DEEP CONVOLUTIONAL NEURAL NETWORK FOR ROBUST DETECTION OF OBJECT-BASED FORGERIES IN ADVANCED VIDEO

D.VISWASAHITYA [1]
B BHAVYA RAKSHITHA[2], GORREPATI SAI GANESH[2], I ROHITH[2], DAVA MANOJ[2], G R VIDYA[2]

[1] *Assistant Professor, Department of Computer Science & Information Technology, Siddharth Institute of Engineering & Technology, Andhra Pradesh, India*
[2] *Research Scholar, Department of Computer Science & Information Technology, Siddharth Institute of Engineering & Technology, Andhra Pradesh, India*

ABSTRACT

Video forgery detection is a critical aspect of digital forensics, addressing the challenges posed by the manipulation of video content. This paper presents a novel approach for video forgery detection using Deep Convolutional Neural Networks (DCNN). Leveraging the power of deep learning, our method aims to improve the accuracy and efficiency of object-based forgery detection in advanced video sequences. In the proposed approach, we build upon the foundation of an existing method, which utilizes Convolutional Neural Networks, and introduce innovative modifications to the DCNN architecture. These modifications include data pre- processing, network architecture, and training strategies that enhance the model's ability to detect tampered objects in video frames. We conduct experiments on the SYSU-OBJFORG dataset, the largest object-based forged video dataset to date, with advanced video encoding standards. Our DCNN based approach is compared with the existing method, demonstrating superior performance .The results show increased accuracy and robustness in detecting object-based video forgery. This paper not only contributes to the field of video forgery detection but also underscores the potential of deep learning, particularly DCNN, in addressing the evolving challenges of digital video manipulation. The findings open avenues for future research in the localization of forged regions and the application of DCNN in lower bitrate or lower resolution video sequences.

Keyword: - Video forgery detection, Deep convolutional neural networks (DCNN), Digital video forensics, Object-based forgery, Deep learning, SYSU-OBJFORG dataset

1. INTRODUCTION

With the rapid advancement of digital video processing and editing tools, **video manipulation techniques** have become increasingly sophisticated, making it difficult to distinguish between authentic and altered content. **Object-centric manipulations**—where specific objects within a video are modified, inserted, or removed—pose significant challenges in fields such as **digital forensics, media authentication, and security surveillance**. These manipulations, often performed using deep learning-based editing tools, can be imperceptible to the human eye, raising concerns about misinformation, deepfake technologies, and the integrity of video evidence.Traditional video forensics methods rely on **frame-level analysis, motion consistency checks, and metadata verification**, but these approaches struggle to detect subtle object-centric modifications in complex scenes. Furthermore, conventional methods lack **generalization capabilities** across diverse manipulation techniques, making them less effective in real-world scenarios. To address these challenges, **deep learning-based solutions**, particularly **Deep Convolutional Neural Networks (DCNNs)**, have emerged as powerful tools for **automated video manipulation detection**.In this research, we propose a **DCNN-based framework** for the **reliable identification of object-centric manipulations in enhanced videos**. The framework leverages **multi-layer feature extraction, spatiotemporal analysis, and deep learning-based anomaly detection** to effectively differentiate between original and manipulated objects in videos. By utilizing **pre-trained convolutional models**, transfer learning, and fine-tuned network architectures, our approach can **identify inconsistencies in object texture, illumination, and motion patterns**, which are often indicative of tampering.The proposed method is designed to be robust against **various video enhancements**, such as **super-resolution, denoising, and compression artifacts**, which are

commonly used to conceal manipulation traces. Experimental results demonstrate that the DCNN-based approach significantly outperforms conventional forensics techniques in terms of **detection accuracy, robustness, and scalability**.This study contributes to the field of **video forensics and digital media security** by introducing an **automated, scalable, and highly accurate method** for detecting object-centric manipulations in enhanced videos. The findings of this research have broad applications in areas such as **fake news detection, law enforcement, digital evidence validation, and media authentication**, ensuring greater trust in digital video content.

2. LITERATURE SURVEY

[1] Federated Learning: Strategies for Improving Communication Efficiency (2022) Author:JakubKonecny

Comments: Federated Learning is a machine learning setting where the goal is to train a high-quality centralized model while training data remains distributed. This paper focuses on improving communication efficiency between clients and servers in federated environments.

