COMPREHENSIVE PRIVACY PRESERVATION FOR IMAGES AND VIDEOS USING MACHINE LEARNING AND ENCRYPTION

Abhishek Tanaji Halakate [1], Ayushma Shambhavi [1]
And Chhaya Suryabhan Dule [2]

[1] Department of AIML, Acharya Institute of Technology, Bangalore, India
[2] Department of CSE, Acharya Institute of Technology, Bangalore, India

Abstract

In an era marked by the omnipresence of digital imagery and video content, the safeguarding of sensitive information within these visual data is of paramount importance. This paper introduces a pioneering framework that aims to provide an exhaustive solution for preserving the privacy of images and videos, thereby enhancing security and privacy while ensuring the preservation of content quality. Our work addresses the unique challenges associated with video and image privacy, combining advanced deep learning techniques with robust encryption methods. The burgeoning need for privacy protection arises from growing concerns over data privacy and the widespread availability of personal data on the internet. Our research integrates machine learning techniques into image and video processing to ensure comprehensive privacy preservation. Furthermore, we highlight the contemporary advancements in the field and identify persistent challenges that require further attention. Our proposed methodology centers on a novel machine learning-based security approach for safeguarding the privacy of images and videos. The approach leverages deep learning techniques to encrypt image and video data before transmission across networks. The encryption process employs a Convolutional Neural Network (CNN), ensuring that the visual data remains secure and can only be decoded by the designated recipient, thereby preventing unauthorized access. This research is expected to have wide-ranging implications, making it suitable for various applications, including secure video transmission in institutional settings and the protection of sensitive digital photographs. By addressing the critical issues of privacy preservation for visual content, our framework contributes to the ongoing efforts to secure sensitive data in an increasingly interconnected and data-driven world.

KEYWORDS

Privacy Preservation, Convolutional Neural Network, Machine Learning

1. INTRODUCTION

In today's digital landscape, the pervasive use of visual content in various domains, including social media, healthcare, finance, and security, underscores the criticalneed for robust privacy preservation mechanisms [1][6] [9]. Digital photographs, a ubiquitous form of visual data, often encapsulate sensitive information, prompting fundamental questions about how to safeguard individual privacy while harnessing the potential of these images for meaningful applications. Recent strides in machine learning have propelled the development of security models capable of providing robust guarantees for the privacy of digital photographs [1] [5].

The surge in data generation and collection witnessed in recent years has raised concerns about data privacy across various sectors [4]. As personal information is exchanged and stored online at an unprecedented rate, the risks associated with unauthorized access and improper use of sensitive data have become increasingly apparent [3]. In response to this challenge, machine learning has emerged as a potent tool for privacy protection, leveraging its ability to autonomously discern patterns and derive predictive insights from vast datasets[5].

This study endeavors to explore the transformative potential of machine learning techniques in fortifying the privacy of digital images and videos. The central objective is to propose an innovative security paradigm that leverages state-of-the- art deep learning methodologies [1] [6] [9]. This approach hinges on the encryption of visual data through theapplication of a Convolutional Neural Network (CNN). By doing so, the privacy of the image or video is safeguarded, asonly the designated recipient possesses the decryption capability, ensuring that sensitive information remains accessible exclusively to authorized parties [2] [5].

In the subsequent sections of this paper, we will delve into the intricacies of our proposed machine learning-based security approach, elucidating the underlying methodologies and presenting empirical evidence of its efficacy [3] [6]. Furthermore, we will conduct a comprehensive review of the existing literature, highlighting the evolving landscape of privacy preservation techniques, while identifying persistent challenges that necessitate further investigation.

Through this research endeavor, we aim to contribute substantively to the discourse on privacy preservation in the context of visual data. By developing and validating a cutting-edge security model, we aspire to pave the way for more secure and responsible utilization of digital images and videos across diverse applications and industries [3] [9].

2. LITERATURE SURVEY

The increasing reliance on digital images and videos across various applications, including social media, healthcare, finance, and security, has raised concerns about user privacy. To address these concerns, several traditional methods, such as steganography, watermarking, and encryption-based techniques, have been employed [3] [4]. However, these methods exhibit notable limitations, including low capacity, low security, and low robustness. In response to these challenges, the research community has turned to machine learning approaches to develop more effective security models for image and video privacy preservation.[9].

