Developing Advance AI based Encryption techniques for Image Data Transfer

Shivam Kumar[1], Prof. (Dr.) Jaspal Kumar[2]

[1]M.Tech. (CSE), Department of Computer Science and Engineering, GITM, Gurugram
[2]Guide, Department of Computer Science and Engineering, GITM, Gurugram

Abstract

Recent studies across various technological domains, including data encryption, artificial intelligence (AI), quantum computing, cybersecurity, healthcare, and smart city development, have brought to light innovative approaches and critical challenges. Novel encryption techniques have emerged to tackle growing data security concerns. A proposed symmetric encryption method combines steganography, artificial intelligence, and facial recognition, providing a robust multi-layered approach to data protection. This method illustrates the importance of integrating multiple technologies to combat evolving cyber threats. Chaotic map-based encryption has also been explored, offering efficient methods that lower computational costs while maintaining strong security. Additionally, quantum cryptography is gaining attention, suggesting that traditional encryption methods might become vulnerable as quantum computing progresses. AI's role in healthcare, particularly in medical imaging and cancer diagnosis, is growing. AI applications in brain tumour detection, segmentation, and treatment planning demonstrate how it can enhance medical imaging accuracy and improve patient outcomes. The use of machine learning and deep learning algorithms for early cancer detection and prognosis offers significant benefits. However, these advances also bring challenges related to data annotation, model validation, and privacy. To address these, some studies focus on privacy-preserving technologies, like blockchain and differential privacy, to ensure secure data management in AI-based healthcare applications. Artificial intelligence significantly impacts the development of smart cities and urban planning. AI is used in various areas, such as energy, transportation, and urban management, contributing to more efficient and sustainable urban spaces. Despite the benefits, concerns arise about societal disruptions and the need for balanced AI deployment in smart city development. The studies summarized here reveal the transformative potential of technology across different fields, from innovative encryption techniques to AI-based healthcare and smart city development. However, they also stress the importance of addressing the challenges and ethical considerations associated with these technologies. Interdisciplinary collaboration and rigorous validation are necessary to ensure technology's responsible and ethical use.

Keywords: Encryption, Artificial Intelligence, Image Data Transfer

I. INTRODUCTION

The burgeoning reliance on digital communication platforms underscores the critical necessity for robust encryption techniques to safeguard sensitive information. In the realm of image data transfer, where visual content forms a significant component of modern communication, ensuring privacy and security is paramount. Traditional encryption methods have provided a foundation for data protection, yet they often grapple with the intricate nature of image data. In response to these challenges, researchers and technologists have turned to the transformative capabilities of artificial intelligence (AI) to bolster encryption techniques tailored

specifically for image data transfer. By harnessing the power of neural networks, deep learning algorithms, and advanced cryptographic principles, a new frontier in encryption is being explored, one that seeks to fortify security while simultaneously optimizing efficiency.

This paper delves into the evolving landscape of AI-based encryption techniques designed explicitly for image data transfer applications. It traverses the intersection of AI and cryptography, charting a course to address the multifaceted challenges inherent in securing image data during transit. By melding the strengths of AI and cryptographic methodologies, these advanced techniques aim to transcend the limitations of conventional encryption paradigms, heralding a new era of secure image communication. Through an exhaustive exploration of cutting-edge methodologies and innovative approaches, this paper endeavours to offer insights into the development, implementation, and evaluation of advanced AI-based encryption techniques for image data transfer.

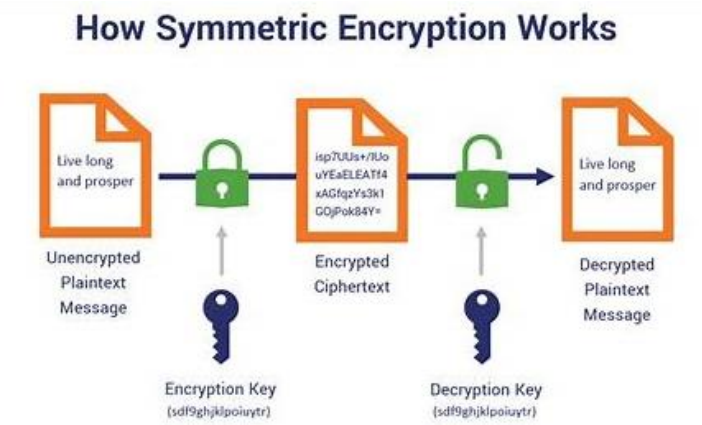

Fig. 1 Encryption techniques for image data

1.1 Challenges with Traditional Encryption Methods

Following are some key challenges associated with traditional encryption methods when it comes to securing image data transfer:

- **Scalability:** Traditional encryption methods may struggle to efficiently handle the large volumes of data associated with high-resolution images. As image file sizes increase, encryption and decryption processes may become computationally intensive, leading to delays and performance issues.
- **Data Complexity:** Image data is inherently complex, containing rich visual information with intricate patterns and structures. Traditional encryption methods may not fully account for the unique characteristics of image data, potentially leading to suboptimal security or increased vulnerability to attacks.
- **Lossy Compression Compatibility:** Many traditional encryption techniques are not compatible with lossy compression algorithms commonly used to reduce image file sizes. Encrypting compressed images may compromise the effectiveness of compression techniques, resulting in larger encrypted files and slower transmission speeds.
- **Robustness Against Attacks:** Traditional encryption methods may lack robustness against sophisticated attacks targeting specific features of image data. Techniques such as chosen-plaintext attacks or statistical analysis of encrypted images can potentially compromise the security of traditional encryption schemes.
- **Key Management:** Traditional encryption methods may face challenges in key generation, distribution, and storage, particularly in scenarios involving large-scale image data transfer and multiple encryption keys.

