QR Code Watermarking on Digital Signature Images Using DFT with PSO Optimization for Document Authentication

Azwa Fazilatunnisa[a*], Didi Rosiyadi[b], M. Iman Wahyudi[c]

[a,c]Departement of Informatics
Universitas Islam Negeri Sultan Maulana Hasanuddin Banten
Jl. Syech Nawawi Al-Bantani, Curug, Kota Serang
Banten, Indonesia
[b]Research Center for Cybersecurity
National Research and Innovation Agency
Jl. Sangkuriang, Dago
Bandung, Indonesia
Corresponding_azwanisaa01@gmail.com

Abstract

Electronic document forgery, including manipulation of digital signatures, has been reported as a measurable component of cybercrime cases in Indonesia. This study proposes a watermarking scheme that embeds a QR Code containing identity information into a digital signature image using the Discrete Fourier Transform (DFT), restricted to the mid-frequency region of the spectrum. The embedding strength parameter (α) was determined using Particle Swarm Optimization (PSO), with a fitness function combining Peak Signal-to-Noise Ratio (PSNR) and Normalized Cross-Correlation (NCC) across simulated attack conditions. A manually configured baseline (α = 0.05) produced a PSNR of 39.25 dB and an NCC of 1.0000 under no-attack conditions. After PSO optimization, the selected α (0.1007) produced a PSNR of 51.15 dB and an NCC of 0.9499 under no-attack conditions, corresponding to an 11.90 dB increase in PSNR relative to the baseline. Under six simulated attack conditions, JPEG compression at quality factors 75 and 50, Gaussian noise at standard deviations 10 and 25, rotation at 5°, and brightness adjustment of +50, NCC values ranged from 0.0006 to 0.3690, all below the 0.50 threshold used to classify watermark recovery as Moderate or higher. The non-blind, subtraction-based extraction method used in this study is identified as a contributing factor to the observed NCC values under attack conditions. These results indicate that mid-frequency DFT embedding with PSO optimized α produced measurable improvement in PSNR without a corresponding increase in NCC under the tested attack conditions.

Keywords: digital image watermarking, DFT, PSO, QR code, document authentication, non-blind extraction

I. INTRODUCTION

Documents in digital form are increasingly used in administrative and legal contexts, including those bearing handwritten signatures. In Indonesia, electronic document forgery accounts for approximately 22% of digital crime reports recorded by the National Cyber and Crypto Agency in 2023 [1]. One documented case occurred at the Jakarta Administrative Court in 2022, where forged government documents were identified through forensic metadata and digital signature analysis [1]. Separately, classifier-based methods for detecting forged handwritten signatures report persistent difficulty in distinguishing forged from genuine samples, due to natural variation among genuine signatures from the same individual [2]. These findings indicate a measurable gap in signature-level authentication mechanisms for digital documents.

Digital image watermarking embeds auxiliary information into an image for the purpose of authentication or ownership verification. Watermarking schemes are classified as blind, where the watermark is extracted without reference to the original image, or non-blind, which requires the original image during extraction [3]. In the additive embedding method, the watermark is added to image components via a mathematical operation, with a scaling factor controlling embedding strength [3].

Among frequency-domain methods, watermark embedding in the Discrete Fourier Transform (DFT) domain has been reported to provide resistance to rotation, scaling, and translation [4]. Embedding restricted to the mid-frequency region has been used to avoid the high sensitivity of low-frequency coefficients to modification and the susceptibility of high-frequency coefficients to attenuation under compression [4]. Selection of the embedding strength parameter, denoted α, is commonly performed manually; this approach requires repeated trial-and-error and does not generalize across different cover images [5].

Manuel et al. applied Particle Swarm Optimization (PSO) to determine α in a DFT-based watermarking scheme, reporting changes in PSNR and NCC values relative to manually configured baselines [5]. Wang et al. applied PSO with a fitness function combining PSNR and NCC across multiple simulated attacks in a medical image watermarking scheme using a wavelet-based

transform [6], indicating that PSO-based parameter search has been applied across more than one transform domain.

