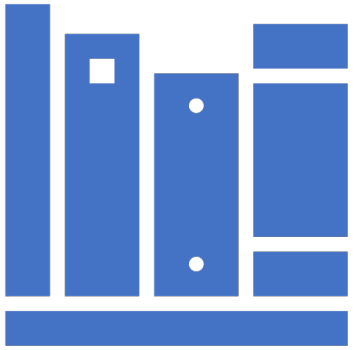


PROPOSAL PRESENTATION

Lokesh Kishor Nandanwar
WMA190005

RESEARCH TOPIC:

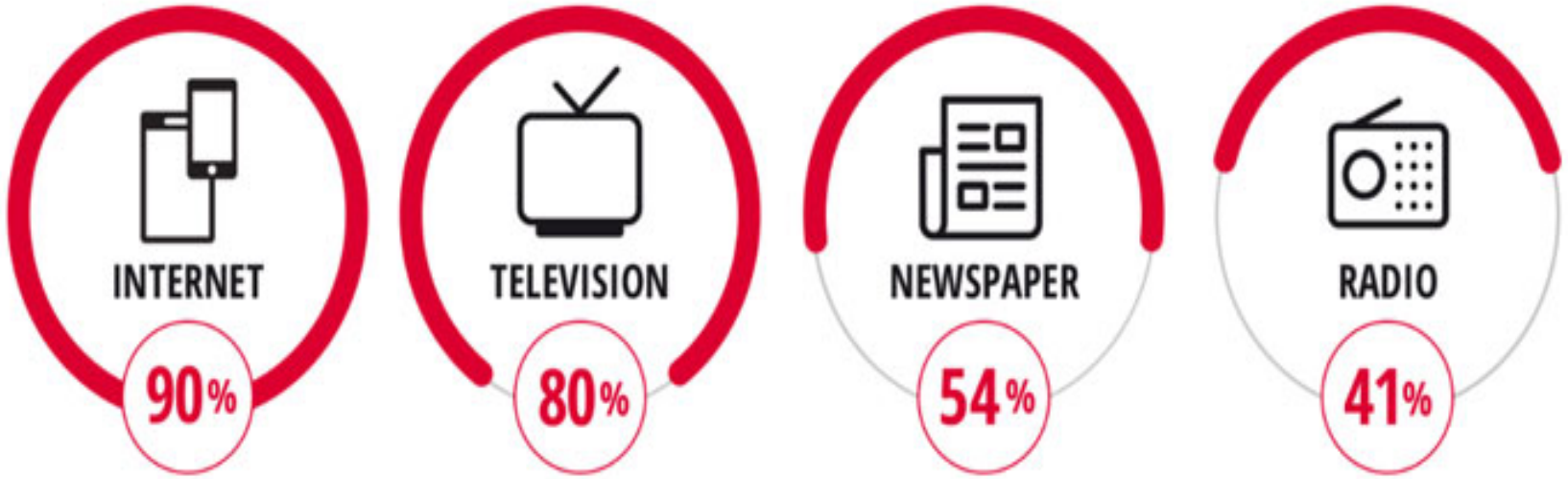
Forged text detection method in Video, Natural Scene and Document Images

CONTENT OVERVIEW

- Introduction
- Literature Review
- Problem statement
- Research Questions
- Research Objectives
- Scope of Study
- Proposed Methodology
- Preliminary Results
- Significance of the Work
- Research Study Timeline

INTRODUCTION

MULTIMEDIA CONSUMPTION AROUND THE WORLD



- Prominent methods of exchanging information
- Increase in easy to use and inexpensive devices.
- Social Media platforms
- Use of Internet cloud
  - Easy to access, process, store and share.

INTRODUCTION:

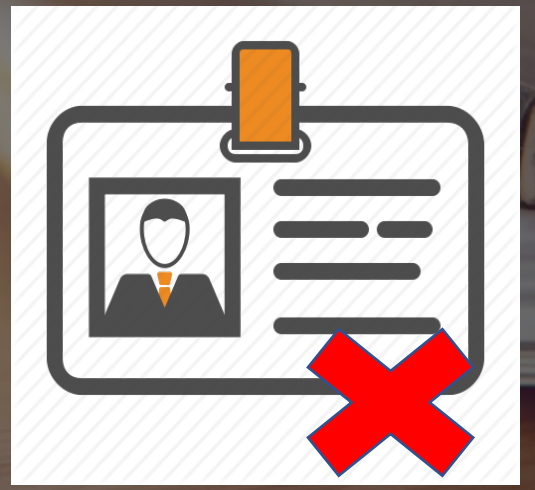
Rate of visual media consumption has increased the rate of crimes and frauds.

Low-cost digital imaging devices available with advanced features.

Easy to manipulate the visual media using these softwares.

