

**M.Tech
(Computer
Science
Engineering)**

**Akshat
Singhal
2019**

DETECTING FAKE VIDEOS

A DISSERTATION

SUBMITTED IN PARTIAL FULFILMENT OF THE
REQUIREMENTS

FOR THE AWARD OF THE DEGREE

OF

MASTER OF TECHNOLOGY

IN

COMPUTER SCIENCE ENGINEERING

Submitted by:

Akshat Singhal

2K16/CSE/01

Under the supervision of

Mr Manoj Sethi



COMPUTER SCIENCE DEPARTMENT

DELHI TECHNOLOGICAL UNIVERSITY

(Formerly Delhi College of Engineering)

Bawana Road, Delhi-110042

FEBRUARY 2019

DELHI TECHNOLOGICAL UNIVERSITY

(Formerly Delhi College Of Engineering)

Bawana Road, Delhi-110042

CANDIDATE'S DECLARATION

I, Akshat Singhal, Roll No. 2K16/CSE/01 of M.Tech (Computer Science Engineering), hereby declare that the project Dissertation titled “Detecting Faking News” which is submitted by me to the Department of Computer Science Engineering, Delhi Technological University, Delhi in partial fulfilment of the requirement for the award of the degree of Master of Technology, is original and not copied from any source without paper citation. This work has not previously formed the basis for the award of any Degree, Diploma Associateship, Fellowship or other similar title or recognition.

Place: Delhi

AKSHAT SINGHAL

Date: 28-02-2019

DELHI TECHNOLOGICAL UNIVERSITY

(Formerly Delhi College Of Engineering)

Bawana Road, Delhi-110042

CERTIFICATE

I hereby certify that the project Dissertation titled “Detecting Faking News” which is submitted by Akshat Singhal, 2K16/CSE/01 to the Department of Computer Science Engineering, Delhi Technological University, Delhi in partial fulfilment of the requirement for the award of the degree of Master of Technology, is a record of the project work carried out by the student under my supervision. To the best of my knowledge this work has not been submitted in part or full for any Degree or Diploma to this University or elsewhere.

Place: Delhi

(PROF.) MANOJ SETHI

Date: 28-02-2019

SUPERVISOR

ABSTRACT

As the World Wide Web usage continues to grow, people all over the world are relying more and more everyday on it in different ways like social networking, making online payments, entertainment purposes like watching videos and content sharing, educational purposes as well as professional uses too. One such common use is watching videos on the web or having update feeds in form of videos from social networking websites. This work is an effort towards helping the users in identifying the content in the videos as fake or real. Thus the user is alerted from believing false information which might lead to unwanted outcomes for the user like money loss for instance if the video was regarding share market or identifying rumors circulating on web. For the above stated aim, an application using Python has been developed. The application follows supervised learning with a training data set of 574 videos having fake as well as real videos. The technique used is taking into consideration the audio component of the video in addition to the video component. Also, the accuracy percentage of the subsequent test results using LSTM, CNN and Naïve Bayes model is displayed.

ACKNOWLEDGEMENT

Foremost, I would like to thank my supervisor Prof. Manoj Sethi for his motivation, patience and knowledge on the matter. Besides my supervisor, I thank the Head of Department, Dr Rajni Jindal for her immense cooperation and support. Also I am grateful to Delhi Technological University, which gave me a platform for the work. My sincere thanks to my parents for being the supporting figures in my life.

CONTENTS

1. Cover Page and Title Page
2. Candidate's Declaration
3. Certificate
4. Abstract
5. Acknowledgements
6. Contents
7. List Of Figures
8. List Of Symbols, Abbreviations and Nomenclature
9. Chapter 1: Introduction
10. Chapter 2: Literature Survey
11. Chapter 3: Methodology
12. Chapter 4: Results and Conclusions
13. Appendix
14. References

LIST OF FIGURES AND TABLES

- Figure 1: A Basic DPCM/DCT Encoder for Motion Compensated Video Compression
- Figure 2: Features used for Video Forgery Detection
- Figure 3: Types of Video Forgeries
- Figure 4: Features used in this work
- Figure 5: Parts of speech bar chart comparison
- Figure 6: Average match percent on web comparison
- Figure 7: Video forgery detection process used
- Figure 8: CCCoGV vectors in database
- Figure 9: An example of transcribed text file
- Figure 10: Parts of Speech percentages
- Figure 11: URL, Topic, File_Name in database
- Figure 12: File_Name, Average_match_percent in database
- Figure 13: Features table
- Figure 14: Training loss evolution for LSTM
- Figure 15: Training loss evolution for CNN
- Table 1: Classification Accuracies for different classifiers

LIST OF SYMBOLS, ABBREVIATIONS AND NOMENCLATURE

- POS tagging: Part of Speech tagging
- NLTK: Natural Language Toolkit
- API: Application Programming Interface
- URL: Uniform Resource Locator
- CNN: Convolutional Neural Network
- LSTM: Long Short Term Memory

CHAPTER 1: INTRODUCTION

The term “Fake News” was named the 2017 term of the year by Collins dictionary. It has been noted that the term increased in usage by 365% in the recent past. Fake news is defined as spreading hoaxes as news content with an intent to deceive. With the increasing popularity of social media, online news portals more and more people are relying on internet news platforms for news content. In a recent survey, it was found that 50% of the people in the age group 18-29 relied on internet platforms like websites, apps and social media for news. The video statistics on social media has been stated in [45] as follows:

- 82% of Twitter users watch video content on Twitter
- YouTube has over a billion users, almost one-third of total internet users.
- 45% of people watch more than an hour of Facebook or YouTube videos a week.
- More than 500 million hours of videos are watched on YouTube each day.
- More video content is uploaded in 30 days than the major television networks have created in 30 years.
- 72 Hours of video are uploaded to YouTube every 60 seconds.
- One-third of online activity is spent watching video.

- Every second, a million minutes (17,000 hours) of video content will cross global IP networks by 2021, according to Cisco (via Forbes).
- The 25-34 (millennial) age group watches the most online videos
- Over 500 million (half a BILLION) people are watching video on Facebook every day (via Forbes) [39].

In light of the above statistics and the ever expanding world of social media, one of the ways of recovering from the problem of fake information dissemination on social media is by using data mining, machine learning techniques to identify such news content. In this work I apply domain specific knowledge and deep learning techniques to overcome this problem. More specifically, the model is aimed at detecting inter-frame forgeries for detecting fake videos and how different classifiers perform on a given set of videos in classifying them into either ‘fake’ or ‘real’ is explored in this work. Using the domain specific knowledge and machine learning techniques, it is expected that given a video the model will classify it into a real video or a fake video with reasonable accuracy.

CHAPTER 2: LITERATURE SURVEY

2.1 Introduction

Below we shall review the literature for the various factors facilitating spreading of fake news, impact of fake news on the readers, medium by which fake news reaches the readers, approaches proposed for detecting fake news. Also we shall review different methods proposed by various authors in the previous literature for detecting inter-frame forgery in videos.

2.2.1 Factors influencing spread of fake news

The spread of fake news is influenced by many determinants ranging from the drive to maximize profit to the tendency of confirmation bias on the consumers' part. Following factors favoring the spread of fake news were cited by Shu, Sliva, Wang, Tang and Liu [4] in their work:

- Short Term Utility on publisher's part: Defined as the incentive to maximize profit. It is positively related to the number of consumers reached by the publisher
- Psychological Utility on consumer's part: Defined as receiving news that satisfies the prior opinions/worldviews and social needs of consumers
- Desire to maximize social acceptance by the consumers in their immediate social network
- Echo Chamber Effect: Tendency of like-minded people to form a group which polarizes their opinions

- **Social Credibility Factor:** A piece of circulating news becomes more believable to a person if other people consider the news source as credible, especially when more information is not available
- More often any information is repeated, more it becomes believable.

In addition to the above factors helping the proliferation of fake news, this work would like to discuss the role of filter bubbles. The term “Filter Bubble” was coined by Eli Pariser in 2010. It refers to the phenomena that people are not getting exposed to viewpoints different than their own in the online world due to specialized algorithms working at the back end which take into account the user’s past searches, clicks history before displaying the results for the particular user. For instance, if two different persons search for the same query on the search engine, it displays different results for each of them, favoring their individual viewpoints. In this way, a person is not exposed to a viewpoint different than his own. This creates an effect similar to the Echo Chamber effect.

2.2.2 How does fake news reach the audience?

Prior researches done on the topic suggest some of the channels by which fake news reaches the readers. Chen, Conroy and Rubin [7] address clickbaiting as the preferred means by which fake news spreads. Clickbaiting is defined as posting content online whose main purpose is to attract attention and encourage visitors to click on a link to a particular web page. Often it consists of an image and hyperlink text to arouse the curiosity of readers. Shu, Sliva, Wang, Tang and Liu [4] discuss the role played by users on the social media in proliferating such content. For instance, the authors classify the social media accounts found to be engaged in spreading fake news in the following three categories: Social Bots, Trolls, and Cyborg Users. Social Bots are the accounts which are controlled by a computer algorithm to automatically produce content and interact with

humans on social media. Trolls refer to human users who disturb the online community by provoking consumers into an emotional response. Cyborg users are accounts which are registered by humans after which, automated programs are set on the account to interact with social media. Cyborg accounts have an advantage of an easy switch of account between bots and humans which render unique opportunities to cyborg users for disseminating spurious content. Shu, Sliva, Wang, Tang and Liu [4] identify two types of propagators of fake news: ‘clarifiers’ and ‘persuaders.’ Clarifiers are the users who try to clear the fake news by suggesting skeptical viewpoints and persuaders are users who try to propagate the fake news by aligning their opinions in favor of the news content. The authors suggest the detection of clarifiers and persuaders as an open area for future research on detecting fake news.

2.2.3 Approaches proposed to detect fake news

Several methods are reported in the literature to address this issue. Broadly these approaches can be classified as Model Based and Network Based approaches [4].

