IJITCE

ISSN 2347- 3657

International Journal of Information Technology & Computer Engineering

Email : ijitce.editor@gmail.com or editor@ijitce.com

International Journal of Information Technology & Computer Engineering
ISSN 2347–3657
Volume 13, Issue 2, 2025
https://doi.org/10.62647/ijitce.2025.v13.i2.pp562-571

A DEEP LEARNING FRAMEWORK FOR ROBUST DETECTION OF OBJECT-BASED FORGERIES IN VIDEO

[1]*Mekala Lakshmi, MCA Student, Department of MCA*

[2] *CH Sri Lakshmi Prasanna, M.Tech,(Ph.D), Assistant Professor, Department of MCA*

[12]*Dr KV Subba Reddy Institute of Technology, Dupadu, Kurnool*

ABSTRACT

A crucial component of digital forensics is video forgery detection, which tackles the difficulties caused by video content tampering. In this study, a unique method for detecting video forgeries using Deep Convolutional Neural Networks (DCNN) is presented. Our approach seeks to increase the precision and effectiveness of object-based counterfeit detection in complex video sequences by using deep learning. The suggested strategy introduces novel changes to the DCNN architecture while building on the framework of an established technique that makes use of convolutional neural networks. The network design, training techniques, and data preparation are some of the changes that improve the model's capacity to identify tampered objects in video frames. We explore with sophisticated video encoding standards using the SYSUOBJFORG dataset, which is the biggest object-based fake video dataset to date. When our DCNN-based technique is compared to the current one, it performs better. The findings demonstrate improved resilience and accuracy in identifying object-based video forgeries. This work highlights the promise of deep learning, namely DCNN, in tackling the changing issues of digital video manipulation in addition to making a contribution to the area of video forgery detection. The results pave the way for further investigation into the localisation of fabricated areas and the use of DCNN in video sequences with lower bitrates or resolutions.

I. INTRODUCTION

The alteration and tampering of video footage has grown more accessible and sophisticated in an era marked by the widespread use of digital video technologies. The need for reliable and effective ways to identify such tampering is greater than ever as video forgery techniques continue to develop. In a variety of fields, such as law enforcement, surveillance, and multimedia forensics, video forgery detection is essential to maintaining the integrity of digital video material and guaranteeing the validity of video-based evidence. A wide range of manipulative techniques, including adding new items to video sequences or deleting old ones, are included in video forgeries, often with the goal of misleading or tricking viewers. Object-based forgeries is a kind of tampering that presents a unique detection problem. The temporal and contextual complexity of video sequences makes traditional techniques for image-based forgery detection unsuitable for video material. The topic of video forgery detection has seen a boom in interest in recent years, which has prompted the creation of several strategies and tactics. The use of deep learning, with a focus on Convolutional Neural Networks (CNNs), has been one prominent development. In computer vision tasks, deep learning—and CNNs specifically—has shown impressive performance, allowing for the fast generation of representations and the automated extraction of high-dimensional features.

In this study, we provide a unique method for detecting video forgeries using Deep Convolutional Neural Networks (DCNNs), primarily focussing on object-based forgeries. Our technique offers novel changes to the DCNN architecture, data preparation, and training methodologies, while building on the basis of an existing methodology that uses CNNs. Improving the model's efficiency and accuracy in identifying

International Journal of Information Technology & Computer Engineering
ISSN 2347–3657
Volume 13, Issue 2, 2025
https://doi.org/10.62647/ijitce.2025.v13.i2.pp562-571

tampered items in video frames is the goal [1]. We do extensive tests on the SYSU-OBJFORG dataset, encoded using advanced video standards, which has been stated to be the biggest object-based forged video dataset to date [2]. We systematically evaluate our DCNN-based strategy to the current method and find that it performs better. The results show increased resilience and accuracy in identifying object-based video forgeries.

In addition to advancing the field of video forgery detection, our work highlights the promise of deep learning—specifically, DCNNs—in tackling the growing problems associated with digital video modification [3]. It draws attention to how DCNNs may improve video forensics' detection skills, which is a positive development in the continuous fight against video manipulation.