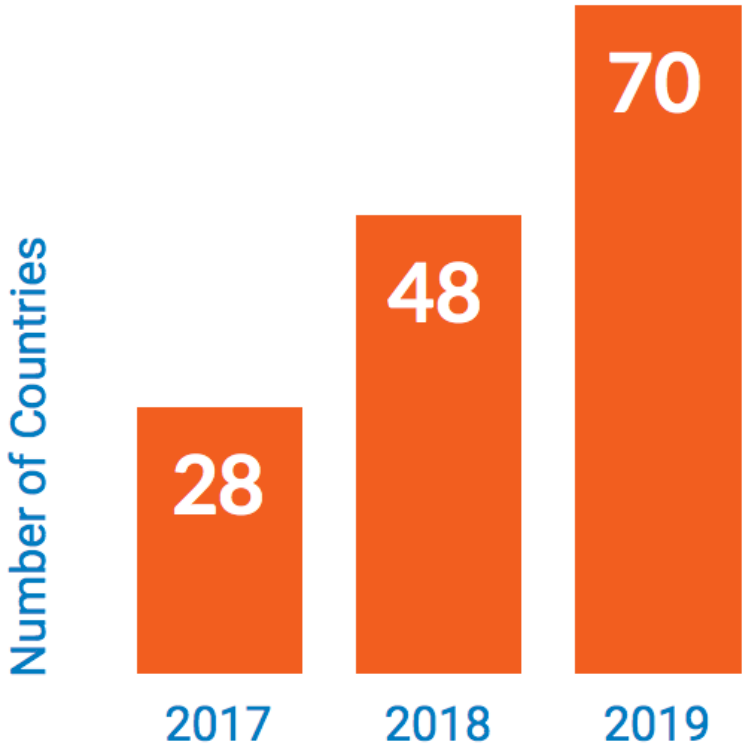
INTRODUCTION:

- The credibility of digital multimedia content is no longer be taken for granted.
- Altering, tampering and forging content is a serious threat for forensic applications such as:
  - forging property, insurance, certificates, banking documents
  - creating fake suicide notes and fake answer scripts.
  - image manipulation on medicine, justice, news reporting and accounting professions, etc



INTRODUCTION

Hers's how social media misinformation/crimes/frauds increased in the world



150%

the increase in countries using organised social media manipulation campaigns over the last two years