To guess whether the news is real or fake, first step is to collect the data on the basis of which guess can be made. This section presents the features which have been suggested by several authors. The features can be categorized as linguistic features, domain specific features, visual features, user level features, group level features or psychological features. Linguistic features characterize a particular aspect of the language. Several authors have used the linguistic features in their research. For instance, Chen, Conroy and Rubin [7] propose that for detecting fake news spread by clickbaiting hints like unresolved pronouns, suspenseful language and reverse narrative style can be used. Alternatively, Horne and Adah [6] argue that fake news can be

identified by carefully analyzing the title of the fake news article for linguistic features. The authors used the fact that fake news uses heuristics to convince the readers whereas real news relies on arguments. Therefore, the beneficial linguistic features to identify the content as real or fake would be verb phrases and name entities as fake news uses them in titles to get many points across, while real title opts for a brief and general summary statement as title. Elkasrawi [3] emphasizes on detecting the alteration in images presented in news articles from the original image source to detect fake news content. Horne and Adah [6] have used features to capture the sentence complexity and attributes like Readability, Vocabulary and Fluency for the article. Sentence complexity is said to be high if they have more words per sentence and deeper syntax trees. A higher readability implies that the article takes higher education level to be read. It is measured by grade level readability indexes: Gunning Fog, SMOG Grade and Flesh-Kincaid Grade. Vocabulary is used to measure the word diversity of article. It is measured by dividing number of unique words by total number of words in the article. Fluency is used to measure the vocabulary of the article to be common or specialized. Shu, Sliva, Wang, Tang and Liu [4], in their study suggest the following features: total number of words in the news content, number of characters per word, frequency of large words, number of unique words, n-grams, punctuations and POS tagging. Domain specific features are defined as the features pertaining to the problem domain. For example, Figueira and Oliveira [8] discuss the FiB system, developed by four students at Princeton University, which focused on checking fake or real news feeds. This system used the following domain specific features: Google/Bing search results for verifying the authenticity of the text content of news feed, website reputation score for the links provided in the news feed and extraction of text from Twitter snapshots to confirm their veracity. Shu, Sliva, Wang, Tang and Liu [4] suggested the following domain specific features: quoted words in the

text, external links in the content and number of graphs and average length of graphs. Visual features refers to features which are derived from images and videos in the news content. Prior research suggests that authors have used visual features to verify the authenticity of the images in the news content. Elkasrawi, Bukhari, Abdelsamad and Dengel [3] use the SURF features extracted from the images for image alignment and consequently to find out if the image was doctored. User level features refer to the features extracted for a user on the social media. For instance, the age of the user, number of posts by the user, images posted by the user, number of followers of the user and number of followees of the user. In studying the helpful features for detecting fake news on social media domain the authors [4] have arranged the user level features as individual level features, group level features, post level features and temporal level features. Group level features were stated as those aimed to capture characteristics of group as a whole by aggregating the individual level features say, for some similar news articles. Temporal level features take into consideration the changes of post level feature values with respect to time. Psychological features include the opinions of the users with respect to some content which may be obtained by sentiment analysis as suggested by many authors. The literature pertaining to the issue suggests the following two types of approaches:

1) Network based approaches

Network based approaches tend to focus on the network specific information to predict the content as real or fake. Conroy, Rubin and Chen [1] argue that network information, such as message metadata or structured knowledge network queries can be harnessed to provide aggregate deception measures. Figueira and Oliveira [8] cite the example of Facebook task force for identifying fake news which applies network based approaches like finding the relationship between the person who shared a news article and those who

like, share and comment. Another point which was shared by the task force was considering the posts which were hidden by users from certain other users as it increases the probability of the content being spurious. Social graphs have also been used by Facebook to check the spreading of fake news. Shu, Sliva, Wang, Tang and Liu [4] state that among all the users who have published related social media posts, four types of specific networks can be formed to extract features. These features are then to be used to identify spurious content. The four types of specific networks discussed are Stance Network, Co-occurrence Network, Friendship Network and Diffusion Network. Stance Networks are built around the concept of stance. The stance of a user is defined as whether the user agrees, disagrees or simply discusses pertaining to some post on social media. In a stance network nodes are the tweets relevant to the news being investigated and edges between them denote the weights of similarity of stances. Co-occurrence networks link those users whose posts are relevant to similar news articles. Friendship networks aim at capturing the relationship of following/followee among the users who are posting similar posts. Finally, Diffusion Networks track the path of spread of fake information. It does so by making a path between the user u_i and user u_j if u_j follows u_i and u_j posts about some information only after u_i does so. Sirajudeen, Azmi and Abubakar [9] propose DNS hijacking based approach to detect the sources involved in spreading fake news. By means of Wireshark application, the IP addresses of source and destination are identified. If the IP address for the destination is constantly changing, it indicates DNS hijack. Consequently, it increases the probability of the source being fake.

2) Model based approaches

Model based approaches aim to build practical models which can be used to classify the news as real or fake. The features extracted for the model may be of any of the type as discussed. The authors [4] have discussed News Content Models and Social Context Models. News Content Models are based on the features which are derived from actual factual sources and a classification algorithm is applied on top of it. Knowledge based news content models may rely on human expert oriented fact checking systems like snopes.com, they may also rely on crowdsourcing or the model may be an automatic computational system. The derived features aim to measure how deceptive the content seems or the objectivity of the content. Social context models capture the features based on stance and the propagation of content.

2.2.4 Proposed future research

As the authors note earlier, more work is necessary to resolve this issue. The direction of the future research to further improve the detection of fake news has been proposed by the authors in prior research. Shu, Sliva, Wang, Tang and Liu [4] state that most existing research is concerned with detecting the authenticity of news content under examination but tend to ignore the ‘Intent’ aspect of fake news generation. ‘Intention detection’ can be of help in issues like capturing the echo chamber effect. The authors propose the use of ensemble classifiers to take advantage of the extracted features better. Also, existing approaches are making use of supervised learning methods which requires a pre-annotated dataset to train the classifier. In this area of research it is laborious process as it requires manual analysis of many news articles. Therefore, semi-supervised or unsupervised learning models are more practical in this sense.

2.2.5. Survey on Inter-Frame Video Forgery Detection

Video compression artifacts play an important role in the detection of video forgeries. This has been used as basis for research by many authors in the literature. Therefore, the basics of video compression are discussed firstly. As in [40], video compression standards extend the transform-based, still image compression techniques to include methods for reducing temporal or frame-to-frame redundancies. Most of the video coding standards rely on similar video compression techniques. The input to the video coding algorithm may be a conventional block of image data or the difference between a conventional block and a prediction of it based on similar blocks in previous and/or subsequent video frames. This leads to three types of encoded output frames:

- a. Intra-frame or independent frame (I-frame): Compressed independently of all previous and future frames. Reference point for the motion estimation needed to generate subsequent P-frames and B-frames. All standards of video compression require periodic insertion of I-frames in compressed code stream [40].
- b. Predictive frame (P-frame): Compressed difference between current frame and a prediction of it based on the previous I-frame or P-frame [40].
- c. Bidirectional frame (B-frame): Compressed difference between the current frame and a prediction of it based on the previous I- or P-frame and next P-frame. Hence, the encoded frames are reordered before transmission and the decoder reconstructs and displays them in proper sequence [40].

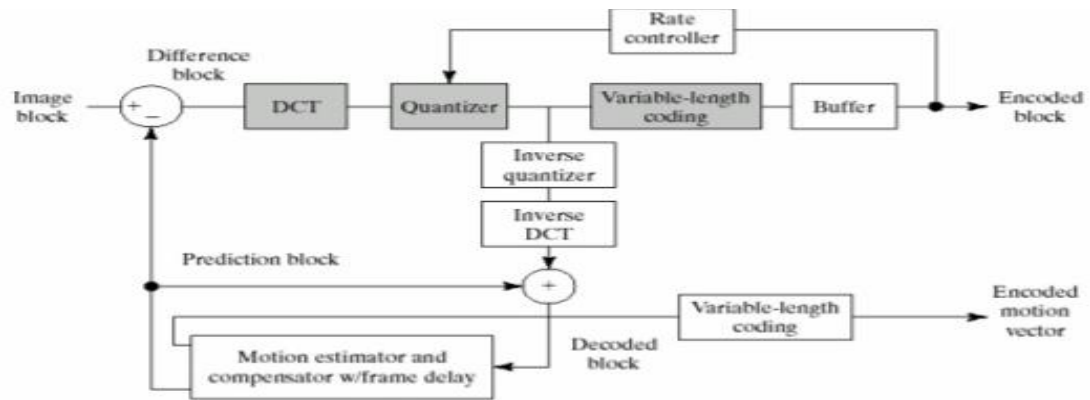


FIGURE 1. A Basic DPCM/DCT Encoder for Motion Compensated Video Compression [33]

Many authors have studied the problem of video forgery detection and have used some feature or other in order to examine the video for manipulation. A brief overview of the features used for forgery detection in digital videos are shown below in the figure as in [30] before discussing the techniques proposed to detect video forgery.

