Journal of Discrete Mathematical Sciences & Cryptography
ISSN 0972-0529 (Print), ISSN 2169-0065 (Online)
Vol. 29 (2026), No. 1, pp. 349–361
DOI : 10.47974/JDMSC-2608

Secure image transmission using chaotic encryption and DWT watermarking on reconfigurable platform

Shweta Salunkhe [†]
Department of Electronics and Telecommunication
Bharati Vidyapeeth's College of Engineering for Women
Pune 411043
Maharashtra
India

Altaf Osman Mulani [*]
Department of Electronics and Telecommunication
SKN Sinhgad College of Engineering
Korti
Pandharpur 413304
Maharashtra
India

Deepali Shahane [§]
Department of Computer Science and Applications
School of Computer Science and Engineering
Dr. Vishwanath Karad MIT World Peace University
Pune 411038
Maharashtra
India

Manish Rana [‡]
Department of Computer Engineering
Vidyalankar Institute of Technology
Wadala East
Mumbai 400037
Maharashtra
India

[*] *E-mail:* **shwetasalunkhe16@gmail.com**
[†] *E-mail:* **draomulani.vlsi@gmail.com (Corresponding Author)**
[§] *E-mail:* **shahanedeepali@gmail.com**
[‡] *E-mail:* **manishrana23@gmail.com**

Shivam Mahendra Shukla [@]
Department of Mechanical Engineering
University of Mumbai
Mumbai 400032
Maharashtra
India

Makarand M. Jadhav [#]
Department of Electronics and Telecommunication
Mukunddas Lohia College of Engineering
Pune 411004
Maharashtra
India

Abstract

With the exponential rise in digital image transmission across unsecured networks, ensuring image confidentiality and authenticity has become essential. Traditional cryptographic methods like AES provide strong confidentiality but lack built-in authentication mechanisms. On the other hand, digital watermarking, especially in the Discrete Wavelet Transform (DWT) domain, offers robust image authentication. Combining both techniques and deploying them on reconfigurable platforms such as FPGAs addresses the growing demand for secure, high-performance image communication systems. This paper presents a hybrid image authentication framework that integrates AES encryption for confidentiality and DWT-based invisible watermarking for authenticity. The process involves preprocessing the image, applying AES encryption, embedding a watermark in the high-frequency sub-bands of the DWT domain, and implementing the system on an FPGA using Verilog HDL. The AES and DWT modules are designed as separate cores, synthesized, and verified using Xilinx tools on Spartan-6 FPGA. The watermark, encrypted if necessary, is embedded in the HH sub-band to ensure robustness and imperceptibility. Simulations conducted on standard grayscale images (e.g., Lena, Cameraman) demonstrate high image fidelity, with PSNR exceeding 40 dB and SSIM values above 0.95. The watermark remained resilient under Gaussian noise, JPEG compression, and median filtering, with a bit error rate below 2%. FPGA implementation showed efficient resource utilization, consuming 4321 LUTs and 2176 flip-flops, with a total power consumption of 354 mW and latency of 1.02 µs. These results confirm the system's real-time suitability and robustness. The proposed hybrid image authentication system successfully ensures both security and authenticity in an image.

Subject Classification: *94A08, 68U10, 68M10.*

Keywords: *Image authentication, AES encryption, DWT watermarking, FPGA implementation, Reconfigurable system.*