INTRODUCTION

OUR FOCUS : FORGED TEXT DETECTION

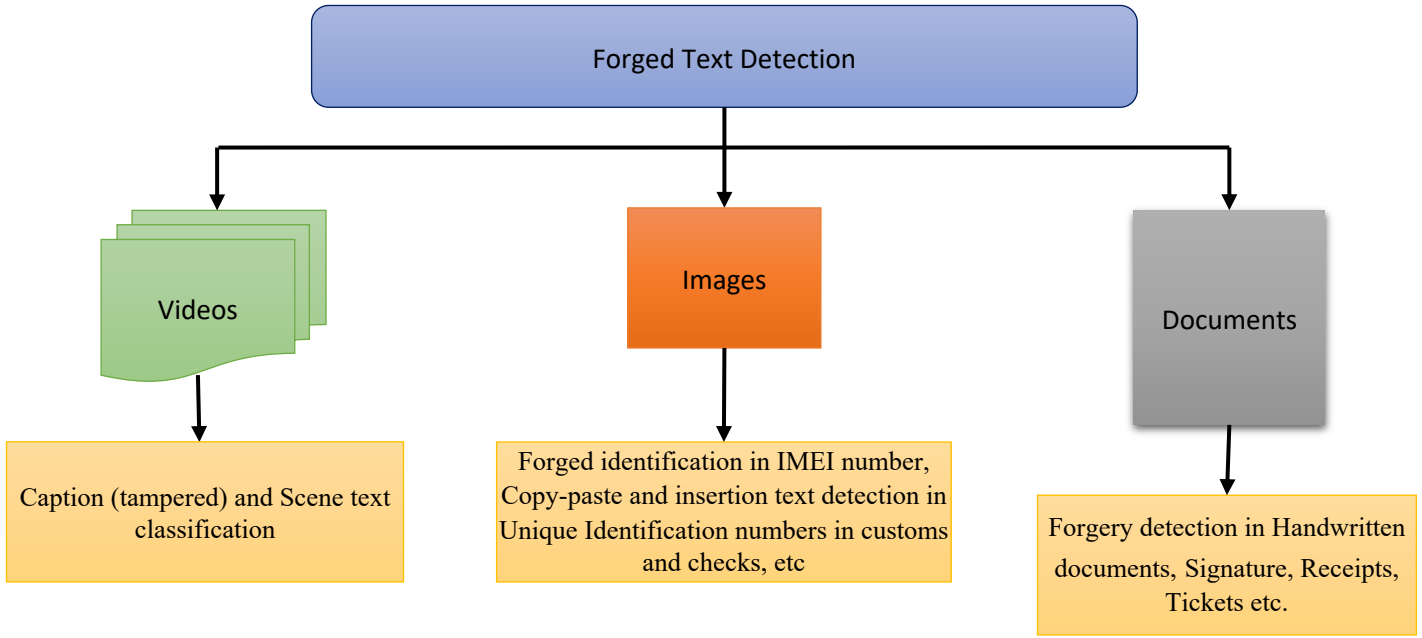
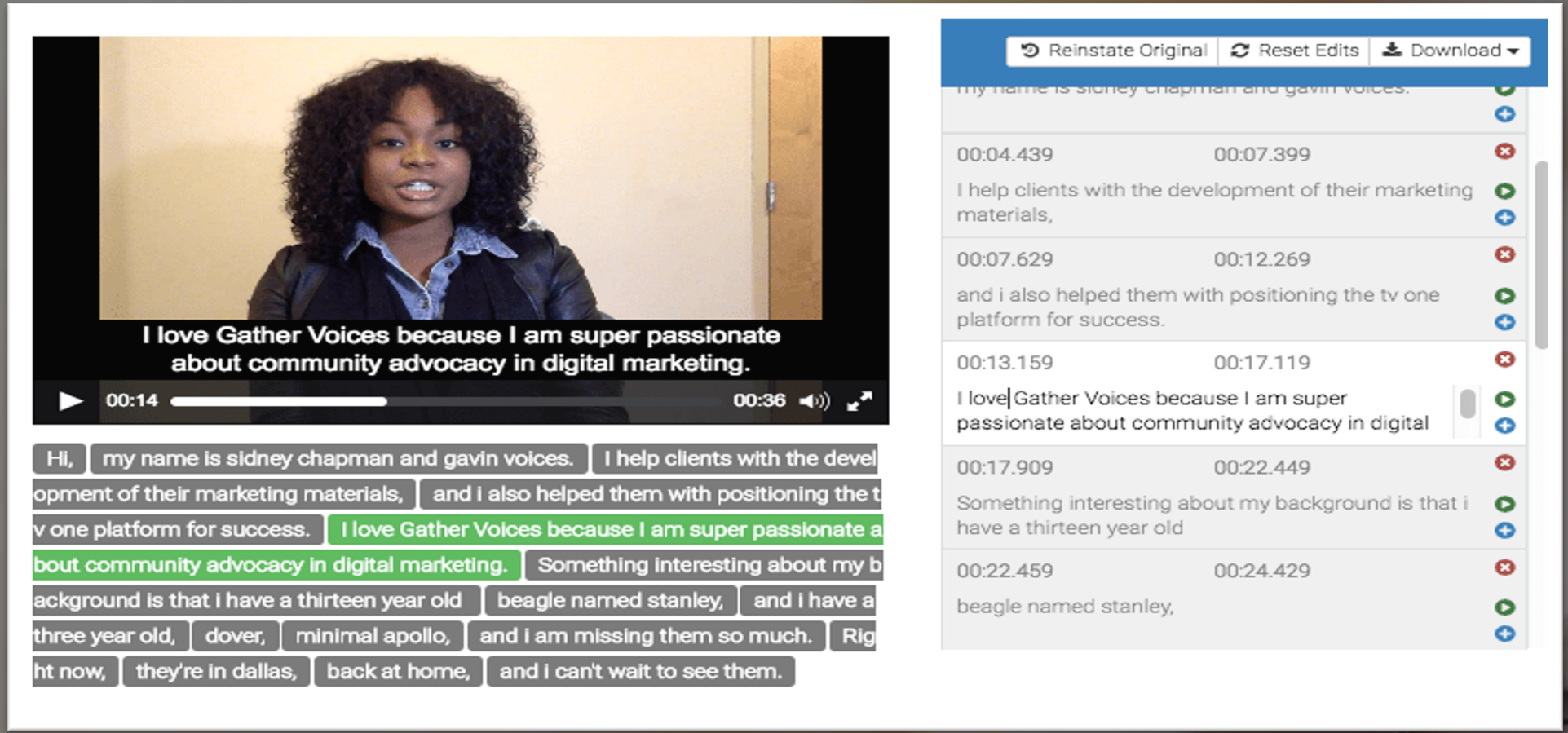