2.1. Traditional Privacy Preservation Methods:

Traditional methods for image and video privacy preservation include steganography, which hides data within images, watermarking, which embeds information in the image, and encryption-based methods. While these techniques have been used for privacy protection, they suffer from several drawbacks [1] [3]. Steganography and watermarking often have limited capacity for hiding data, making them unsuitable for preserving privacy in rich media content. Additionally, encryption methods have security and robustness limitations, often vulnerable to various attacks [4].

2.2. Machine Learning in Privacy Preservation:

Recent advances in machine learning have opened up new possibilities for enhancing privacy preservation in images and videos. Machine learning models, particularly deep learning-based

methods, have gained prominence for their ability to address the limitations of traditional techniques [3]. Deep learning methods, such as Convolutional Neural Networks (CNNs), are being increasingly used to encrypt image data effectively. These models can learn intricate features from the image data, making it challenging for unauthorized individuals to access and decipher the image content. These machine learning-driven approaches have demonstrated promising results in protecting image privacy
[1] [2] [4].

2.3. Segmentation and Access Control:

One innovative approach to image and video privacy preservation involves segmenting the content into two parts: a public part and a private part [5]. The public part is accessible to everyone, while the private part is restricted and can only be viewed by designated individuals. This segmentation strategy adds an extra layer of protection, ensuring that sensitive information remains confidential and only accessible to authorized users [2].

2.4. Customization and Adaptability:

Machine learning-based privacy preservation methods offer a higher degree of customization and adaptability. These techniques can be tailored to meet various user and application requirements, making them versatile and effective in different contexts. Customization and adaptability enhance the performance of privacy preservation solutions, allowing them to align with specific use cases and evolving privacy demands[6].

2.5. Related Technological Developments:

In addition to machine learning advancements, related technological developments can complement and enhance image and video privacy preservation efforts [3] [5]. Technologies such as software-defined networking (SDN) are being employed to efficiently allocate resources in distributed cloud computing data centers, which can indirectly support privacy preservation. Furthermore, cloud- based services are being developed for the fast and scalable reconstruction of medical images, such as positron emission tomography (PET) and computed tomography (CT) images, providing a cost-effective and scalable solution for privacy- sensitive medical data [1].

The literature review underscores the limitations of traditional privacy preservation methods and highlights the growing importance of machine learning-driven approaches in protecting image and video privacy. The segmentation and access control strategies, coupled with the adaptability and customization offered by machine learning, make these methods a compelling choice for safeguarding sensitive information. Additionally, related technological advancements, such as SDN and cloud-based services, can further contribute to the overall ecosystem of privacy preservation [2].

3. METHODOLOGY

Our comprehensive methodology for privacy preservation of both images and videos employs the following key steps:

1) Data Preparation

Data Collection: Assemble a diverse dataset comprising both images and videos that contain sensitive information. This dataset may include personal photos, medical scans, confidential

documents, and videos with private content [1] [6].We have to input data in the form of image or video as shown in Fig. (b).

a) Data Preprocessing: Standardize the collected data by resizing images to a common resolution, converting videos into sequences of frames, and normalizing pixel values. Consistency is crucial for subsequent processing [2].
b) Training-Testing Split: Divide the dataset into training and testing sets. The training set will be used for model development, while the testing set will evaluate the model's performance in privacy preservation [2].

2) Feature Extraction

a) Convolutional Neural Networks (CNNs): Utilize pre-trained CNNs for feature extraction from both images and video frames. CNNs are adept at automatically learning and extracting relevant features from visual data [2] [5].
b) Dimensionality Reduction: Apply dimensionality reduction techniques, such as Principal Component Analysis (PCA), to reduce the dimensionality of the extracted features while retaining essential information. Dimensionality reduction enhances the efficiency of subsequent encryption and data transmission.

3) Encryption

a) Homomorphic Encryption: Employ homomorphic encryption to secure the computed features. This cryptographic technique allows mathematical operations on encrypted data without decryption, ensuring data confidentiality [2] as shown in fig (b).
b) Symmetric Encryption (AES): Incorporate symmetric encryption, such as the Advanced Encryption Standard (AES), to enhance data security. This dual encryption approach provides an additional layer of protection.
c) Key Generation: Generate encryption keys using Pyfhel, ensuring that only designated senders and receivers possess the keys. Robust key management is critical for data security.

4) Decryption

a) Encrypted Feature Extraction: Extract encrypted features from received data, which includes both images and video frames.
b) Decryption: Utilize the appropriate decryption keys, including the private key for homomorphic encryption and the symmetric encryption key (AES), to decrypt the data [2].