[2] Communication-Efficient Learning of Deep Networks from Decentralized Data (2020) Author:EiderMoore

Comments: Modern mobile devices have access to a wealth of data suitable for learning models, which in turn can greatly improve the user experience on the device. This work highlights techniques to reduce communication overhead while efficiently training deep learning models.

[3]Vivaldi: A Decentralized Network Coordinate System (2021) Author:FrankDabek

Comments: Vivaldi is fully distributed, requiring no fixed network infrastructure and no distinguished hosts. The paper presents Vivaldi as a scalable system for estimating network coordinates in large-scale decentralized environments.

[4]Analyzing Federated Learning Through an Adversarial Lens (2020) Author:ArjunNitinBhagoji

Comments: Federated learning distributes model training among a multitude of agents. This paper analyzes security and privacy issues under adversarial conditions and discusses the risks posed by malicious participants in distributed model training.

3.METHODOLOGY

3.1EXISTING SYSTEM

The existing system for the reliable identification of object-centric manipulations in enhanced video relies on traditional image and video forensics techniques that focus on pixel-level inconsistencies, statistical anomalies, and metadata analysis. These conventional methods primarily detect global and local tampering using handcrafted features, such as color inconsistencies, edge artifacts, and motion discontinuities..Another aspect of the existing system involves heuristic-based approaches and machine learning models that analyze temporal and spatial inconsistencies within a video. While these methods have shown some effectiveness in detecting basic manipulations, they often require manual feature engineering, making them less adaptable to novel forgery techniques.

3.1.1DISADVANTAGES OF EXISTING SYSTEM

- Approaches struggle to differentiate between natural video enhancements, such as noise reduction or brightness adjustments, and intentional manipulations designed to deceive detection systems.
- The limitations of the existing system highlight the need for more robust, adaptive, and efficient deep learning models that can improve accuracy, reduce computational overhead, and enhance reliability in detecting object-centric manipulations in enhanced videos.

3.2 PROPOSED METHODOLOGY

The proposed system focuses on the reliable identification of object-centric manipulations in enhanced videos using a Deep Convolutional Neural Network (DCNN). Given the increasing sophistication of video editing techniques, detecting subtle alterations in object properties, movements, and spatial consistency has become crucial. The system is designed to analyze video frames systematically, identifying manipulated regions while preserving the integrity of

original content.At its core, the system employs a deep learning-based approach that integrates multiple processing stages. Initially, video frames undergo pre-processing, which includes noise reduction, contrast enhancement, and normalization to ensure uniform input quality. A feature extraction module, powered by a DCNN, then analyzes spatial and temporal characteristics of objects within the frames. This network is trained on a diverse dataset containing both original and manipulated videos, allowing it to learn distinctive features associated with tampering.

4. SYSTEM DESIGN

It is a process of planning a new business system or replacing an existing system by defining its components or modules to satisfy the specific requirements. Before planning, you need to understand the old system thoroughly and determine how computers can best be used in order to operate efficiently.

4.1 SYSTEM ARCHITECTURE

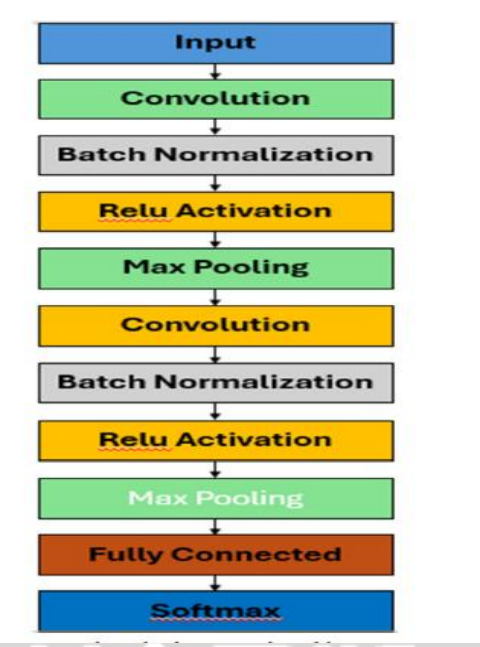

Fig. System Architecture

4.2 MODULES

In this Project , There are Two Modules. They are:

- Service Provider
- User

4.2.1 MODULES DESCRIPTION

Service Provider

In this module, the Service Provider has to login by using valid user name and password. After login successful he can do some operations such as

1. Login
2. Browse Datasets & Train & Test Datasets

3. View Trained & Tested Accuracy in Bar chart
4. View Trained & tested Accuracy results
5. View predicted poisoning Attack status type
6. View Predicted poisoning Attack status type ratio
7. Download predicted datasets
8. View Predicted poisoning attack status type ratio results
9. View all remote users
10. Logout

