



A Google Colab-Based Multi-Transform Watermarking Framework for Image Authentication

Noor Jassim^{*} , Khalid Kadhim Jabbar¹ 

Department of Computer Science, College of Education, University of Mustansiriyah, Baghdad 10052, Iraq

Corresponding Author Email: nooralhussani612@gmail.com

Copyright: ©2026 The authors. This article is published by IETA and is licensed under the CC BY 4.0 license (<http://creativecommons.org/licenses/by/4.0/>).

<https://doi.org/10.18280/ijssse.160805>

ABSTRACT

Received: 17 May 2026

Revised: 5 July 2026

Accepted: 17 July 2026

Available online: 31 August 2026

Keywords:

digital watermarking, DWT-DCT-SVD, robustness, cloud system

One of the primary reasons behind the need to secure image integrity is that digital systems make it very easy for users to modify scanned documents without giving a clue that an alteration has been made. This working watermarking system creates a watermark using frequency-based domain operations through discrete cosine transforms (DCT) and discrete wavelet transforms (DWT) as well as singular value decomposition (SVD), and provides five distinct modes for watermarking and watermark retrieval operations. Users can perform any operation within the entire system by way of this cloud-based system, which allows the user to perform all tests that the entire system provides in Google Colab without requiring any sort of download or installation of any software, and also provides a whole system operation from creating watermarks to applying it and finally watermark retrieval and verification and attack generation. A system using Peak Signal-to-Noise Ratio (PSNR), Mean Squared Error (MSE) and Structural Similarity Index (SSIM) is proposed for the evaluation of images and uses Normalized Cross-Correlation (NCC) to test against a variety of attacks, which include noise attack, cropping attack, compression attack and rotation attack. The proposed system provides good levels of invisibility and robustness for validating educational and administrative images and it is shown by experiments conducted, that the system provides 48.85 dB PSNR and $0.999 + \text{SSIM}$ with complete watermark retrieval ($\text{NCC} = 1.0$, Bit Error Rate (BER) = 0) under normal operations and for common attacks like JPEG compression, Gaussian noise, Salt & pepper noise near-zero BER with >0.97 NCC values are achieved, balancing both the invisibility and the robustness.

1. INTRODUCTION

The combination of administrative offices, learning institutes, and medical services increasingly requires a reliable approach to verify the integrity of documents since they increasingly use digital documents and scanned files. These documents can easily be modified using today's editing software in a way that does not leave any traces of the changes [1]. Image authentication is a kind of active method; digital watermarking has been demonstrated as one of the most robust approaches. Digital watermarking is a technique in which imperceptible information is embedded in a host image and extracted later on to verify the integrity of image [2]. A lot of work has been carried out in frequency-domain watermarking methods, using discrete cosine transforms (DCT), discrete wavelet transforms (DWT), and singular value decomposition (SVD) techniques to achieve a reasonable security level and robustness to various signal processing attacks like compression, noise, and geometric distortions. This allows distributing watermarks over frequency coefficients [3, 4].

Several practical problems continue to face the watermarking process for document-like images despite great achievements in the technology. Document images contain less visual redundancy compared to natural photographs, so it

can be easily degraded if a moderate embedding strength is applied [5]. Many existing watermarking techniques only apply one transform domain as the method for security, whether it is DCT, DWT, or SVD, it has limitation in achieving invisibility and robustness [6]. The hybrid approach using DWT and DCT or DCT, DWT and SVD in the transform domains achieves better performance of both requirements [7]. But most of the approaches are designed for photographs or medical images while ignoring the characteristics of educational and administrative documents [8].

Looking back at the recent literature, some frameworks for cloud-based watermarking for healthcare applications have been proposed [9]. However, they are hardly able to present a reproducible cloud-based implementation for supporting multiple watermark types and embedding modes in a single framework. Furthermore, many methods were proposed to authenticate the documents based on cryptographic hashing and blockchain authentication [10]; however, few explored the combination of a multi-transform watermarking method with the practical and no-installation cloud-based process for educational documents such as certificates, transcripts and administrative reports [11]. There is a lack of a united system that integrates multi-mode frequency-domain watermarking methods, multiple watermarking formats, systematic

robustness testing, and visual detection of tampering in the cloud environment [12].

It is a great advantage for the proposed framework to be applied in image-based document authentication scenarios, such as those faced by educational institutions and public administrations. Academic certificates, transcripts, degrees, scanned administration reports, employment certificates, official forms and other documents commonly spread on electronic channels can all serve as examples. Once the watermark is invisible, the integrity of the document will be verified through the watermarking mechanism, so that any falsification, replication or unauthorized modification can be detected while the original appearance is kept.

Compared to other works, which typically focus on the investigation of a hybrid watermarking scheme, a novel and replicable watermarking framework including five different transform domain modes for embedding different types of watermarks is constructed in a cloud Google Colab space. Watermark generation, embedding, extraction, authentication, attack simulation, performance assessment and tamper localization are combined into an end-to-end cloud workflow.