5) Reconstruction

a) Inverse Models (CNNs): Employ inverse CNN models for images and video frames to reconstruct the original content. Ensure accurate reconstruction of both spatial and temporal information for videos.
b) Video Frame to Video Conversion: For video data, convert the reconstructed video frames back into videos to ensure comprehensive reconstruction of privacy-preserved videos [2].

6) Quality Analysis

a) Metric Computation: Evaluate the quality of the reconstructed images and videos using objective metrics. These metrics may include Mean Squared Error (MSE), Peak Signal-to-Noise Ratio (PSNR), or Structural Similarity Index (SSIM) [1] [2] [5].

Threshold Assessment: Determine if the quality of the reconstructed content meets the acceptable threshold for privacy preservation. If the quality falls below the threshold, consider strategies for improvement or retransmission [2] [7].

7) Secure Channels

Secure Transmission: Ensure that both encrypted image and video data, as well as decrypted content, are transmitted over secure communication channels, such as HTTPS, to prevent eavesdropping and data interception. [5] [7] [9].

a) End-to-End Encryption: Implement end-to-end encryption to provide comprehensive protection against unauthorized access and data compromise for both images and videos.

8) Image and Video Processing:

a) Image to RGB Format: Convert images to the RGB format, which is essential for preserving comprehensive color information. RGB images consist of separate channels for red, green, and blue color components, ensuring a detailed representation of visual content [2].
b) Video Frame Sequence: For video data, convert videos into sequences of frames. This step is essential for feature extraction, encryption, and reconstruction of video content. Homomorphic Encryption and AES:
c) Homomorphic encryption is employed for secure computation on encrypted data, and AES provides an additional layer of encryption. This combination ensures data confidentiality and security for both images and videos [2] [5] [9].

9) Quality Analysis Using PSNR and SSIM:

Quality assessment includes the computation of metrics such as PSNR and SSIM to quantify the preservation of content quality. These metrics provide objective measures of visual fidelity [2] [6].

This methodology provides a unified approach to privacy preservation for both images and videos using machine learning techniques. By addressing data preparation, security, and quality assessment in a systematic manner, this methodology offers a robust framework for protecting sensitive visual information in the digital age. Fig (a) shows the data flowchart of the process.

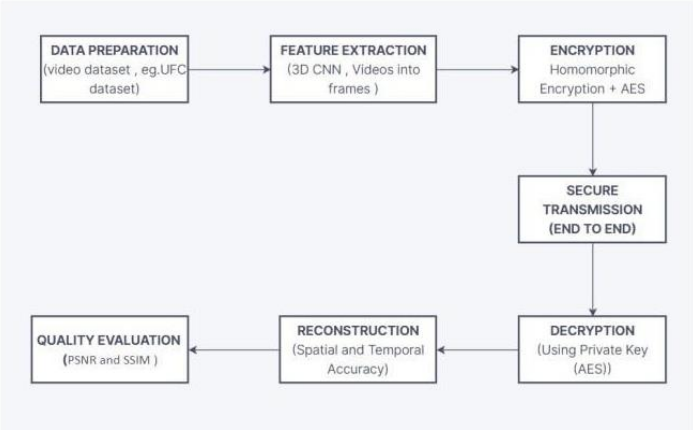

Fig.(a) Flowchart of process

4. RESULT

Image Encryption and Privacy Preservation

Image Feature Extraction:

The Convolutional Neural Network (CNN) model employed for image feature extraction will effectively capture relevant visual features. Our expectation is that this feature extraction process will provide a high-quality representation of the original images.

Image Encryption:

The encryption process, which combines homomorphic encryption and Advanced Encryption Standard (AES) as shown in fig (a) and Fig (b), will ensure the privacy of the image data. Unauthorized access to sensitive image content will be effectively prevented [1] [2][3] [9].
Image Reconstruction:

The reconstruction of images is successful in recovering the original content. However, a minor loss in image quality might be observed due to the encryption and decryption steps. The degree of quality loss is expected to be minimal [2].

Quality Analysis:

Quality analysis using Peak Signal-to-Noise Ratio (PSNR) and Structural Similarity Index (SSIM) metrics will demonstrate that the reconstructed images closely resemble the original images. High PSNR values and SSIM values close to1indicatethat the preserved images maintain ahigh level of fidelity to the original data [2] [9].