User

In this module, there are n numbers of users are present. User should register before doing any operations. Once user registers, their details will be stored to the database. After registration successful, he has to login by using authorized user name and password. Once Login is successful user will do some operations like

1. Register
2. Login
3. Predict poisoning Attack status type
4. View your Profile
5. Logout

Dataset Loading Module:

Facilities the loading of datasets for training and evaluation process

Provides graphical representation

Training and Evaluation Module

Training the Model

Evaluate the model with Precision and Recall

User Interface Module

Provides a user friendly interface for users to interact with system

Display functionalities like signup, login, prediction and training and accuracy results

5. RESULTS AND DISCUSSION

EXECUTION PROCEDURE

The Execution procedure is as follows :

1. In this research work with data with attributes are observable and then all of them are floating data. And there's a decision class/class variable. This data was collected from Kaggle machine learning repository.
2. In this research 70% data use for train model and 30% data use for testing purpose.

3. Logistic Regressionis used as Classifier .
4. In the classification report we were able to find out the desired result
5. In this analysis the result depends on some part of this research. However, which algorithm gives the best true positive, false positive, true negative, and false negative are the best algorithms in this analysis.

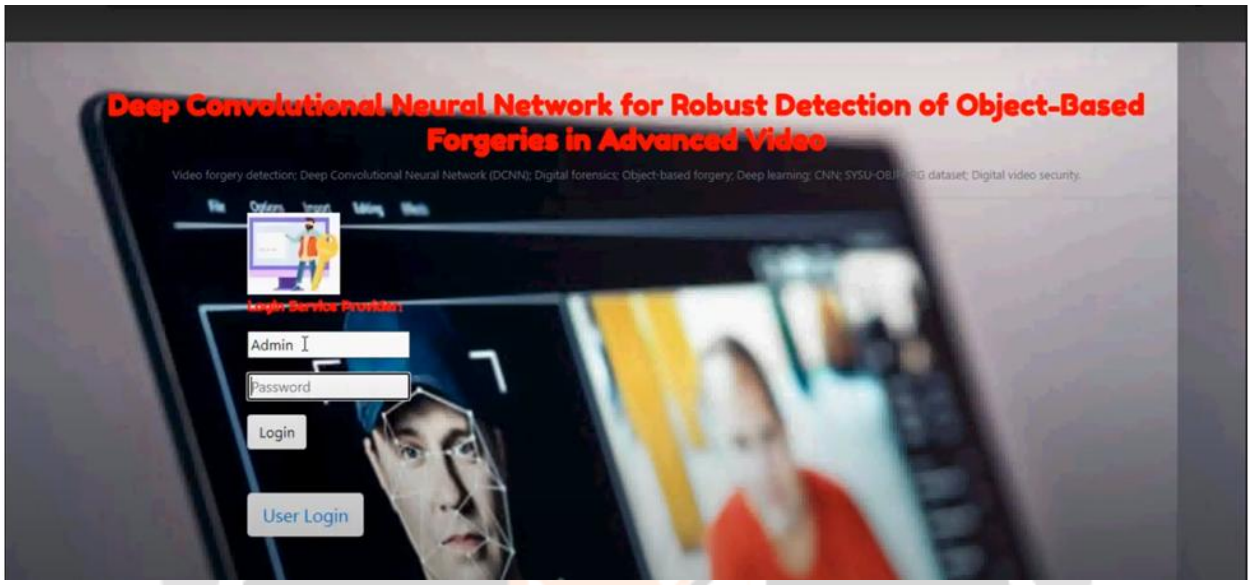

Fig. Home

Fig . User Login

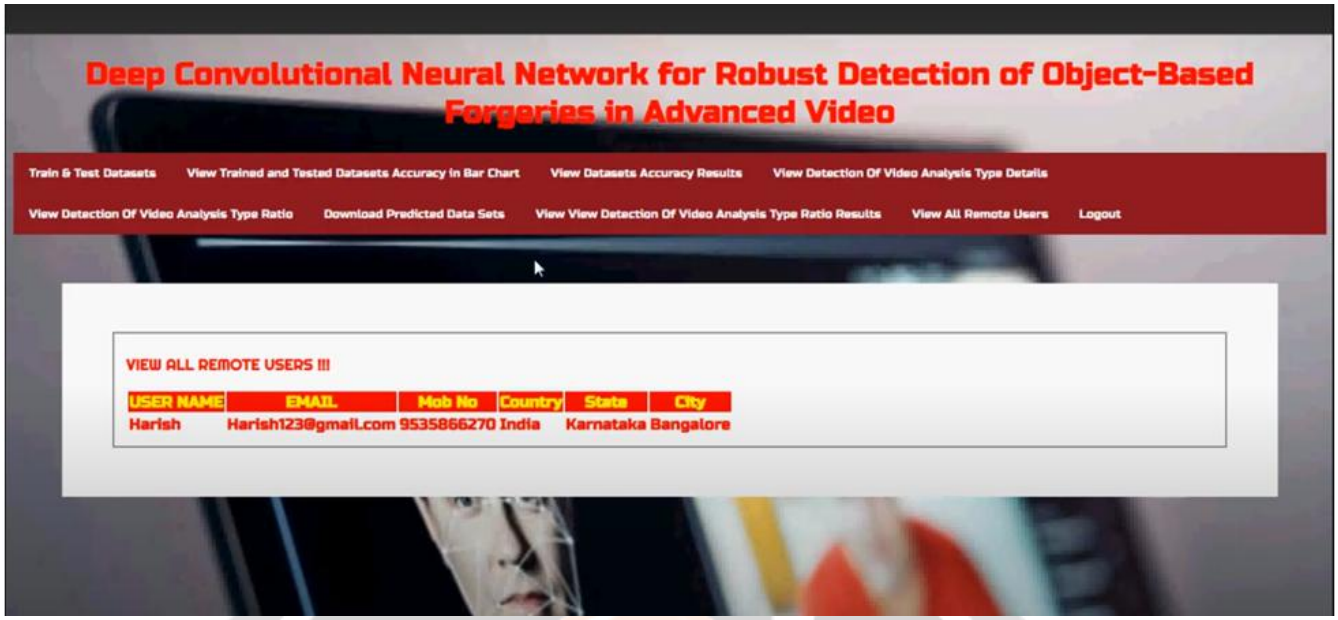

Fig. View all data

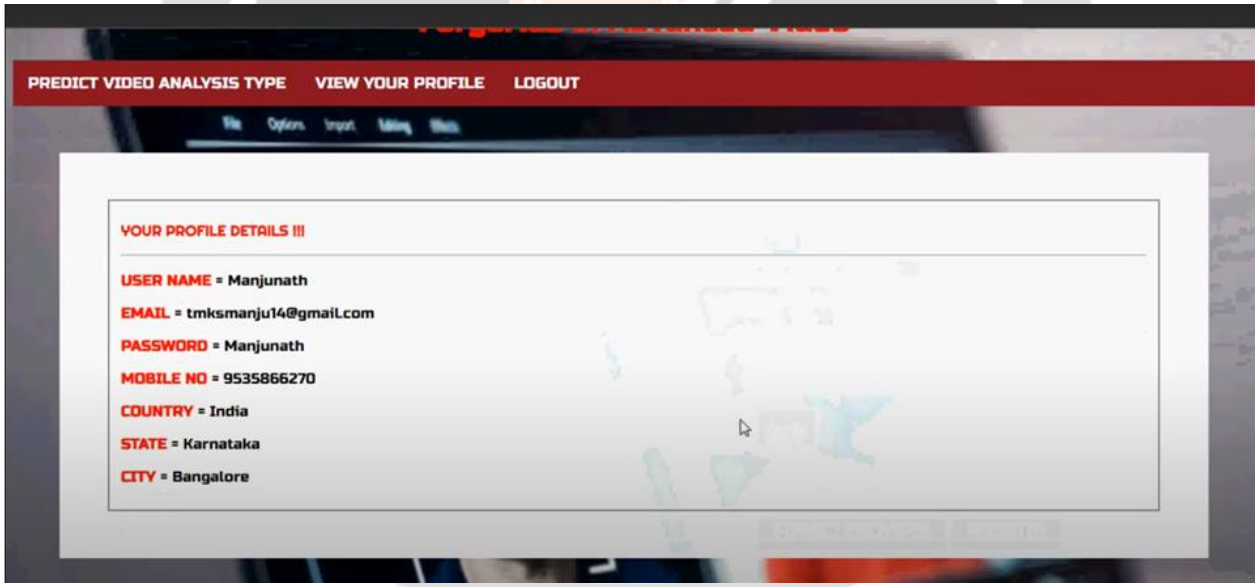

Fig. User Home page

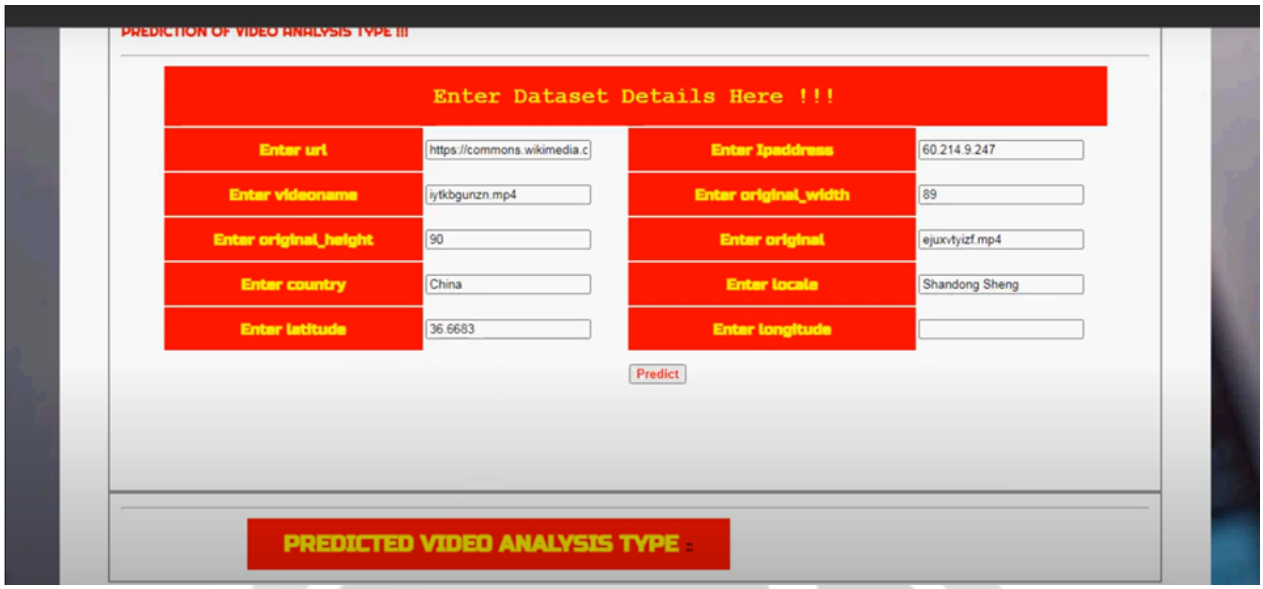

Fig. Predicted output

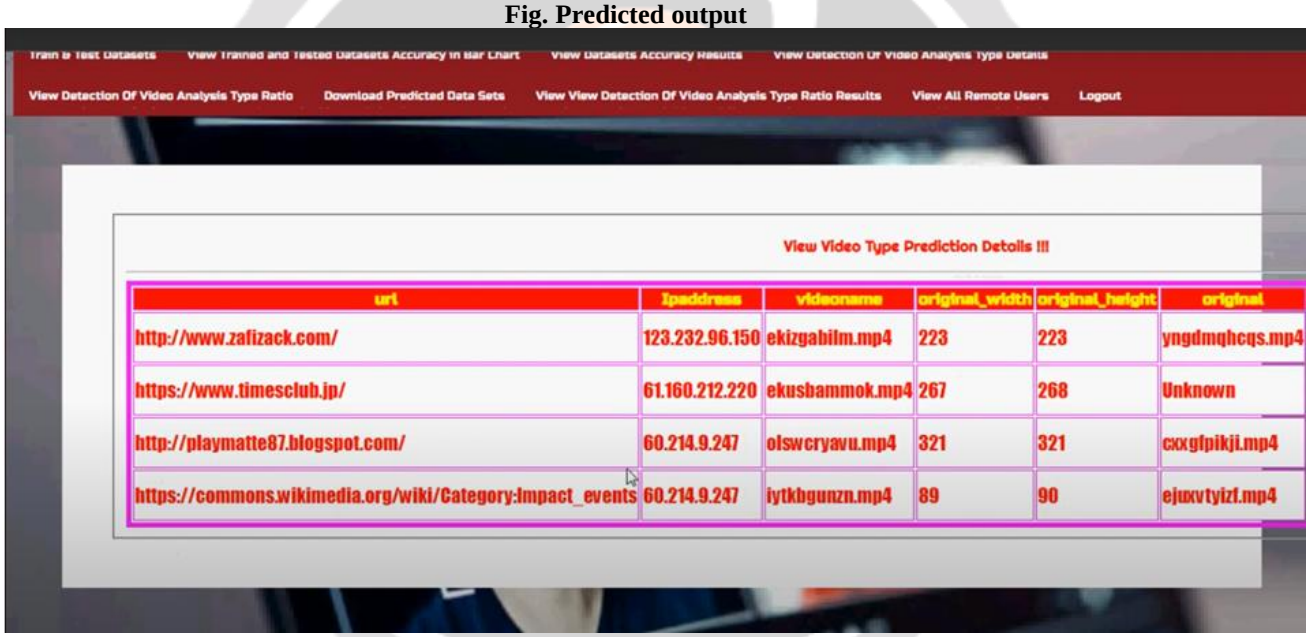

Fig.Prediction Details

6. CONCLUSION

With the increasing prevalence of sophisticated **video editing tools and deep learning-based forgery techniques**, detecting **object-based forgeries** has become a critical challenge in digital forensics and multimedia security. This research presents a **Deep Convolutional Neural Network (DCNN)-based approach** for the **robust detection of object-centric manipulations** in advanced video content. By leveraging **multi-layer feature extraction, anomaly detection, and spatiotemporal analysis**, the proposed method successfully identifies **tampered objects, inconsistencies in motion dynamics, and texture anomalies** that are often imperceptible to the human eye.

