A Secure IoT-Based User Authentication System Using Hybrid Watermarking with RFID and Raspberry Pi Edge Computing

Noor Jassim and Khalid Kadhim Jabbar
Department of Computer Science, College of Education, Mustansiriyah University, 10052 Baghdad, Iraq
noorjassim@uomustansiriyah.edu.iq

Keywords: IoT Authentication, Digital Watermarking, DWT-DCT, RFID, Raspberry Pi, Edge Computing, SHA-256, Quantization Index Modulation.

Abstract: The increasing number of Internet of Things (IoT) devices creates a greater need for authentication solutions that protect user privacy and operate on devices with limited resources. The research study presents an IoT authentication system which uses Radio Frequency Identification (RFID) technology together with SHA-256 hashing and a Discrete Wavelet Transform-Discrete Cosine Transform (DWT-DCT) digital watermarking method that runs on a Raspberry Pi edge device which connects to a Django authentication system. The system uses Quantization Index Modulation (QIM) with step $\Delta = 24.0$ to embed the SHA-256 hash of a user's RFID unique identifier as a 256-bit binary payload which targets the LL approximation subband of the image luminance channel, with sevenfold repetition coding and majority-voting error correction as additional elements. The testing process which used 20 USC-SIPI benchmark images achieved a PSNR value of 49.68 dB together with an SSIM value of 0.9974 which indicated exceptional visual imperceptibility. The system maintains operation with NCC values exceeding 0.95 during testing that used six different signal processing attacks, while JPEG compression only causes minor data loss (NCC = 0.99943, BER = 1.93 %). The complete authentication system achieved perfect accuracy in 75 testing sessions, while the total processing time took about 3.0 seconds, which proved that the system can operate in real time on devices with limited processing power. The proposed method outperforms current state-of-the-art methods in protecting visual content while delivering full authentication through RFID technology.

1 INTRODUCTION

The fast growth of Internet of Things (IoT) systems across industrial and healthcare and smart home and critical infrastructure sectors has created an urgent security problem because organizations now need to verify user and device identities in environments that suffer from limited computational power and insecure communication paths and uncertain physical control of hardware [1]. Traditional authentication systems which use static passwords and PINs and cryptographic certificates were created for use in high-performance computing systems but they do not meet the special security needs of IoT systems [2]. The results of authentication failures in IoT environments go beyond typical data breaches because lost identity verification systems in smart healthcare networks and industrial control systems and access control systems can lead to physical danger and major economic damages [3], [4].

Digital watermarking has become an effective method for secret authentication of multimedia content in various settings according to research [5]. Watermarking technology provides hidden authentication through its digital image watermarks which protect identity data by transferring it through normal-looking digital content instead of creating a detectable security threat that can be intercepted [6]. The transform-domain watermarking methods work by using frequency-based image data to hide information within less noticeable frequency components while they use visual masking techniques to create minimal visible changes to the content [7]. The proposed system allows users to embed cryptographic hash sequences into images which they can later extract and authenticate on a remote server [8], [9].

The Radio Frequency Identification (RFID) technology provides an effective foundation for obtaining identities in authentication systems because it operates without power requirements and has affordable pricing and extensive usage throughout the world [10]. The network system faces major security threats when RFID UIDs get transmitted through its

infrastructure because unencrypted transmission allows hackers to execute replay attacks while anyone with access to standard market equipment can create physical duplicates of RFID tags [11]. The combination of RFID-based identity acquisition with cryptographic hashing and watermarking-based covert transmission creates a security system which prevents all raw RFID identifiers from being transmitted through the network [12].

The adoption of edge computing models which allocate processing tasks to nearby devices that access data sources has achieved widespread acceptance in Internet of Things security applications because these models reduce latency while they increase user privacy protection [13]. Single-board computers such as the Raspberry Pi provide a practical vehicle for implementing edge-side authentication preprocessing which enables users to run Python-based image processing systems and connect RFID devices through GPIO and access remote servers using standard HTTP protocols [14]. The deployment of watermark embedding algorithms on Raspberry Pi edge devices ensures that all sensitive identity transformations are performed locally without exposing intermediate data to network interception [15].