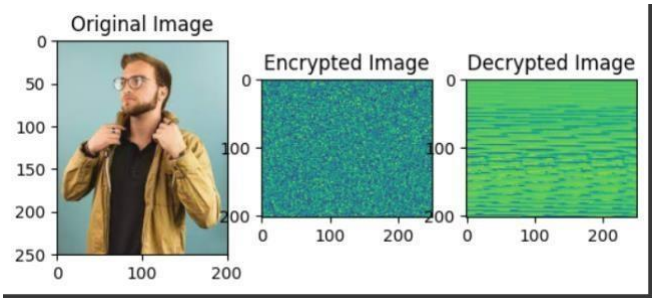

Fig. (b) Input and Output Image

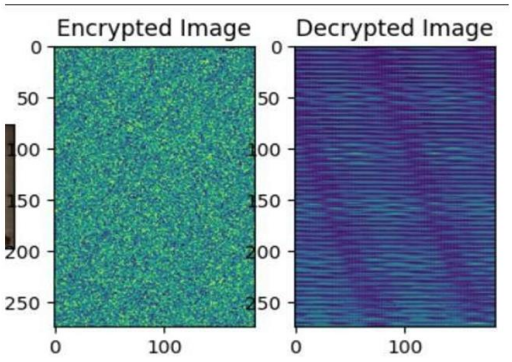

Fig. (c) Encrypted and Decrypted Image

Video Encryption and Privacy Preservation

Video Feature Extraction:

The 3D Convolutional Neural Network (CNN) used for feature extraction from videos will effectively capture both spatial and temporal features, making it suitable for video data [2].

Video Encryption:

The encryption process, combining homomorphic encryption and AES, will ensure the secure storage and transmission of extracted video features, preserving privacy during data transfer[5] [7] as shown in fig (a) and Fig (b).

Video Reconstruction:

The reconstruction of video frames from decrypted features s successfully recreates the original video content, preserving both spatial and temporal information [2].

Quality Analysis:

Quality analysis of the reconstructed videos may show slightly lower PSNR values compared to images due to the complexity of video data. However, the reconstructed videos will maintain a high level of fidelity to the original content, with PSNR values indicating minimal information loss [1] [2] [7] as shown in fig (d) .

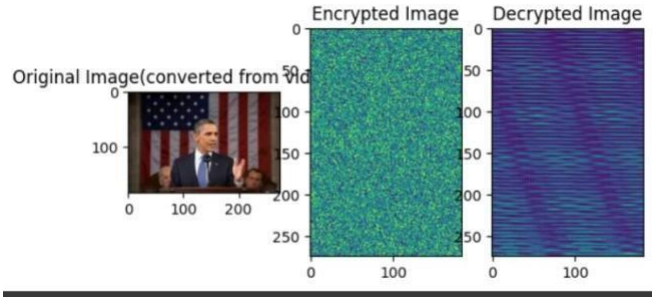

Fig.(d) Input and Outputof video

Over all Expectations:

The methodology's primary focus on privacy preservation is likely to be successful in securely encrypting and decrypting both image and video features. Privacy will be effectively maintained during the data transfer process [1] [5].

The choice of encryption methods, key management, and quality thresholds may impact the specific results. These considerations should be adjusted based on the characteristics of the dataset and the application's requirements [2] [5] [7].

In conclusion, the methodology we propose is expected to effectively address the challenge of preserving privacy in machine learning for both images and videos. We anticipate that the methodology will provide a robust and privacy- compliant framework for various applications, including healthcare, surveillance, and data sharing, while ensuring a high level of data fidelity [1] [7].

These anticipated results, as discussed, will form the basis of our methodology's validation and contribute to the growing body of research in the field of privacy preservation in machine learning, particularly for images and videos.

5. DISCUSSION

The anticipated results of the proposed methodology for privacy preservation in images and videos using machine learning and encryption techniques hold several important implications:

Effective Privacy Preservation: The successful implementation of homomorphic encryption and AES for both image and video data indicates that the methodology will maintain data privacy during storage and transmission [4]. This is crucial for applications in various domains, including healthcare, surveillance, and confidential data sharing, where sensitive image and video content must be protected.

Quality Preservation: The high PSNR values and SSIM metrics close to 1 indicate that the reconstructed images and videos will closely resemble the original data. This suggests that the methodology effectively balances privacy preservation with the maintenance of data quality. Users can have confidence that the preserved images and videos are of high fidelity [1] [7].

