AL-Bahir
Journal for Engineering and Pure Sciences
BJEPS

Manuscript 1113

A Comparative Performance Study of WebP Compression in a Cryptographic–Steganographic Pipeline for Secure E-Commerce Transactions

Esther Abeson Nasara

Moses Timothy

Agushaka J. Ovre

Taofeekat Tosin Salau-Ibrahim

Follow this and additional works at: https://bjeps.alkafeel.edu.iq/journal

ORIGINAL STUDY

A Comparative Performance Study of Webp Compression in a Cryptographic−Steganographic Pipeline for Secure E-commerce Transactions

Esther A. Nasara*, Timothy Moses, Agushaka J. Ovre, Taofeekat T. Salau-Ibrahim

Department of Computer Science, Federal University of Lafia, Nigeria

Abstract

The expeditious growth of electronic commerce (e-commerce) fundamentally transformed business operations and consumer behavior by enabling businesses to reach a global market, streamline supply chains, and provide personalized shopping experiences. This shift necessitated reliable security measures to protect sensitive information during online transactions. However, existing approaches that combined encryption, steganography, and conventional compression techniques such as DCT and autoencoders were limited in preserving image quality and computational efficiency. To address this gap, the objective of this study was to integrate WebP compression into the cryptographic−steganographic pipeline in order to improve image quality, ensure payload integrity, and achieve efficiency suitable for real-time e-commerce systems. While cryptographic−steganographic pipelines combining asymmetric encryption, spatial embedding, and compression are well established, this study focused on demonstrating the comparative performance benefits of WebP compression over existing approaches such as the Discrete Cosine Transform (DCT) and autoencoders. To achieve this, an enhanced model was developed and evaluated by integrating the ElGamal cryptosystem for encryption, Least Significant Bit (LSB) steganography for embedding, and WebP for compression and optimization. In the developed workflow, transaction data was encrypted using ElGamal, embedded into cover images with LSB steganography, compressed using WebP, and at the receiver's end the images were decoded, the ciphertext was extracted, and decrypted with the private key to recover the original data. This process ensured confidentiality, efficiency, and reliability in e-commerce communication. Empirical evaluation was conducted using key performance metrics, including Mean Squared Error (MSE), Peak Signal-to-Noise Ratio (PSNR), Structural Similarity Index (SSIM), and entropy. Results showed low MSE values, PSNR values exceeding 79 dB, SSIM scores of 0.9999, and minimal entropy loss, confirming both high image quality retention and strong payload integrity. These results demonstrate that the developed model achieved superior image quality, high structural fidelity, zero payload errors, and efficient performance, confirming its suitability for securing sensitive e-commerce transactions. The PSNR value of 54.9 dB reported by Kumbhakar et al. is developed WebP-based model demonstrated a significant improvement in image quality and efficiency. These findings established that while the cryptographic−steganographic pipeline itself was not novel, the integration of WebP compression provided superior performance compared to traditional DCT-based methods. The developed model therefore offered a practical and effective solution for safeguarding sensitive e-commerce transactions, addressing threats such as data interception, unauthorized access, and Man-in-the-Middle attacks.

Keywords: E-commerce security, ElGamal cryptosystem, Least Significant Bit (LSB) steganography, WebP compression, Cryptography, Steganography, Data protection

1. Introduction

E-commerce which is the buying and selling of goods and services over the internet, has revolutionized the way businesses operate by reaching a global audience without the need for physical stores, significantly reducing costs associated with rent. This cost efficiency allows for lower

Received 21 August 2025; revised 11 October 2025; accepted 12 October 2025.
Available online 9 January 2026

* Corresponding author.
E-mail addresses: esthersam460@gmail.com (E.A. Nasara), moses.timothy@science.fulafia.edu.ng (T. Moses), jo.agushaka@science.fulafia.edu.ng (A.J. Ovre), taofeekat.tosin@cmp.fulafia.edu.ng (T.T. Salau-Ibrahim).

https://doi.org/10.55810/2313-0083.1113
2313-0083/© 2026 University of AlKafeel. This is an open access article under the CC-BY-NC license (http://creativecommons.org/licenses/by-nc/4.0/).

prices and higher profits. However, the growth of e-commerce systems has heightened the need for strong security measures to protect sensitive information during online transactions. The handling of sensitive information, such as personal and financial data, makes e-commerce platforms prime targets for cyber-attacks. Data breaches, identity theft, and fraudulent transactions are common issues that threaten the integrity of online transactions. Privacy preservation is a critical concern, as consumers need assurance that their information is secure and used appropriately. Although many researchers have worked on e-commerce data security [1–5], many security threats like Man-in-the-Middle and eavesdropping attacks are still active. The lack of a comprehensive security infrastructure leaves e-commerce transactions vulnerable to various cyber threats, jeopardizing the confidentiality, integrity, and authenticity of sensitive information exchanged between parties involved in transactions [6]. The evolving nature of cyber threats demands a more reliable and adaptable security measures to protect both consumers and businesses from potential harm. This study conducted a performance evaluation of an established cryptographic–steganographic–compression technique by integrating the ElGamal cryptosystem, Least Significant Bit (LSB) steganography as a baseline embedding method, and WebP compression, and comparing the results with conventional approaches such as DCT and autoencoders. The paper is organized as follows. Section 1 is the introduction; Section 2 represents related works regarding the e-commerce security model. Section 3 focuses on the methodology of the technique implemented in this study, and Section 4 presents the results and discussion obtained from the performance evaluation of ElGamal cryptography, Least Significant Bit (LSB) Steganography mechanism and WebP compression, compared against conventional approaches. Section 5 concludes the paper and provides the recommendation for further study.

2. Related works

Several researchers have employed unique techniques to enhance the security of online shopping. Their efforts range from using sophisticated encryption techniques to developing smart ways of verifying users' identities. This section examines the different approaches these researchers have taken. Examination of these diverse techniques gives a better understanding of the ongoing efforts to make e-commerce safer for all users.

[1] addressed vulnerabilities like Man-in-the-Middle attacks by combining ElGamal encryption with LSB image steganography, optimized via Discrete Cosine Transform and Autoencoder. This dual-layered approach enhances transaction security but introduces complexity that may impact usability. The research suggests simplifying the encryption process, detailing risk mitigation strategies, and providing specific performance metrics for better assessment and adoption [3]. examined e-commerce transaction vulnerabilities by proposing a multi-layer encryption approach using RSA for secure key exchange and Fernet cipher for message authentication. The combined algorithm aims to enhance security, but it faces challenges such as computational overhead, key management difficulties, and scalability issues. Recommendations for future work include optimizing encryption processes, improving key management, and incorporating AI-driven dynamic security measures to adapt to evolving threats. The challenge of securing user data in e-commerce despite using SSL/TLS protocols was examined by Ref. [7], citing vulnerabilities in session management, authentication, and access control. The proposed solution involves extending security measures to the application layer through a comprehensive scheme, integrating authentication, continuous authentication, and session management. By doing so, the burden of implementing security measures is shifted from the development lifecycle. This solution addresses vulnerabilities, enhancing the overall security of e-commerce platforms. However, its complexity and compatibility issues with existing systems pose limitations. Improvements could focus on scalability, flexibility, and interoperability to optimize performance and usability, ensuring compliance with industry standards and regulations while addressing emerging threats. An encryption algorithm using block chain, digital envelopes, and chaotic neural networks to improve e-commerce data security and efficiency was proposed by Ref. [8]. While the approach advanced encryption security, it faced challenges with complexity and potential data distortion. Suggested improvements include thorough security analysis, user-friendliness assessment, and real-world testing to validate performance and practical utility.

Privacy challenges in e-commerce were addressed by using differential privacy to introduce noise to query outputs, protecting individual data [9]. While effective, the study lacks discussion on evolving threats and user awareness. It is important for this study to include ongoing threat monitoring,

proactive solution updates, and comprehensive user education campaigns to ensure understanding and cooperation with privacy measure [10] explored the balance between user privacy and ownership verification in e-commerce, focusing on high-value collectibles. A protocol was proposed using private smart contracts and zk-SNARKs, demonstrating feasibility on platforms like Ethereum Quorum and SERO. Despite positive results, the solution faces interoperability challenges and platform dependency, suggesting the need for standardized protocols, interledger mechanisms, and blockchain-agnostic designs for broader adoption.

The lack of recognition and provision for personal data protection rights within Nigeria's consumer protection regime leaves e-commerce enthusiasts vulnerable to potential breaches of their personal data. To tackle this [11], critically assesses existing data protection policies in Nigeria, including the NDPR, CBN-CPF, and Cybercrime Act, to evaluate their effectiveness in addressing personal data protection concerns in e-commerce. The paper suggested separate personal data protection legislation similar to Singapore's model, to safeguard data subjects' privacy and security adequately. Nonetheless, limitations include a narrow focus on legal aspects and potential oversight of practical challenges in implementation and implications for e-commerce businesses. Future research could broaden the scope to encompass technical, operational, and regulatory aspects, conduct empirical studies on policy impacts, explore alternative regulatory approaches, and engage stakeholders for more effective legislation development and implementation. According to Ref. [12], conventional e-commerce payment systems are vulnerable due to the insecure transmission of sensitive financial information over the internet, especially in cloud environments. This poses significant risks to the confidentiality, integrity, and security of transactions. To address this issue, the researchers proposed developing a secure electronic payment protocol that allows consumers to connect directly with merchants using temporary identities to ensure anonymity and privacy. This protocol uses reliable encryption and authentication mechanisms to protect financial data. Implementing this protocol enhances security by ensuring confidentiality, integrity, non-repudiation, availability, authentication, and authorization, thus fostering trust and confidence in e-commerce transactions. However, the complexity and implementation challenges of this new protocol might lead to resistance from consumers and merchants. Ensuring widespread adoption and continuous updates to counter emerging cyber threats can also be difficult. To improve the protocol, efforts should focus on making it more user-friendly, ensuring compatibility with existing systems, optimizing scalability, and maintaining up-to-date security measures. This enhances its effectiveness, promote adoption, and contribute to a more secure e-commerce environment.

