ISSN: 2096-3246
Volume 58, Issue 01, 2026

# A COMPARATIVE ANALYSIS OF A HYBRID CRYPTOGRAPHIC FRAMEWORK FOR SECURE IMAGE TRANSMISSION IN CLOUD ENVIRONMENTS

**[1] D Shivarama Krishna,[2] Dr M.Nagaratna,**
[1] Research scholar,Department of CSE, Jawaharlal Nehru Technological University Hyderabad,Kukatpally, Hyderabad - 500 085, Telangana, India.
Mail id : devallashivaramakrishna@gmail.com
[2] Professor ,Department of CSE,University College of Engineering , Science & Technology Hyderabad.
Mail id : mratnajntu@jntuh.ac.in

**Abstract**

The rapid adoption of cloud computing for multimedia storage and transmission has intensified concerns related to data confidentiality, integrity, and unauthorized interception, particularly for sensitive image data. Conventional single-layer cryptographic techniques are increasingly inadequate against advanced cyber threats, dynamic attacks, and emerging quantum adversaries. This paper presents a comparative analysis of a hybrid cryptographic framework designed to enhance secure image transmission in cloud environments by integrating encryption, encoding, and covert communication mechanisms. The proposed framework combines AES, One-Time Pad (OTP), and RSA to achieve secure and adaptive key management with time-limited access control, ensuring strong confidentiality and resistance to key compromise. To preserve image integrity and minimize transmission distortion, a Federated Wavelet-Based Convolutional Quotient Multipixel Value Differencing (F-WCQMVD) scheme is employed, enabling efficient and privacy-preserving encoding across distributed cloud nodes. Furthermore, isogeny-based cryptography integrated with spread spectrum steganography is utilized to provide post-quantum security and stealthy communication, concealing the very existence of sensitive image data during transmission. A comprehensive comparative evaluation is conducted against conventional cryptographic, steganographic, and hybrid approaches using metrics such as Peak Signal-to-Noise Ratio (PSNR), Mean Squared Error (MSE), Structural Similarity Index (SSI), encryption and decryption time, latency, and security efficiency. Experimental results demonstrate that the proposed hybrid framework significantly outperforms existing methods in terms of image quality preservation, computational efficiency, robustness to steganalysis, and quantum resistance. The findings confirm that the integration of adaptive encryption, wavelet-based federated encoding, and isogeny-driven covert communication provides a scalable and resilient solution for secure image transmission in modern cloud environments.

**Keywords:** Cloud Computing Security, Hybrid Cryptography, Isogeny-Based Cryptography, Secure Image Transmission, Wavelet-Based Steganography

## 1. Introduction

The phenomenal expansion of cloud computing has revolutionized the digital image storage, processing, and transmission in the distributed environment, which allows scalability of access, economical nature and smooth data sharing of digital data[1]. Nevertheless, this has seen a mass adoption that have come with serious security issues especially with respect to passing sensitive image information over untrusted cloud setups[2]. Images that are involved

in fields like healthcare, defence, surveillance, and financial services can usually include confidential data, and in such a case, they are the most appealing targets of cyberattacks, data exfiltration, and unauthorized use[3]. Conventional security solutions, based on single-layer encryption or key management that is static, are becoming less effective when it comes to dealing with advanced persistent threats, dynamic attacks and the increased threat of quantum-enabled adversaries emerge[4]. Standard cryptographic tools like AES, RSA, and ECC provide high-security when applied as single tools, but each one of them has certain limitations in the context of cloud-based transmission of images[5]. Symmetric schemes are fast, but prone to key distribution and reuse security issues, whereas asymmetric strategies have very high computational costs and scalability[6]. Furthermore, cryptographic security in itself does not hide the fact that there is sensitive data, which encrypted photos are susceptible to traffic and steganalysis attacks[7]. Other recent developments in steganography and wavelet-based encoding have enhanced the level of imperceptibility and robustness but most of the current techniques are not flexible, centrally resilient to security, and post-quantum[8]. These inadequacies demonstrate the need to have a multi-layered security architecture that is both confidentially assured, integrity assured, access control assured and covert communication assured[9].

In order to overcome these issues, this paper will provide a detailed comparative study of a hybrid cryptographic system using cloud-based systems to transmit images safely. The suggested structure combines AES, One-Time Pad (OTP), and RSA in order to provide flexible encryption, safe exchange of keys, and temporary access controls. The further improvement of Image integrity and transmission quality is done with the help of a Federated Wavelet-Based Convolutional Quotient Multipixel Value Differencing (F-WCQMVD) scheme, which facilitates privacy-aware encoding among the distributed cloud nodes. They also use isogeny-based cryptography and spread spectrum steganography to provide quantum-resistant and stealthy communication, which is an effective way of hiding sensitive images during communication. Using vast comparisons of the conventional cryptographic, steganographic and hybrid solutions when put through the normal standards of performance and security, the study shows that the proposed structure is more superior in delivering solid, scalable, and future-proof secure image transmission across the contemporary cloud platform.

**1.1 Research Motivation**

This study is motivated by the fact that the conventional single-layer cryptographic and steganographic methods have become increasingly ineffective in protecting the transmission of images in a cloud system against sophisticated cyber-attacks and new quantum attacks[10]. Current practices tend to be inflexible in key management, centralized, lack of flexibility and have inadequate protection against traffic analysis and steganalysis[11]. Further, the solutions available are mostly focused on encryption, image integrity or covert communication as opposed to a single security approach. These constraints have necessitated a pressing system of a versatile, adaptive and quantum-secure framework comprising of combined encryption, powerful image coding and stealth communication. The need to develop and comparatively analyse a multi-layered security architecture that is capable of providing confidentiality, integrity, access control, and imperceptibility in transmitting images in current cloud computing platforms is therefore the reason behind this research.

### 1.2 Research Significance

The importance of this study is that it will help in developing secure image transmission in cloud based systems by offering a unified and hybrid security architecture that will serve a variety of protection layers at the same time[12]. The method raises the level of confidentiality, image integrity, access control, and covert communication over the current conventional methods because of the adaptive hybrid cryptography, wavelet-based federated encoding, and post-quantum isogeny-based steganography. The comparative study shows quantifiable gains in the security strength, preservation of image quality, and computational power, which makes the framework very applicable in real world cloud based usages of sensitive visual data. In addition, the provision of quantum-resistant methods makes this study a progressive solution, which provides the security resiliency of future cloud-based multimedia systems.