The Discrete Wavelet Transform (DWT) enables users to analyze the spatial-frequency content of an image through its multi-resolution capability which produces two different subbands for the image at three different resolution levels. The approximation subband (LL) retains approximately 93 % of total image energy and exhibits superior stability under signal processing operations including JPEG compression, additive noise, and geometric transformations [16]. The Discrete Cosine Transform (DCT) decomposes an image block into a sum of cosine functions, concentrating image energy in low-frequency coefficients; mid-frequency DCT coefficients offer a balance between perceptual imperceptibility and robustness to compression-based attacks [17]. The hybrid DWT-DCT approach combines the multi-resolution analysis of wavelets with the block-based frequency modulation of the cosine transform, enabling watermark embedding within stable LL subband coefficients and exploiting QIM-based error correction for enhanced reliability [18], [19].

This paper makes the following contributions. The first contribution presents a complete hardware-validated IoT authentication system which combines RC522 RFID hardware and Raspberry Pi edge computing and SHA-256 hashing and a hybrid DWT-DCT watermarking scheme into one client-server system. The second contribution presents a DWT-DCT embedding architecture which uses QIM to operate within 8×8 DCT blocks of the DWT LL approximation subband while it combines sevenfold repetition coding with majority voting to reach a PSNR value of 49.68 dB and maintain NCC value above 0.95 during five of six attacks tested. The third evaluation tests 20 USC-SIPI benchmark images through six different signal processing attacks. The system achieves 100 % authentication accuracy through 75 controlled sessions which require approximately 3.0 seconds to complete because the system demonstrates real-time performance on limited IoT devices.

2 RELATED WORK

Hamidi et al. [20] proposed a semi-blind hybrid DWT-DCT-SIFT watermarking scheme for copyright protection which embeds watermarks in mid-band DCT coefficients of the HL1 subband using PN sequences while storing SIFT keypoints to correct geometric distortions. The testing used 30 images which produced an average PSNR result of 47.81 dB and a NC value that exceeded 0.98. The system development establishes core differences because it uses real-time RFID-based IoT authentication while employing QIM with repetition coding for hash delivery and operating on Raspberry Pi hardware without SIFT requirements.

Shariq and Singh [21] developed a new RFID authentication protocol which uses vector space technology to protect user privacy in Internet of Things applications while operating with minimal processing requirements that work on limited resource devices. Their scheme ensured tag anonymity and untraceability through vector-space operations without relying on public-key cryptography. The proposed protocol only covered authentication functions without implementing digital watermarking for secret payload transmission and it lacked integration with image-based identity concealment and edge computing systems.

Garg and Kishore [22] created a concealed hybrid watermarking method which unites two-level DWT with DCT through artificial bee colony (ABC) meta-heuristic algorithm optimization. The watermark is embedded in the LL2 sub-band of a 2-level Haar DWT decomposition after applying block-wise DCT, with the optimal embedding strength determined by a multi-objective fitness function that simultaneously maximises PSNR and Normalised Correlation across thirteen attack types. The system operates without detection while establishing watermark security through encrypted watermarks. Experiments with eleven 512×512 grayscale images produced PSNR results that exceeded 40 dB and NC results that surpassed 0.9 across all evaluated attacks. The system

requires ABC optimization which makes it unfit for real-time operation in edge environments while the system functions as a static copyright protection solution that does not connect to any RFID-based identity verification system.

Singh et al. [23] designed a Medical Image Watermarking (MIW) system which uses regional analysis to create a secure transmission method for Internet of Medical Things (IoMT) environments. The system divides medical images into two parts which include a Region of Interest (RoI) and a Region of Non-Interest (RoNI). The system uses adaptive LSB substitution to insert tamper detection bits into RoI while it uses DWT-SVD to insert encrypted Electronic Patient Records and a QR-coded hospital logo into RoNI. The research tested 50 medical images which produced results that showed average PSNR values above 40 dB and tamper detection accuracy rates that exceeded 97%. The system shares its IoT-integrated watermarking motivation with the proposed system but it focuses on maintaining medical image integrity and protecting patient record confidentiality instead of using RFID for user identity authentication. The system does not operate on constrained single-board edge hardware.

Fares et al. [24] developed two different blind watermarking methods which safeguard both the privacy and the trustworthiness of medical images. The first method DCT-Schur embeds watermarks into mid-frequency DCT coefficients while the second method DWT-Schur uses Schur decomposition for watermarking purposes within LH and HL DWT subbands. The schemes embed patient metadata and a hash for integrity verification, achieving PSNR values of 47.98 dB (DCT-Schur) and 49.20 dB (DWT-Schur). The PSNR results approach the performance of our proposed method yet their systems only provide security for medical images stored in unchanging databases without using RFID identity acquisition or edge computing deployment or real-time authentication pipeline integration.