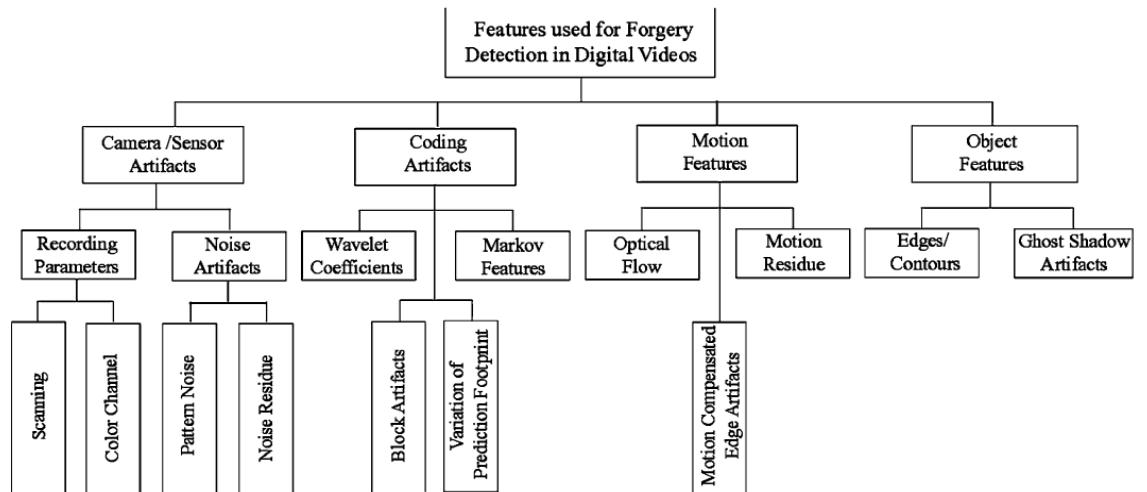


FIGURE 2. FEATURES USED FOR VIDEO FORGERY DETECTION [16]

As classified in [13], video forgery detection approaches can be classified as Active or Passive. Active approach relies on the assumption that if the video is forged then recovery of the watermark or digital signature from the video is not possible, thereby indicating video tampering. However, it is not very useful if pre-processing insertions like watermarking or digital signatures is not applied to the original video file. Passive approach, on the other hand, does not rely on the presence of pre-processing insertions in the original video, rather, the content of the video is examined using various video processing and image processing techniques to arrive at a conclusion. This section provides a short summary of the passive video forgery detection techniques which have been proposed by several authors.

Broadly speaking, any video forgery falls in one of the two categories: Inter-Frame Forgery and Intra-Frame Forgery [30]. Several authors have proposed methods for the detection of inter-frame forgery and intra-frame forgery techniques and also for detecting both kinds of forgeries simultaneously. Before proceeding with summarizing the work of authors let us see common types of inter-frame forgery and intra-frame forgery as in [30].

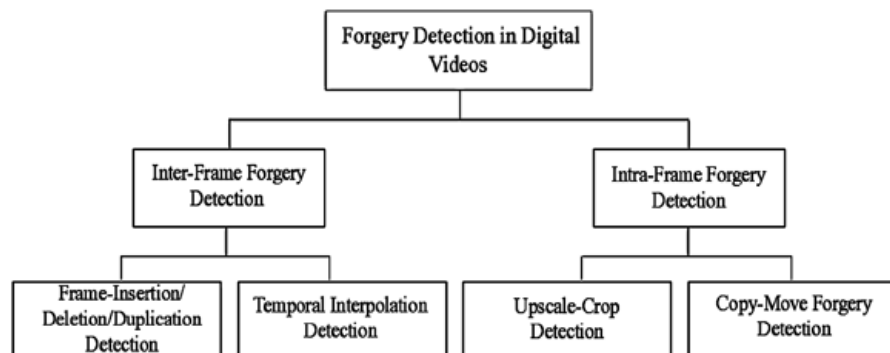


FIGURE 3. Types of Video Forgeries in [30]

- a. **Inter-frame forgery detection:** In this type of forgery, the sequence of the frames is altered in some way. For example, frame addition, deletion or duplication. There is

literature available on the topic of inter-frame forgery detection in videos. In [14], Li, Wang and Xu propose an algorithm to detect inter-frame forgery based on 2D phase congruency and k-means clustering. First 2D Phase Congruency for each frame is calculated followed by correlation coefficients of adjacent frames and variation of consecutive correlation coefficients are obtained. At last, discontinuous points are detected using k-means clustering which indicate points of tampering in the video. In [10], Long, Basharat and Hoogs have proposed a deep learning based approach to detect frame duplication in a given video. The scheme proposed is to first run the I3D network to extract deep spatial-temporal feature and build the coarse sequence-to-sequence distance to determine the possible frame sequences that are likely to have frame duplication. Thereafter, ResNet-based Siamese network is applied to confirm whether there exists frame duplication manipulation. For the further identification of the video temporal localization, an I3D based inconsistency detector to distinguish the duplicated frames from the selected frames is applied. The method applied by authors in [20] is a compression artifact based video forgery detection technique. The authors in [20] have used the observation that when an encoded video with GOP size $G1$ is re-encoded with GOP size $G2$, using only I-frames and P-frames and originally encoded I-frame is re-encoded as P-frame, an abnormal decrease in the amount of S-MBs (Skipped Macroblocks) happens. This is known as Variation in Prediction Footprint (VPF). Further in [33], the authors have improved upon the limitations in [20] to allow double encoding detection even if group of leading frames is removed and can detect removal and insertion of frames throughout the video by increasing the robustness of VPF proposed in [20]. Sun, Wang and Jiang [23] detect double MPEG compression in video by using the

observation that double compression using MPEG standard disturbs the Discrete Cosine Transform coefficients which results in a violation of parametric logarithmic law. Hence, the video is detected to be doubly compressed. Further, authors have used SVM classifier. Wang and Farid [22] detect the presence of double quantization in video to verify if it has been forged. Dong, Yang and Zhu [11] rely on Motion Compensated Edge Artifacts for classifying videos. The basis of MCEA in [11] is as follows: For typical in video codec, when coarse quantization is combined with motion compensation prediction, the blocking artifacts propagate from I-frames into subsequent frames, causing structured high frequency noise that is no longer located at block boundaries. These kind of motion compensated edge artifacts (MCEA) are referred to be false edges, and their energies accumulate in each GOP [11]. The authors propose computing the difference of MCEA value between adjacent P-frames and applying Fourier Transform on the result. If there are spikes in the Fourier Transform, the video is labelled as tampered. Ravi and Subramanyam [18] analyze compression noise for solving the problem. First, the compression noise is extracted from the video. Thereafter, Markov Feature Extraction is done for the extracted noise and a SVM classifier is applied on top of it. The method is based on the observation that the correlation of spatial domain noise is disturbed if a single video is doubly compressed [18]. Fadl, Han and Li [28] detect fake videos by observing abnormal points in the differential energy of residue after the video is compressed again. The authors argue that different types of manipulations produce different effects on the residue and abnormal points detected therein provide clues to the video tampering and also type of video tampering. Wang, Li, Zhang and Ma [35] have observed that in the original video the Correlation Coefficients of Gray Values is

consistent whereas this is not the case in fake video. Using this observation and using CCCoGV as feature, the authors have applied it to Support Vector Machine (SVM) to classify the video as real or fake. Bozkurt, Bozkurt and Ulutas [12], use the correlation between frames in the video to detect forgery in a novel way. First the DCT transform is applied for all frames and is binarized. Thereafter a correlation image is calculated using the binarized DCT features [12]. To detect coarse forgery line, Hough Transform is applied to the correlation image and to further find the finer forgery line, the line amongst all the forgery lines which have the highest value for average Peak Signal to Noise Ratio (PSNR) is chosen as the fine forgery line [12]. This method has the added advantage that by applying shrinking and expanding procedure on forgery line, the forgery areas in the image can be detected [12]. Li, Mei, Li and Wu [31] propose a method to detect frame repetition forgery by detecting varying noise level over time. Wavelet coefficients for the frames are extracted and Mean Absolute Deviation (MAD) for the wavelet coefficients is calculated to give the average Gaussian noise value in the frame [31]. Thereafter, Fast Fourier Transform (FFT) is calculated which is used to locate the Peak-Mean Ratio (PMR) of the amplitude spectrum [31]. Finally, on basis of threshold value, periodicity in temporal domain is identified which reflects Frame Repetition [31]. In [19], the authors propose technique to detect frame deletion type of forgery. The authors have used supervised learning technique with Convolutional Neural Network (CNN) to train the machine for frame deletion type of forgery. In [25], the authors use the optical flow of a video to detect if it has been manipulated. For a video that has been manipulated, the optical flow is not uniform unlike the real videos. The fake videos optical flow has discontinuity points which can be used to detect video manipulation [25]. Voronin,

Zelensky and Svirin [32] take a new approach towards preventing the problem by using Blockchain Technology.

2.2.5.1. Limitations of Previous Research

Although studies have been conducted by many authors, the problem of video forgery detection is still insufficiently explored. As stated by authors in [30], previous studies have almost exclusively focused on the video manipulation aspect of video forgery detection. A closer look to the literature on video forgery detection reveals some shortcomings. To fill this literature gap, this paper presents a methodical approach to using audio content in analysis of fake video content. Some of the interesting research questions in this context are:

- 1) How does combining the audio aspect of video to the visual component effect the overall efficiency of the video forgery detection technique?
- 2) How can we distinguish parody videos from fake videos based on video content alone?

CHAPTER 3: METHODOLOGY

3.1 Introduction

The literature review shows that many authors have tried to use features like linguistic features, domain specific features, visual features, psychological features and network features to predict the possibility of the news content as fake and features mentioned in Figure 2 to identify video forgery. Also, authors have contributed to an understanding of various approaches which can be used to detect spurious information. However, more work is necessary to resolve this issue. This work adds to the literature by using audio component of the video as well for video forgery identification. Additionally, the proposed model exploits the fact that fake content uses a language which is repetitive and attention seeking by appealing to the consumers more than in a

factual way. Also, deep learning approach has been used to identify inter-frame forgery in fake videos from real videos. More specifically, the work seeks to answer the question, how can incorporating the audio component of the video enhance accuracy of video forgery detection models?

3.2 Dataset Used

For this study, the video dataset has been collected from <https://www.youtube.com>. The video dataset is divided into two sets: training dataset and testing dataset. Each of the two datasets consists of fake as well as real videos. The fake video set comprises of edited videos uploaded on Youtube by various users, which, are consequently known to have inter-frame video forgery in them. The real video set comprises of news bulletins and also the satire news. The training dataset consists of 574 videos divided into real and fake videos. The testing dataset consists of 278 videos. Label '0' is used for fake videos and '1' is used for real videos.

3.3 Conceptual Design

For the problem at hand, deep learning approach using supervised learning has been used to train the machine in recognizing the fake video content and Python along with Scrapy framework have been used to find out the magnitude of average match percent of the video content on the world wide web. The model builds improves upon the previous work in [35] by including the audio components of the videos as well. The model uses CCCoGV features mentioned in [35]. Also, it uses semantic features of English language like Parts Of Speech percentage in the content and domain specific features like average match percent of the content on the web.