2. RELATED WORKS

2.1 Deep learning-based watermarking methods

Recent advances in deep learning have significantly enhanced the performance of digital image watermarking by enabling the automatic learning of robust feature representations for watermark embedding and extraction. In particular, convolutional neural network (CNN)-based approaches have demonstrated superior robustness, imperceptibility, and resistance to common image processing attacks. Tavakoli et al. [13] proposed a CNN-based image watermarking framework integrated with the DWT, leveraging the complementary strengths of deep feature learning and frequency-domain processing to achieve improved watermark robustness while preserving image quality. to perform watermark recovery more effectively with superior feature learning and embedding characteristics. Likewise, a screen-shooting-resistant watermarking scheme [14] based on cross-attention mechanisms with a U-Net architecture to reach a watermarked image recovery rate of 95.7% when subject to a mobile phone screen-shooting attack. However, such methods require a very large training dataset and significant computing resources in the form of GPU and large time costs, and cannot meet the requirements of interactive image authentication systems, which would have been deployed to the cloud with lower computational cost, transparency of algorithm and capability to be put on lightly loaded environments.

2.2 Transform-domain watermarking methods

Transform-domain watermarking has been among the most popular methods for digital image authentication because a watermark can be implanted to frequency components with high visual quality and robustness to common signal-processing attacks. Hybrid watermarking integrating DWT, Hessenberg matrix decomposition (HMD), SVD, and Arnold scrambling has been used for medical image protection, achieving a Peak Signal-to-Noise Ratio (PSNR) of 48.94 and demonstrating robustness to noise and compression [15].

DWT-DCT watermarking scheme has also been proposed to combine with scale-invariant feature transform (SIFT) key points to increase the resistance to geometric distortions [16]. A DWT-DCT-SVD scheme based on biometrics (fingerprint, signature) is presented to improve the authentication and protection level of images [17].

Many attempts have also been made to combine DWT with DCT and SVD for improved robustness and imperceptibility. IWT-DCT-SVD framework [18] has been used to embed a watermark into singular values after 3 levels of IWT, achieving high Structural Similarity Index (SSIM) and Normalized Cross-Correlation (NCC) values with fine imperceptibility. DWT-SVD watermarking for medical image security based on LL sub-band information [19] achieves high robustness to JPEG compression and noise. Overall, hybrid transform domain watermarking schemes have made significant contributions to the balance between image quality and robustness, but most of them focus on copyright protection or medical imaging security rather than educational/administrative document authentication.

2.3 Tamper detection and image authentication methods

Other research lines focus on image authentication and tamper localization methods, which are important to guarantee the integrity of images. A fragile watermarking scheme based on bidiagonal SVD and LSB substitution achieves the detection and localization of tampered image regions [20]. A semi-fragile watermarking method based on QDFT, dual complementary watermarking, and multi-view fusion improves tamper localization, with an approximately 11% increase in F-measure [21]. Combined DWT and Schur decomposition were used to design a hybrid fragile and semi-fragile system for better tamper detection and quality of restoration [22].

Methods have been proposed to verify image authentication via transform domain verification and encryption. Frequency-domain authentication through transform-domain processing has been used to verify the integrity of color images [23]. Reversible logic key generation combined with DCT embedding enables tamper detection [24]. An image encryption framework in the DCT domain combines RSA encryption with reversible logic key generation, while low-frequency DCT coefficients provide sufficient image security with low computational complexity [25]. Spatial-domain watermarking based on LSB and MSB embedding, guided by a self-organizing map, has also been explored to improve watermarking positions and imperceptibility [26]. Although effective, these techniques normally consist of a single embedding strategy, lacking multiple watermark types and embedding modes within an integrated framework.

2.4 Research gap and motivation

As described above, great achievements have been made in the areas of deep learning-based watermarking, hybrid transform domain embedding, and tamper detection and authentication of images. However, most of them focused on a single embedding algorithm or application scope (e.g., copyright protection, medical image authentication) and are implemented as individual standalone systems. Frameworks that integrate multiple watermark types, multiple transform domain embedding modes, attack simulation, authentication and tamper detection capabilities within a unified and

repeatable platform are scarce.

In light of this gap, we propose a unified Google Colab based watermarking framework which integrates five different embedding modes (DCT, DWT, SVD, DCT-DWT, DCT-DWT-SVD), various watermark types (text, logo, QR code and hash pattern), watermark generation, embedding, extraction, authentication, robustness verification and tamper detection as an integral repeatable workflow for the application in authentication of educational and administrative documents.

3. THE PROPOSED METHOD

3.1 System model

The system implementation employs a standard digital image authentication framework. When an authorized user wishes to watermark an image, they upload it to the embedding module, which subsequently injects a private watermark prior to storing the image and distributing it across various media. The watermarked image can be sent through non-secure channels, after which it is subject to multiple alterations and manipulations. The authentication phase of the system inspects an image, which may have been modified. The extraction algorithm then reconstructs the embedded watermark from this potentially corrupted image and compares it to a reference watermark that was previously saved. The decision-making process regarding the image's authenticity is achieved by comparing a correlation metric (which includes NCC) to a pre-defined threshold: high similarity scores mean an authentic image, while low similarity scores indicate a tampered one.

3.2 Watermark generation

Two types of digital watermarks are supported in this system: fixed watermarks, which carry institutional logos and short textual information of the institution in order to establish a strong identity during watermark embedding; and dynamic watermarks, which carry QR codes and cryptographic hash values (SHA-256) representing a unique digital fingerprint of the file. Before being applied to the image in the system, the watermark is transformed into a matrix, converted to binary or grayscale, resized according to the size required to overlay the host image at the selected position in the transform domain, and finally embedded.

