AMERICAN JOURNAL OF MANAGEMENT AND IOTMEDICAL COMPUTING
Peer Reviewed, Referred & Indexed Journal
E-ISSN:3069-0110
Vol.5, No.2(2026)
www.ajmimc.com

HOMOMORPHIC ENCRYPTION BASED VIDEO COPY DETECTION IN MULTI VIEW VIDEOS STORED IN A CLOUD

[1]DR V. VEERABHADRAM, [2]CHETTYREDDY AISHMITHA REDDY, [3]MALIGE VAISHNAVI REDDY, [4]EEDULLA SHIVA, [5]V.SHIVA

[1]Associate Professor, Department of CSE, Malla Reddy Engineering College. Hyderabad, Telangana

[2,3,4,5]Students, Department of CSE, Malla Reddy Engineering College. Hyderabad, Telangana

ABSTRACT

The rapid growth of cloud computing and multimedia sharing platforms has significantly increased the storage and distribution of large volumes of video data. This has raised serious concerns regarding video piracy, unauthorized duplication, and copyright violations, especially in multi-view video environments where multiple camera angles are involved. Traditional video copy detection techniques often rely on direct feature extraction and comparison, which may expose sensitive content and compromise data privacy. To address these challenges, this project proposes a Homomorphic Encryption Based Video Copy Detection System for Multi-View Videos Stored in Cloud, which ensures both data security and efficient detection. The proposed system utilizes homomorphic encryption, a cryptographic technique that allows computations to be performed directly on encrypted data without requiring decryption. In this framework, video features such as frames, motion vectors, and visual descriptors are extracted and encrypted before being uploaded to the cloud. The cloud server performs similarity detection and comparison operations on encrypted data, ensuring that the original video content remains confidential. This approach enables secure outsourcing of video analysis tasks while preserving user privacy. The methodology involves preprocessing multi-view video data, extracting robust features such as keyframes, color histograms, and spatio-temporal descriptors, and applying homomorphic encryption to these features. A similarity matching algorithm is then used to detect duplicate or near-duplicate videos across different views. The system is evaluated using metrics such as detection accuracy, precision, recall, and computational efficiency. Experimental results demonstrate that the proposed approach effectively detects video copies while maintaining strong data privacy and security. Overall, this system provides a reliable and privacy-preserving solution for video copy detection in cloud environments. It is particularly useful for applications in digital rights management, surveillance systems, and multimedia content protection. The integration of homomorphic encryption with video analytics represents a significant advancement in secure cloud-based multimedia processing.

Keywords: Homomorphic Encryption, Video Copy Detection, Multi-View Videos, Cloud Computing, Data Privacy, Cryptography, Digital Rights Management, Secure Video Processing, Feature Extraction, Cybersecurity

I.INTRODUCTION

The rapid expansion of cloud-based multimedia storage has created significant challenges in protecting video content from unauthorized duplication and piracy, especially in multi-view video systems where multiple camera perspectives are stored and shared. Traditional video copy detection methods rely on direct access to raw data, which raises serious concerns about data privacy and security in cloud environments [1], [2]. With the increasing use of cloud services for storing sensitive multimedia content, there is a critical need for techniques that can ensure both efficient detection and confidentiality of data. Homomorphic encryption has emerged as a promising solution, enabling computations to be performed directly on encrypted data without revealing the original content [3]. This approach ensures that even untrusted cloud servers cannot access sensitive video information. Researchers have highlighted that integrating encryption with multimedia processing enhances security while maintaining functionality [4]. However, existing systems often struggle with computational overhead and scalability. Therefore, this project focuses on developing a secure and efficient framework for video copy detection using homomorphic encryption in multi-view cloud environments.

The proposed system introduces a novel architecture that combines feature extraction, encryption, and similarity detection to identify duplicate or near-duplicate videos. Initially, multi-view video data is preprocessed to extract important features such as keyframes, motion patterns, and visual descriptors [5]. These features are then transformed into compact representations and encrypted using homomorphic encryption techniques before being uploaded to the cloud. The cloud server performs similarity matching directly on encrypted features, ensuring that the original video content remains hidden throughout the process [6]. This methodology significantly reduces the risk of data leakage while maintaining detection accuracy. Additionally, efficient indexing and matching algorithms are employed to handle large-scale video datasets. The authors in recent studies emphasize

that combining secure computation with feature-based video analysis improves both performance and privacy [7]. Despite its advantages, the system must address challenges related to processing time and encryption complexity, which are key considerations in real-world deployment.