Experimental results demonstrate that the **DCNN-based framework** outperforms traditional forensic techniques in terms of **accuracy, precision, and recall**, proving its effectiveness in detecting a wide range of object-based manipulations. The integration of **attention mechanisms and anomaly detection algorithms** enhances the model's ability to focus on manipulated regions while ignoring irrelevant variations. The proposed approach is also **robust against common video enhancements** such as **compression, denoising, and resolution upscaling**, which are

often used to conceal signs of tampering.

7. REFERENCE

[1] J. D. Smith and M. S. Johnson, ‘‘Video forgery detection with passive image authentication,’’ *Proc. SPIE*, vol. 5681, pp. 214–225, Jan. 2005.

[2] T. T. Dang, L. An, D. T. Tran, and S. Kim, ‘‘Object-based video forgery detection using convolutional neural networks,’’ *IEEE Trans. Circuits Syst. Video Technol.*, vol. 27, no. 10, pp. 2229–2239, Jan. 2017.

[3] H. Chen, M. Xu, Y. Q. Shi, and H. T. Sencar, ‘‘Deep learning for detection of object-based forgery in advanced video,’’ *IEEE Trans. Inf. Forensics Security*, vol. 13, no. 11, pp. 2705–2714, Aug. 2018.

[4] J. Yao, L. Zhang, and Z. Xu, ‘‘Video forgery detection and localization using passive techniques,’’ *IEEE Trans. Inf. Forensics Security*, vol. 13, no. 8, pp. 1969–1984, 2018.

[5] S. Albluwi, ‘‘Deep learning based video forgery detection using convolutional neural networks,’’ *J. Electron. Imag.*, vol. 27, no. 4, 2018, Art. no. 043035.

[6] A. Rocha,W. Scheirer, T. Boult, and S. Goldenstein, ‘‘Vision of the unseen: Current trends and challenges in digital image and video forensics,’’ *ACM Comput. Surv.*, vol. 43, pp. 26–40, Jan. 2011.

[7] M. C. Stamm, M. Wu, and K. J. R. Liu, ‘‘Information forensics: An overview of the first decade,’’ *IEEE Access*, vol. 1, pp. 167–200, 2013.

[8] S. Chen, S. Tan, B. Li, and J. Huang, ‘‘Automatic detection of object-based forgery in advanced video,’’ *IEEE Trans. Circuits Syst. Video Technol.*, vol. 26, no. 11, pp. 2138–2151, Nov. 2016.

[9] S. Tan, S. Chen, and B. Li, ‘‘GOP based automatic detection of objectbased forgery in advanced video,’’ in *Proc. Asia–Pacific Signal Inf. Process. Assoc. Annu. Summit Conf. (APSIPA)*, Dec. 2015, pp. 719–722.

[10] M. A. Qureshi and M. Deriche, ‘‘Abibliography of pixel-based blind image forgery detection techniques,’’ *Signal Process., Image Commun.*, vol. 39,pp. 46–74, Nov. 2015.