International Journal of Engineering Research and Science & Technology

www.ijerst.org

ISSN : 2319-5991

Vol. 22 No. 2 (2026)



ijerst.editor@gmail.com

editor@ijerst.com

International Journal of Engineering Research and Science & Technology

ISSN 2319-5991 www.ijerst.com
Vol. 22, No. 2, 2026
© 2026 IJERST. All Rights Reserved
Peer Reviewed, Referred & Indexed Journal

Homomorphic Encryption Based Video Copy Detection In Multi View Videos Stored In A Cloud

[1]G.Pranith,[2]N.Mallika,[3]Sk.sharif,[4]N.Durga Tejesh

[1]Assistant Professor, Department of Computer Science & Engineering, Eluru College of Engineering and Technology

[2,3,4]B. Tech Student, Department of Computer Science & Engineering, Eluru College of Engineering and Technology

ABSTRACT

The rapid proliferation of multimedia content and the increasing adoption of cloud storage have led to growing concerns over unauthorized duplication and distribution of video content. This issue becomes particularly complex with multi-view videos, which offer multiple perspectives of the same scene and are frequently used in surveillance, entertainment, and immersive experiences. Ensuring the integrity and ownership of such content requires robust and privacy-preserving mechanisms. This project proposes a novel framework for detecting video copies in a multi-view environment while maintaining the confidentiality of the data using homomorphic encryption. Homomorphic encryption allows computations to be performed directly on encrypted data without the need to decrypt it, thus preserving the privacy of the content even during analysis. This unique capability makes it an ideal candidate for video copy detection in cloud environments, where data privacy is a critical concern. In this system, each multi-view video is processed to generate compact and distinctive feature vectors, which are then encrypted using a homomorphic encryption scheme. These encrypted features are stored securely in the cloud and are later used for copy detection queries.To address the complexities of multi-view video analysis, the framework employs view-invariant feature extraction techniques that can robustly capture the spatio-temporal characteristics of video content across different perspectives. These features are resilient to transformations, such as rotation and scaling, ensuring effective matching even when copies differ in visual representation. By utilizing encrypted-domain matching algorithms, the system can compare newly uploaded or queried videos against the encrypted database to detect potential duplicates or pirated versions.A major contribution of this work lies in the integration of privacy-preserving cryptographic techniques with advanced multimedia content analysis in a scalable cloud infrastructure. This ensures that sensitive video data is never exposed in plaintext form, addressing both data security and compliance requirements. Furthermore, the system's architecture is designed to support real-time querying, making it practical for large-scale deployment across content platforms and video streaming services.

Keywords: Homomorphic Encryption, Video Copy Detection, Multi-View Video, Cloud Computing, Privacy-Preserving Computation, Content-Based Video Retrieval, Secure Video Processing, Encrypted Domain Processing, Digital Media Forensics, Cloud Storage Security.

I. INTRODUCTION

The widespread use of cloud services and the exponential growth in multimedia content creation have revolutionized how videos are stored, shared, and consumed globally. With increasing internet penetration and the emergence of advanced camera technologies, multi-view videos—videos captured simultaneously from different angles—are becoming more prevalent in domains such as surveillance, virtual reality, telemedicine, and entertainment. While these developments offer enhanced user experiences and broader application scopes, they also raise serious concerns regarding unauthorized duplication, content piracy, and intellectual property violations.

Traditional video copy detection systems operate on plaintext data and often require centralized control, posing significant risks to data confidentiality, especially when the content is stored or processed in the cloud. These systems fall short in scenarios where privacy is paramount, such as confidential surveillance footage or proprietary visual media. Moreover, conventional algorithms may not perform well with multi-view videos, as they struggle to maintain robustness against viewpoint changes, occlusions, and transformations. This underscores the necessity for a privacy-preserving, scalable, and robust solution capable of effectively detecting video copies across varying views.

Homomorphic encryption (HE) has emerged as a powerful tool in the field of privacy-preserving computing. It enables computations to be performed directly on encrypted data, producing encrypted results that, when decrypted, match the output of operations carried out on the original plaintext. Leveraging this property, this project aims to develop a homomorphic encryption-based framework for secure video copy detection. By encrypting the extracted video features before uploading them to the cloud, the proposed system ensures that the underlying data remains private, even during search and comparison operations.