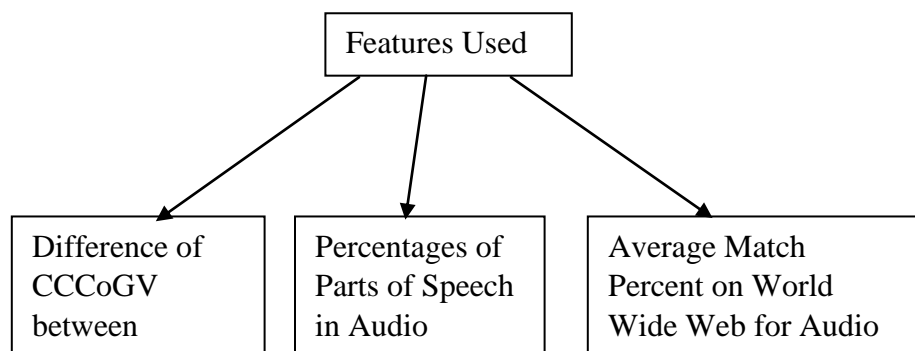


FIGURE 4. Features Used in this Work

The work builds upon the idea in [35] that the Difference of Correlation Coefficients between adjacent frames is not consistent in the forged videos due to some kind of manipulation like frame insertion, frame deletion or frame duplication. The forged video can hence be identified on the basis of the discontinuity in the CCoGV as in [35]. This work adds two more features to the above work which are as follows: Percentages of Parts of Speech in Audio Component and Average Match Percent on World Wide Web for Audio Component.

The idea is that fake news tries to pack a lot of content with less amount of words as it is made to grab the attention of the consumers. Hence, if we analyze the Parts Of Speech percentages for the real and fake content, respectively, we find that the fake content has less percentage of nouns as compared to the fake content and also it is more coherent as compared to the fake content. The coherency of real content is reflected in the observation that the real content had a larger percentage of pronouns than the fake content (Figure 5).

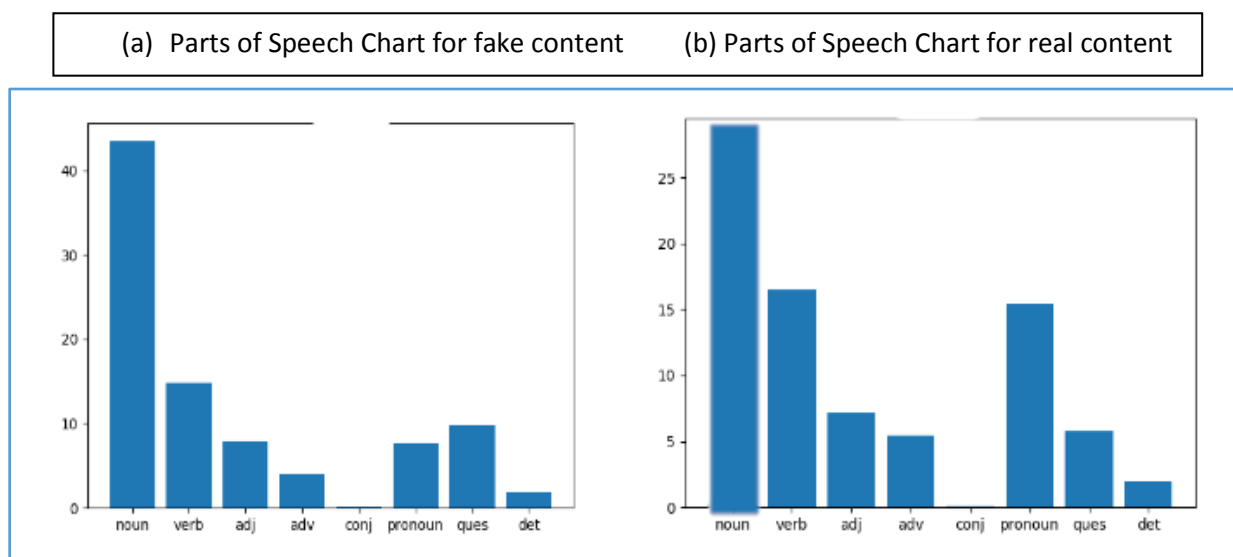


FIGURE 5. Parts Of Speech Bar Chart Comparison

Also, if we search the web and find out how much the content matches with the website contents returned by the search engine, it is found that, the fake content has a higher average match percent as compared to the real content due to its attention seeking nature (Figure 6).

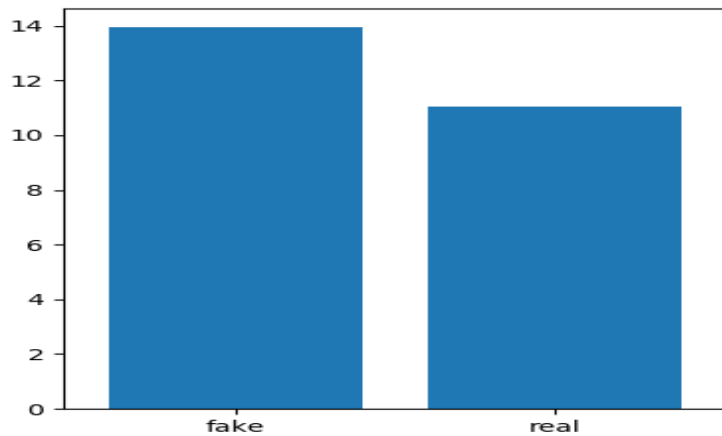


FIGURE 6. Average Match Percent on Web Comparison

The following process (Figure 7) has been used in the model to identify fake videos from real videos:

- a. Convert the frames into grayscale format in order to reduce the complexity of processing
- b. Calculate the Correlation Coefficients for the pixels between adjacent frames
- c. Compute the difference between Correlation Coefficients between adjacent frames
- d. Normalize the vector obtained by dividing it by maximum value in the vector
- e. Quantize the above vector into the vector of size 50 and store it in database
- f. Extract the audios from the videos in the dataset
- g. Split the extracted audios in 30 second chunks
- h. For each audio chunk for an audio file transcribe the contents into text document
- i. Calculate Parts Of Speech percentages for different parts of speech from the above text documents for each audio file and store in database

j. Apply Latent Dirichlet Allocation (LDA) Topic Modelling on the text files for each audio and store results in the database

k. For the topics stored in the database, compute average match percent for each topic on the web

l. Apply LSTM (Longest Short Term Memory) on the features computed

m. Apply CNN (Convolutional Neural Network) on the features computed

n. Apply Naïve Bayes Classifier on the features computed

The model is built in Python and uses supporting libraries.

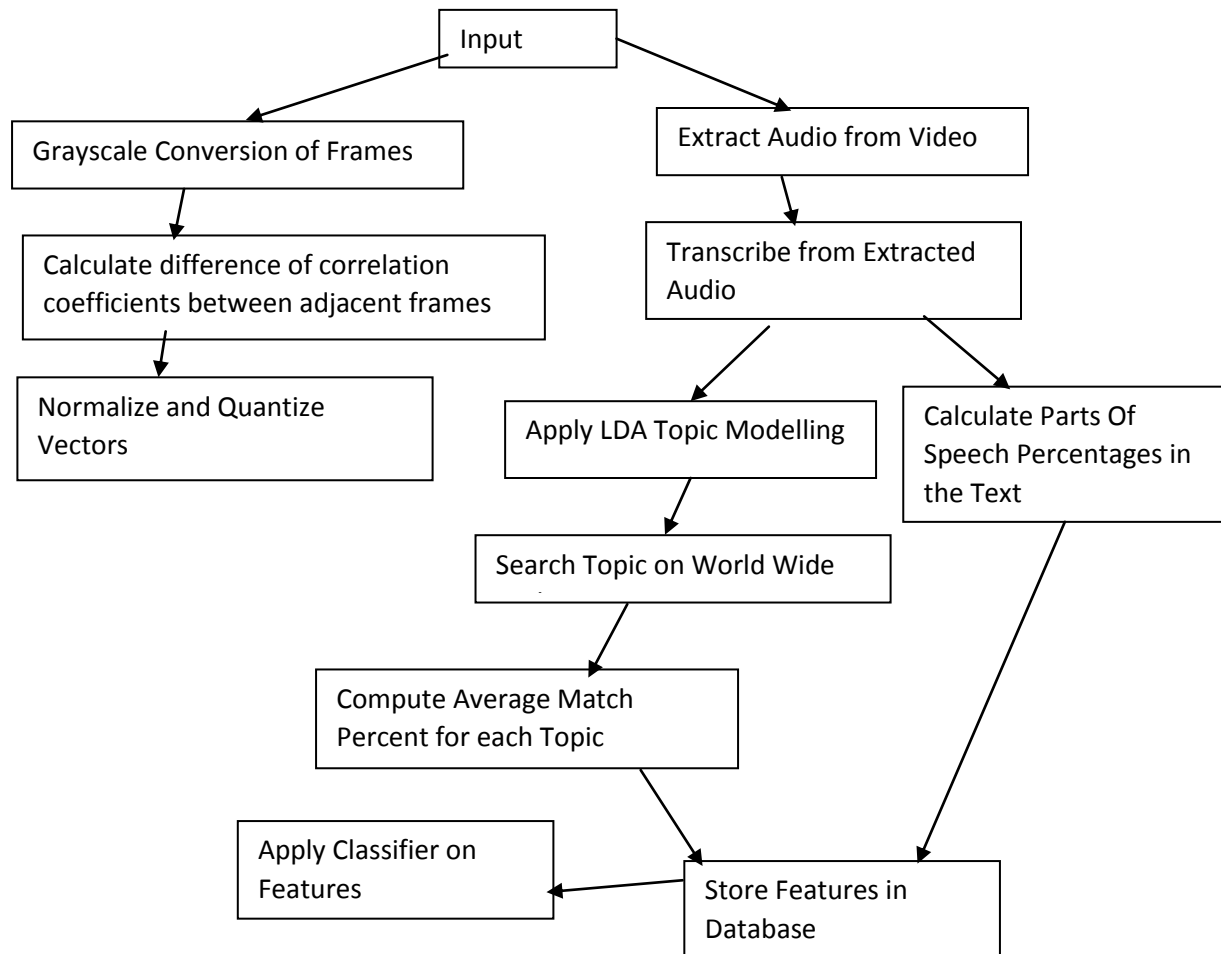


FIGURE 7. Video Forgery Detection Process Used

For the database operations SQLite3 has been used with python. Video analysis to detect inter-frame forgery has been carried out using OpenCV library. The corresponding vector obtained after video analysis, normalized and quantized is stored in the database (Fig. 8).

