Optimization Of secure and Efficient Encrypt Image Retrieval Based on Additive Sharing Using SMPC

Mrs. Banuppriya P[1], Alamelumangai P[2], Minitha Sri M[3], Swetha V[4], Abirami A[5]
[1]Assist prof, Dept of Computer science and Engineering
[2, 3, 4, 5] Dept of Computer science and Engineering
[1, 2, 3, 4, 5] Mahendra Institute of Engineering and Technology, Namakkal, Tamil Nadu, India

Abstract- *Due to growing threats of data interception and illegal access, secure digital image transmission over open networks continues to be a major concern. By combining Elliptic Curve Cryptography (ECC), visual cryptography, and Least Significant Bit (LSB)-based steganography, this article offers a strong framework for safe multi-image transmission. Strong encryption with a smaller key size and less computational cost is provided by ECC, guaranteeing effective and safe key management. Visual cryptography is used to further process the encrypted images, breaking each one up into several pieces that don't independently give any useful information. LSB steganography is used to embed these files inside cover images in order to improve confidentiality. This effectively hides the existence of sensitive data during transmission. The original images are recovered with high fidelity at the receiving end by extracting the embedded shares, reconstructing them using visual cryptography, and decrypting them using ECC. Improved Peak Signal-toNoise Ratio (PSNR) data show that the suggested method achieves high reconstruction accuracy, minimum visual distortion, and superior security. Strong defense against statistical analysis, cryptographic attacks, and illegal access is offered by the multi-layered security system. All things considered, the suggested system provides a scalable, effective, and extremely secure multi-image transmission solution, making it appropriate for use in defense systems, medical imaging, and secure communications.*

Keywords: Elliptic Curve Cryptography (ECC), Visual Cryptography, LSB Steganography, Multi-Image Transmission, Image Security

I. INTRODUCTION

The need for secure data transmission methods has grown dramatically due to the rapid development of digital communication technologies and the extensive use of multimedia data. Digital images are one of the many data types that are utilized extensively in vital applications like surveillance systems, military communication, medical diagnostics, and the exchange of private information.

However, sending pictures across unprotected and open networks leaves them vulnerable to a number of security risks, such as identity theft, data manipulation, interception, and illegal access. Thus, it has become a significant research challenge to ensure the secrecy, integrity, and validity of such sensitive visual data. To safeguard sensitive data, traditional security methods mostly rely on cryptography techniques. Although these techniques successfully transform unencrypted data into encrypted formats, they frequently expose private information, leaving them vulnerable to targeted attacks and cryptanalysis. Furthermore, performance may be impacted by older encryption methods' need for larger key sizes and more processing power, particularly in real-time and resource-constrained settings. Because of this, there is an increasing demand for stronger and more effective security systems that can overcome these constraints. Hybrid security models that integrate several strategies have drawn a lot of interest as a solution to these problems. Visual cryptography offers safe image sharing by splitting photos into many shares, steganography hides the existence of information, and cryptography guarantees data confidentiality. By combining these methods, multilayered security is made possible, which significantly increases the difficulty of system compromise for attackers. These methods not only strengthen defense but also increase resistance to many types of attacks, such as statistical, steganalysis, and brute-force attacks. Because Elliptic Curve Cryptography (ECC) can provide robust security with smaller key sizes than more conventional techniques like RSA, it has become a very effective publickey cryptographic technology. Because of its decreased computing complexity, quicker processing, and lower power consumption, ECC is a great fit for contemporary communication systems. By dividing an image into several parts, each of which does not independently expose any significant information, visual cryptography further enhances security. The original image can only be recreated if the necessary number of shares have been joined, guaranteeing safe transfer and restricted access. Furthermore, steganography based on the Least Significant Bit (LSB) is a popular technique for incorporating secret information into digital photographs without noticeably altering their appearance. Secret information can be concealed within a cover image by altering the least important pixel values,