The experimental setup, results, and our suggested DCNN-based technique are covered in detail in the next parts of this work. The ramifications of our findings are also discussed. We conclude by outlining the findings and potential paths forward in the realm of video forgery detection.

Over the last several years, passive video forensics has made considerable strides, particularly in identifying object-based forgeries in video sequences. We provide a summary of the body of research on video forensics and forgery detection, based on strategies and tactics that have helped to establish our DCNN-based methodology.

A. Video Forgery Detection

The widespread use of digital video technology has made the detection of video forgeries—particularly object-based forgeries—even more important. Modifying or tampering with video sequences is known as video forgery, and it may have serious repercussions for matters like disinformation, content validity, and legal investigations [1]. The image-based techniques used in conventional video forensics tools were inadequate for handling temporal correlations. These techniques often use a frame-by-frame similarity analysis [8]. Pixel correlations may be utilised to identify assaults that are based on images or videos, according to Bestagini et al. [9]. Lin and Tsay created a passive technique to identify region-level forgeries in video sequences based on spatiotemporal coherence analysis. In other techniques, statistical characteristics that may be utilised to categorise video frames were examined. Chen et al.'s work [11] used support vector machines (SVM) in conjunction with statistical characteristics to identify video forgeries. SIFT features were applied to video frames in order to detect spatial copy-move forgeries, and K-nearest neighbour matching (K-NN) was used in conjunction with SIFT features [12]. These techniques' dependence on manually created characteristics restricted them even if they were successful.

B. Deep Learning in Video Forensics

Because of their exceptional performance in deep learning, convolutional neural networks, or CNNs, are often used in computer vision applications. Because deep neural networks can automatically identify high-dimensional characteristics and develop efficient representations, they may be used for forgery detection [14].

Deep learning methods that have proven effective in video forensics provide the foundation for the identification of object-based forgeries. Deep learning techniques have been used to evaluate a number of video forensics elements, such as camera model identification [13], steganalysis [15], picture recapture forensics [16], image alteration detection [17], and image copy-move forgery detection [18].

Automatic feature learning has replaced human feature engineering with the advent of deep learning-based methods, particularly CNNs. Unlike conventional approaches that depend on manually created features, our DCNN-based model is built to extract intricate features straight from picture patches.

II. LITERATURE SURVEY

International Journal of Information Technology & Computer Engineering
ISSN 2347–3657
Volume 13, Issue 2, 2025
https://doi.org/10.62647/ijitce.2025.v13.i2.pp562-571

detection of video forgeries using passive image authentication.

Johnson, M. S., and Smith, J. D.

The ability of video forgeries to propagate misinformation, distort the content, or fabricate a story has made it a major problem in recent years. The development of technology has made it simpler to produce videos that appear genuine and can be used to trick viewers. Finding out whether a video has been edited or modified in any manner is known as video forgery detection. Inter-frame video forgeries come in a variety of forms, including frame insertion, deletion, duplication, and shuffling. A kind of video manipulation known as "frame insertion forgery" involves adding additional frames to a video sequence with the intention of misleading viewers or changing the movie's content. We provide a multi-level passive video frame insertion forgery detection technique in this study. Using temporal perceptual information measurement, also known as temporal information, we ascertain temporal properties between neighbouring frames at the first level. To find counterfeit spots and identify outliers, the z-score is computed. A structural similarity index measurement (SSIM) is computed for added frames that fall between identified sites in the second stage of authentication. To confirm that the added frames are from a different video, their SSIM is compared to the original video frames. The TDTVD dataset is used to assess the approach. With an accuracy of 94.44%, the experimental results demonstrate that the suggested approach outperforms the others in identifying frame insertion forgeries. The suggested technique is contrasted with other methods currently used in the area of video forgery detection.

detection of object-based video forgeries using convolutional neural networks.

Kim, S., Tran, D. T., An, L. X., and Dang, T. T.

Nowadays, the most popular and convenient way to consume digital multimedia information is in large quantities. Images, text, video, music, and other media form the foundation of this digital interactive environment. The danger of creating false information and fabricating original content is further increased by technological advancements. For an individual, a video is the most reliable source; nonetheless, sophisticated programs may quickly falsify the video material. A scientific method is necessary to preserve the video's validity. In order to detect signs of fraud in surveillance footage, we presented a pixel-based motion residual approach in this study. An optimised CNN with 92% accuracy was then tested. The suggested network is new since it optimises trainable parameters, reduces network complexity, operates quickly, and is computationally inexpensive without sacrificing accuracy.