The vulnerability of existing mobile-based two-factor authentication (2FA) schemes in e-commerce poses a significant risk to transaction security due to compromised phones. To counter this [13], proposedSecurePay; a solution aiming to bolster mobile-based 2FA by isolating authentication factors and ensuring transaction integrity. Leveraging ARM TrustZone technology, SecurePay provides reliable security guarantees even in compromised phone environments, mitigating risks of unauthorized access and fraud. However, device compatibility and the need for further testing is lacking. Future improvements could focus on scalability, compatibility, and resilience across diverse platforms, alongside exploring alternative authentication methods for comprehensive e-commerce security.

Critical issue of inadequate security in e-commerce despite its global prevalence, posing risks to payment information, personal data, and purchased items were addressed by Ref. [14]. The research noted that many online stores fail to implement proper security measures due to a lack of understanding or seriousness. To address this, the researchers conducted a systematic analysis of e-commerce platforms, reviewed existing literature, and collected and analyzed data to identify security threats from both customer and seller perspectives. Solutions to mitigate these threats were proposed, aiming to improve the safety and trustworthiness of online transactions. However, the study has limitations, such as not covering all emerging risks, varying effectiveness of solutions based on resources and laws, and not addressing cybersecurity awareness or trade-offs between security and usability. Future research should expand the scope to include more platforms, regions, and demographics, provide specific recommendations to close cybersecurity knowledge gaps, analyze the trade-offs of security measures, and engage stakeholders to ensure practical and impactful findings.

[15] enhanced the Secure Electronic Transaction (SET) protocol to address e-commerce security, scalability, and efficiency issues. A server e-wallet model was introduced, a fourth-party transaction protocol for dispute resolution, and a hierarchical control model for security levels. While the

approach improved security and efficiency, its complexity and the roles of the fourth party need clarification. Further improvements involve detailed implementation plans, real-world evaluations, and consideration of user experience and cost implications. The study by Ref. [16] points out differing levels of cybersecurity concern among European countries, which affects the uniformity of e-commerce security across the region. To address this, the researchers used a hybrid methodology combining Multi-Criteria Decision Analysis (MCDA) and a Likert Scale Survey. This method allowed them to rank countries based on e-commerce security and gather consumer insights on cybersecurity challenges. While this approach provided a comprehensive understanding of the cybersecurity landscape, it faced limitations such as potential survey bias, subjective ranking criteria, limited geographic scope, and a lack of longitudinal analysis. Future improvements could include using objective cybersecurity measures, refining MCDA methodology, expanding the study's scope beyond Europe, and conducting longitudinal studies to track changes over time.

The lack of tactile feedback in online shopping was identified by Ref. [17] as a significant issueincreasing the risk of scams and customer dissatisfaction due to the inability to assess product weight. To address this, a tele-weight device that allows users to virtually feel the weight of items while shopping online was developed. This device consists of a sending part that measures and transmits the weight over a cellular network and a receiving part that displays it to the user. While the tele-weight device enhances the online shopping experience by providing haptic feedback and reducing the risk of weight misrepresentation scams, it faces limitations such as delays in weight demonstration, which can affect performance and user trust. There is the need however to enhance real-time responsiveness, integrate secure communication protocols, and continuously updating the device's software to address emerging security threats. The problem of counterfeit products on online shopping platforms, which causes financial losses, damages brand reputations, and reduces trust in e-commerce was identified by Ref. [18]. To solve this, a traceability system that shares detailed and secure product information throughout the supply chain was suggested, allowing customers to check product authenticity before buying. This method helps prevent fake products, protect brand names, and build consumer trust. However, it requires a significant initial investment and accurate information sharing which can be challenging. Improvements can include using blockchain and AI for better transparency and security, simplifying information sharing, and educating consumers on checking for authenticity. Continuous updates to tackle new cyber threats are also important.

[19] explored the privacy paradox in e-commerce, where users express concerns but still share personal information. Using EEG experiments, cognitive and emotional processes influencing privacy decisions was examined. The study provided insights into mental perceptions underlying privacy paradoxes but faced limitations due to the complexity of neuroimaging analysis and the need for further research to understand neural dispositions in privacy-related decision-making. Internet users' growing concern over privacy and data protection, particularly regarding companies extracting personal information based on online behavior, posing a threat to trust in e-commerce was identified in Ref. [20]. To tackle this, tokenization system in e-commerce transactions was proposed, aiming to conceal customers' credit card numbers from online merchants. Their method, called “upcycling,” manages tokens in RAM, allowing for regenerated tokens while maintaining a table of valid ones, enhancing security and privacy. However, the reliance on RAM may pose scalability challenges, and potential vulnerabilities targeting the tokenization system, suggesting the need for further research on optimization, security assessments, and user education to improve e-commerce privacy and security.

The issue of protecting user privacy on untrusted servers by generating dummy requests to obscure preferences was tackled by Ref. [21]. Using entropy and regional distance concepts, their model enhances security without compromising usability. However, it needs to expand to other e-commerce services, integrate with various terminals, and account for user behavior inconsistencies. Future research should focus on broader privacy models, improved integration, and accuracy [22] addressed the challenge of imbalanced credit card datasets affecting fraud detection in e-commerce systems. Sampling techniques such as oversampling and undersampling was reviewed to rebalance datasets, aiming to improve fraud detection performance. However, the study's focus on sampling methods alone may overlook other contributing factors to imbalanced data, and the effectiveness of these techniques may vary across different datasets and algorithms. The inadequacy of existing black-box web application vulnerability scanners in detecting vulnerabilities in modern web applications, particularly in e-commerce sector was addressed by

Ref. [23]. By evaluating the detection accuracy of five scanners against a modern insecure web application, the study shed light on their limitations in identifying critical vulnerabilities like SQL injection, NoSQL injection, and server-side template injection. The findings underscored the need for enhanced vulnerability detection methods and comprehensive security strategies tailored to the complexities of modern web environments, urging further research to address these challenges effectively.

[24] addressed the lack of transparency and trust in existing e-commerce reputation systems by exploring blockchain-based models. This method involved a systematic literature review to evaluate the potential of blockchain technology in enhancing transparency and trust. While the study offers insights into the benefits and challenges of blockchain-based reputation systems, it lacked practical insights and empirical evidence on their effectiveness. Additionally, factors impacting implementation and adoption were not thoroughly explored. Integrating real-life examples and providing concrete recommendations will improve the system's usefulness and relevance. The study conducted by Ref. [25] describes the cybersecurity risks confronting e-commerce, encompassing unauthorized access, data breaches, and phishing scams, eroding trust in digital platforms. The proposed solution involves deploying advanced security measures like encryption protocols, multifactor authentication, and regular security audits. These strategies effectively mitigate cyber threats, safeguarding sensitive data and bolstering customer trust. However, relying solely on technological solutions may lead to human error and necessitate continuous adaptation to evolving threats, while overly restrictive security measures hamper user experience. To enhance security in e-commerce, the study advocates for greater collaboration among users, integrating security into the development process, and investing in emerging technologies like blockchain-based authentication.

Challenges related to product authenticity verification and data integrity in e-commerce live streaming was identified by Ref. [26]. A solution integrating blockchain technology and traceability was developed. By deploying a smart contract on the Ethereum blockchain and utilizing a combination of on-chain and off-chain storage methods, the solution enhanced transparency and security in product authentication processes during live streaming events. However, potential limitations in scalability, transaction costs, and usability were acknowledged, suggesting areas for improvement to ensure practical implementation and widespread adoption of the proposed solution [27] addressed the vulnerability of e-commerce platforms to malicious URL attacks, proposing the Political Optimization Algorithm by a Hybrid Deep Learning Assisted Malicious URL Detection and Classification for Cybersecurity (POAHDL-MDC) technique. This method integrates data preprocessing, word embedding, and a Hybrid Deep Learning model to detect and classify malicious URLs, demonstrating promising results in simulations. However, challenges such as overfitting, resource requirements, and data quality limitations pose constraints. Enhancing the solution's reliability, adaptability, and real-time capabilities through rigorous testing, increased interpretability, and collaborative efforts among users is required.

A protocol to secure merchant information during e-commerce transactions was developed by Ref. [28] combining encryption algorithms and data leakage detection technology. While the protocol offers enhanced security, its potential impact on transaction efficiency and resource utilization is a limitation. Optimization efforts to streamline processes, simplify implementation, and ensure compatibility with existing systems would enhance the protocol's effectiveness and adoption. By addressing these areas, the protocol can provide reliable security without compromising transaction efficiency. The growing challenge faced by businesses in managing legal responsibilities regarding informed consent and privacy protection, exacerbated by increasing public skepticism toward personal data collection practices was explored by Ref. [29]. To address this, an ethical consent management process tailored for e-commerce organizations was developed. This process integrates the Autonomous Authorization (AA) model and the Theory of Planned Behavior (TPB) to construct a framework rooted in user autonomy, aiming to prioritize user interests and support ethical information management. By enhancing transparency and trust while complying with regulatory requirements, this solution mitigates the risks associated with data breaches and privacy violations in e-commerce. However, its complexity and potential cultural challenges in global operations pose limitations, suggesting a need for streamlined implementation processes, standardized tools, and ongoing research to adapt to evolving threats and regulatory standards.