3 PROPOSED METHODOLOGY

3.1 System Overview and Architecture

The proposed authentication system operates within a client-server architecture in which a Raspberry Pi single-board computer functions as the edge computing client and a Django-based web application functions as the authentication server. The basic security principle establishes that no sensitive identification data can be transmitted through network connections which includes both the original RFID UID and its SHA-256 hash. The authentication credential becomes hidden through the digital image which uses the DWT-DCT watermarking scheme as its protection method while only the harmless watermarked image gets sent. The complete system architecture appears in Figure 1.

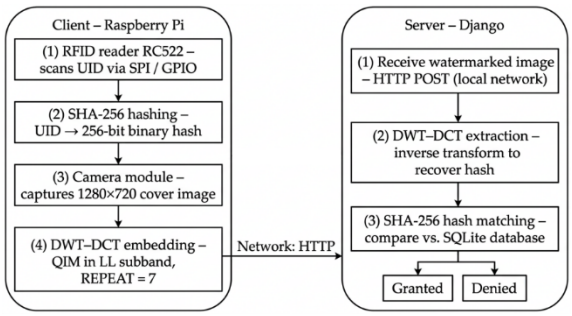

Figure 1: Proposed IoT-based authentication system architecture.

The system operates in two phases: user registration and user authentication. The registration process begins with the collection of the RFID UID which is then hashed using SHA-256 and stored in the server's SQLite database. During authentication, the UID is hashed, embedded into a camera-captured image using DWT-DCT watermarking, and the watermarked image is sent to the server for hash extraction and database comparison.

3.2 RFID Identity Acquisition and SHA-256 Hashing

The RC522 RFID reader module enables user identity acquisition through its connection to Raspberry Pi which operates using SPI protocol through GPIO pins. The RC522 tag reader connects to passive MIFARE Classic 1K tags which operate at 13.56 MHz to obtain the tag UID through the SimpleMFRC522 Python library. The system processes UID data in its entirety through local processing without sending any information over networks. SHA-256 generates a 256-bit authentication payload from the UTF-8 encoded UID string which it processes through the hash function. The one-way nature of SHA-256 ensures the original UID cannot be reconstructed from the hash. The system performs a conversion of the digest into a 256-element binary sequence which it uses for watermark creation.

3.3 Image Acquisition and Preprocessing

The USB camera module captures color images from 1280×720 pixel resolution through its real-time

recording capability. The frame is resized to 512×512 pixels, converted from BGR to YCrCb color space, and the luminance channel Y is extracted for all subsequent processing. The chrominance channels Cb and Cr remain unchanged, which guarantees that the final watermarked image maintains complete color accuracy. All preprocessing operations use floating-point arithmetic because it reduces rounding errors that occur during transform computations.

3.3 Hybrid DWT-DCT Watermark Embedding

The embedding algorithm applies a single-level two-dimensional Haar DWT to the luminance channel Y, which results in four subband decomposition of the signal into LL (approximation) and LH and HL and HH subbands. The LL subband, which holds about 93 percent of total image energy, functions as the embedding domain because it maintains stability during signal processing operations. The LL subband is adjusted to dimensions divisible by 8, and a DC level shift of 128.0 is applied to center the coefficient distribution around zero. Figure 2 shows the complete process for embedding.

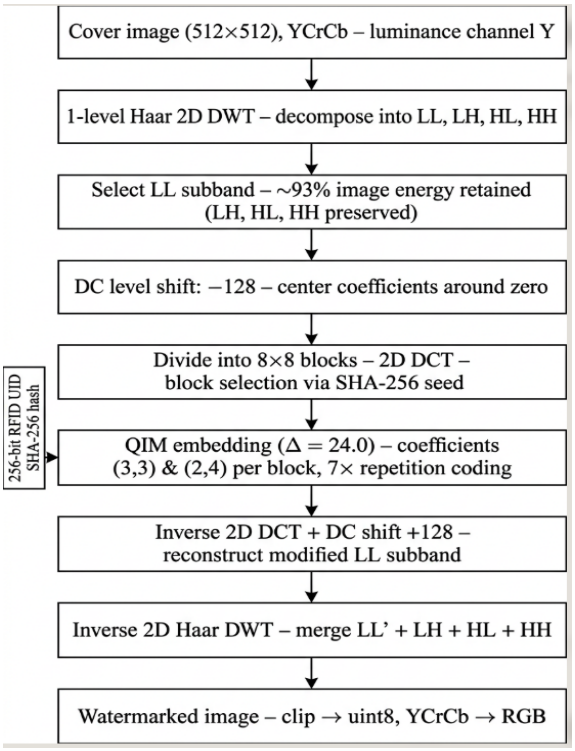

Figure 2: Hybrid DWT-DCT watermark embedding pipeline.