### 1.3 Key Contribution

1. Designed a hybrid system that used AES-OTP encryption, RSA-based key exchange, wavelet-based federated steganography, and isogeny-based cryptography to realize secure and hidden transmissions of images in the cloud.

2. Adaptive key management was introduced with dynamic rotation of keys and time-limited access policy to prevent insider threat, key compromise and unauthorized access to cloud data.

3. Developed a federated CNN-based driven steganographic scheme of wavelet and QMPVD that maximizes imperceptibility, capacity, and hardening and maintains data privacy over distributed learning.

4. Combined isogeny-based cryptography and spread spectrum steganography to offer post-quantum security and stealth image transmission impervious to traffic analysis and steganalysis.

5. Implemented a comprehensive comparative study with traditional cryptographic and steganographic techniques in terms of security, image quality, and computational factors, showing better results in terms of scalability and performance in the transmission of images in clouds.

### 1.4 Structure of the Paper

The paper has the following structure. Section 1 presents the research problem, motivation, and objectives that are associated with the secure transmission of images in cloud environments. Section 2 provides a review of literature on cryptographic, steganographic and hybrid security methods. Section 3 has the hybrid approach that combines the encryption, steganography, quantum-resistant mechanism. Section 4 deals with experimental findings and performance comparison. Section 5 is a conclusion and it also gives directions on future research.

## 2. Literature Review

The Internet of Things (IoT) age has made the secure transmission of medical scan images in collaborative diagnosis a paramount necessity in telemedicine networks. The transmission of sensitive medical data must be kept safe so that patient privacy and unauthorized access can be avoided. In an attempt to overcome these issues, Shafique et al.[13]introduce a powerful hybrid encryption framework grounded on the combination of quantum and classical cryptography measures is established to promote the safety of medical

image transmission in telemedicine systems relying on IoT networks. The proposed model does not only mitigate cyber-attacks on the medical images, but also delivers a secure and efficient key management. The first step involves the use of Quantum Key Distribution (QKD) to manufacture a consumed secret key, which is then encrypted with One-Time Pad (OTP). All colour words of medical image are separated into bit-planes and the planes extracted are scrambled with randomly generated 6D hyperchaotic Chen system and Ikeda map. Multi-stage pixel scrambling operations in the form of pixel position permutation, pixel value shuffling, rotation and flipping are used to enhance the confusion process. Diffusion is then obtained by means of affine transformations, nonlinear functions, Discrete Cosine Transform (DCT) with complex modulation, Discrete Wavelet Transform (DWT) with random phase modulation, bilinear transformations, and nonlinear polynomial mapping. In order to decrease the computational complexity, theMost Significant Bit-Planes (MSBs) that carry more than 94 percent of the image information are only encrypted. The efficacy of the framework is verified by extensive experimental assessments such as an entropy analysis, key sensitivity analysis, correlation analysis, histogram analysis, and lossless reconstruction analysis.

Pothireddy et al.[14]emphasize the fact that hybrid encryption methods are increasingly being adopted in cloud computing is due to the fact that they help in mitigating challenges in data security and storage. In a bid to guarantee data confidentiality during the lifecycle of cloud processing, a new hybrid cryptographic model is suggested that combines Fully Homomorphic Encryption (FHE) and Secure Hash Algorithm SHA-3 that will work wonders in withstanding the escalating cyber-attacks. The FHE and the SHA-3 together provide secure computation of data and retain the integrity and confidentiality. The suggested framework is tested with several datasets to determine the level of performance and security efficiency, taking into account such aspects as computational load, complexity of algorithms, key management concerns, and inaccessibility to special hardware or software needed to homomorphic encryption. In spite of these difficulties, the hybrid scheme can scale effectively over distributed cloud nodes, and thus it can be used in the large scale cloud infrastructures of mission critical workloads. The experimental findings indicate that the FHE-SHA-3 hybrid can contribute significantly to the cybersecurity stance of the cloud-based systems. The comparisons of performance indicate better efficiency as compared to current techniques such as standalone homomorphic encryption techniques and also hybrid techniques like RSA AES, AES DSA and AES RSA.

The large-scale use of cloud computing has escalated the requirement of superior security systems to safeguard confidential information on distant computers. Although cloud platforms are scalable and flexible, they also cause serious security threats, especially in terms of maintenance of confidentiality of private data placed on third-party platforms. To solve these issues, Shivaramakrishna and Nagaratna[15]suggest an original hybrid cryptographic system is suggested to be used in order to store data securely in the clouds. The model incorporates the time boundary based access control, dynamic key management and a two-layer encryption plan consisting of the RSA and Advanced Encryption Standard-One Time Password (AES-OTP). Using asymmetric and symmetric encryption, the framework will increase data confidentiality and integrity. The key management module is adaptive which allows secure generation, distribution of keys and rotate keys periodically which enhances resilience of cryptography in the long run. Moreover, time-bounded access control limits the availability of data, which

minimises the likelihood of hacking and violating security. The implementation of the approach has been shown to be effective, with a result of 99.12, 98.78, 98.11, and 98.56 accuracy, precision, recall, and F1-score values respectively, a finding that the approach is appropriate in terms of secure and privacy-based cloud data storage.

Shivaramakrishna and Nagaratna [16]discuss the issue of the security of digital images relayed through distributed communication channels is a major concern since image data shall not be exposed to unauthorized access. Encryption, steganography and watermarking are common methods that are used to attain major security goals such as confidentiality, integrity and reliability. Steganalysis is also important in the process of identifying hidden messages in the allegedly innocent pictures. But the aspects of steganography have had a recent development that has rendered the use of steganalysis a hard task, and much of the available way or even the customary methods of detection have been known to perform with low grades. The authors offer a high-capacity image steganography framework combined with the IoT and deep learning technologies to address these limitations. Under the proposed method, secret data is encrypted by an effective transient homomorphic encryption algorithm to increase their resistance to detection. Embedding capacity and robustness are enhanced by use of Extended Wavelet Convolutional Equilibrium optimizer with Quotient Multi-Pixel Value Differencing (EWCE–QMPVD) to provide the advantage of data hiding and quality restoration of full-size images. As the majority of information that is hidden is captured by the high-frequency image components, the transformations performed are the wavelet-based ones, in order to extract these features. Then, a federated Convolutional Neural Network (CNN) is used to acquire high-level steganalysis features using the transformed images. IoT integration provides reliable exchange of stego-images so that service providers or the middlemen will not gain access to the encrypted message.