3.3 Multi-mode embedding and extraction

There are five possible watermarking methods used in the system. They all employ different methods to embed and extract watermarks from the image in a transform domain. All modes were labeled with the same names during implementation and experimental write-ups. The modes are defined as $M = \{DCT, DWT, SVD, DCTDWT, DCTDWT-SVD\}$. The DCT mode implements a standard DCT over 8×8 blocks of the luminance component, where some mid-frequency coefficients of each block are modified to carry the watermark bits. The DWT mode utilizes a single-level DWT on the luminance component and applies watermark embedding on the chosen sub-band of the wavelet-decomposed image. SVD is used to decompose a chosen region or the luminance component of the host image into its

singular values, which contain most of the energy and are highly stable; then the singular values are manipulated to hide the watermark information in SVD mode. For DCTDWT mode, the DWT decomposition is performed on the host image, then an arbitrary sub-band is selected and DCT is used for watermark embedding in the selected sub-band block. Finally, DCTDWT-SVD mode combines DWT decomposition on the host image, DCT modification on chosen sub-bands and SVD on the selected component to embed the watermark across multiple transform domains such that high degree of imperceptibility is maintained, also making it the most robust method among the chosen ones. Algorithm 1 describes the watermark embedding process, whereas Algorithm 2 illustrates the watermark extraction and verification process.

Algorithm 1. Multi-mode watermark embedding

Input: Host image(I), Watermark(W), selected method: method {DCT, DWT, DCTDWT, SVD, DCTDWT_SVD}
Output: One watermarked image (Iw), Quality metrics: Mean Squared Error (MSE), PSNR, SSIM

1. Load host image I; convert it to Y, Cb, Cr, then transform to Y only (for color images), and finally to grayscale. Rescale and normalize the pixel values to the desired ranges.
2. Load watermark W; convert it to a binary watermark image (0/1) and resize it to the desired capacity of watermark insertion.
3. Select mode method according to the user's choice on the interface.
4. Based on the selected mode, call the respective embedding block:
 - If method = DCT, apply the DCT embedding procedure (block-based DCT is performed on Y channel (88 blocks), then watermark bits modify some coefficients of mid-frequency range)
 - If method = DWT: apply the DWT embedding procedure (DWT is applied on Y channel, watermark is hidden in a particular sub-band)
 - If method = SVD: apply the SVD embedding procedure (SVD of Y channel or a block of Y channel is calculated, then watermark bits modify the top singular values of Y channel)
 - If method = DCT_DWT: apply the hybrid DWT-DCT procedure (DWT on Y channel, selection of sub-band and then DCT on selected sub-band to hide watermark)
 - If method = DCTDWT-SVD: apply the COMBO mode procedure, which embeds the watermark through the combination of all 3 transform domain schemes.
5. Convert the resultant Y, Cb, Cr (original for BW and manipulated for color) to the spatial domain image Iw; clip pixel values within [0, 255] and return to 8-bit RGB format if applicable.
6. Compute the values of MSE, PSNR, and SSIM between host image I and watermarked image Iw; decide the quality of image (Excellent, Good, Fair, Poor) based on these values.
7. Save the host image I, watermark W, watermarked image Iw, and the metric values.

Algorithm 2. Multi-mode watermark extraction

Input: Suspected watermarked image (Iw), Original watermark(W), selected method: method {DCT, DWT, DCTDWT, SVD, DCTDWT_SVD}
Output: Extracted watermark (), Similarity measures: NCC, Bit Error Rate (BER), Final decision: Authentic / Tampered

1. Load suspected watermarked image Iw; transform it to grayscale (assuming color images) and resize it to match the Algorithm 1 parameter.
2. Set the extraction method = m, based on the user's selected mode on the interface.
3. Based on the selected mode, call the respective extraction block:
 - If method = DCT: apply the DCT extraction procedure ((8×8))

DCT is applied to Y channel, then watermark bits are extracted from signs / magnitudes of selected DCT coefficients)

If method = DWT: apply the DWT extraction procedure (DWT applied to Y channel, then watermark bits are extracted from chosen sub-band)

If method = SVD, apply the SVD extraction procedure (using modified singular values, a watermark-like image is reconstructed)

If method = DCT_DWT: apply the hybrid DWT-DCT extraction procedure (DWT sub-band, followed by DCT on it to extract watermark bits)

If method = DCTDWT_SVD, apply the COMBO mode extraction procedure that replicates embedding.

4. Perform post-processing on extracted image pattern (thresholding to binary format) and represent as.

5. Calculate the NCC between and W.

6. Calculate the BER and W: BER = number of mismatched bits/total number of bits

7. Compare the values of NCC (and possibly BER) with predefined thresholds:

If $NCC \geq 1$ threshold, image is considered authentic.