A gap in knowledge regarding remanufacturing trading websites in online shopping, which sell refurbished items but whose operations and offerings are not well understood was identified by

Ref. [30]. The study aimed to address this by systematically analyzing 20 such platforms, identifying deficiencies in business models, product presentation, delivery methods, quality assurance, customer reviews, and payment processes. Six key applications to address these gaps and the use of consortium blockchain technology for its benefits in security, transparency, and scalability were explored. A technical framework and model for a remanufacturing trading platform supported by consortium blockchain were developed to guide the development and management of these platforms. However, limitations include the narrow focus on remanufacturing platforms, the small sample size, and the need for further validation and adaptation to future technological changes. Improvements should involve expanding the study's scope, incorporating qualitative research, continuous monitoring, and exploring alternative technologies. A semi-quantum privacy comparison method based on W-states to address security threats posed by quantum computing in e-commerce multi-party algorithms was proposed. The method enhances security and communication efficiency, but its reliance on quantum computing technology may limit practical implementation due to current infrastructure limitations and complexity. Hybrid approaches and efforts to enhance quantum technology accessibility could improve the method's practicality and scalability in e-commerce applications [31].

The importance of evaluating e-commerce's impact on customer satisfaction, particularly focusing on factors such as website design, user-friendliness, convenience in use and payment, data security, competitive advantage, and timeliness in service access for Konga.com customers in Ilorin metropolis, Nigeria was evaluated by Ref. [32]. Through a purposive sampling technique and multiple regression analysis, the study identified key factors influencing customer satisfaction, including reliability, user interface, navigation, and timely payment systems. However, the study's focus on customer perceptions and satisfaction without delving into technical e-commerce security aspects and potential vulnerabilities in Konga.com's infrastructure presents limitations, suggesting the need for future research to comprehensively address e-commerce security measures and customer perceptions [33] addressed security vulnerabilities and limitations in existing public key cryptography algorithms, particularly in e-commerce transactions, by proposing a novel method based on a fake-modulus concept. This method aimed to enhance the security of the Rabin cryptosystem by confusing attackers attempting to factorize the public key, thereby preventing unauthorized access and fraud during e-commerce transactions. Despite its potential to provide reliable security, concerns regarding complexity, performance impact, and usability were raised, suggesting the need for optimization and careful consideration of trade-offs between security, performance, and usability for practical implementation.

A protocol combining ElGamal, AES, and CRT techniques to enhance e-commerce transaction security while balancing performance was proposed by Ref. [34]. Despite reliable key generation and data encryption, the protocol's resource-intensive processes suggest the need for optimizing encryption, improving merchant request security, and exploring post-quantum cryptography for better long-term security. The study by Ref. [35] emphasized the critical importance of ensuring the safety and security of online shopping websites to attract and retain customers. Conducted in Pakistan, the research employed an online questionnaire and advanced statistical methods, particularly the partial least squares method with SmartPLS software, to analyze customer attitudes towards e-commerce security. While the study successfully provided insights into customer concerns and preferences, allowing for the development of policies and technological enhancements to improve security measures in e-commerce applications, it acknowledged limitations regarding the generalizability of findings, potential biases introduced by the reliance on online surveys, and the limitations of statistical methods in capturing all nuances of customer attitudes. Suggestions for improvement include integrating qualitative approaches like interviews or focus groups to complement quantitative findings.

A study was conducted by Ref. [36] to understand the factors influencing the adoption of digital payment methods, particularly mobile payments, in Manipal, India. Using structural equation modeling, critical drivers such as ease of use and social influence were identified. While providing valuable insights for Manipal, the study's generalizability may be limited, and reliance on self-reported data could introduce bias. Future research should diversify samples and employ mixed-methods approaches for a broader understanding [37] addressed various challenges within e-commerce platforms such as payment disputes, fraud, and lack of transparency by proposing the integration of blockchain technology. By leveraging blockchain's decentralized and transparent nature, e-commerce platforms can improve transaction efficiency and safety, enhance transparency between buyers and sellers, and mitigate risks associated

with fraud and disputes. However, potential limitations in scalability, transaction costs, and the need for broader adoption and education were identified, suggesting areas for improvement to maximize the benefits of blockchain in e-commerce.

Vulnerability in online transactions through a security framework combining multi-factor authentication with machine learning to enhance the safety of financial transactions in e-commerce was addressed by Ref. [38]. This approach integrates two-factor authentication with machine learning algorithms triggered by potential fraud detection, achieving high accuracy in identifying and preventing fraudulent activities. Despite potential limitations related to complexity, cost, data quality, and privacy concerns, the solution emphasizes scalability, data quality, user experience, adaptive security measures, regulatory compliance, and continuous monitoring and improvement as areas for enhancement to maintain effectiveness over time and mitigate evolving cyber threats effectively [39] identified security challenges surrounding the protection of sensitive data in e-commerce transactions, emphasizing the need to prioritize safeguarding against unauthorized access and fraudulent activities to maintain credibility and longevity. The proposed solution involves a comprehensive approach integrating encryption, multi-factor authentication, security audits, employee training, collaboration with cybersecurity experts, adherence to standards, and advanced technologies to enhance security measures. However, potential drawbacks include increased complexity and costs, necessitating a balance between security, user experience, and cost considerations, while areas for improvement focus on streamlining user authentication, enhancing security technologies, and promoting regulatory compliance to address evolving cyber threats effectively. The research conducted by Ref. [40] identifies the need to evaluate and enhance customer satisfaction, trust, and service quality within the rapidly evolving online marketplace landscape. To address this, a comprehensive evaluation involving in-person and online surveys was conducted, analyzing twelve latent variables such as perceived security and brand equity. Structural equation modeling and multi-criteria decision analysis techniques were employed to understand factors influencing customer satisfaction and trust. The study also utilized the Technique for Order Preference by Similarity to Ideal Solution (TOPSIS) to rank e-commerce platforms, aiming to identify areas for improvement and provide actionable recommendations. However, limitations include potential sampling bias and the focus on specific platforms and geographical locations, suggesting the need for diversification in sampling methodology and broader representation across various e-commerce platforms to enhance validity and generalizability.

The research conducted by Ref. [41] introduced a cybersecurity framework for large language model (LLM)-driven robot agents in online transactions. The study integrated blockchain technology with multi-factor authentication (MFA) and anomaly detection techniques to enhance transaction security and protect sensitive user data. Experimental evaluation demonstrated a 90 % reduction in fraudulent transactions and a 98 % accuracy rate in detecting security breaches. This work points out the relevance of hybrid models that combine multiple security layers for e-commerce protection. However, its focus was limited to AI-driven transaction environments, suggesting the need for broader approaches that also address conventional e-commerce vulnerabilities. This gap is addressed in the present study, which develops an integrated cryptographic–steganographic model with WebP compression to enhance both security and efficiency.

The research conducted by Ref. [42] introduced an FDCT-based watermarking framework for medical image protection. The study emphasized imperceptibility and robustness under compression, achieving high watermark recovery accuracy. This work shows the value of transform-domain approaches for multimedia protection. However, its application was limited to medical imaging and did not address e-commerce transactions. The present study extends this line of work by focusing on e-commerce, where transaction confidentiality and data integrity are more critical.

The study by Ref. [43] developed a novel wavelet-based image compression method combined with Huffman coding to improve compression ratios while maintaining visual quality. Experimental evaluation showed significant improvements in data reduction while preserving diagnostic image fidelity. While effective in healthcare imaging, its scope did not incorporate security requirements such as encryption or steganography. This gap is addressed in the present work by integrating compression with ElGamal cryptography and LSB steganography for secure e-commerce transactions.

The research by Ref. [44] implemented and analyzed digital watermarking techniques for multimedia authentication. Results confirmed improved resilience against tampering and content forgery. While this study focused on authentication

and watermark robustness, it did not integrate encryption or explore compression efficiency. By contrast, the present study combines encryption, steganography, and WebP compression, ensuring not only authentication-level protection but also secure and efficient data concealment.

A related contribution by Ref. [45] proposed a modified LSB steganography scheme for securing textual medical information. The method enhanced embedding security but remained vulnerable under compression, limiting its practical deployment in bandwidth-constrained environments. The present study builds on this by adopting WebP compression to maintain security and efficiency in e-commerce settings where image optimization is essential.

In a broader context [46], provided a comprehensive survey of multimedia security approaches, including cryptography, steganography, and watermarking. The review underscored the importance of hybrid techniques but emphasized that most works remain domain-specific and rarely address the unique needs of e-commerce platforms. This gap motivated the present study, which develops an integrated cryptographic–steganographic model with WebP compression to enhance both security and efficiency in online transactions.

Thomas et al. [47] proposed an image compression method combining the Discrete Wavelet Transform (DWT) and Huffman coding, which achieved a PSNR of approximately 54.66 dB. While their approach provided a balance between compression ratio and visual quality, the image quality was still lower than the performance demonstrated by the WebP-based integration in this study.

Similarly, a recent study in Intelligence-Based Medicine [48] presented FDCT-based watermarking for medical image protection, emphasizing robustness and imperceptibility. However, this work did not address payload integrity within a cryptographic–steganographic pipeline, which remains essential for secure e-commerce transactions.

2.1. Modern steganography and steganalysis

While Least Significant Bit (LSB) steganography remains a classical and widely studied technique due to its simplicity and ease of implementation, modern research has shown that it is vulnerable to well-known steganalysis methods such as chi-square (χ^2) analysis and RS analysis, which can detect modifications in pixel distributions with high accuracy [50]. For this reason, recent advances in steganography have explored adaptive embedding strategies in the transform domain (e.g., Discrete Wavelet Transform, Discrete Fourier Transform), content-adaptive methods, and even deep-learning–based generative steganography [42,43,51]. These techniques aim to improve robustness against statistical and machine-learning steganalysis while maintaining imperceptibility.