[@] *E-mail:* **shivam.shukla269@gmail.com**
[#] *E-mail:* **makj123@yahoo.com**

1. Introduction

The digital age has revolutionized the way information is created, shared, and consumed. With the widespread use of smartphones, digital cameras, and social media platforms, images have become a primary medium for communication. However, this proliferation of digital content has also made it easier for malicious actors to tamper with or duplicate visual data. Image authentication, therefore, is an essential aspect of digital security that ensures the originality and integrity of image content. Traditional cryptographic techniques such as the Advanced Encryption Standard (AES) are effective for securing image data against unauthorized access. AES is a symmetric key encryption algorithm that provides robust protection by transforming plaintext images into unreadable cipher images. However, while AES ensures confidentiality, it does not inherently provide mechanisms for authenticity verification or tamper detection. This is where digital watermarking techniques, particularly in the Discrete Wavelet Transform (DWT) domain, complement cryptography by embedding imperceptible but retrievable authentication data within the image. DWT watermarking transforms the image into the frequency domain, allowing for robust and imperceptible embedding of authentication signals. By embedding watermark information into high-frequency coefficients, the watermark remains resilient to various image manipulations, including compression, noise, and filtering. The combination of AES and DWT leverages the strengths of both techniques—encryption for confidentiality and watermarking for authenticity.

Field Programmable Gate Arrays (FPGAs) offer an ideal platform for deploying such hybrid security systems. Unlike general-purpose processors, FPGAs provide hardware-level parallelism and customizability, enabling high-speed and power-efficient processing. Reconfigurable platforms also offer flexibility in adapting to new security protocols, making them suitable for future-proof implementations in sensitive applications such as military surveillance, medical diagnostics, and forensic imaging.

This paper aims to develop a secure, high-speed, and efficient image authentication system using AES encryption and DWT-based invisible watermarking on an FPGA platform. The key objectives include:

1. Ensuring the confidentiality of image data through AES encryption.
2. Embedding an invisible and robust watermark using DWT.
3. Implementing the combined system on a reconfigurable FPGA platform.
4. Evaluating the system's performance in terms of PSNR, SSIM, latency, and area efficiency.
5. Testing the resilience of the watermark against common image processing attacks.

2. Literature Survey

Image security and authentication have gained considerable attention due to the increasing need for secure multimedia transmission. Chaotic systems are

widely employed due to their deterministic and sensitive nature, ideal for encryption purposes. Singh et al. [1] introduced a chaotic map-based visually meaningful image encryption scheme, enabling secure and authenticated data transmission. Similarly, Al-Hyari et al. [2] utilized chaotic maps coupled with the Collatz conjecture to generate powerful encryption keys, enhancing image cryptography. Haq and Shah [3] developed a 4D mixed chaotic system employing substitution-diffusion operations for RGB image encryption. Shang et al. [4] focused on facial image encryption using Zaslavsky and Arnold cat maps with bit-plane decomposition. Singh et al. [5] systematically reviewed chaotic map-based image security methods, while Kamarposhti, Ghorbani, and Yadollahi [6] presented a comprehensive survey detailing taxonomy and challenges in image encryption. Zhou et al. [7] proposed a chaos and Line map-based encryption algorithm, while Hu, Wu, and Zhou [8] introduced a color image encryption system using a 2D hyperchaotic Henon map with cross diffusion. Zhou et al. [9] presented a bit-level multiple color image encryption scheme, and Zhang et al. [10] emphasized visual encryption for secure traffic image transmission. Modern developments integrate compression and security. Tiwari et al. [11] leveraged 3D chaotic maps for compressed image encryption. Hazzazi et al. [12] adopted chaotic maps with Fibonacci and Tribonacci transformations alongside DWT for robust encryption. In watermarking, Poonam and Arora [13] proposed a DWT-SVD technique for robust digital image watermarking. Alrammahi and Sajedi [14] combined DWT, RDWT, and Möbius transformations for robust watermarking schemes.