Convolutional neural networks for video forgery detection based on deep learning.

Albluwi, S.

A crucial component of digital forensics is video forgery detection, which tackles the difficulties caused by video content tampering. In this study, a unique method for detecting video forgeries using Deep Convolutional Neural Networks (DCNN) is presented. Our approach seeks to increase the precision and effectiveness of object-based counterfeit detection in complex video sequences by using deep learning. The suggested strategy introduces novel changes to the DCNN architecture while building on the framework of an established technique that makes use of convolutional neural networks. The network design, training techniques, and data preparation are some of the changes that improve the model's capacity to identify tampered objects in video frames. We explore with sophisticated video encoding standards using the SYSU-OBJFORG dataset, which is the biggest object-based forged video dataset to date. When our DCNN-based technique is compared to the current one, it performs better. The findings demonstrate improved resilience and accuracy in identifying object-based video forgeries. This work highlights the promise of deep learning, namely DCNN, in tackling the changing issues of digital

International Journal of Information Technology & Computer Engineering
ISSN 2347–3657
Volume 13, Issue 2, 2025
https://doi.org/10.62647/ijitce.2025.v13.i2.pp562-571

video manipulation in addition to making a contribution to the area of video forgery detection. The results pave the way for further investigation into the localisation of fabricated areas and the use of DCNN in video sequences with lower bitrates or resolutions.

Detecting and locating video forgeries using passive methods

Zhang, L., Xu, Z., and Yao, J.

With today's easy-to-use editing tools, movies may be captured and edited with ease. False propaganda may be created by sharing these films on social media. The texture and micro-patterns of the frames change throughout the spatial forging process, as seen by the difference between two successive frames. This discovery has led to the proposal of a technique for localising forged frames and detecting forged video segments. The inconsistency buried in the frames as a result of forgery is modelled using a novel descriptor that makes use of the Chrominance value of Consecutive frame Difference (CCD) and Discriminative Robust Local Binary Pattern (DRLBP). To determine if a pair of successive frames is forged, Support Vector Machines (SVM) are used. The video segment is anticipated to be forged and the forged frames are localised if at least one pair of consecutive frames is found to be forged. Extensive tests are conducted to verify the method's performance on a pooled dataset of films that were altered using splicing and copy-move techniques. The video accuracy is 98.32 percent, while the detection accuracy on a big dataset is 96.68 percent. Even with cross-dataset validation, the comparison demonstrates that it performs better than the state-of-the-art techniques.

Using deep learning to identify object-based forgeries in sophisticated video

Chen, H., Sencar, H. T., Shi, Y. Q., and Xu, M.

In recent years, passive video forensics has gained a lot of interest. Research on object-based forgery detection is still quite difficult, however, particularly when it comes to counterfeit videos that are encoded using sophisticated codec frameworks. In this work, we provide a deep learning-based method for identifying object-based forgeries in sophisticated videos. A convolutional neural network (CNN) is used in the deep learning method that is being described to automatically extract high-dimension characteristics from the input picture patches. We allow video frames to pass through three preprocessing layers before to being input into our CNN model, which is different from the conventional CNN models utilised in the computer vision field. They consist of a high-pass filter layer to improve the residual signal left by video forgeries, a max pooling layer to lower the computational cost of image convolution, and a frame absolute difference layer to decrease temporal redundancy between video frames. To get an equal number of positive and negative picture patches prior to training, an asymmetric data augmentation technique has also been developed. Experiments have shown that the suggested CNN-based model with preprocessing layers has produced very good outcomes.

III. SYSTEM ANALYSIS AND DESIGN

EXISTING SYSTEM

The widespread use of digital video technology has made the detection of video forgeries—particularly object-based forgeries—even more important. Modifying or tampering with video sequences is known as video forgery, and it may have serious repercussions for matters like disinformation, content validity, and legal investigations [1]. The image-based techniques used in conventional video forensics tools were inadequate for handling temporal correlations. These techniques often use a frame-by-frame similarity analysis [8]. Pixel correlations might be utilised to identify assaults that are based on images and videos, according to Bestagini et al. [9]. Lin and Tsay created a passive technique to identify region-level forgeries in video sequences based on spatiotemporal coherence analysis.