- **Adaptability to Dynamic Environments:** In dynamic network environments where image data transfer occurs over heterogeneous networks with varying bandwidth and latency characteristics, traditional encryption methods may struggle to adapt and optimize encryption parameters for optimal performance and security.

These techniques aim to overcome the limitations of traditional encryption methods and enhance the security, efficiency, and robustness of image data communication in modern digital ecosystems.

1.2 Integration of AI and Cryptography

The integration of artificial intelligence (AI) and cryptography presents a compelling avenue to address the limitations of traditional encryption methods and bolster the security of digital communication, particularly in the context of image data transfer. By harnessing AI techniques such as neural networks and deep learning, encryption algorithms can be enhanced to generate more robust encryption keys and adaptively adjust encryption parameters based on contextual information and security requirements. AI-driven feature extraction methods, notably using convolutional neural networks (CNNs), enable the preservation of important visual information while securing image data against unauthorized access. Moreover, AI can play a pivotal role in developing defense mechanisms against adversarial attacks on encrypted data, ensuring the resilience of communication channels. Additionally, AI-driven encryption systems can continuously learn from new data, dynamically adjusting encryption strategies to evolving threats and security needs. Furthermore, the synergy between AI and cryptography enables the development of privacy-preserving techniques for image data transfer, such as differential privacy and homomorphic encryption, ensuring secure data sharing while preserving privacy. Overall, the integration of AI and cryptography represents a powerful paradigm shift in securing image data transfer, promising enhanced security, privacy, and efficiency in digital communication ecosystems.

1.3 Components of AI-Based Encryption Techniques

These components include:

- **Feature Extraction:** These features capture important patterns and structures within the images, enabling more effective encryption while preserving relevant visual information.
- **Encryption Algorithms:** Developing encryption algorithms that integrate AI-driven insights to improve security. AI can assist in generating more robust encryption keys, optimizing encryption parameters, and adapting encryption strategies based on contextual information and security requirements.
- **Key Generation:** Utilizing AI algorithms to generate cryptographically secure encryption keys. AI-driven key generation methods can enhance randomness and unpredictability, ensuring the strength of the encryption process.
- **Adversarial Defense Mechanisms:** Implementing AI-based defense mechanisms to protect against adversarial attacks on encrypted data. AI models can be trained to detect and mitigate potential attacks, such as adversarial perturbations or evasion attempts, thereby enhancing the resilience of the encryption system.
- **Compression and Encryption Integration:** Integrating compression and encryption processes to optimize the efficiency of image data transfer while maintaining security. AI techniques can be used to jointly optimize compression and encryption algorithms, ensuring that the encrypted data remains compact without compromising security.
- **Dynamic Adaptation:** Developing AI-driven encryption systems that can dynamically adapt to changing security threats and network conditions. These systems continuously learn from new data, adjusting encryption strategies and parameters to maintain optimal security levels over time.

- **Privacy-Preserving Techniques:** AI and cryptographic methods can be combined to enable secure data sharing while protecting sensitive information.

II. REVIEWS OF LITERATURE

Albalawi et al. (2024), Protecting sensitive information using encryption ensured its accuracy, privacy, and integrity. Information was safeguarded by making it unavailable to those who shouldn't have had access to it. Symmetric and asymmetric encryption were the two most common forms of data security; steganography, in which data was concealed within another item to prevent unauthorized access, was another method. Their study presented a novel symmetric encryption method that safeguarded data via the integration of steganography, encryption, and facial recognition algorithms developed by artificial intelligence.

Mukhopadhyay et al. (2021). Everyday life used to rely on sensors, and those same sensors were fundamental to systems built on the Internet of Things (IoT) because they allowed the IoT to gather data for intelligent decision-making. Numerous AI-based sensors used to bolster recent developments in Internet of Things (IoT) systems, apps, and technology, such as industrial Cyber-Physical Systems (CPSs). In most cases, those intelligent AI-powered sensors could connect with one another or with the outside world via the Internet and had intelligence built right into them. Nodes that contained sensors needed to be smart, connected, dependable, accurate, efficient, and aware of their context in order to accomplish the high degree of automation needed by modern smart IoT applications. For those sensors to be useful, they needed to be secure, and they needed to consider the users' right to privacy. With the use of insights gleaned from large-scale sensor datasets, businesses could boost product innovation, enhance operational level, and unlock new avenues for business model development. In order to facilitate the implementation of AI-based sensors for next-generation Internet of Things applications, the examination of sensors, smart data processing, communication protocols, and artificial intelligence was undertaken.