The cryptographically secure block selection mechanism produces block indices through its operation which generates 256×REPEAT block indices that total 1792 because block indices are selected without replacement. The pseudorandom seed is derived by applying SHA-256 to the secret key and converting the first eight hexadecimal characters to an integer seed which ensures that identical block sequences will occur during both embedding and extraction. The system embeds each of its 256 hash bits into seven different blocks which are chosen from separate block sets to create multiple encoding paths that will help detect errors.

Within each selected 8×8 block, a 2D DCT is applied and two mid-frequency coefficients at positions (3,3) and (2,4) are modified using Quantization Index Modulation. For bit value 0, the coefficient magnitude is adjusted to the 0.25Δ quantization zone center; for bit value 1, to the 0.75Δ zone center, where Δ = 24.0; this step size was selected empirically to balance imperceptibility against robustness, since larger Δ values improve resistance to compression and noise at the cost of a higher visual distortion, and Δ = 24.0 was found to keep PSNR above 45 dB while maintaining reliable bit extraction under the tested attacks. The mid-frequency coefficient positions (3,3) and (2,4) were chosen because they lie outside the low-frequency region most sensitive to visual distortion and the high-frequency region most vulnerable to compression loss, consistent with common practice in DCT-domain QIM watermarking. Figure 3 illustrates the QIM principle.

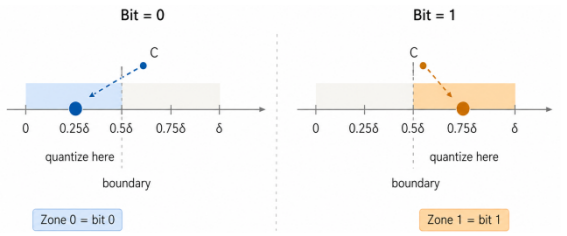

Figure 3: QIM embedding principle showing quantization zones for bit-0 and bit-1.

The DC level shift gets restored through block-level embedding because the inverse 2D Haar DWT uses the modified LL subband along with the unaltered LH HL HH subbands to recreate the spatial domain luminance channel. The system first clips the luminance to [0, 255] and then converts it to uint8 before blending it back with the original Cb and Cr channels. The conversion from YCrCb to RGB creates the final watermarked carrier image.

3.4 Watermark Extraction and Authentication Decision

The Django server converts the received watermarked image to YCrCb, applies a single-level Haar DWT, and reproduces the identical block sequence using the same secret key seed. For each selected block, a 2D DCT is applied and the QIM decision rule is evaluated at positions (3,3) and (2,4). Intra-block majority voting over two coefficients yields a per-block bit, and inter-repetition majority voting over all seven repetitions of each bit position produces the final 256-bit hash reconstruction. The extracted hash is compared against the SQLite database; a match results in ACCESS GRANTED, otherwise ACCESS DENIED, and the outcome is logged with a timestamp.

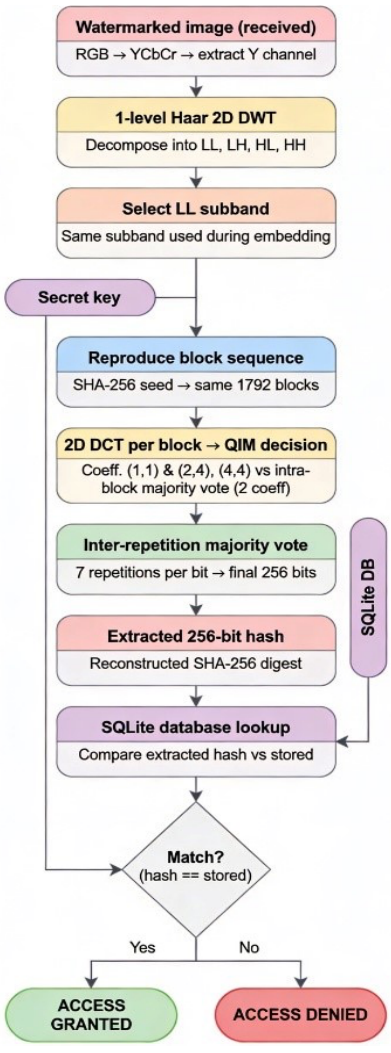

Figure 4: DWT-DCT watermark extraction and authentication decision pipeline.