Robustness against image-processing operations is commonly assessed by simulating attacks such as JPEG compression, noise addition, and geometric distortion, then measuring the similarity between the original and extracted watermark. Strength-balanced optimization approaches have been proposed to address the trade-off between imperceptibility and robustness under such conditions, demonstrating that watermark strength can be adaptively adjusted according to the specific distortion intensity a watermarked image is expected to undergo, rather than fixed at a single predetermined value [7]. This indicates that the relationship between embedding strength and robustness is not fixed, but can be optimized according to the specific distortion conditions involved.

The choice of frequency band for embedding has also been reported to affect robustness outcomes differently depending on the type of distortion applied. Mid-frequency embedding has been associated with a balance between visual quality and resistance to common distortions, since low-frequency coefficients carry most of the image energy and are highly sensitive to modification, whereas high-frequency coefficients are more susceptible to attenuation under compression [4]. This pattern is consistent with the rationale for restricting the optimized embedding strength α to the mid-frequency region in the present study, in contrast to schemes that embed across the entire frequency spectrum without optimization-guided coefficient selection [5].

QR Code has been used as an information carrier in document authentication schemes. Yulianto and Wendanto reported a QR Code-based digital signature scheme using cryptographic hashing and encryption, with extraction tested under rotation, sharpening, and Gaussian noise conditions [8]. Sanivarapu et al. embedded a QR Code containing a cryptographic key pair into a host image for ownership verification [9]. Both schemes rely on cryptographic embedding rather than frequency-domain watermarking.

Three gaps follow from this review. First, DFT-based watermarking with manually configured α has been reported without an automated optimization procedure in [3] and partially addressed in [5]. Second, PSO-based parameter optimization has been reported for wavelet-based transforms [6], with limited reporting for mid-frequency DFT embedding specifically. Third, QR Code-based authentication schemes reported in [9] and [7] use cryptographic embedding rather than imperceptible watermarking. This study embeds a QR Code into the mid-frequency DFT domain of a digital signature image, with α determined using PSO, and evaluates the resulting PSNR and NCC under six simulated image-processing conditions.

II. METHOD

A. Dataset

The dataset consisted of one grayscale digital signature image used as the cover image and one QR Code image containing an encoded identity string used as the watermark payload. Both images were represented in 8-bit grayscale format. Figure 1. shows the system pipeline.

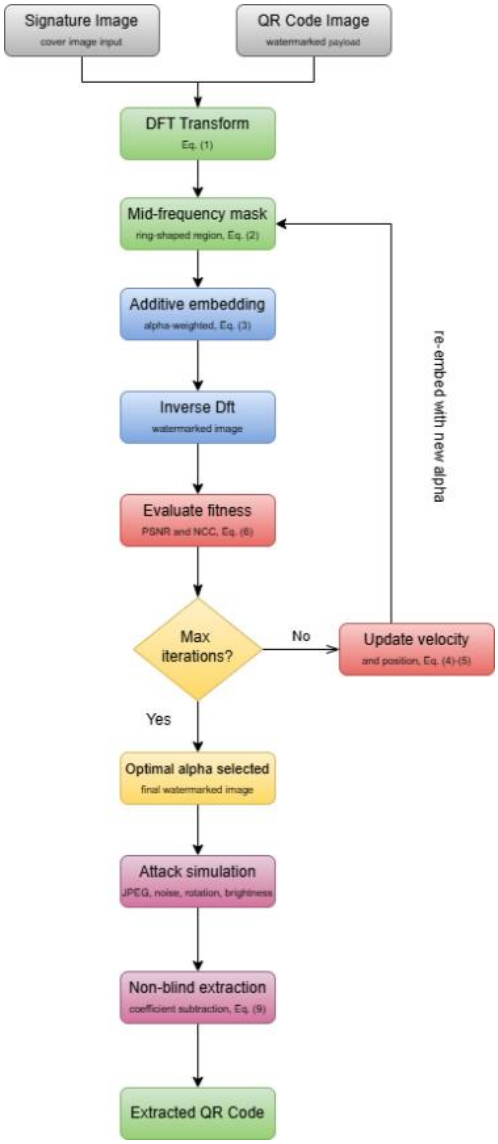

Figure 1. System flowchart DFT-PSO Watermarking Scheme

B. DFT-Based Mid-Frequency Embedding

The cover image was converted to the frequency domain using the two-dimensional DFT:

$$F(u,v) = \sum_{x=0}^{M-1} \sum_{y=0}^{N-1} f(x,y)\; e^{-j2\pi\left(\frac{ux}{M}+\frac{vy}{N}\right)} \quad (1)$$

where $f(x,y)$is the spatial-domain pixel value, $F(u,v)$is the frequency-domain coefficient, and $M, N$are the image dimensions. The spectrum was shifted to center the zero-frequency component, producing $F_{shift}(u,v)$.

Embedding was restricted to a ring-shaped region defined as:

$$Mask(u,v) = \begin{cases} 1, & r_{min}R \le d(u,v) \le r_{max}R \\ 0, & \text{otherwise} \end{cases} \quad (2)$$

where $d(u,v)$is the distance from coefficient $(u, v)$to the spectrum center, $R = \min(M,N)/2$, $r_{min} = 0.10$, and $r_{max} = 0.40$. This range was selected based on the reported sensitivity of low-frequency coefficients to modification and the reported attenuation of high-frequency coefficients under compression [4].

The QR Code, resized to 64×64 pixels, was embedded using:

$$F_w(u,v) = F_{shift}(u,v) + \alpha \cdot Q(u,v), \quad \forall (u,v) \in Mask \quad (3)$$

where $Q(u,v)$is the resized QR Code pixel value and $\alpha$is the embedding strength factor [3]. The watermarked image was obtained via inverse shift and inverse DFT.

C. Parameter Optimization Using PSO

The value of $\alpha$was determined using PSO rather than manual configuration [5]. Each particle i represents a candidate α value, updated according to:

$$v_i^{t+1} = wv_i^t + c_1 r_1 (p_i - x_i^t) + c_2 r_2 (g - x_i^t) \quad (4)$$

$$x_i^{t+1} = x_i^t + v_i^{t+1} \quad (5)$$

where $w$is the inertia weight, $c_1$and $c_2$are acceleration coefficients, $r_1$and $r_2$are random values in $[0, 1]$, $p_i$is the personal best position, and $g$is the global best position [10]. The swarm consisted of 15 particles over 25 iterations, with $\alpha \in [0.05, 0.50]$.

Fitness was calculated as:

$$Fitness(\alpha) = w_1 \cdot \frac{PSNR(\alpha)}{PSNR_{max}} + w_2 \cdot \bar{NCC}(\alpha) \quad (6)$$

with $w_1 = 0.25$, $w_2 = 0.75$, and $\bar{NCC}(\alpha)$averaged across four simulated attack conditions during optimization. Candidates producing PSNR below 30 dB were assigned a fitness value of zero. Fitness evaluation (6) and parameter update (4) (5) were repeated for 25 iterations, after which the global best $\alpha$was recorded.

D. Evaluation Metrics

PSNR was calculated as:

$$PSNR = 10\log_{10}\left(\frac{255^2}{MSE}\right), \quad MSE = \frac{1}{MN}\sum_x \sum_y [f(x,y) - f_w(x,y)]^2 \quad (7)$$

NCC was calculated as:

$$NCC = \frac{\sum_x \sum_y W(x,y)\, W'(x,y)}{\sqrt{\sum_x \sum_y W(x,y)^2 \cdot \sum_x \sum_y W'(x,y)^2}} \quad (8)$$

where $W(x,y)$and $W'(x,y)$are the original and extracted watermark pixel values [11].

E. Extraction and Robustness Testing

Extraction subtracted the cover image's DFT coefficients from the (possibly attacked) watermarked image's coefficients within the mask region, followed by inverse DFT:

$$Q'(u,v) = \frac{F'_w(u,v) - F_{shift}(u,v)}{\alpha}, \quad \forall (u,v) \in Mask \quad (9)$$

The result was normalized and binarized using Otsu's method before NCC computation. Six attack conditions were tested: JPEG compression at quality factors 75 and 50, Gaussian noise at standard deviations 10 and 25, rotation at 5°, and brightness adjustment of +50 [3]. NCC values were categorized as >0.85, >0.70, >0.50, and ≤0.50 following thresholds reported in prior watermarking evaluation studies [11].