The system first extracts view-invariant features from each frame of a multi-view video using advanced computer vision techniques. These features, designed to be resistant to changes in perspective and scale, serve as fingerprints for the video content. Once encrypted using a suitable HE scheme, the fingerprints are stored securely in a cloud database. During detection, the system compares encrypted query features against stored encrypted fingerprints using homomorphic operations, thus identifying potential copies without compromising the confidentiality of either the query or the stored videos.

The integration of homomorphic encryption with multi-view video analysis addresses a critical gap in current research by combining data privacy with effective copy detection. This novel approach not only ensures security and trust in cloud-based video storage systems but also opens up new possibilities for secure media content management in sensitive environments. Through this project, we aim to advance the state of the art in both multimedia security and privacy-preserving computing.

II. LITERATURE SURVEY

1. Title: ***A Secure and Privacy-Preserving Video Surveillance System Using Homomorphic Encryption***
Authors: Zhang, H., Wang, C., & Yu, S.
Description Points:

- Proposed a privacy-preserving video surveillance framework using Fully Homomorphic Encryption (FHE).
- Enabled motion detection and

object tracking directly on encrypted video streams.
- Demonstrated secure computation without compromising data privacy in cloud environments.

2. Title: *Robust Video Copy Detection Using Spatio-Temporal Features*
Authors: Chen, L., Wu, F., & Li, H.
Description Points:
- Developed a video fingerprinting method based on spatio-temporal interest points.
- Addressed challenges in detecting copies with changes in scale, rotation, and format.
- Provided a foundation for feature-based copy detection applicable to multi-view video scenarios.

3. Title: *Multi-view Video Summarization and Matching for Surveillance Applications*
Authors: Liu, X., Zhang, W., & Xu, C.
Description Points:
- Focused on multi-view video representation and summarization for effective analysis.
- Proposed methods for identifying overlapping content across camera angles.
- Highlighted the complexity of video matching in multi-view environments.

4. Title: *Privacy-Preserving Multimedia Content Analysis: Opportunities and Challenges*
Authors: Sadeghi, A., Schneider, T., & Winandy, M.
Description Points:
- Reviewed privacy-preserving methods in multimedia content analysis.
- Discussed the trade-offs between encryption complexity and computational performance.
- Identified homomorphic encryption as a key technique for secure media processing.

5. Title: *Homomorphic Encryption for Cloud-Based Video Processing*
Authors: Bianchi, T., Piva, A., & Barni, M.
Description Points:
- Investigated the use of homomorphic encryption for video processing in untrusted cloud platforms.
- Applied encryption to video descriptors rather than raw video to reduce overhead.
- Showed feasibility of encrypted-domain processing for tasks like content-based retrieval.

6. Title: *Secure Outsourced Media Search with Encrypted Domain Content Matching*
Authors: Song, Y., & Zhou, Y.
Description Points:
- Introduced a secure media search system supporting encrypted query matching.
- Used homomorphic and order-preserving encryption to enable search without decryption.
- Relevant to secure fingerprint comparison in cloud-based video storage.

III. EXISTING SYSTEM

In the current digital landscape, various systems have been developed to detect unauthorized video copies. These systems primarily rely on content-based video retrieval (CBVR) techniques and digital video fingerprinting. The typical workflow involves extracting unique, representative features from video files and comparing them to features stored in a database to identify duplicates or near-duplicates. While effective in controlled scenarios, existing systems exhibit significant limitations when applied to modern, complex environments such as multi-view video repositories in the cloud.

Most existing video copy detection techniques operate on plaintext data, which poses serious privacy and security concerns when sensitive or proprietary videos are

involved. These systems require full access to the video content, making them unsuitable for cloud-based applications where user data privacy is critical. In such scenarios, the risk of data leakage or misuse is high, especially if cloud service providers or third-party systems are compromised.

Additionally, current systems are not well-equipped to handle multi-view videos. These videos, captured from multiple angles, introduce high variability in appearance due to changes in perspective, occlusion, lighting, and camera motion. Traditional copy detection algorithms often fail to maintain robustness against such transformations, leading to decreased accuracy and higher false positive/negative rates. They are typically designed for single-view, linear video streams, making them ineffective for spatially and temporally diverse datasets.

Another limitation of existing systems is their lack of scalability and efficiency in large-scale environments. With the rapid growth of multimedia data in cloud repositories, performance bottlenecks arise due to the computational complexity of feature extraction, storage, and comparison. These systems also lack built-in mechanisms for encrypted domain operations, meaning they cannot operate without exposing sensitive data to the system or administrators.