Fig. 1. Forged text detection in multimedia



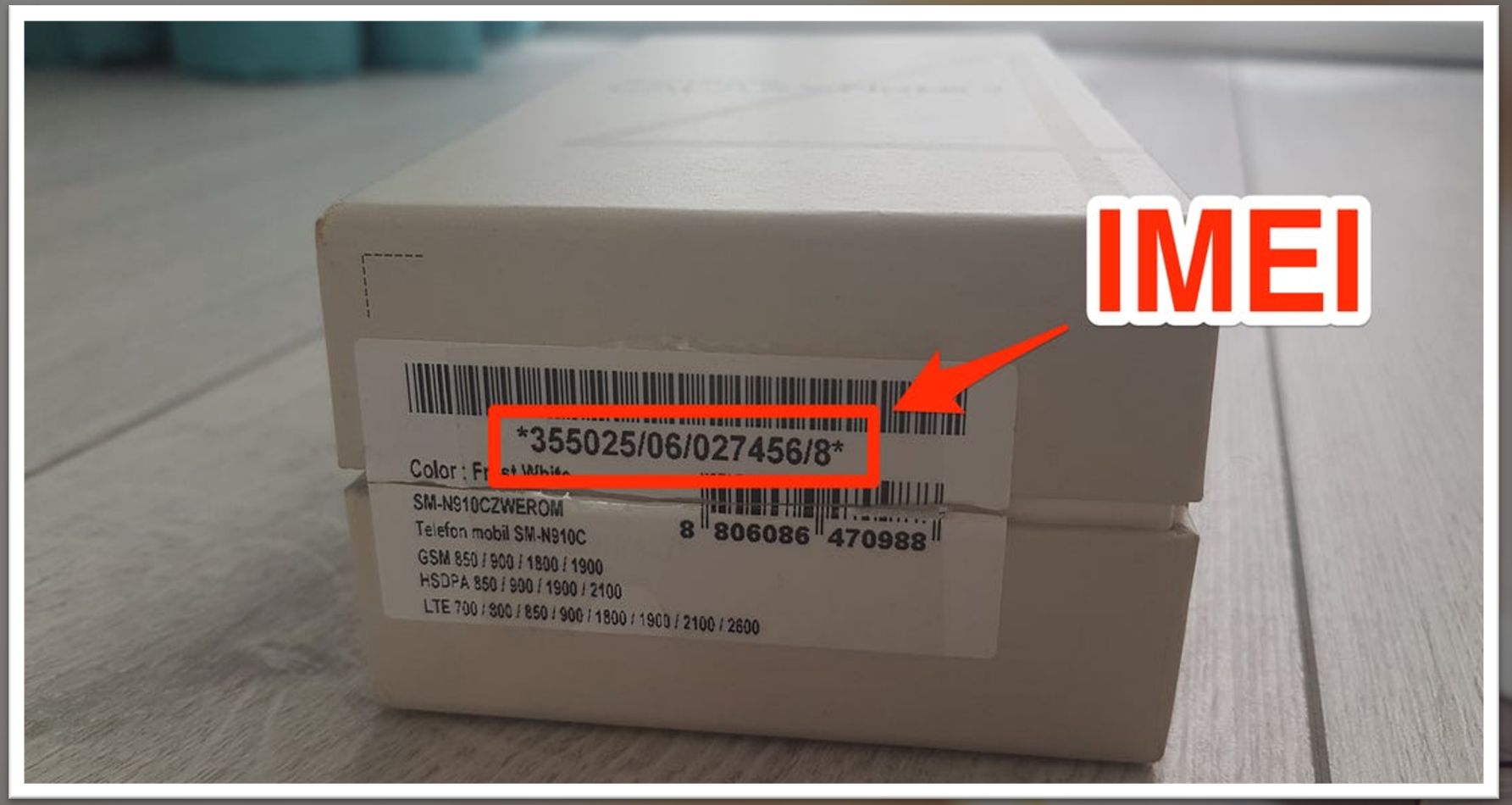
Applications: Caption and Scene text classification Video annotation or video understanding at semantic level

Forged text detection in Videos

(a) Scene text image (b) Caption (tampered) text image

Fig. 2. Example of Scene and Caption text in action videos.

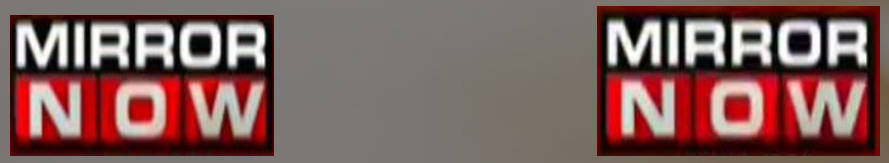
- Caption text is used to annotate at semantic level.
- Scene text is used to understand the content.
- Caption text is inserted text.
- Example: News reporting, teleshopping's, Cooking shows, Defence discoveries, Social Media etc.



Applications: IMEI number forgery detection
Avoid smuggling and illegal selling, second handle mobile selling

Forged text detection in still images

(a) Original and forged IMEI numbers created using copy-paste operations are marked by a green and red color, respectively.



(b) Original and forged text created using copy-paste operation in still images.

(c) Original and forged text created using insertion operation in still images.

Fig.3. Examples of copy-paste and insertion operations for creating forged text images.

- Forensics and Forgery identification.
- Copy-paste and insertion operation are used.
- Hard to notice the difference between the original images and the forged ones.
- Detect smart phones for stealing and smuggling them illegally.
- Second handle mobile selling
- Customs and import/export items UID check, etc.