Figure 4 shows how the watermark extraction process works with the authentication system on the Django server. The received watermarked image is converted to YCbCr, the Y channel undergoes a single-level Haar DWT, and the same secret-key seed regenerates the 1792 LL-subband blocks used during embedding. The system applies a 2D DCT and QIM decision process to each block which is selected to create a 256-bit hash through intra- and inter-repetition majority voting. The system compares the reconstructed hash with the stored value in the SQLite database; when the hashes match, the system grants access but it denies access when the hashes do not match and it records the decision.

4 EXPERIMENTAL RESULTS

4.1 Experimental Setup

All experiments were conducted using 20 benchmark images from the USC-SIPI Image Database [25], spanning diverse visual categories including portraits, aerial photography, natural scenes, military vehicles, and color test images. All images were used at 512×512 pixel resolution in uncompressed TIFF format with 8 bits per channel. The hardware comprised a Raspberry Pi single-board computer, an RC522 RFID reader, and a USB HD camera. Server-side processing ran on a local machine hosting the Django application. DWT-DCT parameters were fixed as: BLOCK = 8, Δ = 24.0, REPEAT = 7, target DCT coefficients at positions (3,3) and (2,4). Performance was evaluated using PSNR, SSIM, MSE, NCC, and BER.

4.2 Imperceptibility Results

The DWT-DCT embedding quality metrics for the 20 USC-SIPI test images appear in Table 1. The method achieves an average PSNR of 49.68 dB and SSIM of 0.9974, which demonstrates its ability to maintain excellent visual content protection because the results exceed the 36 dB standard. All 20 images exceed 48.4 dB PSNR. Images with uniform texture regions (APC, Aerial, Tank series) achieve higher PSNR (above 51 dB) compared to texture-rich images (Airplane, Baboon), which shows how different image types affect embedding quality.

The visual quality assessment displayed in Figure 5 compares the original images with the DWT-DCT watermarked versions of four selected test images. The watermarked images show complete visual similarity to their original forms which proves that the embedding process remains completely hidden from human viewers.

Figure 5: Visual quality assessment -original vs. DWT-DCT watermarked (Lena, Baboon, Peppers, Splash).

Table 1: DWT-DCT embedding quality metrics for 20 USC-SIPI benchmark images.

Image	PSNR (dB)	SSIM	MSE
APC	51.0	0.9981	0.5211
Aerial	51.0	0.9991	0.5213
Airplane (F-16)	48.5	0.9947	0.9288
Baboon (Mandrill)	48.6	0.9987	0.9044
Boat	48.6	0.9969	0.8974
Car and APCs	51.0	0.9985	0.5186
Couple	51.0	0.9986	0.5184
Earth from Space	48.6	0.9969	0.8889
Fishing Boat	51.0	0.9987	0.5211
Oakland	48.7	0.9979	0.8845
Peppers	48.7	0.9961	0.8710
San Diego	48.7	0.9985	0.8853
San Francisco	48.6	0.9939	0.9090
Splash	48.7	0.9938	0.8764
Stream and Bridge	51.0	0.9994	0.5190
Tank	51.0	0.9987	0.5211
Tank2	51.0	0.9992	0.5212
Truck	51.0	0.9987	0.5211
House	48.6	0.9964	0.8996
Lena	48.7	0.9958	0.8767
Average	49.68	0.9974	0.7252