8. Otherwise, image is identified as tampered.

9. Save extracted watermark, NCC, BER, and the decision for the results table.

The parameter embedding strength was empirically chosen from a set of preliminary experiments to balance imperceptibility with robustness. Values for $\alpha = 0.03$ were chosen for DCT, DWT, DCTDWT, and DCTDWT_SVD modes, while $\alpha = 0.01$ was chosen for SVD mode, as larger perturbations of singular values would result in clearly discernible degradation in the image. For DWT-based embedding, the HL sub-band was chosen, which provides a reasonable trade-off between robustness and visual fidelity. In the DCT-based modes, the watermark bits were embedded within the mid-frequency coefficients within each 88 block such that it does not cause perceivable degradation to the image but still offer resistance against compression attacks. For authentication purposes, an image is said to be genuine when NCC is 0.95; otherwise, the image is said to be tampered with. This threshold was obtained by conducting various experiments on the robustness of the system under the above-discussed attacks.

3.4 Attack simulation and evaluation metrics

The system generates a fast-detection scheme that verifies the extracted watermark by directly comparing it with the original one (W) using NCC and BER. The same module lets the user input typical digital attacks such as JPEG compression, additive Gaussian noise, salt-and-pepper noise, blurring, rotation, cropping and scaling. The watermarked image will be treated for every attack by watermark re-extraction and, recalculation of NCC and BER to determine the influence of the attack. The system generates a simple tamper-localization map by drawing red dots on locations suffering from worst watermark degradation showing some points of alteration if there exists.

To maintain equal experimental conditions during robustness evaluation, the parameters of attacks were kept constant. JPEG compression was carried out with a quality factor of 50, Gaussian noise with zero mean and variance 0.01, salt and pepper noise with density of 0.02, central cropping with area of 10% of image area, Gaussian blur with kernel size of 5×5 , scaling factor of 0.8 and image rotation by 5 degrees. These attacks are commonly encountered during document dissemination.

Five metrics have been employed in the performance evaluation. Visual quality imperceptibility has been assessed with MSE, PSNR and SSIM. These metrics achieve good results if MSE is low, while PSNR and SSIM should be high (close to 1). NCC and BER have been used to determine its authentication and robustness properties. Successful watermark recovery appears through high NCC and low BER, whereas tampered results are detected by low NCC or high BER. Authentic class has been given to all the images whose NCC is equal or greater than the given threshold, while the rest of the images have been classified as Tampered. The value for each of the metrics calculated in this experiment has been compiled in the Results and Discussion.

3.5 System workflow

The full process of the suggested system is illustrated in Figure 1. The user will create the necessary project folders and a storage area before uploading a host image. After uploading a host image, the user is required to select one of four kinds of watermarks namely text and logo, QR code, hash-based pattern, etc. And one of five embedding methods, namely DCT, DWT, SVD, DCT_DWT, COMBO, etc. After the watermark embedding, by the quick extract function, the system will calculate NCC to test proper watermarking. Apply digital attacks, including JPEG, Gaussian noise, salt-and-pepper, cropping, rotating, and blurring, etc on the image, and then re-extract the watermark to recalculate NCC and BER. The system automatically saves the images, tamper maps, and metrics in the summary file. A final decision is made as authentic when NCC is greater than or equal to, and the others are tampered with.

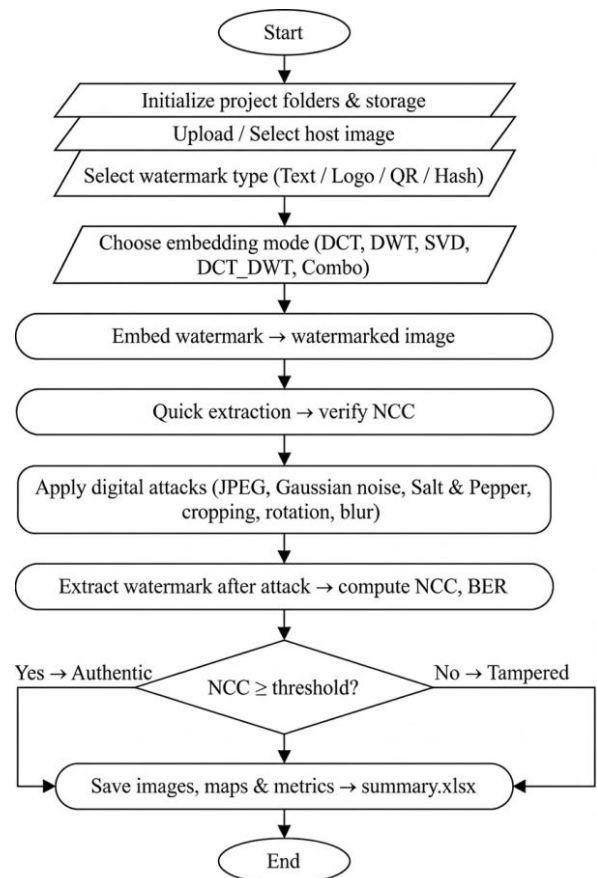


Figure 1. System-level workflow of the proposed watermarking system

4. IMPLEMENTATION

4.1 Development environment

It runs from the cloud system, which provides code to run on Python 3.x on Google Colab; thus, the users do not have to install software on their machines. Google Colab gives instant access to a cloud CPU enough to perform transform-based image processing and a consistent run time for consistent results to perform various tests for easy experiment and to share with just a notebook link for the users to execute. The code is written with the use of NumPy for computations, cv2 and pillow for images (opening/saving images) and PyWavelets for DWT transformation and scikit-image for quality measurements like MSE and SSIM and pandas to get results from the automatic results file summary.xlsx and for plotting and ipywidgets for an interactive button interface running within the notebook. Google Drive can be considered as a permanent storage system which creates a hierarchical structure of folders namely host images, watermark images, embedded images, extracted watermarks, attack results, tamper maps, and summary log file, as the notebook is successfully connected to the drive.