The impressive growth of cloud computing has revolutionized the data storage and communication aspects among individuals and institutions and has at the same time raised serious issues pertaining to data security and confidentiality. To overcome these challenges, Shivaramakrishna and Nagaratna [17]introduce the new system is put forward synthesizing the spread spectrum steganography and the isogeny-based cryptography which allows to provide safe and hidden communication of data over clouds. The main goal of the methodology is to enable the two users to freely share confidential information in a cloud infrastructure at the same time maintaining secrecy and defying against any new security threats. The framework uses isogeny based cryptography to create secure communication environments using the mathematical properties of elliptic curve isogenies. The method has high security assurances including the ability to withstand quantum computing and thus, increases the strength of transmission of data via the cloud. To complement this, there is the application of Spread Spectrum Image Steganography (SSIS) that involves embedding common secrets in digital images in a covert way. SSIS enhances the security of data through encryption, copying and interweaving the concealed data and coding it with pseudorandom noise sequences as vectors. Post embedding: This is followed by filtering of the stego-images in order to maintain the visual quality and to make them imperceptible. With the help of isogeny-based cryptography and spread spectrum steganography, the suggested framework allows a safe key exchange,

concealment of hidden messages, and safe communication and reduces the danger of untrusted intermediaries.

## 3. Integrated Hybrid Cryptographic and Steganographic Framework for Secure and Covert Image Transmission in Cloud Environments (IHCSF-CIT)

The suggested model deploys a multi-level security system in the storage and transfer of cloud images with hybrid cryptography, federated wavelet-based steganography, and post-quantum covert communication. The confidentiality and access control by use of the AES-OTP encryption with RSA-based key exchange, adaptive key management, time-limited access, and key rotation to control unauthorized access and insider threats. The second layer uses Wavelet-Based F-WCQMVD, which utilizes discrete wavelet transform, federated CNN learning and entropy-driven feature selection to guarantee imperceptibility, robustness and preserve high-frequency feature. Lastly, isogeny-based cryptography that includes spread spectrum steganography offers quantum-resistant, covert communication, guarantees confidentiality, integrity, access control, imperceptibility, and future-proof security, is more effective in image quality and computational performance measures, than traditional cryptographic and steganographic techniques.Fig.1 shows the comparative study.

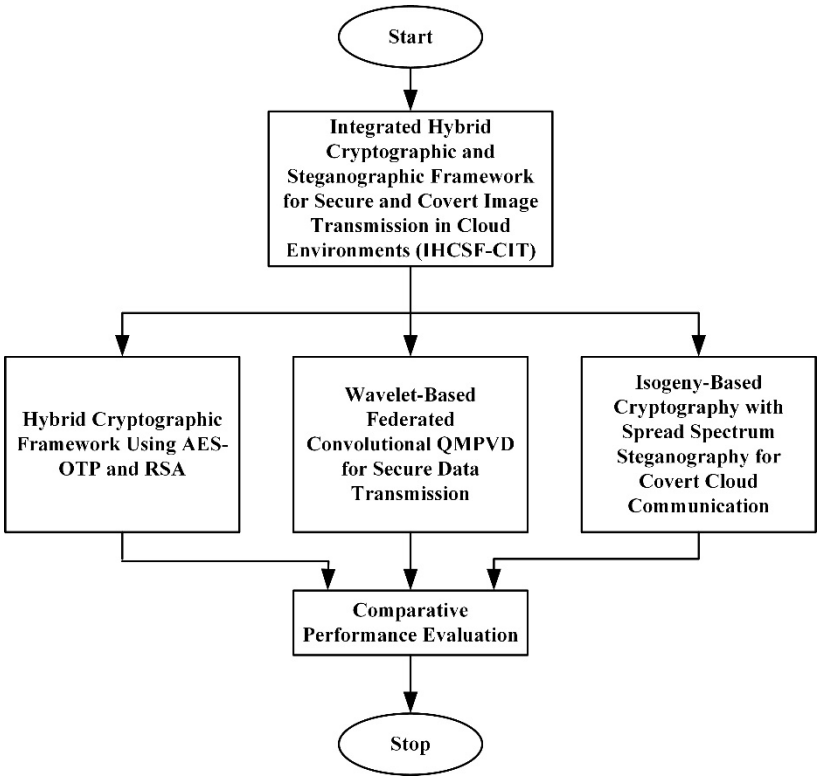


Fig.1. Comparative Study of IHCSF-CIT

### 3.1 Hybrid Cryptographic Framework Using AES-OTP and RSA

Cloud computing enhances accessibility and scalability of data, but contributes to the risk of breach and insider threat because the third party controls it. In this work, a hybrid cryptographic design that goes hand in hand with RSA key exchange, adaptive key management, time-limited access, and AES-OTP encryption is proposed to guarantee the secure, compliant, and dynamic data transfer in cloud-based settings.

#### 3.1.1 Data Collection

The suggested hybrid cryptographic system is tested on the real healthcare information to determine its efficiency in safeguarding confidential information, integrity, and secure access control to any information stored in the clouds or transmitted to high-risk settings[18].

### 3.1.2 Secure Key Exchange and Data Encryption Using AES-OTP and RSA

To secure cloud data storage and transmission, both AES and OTP are used that provide fast and highly randomized symmetric encryption with the help of AES and secure key exchange with the help of RSA. AES achieves block level encryption in several rounds of SubBytes, ShiftRows, MixColumns and AddRoundKey encryptions of a 4x4 state array. SubBytes operation is based on non-linearity with an S-box substitution as in the following eqn. (1):

$$SubBytes = \begin{bmatrix} 81 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{bmatrix} \quad (1)$$

The rows of the state matrix are cyclically shifted in order to promote diffusion in ShiftRows as shown in equation (2):

$$ShiftRows = \begin{bmatrix} 81 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{bmatrix} \quad (2)$$

MixColumns creates more confusion by multiplying each column by a constant matrix, as shown in the expression in the form of equation (3):

$$MixColumns = \begin{bmatrix} 205 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{bmatrix} \quad (3)$$

Lastly, the AddRoundKey is a process that mixes the round key with the state matrix using XOR as indicated in Eq. (4):

$$AddRoundKey = \begin{bmatrix} 112 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{bmatrix} \quad (4)$$

OTP provides another addition to security by XORing plaintext with a one-time key generated randomly, so that in the event of correct implementation cryptanalysis is infeasible. RSA ensures privacy, integrity, and authenticity of AES-OTP key by randomly assigning the key.