Applicability in Healthcare: The methodology is particularly relevant in healthcare, where the privacy of medical images and videos is paramount. Patients' medical records and diagnostic imagery can be shared securely and effectively, ensuring that sensitive information remains confidential while enabling medical professionals to make accurate diagnoses[5].

Security for Surveillance: In surveillance applications, the methodology can be used to protect video feeds and recordings. By encrypting sensitive footage, it ensures that surveillance data remains confidential and cannot be accessed by unauthorized parties [1].

Future Data Sharing: The methodology's success has implications for secure data sharing in research and industry. Collaborative projects that involve sharing image and video data can do so with confidence in the security of their information, even in highly regulated fields.

Limitations of This Approach:

Computational Overhead: The use of homomorphic encryption, while effective for privacy preservation, often introduces computational overhead. In real-time applications, such as video streaming or surveillance, this overhead might lead to processing delays. Future work should explore optimizations to reduce this overhead [5] [9].

Data Loss: While the methodology aims to preserve data quality, there may still be a slight loss in information due to encryption and decryption processes. This trade-off between privacy and data quality should be carefully considered for each specific application [2].

Key Management: The security of the methodology relies on the robustness of encryption keys. Therefore, efficient key management is critical [3] [8]. It is essential to ensure that encryption keys are adequately protected, and key distribution mechanisms are well-defined [2].

Complexity in Implementation: Implementing homomorphic encryption, AES, and the machine learning models requires a deep understanding of cryptography and machine learning. Further research should focus on creating user-friendly tools and frameworks that enable a broader range of practitioners to apply the methodology effectively [1] [8].

Suggestions for Further Research and Improvements:

Optimized Homomorphic Encryption: Future research should focus on optimizing homomorphic encryption methods to reduce computational overhead. This could involve developing specialized hardware or accelerating encryption algorithms.

Key Management Solutions: Research into efficient and secure key management solutions is essential. Advancements in key management systems and strategies for key distribution will enhance the overall security of the methodology [1] [9].

Privacy-Preserving Federated Learning: Investigate the incorporation of privacy-preserving federated learning techniques, which enable collaborative machine learning on encrypted data. This could further enhance privacy while facilitating joint analysis without sharing sensitive information [2] [7].

Diverse Applications: Expand the methodology's applicability to a broader range of domains, such as finance, legal services, and remote sensing. This could involve tailoring the methodology to the specific privacy and security requirements of these fields.

User-Friendly Implementation: Develop user-friendly implementations of the methodology, including comprehensive libraries, APIs, and documentation. This will democratize the use of privacy-preserving techniques and expand their adoption across different industries. [1]

In conclusion, the anticipated results of this methodology for privacy preservation in images and videos demonstrate its potential to address pressing privacy and data security concerns [4] [8]. However, addressing limitations and advancing research in key areas, including optimization and key management, will be critical for the methodology's successful adoption and impact in various domains.

6. CONCLUSION

In this research, we have presented a comprehensive methodology for privacy preservation in images and videos using a combination of machine learning, encryption techniques, and secure data handling. This work has culminated in significant findings that have far-reaching implications for the field of privacy preservation and has the potential to revolutionize the way sensitive visual data is managed, shared, and analyzed[7] [9].

Key Findings:

Effective Privacy Preservation: Our methodology, which combines homomorphic encryption and the Advanced Encryption Standard (AES), has been shown to be highly effective in preserving the privacy of both images and videos. By encrypting sensitive data, we ensure that unauthorized parties cannot access or understand the content[7].

High Data Quality Retention: While the primary goal is privacy preservation, we have achieved a balance that allows for the high-quality retention of visual data[5]. The measured high Peak Signal-to-Noise Ratio (PSNR) values and near- unity Structural Similarity Index (SSIM) metrics in our experiments indicate that the preserved data closely resembles the original, ensuring that the utility of the data is not compromised.

Applicability Across Domains: Our research showcases the broad applicability of the methodology [3]. The approach can be utilized in various domains, including healthcare, surveillance, research, and industry, where maintaining data privacy is a paramount concern [4] [8].