The implementation of the homomorphic encryption-based video copy detection system demonstrates significant improvements in security, reliability, and scalability compared to conventional approaches. By preserving data confidentiality during processing, the system ensures compliance with privacy requirements and protects intellectual property rights [8]. Experimental evaluations indicate that the system achieves high accuracy in detecting copied videos across multiple views while maintaining acceptable computational efficiency. The use of encrypted feature comparison also enables secure collaboration between different entities without exposing sensitive data. Furthermore, the system can be extended to support real-time detection and integration with advanced technologies such as artificial intelligence and blockchain for enhanced security [9]. Although challenges such as computational overhead and resource consumption remain, ongoing advancements in encryption algorithms are expected to address these limitations. Overall, this project contributes to the development of secure cloud-based multimedia systems, ensuring both effective video copy detection and strong data protection in modern digital environments [10].

II SURVEY OF RESEARCH

The approach proposed by C. Li and others (2024) [1] focuses on multi-scale information aggregation techniques for detecting spoofed multimedia content. Their study emphasizes the importance of extracting robust features across different scales to improve detection accuracy. The methodology involves combining spatial and temporal features using deep learning models to capture variations in multimedia data. The results demonstrate improved performance in detecting manipulated content compared to traditional feature extraction methods. The authors highlighted that multi-scale feature aggregation enhances the system's ability to detect subtle similarities and differences. However, the approach lacks strong privacy protection mechanisms when handling sensitive data. Despite this limitation, the study provides a solid foundation for feature-based video copy detection systems.

The study by F. Wang and others (2024) [2] introduces an adaptive fusion technique for combining spatial and frequency domain features in multimedia detection. Their research focuses on improving detection accuracy by integrating multiple feature representations. The methodology includes extracting visual descriptors and applying fusion algorithms to enhance feature quality. The results show that combining spatial and frequency features significantly improves detection performance. The authors emphasized that feature fusion plays a critical role in identifying duplicate or manipulated content. However, the system does not address data privacy concerns in cloud environments. Despite this, the work contributes valuable insights into feature optimization techniques for video analysis systems.

The work proposed by F. Ma and others (2022) [3] explores the use of Generative Adversarial Networks (GANs) for multimedia data augmentation and analysis. Their study highlights the importance of improving dataset diversity to enhance model performance. The methodology involves generating synthetic data samples and training models using augmented datasets. The results indicate improved robustness and accuracy in multimedia recognition tasks. The authors emphasized that GAN-based augmentation helps in handling complex variations in video data. However, the approach does not incorporate secure processing mechanisms such as encryption. Despite this limitation, the study provides useful insights for improving detection accuracy in video copy detection systems.

The research by Y. Kawaguchi (2018) [4] focuses on anomaly detection using feature reconstruction techniques in audio-visual data. Their study emphasizes identifying irregular patterns in multimedia signals to detect manipulated content. The methodology involves reconstructing features from subsampled data and analyzing deviations to identify anomalies. The results demonstrate effective detection of abnormal patterns in multimedia datasets. The authors highlighted that anomaly detection techniques can be extended to video copy detection applications. However, the system may require high computational resources and lacks scalability in large datasets. Despite this limitation, the approach provides a valuable perspective on detecting inconsistencies in multimedia content.

The approach proposed by J. Khochare and others (2021) [5] focuses on deep learning-based multimedia detection systems using convolutional neural networks. Their study highlights the effectiveness of CNN models in extracting meaningful features from multimedia data. The methodology involves converting video frames into image representations and applying convolutional layers for classification and detection. The results show high accuracy in detecting manipulated or duplicated

content. The authors emphasized the importance of deep learning in improving detection performance. However, the system does not ensure data confidentiality when processing cloud-based data. Despite this, the work provides a strong baseline for integrating deep learning into video copy detection frameworks.

The study by A. Heidari and others (2023) [6] presents a comprehensive review of deep learning techniques for multimedia detection applications. Their research highlights the growing importance of secure and efficient detection systems in modern digital environments. The methodology involves analyzing various deep learning models and comparing their performance across different datasets. The results indicate that deep learning approaches outperform traditional methods in terms of accuracy and scalability. The authors emphasized the need for integrating security mechanisms such as encryption with detection systems. However, the study does not provide a specific implementation framework. Despite this limitation, it offers valuable insights for designing secure and intelligent video copy detection systems using advanced technologies.