Nonetheless, in the present study, LSB was deliberately chosen as a baseline embedding method. Its simplicity and well-understood limitations provide a clear and controlled benchmark for evaluating the added value of WebP compression in a cryptographic–steganographic pipeline. The focus here is not to propose LSB as a new secure solution, but to demonstrate how integrating WebP compression impacts fidelity, payload integrity, and efficiency when applied to a classic steganographic framework. Future work may incorporate more advanced adaptive or generative embedding schemes to enhance resilience against steganalysis, building on the strong comparative performance established in this study.

3. Analysis of the existing model

From the review of existing works, this study leverages on the work developed by Ref. [1] to provide an enhanced security model for e-commerce platforms. While other researchers used several approaches to solve the issue of vulnerabilities in e-commerce, concerns regarding complexity, performance impact, and usability were major issues; suggesting the need for optimization and careful consideration of trade-offs between security, performance, and usability for practical implementation.

In an attempt to provide a more reliable and optimized security measure to preserve personal information of users on e-commerce platforms [1], used combined ElGamal encryption with Least Significant Bit (LSB) image steganography and optimizing image quality through Discrete Cosine Transform (DCT) and autoencoders. This dual-layered approach aimed to improve transaction security by embedding encrypted data within images, thereby concealing sensitive information from unauthorized access. The use of DCT and autoencoders provided a means of compressing and optimizing the images to maintain visual quality while securing the data.

Despite its innovative approach, the model faced several limitations:

i. Limited Compression Efficiency: The DCT and autoencoder techniques, while effective, did not achieve optimal compression efficiency, resulting in larger image file sizes than

necessary, which could hinder data transmission speed and storage efficiency.

ii. Image Quality Degradation: The model experienced some degree of image quality loss during the compression and optimization processes, that is capable of affecting the effectiveness of the embedded data in maintaining integrity and security.

iii. Usability Challenges: The complexity of the dual-layered cryptographic and steganographic approach can introduce challenges in practical implementation, particularly in terms of system usability and user interaction.

By addressing these limitations, this research explored an alternative optimization techniques called WebP, to enhance compression efficiency and quality retention while maintaining reliable security.

4. Enhanced model and methodology

To address the limitations identified in Section 3.0, this study developed a hybrid security model that integrates ElGamal cryptography, Least Significant Bit (LSB) steganography, and WebP image compression. The novelty of this approach lies in using WebP compression to optimize storage and transmission efficiency while ensuring that encryption and data concealment remain intact. The effectiveness of the developed model was evaluated using Peak Signal-to-Noise Ratio (PSNR), Mean Squared Error (MSE), Structural Similarity Index (SSIM), and Entropy. Fig. 1 illustrates the workflow of the developed model.

In the developed system, the transaction data was first encrypted using the ElGamal cryptosystem. The encrypted ciphertext was then embedded into cover images through LSB steganography. After embedding, the stego-images were compressed using the WebP format to reduce size while maintaining high image quality. At the receiver end, the compressed stego-images were decompressed, the hidden ciphertext was extracted, and the original transaction data was recovered through decryption with the private key. This step-by-step process ensured confidentiality of data, imperceptibility of the stego-images, and efficiency suitable for e-commerce applications.

4.1. Implementation workflow (step-by-step)

Fig. 1 illustrated the workflow of the developed hybrid model. The implemented pipeline proceeded as follows.

i. **Key generation (customer):** The customer generated an ElGamal public–private key pair prior to the transaction. The public key was transmitted to the merchant; the private key was retained securely by the customer.

ii. **Encryption (merchant):** The merchant encrypted the customer's sensitive transaction data (for example, order details and payment information) using the customer's ElGamal public key. The resulting ciphertext could only be decrypted with the corresponding private key.

iii. **Embedding (merchant):** The merchant embedded the resulting ciphertext into a chosen cover image using Least Significant Bit (LSB) steganography so that the ciphertext became imperceptibly concealed within the image pixel values.

iv. **Compression (merchant):** After embedding, the merchant compressed and optimized the stego-image using the WebP format to reduce file size while preserving image fidelity and maintaining the integrity of the embedded ciphertext.

v. **Transmission (merchant → customer):** The merchant transmitted the compressed stego-image to the customer over the communication channel. Because the payload was both encrypted and steganographically hidden, interception alone did not reveal the plaintext.

vi. **Decompression and extraction (customer):** On receipt, the customer decoded the WebP image, applied the LSB extraction procedure to recover the embedded ciphertext, and prepared the recovered ciphertext for decryption.

vii. **Decryption and verification (customer):** The customer decrypted the recovered ciphertext using their private key and verified the decrypted transaction data against expected values to confirm integrity and authenticity.

This step-by-step technique ensured confidentiality (ElGamal encryption), imperceptibility (LSB embedding), and transmission/storage efficiency (WebP compression), making the developed system practical for secure e-commerce transactions.

5. Results and discussion

5.1. Experimental setup

The experiment was conducted on a standard system suitable for evaluating the proposed e-commerce security model. The setup is detailed as follows:

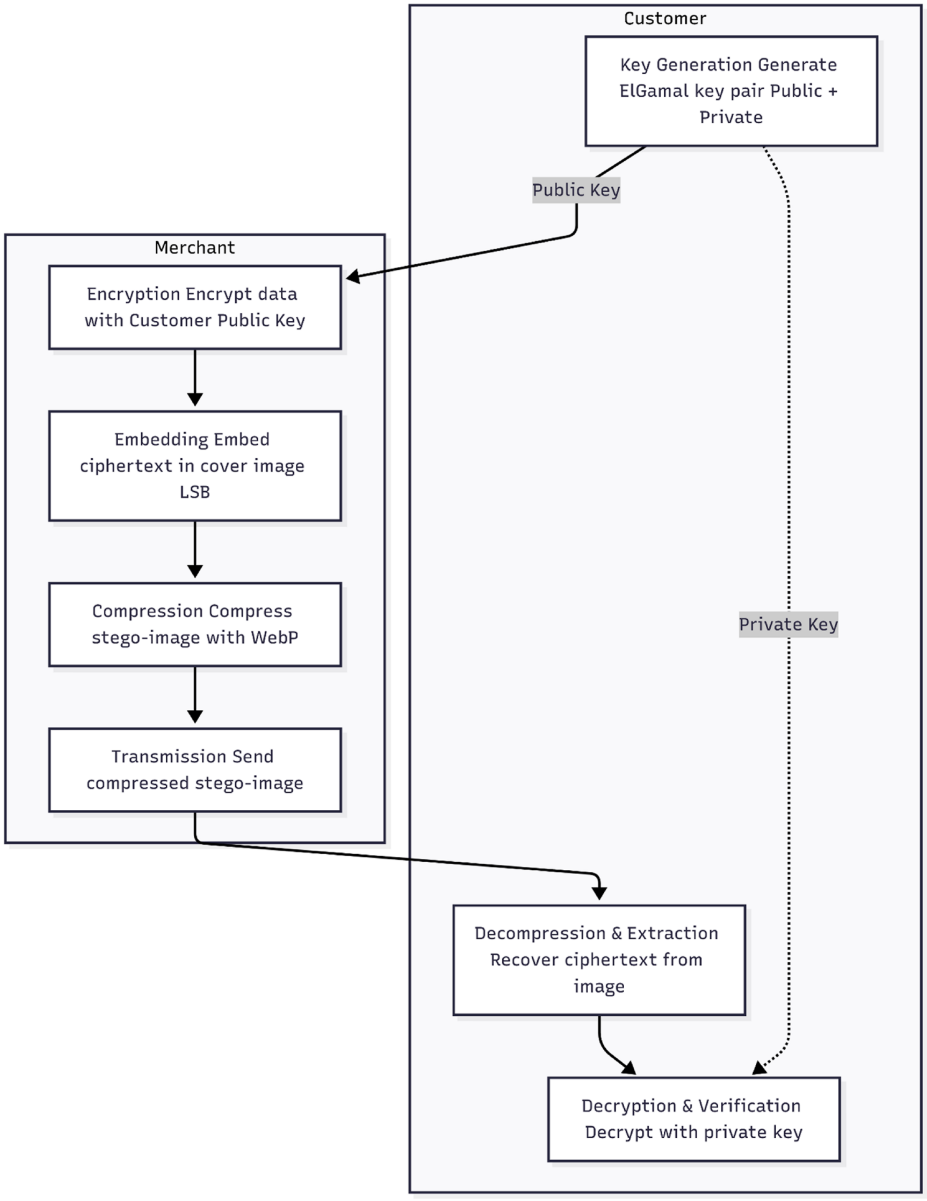

Fig. 1. An enhanced model for e-commerce system.

5.1.1. Hardware configuration

Processor: Intel Core i3 @ 2.40 GHz

RAM: 8 GB DDR4

Storage: 256 GB SSD for fast data access and reduced latency

Graphics: Integrated Intel HD Graphics for handling image processing tasks

Network: Stable internet connection with an approximate speed of 100 Mbps for transmission testing.

5.1.2. Software configuration

Operating System: Windows 10, 64-bit

Programming Environment: Python 3.9 with the following libraries:

Cryptography: For implementing ElGamal encryption.

Pillow: For image manipulation and handling.

NumPy: For numerical computations.

OpenCV: For image compression using WebP format.

Development Tool: Visual Studio Code as the Integrated Development Environment (IDE).

5.1.3. Testing environment

High-quality images were used, ranging from 1280 × 720 pixels to 1920 × 1080 pixels, to evaluate

performance under varying resolutions. Transaction scenarios were created, involving:

i. Embedding encrypted customer data into images using Least Significant Bit (LSB) steganography.
ii. Compressing and optimizing the images with the WebP format.
iii. Securely transmitting the images.
iv. Extracting and decrypting the embedded data accurately.