Fake e-ticket cases at airports in 2018 highest in four years; agencies mull alternatives

PTI | Dec 30, 2018, 05.19 PM IST

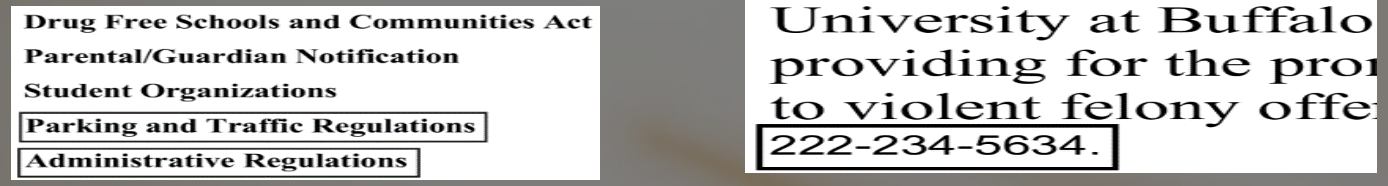
NEW DELHI: Incidents of fake e-tickets usage to gain illegal entry into Indian airports were highest in 2018 in past four years, prompting security agencies to moot biometric or barcode-based access system for passengers.

While security officials ruled out any terror-like or extreme sabotage threat in these recorded incidents, they expressed concern over the potential of this menace being misused in future to breach the airport security.

As per a CISF data accessed by PTI, a total of 140 incidents (about 26 per cent more) of illegal entries of passengers using fake or cancelled e-tickets were intercepted till early December as compared to 111 such incidents registered last year. The comparative figures for 2016 were 74 while for 2015 it was 43.

Applications: Forgery detection in Documents: Avert breaching of airport security (Air ticket forgery).

Forged text detection in documents



Copy-paste operation

Insertion (imitation) operation

(a) Illustration of sample forged PDF document images by copy-paste and insertion operations. Note: altered texts are enclosed by bounding boxes, which appear to be genuine text in terms of font, color and size.

Original handwritten word

Forged handwritten word

(b) Illustration of sample forged Handwritten document images by insertion of characters. These can also be seen also be evident in case of forged signatures in documents.

(c) Original and forged Air-ticket traveler name created using copy-paste operation are marked by green and red color respectively.

Fig. 4. Example of forgery in Printed Documents and Handwritten documents.

- Avert breaching of airport security (Air ticket forgery).
- Reduce crimes in Forged property documents for ill intensions.
- Fake suicide note detection in crimes.
- Detect fake certificates.

LITERATURE REVIEW:

The methods are classified in three broad categories:

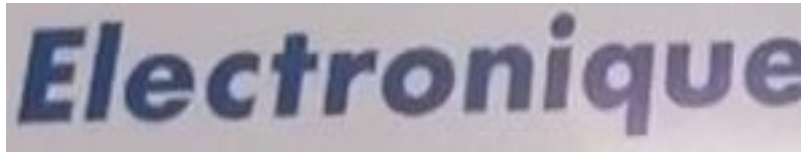
a) Forged text detection in Videos
b) Forged text detection in still images
c) Altered text detection in documents

(a) Forged text detection in Videos:

Method	Objective	Concept	Drawbacks	Multimedia formats supported
Shivakumara et al. [16], 2014	Separation of graphics and scene text in video	• Works based on the fact that caption text has high contrast and clarity, while scene text does not.	• Not robust to features as it is based on contrast and clarity. • Not adequate for text level forgery. • Not effective in case of documents	• Videos • Images
Xu et al. [17], 2014	Graphics and scene text classification in video.	• based on contrast and clarity • Extracting distinct features through distribution of Eigen values.	• Not robust to features as it is based on contrast and clarity. • Not adequate for text level forgery. • Not suitable for documents	• Videos • Images
Roy et al. [18], 2016	Tampered features for scene and caption text classification in video frames	• DCT coefficients to differentiate caption text from scene text.	• Not effective for Documents images • Poor performance for complex images	• Videos • Images
Bhardwaj and Pankjakshan [19], 2016	Image overlay text detection based on JEPG truncation error analysis.	• Extracts tampered features through truncation errors given by a color filter array for detecting caption text in video	• Not adequate for forged text caused by copy-paste and insertion operations • Poor Performance for Documents images.	• Videos • Images
Chen et al. [7], 2016	Automatic detection of object-based forgery	• Frame Manipulation Detector and Forgery Identification	• Focus on visual content and not text in videos frames • Not robust for forged text caused by copy-paste and insertion operations	• Video
Feng et al. [8], 2017	Digital video forensic	• motion adaptive frame deletion detection		• Video
Amiano et al. [9], 2018	Video copy-move detection and localization	• patch match based dense field algorithm		• Video • Images
Fadi et al. [15], 2019	Inter-frame forgery detection	• Use of spatio-temporal information		• Video
Ghosh et. al [20], 2019	Presence of graphical text in scene images	• Based on CNN • Edited text and text in natural scene images as a graphical text for classification	• Method does not consider caption and scene text in video images • Not robust as Graphical text can also be present as caption or scene text.	• Video • Images

IMPLEMENTATION OF EXISTING METHODS

Caption text (Forged/Edited)



Scene text(Original)

(a) Roy et. al [18] (2016) classifies Caption text as scene text and vice-versa due of weak feature extraction as distortion is not noticeable

Caption text detected as Scene text

Scene text detected as Caption text

(b) Ghosh et. al [20] (2019) based on CNN failed to detect the forgery classifies caption text as scene text and scene text as caption text due to blurriness and consistency in shape respectively.