	fname	input_vector	label
1	f0	1250, 179, 94, 58, 40, 24, 16, 12, 7, 12, 7, 5, 7, 5, 2, 1, 2, 4, 0, 2, 0, 0, 0, 2, 0, 1, 0, 2, 1, 0	0
2	f10	547, 76, 58, 42, 9, 23, 7, 5, 6, 2, 3, 2, 7, 5, 2, 1, 0, 1, 2, 1, 2, 0, 1, 2, 1, 0, 0, 1, 1, 0, 0, 2	0
3	f11	1210, 89, 28, 7, 8, 6, 4, 3, 3, 1, 1, 0, 2, 1, 0, 0, 0, 0, 2, 1, 0, 0, 1, 0, 2, 0, 0, 0, 0, 0, 0	0
4	f12	1661, 113, 34, 33, 12, 14, 8, 8, 3, 2, 2, 1, 1, 0, 2, 0, 4, 1, 1, 0, 3, 0, 0, 2, 1, 1, 0, 0, 0, 0, 0	0
5	f13	873, 114, 39, 12, 7, 8, 2, 4, 4, 2, 3, 3, 1, 1, 1, 3, 3, 0, 0, 1, 1, 0, 1, 0, 0, 0, 1, 1, 0, 0, 0	0
6	f14	798, 69, 50, 26, 21, 13, 4, 7, 5, 5, 1, 1, 2, 3, 2, 1, 3, 3, 0, 1, 1, 1, 2, 2, 0, 0, 0, 0, 0, 0, 0	0
7	f15	3220, 260, 87, 35, 25, 19, 15, 15, 8, 10, 3, 3, 3, 5, 8, 3, 3, 3, 5, 1, 1, 2, 0, 0, 2, 3, 2, 0, 2, 1	0
8	f16	2348, 86, 42, 16, 10, 4, 12, 4, 4, 3, 2, 4, 4, 3, 2, 3, 4, 2, 1, 1, 2, 2, 2, 1, 0, 0, 2, 1, 1, 0, 1	0
9	f17	3005, 307, 121, 39, 18, 16, 11, 20, 8, 4, 6, 2, 8, 4, 1, 5, 8, 3, 1, 2, 1, 4, 1, 5, 1, 1, 1, 0, 1, 1	0
10	f18	2535, 181, 75, 39, 19, 23, 12, 5, 9, 2, 5, 5, 2, 2, 3, 4, 2, 4, 1, 3, 4, 0, 0, 1, 3, 2, 1, 0, 0, 0	0
11	f19	1269, 75, 19, 14, 5, 8, 6, 5, 1, 1, 1, 2, 0, 0, 0, 0, 0, 0, 2, 1, 1, 0, 0, 0, 0, 0, 1, 0, 0, 0	0
12	f1	1068, 183, 89, 69, 45, 32, 21, 11, 7, 9, 4, 10, 3, 2, 1, 0, 1, 1, 1, 2, 0, 2, 2, 2, 0, 0, 2, 1, 2, 0	0
13	f20	1654, 280, 162, 58, 53, 23, 20, 15, 20, 9, 3, 2, 3, 4, 5, 2, 1, 3, 1, 0, 2, 2, 2, 2, 1, 1, 3, 4, 1	0
14	f21	1286, 245, 76, 40, 24, 17, 12, 7, 9, 7, 7, 6, 5, 10, 7, 4, 4, 3, 0, 6, 2, 1, 5, 2, 5, 1, 1, 1, 1, 0	0
15	f22	1794, 430, 156, 89, 59, 41, 27, 27, 15, 10, 14, 17, 10, 5, 4, 10, 7, 0, 6, 2, 3, 7, 1, 2, 1, 3, 2, 2	0
16	f23	2318, 299, 123, 60, 43, 24, 19, 19, 11, 15, 5, 3, 7, 4, 0, 2, 3, 2, 5, 5, 1, 3, 0, 1, 0, 1, 3, 3, 0	0
17	f24	872, 118, 34, 12, 5, 4, 4, 2, 2, 1, 1, 0, 2, 0, 1, 1, 0, 2, 1, 1, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0	0
18	f25	741, 149, 49, 40, 26, 9, 5, 2, 4, 1, 3, 4, 2, 2, 1, 4, 0, 1, 2, 0, 3, 3, 2, 1, 0, 0, 0, 1, 0, 1	0
19	f26	1778, 172, 73, 49, 25, 17, 14, 13, 0, 3, 1, 2, 0, 1, 0, 0, 0, 2, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 1, 0	0
20	f27	1834, 227, 73, 26, 29, 15, 10, 4, 3, 7, 7, 1, 2, 1, 3, 3, 3, 2, 0, 1, 3, 1, 1, 0, 0, 1, 1, 0, 0, 0	0
21	f28	2162, 199, 66, 38, 17, 14, 13, 9, 6, 4, 8, 5, 5, 7, 4, 2, 3, 3, 3, 2, 0, 3, 3, 0, 1, 2, 2, 0, 2, 0	0
22	f29	1700, 295, 108, 39, 23, 15, 16, 9, 5, 4, 3, 7, 4, 4, 4, 7, 3, 3, 0, 2, 5, 3, 2, 2, 1, 1, 1, 0, 1, 1	0
23	f2	802, 186, 90, 37, 20, 19, 13, 7, 3, 4, 0, 2, 3, 4, 2, 4, 3, 0, 2, 3, 2, 3, 1, 3, 1, 1, 0, 2, 0, 1, 1	0

FIGURE 8. CCCoGV vectors in database

To extract the audio from video file, MoviePy API for python is used. Thereafter, for each audio file, split into 30 second chunks, SpeechRecognition library which uses Google API for speech recognition is used to transcribe the audio file in a text file. The extracted audio file is split into 30 second chunks in order to optimize the performance of the transcribing process (Figure 9).

Eight different parts of speech are used to calculate the percentage of each part of speech. They are as follows: Nouns, Verbs, Adjectives, Adverbs, Conjunctions, Pronouns, Questions and Determiners. An average match for each of these parts of speech is shown in Figure 5 for both the real as well as fake videos. NLTK library in Python allows for identifying the part of speech for each token in a given text. Using the above, the percentage values for all the above eight parts of speech are calculated and stored in database as shown in Figure 10.

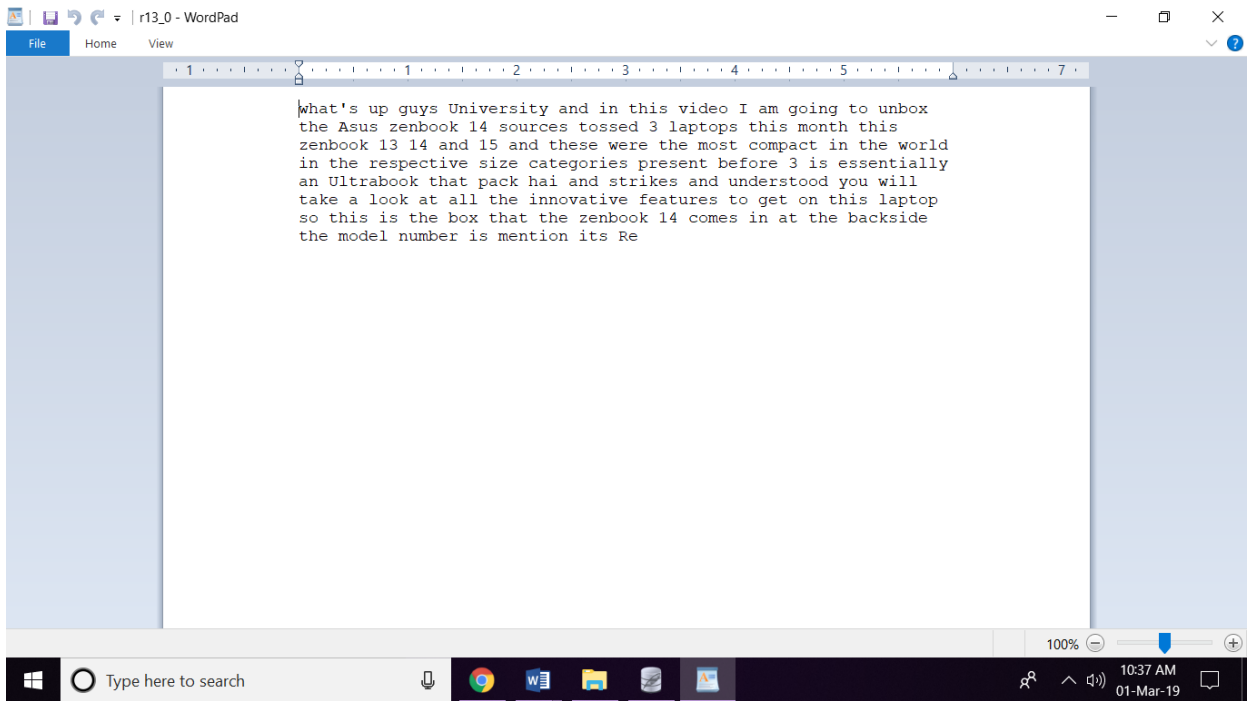


FIGURE 9. An Example of Transcribed Text File

SQLiteStudio (3.1.1) - [topics_pos (fvc)]