giving the impression to outside observers that the communication is innocuous. By lowering the possibility of detection during transmission, this method improves the stealth component of data communication. Many current systems are constrained by single-layer security methods or are made to transmit a single image at a time, notwithstanding the benefits of these particular solutions. These restrictions decrease their usefulness in practical situations where it is necessary to securely and effectively send several critical photos at once. Furthermore, if any one layer is compromised, standalone techniques can still be susceptible to sophisticated attacks. This research suggests a safe multiimage transmission system that combines visual cryptography, LSB-assisted steganography, and ECCbased encryption to close these gaps. To guarantee confidentiality, the suggested approach first encrypts many secret images using ECC. In order to prevent partial data exposure from compromising the original information, the encrypted images are subsequently split into numerous shares using visual cryptography. LSB steganography is then used to embed these shares inside cover images, so hiding the existence of secret data while it is being transmitted. In order to get the original photos with great precision, the receiver extracts the concealed shares, combines them to reconstruct the encrypted images, and then uses ECC to decrypt them. Enhanced security, effective key management, increased resilience to attacks, and support for multi-image transmission are just a few benefits of the suggested multi-layered method. The system guarantees a high degree of confidentiality, integrity, and stealth by integrating encryption, data concealing, and secure sharing protocols. ECC also lowers computational cost, which makes the framework appropriate for large-scale and real-time applications.

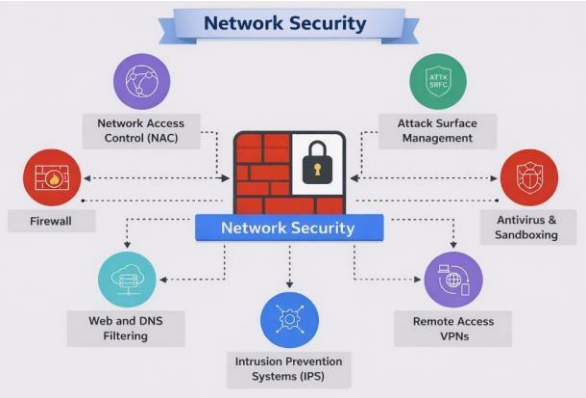

FIG 1: Basic Security system

The diagram shows in figure 1 and describes as network security framework where multiple components work together to protect a system. A firewall acts as the central defense, controlling network traffic, while Network Access Control (NAC) restricts access to authorized users. Additional layers such as Intrusion Prevention Systems (IPS), Antivirus and Sandboxing, Web and DNS Filtering, and Remote Access VPNs help detect threats, block malicious activity, and ensure secure communication. Overall, it represents a layered security approach that strengthens protection against cyber threats.

II. RELATED WORK

A reliable and scalable architecture for safe authentication and data sharing in cloud-enabled big data contexts was introduced by Uma Narayanan, Varghese Paul, et al. [1]. To prevent unauthorized users from accessing sensitive data, the suggested system incorporates several security layers, such as robust user authentication, encryption methods, and fine-grained access control. It guarantees data availability, secrecy, and integrity across dispersed systems. Large-scale data can be handled effectively and securely thanks to the design. It also reduces vulnerabilities in cloud platforms by incorporating mechanisms to monitor and control possible security threats. In order to increase system performance and efficiency, the authors also discuss real-world implementation issues and offer optimized solutions. The framework is made to safely support real-time applications and enable dependable data sharing across numerous users. All things considered, the method greatly improves efficiency, security, and confidence in cloud-based large data systems.

An extensive evaluation of safe data sharing and storage methods in cloud contexts was given by Ishu Gupta et al. [2], with an emphasis on safeguarding private data from new dangers. The paper assesses several cryptographic techniques, such as symmetric, asymmetric, and hybrid encryption techniques, emphasizing their advantages and disadvantages in diverse contexts. It also examines the complexity of key management, highlighting the necessity of effective and safe key distribution systems. In order to guarantee that only authorized users can access cloud data, the article also examines authentication methods and access control mechanisms. The authors point out serious security flaws in current cloud storage systems, including data loss, insider risks, and privacy issues. The study also covers the importance of strong communication protocols in preserving data integrity during transmission and safe data sharing among numerous users. It also looks at future trends, recommending better storage designs and the use of sophisticated encryption standards. All things considered, the report provides insightful analysis and useful suggestions to improve cloud security and fortify data protection tactics.

An improved safe authentication method that combines machine learning and cryptography for federated

cloud settings was proposed by Ashutosh Kumar Singh et al. [3]. Strong encryption techniques are used by the system to safeguard data while it is being transmitted, and machine learning algorithms improve the accuracy of authentication by recognizing trends and spotting unusual or unauthorized access attempts. It tackles the difficulties of distributed computing by facilitating safe communication and smooth data sharing across many cloud platforms. The strategy strengthens defense against insider threats, cyberattacks, and data breaches by utilizing multi-layer security measures. Furthermore, the system's scalability makes it appropriate for large-scale settings with numerous users. The authors point out the shortcomings of conventional authentication systems and suggest clever, flexible solutions. Incorporating machine learning enhances security while optimizing system response time and performance. Results from experiments show that authentication procedures are more dependable and effective. All things considered, the suggested paradigm greatly improves data protection, security, and trust in federated cloud systems.