In other techniques, statistical characteristics that may be utilised to categorise video frames were

International Journal of Information Technology & Computer Engineering
ISSN 2347–3657
Volume 13, Issue 2, 2025
https://doi.org/10.62647/ijitce.2025.v13.i2.pp562-571

examined. Chen et al.'s work [11] used support vector machines (SVM) in conjunction with statistical characteristics to identify video forgeries. SIFT features were applied to video frames in order to detect spatial copy-move forgeries, and K-nearest neighbour matching (K-NN) was used in conjunction with SIFT features [12]. These approaches' dependence on manually created features restricted them even if they were successful.

Because of their exceptional performance in deep learning, convolutional neural networks, or CNNs, are often used in computer vision applications. Because deep neural networks can automatically identify high-dimensional characteristics and develop efficient representations, they may be used for forgery detection [14]. Deep learning methods that have proven effective in video forensics provide the foundation for the identification of object-based forgeries. Deep learning techniques have been used to evaluate a number of video forensics elements, such as camera model identification [13], steganalysis [15], picture recapture forensics [16], image alteration detection [17], and image copy-move forgery detection [18].

Disadvantages

• Data complexity: To identify forgeries in advanced video, the majority of machine learning models now in use need to be able to correctly analyse large and intricate datasets.

• Data availability: In order to provide precise predictions, the majority of machine learning models need a lot of data. The accuracy of the model may degrade if data is not accessible in large enough amounts.

• Inaccurate labelling: The accuracy of the machine learning models that are now in use depends on how well the input dataset was used for training. Inaccurate labelling of the data prevents the model from producing reliable predictions.

PROPOSED SYSTEM

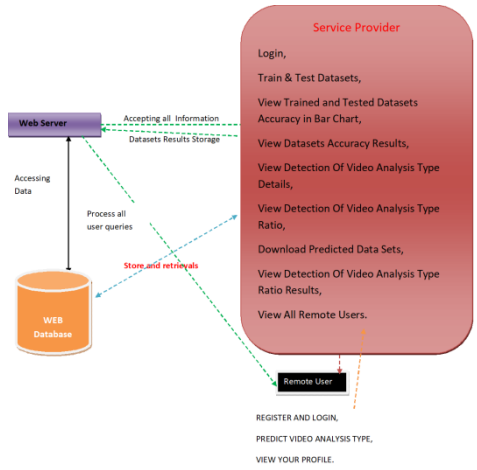
In this study, we provide a unique method for detecting video forgeries using Deep Convolutional Neural Networks (DCNNs), primarily focussing on object-based forgeries. Our technique offers novel changes to the DCNN architecture, data preparation, and training methodologies, while building on the basis of an existing methodology that uses CNNs. Improving the model's efficiency and accuracy in identifying tampered items in video frames is the goal [1]. We do extensive tests on the SYSU-OBJFORG dataset, encoded using advanced video standards, which has been stated to be the biggest object-based forged video dataset to date [2]. We systematically evaluate our DCNN-based strategy to the current method and find that it performs better. The results show increased resilience and accuracy in identifying object-based video forgeries.

Advantages

- In addition to making a contribution to the field of video fraud detection, this research highlights the promise of deep learning—specifically, DCNNs—in tackling the growing problems associated with digital video manipulation [3]. It draws attention to how DCNNs may improve video forensics' detection skills, which is a positive development in the continuous fight against video manipulation.
- The experimental setup, results, and our suggested DCNN-based technique are covered in detail in the next parts of this work. The ramifications of our findings are also discussed. We conclude by outlining the findings and potential paths forward in the realm of video forgery detection.
- The suggested approach for video forgery detection is thorough, using Deep Convolutional Neural Networks (DCNNs) and concentrating especially on object-based counterfeiting.