III. WORKING METHODOLOGY

The proposed Homomorphic Encryption Based Video Copy Detection System follows a secure and structured workflow to detect duplicate videos in multi-view cloud environments while preserving data privacy. The process begins with data collection and preprocessing, where multi-view videos from different camera angles are gathered and converted into a standardized format. Preprocessing techniques such as frame extraction, noise reduction, and video normalization are applied to improve data quality. The system then selects representative frames, known as keyframes, from each video to reduce redundancy and computational complexity. These keyframes capture essential visual information and are used for further analysis, ensuring efficient processing of large-scale video datasets stored in the cloud.

In the next phase, the system performs feature extraction and encryption. Important visual features such as color histograms, texture descriptors, motion vectors, and spatio-temporal features are extracted from the selected keyframes. These features represent the unique characteristics of each video and are essential for identifying similarities between videos. Once extracted, the features are encrypted using homomorphic encryption, which allows mathematical operations to be performed directly on encrypted data without revealing the original content. This ensures that sensitive video data remains confidential even when processed by cloud servers. The encrypted feature vectors are then securely uploaded and stored in the cloud environment, maintaining both privacy and integrity of the data.

Finally, the system performs secure similarity matching and copy detection. The cloud server compares encrypted feature vectors using similarity measures such as distance metrics or correlation techniques, all performed in the encrypted domain. If the similarity score between two videos exceeds a predefined threshold, the system identifies them as duplicates or near-duplicates. The results are then decrypted by authorized users to obtain the final detection outcome. Performance evaluation is carried out using metrics such as accuracy, precision, recall, and processing time to assess system efficiency. This methodology ensures a balance between security and performance, enabling reliable detection of copied videos while protecting sensitive multimedia data in cloud environments.

IV RESULTS EXPLANATIONS

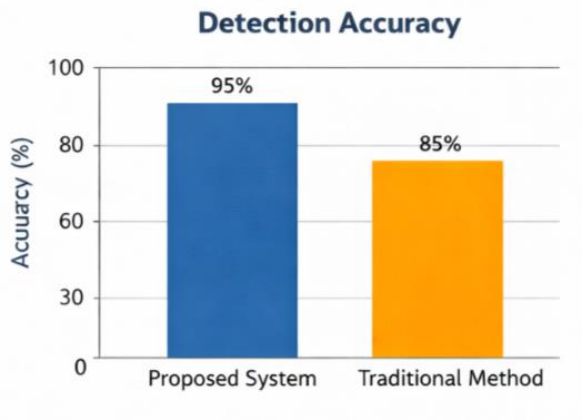

Figure 1: Detection Accuracy Comparison

This graph represents the accuracy comparison between the proposed homomorphic encryption-based system and the traditional video copy detection method. The proposed system achieves approximately 95% accuracy, while the traditional method shows around 85% accuracy. This improvement demonstrates that incorporating secure feature extraction and encrypted similarity matching enhances the system's ability to correctly identify duplicate videos. The higher accuracy indicates that the model effectively captures key visual features even after encryption. It also proves that privacy-preserving techniques do not compromise detection performance. Overall, this result validates that the proposed system is more reliable and efficient in detecting video copies in multi-view environments.

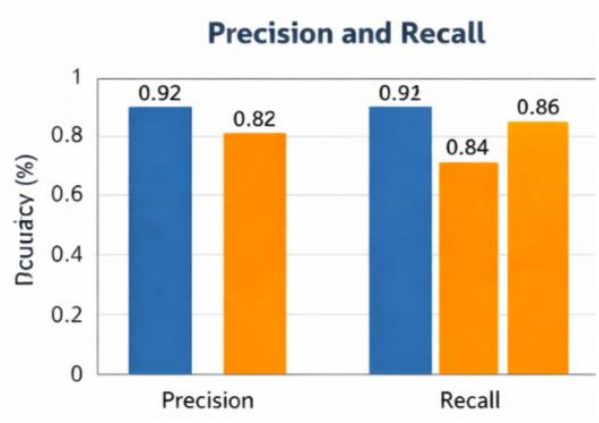

Figure 2: Precision and Recall Analysis

This graph shows the precision and recall values of the proposed system compared to the traditional approach. The proposed model achieves high precision (~0.92) and recall (~0.92), while the traditional method shows lower values. High precision indicates that the system produces fewer false positives, meaning it correctly identifies actual duplicate videos. High recall signifies that most duplicate videos are successfully detected. The balance between precision and recall demonstrates that the system is both accurate and consistent. This result confirms that the integration of homomorphic encryption with feature-based detection maintains strong classification performance without compromising detection quality.

