S. Rajesh, K. M. Hosny, and M. M. Fouda, "Digital watermarking system for copyright protection and authentication of images using cryptographic techniques," *Applied Sciences (Switzerland)*, vol. 12, no. 17, 2022, doi: 10.3390/app12178724.

[27] D. Wu, X. Zhang, J. Wang, L. Li, and G. Feng, "Novel robust video watermarking scheme based on concentric ring subband and visual cryptography with piecewise linear chaotic mapping," *IEEE Trans. Circuits Syst. Video Technol.*, vol. 34, no. 10, pp. 10281–10298, 2024, doi: 10.1109/TCSVT.2024.3405558.

[28] M. Ali, "Robust image watermarking in spatial domain utilizing features equivalent to SVD transform," *Applied Sciences (Switzerland)*, vol. 13, no. 10, 2023, doi: 10.3390/app13106105.

[29] M. Li and Y. Yue, "Security analysis and improvement of dual watermarking framework for multimedia privacy protection and content authentication," *Mathematics*, vol. 11, no. 7, 2023, doi: 10.3390/math11071689.

[30] S. Ge, Z. Xia, J. Fei, Y. Tong, J. Weng, and M. Li, "A robust document image watermarking scheme using deep neural network," *Multimedia Tools and Applications*, vol. 82, no. 25, pp. 38589–38612, 2023, doi: 10.1007/s11042-023-15048-y.

[31] Ministry of Finance, "Peraturan Menteri Keuangan RI No. 133/PMK.03/2021," p. 175651, 2021.

[32] PERURI, "Peruri explains the implementation of electronic stamps on electronic documents used as evidence in court during the 37th wednesday discussion of the Bandung administrative court (in Indonesian)," 2023. https://www.peruri.co.id/press-release/peruri-jelaskan-implementasi-meterai-elektronik-pada-dokumen-elektronik-yang-dijadikan-alat-bukti-di-pengadilan-dalam-diskusi-reboan-ke-37-ptun-bandung-1 (accessed Apr. 16, 2024).

[33] M. Gupta and P. Singh, "An image forensic technique based on SIFT descriptors and FLANn based matching," 2021, doi: 10.1109/ICCCNT51525.2021.9579701.

[34] Monika and A. Passi, "Digital image forensic based on machine learning approach for forgery detection and localization," *Journal of Physics: Conference Series*, vol. 1950, no. 1, 2021, doi: 10.1088/1742-6596/1950/1/012035.

[35] K. Chandrasegaran, N. Tran, and A. Binder, "Discovering transferable forensic features," *arXiv:Computer Science Computer Science*, 2022.

[36] A. Samiha, B. Mohamed, and H. Saliha, "DFT processor implementation scheme based on Rader algorithm," *IET Circuits, Devices and Systems*, vol. 13, no. 3, pp. 385–390, 2019, doi: 10.1049/iet-cds.2018.5200.

[37] C. Rajeswari, S. Babu, and P. Venkatesan, "Analysis of MPC image compression using DCT 2 in Matlab," *International Journal of Computer Applications*, vol. 73, no. 14, pp. 25–30, 2013, doi: 10.5120/12809-0050.

[38] X. Xuan, X. Zhang, O. H. Kwon, and K. L. Ma, "VAC-CNN: a visual analytics system for comparative studies of deep convolutional neural networks," *IEEE Transactions on Visualization and Computer Graphics*, vol. 28, no. 6, pp. 2326–2337, 2022, doi: 10.1109/TVCG.2022.3165347.

BIOGRAPHIES OF AUTHORS

Dr. Ir. H. A. Danang Rimbawa, S.Si., M.T., M.Tr(Opsla), CEH, ASEAN Eng., before completing his undergraduate studies at Electronics and Instrumentation UGM in 1994, he joined the ABRI Scholarship Voluntary Officer Education (Dikpasuk) Batch VI in 1993 and was appointed as a TNI Officer. Several military and general education both at home and abroad have been followed. Completed his Masters in multimedia intelligent network ITS in 2005, Masters in marine operations at the Naval Polytechnic, Master's in business analysis and Doctoral Program (S3) in strategic (cyber operation) at Trisakti University Jakarta in 2021. Has several certifications and competencies in the fields of cyber, business analysis, and auditor. Currently serves as head of the cyber defense engineering master study program and lecturer in electrical engineering, Faculty of Defense Science and Technology, Defense University of Indonesia. He can be contacted at email: hadr71@idu.ac.id.

Sirojul Alam, S.Kom., received a bachelor of computer in information technology from Buana Perjuangan University, Indonesia. Currently, he is a hardware security modul (HSM) administrator in the digital business of The Indonesian Government Minting and Security Printing Corp. a.k.a Perum Peruri Indonesia. He also enrolled as a student of master of cyber defense engineering at The Republic of Indonesia Defense University. His research interests are data mining, machine learning, artificial intelligence, sentiment analysis, and Python programming. He can be contacted at email: sirojul.alam@tp.idu.ac.id, sirojmu@gmail.com, and sirojul.alam@peruri.co.id.

Prof. Ir. Joko. W. Saputro, M.B.A., Ph.D., after completing his Ph.D. at the University of Wisconsin – Madison, he has taught in several universities in the US as well as in Canada, Brazil, and Malaysia. He previously earned MS in computer science at the University of Hawaii at Manoa and the University of Illinois at Urbana-Champaign, and MBA at the University of Wisconsin – Madison as well. In 1995 while completing his Ph.D., he initiated the Indonesian Olympiad in Informatics (TOKI) which has been instrumental in nurturing the best young talents in informatics. After more than 20 years in the US, he returned to Jakarta and was tasked to lead several prominent initiatives including the Executive Director of Millennium Challenge Account (MCA) Indonesia, the Founding Director of the Indonesian Science Fund (ISF), and a Senior Advisor for the Green Infrastructure Initiative (GII). His current academic interest is in the area of high-performance computing and quantum computing with a focus on quantum safe cryptography. He currently serves as a lecturer in cyber defense engineering, Faculty of Defense Science and Technology, Defense University of Indonesia and also serves as the Co-Chair of the ASEAN High Performance Computing Task Force. He can be contacted at email: sap@bus.wisc.edu.

Prof. Ir. Teddy Mantoro, Ph.D., is a professor (1050) in computer science and recently serves as a head of computer science program at Nusaputra University, Sukabumi, Indonesia. His research interest is in the areas of information security, computational intelligence, pervasive computing, wireless sensor networks, and intelligent environments. He spent more than 20 years working overseas in various areas of computer science/computer engineering and visiting scholars in various centers of excellence in emerging technologies, including Media Lab – MIT, USA, DFKI-Saarland, Germany; Philip lab – Eindhoven, Nederland; SNAP Lab, UNSW, Sydney Australia, and DGI, Cambridge University, UK. Previously he was a lecturer at Advance Informatics School, Universiti Teknologi Malaysia (UTM) and the Dept. of Computer Science, International Islamic University Malaysia (IIUM) and also an adjunct professor at Taylor's University-Malaysia. He was a system analyst at the Asian Institute of Technology, Bangkok, Thailand, IT manager and a lecturer at the Department of Computer Science, Australian National University, Canberra, Australia, and EDP Manager at Microsoft Indonesia. He can be contacted at email: teddy@ieee.org.