4.2 Cloud storage and logging

The file structure is predefined on Google Drive, which is created by the notebook when the system is started. The root folder host/ will include all the necessary sub-folders, because host-images are the original host images and watermark-images are watermark images and embedded-images are watermarked images using the same timestamp-based file naming convention and attacks-results store the attacked images and extracted-watermarks store the extracted watermarks and tamper-maps store the visual tamper-localization result.

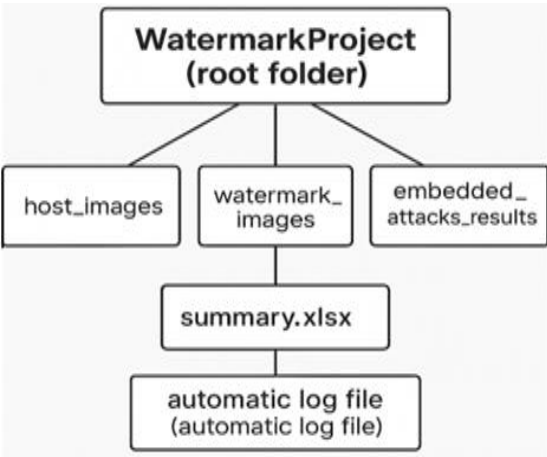


Figure 2. Simplified folder structure of the watermarking project on Google Drive

An Excel file, summary.xlsx, is used to automatically aggregate metadata of each run. This file records information like Image ID, watermark type, embedding mode, attack type, MSE, SSIM, NCC, BER, final decision, and timestamp. Configuration information, along with runtime parameters, will be written into a file. This enables the user to reproduce the state of the environment for different runs (Figure 2). It is worth noting that the system enables end-to-end experiments’

reproducibility. Therefore, different users are able to conduct the same experiments under different Colab sessions.

5. RESULTS AND DISCUSSION

5.1 Experimental setup

The proposed system has been tested on 512×512 benchmark images, which have been stored as PNG images. We have used four types of watermarks: logo, text, QR code, and hash-based watermark. For every image and watermarks five embedding modes (DCT, DWT, SVD, DCT_DWT, COMBO) are utilized and the watermarked images were subjected to standard attacks (JPEG compression, Gaussian and salt & pepper noises, cropping and rotation). The imperceptibility is measured by MSE and SSIM, and NCC and BER used to measure robustness and authentication.

Two exemplary types of documents, such as images, were chosen as test data. Quality images represent digitally generated images with little or no compression artifacts, whereas quality images are produced by moderate JPEG compression and some scanner-related degradation, which try to imitate acquisition in a real administration system. The size of every image was normalized to 512×512 before embedding into the images for fairness.

5.2 Imperceptibility results

In this step of invisibility testing, we examined imperceptibility by considering two images. We analyzed five embedding methods with the same watermark and the same embedding parameters. Before processing the watermark images, they were all standardized with a common resolution. The data in this case demonstrated that MSE values for DCT DWT and DCT_DWT were extremely low, which indicated that the watermark image did not contain any visually discernible distortion and that for SVD and COMBO images higher distortions existed because of their stronger embedding methods. The value of the image quality did not influence the outcome because the algorithm with the preprocessing methods provided an equally effective performance.

Figure 3 illustrates the comparison of the two images and gives a perspective of minor differences between high-quality and low-quality watermark images of different embedding methods. Table 1 gives quantitative imperceptibility values for two images.

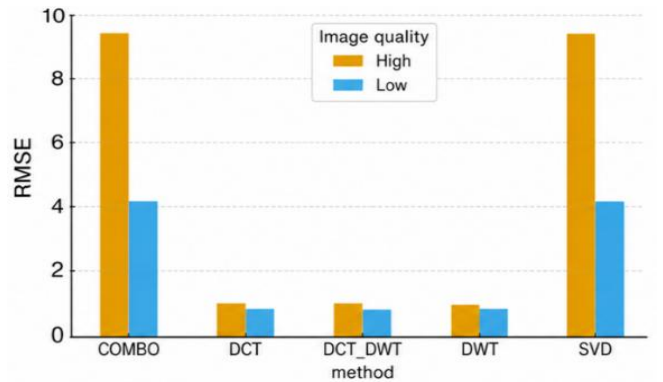


Figure 3. Mean Squared Error (MSE) comparison for high- and low-quality images across embedding methods

Table 1. Baseline imperceptibility for high- and low-quality images

Image Quality	Method	Alpha	PSNR	SSIM	NCC	MSE
watermark -high quality_color.png	DCT	0.03	48.1492	0.9932	1	0.9958
	DWT	0.03	48.1421	0.9932	1	0.9974
	SVD	0.01	38.3051	0.9962	1	9.6065
	DCT_DWT	0.03	48.0065	0.9935	1	1.0290
	COMBO	0.03	38.3051	0.9962	1	9.6065
watermark -low quality_color.png	DCT	0.03	48.6769	0.9991	1	0.8818
	DWT	0.03	48.6599	0.9992	1	0.8853
	SVD	0.01	41.9483	0.9994	1	4.1519
	DCT_DWT	0.03	48.8521	0.9992	1	0.8470
	COMBO	0.03	41.9483	0.9994	1	4.1520