Database Structure View Tools Help

Grid view Form view

Filter data Total rows loaded: 547

	fname	noun_percent	verb_percent	adi_percent	adv_percent	fw_percent	conjunction_percent	pronoun_percent	ques_percent	det_percent
1	f0	20.0	0.0	40.0	20.0	0.0	0.0	0.0	0.0	0.0
2	f1	20.0	0.0	20.0	0.0	0.0	0.0	0.0	20.0	20.0
3	f11	33.333333333...	0.0	0.0	0.0	0.0	8.333333333333332	0.0	0.0	4.16666666666...
4	f12	100.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0
5	f13	25.0	0.0	0.0	16.666666666...	0.0	0.0	0.0	0.0	8.33333333333...
6	f14	33.333333333...	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0
7	f15	24.137931034...	0.0	3.448275862...	10.34482758...	0.0	6.896551724137931	3.4482758620689...	3.44827586206...	3.44827586206...
8	f16	18.181818181...	9.090909090...	9.090909090...	18.18181818...	0.0	0.0	9.09090909090...	0.0	9.09090909090...
9	f17	29.411764705...	0.0	5.882352941...	0.0	0.0	11.76470588235294	5.88235294117647	0.0	0.0
10	f18	7.2727272727...	5.454545454...	9.090909090...	5.454545454...	0.0	7.27272727272727...	14.545454545454...	9.0909090909...	1.81818181818...
11	f20	13.043478260...	4.347826086...	8.695652173...	8.695652173...	0.0	8.695652173913043	8.6956521739130...	0.0	4.34782608695...
12	f21	26.923076923...	0.0	11.53846153...	0.0	0.0	11.5384615384615...	3.8461538461538...	0.0	3.84615384615...
13	f22	12.903225806...	9.677419354...	3.225806451...	12.90322580...	0.0	12.9032258064516...	32.258064516129...	0.0	3.22580645161...
14	f23	16.666666666...	4.166666666...	8.333333333...	8.333333333...	0.0	12.5	8.3333333333333...	0.0	4.16666666666...
15	f24	22.222222222...	0.0	11.111111111...	0.0	0.0	0.0	11.111111111111...	0.0	11.1111111111...
16	f25	23.809523809...	4.761904761...	19.04761904...	0.0	0.0	14.2857142857142...	4.7619047619047...	4.7619047619...	4.76190476190...
17	f27	10.526315789...	4.210526315...	9.473684210...	20.0	0.0	7.368421052631578	5.2631578947368...	5.2631578947...	1.05263157894...
18	f28	12.5	12.5	6.25	1.5625	0.0	9.375	15.625	4.6875	1.5625
19	f29	27.272727272...	0.0	0.0	4.545454545...	0.0	13.6363636363636...	0.0	0.0	4.54545454545...
20	f3	9.0909090909...	9.090909090...	0.0	18.18181818...	0.0	0.0	9.09090909090...	18.181818181...	0.0
21	f30	31.818181818...	0.0	0.0	4.545454545...	0.0	18.1818181818181...	0.0	0.0	4.54545454545...
22	f32	11.111111111...	0.0	0.0	0.0	0.0	22.22222222222222	33.3333333333333...	0.0	0.0
23	f33	10.0	10.0	0.0	10.0	0.0	0.0	20.0	0.0	0.0

site_data (site_db0) search_results (site_db0) cl_attr (site_db0) test_attr (site_db0) test_search_results (site_db0) test_site_data (site_db0) topics (fvc)

FIGURE 10. Parts Of Speech Percentages

In order to compute the appropriate topic for the transcribed text for the audio files, first the Bag of Words (BOW) vector is computed from the transcribed text files and dictionary of unique words in the document is also computed and stored. Latent Dirichlet Allocation (LDA) technique is applied on top of the computed metrics. In this model, LDA is implemented in Python using ‘gensim’ library for the same. Here, the topmost most probable topic is selected for further use even though more than one topics for the same text can be extracted.

For each of the topics extracted, they are consequently searched on Google using ‘googlesearch’ API in Python. Top ten URLs from the search results are retrieved and stored. The consequent data obtained is stored in the database with URL as the primary key, the topic for which the URL was retrieved and the file for which the corresponding topic was computed with LDA. This is shown in Figure 11.

SQLiteStudio (3.1.1) - [topics (fvc)]

Database Structure View Tools Help

Databases

Filter by name

site_db0 (SQLite 3)

Tables (6)

cl_attr

search_results

site_data

test_attr

test_search_results

test_site_data

Views

fvc (SQLite 3)

Tables (12)

av_match_percent

input_vectors

test

test_av_match_percent

test_input_vectors

test_tf_idf

test_topics

test_topics_pos

topics

topics_pos

train

train_tf_idf

Views

Structure

Data

Constraints

Indexes

Triggers

DDL

Grid view

Form view

Column: url

Data type: VARCHAR

Table: topics

ROWID: 3

Constraints: PRIMARY KEY

Filter data

Total rows loaded: 5284

	url	topic	file_name
1	https://en.wikiquote.org/wiki/Sigmund_Freud	Freud dangerous never picture underestimate	f0_
2	https://www.youtube.com/watch?v=9ZNrxn5niyg	Freud dangerous never picture underestimate	f0_
3	https://en.wikipedia.org/wiki/A_Dangerous_Method	Freud dangerous never picture underestimate	f0_
4	https://www.am...	Freud dangerous never picture underestimate	f0_
5	https://www.the...	Freud dangerous never picture underestimate	f0_
6	https://www.yoi...	Freud dangerous never picture underestimate	f0_
7	https://www.ps...	Freud dangerous never picture underestimate	f0_
8	https://www.ba...	Freud dangerous never picture underestimate	f0_
9	https://en.wikip...	Freud dangerous never picture underestimate	f0_
10	https://www.spa...	Freud dangerous never picture underestimate	f0_
11	https://www.jstor.org/stable/1343491	Freud dangerous never picture underestimate	f0_
12	https://brewminate.com/the-story-and-mind-of-sigmund-...	Freud dangerous never picture underestimate	f0_
13	https://www.britannica.com/topic/Spanish-Inquisition	Spanish inquisition	f1_
14	https://simple.wikipedia.org/wiki/Spanish_Inquisition	Spanish inquisition	f1_
15	https://en.wikipedia.org/wiki/Spanish_Inquisition	Spanish inquisition	f1_
16	https://en.wikipedia.org/wiki/Black_Legend_of_the_Spanis...	Spanish inquisition	f1_
17	https://en.wikipedia.org/wiki/The_Spanish_Inquisition_(Mo...	Spanish inquisition	f1_
18	https://en.wikipedia.org/wiki/Medieval_Inquisition	Spanish inquisition	f1_
19	https://www.britannica.com/list/timeline-of-the-spanish-i...	Spanish inquisition	f1_
20	https://history.howstuffworks.com/historical-figures/spani...	Spanish inquisition	f1_
21	https://www.donquijote.org/spanish-culture/history/spani...	Spanish inquisition	f1_
22			

site_data (site_db0)

search_results (site_db0)

cl_attr (site_db0)

test_attr (site_db0)

test_search_results (site_db0)

test_site_data (site_db0)

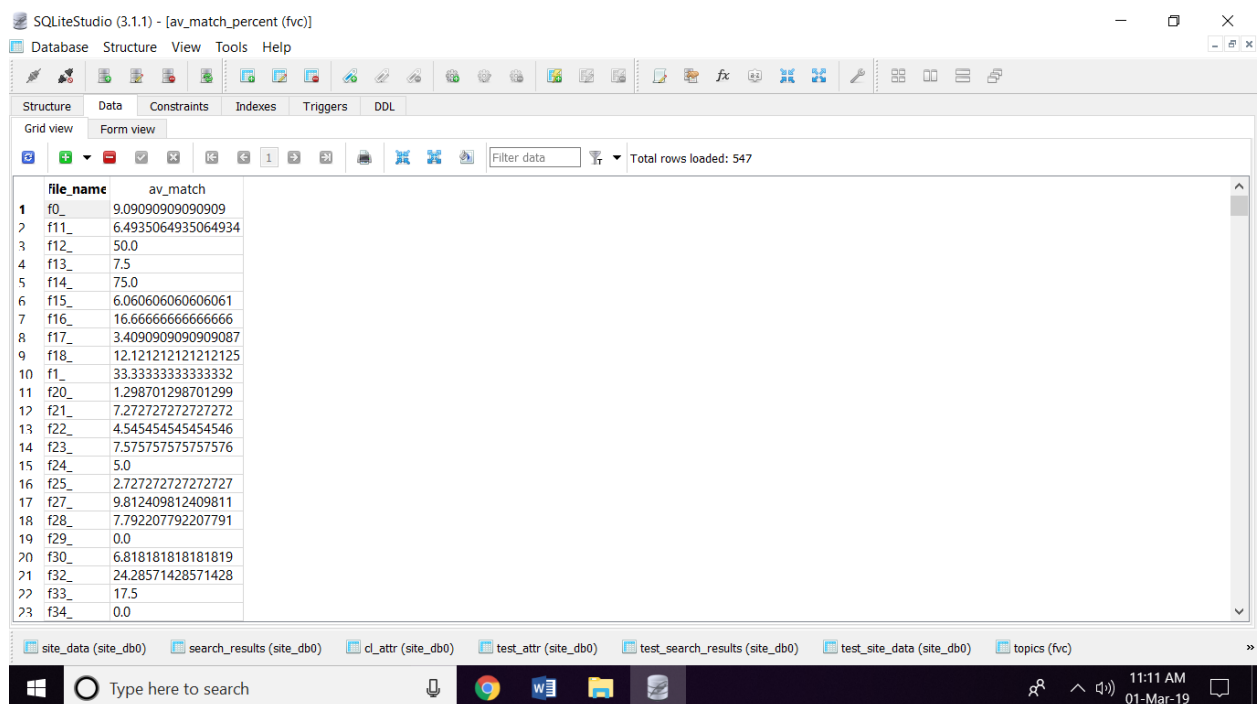
topics (fvc)

Type here to search

11:03 AM 01-Mar-19

FIGURE 11. URL, Topic, File_Name in database

For each of the ten URLs retrieved for each topic, Scrapy Framework is used in Python along with Newspaper3k library. The Newspaper3k library allows for efficient parsing of the web page whose URL is being used to find the match percentage of the topic in the content. Using the Newspaper3k library keywords are extracted from the text of the web page. Thereafter, average match percent is calculated for the topic words in the keywords extracted. In this way, the stance of the topic with the content of the website is calculated and averaged over the ten URLs retrieved for each topic. This gives us a rough idea as to how much the content of each video matches on the web. The average match percent for the web thus obtained for each file is stored in the database as shown in Figure 12.