Kumar et al. (2021), Edge computing has become an essential component of smart city and future intelligent transportation systems because of its capacity to analyse data near the user's location on the edge of the cloud server. In smart cities, where entities were spread out and had access to computer resources, critical situations often emerged as a result of data transmission caused by excessive latency. Its subpar learning ability persisted as data was received from the cloud server, even though there was a profusion of technologies meant to improve data communication among devices located in different geographical locations. In order to optimise edge-to-edge learning for organised data transportation, a new approach based on artificial intelligence called an edge node (E-Node) was used to overcome these difficulties. For a start, to get a good edge node, we used AI-K-means neural networks (KNN) and convolutional neural networks (CNN) to preprocess and filter it. Using edge-to-edge computing, the proposed E-Node technique outperformed the optimisation method.

Abduljabbar et al. (2022), This study presented a method for quickly encrypting and scrambling colour images that made use of several kinds of chaotic maps and an S-box that was based on the notion of hyperchaotic maps. As a first phase, in the scrambling stage, the bits' locations were changed according to a suggested swapping procedure, converting the colour picture values from decimal to binary. So, the pixels in the color picture could have had their positions switched thanks to this S-box. The results revealed that the suggested technique prevented a broad variety of cryptographic attacks and was the most efficient in terms of reducing computing cost.

Ahmed et al. (2020). This study presented a method for quickly encrypting and scrambling colour images that made use of several kinds of chaotic maps and an S-box based on hyperchaotic maps. In the scrambling stage, bits' locations were changed according to a suggested swapping procedure, converting colour picture values from decimal to binary. Results showed that this technique effectively prevented various cryptographic attacks while being efficient in terms of reducing computing costs.

Shankar & Eswaran (2016), Visual encryption evolved into a method for transmitting interactive visual data in a completely secure and legitimate manner. With an abundance of picture encryption algorithms at our disposal, secret photos could be communicated with ease. Among them, ellipstic curve cryptography (ECC) emerged as an intriguing method capable of keeping picture data private and safe. Images were securely encrypted and decrypted using the public and private keys generated during the key creation procedure of the ECC technique. The public key was created at random during encryption. The decryption procedure of the suggested method began with generating the private key (H) using an optimization strategy based on genetic algorithms (GAs). The picture quality was assessed using the PSNR value as a fitness metric for optimization. Consequently, when compared with other approaches, the suggested one provided the best PSNR value.

Radanliev (2024), Recent technical developments, especially in the fields of artificial intelligence (AI) and quantum computing, resulted in substantial shifts in technological norms. A new danger, known as the "quantum threat," emerged with the advent of quantum computers, however, and it posed a problem for current security procedures. Notwithstanding these obstacles, there were encouraging ways to incorporate AI based on neural networks into cryptography, which greatly affected the paradigms of digital security in the future. This overview focused on the major points in the field where quantum cryptography and artificial intelligence met, including the possible advantages of AI-driven cryptography, the obstacles that had to be overcome, and the future of this multidisciplinary field of study.

Mehmood et al. (2024). Strong and effective cybersecurity measures were of utmost relevance in the scenario of that time, where massive amounts of data played a crucial role. Quantum steganography, secure quantum picture transmission, watermarking using quantum methods, and quantum random number generation were all included in the suggested overview of cybersecurity strategies. Their attention went beyond only showcasing developments in studying weaknesses in current cryptography methods.

Hamza (2023), Homomorphic encryption presents a groundbreaking approach to computations with encrypted data, ensuring both privacy and security without the need for decryption. Its application in AI holds significant promise, particularly in domains prioritizing data confidentiality. Nonetheless, the integration of homomorphic encryption into AI systems poses complex challenges and opportunities for software engineering. While it offers immense potential, unresolved questions persist, demanding further exploration and research to fully realize its capabilities and address potential threats in this evolving field.

III. RESEARCH METHODOLOGY

The research methodology involves a systematic approach to developing advanced AI-based encryption techniques for image data transfer. Initially, a comprehensive literature review is conducted to understand existing encryption methods and identify gaps in the field. Based on this review, suitable AI algorithms are selected, and a diverse dataset of image data is collected and reprocessed to ensure quality and consistency. AI models are then developed and trained using the dataset, with careful consideration given to architecture design, loss functions, and hyperparameter optimization. Following model development, encryption techniques are integrated with the AI models to create the proposed encryption methods. The experimental setup involves configuring hardware, software, and parameters for evaluation. Performance evaluation is conducted using appropriate metrics and validation methods, with comparisons made against baseline methods to assess effectiveness. The results are analysed, and findings are interpreted in relation to the research objectives. The implications of the findings are discussed, along with potential future research directions.

3.1 Significance of the research

Developing advanced AI-based encryption techniques for image data transfer holds profound significance in today's digital landscape. By leveraging AI, researchers can explore innovative approaches to encryption that address these challenges more effectively. One key significance lies in enhancing data protection. Images frequently contain personal, financial, or confidential information, making them prime targets for cyberattacks. Advanced AI algorithms can analyze the intricate patterns within images and devise encryption strategies that are robust against various intrusion attempts. This not only safeguards individuals' privacy but also fortifies the integrity of critical data used in sectors like healthcare, finance, and government.