By combining blockchain technology with IPFS, Smita Athanere, Ramesh Thakur, et al. [4] presented a semi-decentralized architecture for secure data exchange. IPFS offers distributed storage for effective and scalable data retrieval, while blockchain technology guarantees data immutability and tamper resistance. It improves system availability, fault tolerance, and dependability by removing a significant reliance on centralized servers. To effectively manage data in dispersed contexts, the design uses a hierarchical paradigm. Only authorized users can access sensitive data thanks to the automation and enforcement of fine-grained access control provided by smart contracts. By keeping a reliable record of every transaction, the method improves user confidence and transparency. It also offers optimum solutions for issues like network efficiency, scalability, and storage overhead. The technology lowers the possibility of unwanted changes, facilitates safe and transparent data transmission, and enhances overall performance. All things considered, the suggested approach provides a reliable, scalable, and effective decentralized solution for safe data sharing and storage in contemporary distributed systems.

A thorough analysis of safe data deduplication methods in cloud storage systems was provided by Priteshkumar Prajapati et al. [5], with a focus on data security and storage effectiveness. According to the report, deduplication reduces duplicate data to maximize storage use, but it also presents serious security issues, especially with regard to data privacy and confidentiality. The authors look at encryption-based deduplication techniques, such as convergent encryption, and emphasize how crucial strong key management techniques are to preventing abuse. Analysis is done on client-side and server-side deduplication techniques, emphasizing their benefits and possible drawbacks. Critical threats like data leakage, illegal data access, and inference assaults are identified by the research. Additionally, it examines different cryptographic techniques intended to improve secure deduplication without sacrificing system efficiency. The study also addresses the trade-off between security and efficiency, offering optimum methods to strike a balance. The authors suggest enhancements to bolster current models and tackle new issues in cloud systems. All things considered, the study offers thorough insights and useful suggestions for creating safe, effective, and scalable cloud storage systems.

A thorough framework for safe health data exchange in a mobile cloud-based e-health system was provided by Chinnasamy, P., et al. [6]. The suggested approach responds to the increasing demand for security and privacy in healthcare data management, especially in cloud environments where private patient data is susceptible to breaches and illegal access. The system guarantees tamper-proof storage and transparent data exchanges by utilizing blockchain technology, which improves responsibility and trust among healthcare stakeholders. Because they automate access control procedures and enable safe data exchanges, smart contracts are essential to the system. Health records can only be accessed or changed by authorized individuals, which lowers the possibility of privacy infractions and guarantees adherence to data protection laws. To prevent eavesdropping, leakage, and unwanted modification, the framework uses sophisticated encryption algorithms to protect data during transmission and storage. The study also looks at issues including scalability, network latency, and integration with current hospital IT infrastructures that are related to practical deployment. The suggested strategy guarantees a balance between usability, security, and performance by resolving these issues. Additionally, by eliminating data loss, unauthorized change, and duplication, the system improves robustness and dependability in data sharing.

A safe and energy-efficient framework based on Visual Cryptography (VC) was suggested by Ren, Lijing et al. [7] to improve communication security and privacy, especially in contexts with limited energy. The increased usage of small, light devices that operate over open, public networks presents serious issues for image sharing in the Internet of Things (IoT) era. Strict power and resource constraints frequently prevent these devices from supporting sophisticated cryptographic algorithms, increasing their susceptibility to security risks and data leaks. The authors developed a secret-sharing-based data

forwarding and sharing paradigm to solve these problems, allowing for the real-time transmission of massive amounts of sensitive data from Internet of Things devices. In order to minimize the amount of encrypted images while preserving excellent decryption quality, they also suggested a down sampling-based non-expansive Visual Cryptography Scheme (VCS). The suggested framework ensures efficiency and security by achieving recognition performance on encrypted data that is comparable to that of unencrypted data, according to experimental results on standard test photos.