Al-Khafaji, Al-Himyari, and Alharbi [15] introduced a genetic algorithm-based DWT-SVD watermarking method ensuring imperceptibility and robustness. A detailed review by Begum and Uddin [16] examined existing digital image watermarking approaches. Genetic algorithms were also employed by Wazirali et al. [17] to optimize steganographic capacity and quality. Robust watermarking under wireless conditions was investigated by Ma, Chen, and Wu [18], while Rajwar, Deep, and Das [19] and Melman and Evsutin [20] surveyed metaheuristic-based optimization in image security systems. FPGA platforms for image authentication were utilized by Mulani and Mane [21], while Deshpande, Karande, and Mulani [22] and Mulani and Mane [23] worked on area-optimized AES implementations for reconfigurable platforms. Kulkarni, Mulani, and Mane [24] implemented robust invisible watermarking for image authentication, whereas Mane and Mulani [25] proposed a high-speed area-efficient AES algorithm on FPGA, enhancing cryptographic processing in real-time applications. Gopalakrishnan *et al.* [26] explored a blockchain-enabled framework to counter deception, deepfake generation, and counterfeit systems, emphasizing decentralized verification and immutable data integrity in digital ecosystems. Kapoor and Gupta [27] proposed a hybrid symmetric cryptography scheme for secure web communication that combines AES and DES algorithms to strengthen encryption efficiency and minimize computational latency. Bermani, Murshedi, and Abod [28] developed a hybrid cryptographic model for cloud storage that integrates RSA and AES to safeguard data confidentiality during transmission and storage, highlighting its adaptability to multi-user cloud

architectures. Similarly, Manaa and Hadi [29] introduced a scalable and robust cryptographic approach leveraging cloud computing to improve encryption throughput and resilience against distributed attacks.

3. Methodology

The proposed methodology for image authentication integrates AES encryption and DWT-based watermarking in a sequential flow, followed by implementation on an FPGA platform. The overall process is structured into four major stages i.e. Image preprocessing, AES encryption, DWT watermarking and FPGA implementation.

3.1 *Image Preprocessing:*

The input image is first resized to a standard dimension (e.g., 256x256 pixels) and converted to grayscale if it is a color image. This step ensures uniformity and reduces complexity during processing. The image is then normalized to a defined pixel intensity range.

3.2 *AES Encryption:*

AES operates on blocks of 128 bits and uses keys of length 128, 192, or 256 bits. The encryption process includes several rounds involving SubBytes (S-box transformation), ShiftRows, MixColumns, and AddRoundKey operations.

Steps of AES Implementation:

1. Convert image data into byte blocks.
2. Apply initial AddRoundKey.
3. Repeat Nr rounds:
4. SubBytes: Byte substitution using a predefined S-box.

Let S(x) represent the AES S-box, then the substituted byte b′ is b′=S(b).

where b is a byte from the state matrix.

5. ShiftRows: Shifting rows of the matrix.
6. MixColumns: Mixing the columns for diffusion.
7. AddRoundKey: XOR with a round-specific key.

$$Stateout = Statein \oplus RoundKey \tag{1}$$

where $\oplus$ denotes bitwise XOR.

The encrypted image appears as an unintelligible cipher image and provides strong protection against data interception.

3.3 *DWT Watermarking:*

Discrete Wavelet Transform decomposes an image into four sub-bands: LL (approximate), LH (horizontal), HL (vertical), and HH (diagonal). Watermark embedding is performed on HL, LH, or HH bands to ensure imperceptibility and robustness.

$$f(x,y) \xrightarrow{DWT} \{LL(x,y), LH(x,y), HL(x,y), HH(x,y)\} \quad (2)$$

where f(x,y) is the spatial domain image and LL, LH, HL and HH are the sub-bands.

Embedding Steps:

1. Perform one-level DWT on the AES-encrypted image.
2. Embed the watermark bits (e.g., binary logo) into the HH sub-band using a spread spectrum or quantization method.

$$HH'(i,j) = HH(i,j) + \alpha \cdot w(i,j) \quad (3)$$

where:
HH(i, j) is the original coefficient
w(i, j)∈{−1,1} is the watermark bit
α is the embedding strength

3. Apply inverse DWT to reconstruct the watermarked encrypted image.
4. Extraction Steps:
5. Apply DWT on the received watermarked image.
6. Extract watermark bits from the HH sub-band using the known embedding rule.