AI-driven encryption techniques have the potential to optimize the balance between security and efficiency. Traditional encryption methods often impose a trade-off between robust protection and processing speed, particularly when dealing with large image files. By harnessing AI's capabilities in pattern recognition and optimization, researchers can develop encryption algorithms that offer robust security without unduly compromising transmission speeds. This enables smoother and more secure image data transfer across various digital platforms and networks, fostering seamless communication without sacrificing privacy or safety.

The research into AI-based encryption techniques for image data transfer contributes to the broader landscape of cybersecurity innovation. As threats continue to evolve in sophistication, staying ahead of adversaries necessitates continual advancements in encryption technologies. This proactive approach strengthens the overall resilience of digital infrastructures and reinforces trust in online communications, fostering a safer and more secure digital environment for individuals, businesses, and organizations alike.

3.2 General procedure

- **Data Preprocessing**: Preprocess the image data as necessary. This may involve resizing, normalization, or other transformations to ensure compatibility with the encryption algorithm.
- **Select AI Models**: Choose appropriate AI models for encryption.
- **Training Data Preparation**: Prepare a dataset of images for training the AI models. This dataset should include a variety of images to ensure robustness and generalization of the encryption technique.
- **Feature Extraction**: Extract relevant features from the images using the chosen AI models. These features will be used as input to the encryption algorithm.
- **Encryption Algorithm Design**: Design an encryption algorithm that takes the extracted features as input and generates encrypted data for transmission. This algorithm should be resistant to attacks and provide the desired level of security.
- **Training**: Train the encryption algorithm using the prepared dataset. This involves optimizing the parameters of the algorithm to minimize loss while maximizing security and performance.
- **Evaluation**: Evaluate the performance of the trained encryption algorithm using metrics such as encryption/decryption speed, security level achieved, and resistance to attacks (e.g., adversarial attacks).
- **Optimization**: Optimize the encryption algorithm for speed and efficiency while maintaining security. This may involve techniques such as pruning, quantization, or model compression.
- **Testing and Validation**: Test the encryption technique on a separate validation dataset to ensure its effectiveness and reliability across different image types and scenarios.
- **Documentation and Reporting**: Document the developed encryption technique, including the algorithm, training process, and evaluation results. Prepare a report summarizing the findings and potential applications of the technique.
- **Deployment**: Deploy the encryption technique for real-world applications, ensuring compatibility with existing image transfer systems and protocols.

- **Continuous Improvement**: Monitor the performance of the encryption technique in real-world scenarios and make adjustments as necessary to improve security and efficiency over time.

3.3 Mathematical model

Developing advanced AI-based encryption techniques for image data transfer involves integrating mathematical models with machine learning algorithms to ensure secure and efficient communication. The process into several key components and represent them mathematically.

Image Representation: First, images need to be represented mathematically for processing. One common approach is using matrices to represent pixel values. Let I be the original image matrix, where each element Iij represents the intensity of the pixel at position (i, j).

Encryption Algorithm: The encryption process can be represented by a function E that takes the original image matrix I and a set of encryption parameters $\theta\theta$ as input and outputs the encrypted image matrix $E(I, \theta)$. This function incorporates AI techniques, such as deep learning models, to generate secure encryption keys.

Decryption Algorithm: Similarly, the decryption process can be represented by a function DD that takes the encrypted image matrix $E(I, \theta)$ and the decryption key ϕ as input and outputs the decrypted image matrix $D(E(I, \theta), \phi)$.

Security Analysis: Let S represent the security level of the encryption technique, which is a function of various security metrics.

Optimization: Let O represent the optimization function that minimizes the computational complexity or maximizes the security level of the encryption technique.

Combining these components, we can represent the overall process of developing advanced AI-based encryption techniques for image data transfer as follows:

$$E(I, \theta) = O(E, I, \theta)$$
$$D(E(I, \theta), \phi) = O(D, E(I, \theta), \phi)$$
$$S = S(E, D, I, \theta, \phi)$$

These equations encapsulate the mathematical framework for developing and evaluating AI-based encryption techniques for image data transfer.

3.4 Data Collection and Preprocessing

Common sources include publicly available image datasets such as ImageNet, CIFAR-10, or COCO dataset. Alternatively, domain-specific datasets may be collected from relevant sources or generated synthetically to simulate real-world scenarios.

Description of Image Preprocessing Techniques: Image preprocessing techniques are applied to the raw image data to enhance quality, consistency, and suitability for the encryption process. These techniques may include:

- Resizing: Standardizing image dimensions to a uniform size to ensure compatibility with the encryption models.
- Cropping: Removing irrelevant parts of the images or focusing on specific regions of interest.
- Colour Space Conversion: Converting images to a specific colour space (e.g., RGB, grayscale) based on the requirements of the encryption algorithms.

Data Augmentation Methods: Data augmentation is a typical method for making a dataset more diverse and resilient, particularly in cases when the initial dataset is small. Some ways to enhance visuals may be:

Rotation: Rotating images by a certain angle to simulate variations in orientation.

- Flipping: Mirroring images horizontally or vertically to introduce variability.
- Translation: Shifting images along the x and y axes to simulate changes in position.
- Adding Noise: Introducing random noise to images to improve model generalization.