III. Result

A. Baseline DFT Implementation

With manually configured α = 0.05 and full spectrum embedding, the watermarked image produced a PSNR of 39.25 dB. Under no-attack conditions, extraction produced an NCC of 1.0000, as summarized in Table 1.

Table 1. Baseline DFT Performance vs Target

Metric	Target	Value
PSNR	> 35 dB	39.25 dB
NCC	> 0.85	1.000

Figure 2. Visualization DFT Baseline

B. PSO Optimized Mid-Frequency Embedding

Applying mid-frequency embedding with PSO-based optimization, the algorithm converged at iteration 15 of 25, with a recorded global best $\alpha = 0.1007$. Under this configuration, PSNR was 51.15 dB and NCC was 0.9499 under no-attack conditions. This corresponds to a PSNR increase of 11.90 dB relative to the manually configured baseline.

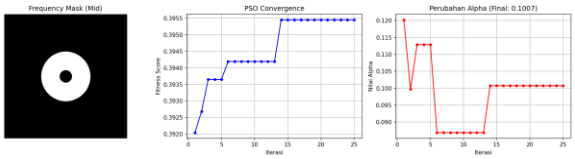

Figure 3. PSO Convergence + Alpha

C. Robustness Testing

Table 2 reports NCC values for six attack conditions using $\alpha = 0.1007$.

Table 2. NCC Under Six Attack Conditions

Attack	NCC	Status
JPEG (Q=75)	0.3690	Weak
JPEG (Q=50)	0.1251	Weak
Gaussian noise (σ=10)	0.1786	Weak
Gaussian noise (σ=25)	0.1090	Weak
Rotation (5°)	0.0006	Weak
Brightness (+50)	0.0482	Weak

The highest NCC after attack was 0.3690, recorded under JPEG compression at quality factor 75. NCC values for the remaining five conditions were: 0.1251 (JPEG quality factor 50), 0.1786 (Gaussian noise σ=10), 0.1090 (Gaussian noise σ=25), 0.0006 (rotation 5°), and 0.0482 (brightness +50). All six values fall below the 0.50 threshold used to classify watermark recovery as Moderate or higher.

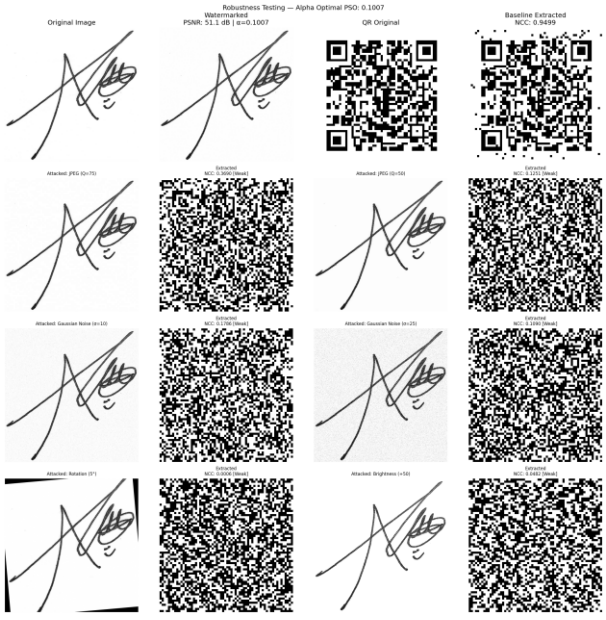

Figure 4. Visualization Robustness Testing

IV. Discussion

The 11.90 dB increase in PSNR between the manually configured baseline (39.25 dB) and the PSO-optimized configuration (51.15 dB) indicates that the search procedure identified an α value associated with lower distortion than the manually selected 0.05. This result is consistent with prior reports that PSO-based parameter search produces PSNR values different from manually configured baselines in DFT-based watermarking [5].