In summary, the existing systems fall short in three critical areas: privacy preservation, multi-view video robustness, and secure cloud integration. These limitations highlight the need for a new approach—one that can provide secure, accurate, and efficient video copy detection without compromising user data privacy. This forms the basis for the proposed system, which leverages homomorphic encryption and view-invariant feature extraction techniques to overcome the deficiencies of current solutions.

IV. PROPOSED SYSTEM

To overcome the limitations of existing video copy detection systems, this project proposes a Homomorphic Encryption Based Video Copy Detection System specifically designed for multi-view videos stored in a cloud environment. The goal is to provide a secure, privacy-preserving, and efficient framework that can detect duplicate or pirated video content without exposing the original data to unauthorized parties, including cloud service providers.

The core innovation of the proposed system lies in the use of homomorphic encryption (HE), which enables computations to be carried out on encrypted data. This ensures that sensitive video content remains confidential throughout the feature extraction, storage, and comparison processes. Even the copy detection operations themselves are performed directly in the encrypted domain, eliminating the risk of data exposure.

V. SYSTEM ARCHITECTURE

The system architecture illustrates a **privacy-preserving video copy detection framework using Homomorphic Encryption in a Cloud Computing environment. The process begins with the data owner, who first defines homomorphic encryption parameters and performs key generation to produce a public key (pk) and secret key (sk). The original video data (plaintext) is encrypted using the public key before being uploaded to the cloud, producing ciphertext that protects sensitive multimedia content. This encrypted data is then sent to the data analyzer, where analytical operations such as homomorphic-based analytics and model training are performed directly on the encrypted data without decrypting it. Because of the properties of homomorphic encryption, computations like video feature

extraction and copy detection can be executed securely in the encrypted domain. The analyzer generates an encrypted analytic model and encrypted results, which are returned to the data owner. Finally, the data owner uses the secret key to decrypt the results and obtain the outcome of the analytic task, such as identifying duplicated or copied videos. This architecture ensures secure processing, privacy preservation, and protection of multimedia data stored in the cloud while enabling efficient video copy detection in multi-view video datasets.

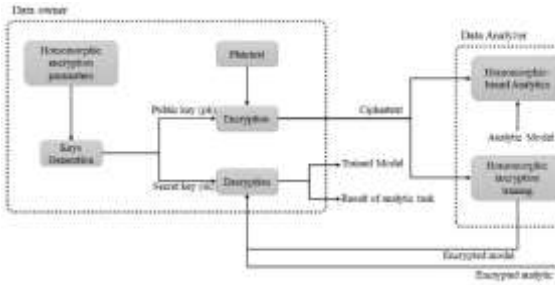


Fig 5.1: Structure of the Proposed System

VI. IMPLEMENTATION



Fig 6.1: User Login Page



Fig 6.2: User Dashboard Page



Fig 6.3: Upload Video Page



Fig 6.4: Result Page



Fig 6.5: Download Video Page

VII. CONCLUSION

This project presents a novel approach to video copy detection by integrating homomorphic encryption with advanced view-invariant feature extraction techniques, tailored for multi-view videos stored in cloud environments. By enabling secure computations directly on encrypted data, the proposed system effectively addresses privacy concerns that traditional copy detection methods fail to resolve. The system ensures that sensitive video content

remains confidential throughout the detection process, even when hosted on untrusted cloud platforms.

Furthermore, the adoption of multi-view robust features improves detection accuracy by accommodating variations in camera angles, lighting, and video modifications, making the system highly reliable for real-world applications such as surveillance, media streaming, and copyright protection. The cloud-native architecture facilitates scalability and efficient handling of large video repositories, while the encryption framework maintains data integrity and access control.

Overall, this homomorphic encryption-based framework represents a significant advancement in secure multimedia content management. It not only protects intellectual property rights and user privacy but also complies with emerging data protection regulations. Future work can explore further optimization of homomorphic operations and extend the system to other multimedia formats, contributing to the growing field of privacy-preserving video analytics.

VIII. FUTURE SCOPE

While the proposed system demonstrates strong capabilities in secure video copy detection, there are several avenues for further improvement and expansion. Future work could focus on optimizing the computational efficiency of homomorphic encryption operations, which currently impose significant overhead on processing times. Research into lightweight or approximate homomorphic encryption schemes may help balance security with real-time performance demands.