SQLiteStudio (3.1.1) - [av_match_percent (fvc)]

Database Structure View Tools Help

Structure Data Constraints Indexes Triggers DDL

Grid view Form view

Filter data Total rows loaded: 547

	file_name	av_match
1	f10_	9.09090909090909
2	f11_	6.4935064935064934
3	f12_	50.0
4	f13_	7.5
5	f14_	75.0
6	f15_	6.060606060606061
7	f16_	16.666666666666666
8	f17_	3.4090909090909087
9	f18_	12.121212121212125
10	f1_	33.333333333333332
11	f20_	1.298701298701299
12	f21_	7.272727272727272
13	f22_	4.545454545454546
14	f23_	7.575757575757576
15	f24_	5.0
16	f25_	2.727272727272727
17	f27_	9.812409812409811
18	f28_	7.792207792207791
19	f29_	0.0
20	f30_	6.818181818181819
21	f32_	24.28571428571428
22	f33_	17.5
23	f34_	0.0

site_data (site_db0) search_results (site_db0) cl_attr (site_db0) test_attr (site_db0) test_search_results (site_db0) test_site_data (site_db0) topics (fvc)

Type here to search

11:11 AM 01-Mar-19

FIGURE 12. File_Name, Average_Match_Percent in database

In all, the following features are extracted from the video file: CCCoGV vector, average match percent on web, noun percentage, verb percentage, adjective percentage, adverb

percentage, conjunction percentage, pronoun percentage, question percentage and determiner percentage. All the features are stored in one table for further processing (Figure 13).

SQLiteStudio (3.1.1) - [train (fvc)]

Database Structure View Tools Help

Grid view Form view Filter data Total rows loaded: 571

	fname	input_vector	av_match_percent	noun_percent	verb_percent	adj_percent	adv_percent	conjunction_percent	pronoun_percent	ques_percent	det_percent	label
1	f0	1250, 179, 94, ...	9.09090909090909	20.0	0.0	40.0	20.0	0.0	0.0	0.0	0.0	0
2	f10	547, 76, 58, 42...	0	0	0	0	0	0	0	0	0	0
3	f11	1210, 89, 28, 7...	6.4935064935064934	33.3333333333...	0.0	0.0	0.0	8.33333333333332	0.0	0.0	4.1666666...	0
4	f12	1661, 113, 34, ...	50.0	100.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0
5	f13	873, 114, 39, 1...	7.5	25.0	0.0	0.0	16.6666666...	0.0	0.0	0.0	8.3333333...	0
6	f14	798, 69, 50, 26...	75.0	33.333333333...	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0
7	f15	3220, 260, 87, ...	6.060606060606061	24.1379310344...	0.0	3.4482758620...	10.3448275...	6.896551724137931	3.44827586206...	3.448275862...	3.4482758...	0
8	f16	2348, 86, 42, 1...	16.666666666666666	18.1818181818...	9.0909090909...	9.0909090909...	18.1818181...	0.0	9.0909090909...	0.0	9.090909...	0
9	f17	3005, 307, 12...	3.4090909090909087	29.4117647058...	0.0	5.8823529411...	0.0	11.76470588235294	5.88235294117...	0.0	0.0	0
10	f18	2535, 181, 75, ...	12.121212121212125	7.2727272727272...	5.4545454545...	9.0909090909...	5.45454545...	7.27272727272725	14.5454545454...	9.090909090...	1.8181818...	0
11	f19	1269, 75, 19, 1...	0	0	0	0	0	0	0	0	0	0
12	f1	1068, 183, 89, ...	33.33333333333332	20.0	0.0	20.0	0.0	0.0	0.0	0.0	0.0	0
13	f20	1654, 280, 16...	1.298701298701299	13.0434782608...	4.3478260869...	8.6956521739...	8.69565217...	8.695652173913043	8.69565217...	11.538461538461538	3.84615384	0
14	f21	1286, 245, 76, ...	7.272727272727272	26.9230769230...	0.0	11.538461538...	0.0	0.0	0.0	0.0	0.0	0
15	f22	1794, 430, 15...	4.545454545454546	12.9032258064...	9.6774193548...	3.2258064516...	12.9032258...	12.903225806451612	32.2580645...	0.0	4.1666666...	0
16	f23	2318, 299, 12...	7.575757575757576	16.6666666666...	4.1666666666...	8.3333333333...	8.33333333...	12.5	8.3333333333...	0.0	4.1666666...	0
17	f24	872, 118, 34, 1...	5.0	22.2222222222...	0.0	11.111111111...	0.0	0.0	11.111111111...	0.0	11.111111...	0
18	f25	741, 149, 49, 4...	2.727272727272727	23.8095238095...	4.7619047619...	19.047619047...	0.0	14.285714285714285	4.76190476190...	4.761904761...	4.7619047...	0

Status

[11:22:18] Committed changes for table 'train' successfully.

site_data (site_db0) search_results (site_db0) cl_attr (site_db0) test_attr (site_db0) test_search_results (site_db0) test_site_data (site_db0) topics (fvc)

Type here to search

11:23 AM 01-Mar-19

FIGURE 13. Feature Table

For classifying the videos into real or fake category, three classifiers (LSTM, Convolutional Neural Network and Naïve Bayes) are used and results are compared from the output of each of the three.

3.4 Importance and Limitations

This work however has some limitation which is that, to transcribe the audio into text file, the audio should be in English language. Therefore, content in other languages is not analyzed in our model.

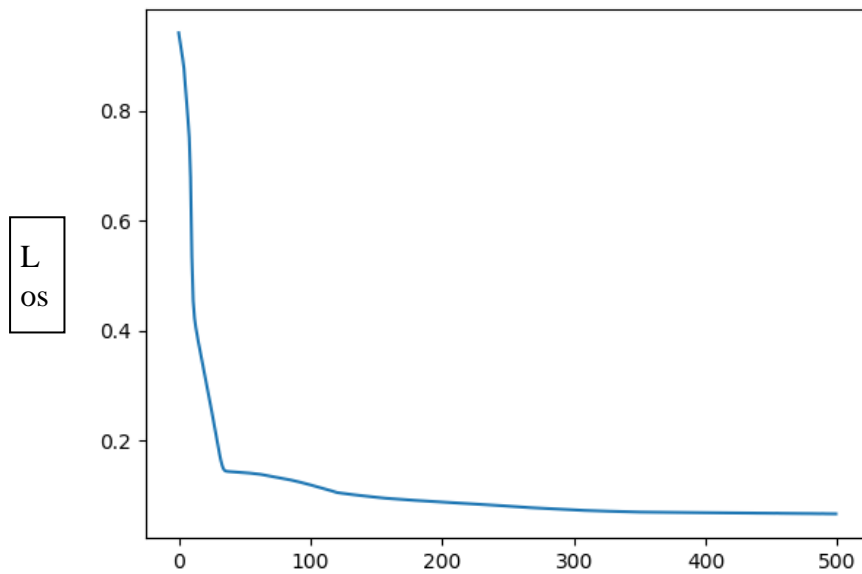
3.5 Ethics

The work has been carried out in accordance with the ethical guidelines. The Scrapy crawler used in the work is in accordance with the “robots.txt” file for the websites from which the features are collected.

CHAPTER 4: RESULTS AND CONCLUSIONS

As mentioned above, the performance of three different classifiers has been compared for the problem at hand. Two of these classifiers (Convolutional Neural Network and LSTM) are based on deep learning techniques and the third classification model used is Naïve Bayes Classifier.

The deep learning classifiers have been trained with keeping number of epochs as 500 in both the classifier models. Figures 14 and 15 show the evolutions of training loss with the epochs for LSTM and Convolutional Neural Network respectively.



Epochs

FIGURE 14. Training Loss Evolution for LSTM

Loss

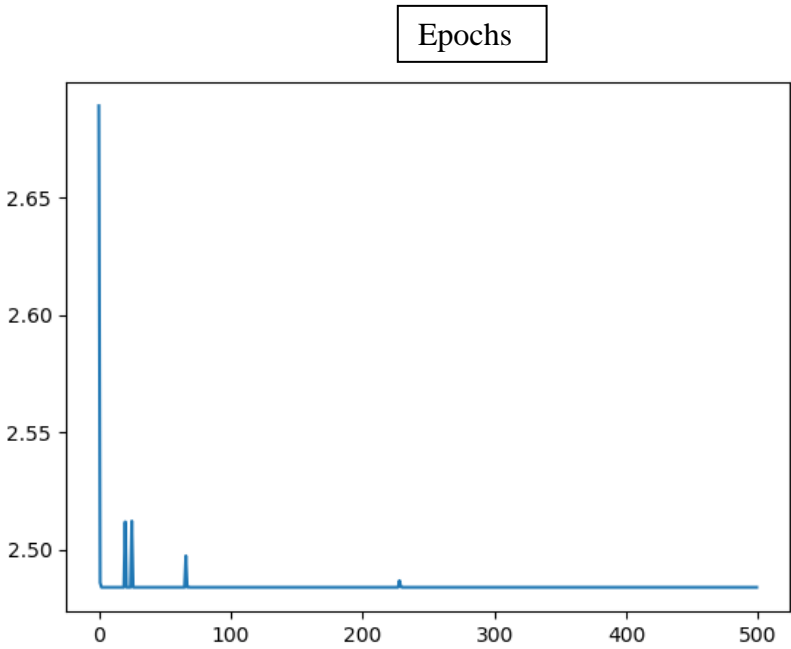


FIGURE 15. Training Loss Evolution for Convolutional Neural Network

To evaluate the classification accuracy of the model with the three classifiers, the performance is tested on the same training and testing dataset. The comparison of classification accuracies is shown in Table 1.