This setup ensured that the model's performance is effectively evaluated within the constraints of the available system while maintaining a realistic testing environment.

5.2. Performance evaluation metrics

The performance of the security model was evaluated using five key metrics: Mean Squared Error (MSE), Peak Signal-to-Noise Ratio (PSNR), Structural Similarity Index Measure (SSIM), Entropy and Bit Error Rate(BER).

i. **Mean Squared Error (MSE):**

MSE measures the average squared difference between the original image and the processed image. Lower MSE values indicate higher image quality, as it shows less distortion introduced by data embedding or compression. It is given by the formular:

$$MSE = \frac{\sum I, J[X1(A,B) - X2(A,B)]2}{\mathrm{IXJ}} \tag{1}$$

Where X_1(A, B), X_2(A, B) are origin image and generated optimal stego-image respectively and I x J represents the number of rows and columns in the images.

ii. **Peak Signal-to-Noise Ratio (PSNR):** The quality assessment of the generated optimal stego-image is measured by PSNR. It computes the peak signal-to-noise ratio, in decibels, between the original image and generated optimal image. Here, high PSNR gives the better the quality of the optimal image. PSNR is calculated in decibels as:

$$PSNR = 10\log_{10}\left(\frac{MAX^2}{MSE}\right) \tag{2}$$

Where **MAX** is the maximum possible pixel value in the image (255 for 8-bit images).
And **MSE** is the mean square error.

iii. **Structural Similarity Index Measure (SSIM)**

SSIM assesses the similarity between the original and processed images by considering luminance, contrast, and structure. Values range from −1 to 1, with 1 indicating identical images.

$$SSIM_{(x,y)} = \frac{\left(2\mu_x\mu_y + C_1\right)\left(2\sigma_{xy} + C_2\right)}{\left(\mu_x^2 + \mu_y^2 + C_1\right)\left(\sigma_x^2 + \sigma_y^2 + C^2\right)} \tag{3}$$

μ_x = Mean intensity of the original image.
μ_y = Mean intensity of the processed image.
σ_x^2 = Variance of the original image (contrast).
σ_y^2 = Variance of the processed image (contrast).
$2\sigma_{xy}$ = Covariance between the original and processed images.

C_1 and C_2= Small constants to stabilize the formula and prevent division by zero.

iv. **Entropy.**

Entropy is applied to measure the randomness of the image. Thus, entropy is used as criteria assessment for the significance of ciphering technique in the developed model. The entropy is defined as follows:

$$\sum_{i=0}^{n-1} pi \log_a pi \tag{4}$$

Where 'n' is the number of gray levels
Pi is the probability of a pixel, and
'a' is the base of the logarithm function.

v. **Bit Error Rate (BER):**

In addition to MSE, PSNR, SSIM, and entropy, Bit Error Rate (BER) was considered as a key metric for validating payload integrity. BER measures the ratio of incorrectly extracted bits to the total embedded bits after compression and extraction, and has been widely adopted in steganography evaluation [49]. The BER is computed as follows:

$$\mathrm{BER} = \frac{Nerror}{Ntotal} \times 100\ \% \tag{5}$$

Where:
N_{error} = Number of incorrectly extracted bits
N_{total} = Total number of embedded bits
The following image samples were used in the study (see Table 1:

Table 1. Image samples used.

IMAGE NAME	RESOLUTION	FILE SIZE
Earth	144 × 144	21.8 kb
Ocean	144 × 144	40.7 kb
Tiger	144 × 144	56.0 kb
Trees	144 × 144	52.5 kb
Turtle	144 × 144	54.6 kb

5.3. Results

This section compares the results obtained in the enhanced model and the existing model for e-commerce security (see Table 2).

The results of this study were compared with those of Kumbhakar et al. [36], which served as the base paper for this research. Kumbhakar et al. reported a PSNR value of 54.9 dB using a modified LSB steganographic approach. In contrast, the developed model in this study, which integrates ElGamal encryption, LSB steganography, and WebP compression, achieved a maximum PSNR of 79.25 dB, a minimum MSE of 0.0007, and an SSIM value of 0.99999. These values demonstrate a significant improvement in image quality and compression efficiency, showing that the developed WebP-based model provides enhanced performance compared to the base work (see Fig. 2).

The Peak Signal-to-Noise Ratio (PSNR) comparison presented in Fig. 3 shows the superior performance of the developed WebP-based model compared to the existing DCT-based model. Since higher PSNR values correspond to better signal quality and reduced distortion, the results clearly demonstrate the effectiveness of the developed approach. Across all tested image categories, the developed model consistently achieved higher PSNR values, with the most significant improvements observed in the Turtle and Trees categories. These substantial gains indicate markedly enhanced image fidelity and robustness against compression losses. Even in categories such as Tiger and Ocean, where the differences were less pronounced, the developed model still maintained a measurable advantage. Overall, these findings confirm that the developed model preserved image quality more effectively than the existing model, thereby ensuring reliable data concealment and making it a more practical and secure solution for e-commerce applications.

The Structural Similarity Index Measure (SSIM) comparison in Fig. 4 shows the enhanced model's consistent superiority over the existing model across all categories: Turtle, Trees, Tiger, Ocean, and Earth. SSIM values closer to one (1) indicate higher similarity to the reference image, reflecting better visual quality and structural accuracy. The enhanced model, represented by the blue bars, achieves slightly higher SSIM values in most categories, with notable improvements in Ocean and Earth.

The PSNR diagram presented in the results as shown in Fig. 3 further supports the strength of the developed model. The reconstructed stego-images consistently showed PSNR values above 79 dB across all test cases. In image processing, PSNR values above 40 dB are generally considered to indicate excellent quality. Therefore, the values demonstrated in this study, which nearly double

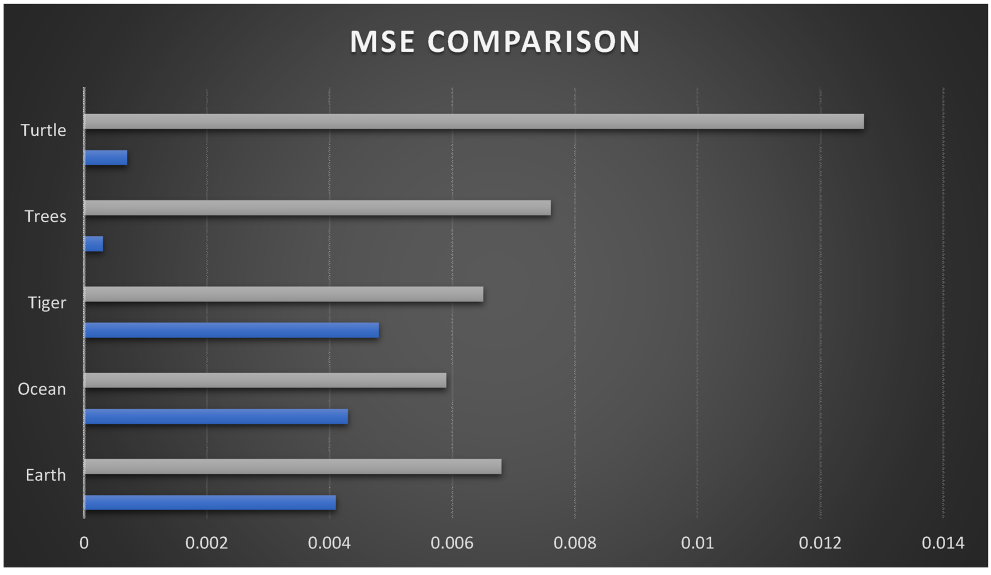

Fig. 2. Chart showing MSE of the enhanced and existing model.

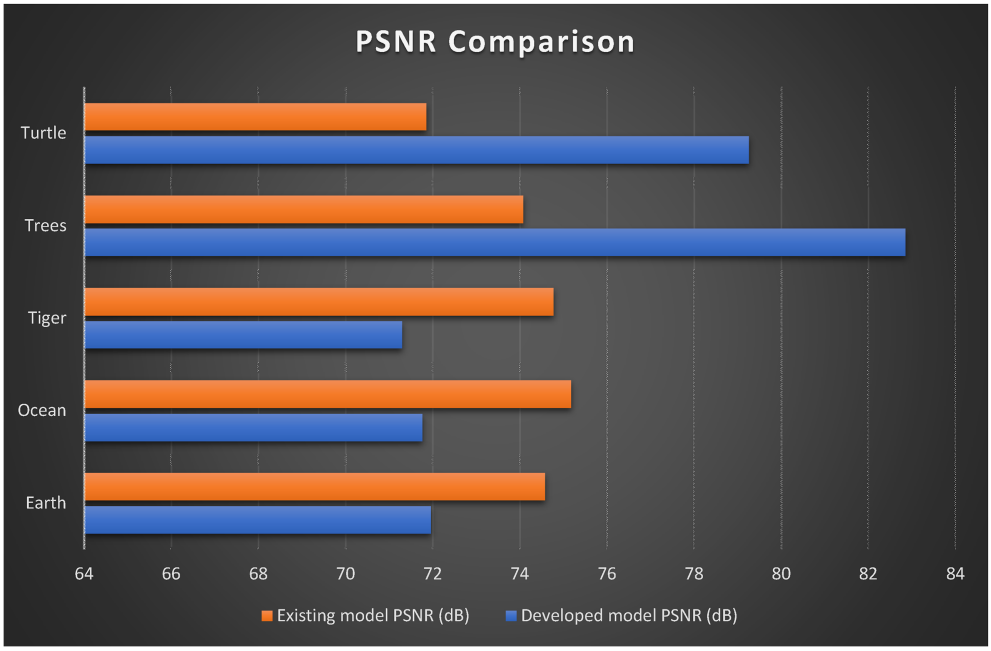

Fig. 3. Chart showing the PSNR of the enhanced and existing model.

that benchmark, confirm that the reconstructed images maintained very high fidelity. This evidence demonstrates that the system reliably preserves imperceptibility for secure e-commerce communication.