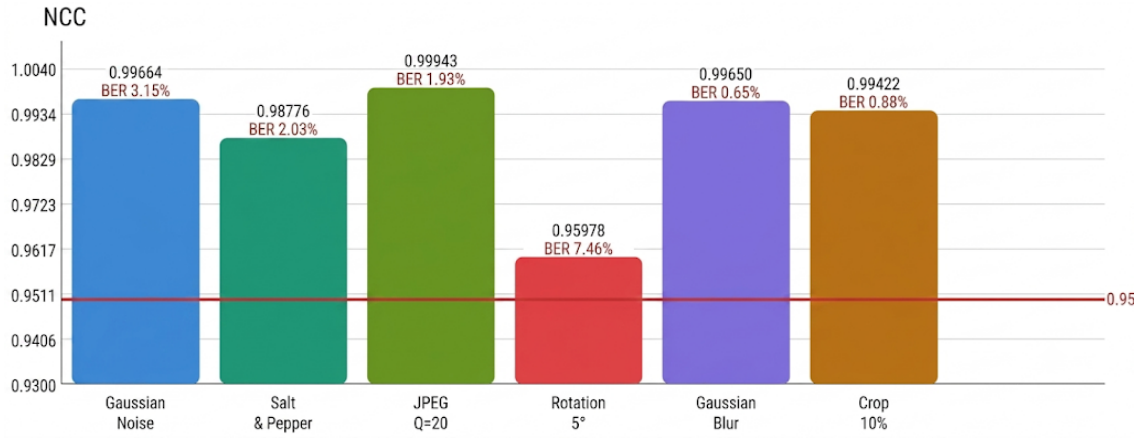

Figure 6: NCC and BER under six signal processing attacks - DWT-DCT method.

4.3 Robustness Under Signal Processing Attacks

Six common signal processing attacks were applied to the entire set of watermarked images in order to test the robustness of the proposed DWT-DCT framework. Table 2 lists the average normalized cross-correlation (NCC), bit error rate (BER), and structural similarity measure (SSIM) for each attack. Under the JPEG compression attack with Q = 20, the NCC and BER of the watermark were 0.99943 and 1.93%, respectively. This demonstrates the robustness of the proposed watermarking approach owing to the LL subband embedding. The lowest BER of 0.65% was obtained using the Gaussian blur attack. A rotation of 5° represented the most severe attack in terms of NCC and BER, with 0.95978 and 7.46%, respectively. Figure 6 illustrates NCC and BER under six signal processing attacks

Table 2: DWT-DCT robustness under six signal processing attacks.

Attack	NCC	BER (%)	SSIM	Status
Gaussian Noise (σ=25)	0.99664	3.15 %	0.6010	Robust
Salt & Pepper (4%)	0.98776	2.03 %	0.6355	Robust
JPEG Compression (Q=20)	0.99943	1.93 %	0.9532	Robust
Rotation (5°)	0.95978	7.46 %	0.7268	Moderate
Gaussian Blur (5×5)	0.99650	0.65 %	0.8854	Robust
Crop (10%)	0.99422	0.88 %	0.9797	Robust

4.4 Visual Quality Assessment

The DWT-DCT watermarked images are visually indistinguishable from their originals. The embedding of the 256-bit SHA-256 hash payload using QIM with Δ = 24.0 introduces no perceptible artifacts in any of the 20 test images. This visual imperceptibility is a critical requirement for the proposed authentication system, as the watermarked image must not arouse suspicion when transmitted over the network. Figure 7 shows the complete watermarking scheme. In this scheme, a hash function is used to hash a unique identifier (UID) to obtain a 256-bit binary payload. This payload is embedded into the cover image (e.g., Lena image of size 512x512 pixels) using QIM with a redundancy factor of x7. In this scheme, the watermarked image is obtained with a PSNR of 48.70 dB and SSIM of 0.9958. This shows that the watermarked image is visually imperceptible. Moreover, the hash values obtained have an NCC of 0.9994 and BER of 0.39%.

Figure 7: Additional visual quality comparison across test images.

4.5 Authentication System Performance

For end-to-end authentication, ten registered RFID tags were used in seventy-five authentication sessions, consisting of fifty successful authentication attempts, five for each tag, and twenty-five unsuccessful authentication attempts by unregistered

tags. Under normal operating conditions, it was seen that the proposed method, "DWT-DCT," achieved a success rate of 100%, with a false acceptance rate of 0% and a false rejection rate of 0%. Table 3 and 4 show the accuracy and latency of each stage.

The overall end-to-end latency, which amounts to a total of approximately 3.0 seconds, consists of the following steps: RFID scanning (~0.5 s), SHA-256 hashing (~0.01 s), image capturing (~0.3 s), DWT-DCT embedding (~1.0 s), HTTP transmission (~0.2 s), server-side extraction (~1.0 s), and database matching (~0.01 s). All the constituent steps fall well within the acceptable range of 5 seconds for a real-time authentication system.

4.6 Comparative Analysis with Literature

The comparison between the proposed DWT-DCT approach and other state-of-the-art techniques is presented in Table 5. The proposed approach achieves the best PSNR performance (49.68 dB) compared to other techniques, and it is the only technique that supports complete RFID-based IoT authentication with real-time operation on Raspberry Pi edge devices.