3.4 *FPGA Implementation:*

The entire system is described using Verilog HDL. Xilinx Vivado is used for synthesis, implementation, and simulation. The AES core and DWT modules are designed as individual functional blocks.

Implementation Steps:

Following steps were followed during implementation:

1. Design an AES core with a pipelined structure.
2. Create DWT modules (forward and inverse) using the lifting scheme.
3. Integrate watermark embedding logic.
4. Perform simulation and functional verification.
5. Synthesize and deploy on FPGA (e.g., Spartan-6, Zynq-7000).

Figure 1 shows a block diagram of the proposed system.

The use of hardware description languages and hardware simulation tools allows optimization for speed, area, and power.

Security Considerations:

1. AES key is securely stored or dynamically generated.
2. Watermark can be encrypted before embedding.
3. Any tampering of the image alters the frequency components, making it detectable during extraction.

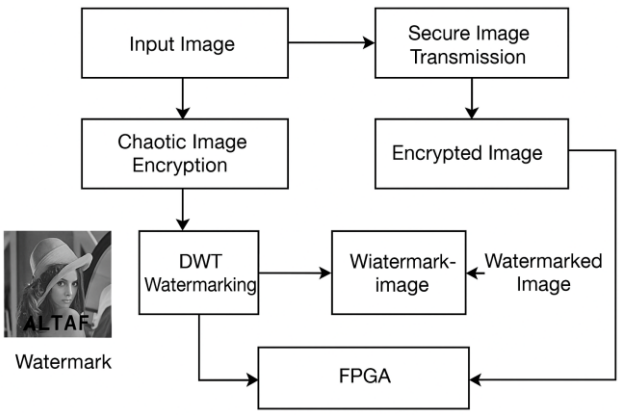

Figure 1
Proposed methodology

Performance Metrics:

1. PSNR and SSIM for image fidelity.
2. Resource utilization: number of LUTs, flip-flops, and slices used.
3. Latency and throughput analysis.

4. Results and Discussion:

To validate the performance of the proposed hybrid image authentication system, extensive simulations and hardware implementations were conducted. The system was evaluated using standard grayscale images such as Lena, Cameraman, and Barbara at a resolution of 256×256 pixels. The following metrics were considered:

1. Peak Signal-to-Noise Ratio (PSNR)
2. Structural Similarity Index Measure (SSIM)
3. Bit Error Rate (BER) for watermark retrieval
4. Hardware resource utilization (LUTs, FFs, Slices)
5. Power consumption and latency

4.1. *Simulation Setup:*

All image processing and watermark embedding operations were first validated using MATLAB. AES encryption and DWT watermarking were verified independently before integration. Verilog HDL was used to describe hardware components and the design was simulated using Xilinx ISim and synthesized on the Spartan-6 FPGA platform.

4.2. *Image Quality Evaluation:*

PSNR and SSIM were computed between the original and watermarked images to assess imperceptibility. Higher PSNR (> 40 dB) and SSIM (> 0.95) indicate minimal perceptual difference.

$$PSNR = 10 \cdot log_{10}\left(\frac{MAX_I^2}{MSE}\right) \quad (4)$$

where:

MAX_I is the maximum possible pixel value (usually 255) and

MSE is the mean squared error between the original and processed image

$$SSIM(x,y) = \frac{(2\mu_x\mu_y+C_1)(2\sigma_{xy}+C_2)}{(\mu_x^2+\mu_y^2+C_1)(\sigma_x^2+\sigma_y^2+C_2)} \quad (5)$$

where μx and μy are the means, σ_x^2 and σ_y^2 are the variances, σ_{xy} is the covariance, C_1 and C_2 are the small constants. Table 1 shows PSNR and SSIM for Test Images.

Table 1

PSNR and SSIM for Test Images

Test Image	PSNR (dB)	SSIM
Lena	42.67	0.982
Cameraman	41.85	0.974
Barbara	43.21	0.988

These results show excellent preservation of visual quality even after AES encryption and watermark embedding.