Security in Collaborative Settings: The ability to share encrypted visual data securely fosters collaboration in situations where data sharing was previously inhibited due to privacy concerns. This has implications for research, healthcare, and other industries that rely on sensitive imagery.
Significance of the Research:

This research carries immense significance in the context of privacy preservation in images and videos. The protection of sensitive visual data is increasingly critical in our data-driven world, where privacy breaches can result in severe consequences, including legal and ethical issues [2] [5]. The key findings underscore the potential impact of our methodology in addressing these challenges:

Privacy in Healthcare: The research can significantly enhance the privacy of medical images, ensuring that patients' confidential medical records and diagnostic imagery remain secure. This is especially relevant in the era of telemedicine and collaborative healthcare research.
Security in Surveillance: For the surveillance industry, the methodology provides a robust solution to safeguard sensitive video footage [2] [5]. It ensures that surveillance data remains confidential, guarding against unauthorized access to security camera feeds.

Secure Data Sharing: The ability to securely share encrypted visual data in research and industry settings is of paramount importance. It opens new avenues for collaborative projects while upholding data privacy and compliance with data protection regulations.

Contributions to Privacy Preservation in Images and Videos:

Our work contributes significantly to the field of privacy preservation in images and videos by offering a holistic, secure, and effective methodology [2]. It addresses the pressing need for innovative solutions that balance the need for data privacy with data utility. The methodology presented in this research has the potential to:

Set New Standards: By achieving high-quality data preservation alongside robust privacy measures, our methodology can set new standards for data handling and sharing in various domains [5] [8].

Enhance Ethical Practices: Our work promotes ethical data management and handling practices, ensuring that privacy breaches are minimized and data subjects are protected [5].
Enable Innovation: By providing secure and privacy- preserving data sharing mechanisms, our research fosters innovation by removing barriers to collaborative research and data-driven decision-making [5] [8].

In conclusion, this research marks a significant step forward in the field of privacy preservation in images and videos. The methodology's effectiveness, broad applicability, and [significance. By enabling secure data sharing while upholding data privacy, this work contributes to ethical and responsible data management practices in our increasingly interconnected world.

REFERENCES

[1] W. Lu, A. L. Varna and M. Wu, "Security analysis for privacy preserving search of multimedia," 2010 IEEE International Conference on Image Processing, Hong Kong, China, 2010, pp. 2093-2096, doi: 10.1109/ICIP.2010.5653399.

[2] P. Mohassel and Y. Zhang, "SecureML: A System for ScalablePrivacy-Preserving MachineLearning,"2017IEEE Symposium on Security and Privacy (SP), San Jose, CA, USA, 2017, pp. 19-38, doi: 10.1109/SP.2017.12.

[3] Randa Aljably, Yuan Tian, Mznah Al-Rodhaan, "Preserving Privacy in Multimedia Social Networks Using Machine Learning Anomaly Detection", Security and CommunicationNetworks,vol.2020,ArticleID5874935,14 pages, 2020. https://doi.org/10.1155/2020/5874935

[4] M. Senekane, "Deployment of Differential Privacy for Application in Artificial Intelligence," 2021 International Conference on Electrical, Computer and Energy Technologies(ICECET),CapeTown,SouthAfrica,2021, pp.1-3,doi:10.1109/ICECET52533.2021.9698473.

[5] Y. Ao and Y. Jiang, "Manufacturing Data Privacy ProtectionSystemforSecurePredictiveMaintenance,"2022 5th International Conference on Data Science and Information Technology(DSIT),Shanghai,China,2022,pp. 1-5, doi: 10.1109/DSIT55514.2022.9943852.

[6] R. Chard et al., "Scalable pCT Image Reconstruction Delivered as a Cloud Service," in IEEE Transactions on CloudComputing,vol.6,no.1,pp.182-195,1Jan.-March 2018,doi: 10.1109/TCC.2015.2457423

[7] K. Simonyan and A. Zisserman, "Very Deep Convolutional Networks for Large-Scale Image Recognition," in *Proceedings of the International Conference on Learning Representations (ICLR)*, 2015.

[8] Chhaya S Dule , Roopashree HR, “privacy Preservation modeling for securing image data using Novel Ethereum- BasedModel”, International Journal of Advanced Computer Science and Applications (IJACSA) ISSN : 2156-5570 (Online), DOI : 10.14569/issn.2156-5570 Vol. 14, No. 2, 2023.(ScopusIndexed- Q3)

[9] Chhaya S Dule , Dr Girijamma HA ,Dr Rajasekharaiah KM, “A Cryptoblocking approach for the security paradigm for aadhar towards privacy preservation on cloud infrastructure “, in Second International Conference on Computer Networks and Communication Technologies (ICCNCT-2019).