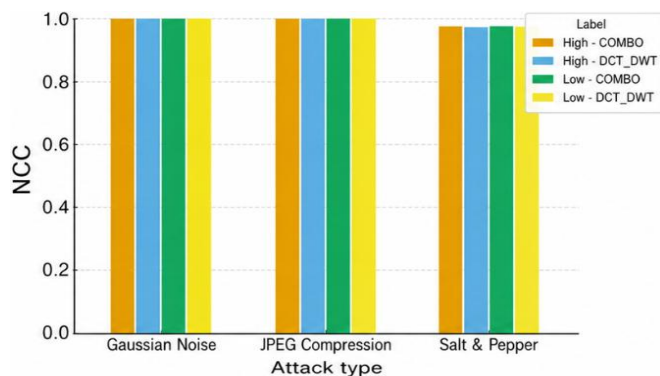
Table 2. Robustness metrics (NCC, BER, SSIM) for DCT_DWT, and COMBO under common attacks

Image Quality	Method	Watermark Type	Attack Type	NCC	BER	SSIM
watermark -high quality	DCT_DWT	HASH	Gaussian Noise	0.9955	0	0.9875
			Salt & Pepper	0.979	0.0203	0.9529
			JPEG Compression	0.9995	0	0.9985
	COMBO		Gaussian Noise	0.9955	0	0.9874
			Salt & Pepper	0.9791	0.0203	0.9524
			JPEG Compression	0.9995	0	0.9985
watermark -low quality	DCT_DWT		Gaussian Noise	0.9951	0	0.9571
			Salt & Pepper	0.9786	0.019	0.9324
			JPEG Compression	0.9996	0	0.984
	COMBO		Gaussian Noise	0.9949	0	0.9565
			Salt & Pepper	0.9758	0.0216	0.9219
			JPEG Compression	0.9996	0	0.984

5.3 Robustness of discrete cosine transforms, discrete wavelet transforms, and COMBO under common attacks

As a further measure of robustness, we examined the two embedding techniques (DCT_DWT and COMBO) with three common attack operations (Gaussian noise, salt-and-pepper noise, and JPEG compression) and with the high- and low-quality versions of each image. For each setup, the NCC, BER, and SSIM were calculated between the attacked and original watermarks. This allows for direct comparison of the two methods as well as showing the effect of image quality on the recovered watermark.

The behavior of the different attacks and image quality is identical as reported in Table 2 containing numerical robustness results.

**Figure 4.** NCC comparison for DCT_DWT and COMBO across attacks and image qualities

In Figure 4, it can be observed that NCC value for all attacks, for both image qualities, remains more than 0.97, BER is almost zero and SSIM is almost one. The observation of the results also proved that the DCT_DWT and COMBO are robust, and the developed system is lightly influenced by

initial image quality. The discrepancy between high- and low-quality images is small, showing robustness with regard to the input image quality.

5.4 Computational cost

The average time taken to embed and extract per image for each of the five embedding modes is shown in Table 3. Each scheme completes both embedding and extraction in less than one second on the test platform. The single-transform methods are faster, and the hybrid methods are slightly more expensive. The increase in time associated with DCT_DWT and COMBO is quite low and should be of no concern for many applications.

Table 3. Average embedding and extraction times per image for the five embedding modes

Method	Embedding Time (s)	Extraction Time (s)
DCT	0.18	0.15
DWT	0.20	0.17
SVD	0.24	0.21
DCT_DWT	0.28	0.24
COMBO	0.35	0.30

5.5 Comparative performance of embedding modes

This suggests that DCT_DWT shows a good balance of robustness and quality, but that COMBO offers high robustness but is more computationally intensive.

Figure 4 displays the complete performance results among five embedding modes for imperceptibility (PSNR, SSIM), robustness (NCC, BER), and complexity (embedding time). As far as the image imperceptibility is concerned, the DCT and DWT modes yield the highest PSNRs (close to 48 dB) whereas the SVD and COMBO modes result in a bit lower PSNRs but with higher SSIM. Under standard conditions, perfect recovery for watermark for all methods has been reached

(NCC = 1.0, BER = 0). The hybrid DCT_DWT mode results in the optimum performance for visual quality and complexity whereas the COMBO mode increases the robustness but requires more execution time.

5.6 Tamper localization results

Besides numerical robustness measurements, system also

offers visual tamper-localization output to indicate affected areas by noise/tampering. With a Gaussian noise added to the extracted watermark as shown in Figure 5, tamper map shows red dots distributed around the affected regions and a normal region is clear. This shows that not only can the system detect tampering, but also intuitively present affected regions.



Figure 5. Tamper-localization output showing red markers over the affected regions

5.7 Overall discussion

The system described proves to achieve the optimal tradeoff between imperceptibility and robustness. All methods in the baseline experiment produce imperceptible embeddings with tiny MSE, perfect watermark retrieval (NCC = 1, BER = 0), and a discrepancy between high- and low-quality images is trivial. In normal attack conditions, the DCT_DWT and COMBO exhibit comparable, steady NCC values and virtually zero BERs, which means that the two algorithms maintain excellent robustness and image quality variation still has an insignificant effect.