4.3. *Robustness Analysis:*

The system's robustness was evaluated against various attacks:

1. Gaussian Noise (σ = 0.01)
2. JPEG Compression (Q = 50)
3. Median Filtering (3×3)

Watermark was successfully extracted from attacked images with minimal BER, demonstrating resilience.

$$BER = \frac{N_{error}}{N_{total}} \times 100\% \quad (6)$$

where N_{error} is the number of erroneous bits and N_{total} is the total number of watermark bits.

Table 2 shows Bit Error Rate (BER) under Attacks.

Table 2

Bit Error Rate (BER) under Attacks

Attack Type	Bit Error Rate (%)
Gaussian Noise (σ = 0.01)	1.5
JPEG Compression (Q = 50)	1.8
Median Filtering (3×3)	1.2

3.4. *FPGA Synthesis Results:*

The hardware implementation was synthesized using Xilinx Vivado. Resource usage and timing performance are detailed in Table 3.

Table 3

FPGA Resource Utilization (Spartan-6)

Resource	Usage
LUTs	4321
Flip-Flops	2176
Slices	1024

Figure 2 demonstrates visual outputs at different stages of the proposed secure image transmission process using chaotic encryption and DWT-based watermarking on an FPGA platform. It contains four sub-images that collectively validate the performance of system:

(a) **Cover Image**: This is the original grayscale input image (e.g., Lena) used as the host for watermark embedding. It represents the unaltered source before any encryption or watermarking is applied.

(b) **Watermarked Image**: This image shows the result after embedding the watermark "ALTAF" using Discrete Wavelet Transform (DWT). The watermark is imperceptibly embedded into the frequency components (specifically HH sub-band), maintaining the visual integrity of the image.

(c) **Encrypted Image**: Post watermarking, the image is encrypted using a chaotic encryption scheme or AES. This sub-image appears as random noise, offering strong protection against unauthorized access or tampering during transmission.

Figure 2
Watermark Extraction

(d) Extracted Watermark: This image illustrates the watermark successfully extracted at the receiver's end. The watermark text "ALTAF" is clearly recovered, confirming the robustness of the watermarking method against encryption and channel interference.

Together, these visuals prove that the system maintains confidentiality (via encryption) and authenticity (via watermarking), even under potential attacks or noise, thereby validating the proposed FPGA-based secure image authentication architecture. Total power consumption was measured at 354 mW with a latency of 1.02 μs for full image processing, indicating suitability for real-time applications.

5. Conclusion

This paper presented a secure and efficient image authentication framework by integrating AES encryption and DWT-based invisible watermarking, implemented on a reconfigurable FPGA platform. The motivation stemmed from the growing need to protect digital image integrity and confidentiality in critical applications. The system successfully combines two complementary techniques: AES for strong encryption of image content and DWT watermarking for authentication. The hybrid approach ensures that even if an image is intercepted, its content remains inaccessible without the AES key, and any modification can be detected through watermark extraction. Implementing the system on an FPGA offers real-time performance with hardware-level security and adaptability. Performance evaluations demonstrated high visual fidelity, robustness to common signal processing attacks, and efficient hardware utilization. PSNR values above 40 dB and SSIM greater than 0.95 affirm the imperceptibility of the watermark. Bit error rates under 2% even in degraded images show the watermark's resilience. The FPGA synthesis results indicate that the design is resource-efficient and well-suited for embedded environments. The proposed architecture is highly relevant for sensitive domains such as medical image transmission, military reconnaissance, and multimedia copyright enforcement. The integration of AES and DWT watermarking on reconfigurable platforms presents a robust and scalable solution for real-time image authentication. Its adaptability, security, and hardware efficiency make it a valuable contribution to the field of digital content protection.