The relationship between PSNR and NCC observed in this study did not follow a proportional pattern. While PSNR increased by 11.90 dB after optimization, the highest post-attack NCC value (0.3690, under JPEG quality factor 75) remained below the 0.50 threshold used to classify recovery as Moderate. Four of the six tested conditions yielded NCC values below 0.20, and rotation by 5° yielded an NCC of 0.0006. This pattern indicates that an increase in PSNR was not accompanied by a corresponding increase in NCC under the tested attack conditions.

A contributing factor is the extraction procedure used in this study, defined in (9), which computes the watermark by subtracting the cover image's DFT coefficients from those of the attacked watermarked image. Under JPEG compression, Gaussian noise, rotation, or brightness adjustment, the DFT coefficients of the attacked image differ from those of the unattacked watermarked image in ways not limited to the embedded region. Because (9) assumes that the only difference between $F_w'(u,v)$ and $F_{shift}(u,v)$ is the embedded term $\alpha \cdot Q(u,v)$, any additional coefficient change introduced by the attack is included in the computed difference, which is then divided by α and treated as part of the recovered watermark. This describes a property of the non-blind subtraction-based extraction method used in this study, rather than a property specific to the cover image or the QR Code payload.

This finding differs from the robustness levels reported in [5], where PSO-optimized DFT watermarking was evaluated under JPEG compression and noise without reporting NCC values below 0.50 across the tested conditions. One difference between the present study and [5] is the extraction method: the present study used coefficient subtraction requiring the original cover image, while robustness comparisons in frequency-domain watermarking literature more commonly report results for blind extraction methods that do not require the original image during extraction [3]. The fitness function in (6) was designed to weight NCC at 0.75 relative to PSNR at 0.25 during optimization; despite this weighting, the optimizer converged to an α value (0.1007) that did not produce NCC values above 0.50

under five of six tested attack conditions. This indicates that, within the search space and attack conditions used during optimization, no tested value of α produced both PSNR above 30 dB and NCC above 0.50 across the four attack types used in the fitness calculation.

The QR Code payload used in this study encodes identity information at a fixed 64×64 pixel resolution. Sanivarapu et al. embedded a QR Code containing a cryptographic key pair using a method not restricted to the DFT domain [9], and reported extraction results without applying the JPEG compression, Gaussian noise, and rotation conditions used in the present study. A direct numerical comparison between the two studies is not possible due to differences in embedding domain, payload size, and tested attack conditions.

These results indicate that, under the tested configuration, mid-frequency DFT embedding combined with PSO optimized α produced measurable improvement in PSNR but did not produce NCC values above 0.50 under five of six tested attack conditions. The non-blind subtraction based extraction method is identified as a contributing factor to this outcome.

V. Conclusion

This study embedded a QR Code watermark into the mid-frequency region of the DFT domain of a digital signature image, with the embedding strength α determined using PSO. Under no-attack conditions, the PSO-optimized configuration (α = 0.1007) produced a PSNR of 51.15 dB and an NCC of 0.9499, compared to 39.25 dB and 1.0000 for the manually configured baseline (α = 0.05). Under six simulated attack conditions, NCC values ranged from 0.0006 to 0.3690, with all values below the 0.50 threshold used to classify watermark recovery as Moderate or higher. The non-blind, subtraction-based extraction method used in this study was identified as a contributing factor to this outcome, since coefficient changes introduced by an attack are not separable from the embedded watermark term during extraction.

These findings indicate that mid-frequency DFT embedding with PSO-optimized α, as implemented in this study, produced measurable improvement in PSNR relative to manual configuration, without a corresponding increase in NCC under the tested attack conditions. Future work may evaluate extraction methods that do not require the original cover image during extraction, and may test embedding strategies combining DFT with other transform domains under the same six attack conditions used in this study.

Declarations

Conflict of Interest

The authors declare no conflict of interest.