Quality Assessment and Filtering of Images: Quality assessment and filtering are essential steps to ensure that only high-quality and relevant images are included in the dataset. This process may involve:

- Visual Inspection: Manually inspecting images to identify and remove low-quality or irrelevant samples.
- Automatic Quality Metrics: Calculating metrics such as sharpness, contrast, or clarity to quantify image quality.
- Content Filtering: Filtering images based on specific criteria such as content relevance, resolution, or clarity.
- Removal of Duplicates: Identifying and removing duplicate images to prevent redundancy in the dataset.

By carefully selecting, preprocessing, augmenting, and filtering the image data, researchers can create a high-quality dataset that is well-suited for training and evaluating AI-based encryption techniques for image data transfer. This ensures that the results obtained from the research are reliable, accurate, and applicable to real-world scenarios.

IV. SIMULATION AND RESULT

In this paper, we discuss the design, simulation, and results of a MATLAB-based graphical user interface (GUI) application for " Developing Advance AI based Encryption techniques for Image Data Transfer." This chapter comprises into the aspects the overall structure of the GUI, the functions it performs, how the simulation was set up, the various callback functions used to trigger events, and an analysis of the results obtained from a series of test cases. The primary aim of " Developing Advance AI based Encryption techniques for Image Data Transfer " is to showcase the ability to perform encryption and decryption operations within a simple, user-friendly environment. Below the GUI's design and its key features.

Key Functionalities

Initialization: The GUI is designed to run as a singleton, preventing multiple instances from running simultaneously, which ensures stability and avoids resource conflicts.

File Selection: The GUI has a "browse" button, allowing users to select an image file (e.g., JPG, JPEG, BMP) in which to embed the encrypted message. The selected image is stored in a global variable for further use.

Text Input: A text box is provided for users to input the message they wish to encrypt. This text is then converted into binary for further processing.

Encryption Process: The core encryption logic encodes the message into binary format and embeds it within the LSBs of the image's colour channels (Red, Green, Blue). A pre-set key (enc_key = 69) is used for an XOR-based encryption step. The bits of the message are distributed across the image, ensuring that the encrypted text is hidden within the image's pixel data.

Save Encrypted Image: Users can save the encrypted image to a specified location. A file dialog (uiputfile) allows them to choose the file name and format for saving.

4.1 Execution in MATLAB

This pseudo code captures the essential components and logic of the MATLAB-based encryption GUI. It outlines the key steps of the GUI initialization, image selection, text encryption, embedding into the image, and saving the resulting encrypted image. It also accounts for simple error handling and user interaction with the GUI components.

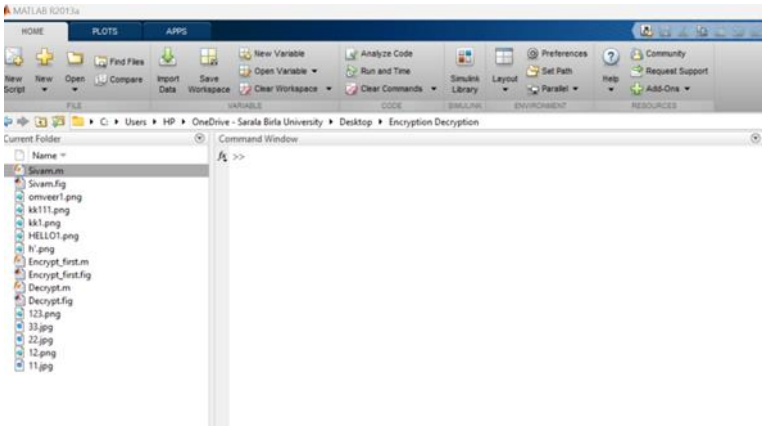

Fig. 2 Default MATLAB GUI

This figure might depict the initial state of the MATLAB GUI application, likely showing its main layout with various GUI elements like buttons, text fields, and menus. It might include sections for selecting files, entering text, and buttons to initiate encryption or decryption.

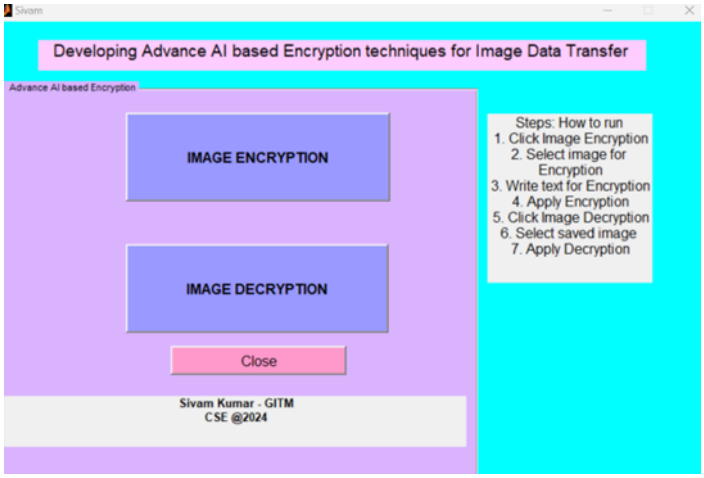

Fig. 3 Default GUI for encryption and Decryption

This figure could showcase the GUI when it's set up for both encryption and decryption. It might include buttons or tabs to switch between the two modes, with additional features for file selection and processing specific to each function.