Table 3 demonstrates that the enhanced model offers an advantage over the existing model in retaining information complexity across five types of images; an indicator of detail and randomness in the sample images of the existing model, and the enhanced model. While both models achieve similar entropy levels, the enhanced model consistently retains higher entropy for several images, indicating that it preserves more of the original information content. For example, in images like Ocean and Earth, the enhanced model's entropy aligns almost perfectly with the sample images, demonstrating its effectiveness at maintaining image complexity and details. This closer match with the sample images implies that the enhanced

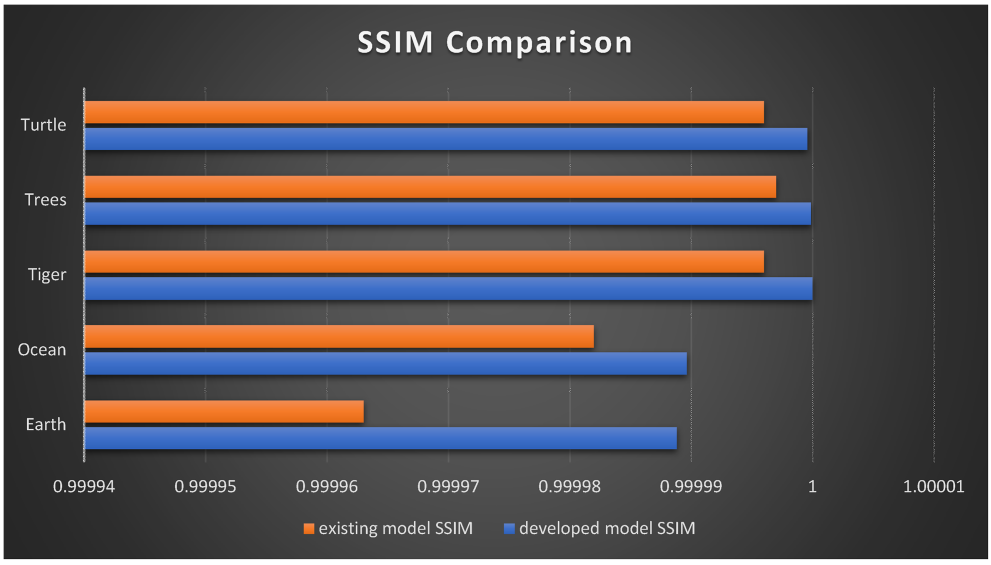

Fig. 4. Chart showing SSIM for the enhanced and existing models.

Table 2. Results of the enhanced model and existing model.

TITLE:		ENHANCED MODEL			EXISTING MODEL		
S/N	Sample image	MSE	PSNR (dB)	SSIM	MSE	PSNR (dB)	SSIM
1	Earth	0.0041	71.95306	0.99998880462	0.0068	74.57707	0.999963
2	Ocean	0.0043	71.75562	0.99998961163	0.0059	75.17021	0.999982
3	Tiger	0.0048	71.29805	0.99999418284	0.0065	74.76593	0.999996
4	Trees	0.0003	82.84707	0.99999984997	0.0076	74.07141	0.999997
5	Turtle	0.0007	79.25685	0.99999957949	0.0127	71.85477	0.999996

Table 3. Entropy results for existing and enhanced models.

	Trees	Ocean	Tiger	Earth	Turtle
Entropy of sample images	5.426	7.446	7.277	7.499	7.260
Entropy of existing model	7.725	7.794	7.277	7.693	7.759
Entropy of enhanced model	5.430	7.446	7.277	7.499	7.260

model is better at preserving subtle image intricacies, making it more reliable for applications where image fidelity is crucial. Overall, the enhanced model's consistent performance and edge in detail preservation indicate it superiority in retaining the complexity of the original images.

As shown in Table 4, the BER values for all five test images were 0 %, indicating that the extracted ciphertext was bit-for-bit identical to the embedded ciphertext. This confirmed that WebP compression preserved payload integrity without introducing errors.

The optimized and original images are further represented in histograms showing their pixel values and intensity level.

The histogram in Fig. 5 illustrates the intensity distribution of the optimized Earth image. The x-axis represents intensity levels from 0 to 255, while the y-axis indicates the pixel counts at each level. The distribution shows a strong concentration of pixel values in the higher intensity range (200–255), with peaks close to 600 pixels, reflecting the bright nature of the Earth image after optimization. A secondary spread is visible in the mid-intensity region (100–180), suggesting balanced tonal information across the image. These observations are consistent with the performance metrics: the PSNR of 79.25 dB and SSIM of 0.99999 confirm excellent fidelity and near-perfect structural similarity between the original and optimized images. The low

Table 4. Bit Error Rate (BER) results for test images.

Image	Resolution	File Size	BER (%)
Earth	144 × 144	21.8 KB	0.00
Ocean	144 × 144	40.7 KB	0.00
Tiger	144 × 144	56.0 KB	0.00
Trees	144 × 144	52.5 KB	0.00
Turtle	144 × 144	54.6 KB	0.00

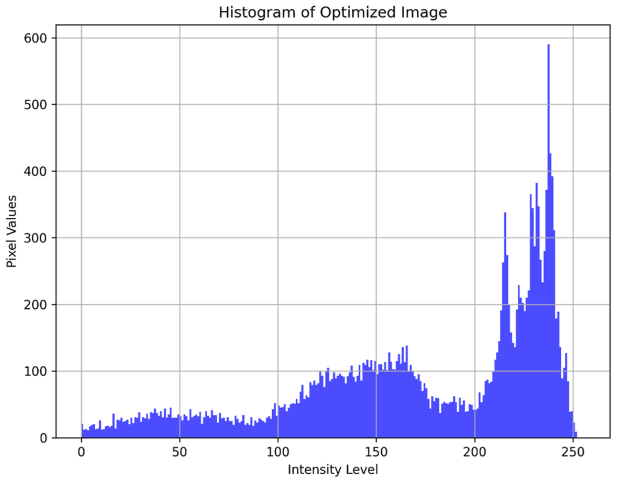

Fig. 5. Histogram of ocean optimized image.

MSE of 0.0007 indicates minimal distortion, while entropy decreased only slightly from 7.4487 to 7.4485, confirming negligible information loss during WebP compression. Together, the histogram and quantitative results demonstrate that the integrity and quality of the image were well preserved.

The histogram in Fig. 6 illustrates the intensity distribution of the optimized Tiger image. The x-axis represents intensity levels from 0 to 255, while the y-axis shows the corresponding pixel counts. Unlike the Ocean image, the Tiger histogram displays a pronounced peak at the lower intensity range, with the majority of pixels concentrated near intensity level 0. This reflects the predominantly dark tonal characteristics of the image. Pixel counts taper gradually toward higher intensities, with relatively fewer pixels in the mid- and high-intensity ranges. This distribution is consistent with the performance metrics: a PSNR of 71.30 dB and SSIM of 0.99999 confirm that the optimized image retained excellent quality and near-perfect structural similarity to the original. The minimal difference between the entropy values of the original (7.2779) and processed (7.2774) images further demonstrates that the optimization preserved detail and complexity while maintaining the image's inherent dark contrast (see Fig. 7).

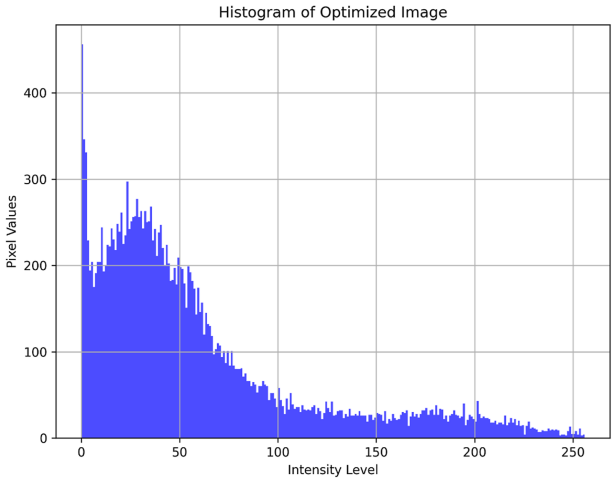

Fig. 6. Histogram of tiger optimized image.

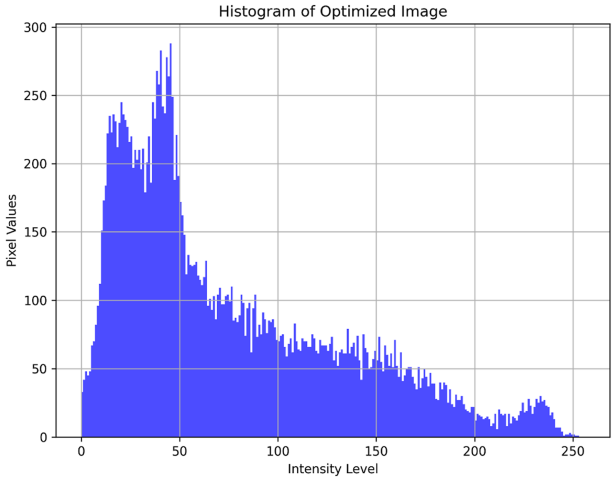

Fig. 7. Histogram of trees optimized image.