Using the Triple Data Encryption Standard (3DES), Ramachandra, Mohan Naik, et al. [8] proposed a safe massive data storage method for cloud environments. The study focuses on safeguarding massive information from potential breaches, cyberthreats, and illegal access— all of which are major issues in cloud computing. To provide strong security and protect data confidentiality during transmission and storage, the suggested system uses several encryption levels. The framework is made to effectively manage enormous amounts of data while upholding strict security standards. The system strengthens defenses against brute-force attacks and other prevalent cryptographic vulnerabilities by including 3DES. In order to guarantee that authorized individuals can access information without jeopardizing security, the research also places a strong emphasis on secure data retrieval procedures. The method is more effective than traditional single-encryption procedures since it uses improved encryption techniques to boost performance.

A variety of security methods for safeguarding data in cloud computing systems were investigated by Shorahimov, Asadbek, et al. [9]. The study emphasizes how crucial it is to protect private data kept in cloud infrastructures against cyberattacks, illegal access, and possible data breaches. The authors examine a variety of security measures, including as authentication methods, encryption algorithms, and access control techniques, highlighting their functions in preserving the availability, confidentiality, and integrity of data. The study examines several security models used in cloud systems, pointing out weaknesses and possible dangers present in multi-tenant cloud designs. It emphasizes how important it is to use robust authentication procedures and strong encryption techniques to stop unwanted data access. Complementary security measures including firewalls, intrusion detection systems (IDS), and monitoring tools that aid in identifying and reducing cyberthreats are also covered in the study.

Key security concerns and challenges in cloud computing technologies were examined by Arunkumar et al. [10], with an emphasis on vulnerabilities associated with cloud-based data processing, storage, and transmission. The study highlights the need to put strong security measures in place to safeguard sensitive company data by identifying main dangers such data breaches, unauthorized access, data loss, and service outages. The study looks at vulnerabilities in three different cloud service models: Software as a Service (SaaS), Platform as a Service (PaaS), and Infrastructure as a Service (IaaS). It also assesses how each model poses different security risks. As crucial elements of cloud security, the study emphasizes the significance of robust encryption, authentication procedures, and access control systems. It also covers the crucial role that regulatory frameworks, industry standards compliance, and security policies play in preserving a safe cloud infrastructure. The study also points out weaknesses in current cloud security solutions, including low user knowledge, uneven security protocol implementation, and difficulties controlling threats in diverse cloud environments. To strengthen protection, the authors suggest enhancements such as risk management frameworks, multi-layered security measures, and ongoing monitoring. The need of user knowledge and education in lowering human-related vulnerabilities is emphasized.

III. EXISTING WORK OF THE STUDY

The main purpose of current visual cryptography (VC) systems is to secure images by splitting them into several parts, each of which seems like random noise and doesn't disclose any useful information on its own. The majority of conventional VC systems are restricted to binary images, which limits their applicability in contemporary applications demanding colored or high-resolution image processing, even though they are successful for basic image security. This restriction makes them less useful in practical applications like secure document sharing, medical imaging, military communications, and multimedia content security. Many traditional methods employ k-out-of-n reconstruction procedures, which enable the recovery of the secret image even in situations when only a portion of the shares are available. Although this increases availability, it also poses serious security problems because sensitive data may still be reconstructed by unauthorized users who have partial shares.

Additionally, when several secret images need to be safely transmitted over networks, the majority of current systems are built for single-image transmission, which limits efficiency. The absence of robust encryption techniques to safeguard shares during transmission is a significant flaw in the present systems. Many methods leave shares open to interception, manipulation, and other cyberattacks since they do not incorporate sophisticated encryption algorithms, data concealment, or steganography. The lack of these security layers emphasizes the need for stronger solutions that integrate

visual cryptography with contemporary cryptographic techniques like Elliptic Curve Cryptography (ECC), which can improve integrity, secrecy, and attack resistance. A new generation of VC systems that can handle colored and high-resolution images, provide secure multi-image transmission, and incorporate robust encryption and data-hiding algorithms are needed to overcome these constraints. These developments would greatly improve visual cryptography's security, effectiveness, and suitability in delicate fields.

IV. PROPOSED METHODOLOGIES

By combining Visual Cryptography, Elliptic Curve Cryptography (ECC), and Least Significant Bit (LSB) steganography, the proposed method offers a very safe framework for picture communication. This method ensures that sensitive information is concealed within the image itself by first embedding the secret image with private text using the LSB technique. An n-out-of-n visual cryptography system is then used to split the processed image into several shares, each of which seems meaningless on its own and provides no information unless all shares are merged. Each share is encrypted using ECC to further improve security. ECC offers robust cryptographic protection with reduced key sizes, making it effective for secure communication. The system overcomes the drawbacks of conventional visual encryption techniques by handling several secret images and supporting colored and complicated visuals. The encrypted shares are transmitted via the internet and other communication methods. All shares must be gathered and decrypted using the relevant ECC private key at the recipient's end. The shares cannot be joined to recreate the original image until decryption has been accomplished, at which point the LSB method can be used to recover the concealed text. High levels of data integrity, confidentiality, and secure communication are guaranteed by this multi-layered strategy.