### 3.1.3 Adaptive Key Management and Time-Limited Access Control

Adaptive key management increases the cryptographic resilience with secure key generation using RSA algorithms and controlled distribution and periodic rotation of keys. Secure vaults or HSMs protect master keys, time-limited, role-based access control is used to protect data access with the use of timestamps and transparent access denial.

### 3.1.4 Logging, Auditing, and Anomaly Detection

The approval, denial, and all the access requests as well as key rotation events are recorded securely in order to provide traceability and regulatory compliance. Access logs are constantly monitored by anomaly detection mechanisms to detect suspicious access patterns or time-based policy violations to respond to security threats proactively.

### 3.2 Wavelet-Based Federated Convolutional QMPVD for Secure Data Transmission

The growth of access to multimedia in the IoT networks creates visibility and security issues to conventional cryptography and steganography. This paper has the opportunity to introduce EWFCQMPVD as an example of a steganographic system based on a deep learning method in the synthesis of a wavelet transformation, federated CNN computing and QMPVD. It enhances concealment, accessibility and non-perception of data with the compromised trade-off between quality, capacity and resistance to secured next-gen communication.

#### 3.2.1 Data Source

The suggested steganographic framework is tested on the 100,000 images of ImageNet dataset with 256x156 pixels. The half of images include secret data encrypted by Jsteg with the rest using the F5 algorithm with an embedding rate of 0.9 which makes 200,000 labelled cover and stego images in total. The data will be separated into training and testing sets to confirm the performance of steganalysis under the conditions of realistic transmission.

#### 3.2.2 Feature Extraction

DWT is used to extract texture-based features that are highly sensitive to horizontal, vertical, and diagonal sub-bands of high frequency to ensure that the hidden data is about to be detected. These sub-bands are analysed by federated CNN models each, resulting in a classification of 0.821, 0.799, and 0.815. Entropy-based feature selection is used to optimize the number of features extracted, which are approximately 3000, to increase the level of detection accuracy and decrease redundancy.

##### 3.2.2.1 Wavelet Transform-Based Feature Extraction

Wavelet transform separates a given input image I 0 into various frequency components at L levels. W and S refer to wavelet and scaling matrices respectively. Transformed components at level b of decomposition are as follows (5):

$$\begin{cases} I_{b+1}=SI_bS^T \\ I^h_{b+1}=WI_bS^T \\ I^v_{b+1}=SI_bW^T \\ I^{dv}_{b+1}=WI_bW^T \end{cases} \tag{5}$$

All the outputs are down-sampled and generate compact high-frequency representations.

##### 3.2.2.2 Federated CNN-Based Feature Extraction

Federated CNNs allow learning privacy-preserving on decentralized datasets $D_1, D_2, \ldots, D_3$. The gradient descent is applied to update model parameters locally in (6&7):

$$\theta_u^0 = \theta - \eta \nabla L_u(\theta) \tag{6}$$

$$\theta_u^t = \theta_u^{t-1} - \eta \nabla L_u(\theta_u^{t-1}) \tag{7}$$

Local updates are accumulated at the server to constitute a global model in (8):

$$\theta_{global}^t = Aggregate(\Delta\theta_1, \Delta\theta_2, \ldots, \Delta\theta_n) \tag{8}$$

Once convergence has been reached, the CNN obtains feature vectors in (9):

$$F(X) = \{f_u\} \tag{9}$$

The informative features are also retained in (10) using entropy based selection.

$$F_{final}(X) = \{f_u | G(f_u) \geq \text{threshold}\} \tag{10}$$

#### 3.2.3 Optimal Transient Homomorphic Encryption (OTHE)

OTHE can do computation on encrypted images without decryption. The public keys encrypt the image pixels, which are safely processed and stored in the cloud and the decryption is done with the help of authorized users, this makes the transmission and processing of the image pixels confidential.

**3.2.4 QMPVD-Based Steganographic Embedding**

The QMPVD algorithm inserts coded messages in pixel quotient - difference properties to produce high imperceptibility and steganalysis resistance stego-images assessed by MSE and PSNR to assess image quality and embedding distortion.

**3.3 Isogeny-Based Cryptography with Spread Spectrum Steganography for Covert Cloud Communication**

This paper combines isogeny-based cryptography and SSIS to overcome the quantum threat posed to cloud computing by quantum attacks. The hybrid strategy permits to communicate in a secure and peer-to-peer fashion without trusted intermediaries, even with untrusted cloud infrastructures. The isogeny-based encryption guarantees quantum resistant generation of key, and SSIS hides encrypted messages in noise-modulated pictures, resistant to the attack of traffic analysis and steganalysis.

**3.3.1 Isogeny-Based Cryptographic Model**

Isogeny-based cryptography uses the computational hardness of elliptic curve isogeny problems to provide security and these are computationally hard even when the adversary is a quantum computer. Let D be an elliptic curve and $H \subset D$be a subgroup. An isogeny $\phi: D \rightarrow D/H$ is a map of the curve to a quotient curve, which is the foundation of key generation and encryption. Rational mapping can be represented as (11):

$$(u', v') = \phi(u, v) = \left(\frac{\psi_{u'}(u,v)}{\eta_{u'}(u,v)}, \frac{\psi_{v'}(u,v)}{\eta_{v'}(u,v)}\right) \tag{11}$$

Here, $\psi$and $\eta$ are polynomials functions which determine the isogeny, and the order of subgroup H is the degree of $\phi$. The isogeny is the private key and the source and target curves are the public key. The security of this scheme is based on Supersingular Isogeny Path (SSIP) problem.

To handle computational complexity and maintain security the cryptosystem forms a chain of low degree isogenies with the use of a subgroup generated by point Q expressed in the form (12):

$$(O_D) \subset (S^{e-1}|Q) \subset (S^{e-2}|Q) \subset \cdots \subset \langle |s|Q \rangle \subset \langle Q \rangle = H \tag{12}$$

This subgroup structure which is hierarchical allows the high degree isogenies to be constructed efficiently without losing cryptographic strength.