The tamper-localization output maps the affected areas in a red-dot map, offering a clear view of the attacked regions. All in all, it offers robust authentication and reliable localization. The experimental outcome suggests that the designed framework appears promising in the administrative and educational document authentication field owing to the combined effect of imperceptibility, robustness and reproducibility. Nevertheless, more evaluation based on larger benchmark datasets and various attack cases must be carried out before actual implementation is warranted.

The analysis of Table 4 shows the comparison of the three modes in question. Overall, DCT_DWT achieves an excellent compromise among the measures of imperceptibility, robustness and speed, while COMBO has the highest robustness but a small sacrifice in processing speed.

Table 4. Comparative performance of embedding modes

Method	PSNR (dB)	SSIM	NCC	BER	Embedding Time (s)
DCT	48.15	0.9932	1.000	0	0.18
DWT	48.14	0.9932	1.000	0	0.20
SVD	38.30	0.9962	1.000	0	0.24
DCT_DWT	48.01	0.9935	1.000	0	0.28
COMBO	38.30	0.9962	1.000	0	0.35

The DCT and DWT modes generate the best quality because the watermark energy is injected into a certain number of transform coefficients with only limited modification. The SVD mode results in slightly larger distortion due to singular value perturbation, yet benefits from improved numerical stability. The hybrid DCTDWT mode balances between

imperceptibility and robustness by making use of both frequency localization and energy compaction. The COMBO mode offers further improvement in robustness using multiple-stage embedding, but at the cost of somewhat larger distortion. Therefore, the DCTDWT mode is considered as the best choice in terms of overall performance and it is optimal if robustness against attacks is more essential than visual fidelity, in which the COMBO mode outstands other methods.

6. CONCLUSIONS

In this paper, a cloud-based watermarking method for image authentication is designed. Several types of watermarks, along with five transform domain embedding modes (DCT, DWT, SVD, DCTDWT, and DCTDWTsVD), are designed under the reproducible environment provided by Google Colab. Experimental results prove a clear embedding process with good PSNR and SSIM values; meanwhile, the NCC of hybrid DCTDWT and COMBO is still above 0.97 under the ordinary attacks. As for now, we have only conducted experiments using a small image set and a few typical image attacks. Future research will cover larger benchmark image datasets and more attacks (like print-scan attacks and geometric transformations) and compare them with the state-of-the-art methods based on deep learning techniques.

ACKNOWLEDGMENT

The authors would like to thank Mustansiriyah University, Baghdad, Iraq, for its support in the present work.

REFERENCES

[1] Sharma, S., Zou, J.J., Fang, G., Shukla, P., Cai, W.D. (2024). A review of image watermarking for identity protection and verification. Multimedia Tools and Applications, 83: 31829-31891. <https://doi.org/10.1007/s11042-023-16843-3>

[2] Luo, H.X., Li, L., Li, J.C. (2025). Digital watermarking technology for AI-generated images: A survey. Mathematics, 13(4): 651.