International Journal of Information Technology & Computer Engineering
ISSN 2347–3657
Volume 13, Issue 2, 2025
https://doi.org/10.62647/ijitce.2025.v13.i2.pp562-571

SYSTEM ARCHITECTURE



IV. IMPLEMENTATION

Modules

Service Provider

The Service Provider must use a working user name and password to log in to this module. He may do many tasks after successfully logging in, including Train & Test Data Sets, See the Accuracy of Trained and Tested Datasets in a Bar Chart View Accuracy Results for Trained and Tested Datasets, Download Predicted Data Sets, View Cyber Attack Prediction Status Ratio, and View Cyber Attack Prediction Status See the results of the Cyber Attack Prediction Status Ratio. See Every Remote User.

View and Authorize Users

The administrator may see a list of all registered users in this module. Here, the administrator may see the user's information, like name, email, and address, and they can also grant the user permissions.

Remote User

A total of n users are present in this module. Before beginning any actions, the user needs register. Following registration, the user's information will be entered into the database. Following a successful registration, he must use his password and authorised user name to log in. Following a successful login, the user may do tasks including registering and logging in, predicting the status of cyberattacks, and seeing their profile.

ALGORITHMS

Decision tree classifiers

Decision tree classifiers are effectively used in a wide range of fields. Their capacity to extract descriptive decision-making information from the provided data is their most crucial characteristic. Training sets may be used to create decision trees. The following is the process for this kind of creation based on the set of objects (S), each of which belongs to one of the classes C1, C2, …, Ck:

Step 1: The decision tree for S has a leaf labelled with the class if every item in S is a member of the same class, such as Ci.

Step 2. If not, let T be a test with the potential results O1, O2,..., On. The test divides S into subsets S1, S2,… Sn, where each item in Si has result Oi for T, because each object in S has a single outcome for T. T serves as the decision tree's root, and we construct a subsidiary decision tree for each result Oi by recursively applying the same process to the collection Si.

Gradient boosting

One machine learning method for classification and regression problems is gradient boosting. Usually decision trees, it provides a prediction model in the form of an ensemble of weak prediction models.[1] [2] The resultant technique, known as gradient-boosted trees, often performs better than random forest when a decision tree is the weak learner.Like other boosting techniques, a gradient-boosted trees model is constructed step-by-step; however, it goes one step further by allowing optimisation of an arbitrary differentiable loss function.

K-Nearest Neighbors (KNN)

- A simple but very effective classification technique that uses a similarity metric
- Non-parametric learning and lazy learning don't "learn" until the test example is provided.

International Journal of Information Technology & Computer Engineering
ISSN 2347–3657
Volume 13, Issue 2, 2025
https://doi.org/10.62647/ijitce.2025.v13.i2.pp562-571

- We use the training data to determine the K-nearest neighbours of any fresh data that has to be classified.

Example

- The training dataset comprises the k-closest examples in feature space, which is defined as a space containing categorisation variables (non-metric variables).
- Learning is based on instances, which also facilitates lazy learning because it may take some time for an instance near the input vector for testing or prediction to occur in the training dataset.

Logistic regression Classifiers

The relationship between a collection of independent (explanatory) factors and a categorical dependent variable is examined using logistic regression analysis. When the dependent variable simply has two values, like 0 and 1 or Yes and No, the term logistic regression is used. When the dependent variable contains three or more distinct values, such as married, single, divorced, or widowed, the technique is sometimes referred to as multinomial logistic regression. While the dependent variable's data type differs from multiple regression's, the procedure's practical application is comparable.

When it comes to categorical-response variable analysis, logistic regression and discriminant analysis are competitors. Compared to discriminant analysis, many statisticians believe that logistic regression is more flexible and appropriate for modelling the majority of scenarios. This is due to the fact that, unlike discriminant analysis, logistic regression does not presume that the independent variables are regularly distributed.

Both binary and multinomial logistic regression are calculated by this software for both category and numerical independent variables. Along with the regression equation, it provides information on likelihood, deviance, odds ratios, confidence limits, and quality of fit. It does a thorough residual analysis that includes diagnostic residual plots and reports. In order to find the optimal regression model with the fewest independent variables, it might conduct an independent variable subset selection search. It offers ROC curves and confidence intervals on expected values to assist in identifying the optimal classification cutoff point. By automatically identifying rows that are not utilised throughout the study, it enables you to confirm your findings.