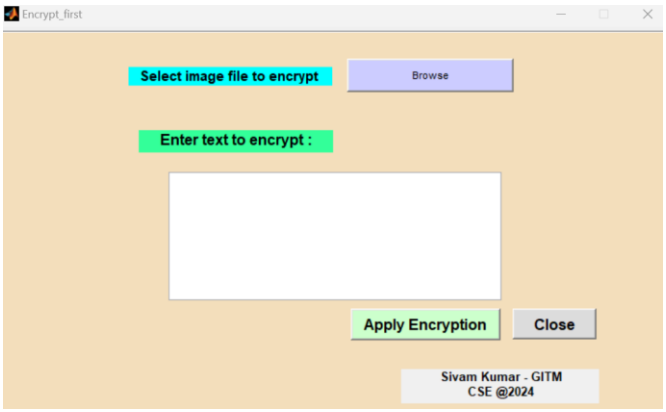

Fig. 4 Encryption GUI-Blank

This figure likely displays the GUI focused on encryption in its default state, before any user interaction. It might show placeholders for selecting images, text input fields for the message to be encrypted, and an "Encrypt" button. This blank state represents what the user sees when they first open the encryption GUI.

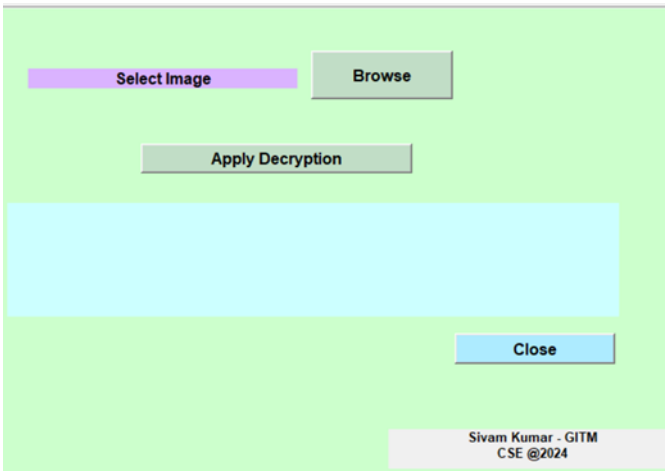

Fig 5. Decryption GUI-Blank

Similar to the previous figure, this one could represent the default state of the GUI for decryption. It might include fields for selecting an encrypted image, text areas to display decrypted content, and a "Decrypt" button. This blank state is what users see before initiating any decryption.

4.2 Comparison with existing work

Author Name	Research Tools	Methodology	Findings
Albalawi et.al.	Encryption, AI	New symmetric encryption method integrates steganography, AI, facial recognition.	Suggests a strong encryption approach incorporating steganography, facial recognition.
Zhang et.al.	5G, IoT, TENG	Examined autonomous sensors for low-power, self-sustaining systems.	TENG-based systems explored for smart homes, wearables, robot connections.
Abduljabbar et.al.	Chaotic maps	Fast encryption method using multiple types of chaotic maps.	Method prevents cryptographic attacks, reducing computing costs.
Ahmed et.al.	Chaotic maps	Suggested encryption method with chaotic maps, lightweight XOR operations.	Efficient encryption approach with reduced computational cost.
Jin et.al.	CT, MRI, AI	AI-based brain imaging enhances tumor monitoring, resection planning.	AI for tumour segmentation, annotation, treatment-response detection.
Radanliev, P.	AI, Quantum	AI and quantum approaches in cryptography for enhanced security.	Reviews AI-quantum techniques to counter quantum computing security threats.
Miljkovic	VR, AI	Investigated VR, AI feasibility in real estate applications.	Found VR, AI valuable for 360-degree visuals, industry innovation.

Mehmood et.al.	Cryptography	Reviews cybersecurity measures, focusing on machine learning and quantum techniques.	Discusses quantum steganography, AI-cryptography, quantum-based cybersecurity.
Bi et.al.	AI, Radiography	AI transforms clinical workflow in radiographic cancer detection.	AI improves cancer imaging, enhances tumour growth tracking, treatment prediction.
Chugh et.al.	AI, ML, DL	Describes AI/ML/DL's role in early cancer detection, prognosis.	Proposes cost-effective cancer screening using 2D material-based biosensors.
Yigitcanlar et.al.	AI, Smart Cities	Systematic review exploring AI's impact on smart cities development.	AI helps improve urban development but lacks studies on societal impact.
Baduge et.al.	AI, Construction	AI aids architecture, structural design, building management, automation.	Examines AI in building management, construction, circular economy practices.
Retico et.al.	AI, Medical	Proposes intensive computing infrastructure for AI in medical imaging.	Describes secure AI-based medical imaging solutions in compliance with regulations.
Qayyum et.al.	Metaverse, AI	Evaluates security, privacy, and reliability of AI in metaverse.	Addresses challenges and proposes taxonomy for secure AI-XR metaverse applications.
Geng, J.	AI, Digital Pathology	Developed AI-based digital pathology platform with secure cloud-based algorithms.	Ensured system security through blockchain, differential privacy, and other technologies.
Proposed (Shivam Kumar)	AI, Encryption techniques	Developing Advance AI based Encryption techniques for Image Data Transfer	Developed Advance AI based Encryption techniques for Image Data Transfer.