**3.3.2 Secure Channel Establishment**

Elliptic curves and secret isogenies are created by each communicating user separately. The exchange of information on the public curves is used to create a secure channel where encrypted communication is done and no disclosure of the secret parameters is obtained. Through the Fiat-Shamir heuristic, interactive proofs are converted to non-interactive zero-knowledge ones to provide authentication and anonymity.

**3.3.3 SSIS**

Cover images with encrypted data are further generated using SSIS to increase confidentiality. The ciphertext is encoded using error-correcting codes, padded, interleaved and

modulated using pseudo-random noise and then added with an image. This creates a stego-image which is indistinguished visually with the original but it has been created in a way that hidden information is safely stored. The embedded data is extracted at the receiver through noise estimation and filtering after which it is decoded and decrypting is performed.

### 3.3.4 Security and Performance Considerations

Isogeny-based cryptography and SSIS used together provide quantum resistance, covert communication and resistance to interception, traffic analysis, and steganalysis. This is a hybrid mode that increases the protection of cloud data significantly without losing scalability and detections.

## 4. Results and Discussion

In this section, a comparative analysis of the three fundamental security elements of the proposed framework, namely, (i) Isogeny-Based Cryptography with Spread Spectrum Steganography (Isogeny-SSS), (ii) Wavelet-Based Federated Convolutional QMPVD, and (iii) AES-OTP-RSA Hybrid Cryptography is provided through benchmarking their performance against the traditional and recent state-of-the-art methods. The metrics compared include well known measures including PSNR, Structural Similarity Index (SSI), MSE, encryption and decryption time, accuracy and quantum-resistance capability. The findings show that there are obvious trade-offs between visual fidelity, computational efficiency, and security strength which allows evaluating the appropriateness of each method to be used in the context of secure image transmission in a cloud-based environment and proves the benefits of the combination of these two technologies in a single hybrid model.

### 4.1 Visual Quality and Steganographic Performance Comparison

Secure image transmission is determined by visual quality and imperceptibility, which have an effect on human perception and steganalysis resistance. In this section, the authors compare Isogeny-SSS, Wavelet-Based Federated Convolutional QMPVD, and AES-OTP-RSA based on a standard image quality parameter like PSNR, SSI, and MSE.

Table 1: Visual Quality Comparison of the Three Proposed Methods

| Method | PSNR (dB) | SSI | MSE |
|---|---|---|---|
| Isogeny-based SSS | 92.00 | 1.00 | – |
| Wavelet-Based Federated Convolutional QMPVD | 92.77 | – | $3.43 \times 10^{-5}$ |
| AES-OTP-RSA | – | – | 0.345 |

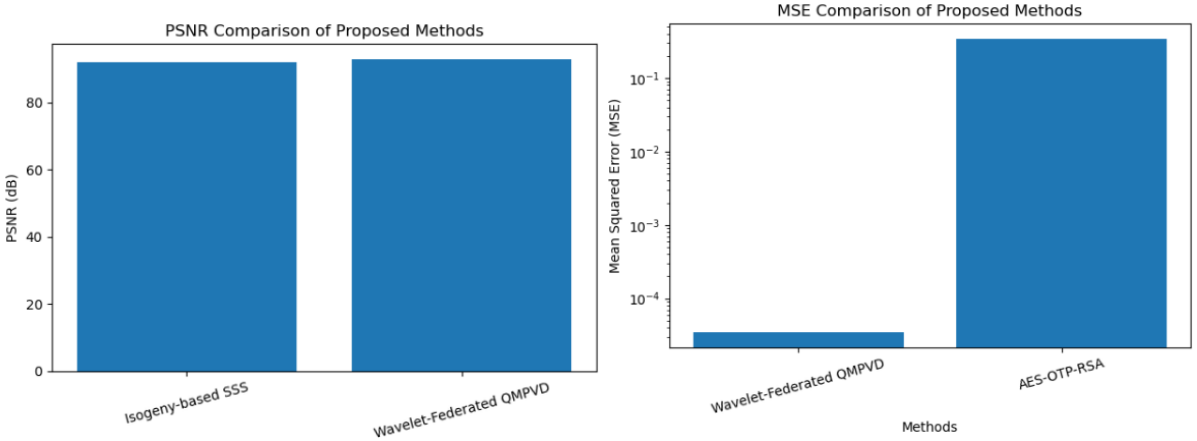

Fig. 2. PSNR, MSE Comparison of Methods

As seen in Table 1, the isogeny-based SSS algorithm produces a PSNR of 92 dB with an ideal SSI of 1.0, which translates to almost lossless reconstruction and great significance of structural content between the original image and stego image. The reason behind this good visual performance has primarily been because of the application of the spread spectrum steganography in which the encrypted payload is more or less spread among the noise elements such that there is no significant perceptual distortion. The best PSNR of 92.77 dB and the worst MSE of 3.43 × 10 -5 demonstrate that the Wavelet-Based Federated Convolutional QMPVD algorithm yields better pixel level fidelity. It is very effective because it combines discrete wavelet transform and federated CNN-based feature extraction, which retains the high-frequency information and entraps encrypted information in a safe place. Conversely, AES-OTP-RSA hybrid algorithm emphasizes on cryptographic security and transmission efficiency over visual disguise, which causes a relatively high value of MSE.