CRediT Authorship Contribution

Azwa Fazilatunnisa: Conceptualization, Methodology, Software, Writing original draft, Visualization, Investigation, Formal analysis; Didi Rosiyadi: Supervision, Validation, Writing, Review and Editing, Resources; M. Iman Wahyudi: Supervision, Validation, Writing, Review and Editing.

Funding

This research received no specific funding from any funding agency.

Acknowledgment

The authors would like to thank the Pusat Riset Kecerdasan Artifisial dan Keamanan Siber (PRKAKS), Badan Riset dan Inovasi Nasional (BRIN), for providing the research facilities during the internship program, as well as Universitas Islam Negeri Sultan Maulana Hasanuddin Banten for academic support throughout this research.

References

[1] E. Setiawan and Hartiwiningsih, "Optimizing the use of Digital Forensics and Information Technology in Proving Criminal Acts of Electronic Document Forgery in Indonesia," *Int. J. Law, Crime Justice*, vol. 2, no. 2, pp. 73–86, 2025, doi: https://doi.org/10.62951/ijlcj.v2i2.587.

[2] P. N. V and S. U. Kulkarni, "HANDWRITTEN SIGNATURES FORGERY DETECTION," *Int. J. Adv. Res. Comput. Commun. Eng.*, vol. 12, no. 5, pp. 1779–1785, 2023, doi: 10.17148/IJARCCE.2023.125298.

[3] S. Boujerfaoui, R. Riad, H. Douzi, F. Ros, and R. Harba, "Image Watermarking between Conventional and Learning-Based Techniques : A Literature Review," vol. 12, no. 1, pp. 1–39, 2023, doi: https://doi.org/10.3390/electronics12010074.

[4] X. Yang, Z. Zhang, Y. Jiao, and Z. Li, "A Robust Video Watermarking Algorithm Based on Two-Dimensional Discrete Fourier Transform," *MDPI J. Electron.*, vol. 12, no. 15, pp. 1–19, 2023, doi: https://doi.org/10.3390/electronics12153271.

[5] M. Cedillo-hernandez, A. Cedillo-hernandez, and F. J. Garcia-Ugalde, "Improving DFT-Based Image Watermarking Using Particle Swarm Optimization Algorithm," *MDPI J.*, vol. 9, no. 15, pp. 1–20, 2021, doi: https://doi.org/10.3390/math9151795.

[6] R. Wang, L. Liu, X. Li, Y. Xiang, and H. Wang, "A medical image watermarking method based on the combination of DTCWT and PSO optimization," *J. King Saud Univ. Comput. Inf. Sci.*, vol. 38, no. 3, pp. 1–23, 2026, doi: 10.1007/s44443-026-00480-5.

[7] H. Deng, F. Chen, P. Gan, R. Liao, and X. Yan, "A Robust Image Watermarking Scheme via Two-Stage Training and Differentiable JPEG Compression," *MDPI J. Electron.*, vol. 14, no. 22, 2025, doi: https://doi.org/10.3390/electronics14224510.

[8] B. D. Yulianto and W. Wendanto, "ENHANCED QR CODE BASED DIGITAL SIGNATURES

FOR SECURE DOCUMENT MANAGEMENT TOWARD SUSTAINABLE GREEN," *J. Ilmu Pengetah. dan Teknol. Komput.*, vol. 11, no. 4, pp. 1370–1380, 2026, doi: 10.33480/jitk.v11i4.7728.

[9] 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," *MDPI J. Appl. Sci.*, vol. 12, no. 17, pp. 1–13, 2022, doi: https://doi.org/10.3390/app12178724.

[10] J. Fang, W. Liu, L. Chen, S. Lauria, A. Miron, and X. Liu, "A Survey of Algorithms , Applications and Trends for Particle Swarm Optimization," *Int. J. Netw. Dyn. Intell.*, vol. 2, no. 1, pp. 24–50, 2023, doi: https://doi.org/10.53941/ijndi0201002.

[11] X. Liu, R. Xu, and Y. Chen, "Securing Digital Media Integrity : A Survey of Watermarking and Manipulation Detection for Image Authentication Securing Digital Media Integrity : A Survey of Watermarking and," pp. 1–35, 2025, doi: https:// doi.org/10.36227.