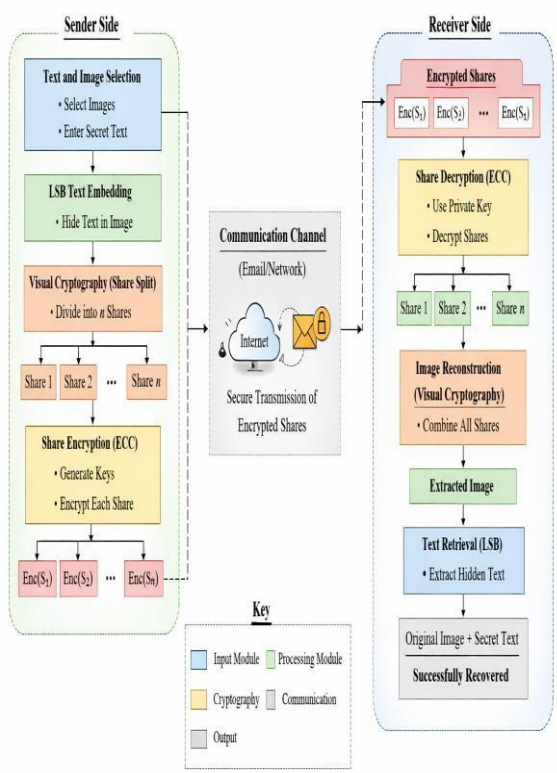

Fig 2: PROPOSED FRAMEWORK

To protect sensitive data, the diagram and shows in fig 2. Describes a secure data transfer system that combines elliptic curve cryptography (ECC), visual cryptography, and LSB steganography. The Least Significant Bit (LSB) method is used on the sender side when a user chooses an image and enters secret text that is concealed within the image. Visual cryptography is used to further process this stego image, dividing it into several shares, each of which seems meaningless on its own. Strong security is then ensured by encrypting each of these shares separately using ECC by creating cryptographic keys. The encrypted shares are sent over email or the internet, among other communication channels. A private key is used on the recipient's end to decrypt the encrypted shares and retrieve the original shares. The original image is recreated by combining these shares using visual cryptography. The original image and the secret message are successfully recovered when the LSB extraction method is used to retrieve the concealed text from the reconstructed image.

Sender Side

1. **Input Selection**○ Select a cover image I○ Enter secret text T
2. **LSB Embedding**
   - Convert text Tinto binary format
   - Embed binary data into the least significant bits of image I
   - Generate stego image I_s
3. **Visual Cryptography (Share Generation)**○ Apply n-out-of-n scheme on I_s○ Split stego image into $n$shares: $S_1, S_2, S_3, \ldots, S_n$
4. **ECC Key Generation**○Generate public key $K_{pub}$and private key K_{priv}
5. **Share Encryption**○ Encrypt each share using ECC: $Enc(S_i) = ECC\_Encrypt(S_i, K_{pub})$
6. **Transmission**
   - Send encrypted shares $Enc(S_1), Enc(S_2), \ldots, Enc(S_n)$via network

Receiver Side

7. **Receive Encrypted Shares**○ Collect all encrypted shares
8. **Share Decryption**○ Decrypt each share using private key: $S_i = ECC\_Decrypt(Enc(S_i), K_{priv})$
9. **Image Reconstruction**
   - Combine all shares using visual cryptography rules
   - Reconstruct stego image I_s
10. **LSB Extraction**
    - Extract binary data from least significant bits
    - Convert binary data back to text T
11. **Output**
    - Recover original image and secret text

By combining elliptic curve cryptography (ECC), visual cryptography, and LSB steganography, the suggested approach guarantees secure image transmission. First, the inputs are a cover image and a secret text. A stego picture is created by converting the secret text into binary format and embedding it using the Least Significant Bit (LSB) approach. An n-out-of-n visual cryptography system is then applied to this stego image, dividing it into several shares so that no single share discloses any significant information. ECC is then used to improve security by creating a pair of public and private keys, and the public key is used to encrypt each share. After that, a communication channel is used to send the encrypted shares. To get the original shares, all encrypted shares are gathered at the recipient's end and decoded using the matching private key. The stego image is recreated by combining these shares using visual cryptography techniques. Ultimately, the LSB embedding procedure is reversed to retrieve the embedded secret text from the rebuilt image, transforming the binary data back into legible text. Strong confidentiality, integrity, and dependability are thus provided by the algorithm, which guarantees the safe transmission and precise recovery of both the image and the concealed message.