Naïve Bayes

The supervised learning technique known as the "naive bayes approach" is predicated on the straightforward premise that the existence or lack of a certain class characteristic has no bearing on the existence or nonexistence of any other feature. However, it seems sturdy and effective in spite of this. It performs similarly to other methods of guided learning. Numerous explanations have been put forward in the literature. We emphasise a representation bias-based explanation in this lesson. Along with logistic regression, linear discriminant analysis, and linear SVM (support vector machine), the naive bayes classifier is a linear classifier. The technique used to estimate the classifier's parameters (the learning bias) makes a difference.

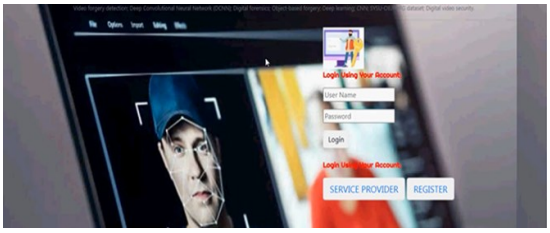
Although the Naive Bayes classifier is commonly used in research, practitioners who want to get findings that are useful do not utilise it as often. On the one hand, the researchers discovered that it is very simple to build and apply, that estimating its parameters is simple, that learning occurs quickly even on extremely big datasets, and that, when compared to other methods, its accuracy is rather excellent. The end users, however, do not comprehend the value of such a strategy and do not get a model that is simple to read and implement.

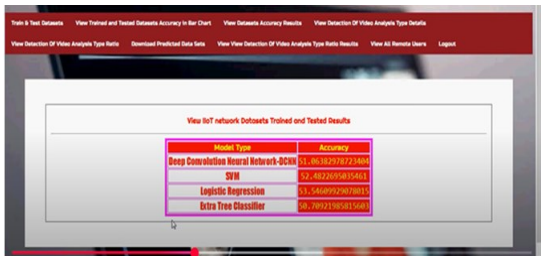
As a consequence, we display the learning process's outcomes in a fresh way. Both the deployment and comprehension of the classifier are simplified. We discuss several theoretical facets of the naive bayes classifier in the first section of this lesson. Next, we use

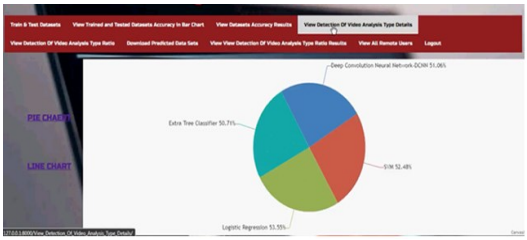
International Journal of Information Technology & Computer Engineering
ISSN 2347–3657
Volume 13, Issue 2, 2025
https://doi.org/10.62647/ijitce.2025.v13.i2.pp562-571

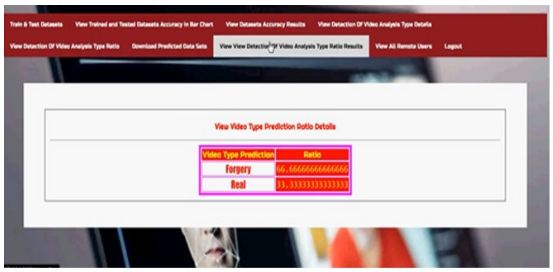
Tanagra to apply the method on a dataset. We contrast the outcomes (the model's parameters) with those from other linear techniques including logistic regression, linear discriminant analysis, and linear support vector machines. We see that the outcomes are quite reliable. This helps to explain why the strategy performs well when compared to others. We employ a variety of tools (Weka 3.6.0, R 2.9.2, Knime 2.1.1, Orange 2.0b, and RapidMiner 4.6.0) on the same dataset in the second section. Above all, we make an effort to comprehend the outcomes.