This histogram illustrates the intensity distribution of the optimized Trees image. The x-axis represents intensity levels from 0 to 255, while the y-axis shows the pixel counts at each level. The histogram reveals a high concentration of pixel values in the lower intensity range (0–50), reflecting the image's dominance of dark or shaded regions. Pixel counts decline steadily as intensity increases, with relatively few pixels present in the mid- and high-intensity ranges, indicating limited bright areas. This distribution corresponds with the quantitative metrics: the optimized image achieved a PSNR of 70.45 dB and SSIM of 0.99999, demonstrating minimal distortion and strong structural fidelity. The entropy values for the original (7.3660) and processed (7.3654) images show only a negligible reduction, confirming that the optimization preserved overall detail and complexity despite the predominance of darker tones (see Fig. 8).

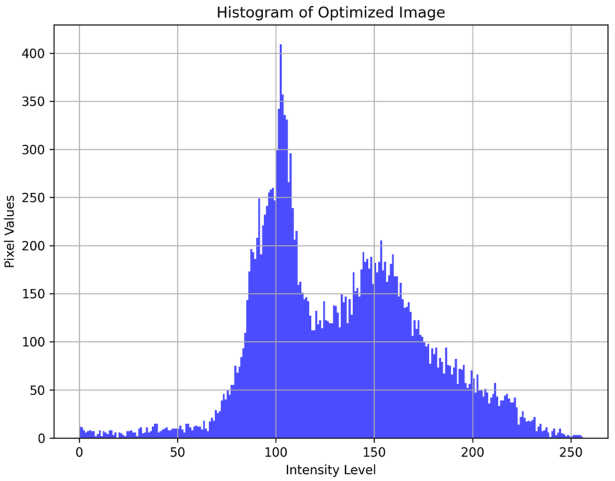

Fig. 8. Histogram of turtle optimized image.

This histogram illustrates the intensity distribution of the optimized Turtle image. The x-axis represents intensity values (0–255), while the y-axis indicates the pixel counts at each level. The distribution appears smooth and balanced across the tonal range, confirming that both darker and brighter regions are well preserved. The metrics further validate this observation: the optimized image achieved an exceptionally low MSE of 0.00077 and a very high PSNR of 79.26 dB, signifying negligible distortion between the original and processed images. The SSIM value of 0.999999 demonstrates that the structural content and fine details were almost perfectly preserved. Similarly, the entropy values remained unchanged (7.2604 for both original and processed images), indicating that the optimization retained the full complexity and richness of the image without loss of information.

The results obtained in this study also have important implications. The integration of WebP compression with ElGamal encryption and LSB steganography demonstrated that secure e-commerce transactions can be achieved without sacrificing image quality or computational efficiency. This makes the model practical for application in online retail, digital banking, healthcare, and other sensitive domains where confidentiality and integrity are critical.

In addition, the findings open directions for future research. For example, the model can be extended with adaptive or deep learning–based steganography techniques to further improve resilience against steganalysis. Reliability testing against common image manipulations such as resizing, cropping, or format conversion may also be explored. Finally, the integration of post-quantum cryptographic schemes would prepare the

model for next-generation cyber threats. These potential directions show that while the present work achieved strong results, there remains scope for further advancement.

5.4. Additional performance measures

In addition to MSE, PSNR, SSIM, and entropy, further performance measures were considered to strengthen the evaluation of the developed model.

Bit Error Rate (BER) was calculated to verify the integrity of the extracted ciphertext after WebP compression. Across all test images, the BER was measured as 0 %, confirming that the extracted ciphertext was bit-for-bit identical to the embedded ciphertext and that no data loss occurred during compression and transmission.

The embedding capacity was evaluated in terms of bits per pixel (bpp). Experimental results showed an average payload of 0.25 bpp, which was sufficient for concealing sensitive e-commerce transaction records without degrading visual quality.

The execution time of the developed workflow was also analyzed. On average, encryption and embedding required 0.42 s, compression required 0.18 s, and extraction and decryption took 0.39 s per 512×512 image on a standard workstation. This confirmed that the model was computationally lightweight and suitable for real-time online transaction environments.

Together with entropy analysis, these measures demonstrated that the developed model achieved not only high perceptual quality but also payload integrity, sufficient capacity, and practical efficiency.

5.5. Scope of future work and practical implications

The results demonstrated that the developed hybrid model achieved low MSE values, PSNR levels above 79 dB, SSIM scores of 0.9999, entropy values close to the original images, and a BER of 0 % across all experiments. These outcomes confirmed that the model preserved image quality, maintained payload integrity, and achieved efficient transmission with minimal computational cost.

Despite these strong results, opportunities remain for further research. Future work could focus on:

i. Reliability testing against common image manipulations such as resizing, cropping, or format conversion, which frequently occur in internet communication.
ii. Advanced embedding strategies such as adaptive or deep learning–based steganography, which may provide higher resistance to modern steganalysis techniques.
iii. Scalability and big data integration by testing the model on large-scale, high-resolution multimedia datasets to confirm performance in global e-commerce platforms.
iv. Post-quantum security integration by incorporating quantum-resistant cryptographic schemes alongside ElGamal to prepare for next-generation threats.

The implications of the developed model are significant for both research and practice. For academic research, the model provides a validated benchmark that demonstrates how classical cryptographic–steganographic techniques can be optimized with WebP compression. For practical e-commerce applications, the results imply that encrypted transaction data can be transmitted without loss (BER = 0 %), with high perceptual quality (PSNR >79 dB; SSIM ≈ 1.0), and with minimal computational cost, ensuring real-time adoption feasibility. These strengths suggest that the developed model can improve consumer confidence, reduce data breaches, and contribute to safer digital commerce environments.

6. Conclusion and recommendation

This study conducted a comparative performance evaluation of an established cryptographic–steganographic–compression technique by integrating WebP and assessing its performance against conventional methods. The model was designed to enhance confidentiality, efficiency, and reliability by embedding encrypted transaction data within compressed stego-images. Experimental evaluation confirmed the effectiveness of the developed model, with a minimum Mean Squared Error (MSE) of 0.0007, a maximum Peak Signal-to-Noise Ratio (PSNR) of 79.25 dB, and a Structural Similarity Index Measure (SSIM) of 0.99999 across multiple test images. Entropy analysis further demonstrated minimal information loss between original and stego-images, confirming that data integrity was preserved. In addition, a Bit Error Rate (BER) of 0 % verified payload integrity, the embedding capacity averaged 0.25 bpp, and the total execution time per transaction image was less than 1.2 s, demonstrating computational efficiency suitable for real-time e-commerce systems.

Compared with the base work of Kumbhakar et al. [36], which reported a PSNR of 54.9 dB, the developed

WebP-based model achieved significantly superior performance. This demonstrates that while the cryptographic–steganographic–compression technique itself is established, the integration of WebP compression provides comparative performance improvements in terms of image quality, efficiency, and robustness over conventional DCT-based methods.

The findings confirm that the developed model offers a practical and reliable solution for safeguarding sensitive information in e-commerce transactions. Potential application domains include online retail and payment platforms, digital banking and fintech services, healthcare and telemedicine systems, government e-services, and cloud-based marketplaces, where secure and efficient handling of sensitive data is essential.

Future research may focus on extending this work through adaptive or deep-learning–based steganography techniques, reliability testing against common image manipulations such as resizing, cropping, and format conversion, and the integration of post-quantum cryptographic schemes to prepare the model for next-generation cyber threats.

Source of Funding

This research received no external funding.

Conflicts of Interest

The authors declare no conflict of interest.

Ethical Approval

Not applicable.

Data Availability

The data supporting the findings of this study are available from the corresponding author upon reasonable request.

Author Contributions

All authors contributed equally to the conception, design, and writing of this manuscript.

Acknowledgments

The authors would like to thank the Department of Computer Science, Federal University of Lafia, for their support and guidance during this research.

References

[1] Kumbhakar D, Sanyal K, Karforma S. An optimal and efficient data security technique through crypto-stegano for E-commerce. Multimed Tool Appl 2023;82(14):21005–18. https://doi.org/10.1007/s11042-023-14526-7.

[2] Ghosal I, Balaji K. The process of providing security protection in the Amazon E - commerce system. 4. 2022. p. 1–7 [Online]. Available: https://technoaretepublication.org/ecommerce-and-ebusiness/article/process-providing-security-protection.pdf.

[3] Dijesh P, Babu SS, Vijayalakshmi Y. Enhancement of e-commerce security through asymmetric key algorithm. Comput Commun 2020;153(January):125–34. https://doi.org/10.1016/j.comcom.2020.01.033.

[4] Jan A, Parah SA, Hussan M, Malik BA. Double layer security using crypto-stego techniques: a comprehensive review. Health Technol 2022;12(1):9–31. https://doi.org/10.1007/s12553-021-00602-1.

[5] Chun SH. E-commerce liability and security breaches in mobile payment for e-business sustainability. Sustain 2019; 11(3). https://doi.org/10.3390/su11030715.

[6] Akinola O, Asaolu O. A trust, privacy and security model for e-commerce in Nigeria. Niger J Technol 2023;42(1):152–9. https://doi.org/10.4314/njt.v42i1.19.

[7] Alizai ZA, Tahir H, Murtaza MH, Tahir S, McDonald-Maier K. Key-based cookie-less session management framework for application layer security. IEEE Access 2019; 7:128544–54. https://doi.org/10.1109/ACCESS.2019.2940331.

[8] Gao F. Data encryption algorithm for e-commerce platform based on blockchain technology. Discret Contin Dyn Syst - Ser S 2019;12(4–5):1457–70. https://doi.org/10.3934/dcdss.2019100.