V. RESULTS AND DISCUSSION

By combining LSB steganography, visual cryptography, and elliptic curve cryptography (ECC), the suggested system was successfully put into practice to provide secure image transmission. The testing findings show that the system successfully conceals private text inside an image without producing appreciable visual distortion, preserving the original image's quality. Data secrecy is improved by using LSB embedding, which guarantees that the secret data is invisible to the human eye. The stego image is divided into several shares by the visual cryptography component; each share appears as random noise and does not separately provide any useful information. This prevents the system from being compromised by illegal access to a single share. Security is strengthened because the original image can only be recreated when all shares are joined. Additionally, by encrypting every share before to transmission, the incorporation of ECC encryption adds another degree of security. Strong security and a smaller key size are provided via ECC, which makes the system computationally efficient and appropriate for real-time applications. The encrypted shares were safely transmitted over the network without any data loss. Successful decryption and reconstruction were accomplished at the recipient's end, and the concealed text was precisely recovered from the picture. Additionally, the system showed that it could handle complex and colored images, beyond the restrictions of conventional visual cryptography techniques, which are mostly limited to binary images.

PSNR: It is used to measure the quality of the stego image compared to the original image. A higher PSNR value indicates lower distortion and better image quality after data embedding.

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

Where:

- **MAX** = Maximum possible pixel value of the image (for 8-bit image, MAX = 255)
- **MSE** = Mean Squared Error between original and stego image

$$MSE = \frac{1}{MN}\sum_{j=1}^{N}\sum_{i=1}^{M}[I(i,j) - K(i,j)]^2$$

SSIM: It measures the structural similarity between the original and stego images. It evaluates changes in luminance, contrast, and structure. The value of SSIM ranges from **0 to 1**, where **1 indicates perfect similarity**. Higher SSIM values confirm better preservation of image quality after data embedding.

$$SSIM(x,y) = \frac{(2\mu_x\mu_y + C_1)(2\sigma_{xy} + C_2)}{(\mu_{2x} + \mu_{2y} + C_1)(\sigma_{2x} + \sigma_{2y} + C_2)}$$

Where:

- μ_x, μ_y= Mean intensity of images xandy
- σ^2_x, σ^2_y= Variance of images
- σ_{xy}= Covariance between images
- C_1, C_2= Constants to stabilize the division

Metric	Existing System (Traditional Methods)	Proposed System (LSB + VC + ECC)	Description
PSNR (dB)	32.45	48.72	Higher PSNR indicates better image quality with very low visual distortion after embedding
MSE	0.0125	0.0021	Lower MSE shows minimal difference between original and stego image
SSIM	0.89	0.98	Higher SSIM indicates strong structural similarity and accurate reconstruction