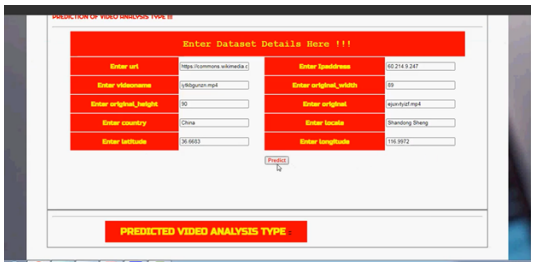
V. SCREEN SHOTS

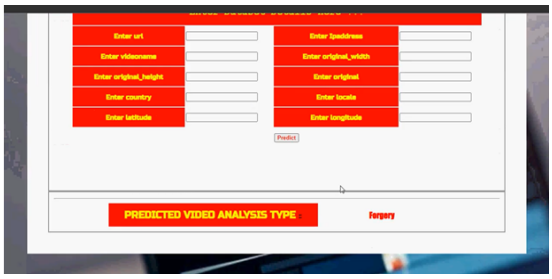


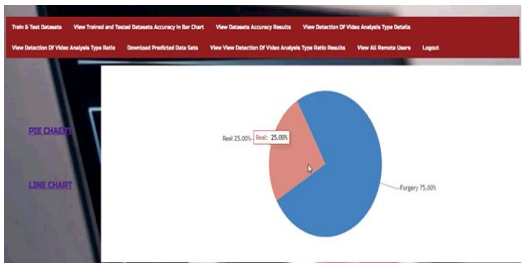












VI. CONCLUSION

This research presents a new method for object-based forgery detection using Deep Convolutional Neural Networks (DCNN). Our method was tested on the SYSUOBJFORG dataset, a large dataset of its type. To summarise our efforts, we have contributed the following:

International Journal of Information Technology & Computer Engineering
ISSN 2347–3657
Volume 13, Issue 2, 2025
https://doi.org/10.62647/ijitce.2025.v13.i2.pp562-571

Model Based on DCNN: In order to capture intricate patterns and representations inside video frames, we suggested a five-layer DCNN model that automatically learns high-dimensional features from picture patches.

Preparing video sequences: Our methodology employs a preprocessing stage that computes absolute differences between successive frames, eliminates temporal redundancy, and improves the evidence of tampering actions in video clips.

Asymmetric Data Augmentation: We developed an asymmetric data augmentation technique to solve the problem of unbalanced data, which enabled us to produce a more balanced dataset for DCNN model training.

Max Pooling and High Pass Filter: Our model was able to withstand changes in motion residual values by using a max pooling technique to decrease the resolution of input picture patches and a high-pass filter to boost residual signals resulting from video fraud.

Our studies' results showed that our DCNN-based strategy outperformed more conventional techniques that relied on manually created features. Our method performed very well, achieving a 100% Video Accuracy (VACC). Furthermore, it performed better than Chen et al.'s approach, which detected object-based forgeries in video sequences using steganalysis feature sets. In the future, we want to enhance the localisation of forged areas inside tampered video frames. Additionally, we want to create a transfer learning method that can identify object forgeries in video sequences with low bitrate and poor quality.

In order to enhance video forensics, we investigate in this work the potential of deep learning, namely DCNNs, for the identification of object-based forgeries in complex video sequences.

REFERENCES

[1] Smith, J. D., & Johnson, M. S. (2005). Video forgery detection with passive image authentication. In Proceedings of SPIE - The International Society for Optical Engineering (Vol. 5681, pp. 214-225).

[2] Dang, T. T., An, L. X., Tran, D. T., & Kim, S. (2017). Object-based video forgery detection using convolutional neural networks. IEEE Transactions on Circuits and Systems for Video Technology, 27(10), 2229-2239.

[3] Albluwi, S. (2018). Deep learning based video forgery detection using convolutional neural networks. Journal of Electronic Imaging, 27(4), 043035.

[4] Yao, J., Zhang, L., & Xu, Z. (2018). Video forgery detection and localization using passive techniques. IEEE Transactions on Information Forensics and Security, 13(8), 1969-1984.

[5] Chen, H., Xu, M., Shi, Y. Q., & Sencar, H. T. (2018). Deep learning for detection of object-based forgery in advanced video. IEEE Transactions on Information Forensics and Security, 13(11), 2705-2714.

[6] Rocha, A.; Scheirer, W.; Boult, T.; Goldenstein, S. Vision of the unseen: Current trends and challenges in digital image and video forensics.ACM Comput. Surv. 2011, 43, 26–40.