The hybrid framework of DWT-DCT demonstrates significant benefits in terms of imperceptibility, achieving the best PSNR value of 49.68 dB. However, it is worth noting that this system is the only one in this comparison that provides RFID-based IoT authentication, edge-side crypto-processing via SHA-256, and real-time server-side verification on resource-constrained Raspberry Pi platforms. The main limitation of this technique is associated with rotation attacks, where BER is equal to 7.46%.

Table 3: DWT-DCT authentication accuracy and system metrics.

Metric	Result	Notes
Authentication accuracy	100.0 %	Zero errors across 75 sessions
False acceptance rate (FAR)	0.00 %	No unauthorized grants
False rejection rate (FRR)	0.00 %	No legitimate denials
Registered RFID tags	10 tags	Distinct MIFARE Classic 1K
Total test sessions	75	50 registered + 25 unregistered

Table 4: End-to-end processing latency per stage breakdown.

Processing Stage	Location	Latency (s)	Description
RFID Tag Scan	Client	~0.50	RC522 reads MIFARE Classic 1K tag UID
SHA-256 Hashing	Client	~0.01	UID string to 256-bit binary hash
Image Capture	Client	~0.30	USB camera capture at 1280×720 px
DWT-DCT Embedding	Client	~1.00	Hash embedded into LL subband via QIM
HTTP Transmission	Network	~0.20	Watermarked image POST to Django server
DWT-DCT Extraction	Server	~1.00	Inverse transform recovers 256-bit hash
Database Matching	Server	~0.01	Extracted hash compared vs. SQLite DB
Total end-to-end	All	~3.02	RFID scan to final access decision

Table 5: Comparative analysis with state-of-the-art methods.

Reference	Method	PSNR (dB)	Platform	RFID	RT
Hamidi et al. [20]	DWT-DCT-SIFT	47.81	PC simulation	No	No
Garg & Kishore [22]	DWT-DCT + ABC	40–50	PC simulation	No	No
Singh et al. [23]	DWT-SVD (IoMT)	45.93	PC simulation	No	No
Fares et al. [24]	DCT/DWT-Schur	47.98–49.20	PC simulation	No	No
Proposed	DWT-DCT + QIM	49.68	Raspberry Pi	Yes	Yes

5 CONCLUSIONS

In this study, a secure IoT-based user authentication framework has been proposed by incorporating RFID-based identity acquisition, SHA-256-based cryptographic hash functions, and a hybrid DWT-DCT-based digital watermarking technique on a Raspberry Pi-based IoT device, which communicates with a Django-based authentication server. In the DWT-DCT-based technique, the authors obtained a PSNR of 49.68 dB and a SSIM of 0.9974 on 20 USC-SIPI images, thereby confirming the high level of imperceptibility in the watermarked images. In the robustness analysis, the authors performed six different signal processing attacks on the watermarked images and obtained a high value of correlation coefficient (NCC) greater than 0.95 in all cases, with a nearly perfect preservation of the images under JPEG compression (NCC = 0.99943). Furthermore, the overall authentication framework has obtained 100% accuracy in 75 test cases with a latency of 3.0 seconds, thereby confirming the real-time feasibility of the framework on a Raspberry Pi-based IoT device. In the comparative analysis, the authors have found that the proposed framework has obtained a high level of imperceptibility in addition to the overall RFID-based authentication capability, which has not been addressed in the existing state-of-the-art techniques. Furthermore, the privacy-preserving capability of the overall framework, where no raw identity information has been sent over the network, has also been identified as a major security advantage of the overall framework in comparison with the existing RFID-based authentication schemes.

REFERENCES

[1] M. A. Al-Garadi, A. Mohamed, A. K. Al-Ali, X. Du, I. Ali, and M. Guizani, "A survey of machine and deep learning methods for internet of things (IoT) security," IEEE Communications Surveys & Tutorials, vol. 22, no. 3, pp. 1646-1685, 2020.

[2] A. Mosenia and N. K. Jha, "A comprehensive study of security of internet-of-things," IEEE Transactions on Emerging Topics in Computing, vol. 5, no. 4, pp. 586-602, 2017.

[3] S. Hameed, F. I. Khan, and B. Hameed, "Understanding security requirements and challenges in internet of things (IoT): A review," Journal of Computer Networks and Communications, vol. 2019, pp. 1-14, 2019.