Caption text detected as Scene text

Scene text detected as Caption text

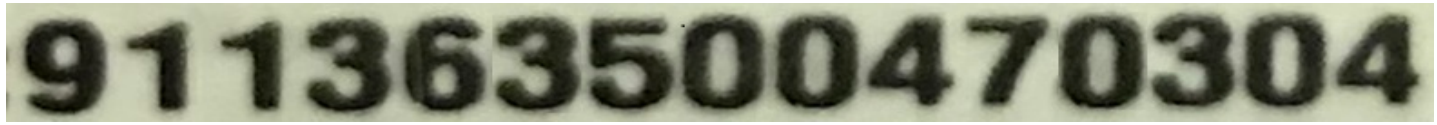
(c) Fadi et. al [15] (2019) based on spatio-temporal information failed to detect the original and tampered text, classifies caption text as scene text due to shadow in text and scene text as caption text due to no character shapes and less distortions

Fig. 5. Example of failure cases in forged video text detection.

(b) Forged text detection in Still Images:

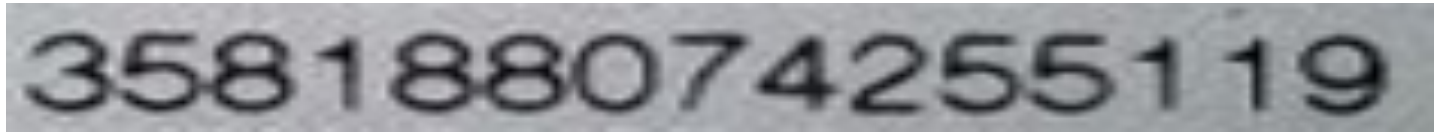
Method	Objective	Concept	Drawbacks	Multimedia formats supported
Pun et al. [21], 2015	Image forgery detection based on matchings	• adaptive over-segmentation and features point matching.	• Based on visual features and not the text information • Not robust at pixel level forgery.	• Images
Yang et al. [22], 2017	Copy-move forgery detection	• Based on hybrid features. • An improved matching algorithm		• Images
Shivakumara et al. [25], 2018	Detecting forged IMEI numbers based on color space and a fusion approach	• The variance of each color space (RGB) is used to obtain a fused image for each input image. • Features based on connected components are extracted from Canny and Sobel edge images of input and fused images for forged IMEI number detection	• If a forged image does not contain sufficient distortion, to be observed in Canny or sobel, the method doesn't work well. • Sensitive to complex background. • Template based classification	• Images • Documents
Kundu et al. [26], 2019	Fourier spectrum for classifying forged handwriting text from original, blurred and noised handwriting text images.	• Extract feature from the Fourier spectrum and the features fed to neural network classifier for classification.	• Performance degrades for character level forgery • Not suitable for small forged operations.	• Images • Documents

IMPLEMENTATION OF EXISTING METHODS



Copy-paste forgery at character level, ”3” at 6th position from left is copy-pasted

(a) Yang et al. [22], (2017) Hybrid method failed to detect the forgery by copy-paste operation due to minute distortions at pixel level in IMEI images



Original Image

(b) Shivakumara et al. [25], (2018) failed to detect the original image because of noise in the image and classified it as forged in IMEI images.

Original

forged

(c) Shivakumara et al. [25], (2018) detects blurred original text as forged and classifies forged image as original due to very less deformation in text image.

Original

forged

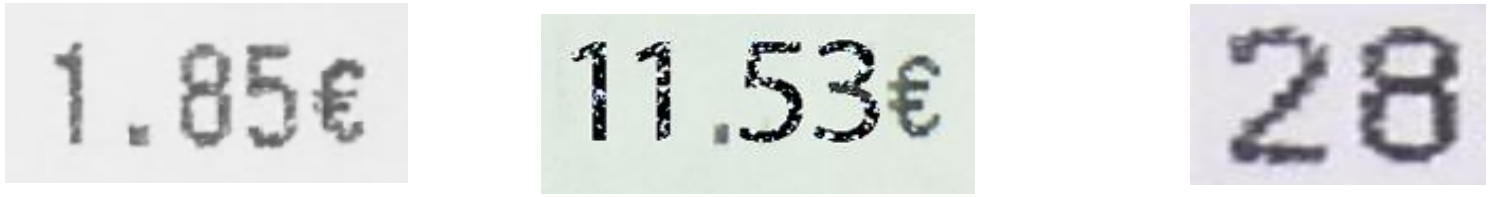
(c) Kundu et al. [26], (2019) detects both as original due to consistency in shape and uniform background even though it has unnoticeable distortions due to insertion operation.

Fig. 6. Example of failure cases in forged text detection in images.