[7] Stamm, M.C.; Wu, M.; Liu, K.R. Information forensics: An overview of the first decade. IEEE Access 2013, 1, 167–200.

[8] Chen, S.; Tan, S.; Li, B.; Huang, J. Automatic Detection of Object-Based Forgery in Advanced Video. IEEE Trans. Circuits Syst. Video Technol. 2016, 26, 2138–2151.

[9] Tan, S.; Chen, S.; Li, B. GOP based automatic detection of objectbased forgery in advanced video. In Proceedings of the Asia-Pacific Signal and Information Processing Association Annual Summit and Conference (APSIPA), Hong Kong, China, 16–19 December 2015; pp. 719–722.

[10] Qureshi, M.A.; Deriche, M. A bibliography of pixel-based blind image forgery detection techniques. Signal Process. Image Commun. 2015, 39, 46–74.

[11] Birajdar, G.K.; Mankar, V.H. Digital image forgery detection using passive techniques: A survey. Digit. Investig. 2013, 10, 226–245.

International Journal of Information Technology & Computer Engineering
ISSN 2347–3657
Volume 13, Issue 2, 2025
https://doi.org/10.62647/ijitce.2025.v13.i2.pp562-571
[12] Al-Qershi, O.M.; Khoo, B.E. Passive detection of copy-move forgery in digital images: State-of-the-art. Forensic Sci. Int. 2013, 231, 284–295.
[13] Sitara, K.; Mehtre, B.M. Digital video tampering detection: An overview of passive techniques. Digit. Investig. 2016, 18, 8–22.
[14] Bestagini, P.; Milani, S.; Tagliasacchi, M.; Tubaro, S. Local tampering detection in video sequences. In Proceedings of the IEEE 15th International Workshop on Multimedia Signal Processing (MMSP), Pula, Italy, 30 September–2 October 2013; pp. 488–493.
[15] Lin, C.S.; Tsay, J.J. A passive approach for effective detection and localization of region-level video forgery with spatio-temporal coherence analysis. Digit. Investig. 2014, 11, 120–140.
[16] Chen, R.; Yang, G.; Zhu, N. Detection of object-based manipulation by the statistical features of object contour. Forensic Sci. Int. 2014, 236, 164–169.
[17] Pandey, R.C.; Singh, S.K.; Shukla, K.K. Passive copy-move forgery detection in videos. In Proceedings of the International Conference on Computer and Communication Technology (ICCCT), Allahabad, India, 26–28 September 2014; pp. 301–306.
[18] Bondi, L.; Baroffio, L.; Güera, D.; Bestagini, P.; Delp, E.J.; Tubaro, S. First Steps Toward Camera Model Identification with Convolutional Neural Networks. IEEE Signal Process. Lett. 2017, 24, 259–263.
[19] Tuama, A.; Comby, F.; Chaumont, M. Camera model identification with the use of deep convolutional neural networks. In Proceedings of the IEEE International Workshop on Information Forensics and Security (WIFS), Abu Dhabi, UAE, 4–7 December 2016; pp. 1–6.
[20] Xu, G.; Wu, H.Z.; Shi, Y.Q. Structural Design of Convolutional Neural Networks for Steganalysis. IEEE Signal Process. Lett. 2016, 23, 708–712.
[21] Yang, P.; Ni, R.; Zhao, Y. Recapture Image Forensics Based on Laplacian Convolutional Neural Networks. In Proceedings of the 15th International Workshop on Digital Forensics and Watermarking (IWDW), Beijing, China, 17–19 September 2016; pp. 119–128.
[22] Bayar, B.; Stamm, M.C. A Deep Learning Approach to Universal Image Manipulation Detection Using a New Convolutional Layer. In Proceedings of the 4th ACM Workshop on Information Hiding and Multimedia Security (IH&MMSec), Vigo, Spain, 20–22 June 2016; pp. 5–10.
[23] Rao, Y.; Ni, J. A deep learning approach to detection of splicing and copy-move forgeries in images. In Proceedings of the IEEE International Workshop on Information Forensics and Security (WIFS), Abu Dhabi, UAE, 4–7 December 2016; pp. 1–6.