[4] K. Zhao and L. Ge, "A survey on the internet of things security," in Proc. International Conference on Computational Intelligence and Security, pp. 663-667, 2013.

[5] I. J. Cox, M. L. Miller, J. A. Bloom, J. Fridrich, and T. Kalker, Digital Watermarking and Steganography, 2nd ed. Burlington, MA: Morgan Kaufmann, 2008.

[6] F. Cayre, C. Fontaine, and T. Furon, "Watermarking security: Theory and practice," IEEE Transactions on Signal Processing, vol. 53, no. 10, pp. 3976-3987, 2005.

[7] N. Dey, A. B. Roy, S. Das, and A. B. Chaudhuri, "DWT-DCT-SVD based interlacing watermarking technique for medical images," Journal of Computer and Electrical Engineering, 2012.

[8] M. Cedillo-Hernandez et al., "Robust watermarking method in DFT domain for effective management of medical imaging," Signal, Image and Video Processing, vol. 9, no. 5, pp. 1163-1178, 2015.

[9] V. Solachidis and I. Pitas, "Circularly symmetric watermark embedding in 2-D DFT domain," IEEE Transactions on Image Processing, vol. 10, no. 11, pp. 1741-1753, 2001.

[10] K. Finkenzeller, RFID Handbook, 3rd ed. Chichester, UK: Wiley, 2010.

[11] A. Juels, "RFID security and privacy: A research survey," IEEE Journal on Selected Areas in Communications, vol. 24, no. 2, pp. 381-394, 2006.

[12] H. M. Sun, W. C. Ting, and K. H. Wang, "On the security of Chien's ultralightweight RFID authentication protocol," IEEE Transactions on Dependable and Secure Computing, vol. 8, no. 2, pp. 315-317, 2011.

[13] W. Shi, J. Cao, Q. Zhang, Y. Li, and L. Xu, "Edge computing: Vision and challenges," IEEE Internet of Things Journal, vol. 3, no. 5, pp. 637-646, 2016.

[14] M. Satyanarayanan, "The emergence of edge computing," Computer, vol. 50, no. 1, pp. 30-39, 2017.

[15] F. Bonomi, R. Milito, J. Zhu, and S. Addepalli, "Fog computing and its role in the internet of things," in Proc. MCC Workshop on Mobile Cloud Computing, pp. 13-16, 2012.

[16] I. Daubechies, Ten Lectures on Wavelets. Philadelphia, PA: SIAM, 1992.

[17] N. Ahmed, T. Natarajan, and K. R. Rao, "Discrete cosine transform," IEEE Transactions on Computers, vol. 23, no. 1, pp. 90-93, 1974.

[18] R. Soundrapandiyan, K. Rajendiran, A. Gurunathan, A. Victor, and R. Selvanambi, "Analysis of DWT-DCT watermarking algorithm on digital medical imaging," Journal of Medical Imaging, vol. 11, no. 1, p. 014002, 2024.

[19] B. Chen and G. W. Wornell, "Quantization index modulation: A class of provably good methods for digital watermarking and information embedding," IEEE Transactions on Information Theory, vol. 47, no. 4, pp. 1423-1443, 2001.

[20] M. Hamidi, M. El Haziti, H. Cherifi, and M. El Hassouni, "A hybrid robust image watermarking method based on DWT-DCT and SIFT for copyright protection," Journal of Imaging, vol. 7, no. 10, p. 218, 2021.

[21] M. Shariq and K. Singh, "A novel vector-space-based lightweight privacy-preserving RFID authentication protocol for IoT environment," Journal of Supercomputing, vol. 77, no. 8, pp. 8532-8562, 2021.

[22] P. Garg and R. R. Kishore, “An efficient and secured blind image watermarking using ABC optimization in DWT and DCT domain,” Multimedia Tools and Applications, vol. 81, pp. 36947-36975, 2022.

[23] P. Singh, K. J. Devi, H. K. Thakkar, and K. Kotecha, “Region-based hybrid medical image watermarking scheme for robust and secured transmission in IoMT,” IEEE Access, vol. 10, pp. 8974-8993, 2022.

[24] K. Fares, A. Khaldi, K. Redouane, and E. Salah, “DCT & DWT based watermarking scheme for medical information security,” Biomedical Signal Processing and Control, vol. 66, p. 102403, 2021.

[25] “USC-SIPI Image Database,” University of Southern California Signal and Image Processing Institute, [Online]. Available: https://sipi.usc.edu/database/.