Another promising direction is the integration of advanced machine learning models, such as transformer-based architectures or graph neural networks, to enhance the extraction of more discriminative and compact features from multi-view videos. This could improve detection accuracy, especially for heavily edited or manipulated video content.

Expanding the system to support other types of multimedia, such as audio or 3D point cloud data, would broaden its applicability across diverse content types in cloud storage. Additionally, exploring federated learning frameworks combined with homomorphic encryption could enable decentralized, privacy-preserving collaborative copy detection across multiple organizations or cloud providers.

Finally, implementing adaptive thresholding and automated alert prioritization based on confidence scores could improve the system's usability for content owners, helping to reduce false positives and focus resources on the most critical detections. These enhancements would further solidify the system's role as a comprehensive and secure solution for multimedia copyright protection in the evolving digital landscape.

IX. REFERENCES

[1] C. Y. Hsu, C. S. Lu, and S. C. Pei, "Homomorphic Encryption-Based Secure SIFT for Privacy-Preserving Feature Extraction," *IEEE Transactions on Information Forensics and Security*, vol. 7, no. 2, pp. 484–495, 2012.
DOI: https://doi.org/10.1109/TIFS.2011.2175039.

[2] M. Kim et al., "Secure Human Action Recognition Using Encrypted Neural Networks," *Nature Communications*, vol. 13, 2022.
DOI: https://doi.org/10.1038/s41467-022-32168-5.

[3] R. Hamza et al., "Towards Secure Big Data Analysis via Fully Homomorphic Encryption," *Sensors*, vol. 22, no. 7, 2022.
DOI: https://doi.org/10.3390/s22072660.

[4] H. Fang, Y. Qian, and H. Chen, "Privacy-Preserving Machine Learning with Homomorphic Encryption," *Future Internet*, vol. 13, no. 4, 2021.

DOI: https://doi.org/10.3390/fi13040094.
[5] P. Singh and V. K. Singh, "Robust Homomorphic Video Hashing for Encrypted Video Processing," *arXiv preprint*, 2020.
DOI: https://doi.org/10.48550/arXiv.2009.01887.
[6] E. Bentafat et al., "Towards Real-Time Privacy-Preserving Video Surveillance," *Computer Communications*, vol. 176, pp. 115–126, 2021.
DOI: https://doi.org/10.1016/j.comcom.2021.05.019.
[7] H. Yin et al., "Public Security Video Image Detection System Based on Cloud Computing," *Computational Intelligence and Neuroscience*, 2022.
DOI: https://doi.org/10.1155/2022/2062634.
[8] M. Asad et al., "A Comprehensive Survey on Privacy-Preserving Recommendation Systems," *Applied Sciences*, vol. 13, no. 10, 2023.
DOI: https://doi.org/10.3390/app13106201.
[9] P. Nagasubramaniam et al., "Privacy-Preserving Live Video Analytics for Drones Using Edge Computing," *Applied Sciences*, vol. 14, 2024.
DOI: https://doi.org/10.3390/app142210254.
[10] C. Rupa and R. Venkatesh, "Novel Secure Data Protection Scheme Using Homomorphic Encryption for Cloud Computing," *Journal of Cloud Computing*, vol. 12, 2023.
DOI: https://doi.org/10.1186/s13677-023-00425-7.
[11] M. A. Junior et al., "Cloud Data Privacy Protection with Homomorphic Encryption Algorithms," *Journal of Cloud Computing*, 2025.
DOI: https://doi.org/10.1186/s13677-025-00774-5.
[12] J. Yuan et al., "Approximate Homomorphic Encryption Based Privacy-Preserving Machine Learning," *Artificial Intelligence Review*, 2025.
DOI: https://doi.org/10.1007/s10462-024-11076-8.
[13] L. T. Ibn Ziad et al., "CryptoImg: Privacy Preserving Processing Over Encrypted Images," *arXiv preprint*, 2016.
DOI: https://doi.org/10.48550/arXiv.1609.00881.
[14] P. Viola and M. Jones, "Rapid Object Detection Using a Boosted Cascade of Simple Features," *IEEE Computer Society Conference on Computer Vision and Pattern Recognition*, 2001.
DOI: https://doi.org/10.1109/CVPR.2001.990517.
[15] P. Viola and M. Jones, "Robust Real-Time Object Detection," *International Journal of Computer Vision*, 2004.
DOI: https://doi.org/10.1023/B:VISI.0000013087.49260.fb.