- <https://doi.org/10.3390/math13040651>
- [3] Soundrapandian, R., Rajendiran, K., Gurunathan, A., Victor, A., Selvanambi, R. (2023). Analysis of DWT–DCT watermarking algorithm on digital medical imaging. *Journal of Medical Imaging*, 11(1): 014002. <https://doi.org/10.1117/1.JMI.11.1.014002>
 - [4] Li, L., Zhang, H.J., Meng, J.L., Lu, Z.M. (2023). Robust PDF watermarking against print–scan attack. *Sensors*, 23(17): 7365. <https://doi.org/10.3390/s23177365>
 - [5] Kumar, C. (2024). Hybrid optimization for secure and robust digital image watermarking with DWT, DCT and SPIHT. *Multimedia Tools and Applications*, 83: 31911–31932. <https://doi.org/10.1007/s11042-023-16903-8>
 - [6] Mokashi, B., Bhat, V.S., Pujari, J.D., Roopashree, S., Mahesh, T.R., Alex, D.S. (2022). Efficient hybrid blind watermarking in DWT-DCT-SVD with dual biometric features for images. *Contrast Media & Molecular Imaging*, 2022(1): 2918126. <https://doi.org/10.1155/2022/2918126>
 - [7] Nawaz, S.A., Li, J.B., Bhatti, U.A., Shoukat, M.U., Li, D.K., Raza, M.A. (2024). Hybrid watermarking algorithm for medical images based on digital transformation and MobileNetV2. *Information Sciences*, 653: 119810. <https://doi.org/10.1016/j.ins.2023.119810>
 - [8] Qu, C.F., Liu, C.Y., Liu, Y.L., Chen, X.H., Peng, D.Z., Guo, F.J. (2023). Towards robust tampered text detection in document image: New dataset and new solution. In 2023 IEEE/CVF Conference on Computer Vision and Pattern Recognition (CVPR), Vancouver, BC, Canada, pp. 5937–5946. <https://doi.org/10.1109/CVPR52729.2023.00575>
 - [9] Anand, A., Singh, A.K. (2021). Cloud based secure watermarking using IWT-Schur-RSVD with fuzzy inference system for smart healthcare applications. *Sustainable Cities and Society*, 75: 103398. <https://doi.org/10.1016/j.scs.2021.103398>
 - [10] Boonkrong, S. (2025). Design of an academic document forgery detection system. *International Journal of Information Technology*, 17: 5175–5187. <https://doi.org/10.1007/s41870-024-02006-6>
 - [11] Li, D., Ran, X.J., Jin, X. (2024). Anti-counterfeit framework of electronic certificate based on QR code and seal watermark. *Multimedia Tools and Applications*, 83: 80523–80542. <https://doi.org/10.1007/s11042-024-18803-x>
 - [12] Nawaz, S.A., Li, J.B., Shoukat, M.U., Bhatti, U.A., Raza, M.A. (2023). Hybrid medical image zero watermarking via discrete wavelet transform-ResNet101 and discrete cosine transform. *Computers & Electrical Engineering*, 112: 108985. <https://doi.org/10.1016/j.compeleceng.2023.108985>
 - [13] Tavakoli, A., Honjani, Z., Sajedi, H. (2023). Convolutional neural network-based image watermarking using discrete wavelet transform. *International Journal of Information Technology*, 15(4): 2021–2029. <https://doi.org/10.1007/s41870-023-01232-8>
 - [14] Liu, L.S., Xu, P., Xue, Q.W. (2025). Screen shooting resistant watermarking based on cross attention. *Scientific Reports*, 15: 17016. <https://doi.org/10.1038/s41598-025-00912-8>
 - [15] Chaudhary, H., Garg, P., Vishwakarma, V.P. (2025). Enhanced medical image watermarking using hybrid DWT–HMD–SVD and Arnold scrambling. *Scientific Reports*, 15: 9710. <https://doi.org/10.1038/s41598-025-94080-4>
 - [16] Hamidi, M., Haziti, M.E., Cherfi, H., El Hassouni, M. (2021). A hybrid robust image watermarking method based on DWT–DCT and SIFT for copyright protection. *Journal of Imaging*, 7(10): 218. <https://doi.org/10.3390/jimaging7100218>
 - [17] Harika, D., Noorullah, S. (2023). Implementation of image authentication using digital watermarking with biometric. *International Journal of Engineering Technology Management Science*, 7(1): 154–167. <https://doi.org/10.46647/ijetms.2023.v07i01.023>
 - [18] Shubuh, S., Ernawan, F., Amrullah, A., Wahyu, P. (2024). Robust image watermarking based on IWT–DCT–SVD for copyright protection. *Iraqi Journal for Computer Science and Mathematics*, 5(4): 3. <https://doi.org/10.52866/2788-7421.1201>
 - [19] Zermi, N., Khaldi, A., Kafi, R., Kahlessenane, F., Euschi, S. (2021). A DWT-SVD based robust digital watermarking for medical image security. *Forensic Science International*, 320: 110691. <https://doi.org/10.1016/j.forsciint.2021.110691>
 - [20] Rijati, N., De Rosal Ignatius Moses Setiadi, P., Andono, N. (2022). Fragile image watermarking based on bidiagonal SVD-LSB for tamper detection and localization. *International journal of intelligent engineering and systems*, 15: 315–324. <https://doi.org/10.22266/ijies2022.1231.30>
 - [21] Ouyang, J., Huang, J.T., Wen, X.Z., Shao, Z.H. (2023). A semi-fragile watermarking tamper localization method based on QDFT and multi-view fusion. *Multimedia Tools and Applications*, 82: 15113–15141. <https://doi.org/10.1007/s11042-022-13938-1>
 - [22] Vaidya, S.P., Kandala, R.N.V.P.S., Mouli, P.V.S.S.R.C., Zaini, H.G., Jaffar, A., Paramasivam, P., Ghoneim, S.S.M. (2025). A robust fragile watermarking approach for image tampering detection and restoration utilizing hybrid transforms. *Scientific Reports*, 15: 17645. <https://doi.org/10.1038/s41598-025-01297-4>
 - [23] Gaid, S.K., Jabbar, K.K. (2021). Frequency domain for color image authentication proofing. *Journal of Physics: Conference Series*, 1963(1): 012094. <https://doi.org/10.1088/1742-6596/1963/1/012094>
 - [24] Ghozzi, F., Jabbar, K.K., Fakhfakh, A. (2025). Image authentication proofing scheme based on RLG by employing the characteristics of DCT. *Iraqi Journal of Science*, 66(9): 3951–3968. <https://doi.org/10.24996/ij.s.2025.66.9.34>
 - [25] Jabbar, K.K., Ghozzi, F., Fakhfakh, A. (2023). Robust color image encryption scheme based on RSA via DCT by using an advanced logic design approach. *Baghdad Science Journal*, 20(6): 2593–2607. <https://doi.org/10.21123/bsj.2023.8715>
 - [26] Jabbar, K.K., Tuieb, M.B., Thajeel, S.A. (2022). Digital watermarking by utilizing the properties of self-organization map based on least significant bit and most significant bit. *International Journal of Electrical and Computer Engineering*, 12(6): 6545–6558. <http://doi.org/10.11591/ijece.v12i6.pp6545-6558>