Table 2: Comparison with Existing Steganographic and Encryption-Based Methods

| Method | PSNR (dB) | MSE |
|---|---|---|
| Isogeny-based SSS | 92.00 | – |
| Wavelet-Based Federated Convolutional QMPVD | 92.77 | $3.43 \times 10^{-5}$ |
| DWT-ECC | 82.75 | 0.0012 |
| PSO-BWT | 50.00 | 0.01 |
| DCT-GAN Hybrid | 62.29 | – |
| Resen-Hi-Net | 40.13 | – |
| AES | 74.00 | – |
| RSA | 40.00 | – |

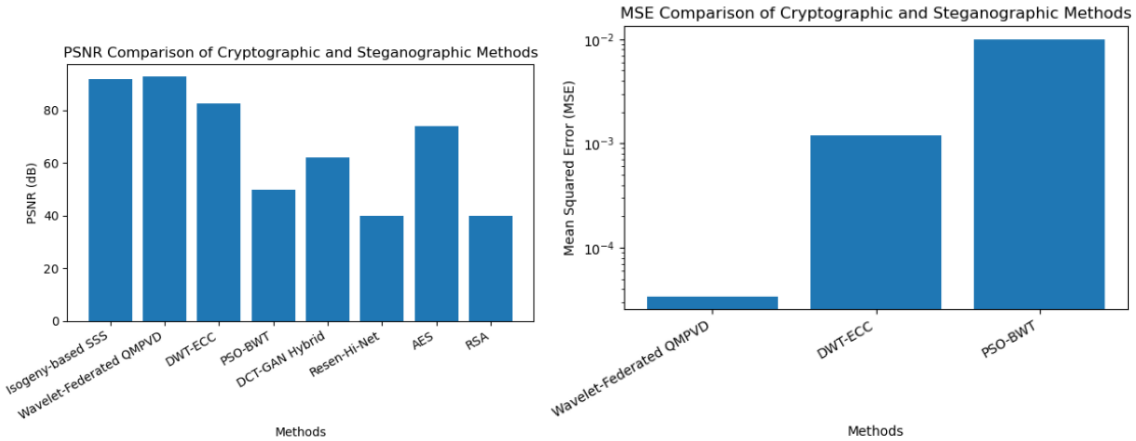


Fig. 3. Comparison of Cryptographic and Steganographic Methods

Table 2 demonstrates that the Isogeny-based SSS and Wavelet-Based Federated Convolutional QMPVD approaches easily surpass the classical cryptographic schemes like AES and RSA, and recent deep learning-based steganography models like DCT-GAN Hybrid and Resen-Hi-Net. Traditional encryption does not employ steganographic embedding which in turn leads to a poor PSNR and poor visual quality. Conversely, the suggested techniques incorporate encrypted information in noise of the image or transform-domain coefficients,

which maintains the image quality almost lossless, hardly visible, and covert communication in the cloud.

### 4.2 Computational Efficiency and Latency Analysis

The security of a transmission of images in cloud and IoT settings requires computational efficiency and latency. This section provides a comparison of the execution time, computation overhead and latency of transmission of Isogeny-SSS, Wavelet-Based Federated Convolutional QMPVD and AES-OTP-RSA hybrid in terms of encryption, decryption and latency.

Table 3: Encryption and Decryption Time Comparison of Proposed Methods

| Method | Encryption Time (s) | Decryption Time (s) |
|---|---|---|
| AES-OTP-RSA | 0.00062 | 0.01 |
| Isogeny-based SSS | 2.133 | 0.513 |
| Wavelet-Based Federated Convolutional QMPVD | – | – |

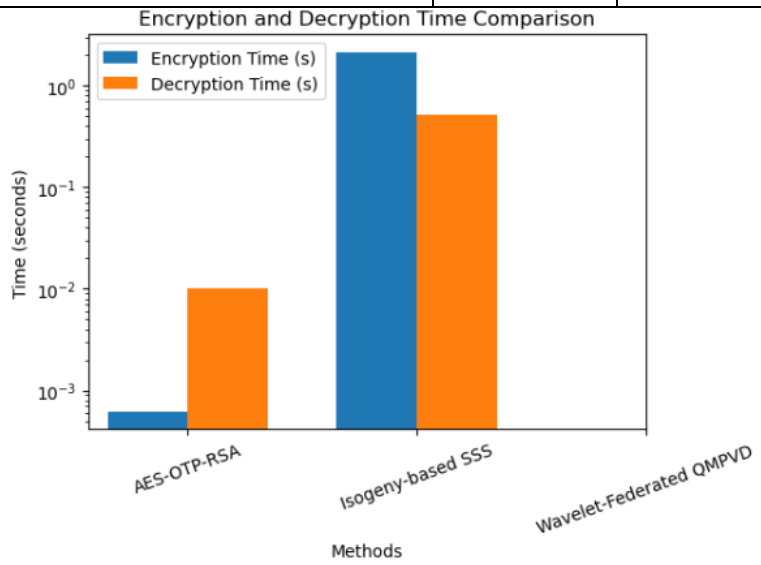


Fig. 4. Comparison of Encryption and Decryption Time

Table 3 demonstrates that the AES-OTP-RSA hybrid cryptographic scheme has the shortest encryption and decryption time, an encryption time of 0.00062 s and a decryption time of 0.01 s. This is highly efficient attributed by the fact that its data protection is done using symmetric AES-OTP, whereas RSA is used in the exchange of secure keys only. Consequently, the scheme is highly applicable in the real-time, latency-sensitive, and high-throughput cloud applications. Comparatively, the SSS with isogeny is recorded encryption time of 2.133s and a decryption time of 0.513s which is a further overhead in computation due to the elliptic-curve isogeny operations coupled with steganographic modulation but is still reasonable as a quantum-resistant cloud communication. Wavelet-Based Federated Convolutional QMPVD will also focus on image quality and safe embedding mainly because of the wavelet decomposition and federated CNN inference, which bring about higher computational costs, and thus not applicable in strict real-time situations.

Table 4: Comparison with Existing High-Overhead Methods

| Method | Encryption Time (s) | Decryption Time (s) |
|---|---|---|
| DCT-GAN Hybrid | – | – |
| Resen-Hi-Net | – | – |
| ECC-Blowfish | 2.483 | 2.973 |
| TKSE | 2.9 | 3.070 |

DCT-GAN Hybrid and Resen-Hi-Net have high computational power to be scientifically trained and inferred, which restricts the scalability in the cloud. Likewise, ECC-Blowfish and TKSE have longer encryption and decryption time and therefore are not so applicable to latency-sensitive applications as AES-OTP-RSA.

Table 5: Latency Analysis of Security Mechanisms

| Method | Effective Latency Level | Suitability for Cloud / IoT |
|---|---|---|
| AES-OTP-RSA | Very Low | Excellent (Real-time) |
| Isogeny-based SSS | Moderate | High (Quantum-secure) |
| Wavelet-Based Federated Convolutional QMPVD | High (Model Inference Overhead) | Medium (Non-real-time) |

Table 5 reveals that there is an apparent security-performance trade-off between the methods tested. The AES-OTP-RSA scheme has the minimised latency thus it is very suitable in real-time and latency sensitive cloud applications where the speed in which encryption and decryption is needed is important. Conversely, the isogeny-based SSS solution provides a balanced and future-compatible solution by providing a high-quality quantum-resistant security at a moderate and acceptable calculation-level. Even though deep learning-driven approaches prove to have the best data concealment and high imperceptibility, at the cost of much higher latency and computational complexity, they cannot be scaled to real-time operation. Altogether, the suggested hybrid framework is a decent and feasible option to secure image transportation within the current cloud and IoT system due to its balanced approach towards computational performance, latency, and security.