	Number of Epochs	Classification Accuracy
Naïve Bayes Classifier	NA	83.45%
Convolutional Neural Network	500	84.59%
LSTM	500	95.45%

TABLE 1. Classification Accuracies for Different Classifiers

Our model outperformed the state of the art method of [35]. Furthermore, it is observed that LSTM model outperformed the other classifiers and achieved classification accuracy as high as 95.45%.

As above, this work however has some limitation which is that, to transcribe the audio into text file, the audio should be in English language i.e. content in other languages is not analyzed in our model. This also forms an interesting area for future research. Also, this model doesn't take into consideration intra-frame forgery in videos.

APPENDIX

- 1) Fig. Choice of news sources for different generations

The Generation Gap

The younger the consumer, the more dramatic the shift away from traditional news outlets. Here's the percentage of each age group who say they often get news from ...

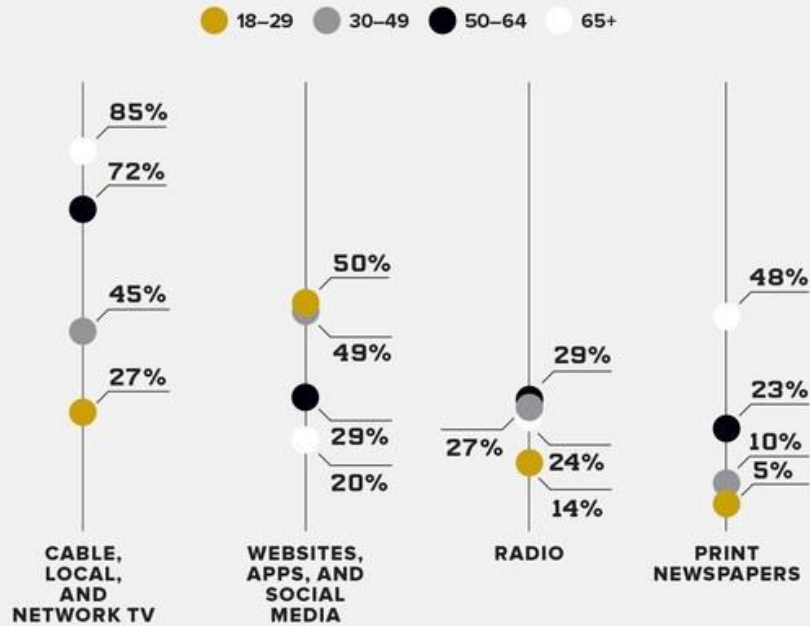


Figure 5. Survey Results

- 2) For interested readers more information on the concept of Filter Bubbles can be found at <https://fs.blog/2017/07/filter-bubbles/> (How filter bubbles distort reality: Everything you need to know)

REFERENCES

- [1] Niall J. Conroy, Victoria L. Rubin and Yimin Chen. Automatic Deception Detection: Methods for Finding Fake News. ASIST, 2015
- [2] Veronica Perez-Rosas, Bennett Kleinberg, Alexandra Lefevre and Rada Mihalcea. Automatic Detection of Fake News, 2017
- [3] Sarah Elkasrawi, Syed Saqib Bukhari, Ahmed Abdelsamad and Andreas Dengel. What you see is what you get? Automatic Image Verification for Online News Content. In IAPR, 2016
- [4] Kai Shu, Amy Sliva, Suhang Wang, Jiliang Tang and Huan Liu. Fake News Detection on Social Media: A Data Mining Perspective. In ACM SIGKDD Explorations Newsletter, 2017
- [5] James Thorne, Mingjie Chen, Giorgos Myrianthous, Jiashu Pu, Xiaoxuan Wang and Andreas Vlachos. Fake News Detection using Stacked Ensemble of Classifiers. EMNLP workshop on Natural Language Processing meets Journalism, pages 80-83, 2017
- [6] Benjamin D. Horne and Sibel Adah. This Just In: Fake News Packs a Lot in Title, Uses Simpler, Repetitive Content in Text Body, More Similar to Satire than Real News. International Workshop on News and Public Opinion at ICWSM, 2017
- [7] Yimin Chen, Niall J. Conroy and Victoria L. Rubin. Misleading Online Content: Recognizing Clickbait as “False News.” In ACM WMDD, 2015
- [8] Alvaro Figueira, Luciana Oliveira. The current state of fake news: challenges and opportunities. Procedia Computer Science, pages 817-825, 2017
- [9] Sakeena M. Sirajudeen, Nur Fatihah A. Azmi, Adamu I. Abubakar. Online Fake News Detection Algorithm. Journal Of Theoretical And Applied Information Technology, 2017

- [10] Chengjiang Long, Arsalan Basharat and Anthony Hoogs. A Coarse to Fine Deep Convolutional Neural Network Framework for Frame Duplication Detection and Localization in Video Forgery. In arXiv:1811.10762v1, November, 2018
- [11] Qiong Dong, Gaobo Yang and Ningbo Zhu. A MCEA based passive forensics scheme for detecting frame-based video tampering. Elsevier, 2012
- [12] Isilay Bozkurt, Mustafa Hakan Bozkurt and Guzin Ulutas. A new video forgery detection approach based on forgery line. Turkish Journal Of Electrical Engineering and Computer Sciences, 2017
- [13] Sowmya K.N., H.R. Chennamma. A Survey On Video Forgery Detection. International Journal of Computer Engineering and Applications, Volume IX, Issue II, February 2015
- [14] Qian Li, Rangding Wang and Dawen Xu. An Inter-Frame Forgery Detection Algorithm for Surveillance Video. In Information, 2018
- [15] Marco Fontani, Simone Milani, Mauro Barni and Alessandro Piva. An overview on video forensics. APSIPA Transactions on Signal and Information Processing, Volume 1, December 2012
- [16] Dario D'Avino, Davide Cozzolino, Giovanni Poggi and Luisa Verdoliva. Autoencoder with recurrent neural networks for video forgery detection. IS&T International Symposium on Electronic Imaging, 2017
- [17] Sowmya K.N. and Dr. H.R. Chennamma. Challenges in Surveillance Video Forgery Detection. In IJSER, Volume 8, Issue 5, May 2017

- [18] Hareesh Ravi and A.V. Subramanyam. Compression Noise based Video Forgery Detection. October 2014
- [19] V. Voronin, R. Sizyakin, A. Zelensky, A. Nadykto and I. Svirin. Detection of deleted frames on videos using a 3D convolutional neural network. November 2018
- [20] D. Vazquez-Padin, M. Fontani, T. Bianchi, P. Comesana, A. Piva and M. Barni. Detection of Video Double Encoding with GOP Size Estimation. In IEEE, 2012
- [21] Aldrina Christian and Ravi Sheth. Digital Video Forgery Detection And Authentication Technique – A Review. In IJSRST, 2016
- [22] Weihong Wang and Hany Farid. Exposing Digital Forgeries in Video by Detecting Double Quantization. In ACM, 2009
- [23] Tanfeng Sun, Wan Wang and Xinghao Jiang. Exposing Video Forgeries by Detecting MPEG Double Compression. In IEEE, 2012
- [24] Davide Cozzolino, Justus Thies, Andreas Rossler, Christian Riess, Matthias Niebner and Luisa Verdoliva. ForensicTransfer: Weakly-supervised Domain Adaptation for Forgery Detection. In arXiv: 1812.02510v1, December, 2018
- [25] Wan Wang, Xinghao Jiang, Shilin Wang and Tanfeng Sun. Identifying Video Forgery Process using Optical Flow. 2014
- [28] Qi Han and Sondas M Fadl. Inter-Frame Forgery Detection Based on Differential Energy of Residue. IET Image Processing, December, 2018

- [29] Jigar Ratnottar, Rutika Joshi and Manish Shrivastav. Comparative Study of Motion Estimation & Motion Compensation for Video Compression. In IJETTCS, Volume1, Issue 1, May-June, 2012
- [30] Raahat Devender Singh and Naveen Aggarwal. Video content authentication techniques: A comprehensive survey. Springer, 2017
- [31] Yanli Li, Lala Mei, Ran Li and Changan Wu. Using Noise Level to Detect Frame Repetition Forgery in Video Frame Rate Up-Conversion. In Future Internet, 2018
- [32] Viacheslav Voronin, Aleksandr Zelensky and Iliya Svirin. Video Content Verification Using Blockchain Technology. In IEEE, 2018
- [33] A. Gironi, M.Fontani, T. Bianchi, A.Piva and M. Barni. A Video Forensic Technique for Detecting Frame Deletion and Insertion. In IEEE, 2014
- [34] A.V. Subramanyam and Sabu Emmanuel. Video Forgery Detection Using HOG Features and Compression Properties. In IEEE, 2012
- [35] Qi Wang, Zhaohong Li, Zhenzhen Zhang and Qinglong Ma. Video Inter-Frame Forgery Identification Based on Consistency of Correlation Coefficients of Gray Values, Journal Of Computer and Communications, 2014
- [36] Moises H.R. Pereira, Flavio L.C. Padua, Adriano C.M. Pereira, Fabricio Benevenuto and Daniel H. Dalip. Fusing Audio, Textual and Video Features for Sentiment Analysis of News Videos. In ICWSM, 2016
- [37] Massimo De Santo, Gennaro Percannella, Carlo Sansone and Mario Vento. Segmentation of News Videos Based on Audio-Video Information. 2007

[38] Hazim Kemal Ekenel and Tomas Semela. Multimodal genre classification of TV Programs and Youtube videos. In Springer, 2013

[39] <https://www.wordstream.com/blog/ws/2017/03/08/video-marketing-statistics>

[40] Gonzales and Woods. Digital Image Processing