References

[1] D. Singh, S. Kumar, C. Verma, Z. Illés, and N. Kumar, "Visually meaningful image encryption for secure and authenticated data transmission using chaotic maps," *J. King Saud Univ. Comput. Inf. Sci.*, vol. 36, no. 10, pp. 102235 (Nov. 2024).

[2] A. Al-Hyari, C. Obimbo, M. M. Abu-Faraj, and I. Al-Taharwa, "Generating Powerful Encryption Keys for Image Cryptography With Chaotic Maps by Incorporating Collatz Conjecture," *IEEE Access,* vol. 12, pp. 4825–4844 (2024), doi: 10.1109/ACCESS.2024.3349470.

[3] T. ul Haq and T. Shah, "4D mixed chaotic system and its application to RGB image encryption using substitution-diffusion," *J. Inf. Secur. Appl.*, vol. 61, pp. 102931 (Jul. 2021).

[4] W. Shang, Z. Liu, S. Wang, L. Ding, X. Shang, Z. Zhou, et al., "Secure color image encryption algorithm for face recognition using Zaslavsky and Arnold cat maps with binary bit-plane decomposition," *Inf. Sci.,* vol. 719, pp. 122502 (Jul. 2025).

[5] D. Singh, S. Kaur, M. Kaur, S. Singh, M. Kaur, and H. N. Lee, "A systematic literature review on chaotic maps-based image security techniques," *Comput. Sci. Rev.,* vol. 54, pp. 100659 (Nov. 2024).

[6] M. Saberi Kamarposhti, A. Ghorbani, and M. Yadollahi, "A comprehensive survey on image encryption: Taxonomy, challenges, and future directions," *Chaos Solitons Fractals*, vol. 178, pp. 114361 (Jan. 2024).

[7] G. Zhou, D. Zhang, Y. Liu, Y. Yuan, and Q. Liu, "A novel image encryption algorithm based on chaos and Line map," *Neurocomputing,* vol. 169, pp. 150–157 (Dec. 2015).

[8] Y. Hu, H. Wu, and L. Zhou, "Color image encryption base on a 2D hyperchaotic enhanced Henon map and cross diffusion," *Alexandria Eng. J.,* vol. 73, pp. 385–402 (Jul. 2023).

[9] N. R. Zhou, L. L. Hu, Z. W. Huang, M. M. Wang, and G. S. Luo, "Novel multiple color images encryption and decryption scheme based on a bit-level extension algorithm," *Expert Syst. Appl.,* vol. 238, pp. 122052 (Mar. 2024).

[10] S. Zhang, Y. Huang, Y. Wang, W. Jiang, and B. Wang, "Secure Color Traffic Image Transmission Through Enhanced Visual Encryption," *IET Image Process*., vol. 19, no. 1 (Jan. 2025).

[11] A. Tiwari, P. Diwan, T. D. Diwan, M. Miroslav Mahdal, and S. P. Samal, "A compressed image encryption algorithm leveraging optimized 3D chaotic maps for secure image communication," *Sci. Rep.,* vol. 15, no. 1 (Apr. 2025).

[12] M. Hazzazi, M. U. Rehman, A. Shafique, A. Amer Aljaedi, Z. Bassfar, and A. B. Usman, "Enhancing image security via chaotic maps,

Fibonacci, Tribonacci transformations, and DWT diffusion: a robust data encryption approach," *Sci. Rep.,* vol. 14, no. 1 (May 2024).

[13] Poonam and S. M. Arora, "A DWT-SVD based Robust Digital Watermarking for Digital Images," *Procedia Comput. Sci.*, vol. 132, pp. 1441–1448 (2018).

[14] A. Alrammahi and H. Sajedi, "A Robust Image Watermarking Based on DWT and RDWT Combined with Möbius Transformations," *Comput. Mater. Contin.,* vol. 84, no. 1, pp. 887–918 (Jun. 2025).