**4.3 Security Strength and Quantum Resistance Comparison**

The three key components compared in terms of security strength (Isogeny-based SSS, AES-OTP-RSA and Wavelet-based Federated Convolutional QMPVD) are analysed comparatively as per key size, resistance to cryptographic attacks and resistance to quantum adversaries. The size of key and the level of security association, where it is evident that the isogeny based cryptography beats any other cryptographic technique in terms of providing high level of security at the minimal key size in table 6.

Table 6: Comparison of Security Strength and Quantum Resistance

| Method | Underlying Security Principle | Key Size for ~256-bit Security | Quantum Resistance | Security Characteristics |
|---|---|---|---|---|
| Isogeny-based SSS | Elliptic curve isogeny hardness (SSIP problem) | 832 bits | Yes (Post-Quantum) | Strong cryptographic security, compact keys, resistant to Shor's algorithm, covert transmission via SSIS |
| AES-OTP-RSA | Symmetric + asymmetric layered encryption | RSA ≈ 15,360 bits | No | High classical security, adaptive key rotation, time-limited access, vulnerable to quantum attacks |
| Wavelet-based Fed-CNN QMPVD | Steganographic concealment + ML detection resistance | Not key-dependent | No | Improves imperceptibility and steganalysis resistance, does not protect against cryptographic attacks |

The security of isogeny-based cryptography is equal or greater than that of classical cryptography (RSA and ECC) with much smaller key sizes. RSA needs keys of size bigger than 15 kbits in order to reach 256-bit security, whereas the isogeny-based algorithm achieves this with 832 bits, much smaller, and making it extremely efficient and suitable to a bandwidth-limited cloud environment. Despite the fact that the AES-OTP-RSA hybrid is not quantum-resistant, the provided method protects against classical attacks and insider threats by applying multilayer encryption, adaptive key management, and time-bound access control. The federated convolutional wavelet approach increases indirectly the security through the increase of the steganalysis and image detection resistance. In general, the architecture provides a secure and well-rounded, and future-oriented security architecture of next-generation cloud systems.

**4.4 Overall Comparative Summary of the Methods**

Table 7 provides general comparison summarises the advantages and disadvantages of the three fundamental security mechanisms that have been combined into the hybrid structure: Isogeny-based SSS, Wavelet-Based Federated Convolutional QMPVD and AES-OTP-RSA Hybrid Cryptography. The methods solve different aspects of security quantum resistance, steganographic imperceptibility and real-time cloud efficiency hence complementary to each other.

Table 7: Overall Comparative Summary of the Three Methods

| Method | Key Strength | Best Metrics Achieved | Limitation |
|---|---|---|---|
| Isogeny-based SSS | Quantum-resistant encryption with covert communication via SSIS | PSNR = 92 dB, SSI = 1.0, compact key size (832-bit for 256-bit security) | Moderate computational overhead compared to symmetric schemes |

| | | | |
|---|---|---|---|
| Wavelet-Based Federated Convolutional QMPVD | High imperceptibility and strong resistance to steganalysis using DWT and federated CNNs | PSNR = 92.77 dB, MSE = $3.43 \times 10^{-5}$ | High training and computational complexity due to deep learning |
| AES-OTP-RSA | Fast, scalable, and highly accurate cloud encryption with adaptive key management | Accuracy = 99.12%, lowest encryption/decryption latency (0.00062 s / 0.01 s) | Not resistant to quantum attacks |

The isogeny-based SSS approach offers future security against quantum adversaries, as well as, high-security of cryptography, high image quality and covert communication. Wavelet-Federated QMPVD model is good at maintaining the visual quality and steganalysis resistant, thus suitable to transmit multimedia, but training and computer cost is high. Alternatively, AES-OTP-RSA has a better speed, precision and scalability and hence it is applicable in real-time cloud application although it is not post-quantum secure. The combination of these complementary methods further facilitates a balanced and effective cloud and IoT infrastructure to transmit image data in security.

**4.5 Discussion**

The experimental findings and the comparison allow concluding that the suggested hybrid cryptographic solution is relevant to balance the security level, the efficiency of the computation, and the imperceptibility of the visual images in the clouds to transmit images securely. The SSS component is isogenous and provides robust security in post-quantum with small key sizes, and the spread spectrum steganography is spread spectrum and allows covert communication with high PSNR, at a moderate increase in the computational overhead. Conversely, the Wavelet-Based Federated Convolutional QMPVD approach performs well in terms of image quality preservation and steganalysis resistance, which is demonstrated by the smallest values of MSE and high PSNR; but, the method has high training and processing complexity because it is based on deep learning algorithms. The AES-OTP-RSA hybrid cryptography scheme is significantly faster to execute, more accurate and has lower latency compared to other cryptography schemes, which is why it is especially appropriate to those real-time cloud and IoT solutions that require fast turnaround and time-constrained access control, although it is not inherently quantum-resistant. All the findings collectively check and confirm that none of the modern threats to cloud security can be completely tackled by one technique, yet their combination as the part of the suggested framework can substantially reduce classical, steganalytic, and new quantum threats. This hybrid solution is a scalable, flexible and future-proof solution to secure cloud-based transmission of images.