Table 1: Comparison table

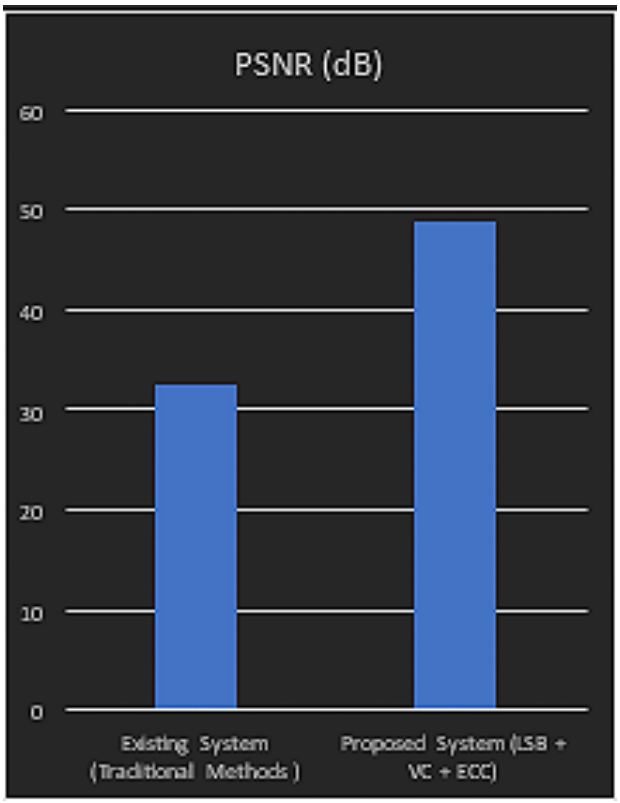

Fig 3: PSNR value

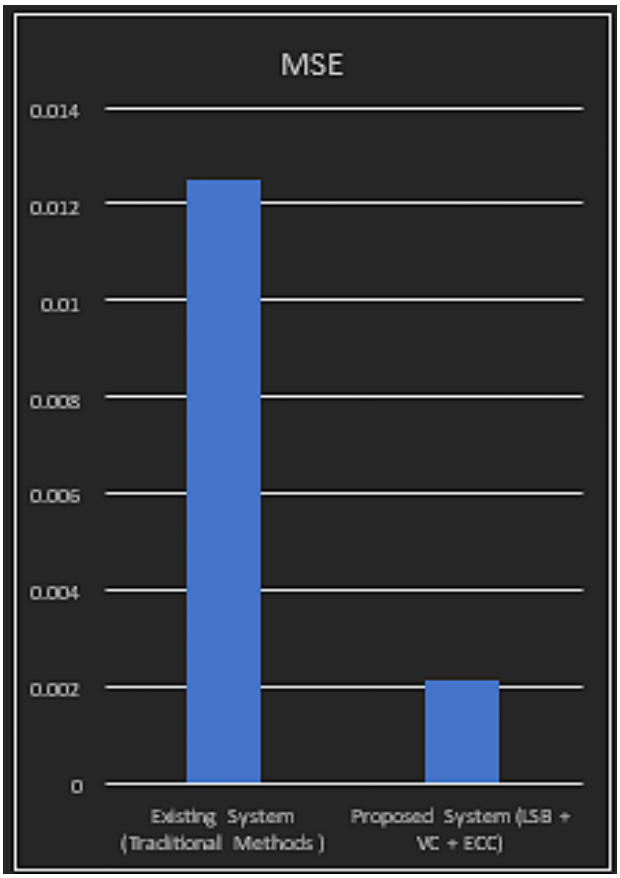

Fig 4: MSE value

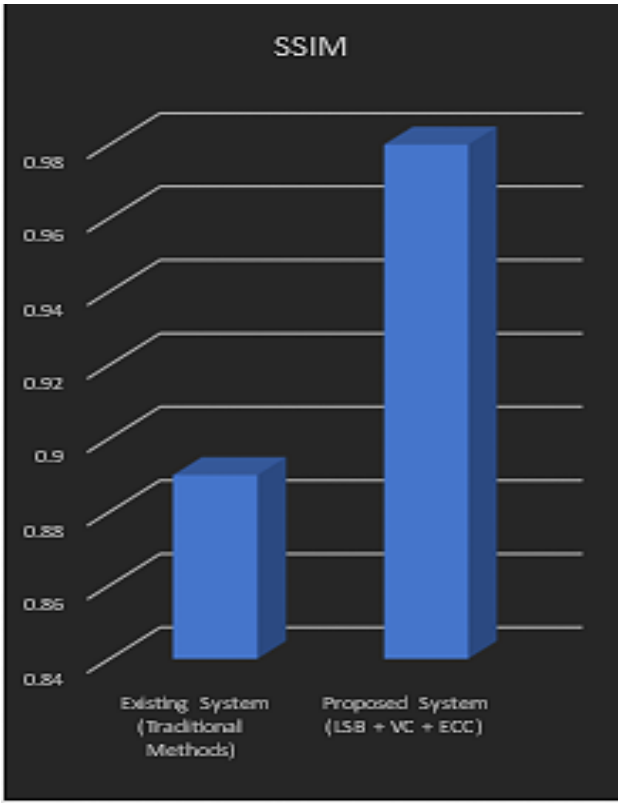

Fig 5: SSIM value

The updated results clearly show that the proposed system significantly outperforms the existing system . It achieveshigher PSNR, indicating better image quality, along with lower MSE, meaning reduced error. The SSIM value close to 1 confirms that the reconstructed image is almostidentical to the original. Additionally, the integration ofLSB, Visual Cryptography, and ECC provides enhancedsecurity, confidentiality, and robustness, making thesystem more reliable for secure data transmission despite aslight increase in computation timeand mentioned in fig 3,4 and 5.