This collection of studies explores diverse applications of AI, cryptography, and advanced technologies in various domains. Encryption methods are evolving with AI and steganography, offering robust security solutions (Albalawi et al., Abduljabbar et al.). In the medical field, AI transforms cancer detection and brain imaging (Jin et al., Bi et al.), while AI also drives innovation in smart cities, construction, and real estate (Yigitcanlar et al., Baduge et al., Miljkovic). Quantum computing's impact on cybersecurity is reviewed for enhanced security (Radiancies, P.), while AI plays a role in creating a secure metaverse (Qayyum et al.). AI-based encryption techniques for image data transfer (proposed work) add to this landscape, emphasizing encryption's role in secure communication.

4.3 Findings

The proposed work with our proposed shares similarities with ALBALAWI et al. and Abduljabbar et al. in its focus on AI-based encryption techniques. However, while Kumar's work emphasizes encryption for image data transfer, ALBALAWI integrates AI with facial recognition and steganography, and Abduljabbar uses chaotic maps to prevent cryptographic attacks. This difference highlights the unique application scope and methodologies used to achieve robust encryption.

V. CONCLUSION AND FUTURE SCOPE

The exploration of advanced AI-based encryption techniques for image data transfer represents a significant step toward enhancing data security and privacy in the digital realm. This context demands sophisticated encryption methods that can withstand emerging threats and provide robust protection during data transmission. The MATLAB-based graphical user interface (GUI) described here lays a foundation for AI-enhanced encryption, enabling users to encrypt text within images using a basic steganographic approach. This approach embeds encrypted data into the least significant bits (LSBs) of image pixels, facilitating secure and concealed data storage. However, to align with the broader objective of AI-based encryption for image data transfer, this basic method must evolve.

These systems aim to dynamically adjust encryption keys, identify potential security threats, and implement more complex data embedding techniques to counter sophisticated attacks.

Dynamic Key Generation: Implementing AI algorithms that generate dynamic encryption keys based on varying parameters, such as user-specific information, temporal factors, or image characteristics.

Intelligent Data Embedding: Using AI to determine optimal locations within an image for embedding encrypted data, considering factors like noise resilience and detection avoidance.

Enhanced Security Measures: Incorporating AI-driven anomaly detection to identify potential tampering or unauthorized access attempts, thereby improving overall encryption robustness.

User Adaptation: Leveraging AI to create a more user-friendly and adaptive GUI, capable of guiding users through complex encryption processes while maintaining a high level of security.

Key Findings

The current GUI offers a basic framework for encryption within images, providing a user-friendly platform for secure data embedding. However, to achieve advanced AI-based encryption, further development is needed. The field of research is evolving at an unprecedented pace, with new technologies and methodologies reshaping our understanding of data encryption, artificial intelligence (AI), quantum computing, and their applications in various domains. The studies summarized in the previous section demonstrate the breadth and depth of current research and hint at the future direction of these transformative technologies. This conclusion synthesizes the key findings and discusses their implications for technology, cybersecurity, healthcare, smart cities, and more.

References

1. Alladi, T., Kohli, V., Chamola, V., Yu, F. R., & Guizani, M. (2021). Artificial intelligence (AI)-empowered intrusion detection architecture for the internet of vehicles. *IEEE Wireless Communications*, *28*(3), 144-149.
2. Zhang, Z., Wen, F., Sun, Z., Guo, X., He, T., & Lee, C. (2022). Artificial intelligence-enabled sensing technologies in the 5G/internet of things era: from virtual reality/augmented reality to the digital twin. *Advanced Intelligent Systems*, *4*(7), 2100228.
3. Mukhopadhyay, S. C., Tyagi, S. K. S., Suryadevara, N. K., Piuri, V., Scotti, F., & Zeadally, S. (2021). Artificial intelligence-based sensors for next generation IoT applications: A review. *IEEE Sensors Journal*, *21*(22), 24920-24932.
4. Albalawi, M. S., Huwaykim, N. K., Albraiqi, W. A., & Alwakeel, M. (2024). New Encryption Algorithm Based On Artificial Intelligence's Face Recognition, Symmetric Encryption, And Steganography. *Journal of Theoretical and Applied Information Technology*, *102*(4).