**5. Conclusion and Future Works**

This paper will conduct a detailed comparative analysis of a hybrid cryptographic scheme of a secure image transmission in cloud-based applications that will deal with key issues regarding the confidentiality, integrity, imperceptibility, and arising quantum threats. The

framework is based on layered and resilient security architecture with the combination of three complimentary mechanisms: AES-OTP-RSA hybrid cryptography, Wavelet-Based Federated Convolutional QMPVD steganography, and Isogeny-Based Cryptography with Spread Spectrum Steganography. Experimental findings reveal that AES-OTP-RSA component has high accuracy, extremely low latency, and high resistance to classical attacks, hence it is highly applicable to real-time and latency-sensitive clouds. The Wavelet-Based Federated Convolutional QMPVD is very good in maintaining image quality and steganalysis resistance, making it distort very little with high visual fidelity. Above all the Isogeny-based SSS element offers post-quantum security with small key sizes and secret communication, and is long-term resilient against quantum-enabled assailants. Comparative analysis- The proposed framework is always superior to conventional single-layer cryptographic and steganographic methods in important parameters like PSNR, SSI, MSE, accuracy and computing performance. In general, the results prove that the hybrid and multi-layered security strategy is vital to secure, scalable, and future-resistant image transmission over the current cloud environments.

Although it has performed well, there are a number of ways through which this research can be extended. It can be hoped that future work can concentrate on optimizing the computational complexity of the isogeny-based cryptographic operations to lower the latency and increase the scale of the large-scale cloud deployment. Wavelet-Based Federated Convolutional model can be further extended with lightweight or transformer-based architectures to minimize their training costs and get high detection rates. Moreover, the framework can be tested with more diverse and larger real-time data, such as video feeds and high resolution medical images, to determine resilience to dynamic network settings. Key protection may also be enhanced by integrating with secure hardware environments like Trusted Execution Environments (TEEs) and Hardware Security Modules (HSMs). Lastly, the discussion of the proposed framework being interoperable with future post-quantum cryptographic standards and edge–cloud architectures will aid in ensuring that this framework can find its use in future cloud, IoT, and smart healthcare ecosystems.

**References**

[1] A. Sen, S.-H. Heng, and S.-C. Tan, “A comprehensive Review of Cryptographic Techniques in Federated Learning for Secure Data Sharing and Applications.,” *IEEE Access*, 2025.

[2] A. Mondal and P. S. Chatterjee, “Cloudsec: A lightweight and agile approach to secure medical image transmission in the cloud computing environment,” *SN Computer Science*, vol. 5, no. 2, p. 237, 2024.

[3] P. Selvi and S. Sakthivel, “A hybrid ECC-AES encryption framework for secure and efficient cloud-based data protection,” *Scientific Reports*, vol. 15, no. 1, p. 30867, 2025.

[4] M. Y. Shakor, N. M. S. Surameery, and Z. N. Khlaif, “Hybrid security model for medical image protection in cloud,” *Diyala Journal of Engineering Sciences*, pp. 68–77, 2023.

[5] A. Abdo, T. S. Karamany, and A. Yakoub, “A hybrid approach to secure and compress data streams in cloud computing environment,” *Journal of King Saud University-Computer and Information Sciences*, vol. 36, no. 3, p. 101999, 2024.

[6] G. A. Nwatuzie, L. A. Enyejo, and C. Umeaku, “Enhancing Cloud Data Security Using a Hybrid Encryption Framework Integrating AES, DES, and RC6 with File Splitting and

Steganographic Key Management," *International Journal of Innovative Science and Research Technology*, vol. 10, no. 1, 2025.
[7] R. R. Irshad *et al.*, "IoT-enabled secure and scalable cloud architecture for multi-user systems: A hybrid post-quantum cryptographic and blockchain-based approach toward a trustworthy cloud computing," *IEEE Access*, vol. 11, pp. 105479–105498, 2023.
[8] A. Gour, S. S. Malhi, G. Singh, and G. Kaur, "Hybrid cryptographic approach: for secure data communication using block cipher techniques," in *E3S Web of Conferences*, EDP Sciences, 2024, p. 01048.
[9] M. K. Abiodun, A. L. Imoize, J. B. Awotunde, A. E. Adeniyi, U. Chioma, and others, "Analysis of a Double-stage Encryption Scheme Using Hybrid Cryptography to Enhance Data Security in Cloud Computing Systems.," *Journal of Library & Information Studies*, vol. 21, no. 2, 2023.
[10] K. K. Singamaneni, A. K. Budati, S. Islam, R. Kolandaisamy, and G. Muhammad, "A novel hybrid quantum-crypto standard to enhance security and resilience in 6G enabled IoT networks," *IEEE Journal of Selected Topics in Applied Earth Observations and Remote Sensing*, 2025.
[11] Z. A. Mohammed, H. Q. Gheni, Z. J. Hussein, and A. K. M. Al-Qurabat, "Advancing cloud image security via AES algorithm enhancement techniques," *Engineering, Technology & Applied Science Research*, vol. 14, no. 1, pp. 12694–12701, 2024.
[12] A. Manivannan, G. Venkateswaran, D. Menaga, S. Sivakumar, M. H. Kumar, and M. S. Jacob, "Privacy-Preserving Image Storage on Cloud Using An Unified Cryptographic Authentication Scheme," *Salud, Ciencia y Tecnología-Serie de Conferencias*, vol. 3, p. 609, 2024.
[13] A. Shafique *et al.*, "A hybrid encryption framework leveraging quantum and classical cryptography for secure transmission of medical images in IoT-based telemedicine networks," *Scientific Reports*, vol. 14, no. 1, p. 31054, 2024.
[14] S. Pothireddy, N. Peddisetty, P. Yellamma, G. Botta, and K. N. Gottipati, "Data Security in Cloud Environment by Using Hybrid Encryption Technique: A Comprehensive Study on Enhancing Confidentiality and Reliability.," *International Journal of Intelligent Engineering & Systems*, vol. 17, no. 2, 2024.
[15] D. Shivaramakrishna and M. Nagaratna, "A novel hybrid cryptographic framework for secure data storage in cloud computing: Integrating AES-OTP and RSA with adaptive key management and Time-Limited access control," *Alexandria Engineering Journal*, vol. 84, pp. 275–284, 2023.
[16] D. Shivaramakrishna and M. Nagaratna, "An Extended Wavelet Based Federated Convolutional Quotient Multipixel Value Differencing for Secured Data Transmission Outline," *Wireless Personal Communications*, pp. 1–20, 2024.
[17] D. Shivaramakrishna and M. Nagaratna, "Enhancing Data Protection and Covert Communication in Cloud Environments with Isogeny-based Cryptography and Spread Spectrum Steganography," 2025.
[18] S. Armoogum and P. Khonje, "Healthcare data storage options using cloud," *The Fusion of internet of things, artificial intelligence, and cloud computing in health care*, pp. 25–46, 2021.