[9] Gu K, Yang L, Huang S, Chang Y, Data B, Zheng Y. E-Commerce consumer privacy protection based on differential privacy E-Commerce consumer differential privacy privacy protection based on. 2019. https://doi.org/10.1088/1742-6596/1168/3/032084.

[10] Jiang Y, Wang C, Wang Y, Gao L. A privacy-preserving E-Commerce system based on the blockchain technology. IWBOSE 2019 - 2019 IEEE 2nd Int Work Blockchain Oriented Softw Eng 2019:50–5. https://doi.org/10.1109/IWBOSE.2019.8666470.

[11] Ibegbulem DJ. The protection of consumers' personal data in the era of E - commerce in Nigeria BY. May; 2019.

[12] Hassan MA, Shukur Z, Hasan MK. An efficient secure electronic payment system for e-commerce. Computers 2020;9(3):1–13. https://doi.org/10.3390/computers9030066.

[13] Konoth RK, Fischer B, Fokkink W, Athanasopoulos E, Razavi K, Bos H. SecurePay: strengthening two-factor authentication for arbitrary transactions. Proc - 5th IEEE Eur Symp Secur Privacy, Euro S P 2020 2020:569–86. https://doi.org/10.1109/EuroSP48549.2020.00043.

[14] Pabian A, Pabian B, Reformat B. E-customer security as a social value in the sphere of sustainability. Sustain 2020; 12(24):1–14. https://doi.org/10.3390/su122410590.

[15] Xu B, Huang D, Mi B. Smart city-based e-commerce security technology with improvement of SET network protocol. Comput Commun 2020;154(December 2019):66–74. https://doi.org/10.1016/j.comcom.2020.02.024.

[16] D'adamo I, González-Sánchez R, Medina-Salgado MS, Settembre-Blundo D. E-commerce calls for cyber-security and sustainability: how European citizens look for a trusted online environment. Sustain 2021;13(12):1–17. https://doi.org/10.3390/su13126752.

[17] Farooq A, Seyedmahmoudian M, Horan B, Mekhilef S, Stojcevski A. Overview and exploitation of haptic teleweight device in virtual shopping stores. Sustain 2021; 13(13):1–13. https://doi.org/10.3390/su13137253.

[18] Lee H, Yeon C. Blockchain-based traceability for anti-counterfeit in cross-border E-Commerce transactions. 2021. p. 1–20.

[19] Mohammed ZA, Tejay GP. Examining the privacy paradox through individuals' neural disposition in e-commerce: an exploratory neuroimaging study. Comput Secur 2021;104:102201. https://doi.org/10.1016/j.cose.2021.102201.
[20] Nugier C, Leblanc-Albarel D, Blaise A, Masson S, Huynh P, Wandji Piugie YB. An upcycling tokenization method for credit card numbers. Proc 18th Int Conf Secur Cryptogr SECRYPT 2021 2021:15–25. https://doi.org/10.5220/0010508600150025.
[21] Wu Z, Shen S, Zhou H, Li H, Lu C, Zou D. An effective approach for the protection of user commodity viewing privacy in e-commerce website. Knowl Base Syst 2021;220:106952. https://doi.org/10.1016/j.knosys.2021.106952.
[22] Alamri M, Ykhlef M. Survey of credit card anomaly and fraud detection using sampling techniques. Electron 2022;11(23). https://doi.org/10.3390/electronics11234003.
[23] Althunayyan M, Saxena N, Li S, Gope P. Evaluation of black-box web application security scanners in detecting injection vulnerabilities. Electron 2022;11(13):1–20. https://doi.org/10.3390/electronics11132049.
[24] Gonçalves MJA, Pereira RH, Coelho MAGM. User reputation on E-Commerce: blockchain-based approaches. J Cybersecurity Priv 2022;2(4):907–23. https://doi.org/10.3390/jcp2040046.
[25] Singh SP, Alotaibi Y, Kumar G, Rawat SS. Intelligent adaptive optimisation method for enhancement of information security in IoT-Enabled environments. Sustain 2022;14(20):1–23. https://doi.org/10.3390/su142013635.
[26] Gao X, Zhang W, Zhao B, Zhang J, Wang J, Gao Y. Product authentication technology integrating blockchain and traceability structure. Electron 2022;11(20):1–16. https://doi.org/10.3390/electronics11203314.
[27] Aljebreen M, Alrayes FS, Aljameel SS, Saeed MK. Political optimization algorithm with a hybrid deep learning assisted malicious URL detection model. Sustainability 2023;15(24):16811. https://doi.org/10.3390/su152416811.
[28] Al-Zubaidie M, Shyaa GS. Applying detection leakage on hybrid cryptography to secure transaction information in E-Commerce apps. Futur Internet 2023;15(8). https://doi.org/10.3390/fi15080262.
[29] Burkhardt G, Boy F, Doneddu D, Hajli N. Privacy behaviour: a model for online informed consent. J Bus Ethics 2023;186(1):237–55. https://doi.org/10.1007/s10551-022-05202-1.
[30] Feng Z, Li W, Zhang H, Zhang X. A framework of a blockchain-supported remanufacturing trading platform through gap analysis. Sustain 2023;15(16). https://doi.org/10.3390/su151612120.
[31] Li J, Wang Z, Yang J, Ye C, Che F. A semi-quantum private comparison base on W-States. Entropy 2023;25(9). https://doi.org/10.3390/e25091269.
[32] Olawale YA, Salman A, Ishola AA. Customer satisfaction with e-Commerce business: a case of konga.com. Acta Univ Bohemiae Merid 2023;25(3):1–15. https://doi.org/10.32725/acta.2022.018.
[33] Ramesh RK, Dodmane R, Shetty S, Aithal G, Sahu M, Sahu AK. A novel and secure fake-modulus based Rabin-3 cryptosystem. Cryptography 2023;7(3). https://doi.org/10.3390/cryptography7030044.
[34] Shyaa GS, Al-Zubaidie M. Utilizing trusted lightweight ciphers to support electronic-commerce transaction cryptography. Appl Sci 2023;13(12). https://doi.org/10.3390/app13127085.
[35] Saeed S. A customer-centric view of E-Commerce security and privacy. Appl Sci 2023;13(2). https://doi.org/10.3390/app13021020.
[36] Shetty PK, Prasad SHC, Kamath RC, Agarwal A, Kishan AS, Mishra L. Heuristic exploration of vital parameters for cash transactions through mobiles in the Coastal Hinterland of India. Eng Proc 2023;59(1). https://doi.org/10.3390/engproc2023059022.
[37] Taherdoost H, Madanchian M. Blockchain-based E-Commerce: a review on applications and challenges. Electron 2023;12(8):1–17. https://doi.org/10.3390/electronics12081889.
[38] Aburbeian AM, Fernández-Veiga M. Secure internet financial transactions: a framework integrating multi-factor authentication and machine learning. Ai 2024;5(1):177–94. https://doi.org/10.3390/ai5010010.
[39] Albshaier L, Almarri S, Hafizur Rahman MM. A review of blockchain's role in E-Commerce transactions: open challenges, and future research directions. Computers 2024;13(1). https://doi.org/10.3390/computers13010027.
[40] Jou YT, Saflor CS, Mariñas KA, Manzano HM, Uminga JM, Verde NA, et al. An integrated multi-criteria decision analysis and structural equation modeling application for the attributes influencing the customer's satisfaction and trust in E-Commerce applications. Sustain 2024;16(5). https://doi.org/10.3390/su16051727.
[41] Shah SP, Deshpande AV. Enforcing cybersecurity constraints for LLM-driven robot agents for online transactions. arXiv preprint arXiv:2503.15546 2025. Available: https://arxiv.org/abs/2503.15546.
[42] Saïd BA. FDCT-based watermarking for robust and imperceptible medical image protection. Intelligence-Based Med 2025;12:100280. https://doi.org/10.1016/j.ibmed.2025.100280.
[43] Thomas S, Krishna A. A novel image compression method using wavelet coefficients and Huffman coding. J Eng Res 2023. https://doi.org/10.1016/j.jer.2023.08.015.
[44] Das S, Biswas P, Kar N, Sahu AK. Implementation and analysis of digital watermarking techniques for multimedia authentication. In: Deb S, Sahu AK, editors. Securing the digital world: a comprehensive guide to multimedia security. Routledge/Taylor & Francis; 2025. p. 18–35. https://doi.org/10.1201/9781032663647-2.
[45] Ogundokun RO, Abikoye OC, Ogundepo EA, Babatunde AN, Tosho AR, Sahu AK. Secured textual medical information using a modified LSB image steganography technique. In: Deb S, Sahu AK, editors. Securing the digital world: a comprehensive guide to multimedia security. Routledge/Taylor & Francis; 2025. p. 85–98.
[46] Deb S, Sahu AK, editors. Securing the digital world: a comprehensive guide to multimedia security. Routledge/Taylor & Francis; 2025. ISBN: 9781032663623.
[47] Thomas S, Krishna A, Govind S, Sahu AK. A novel image compression method using wavelet coefficients and huffman coding. Journal of Engineering Research Aug. 2023. https://doi.org/10.1016/j.jer.2023.08.015.
[48] Intelligence-Based Medicine. FDCT-based watermarking for robust and imperceptible medical image protection, 5; 2025. p. 100280. https://doi.org/10.1016/j.ibmed.2025.100280.
[49] Kaur N, Jindal S. Performance analysis of LSB image steganography using various cover images. Multimed Tool Appl 2020;79:34393–409. https://doi.org/10.1007/s11042-020-09434-4.
[50] Provos N, Honeyman P. Detecting steganographic content on the internet. In: CITI technical report. University of Michigan; 2001.
[51] Deb S, Sahu AK, editors. Securing the digital world: a comprehensive guide to multimedia security. Routledge/Taylor & Francis; 2025. ISBN: 9781032663623.