[15] H. Al-Khafaji, B. Al-Himyari, and H. Alharbi, "Enhancing Image Watermarking: An Innovative Multi-Objective Genetic Algorithm-Based DWT-SVD Approach for Robustness and Imperceptibility," *Int. J. Saf. Secur. Eng.,* vol. 14, no. 6, pp. 1921–1931 (Dec. 2024).

[16] M. Begum and M. S. Uddin, "Digital image watermarking techniques: A review," *Information*, vol. 11, no. 2, pp. 110 (2020).

[17] R. Wazirali, W. Alasmary, M. M. Mahmoud, and A. Alhindi, "An optimized steganography hiding capacity and imperceptibly using genetic algorithms," *IEEE Access,* vol. 7, pp. 133496–133508 (2019).

[18] J. Ma, J. Chen, and G. Wu, "Robust watermarking via multidomain transform over wireless channel: Design and experimental validation," *IEEE Access,* vol. 10, pp. 92284–92293 (2022).

[19] K. Rajwar, K. Deep, and S. Das, "An exhaustive review of the metaheuristic algorithms for search and optimization: Taxonomy, applications, and open challenges," *Artif. Intell. Rev.,* vol. 56, no. 11, pp. 13187–13257 (2023).

[20] A. Melman and O. Evsutin, "Image data hiding schemes based on metaheuristic optimization: A review," *Artif. Intell. Rev.*, vol. 56, no. 12, pp. 15375–15447 (2023).

[21] A. O. Mulani and P. B. Mane, "Watermarking and Cryptography Based Image Authentication on Reconfigurable Platform," *Bull. Electr. Eng. Inf.,* vol. 6, no. 2, pp. 181–187 (Jun. 2017).

[22] H. S. Deshpande, K. J. Karande, and A. O. Mulani, "Area optimized implementation of AES algorithm on FPGA," in *Proc. Int. Conf. Commun. Signal Process.* (ICCSP), pp. 0010–0014 (2025), doi: 10.1109/ICCSP.2015.7322746.

[23] A. O. Mulani and P. B. Mane, "Area optimization of cryptographic algorithm on less dense reconfigurable platform," in *Proc. 2014 Int.*

Conf. Smart Struct. Syst. (ICSSS), Chennai, India, pp. 86–89 (2024), doi: 10.1109/ICSSS.2014.7006201.

[24] P. R. Kulkarni, A. O. Mulani, and P. B. Mane, "Robust Invisible Watermarking for Image Authentication," in Lecture Notes in Electr. Eng., vol. 394, Singapore: Springer (2017).

[25] P. B. Mane and A. O. Mulani, "High Speed Area Efficient FPGA Implementation of AES Algorithm," *Int. J. Reconfig. Embedded Syst. (IJRES)*, vol. 7, no. 3, pp. 157–163 (Nov. 2018).

[26] T. Gopalakrishnan, H. M. A. Ghanimi, T. Alam, K. E. Purushothaman, S. Sengan, and P. Dadheech, "Leveraging blockchain technology to combat deception, deepfake, and counterfeit system," *J. Discrete Math. Sci. Cryptogr.*, vol. 27, no. 7, pp. 2143–2154 (2024).

[27] V. Kapoor and R. Gupta, "Hybrid symmetric cryptography approach for secure communication in web application," *J. Discrete Math. Sci. Cryptogr.,* vol. 24, no. 5, pp. 1179–1187 (2021).

[28] A. K. Bermani, T. A. K. Murshedi, and Z. A. Abod, "A hybrid cryptography technique for data storage on cloud computing," *J. Discrete Math. Sci. Cryptogr.,* vol. 24, no. 6, pp. 1613–1624 (2021).

[29] M. E. Manaa and Z. G. Hadi, "Scalable and robust cryptography approach using cloud computing," *J. Discrete Math. Sci. Cryptogr.*, vol. 23, no. 7, pp. 1439–1445 (2020).

Received July, 2025