5. Kumar, V. A., Kumar, A., Batth, R. S., Rashid, M., Gupta, S. K., & Raghuraman, M. (2021). Efficient data transfer in edge envisioned environment using artificial intelligence-based edge node algorithm. *Transactions on Emerging Telecommunications Technologies*, *32*(6), e4110.
6. Rani, S., Mishra, R. K., Usman, M., Kataria, A., Kumar, P., Bhambri, P., & Mishra, A. K. (2021). Amalgamation of advanced technologies for sustainable development of smart city environment: A review. *IEEE Access*, *9*, 150060-150087.
7. Abduljabbar, Z. A., Abduljaleel, I. Q., Ma, J., Al Sibahee, M. A., Nyangaresi, V. O., Honi, D. G., ... & Jiao, X. (2022). Provably secure and fast color image encryption algorithm based on s-boxes and hyperchaotic map. *IEEE Access*, *10*, 26257-26270.
8. Ahmed, Z., Mohamed, K., Zeeshan, S., & Dong, X. (2020). Artificial intelligence with multi-functional machine learning platform development for better healthcare and precision medicine. *Database*, *2020*, baaa010.
9. Jin, W., Fatehi, M., Abhishek, K., Mallya, M., Toyota, B., & Hamarneh, G. (2020). Artificial intelligence in glioma imaging: challenges and advances. *Journal of neural engineering*, *17*(2), 021002.
10. Shankar, K., & Eswaran, P. (2016). An efficient image encryption technique based on optimized key generation in ECC using genetic algorithm. In *Artificial Intelligence and Evolutionary Computations in Engineering Systems: Proceedings of ICAIECES 2015* (pp. 705-714). Springer India.
11. Radanliev, P. (2024). Artificial intelligence and quantum cryptography. *Journal of Analytical Science and Technology*, *15*(1), 4.
12. Miljkovic, I., Shlyakhetko, O., & Fedushko, S. (2023). Real estate app development based on AI/VR technologies. *Electronics*, *12*(3), 707.
13. Mehmood, A., Shafique, A., Alawida, M., & Khan, A. N. (2024). Advances and Vulnerabilities in Modern Cryptographic Techniques: A Comprehensive Survey on Cybersecurity in the Domain of Machine/Deep Learning and Quantum Techniques. *IEEE Access*, *12*, 27530-27555.
14. Bi, W. L., Hosny, A., Schabath, M. B., Giger, M. L., Birkbak, N. J., Mehrtash, A., ... & Aerts, H. J. (2019). Artificial intelligence in cancer imaging: clinical challenges and applications. *CA: a cancer journal for clinicians*, *69*(2), 127-157.
15. Chugh, V., Basu, A., Kaushik, A., Bhansali, S., & Basu, A. K. (2024). Employing nano-enabled artificial intelligence (AI)-based smart technologies for prediction, screening, and detection of cancer. *Nanoscale*.
16. Yigitcanlar, T., Desouza, K. C., Butler, L., & Roozkhosh, F. (2020). Contributions and risks of artificial intelligence (AI) in building smarter cities: Insights from a systematic review of the literature. *Energies*, *13*(6), 1473.
17. Shi, Q., Dong, B., He, T., Sun, Z., Zhu, J., Zhang, Z., & Lee, C. (2020). Progress in wearable electronics/photonics—Moving toward the era of artificial intelligence and internet of things. *InfoMat*, *2*(6), 1131-1162.
18. Baduge, S. K., Thilakarathna, S., Perera, J. S., Arashpour, M., Sharafi, P., Teodosio, B., ... & Mendis, P. (2022). Artificial intelligence and smart vision for building and construction 4.0: Machine and deep learning methods and applications. *Automation in Construction*, *141*, 104440.
19. Retico, A., Avanzo, M., Boccali, T., Bonacorsi, D., Botta, F., Cuttone, G., ... & Talamonti, C. (2021). Enhancing the impact of Artificial Intelligence in Medicine: A joint AIFM-INFN Italian initiative for a dedicated cloud-based computing infrastructure. *Physica Medica*, *91*, 140-150.
20. Qayyum, A., Butt, M. A., Ali, H., Usman, M., Halabi, O., Al-Fuqaha, A., ... & Qadir, J. (2023). Secure and trustworthy artificial intelligence-extended reality (AI-XR) for metaverses. *ACM Computing Surveys*.

21. Geng, J. (2023). Taking Computation to Data: Integrating Privacy-preserving AI techniques and Blockchain Allowing Secure Analysis of Sensitive Data on Premise.
22. Miyajima, H., Shigei, N., Miyajima, H., & Shiratori, N. (2022). Machine Learning with Distributed Processing using Secure Divided Data: Towards Privacy-Preserving Advanced AI Processing in a Super-Smart Society. *Journal of Networking and Network Applications*, *2*(1), 48-60.
23. Aithal, P. S. (2023). Advances and new research opportunities in quantum computing technology by integrating it with other ICCT underlying technologies. *International Journal of Case Studies in Business, IT and Education (IJCSBE)*, *7*(3), 314-358.
24. Ronaldo, R., Arora, T. K., Agarwal, S., Lobanova, A., Vladimirovna, V. T., & Yadav, A. S. (2022, November). AI Based Periodic Forecasting Rate Prediction with Secured Optimized Cryptographic Method Sales Forecasting in Retail Business Sector. In *2022 International Interdisciplinary Humanitarian Conference for Sustainability (IIHC)* (pp. 1040-1046). IEEE.
25. Hamza, R. (2023, October). Homomorphic Encryption for AI-Based Applications: Challenges and Opportunities. In *2023 15th International Conference on Knowledge and Systems Engineering (KSE)* (pp. 1-6). IEEE.