(c) Forged text detection in documents:

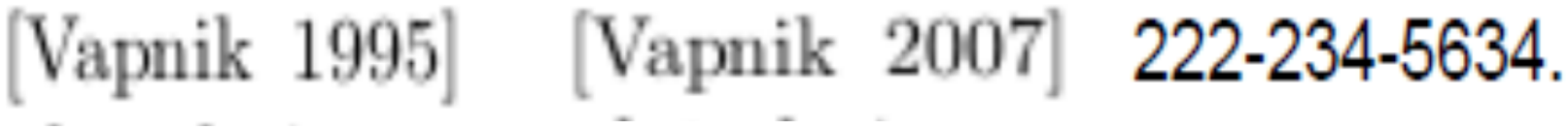
Method	Objective	Concept	Drawbacks	Multimedia formats supported
Halder and Garain [33], 2010	Color features based approach for determining ink age in printed documents.	• Color features for printed text images. • Use of ink quality based features	• Not suitable to image forgery detection, only for age estimation • Not robust for documents with noise/blur or degradations.	• Handwritten Documents
Barboza et al. [32], 2013	Color based model to determine document ages for forensic purposes	• Uses ink quality of handwritten document images captured at different intervals of time. • Identifies a given image as old or new	• Poor performance for printed documents text. • Not robust to pixel level forgery detection.	• Handwritten Documents
Khan et al. [30], 2015	Automatic ink mismatch detection	• Analyses the ink of different pens to find fraudulent documents • Effective for handwritten documents	• Ink features not robust for printed documents.	• Handwritten Documents
Luo et al. [31], 2015	Localized forgery detection in hyperspectral document images	• Explores ink quality in the hyperspectral domain for fraud document identification.	• Not effective on printed texts since when digitized, the quality of handwritten document ink changes are very low.	• Handwritten Documents
Raghunandan et al. [29], 2016	Fourier coefficients for Identifying fraud handwriting documents	• Fourier coefficients for studying the quality of handwriting documents. • Quality-based features • If a document suffers from poor quality, it is considered as an original one else a fraud one.	• Quality-based features not robust for documents affected by adverse factors, such as distortions, noises, blur, and forgery operations. • The method does not work at the text line or word levels and requires the full document	• Handwritten Documents
Wang et al. [35], 2017	Fourier-residual for printer identification from document images.	• Extracts features from residuals given by the Fourier transform for printer identification.	• The primary goal of this method is to identify printers rather than forged/tampered document images.	• Printed Documents
Khan et al. [34], 2018	Automated forgery detection in multispectral document images	• Method explores ink matching based on fuzzy k-means clustering • Partition the spectral responses of ink pixels in handwritten notes into different clusters	• Not suitable for printed text where we can see low changes in ink when digitized.	• Handwritten Documents
Berenguel et al. [28], 2019	Detecting counterfeit documents	• Based on a deep learning model • Expect some abrupt changes in the background texture of the document	• Not suitable for documents with plain background	• Printed Documents

IMPLEMENTATION OF EXISTING METHODS



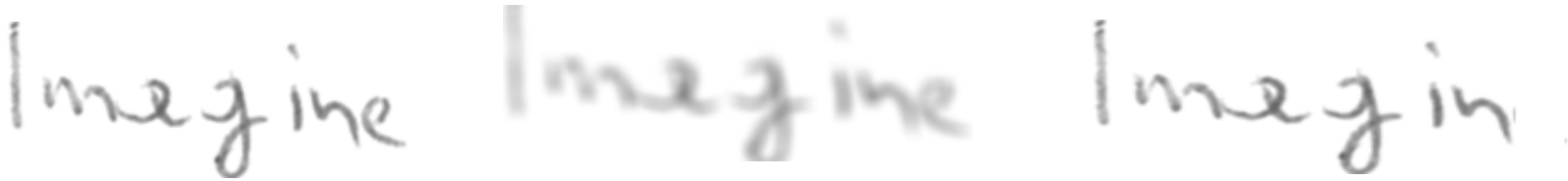
Original Insertion forgery Copy-paste forgery

(a) Wang et al. [35], (2017) fails to detect the forgery of characters in words and classifies both Price Receipts images as original.



Original Copy-paste forgery Insertion forgery

(b) Berenguel et al. [28], (2019), based on deep learning not able to detect the forgery in document images at word level when distortion is not noticeable.



Original blurred forged

(c) Kundu et al. [26], (2019) fails to detect the character level forgery classifies forge image as original and detects blurred original text as forged in air ticket images.

Fig. 7. Example of failure cases in forged text detection in images.

Summary of review:

- Methods are good when there are clear differences between forged and genuine text.
- Fails at a minute difference at the pixel level or character levels.
- Most use images/documents that do not suffer from degradations, noises, blur, poor quality, and ageing for forgery detection.
- Scope limited to single multimedia type only.