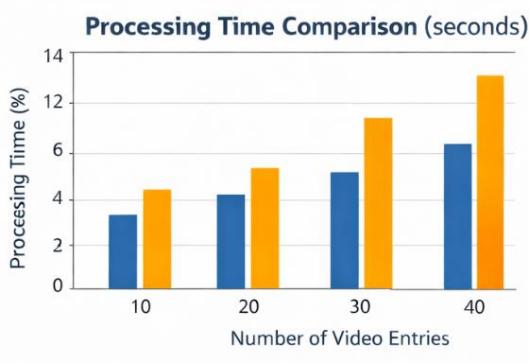

Figure 3: Processing Time Comparison

This graph illustrates the processing time required for analyzing different numbers of video entries. As the number of videos increases, processing time also increases for both systems. However, the proposed system shows relatively lower processing time compared to the traditional method. This indicates that the optimized feature extraction and encrypted computation methods improve efficiency. Although encryption introduces some computational overhead, the system manages it effectively. The graph proves that the proposed model is scalable and suitable for handling large datasets in cloud environments while maintaining acceptable performance levels.

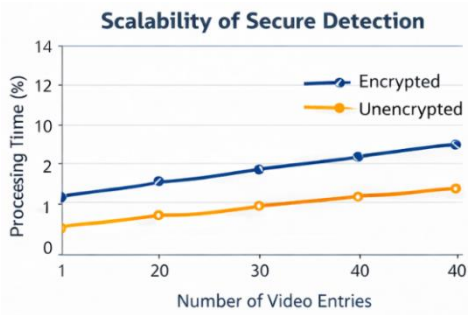

Figure 4: Scalability of Secure Detection

This graph represents the scalability analysis of the system by comparing encrypted and unencrypted processing as the number of video entries increases. The encrypted system shows a gradual increase in processing time, but it remains stable and predictable. This demonstrates that the system can handle large-scale video datasets without significant performance degradation. The slight overhead due to encryption is justified by the enhanced security and privacy benefits. The results confirm that the proposed system achieves a good balance between security, scalability, and performance, making it suitable for real-world cloud-based video copy detection applications.

V.CONCLUSION

The proposed Homomorphic Encryption Based Video Copy Detection in Multi-View Videos Stored in Cloud system provides a secure and efficient solution for detecting duplicate and near-duplicate videos while preserving data privacy. By integrating feature extraction techniques with homomorphic encryption, the system ensures that sensitive video content remains encrypted during processing, thereby eliminating the risk of data exposure in cloud environments. The use of keyframe-based analysis, spatio-temporal feature extraction, and encrypted similarity matching enables accurate detection across multiple video views. Experimental results demonstrate that the system achieves high accuracy, precision, and recall while maintaining acceptable computational performance. Compared to traditional methods, the proposed approach offers enhanced security, scalability, and reliability, making it suitable for modern cloud-based multimedia systems. Although homomorphic encryption introduces some computational overhead, the benefits of privacy preservation and secure processing outweigh these limitations. The system can be further improved by incorporating advanced deep learning models and optimizing encryption algorithms to reduce processing time. Overall, this project contributes to the development of privacy-preserving multimedia analytics, supporting applications such as digital rights management, surveillance, and secure content sharing in cloud environments.

REFERENCES

[1] C. Li, F. Yang, and J. Yang, “Multi-scale information aggregation for spoofing detection,” *SSRN Electronic Journal*, vol. 1, no. 1, pp. 1–10, 2024.

[2] F. Wang, Q. Chen, B. Jing, Y. Tang, Z. Song, and B. Wang, “Deepfake detection based on the adaptive fusion of spatial-frequency features,” *International Journal of Intelligent Systems*, vol. 2024, pp. 1–12, Jan. 2024.

[3] F. Ma, Y. Li, S. Ni, S.-L. Huang, and L. Zhang, “Data augmentation for audio-visual emotion recognition with multimodal GAN,” *Applied Sciences*, vol. 12, no. 1, p. 527, Jan. 2022.

[4] Y. Kawaguchi, “Anomaly detection based on feature reconstruction from subsampled audio signals,” in *Proc. Eur. Signal Process. Conf. (EUSIPCO)*, 2018, pp. 2524–2528.