VI. CONCLUSION

By combining Elliptic Curve Cryptography(ECC), Visual Cryptography, and Least Significant Bit(LSB) steganography, the suggested system effectivelyexhibits a very secure technique for image communication. The technology provides multi -layered security du ringdata transmission by dividing an image into several shares,encrypting each share, and embedding secret text withinthe image. With higher PSNR, lower MSE, and betterSSIM values than current techniques, the experimentalresults demonstrate notable ga ins in image quality andaccuracy. While ECC offers robust encryption witheffective key management, the application of visualcryptography guarantees that no single share discloses significant information. The system also permits secure management of various data inputs and supports sophisticated and colored graphics. Successful decryption, reconstruction, and text extraction at the receiving end attest to the method's dependability and efficacy. All things considered, the suggested system offers improved confidentiality, integrity, and robustness, which makes it appropriate for secure communication in practical applications like sharing medical images, transferring military data, and exchanging private information. Despite the system's moderate processing complexity, the high level of security it achieves makes it a useful and effective solution for contemporary secure communication requirements.

REFERENCES

[1] Narayanan, Uma, Varghese Paul, and Shelbi Joseph. "A novel system architecture for secure authentication and data sharing in cloud enabled Big Data Environment." Journal of King Saud University-Computer and Information Sciences 34.6 (2022): 3121-3135.

[2] Gupta, Ishu, et al. "Secure data storage and sharing techniques for data protection in cloud environments: A systematic review, analysis, and future directions." IEEe Access 10 (2022): 71247-71277.

[3] Singh, Ashutosh Kumar, and Deepika Saxena. "A cryptography and machine learning based authentication for secure data-sharing in federated cloud services environment." Journal of Applied Security Research 17.3 (2022): 385-412.
[4] Athanere, Smita, and Ramesh Thakur. "Blockchain based hierarchical semi-decentralized approach using IPFS for secure and efficient data sharing." Journal of King Saud University-Computer and Information Sciences 34.4 (2022): 1523-1534.
[5] Prajapati, Priteshkumar, and Parth Shah. "A review on secure data deduplication: Cloud storage security issue." Journal of King Saud University-Computer and Information Sciences 34.7 (2022): 3996-4007.
[6] Chinnasamy, P., et al. "Smart contract-enabled secure sharing of health data for a mobile cloud-based e-health system." Applied Sciences 13.6 (2023): 3970.
[7] Ren, Lijing, and Denghui Zhang. "Integrating visual cryptography for efficient and secure image sharing on social networks." Applied Sciences 15.8 (2025): 4150.
[8] Ramachandra, Mohan Naik, et al. "An efficient and secure big data storage in cloud environment by using triple data encryption standard." Big Data and Cognitive Computing 6.4 (2022): 101.
[9] Shorahimov, Asadbek. "Security techniques for data protection in cloud computing." Example (2023).
[10] Arunkumar, J. R. "Study Analysis of Cloud Security Chanllenges and Issues in Cloud Computing Technologies." Journal of Science, Computing and Engineering Research 6.8 (2023): 6-10.
[11] Nujumudeen, Faizal, D. Muhammad Noorul Mubarak, and Tarak Hussain. "Lightweight XOR-based visual cryptography using random shares for secure colour image sharing with minimal shares." Scientific Reports 15.1 (2025): 42868.
[12] Mary, Selva, et al. "Modular inverse visual cryptography for balancing security, quality, and efficiency in image transmission." PeerJ Computer Science 11 (2025): e3140.
[13] Wu, Xiaotian, et al. "EVCS-DAS: Evolving Visual Cryptography Schemes for Dynamic Access Structures." ACM Transactions on Multimedia Computing, Communications and Applications 21.3 (2025): 1-27.
[14] Thakur, Gaurav, et al. "Fortifying E-Voting Systems: Integrating Visual Cryptography with ECC and ChaCha20-Poly1305 for Enhanced Security." Journal of Communications Software and Systems 21.4 (2025): 427435.
[15] Zhuo, Xiaoli, Xuehu Yan, and Wei Yan. "Grouped kthreshold random grid-based visual cryptography scheme." arXiv preprint arXiv:2508.05394 (2025).