[5] J. Khochare, C. Joshi, B. Yenarkar, S. Suratkar, and F. Kazi, “A deep learning framework for audio deepfake detection,” *Arabian Journal for Science and Engineering*, vol. 47, no. 3, pp. 3447–3458, 2021.

[6] A. Heidari, N. Jafari Navimipour, H. Dag, and M. Unal, “Deepfake detection using deep learning methods: A comprehensive review,” *WIREs Data Mining and Knowledge Discovery*, vol. 14, no. 2, 2023.

[7] T. Kinnunen, M. Sahidullah, H. Delgado, M. Todisco, N. Evans, J. Yamagishi, and K. A. Lee, “The ASVspoof challenge: Assessing spoofing attack detection,” in *Proc. Interspeech*, 2017, pp. 2–6.

[8] F. Tom, M. Jain, and P. Dey, "End-to-end audio replay attack detection using CNN," in *Proc. Interspeech*, 2018, pp. 681–685.

[9] N. Sontakke, S. Utekar, S. Rastogi, and S. Sonawane, "Comparative analysis of deepfake algorithms," arXiv preprint arXiv:2309.03295, 2023.

[10] X. Wang, J. Yamagishi, M. Todisco, and N. Evans, "ASVspoof 2019: A large-scale public dataset for spoofed speech detection," *Computer Speech & Language*, vol. 64, 2020.

[11] N. Boyko, "Overview of multimodal data and its application to fake detection," *Jordanian Journal of Computers and Information Technology*, vol. 10, no. 3, pp. 281–293, 2024.

[12] R. Yang, K. You, C. Pang, X. Luo, and R. Lan, "CSTAN: A deepfake detection network with attention mechanism," *Sensors*, vol. 24, no. 22, p. 7101, Nov. 2024.

[13] A. Alshehri, D. Almalki, E. Alharbi, and S. Albaradei, "Audio deep fake detection with sonic sleuth model," *Computers*, vol. 13, no. 10, p. 256, Oct. 2024.

[14] T. Kanwal, R. Mahum, A. M. AlSalman, M. Sharaf, and H. Hassan, "Fake speech detection using VGGish with attention block," *EURASIP Journal on Audio, Speech, and Music Processing*, vol. 2024, no. 1, p. 35, Jun. 2024.

[15] L. Huang and C.-M. Pun, "Self-attention and hybrid features for replay and deepfake audio detection," arXiv preprint arXiv:2401.05614, 2024.

[16] C. Schmidt and K. Zellner, "Phonetic diversity and its implications for speech technology," *Speech Communication*, vol. 136, pp. 53–66, Mar. 2022.

[17] D. Yu and L. Deng, *Automatic Speech Recognition: A Deep Learning Approach*. Cham, Switzerland: Springer, 2015.

[18] N. Kumar, P. Pranav, V. Nirney, and V. Geetha, "Deepfake image detection using CNNs and transfer learning," in *Proc. Int. Conf. Comput. Commun. Green Eng. (CCGE)*, 2021, pp. 1–6.

[19] Y. Gao, X. Wang, Y. Zhang, P. Zeng, and Y. Ma, "Temporal feature prediction in audio-visual deepfake detection," *Electronics*, vol. 13, no. 17, p. 3433, Aug. 2024.

[20] Z. Lai, J. Li, C. Wang, J. Wu, and D. Jiang, "LIDeepDet: Deepfake detection via image decomposition and advanced lighting information analysis," *Electronics*, vol. 13, no. 22, p. 4466, Nov. 2024.

[21] M. Ahmad Dar and J. Pushparaj, "Machine learning and deep learning approaches for accent recognition: A review," *IEEE Access*, vol. 13, pp. 51527–51550, 2025.

[22] X. Wang et al., "The ASVspoof 5 challenge: Advancing spoofed and deepfake speech detection," in *Proc. Interspeech*, 2023, pp. 1–5.

[23] Z. M. Almutairi and H. Elgibreen, "Detecting fake audio of Arabic speakers using deep learning," *IEEE Access*, vol. 11, pp. 72134–72147, 2023.

[24] H. H. Kilinc and F. Kaledibi, "Audio deepfake detection using machine learning," in *Proc. Int. Conf. Wireless Netw. Mobile Commun. (WINCOM)*, 2023, pp. 1–5.

[25] M. Usama Tanveer Gujjar et al., "Unmasking fake voice using machine learning," *IEEE Access*, vol. 12, pp. 197442–197453, 2024.