List of Challenges in Forged Text detection

Videos	Works well when the images are forged at word level but not at character level.
	Not robust to clutter background and degraded text
	Fails when the color and texture of the images varies arbitrarily
Still Images	The methods are not robust to the images affected by different resolution, contrast and blur.
	When the text contains irregular shape/sized characters, the performance of the method degrades.
	Sensitive to causes affected by perspective distortion
Documents	The success of the method depends on text or foreground information
	May not work well for the images of clutter background
	Sensitive to degradations and ageing

PROBLEM STATEMENT:

- Development of a novel method that can detect forged text in noise, blur environment and the images affected by distortion.
- Unified robust system for addressing challenges of three type of images, namely, video, still images and document images.

RESEARCH OBJECTIVES:

- To develop a new method for forged text detection in video images through classification of tampered text and natural scene text.
- To propose a new method for forged text detection in natural scene images by exploring Fourier spectrum analysis.
- To explore a new method for detecting altered text in the document images based on fusion and reconstruction of the images.
- To design and develop a unified method for detecting forgery in video, natural scene and document images.

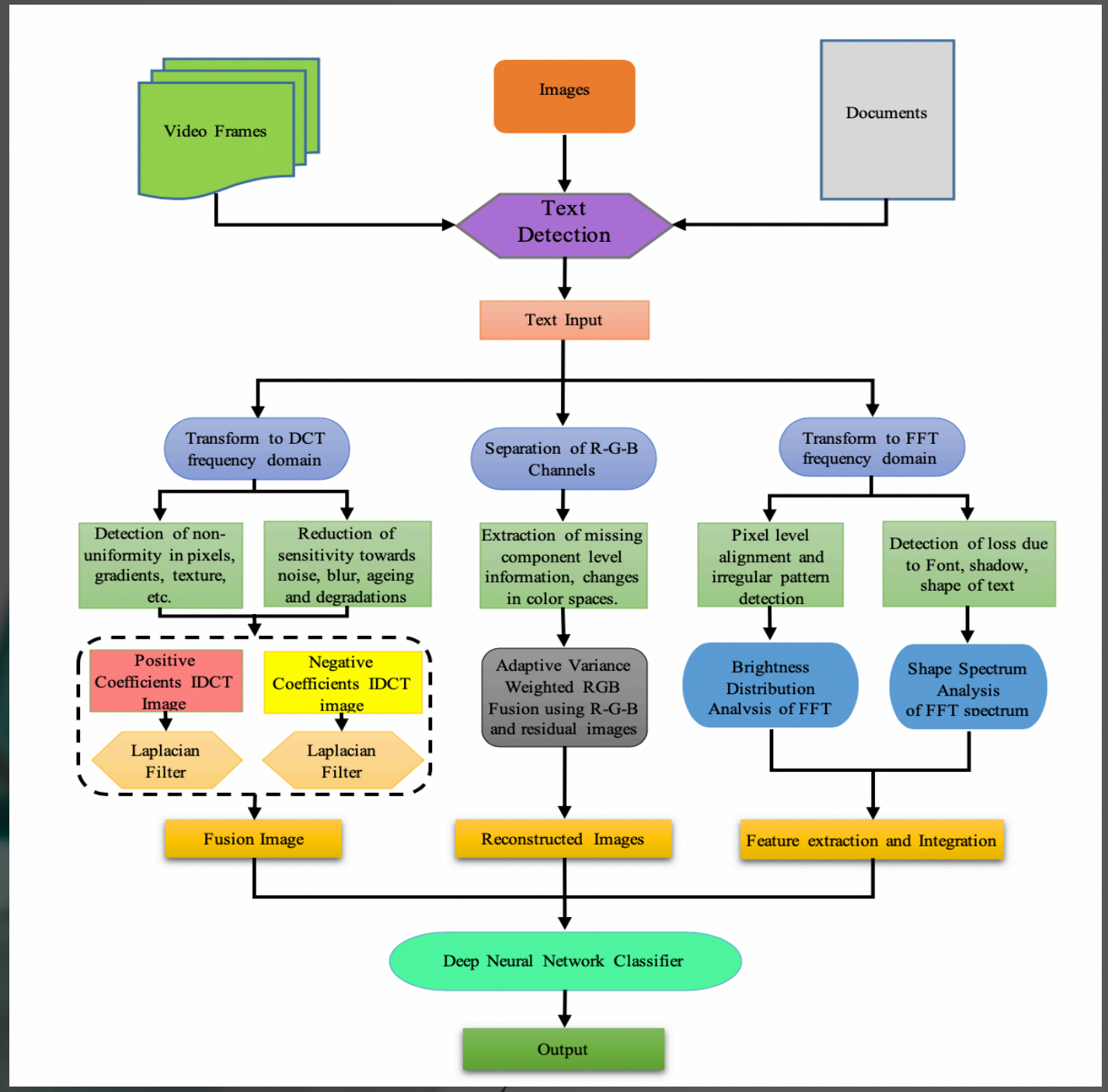
RESEARCH QUESTIONS:

- What is the way to investigate a method for forged detection through classification of tampered text and scene text in videos?
- How to explore and employ Fourier spectrum analysis to detect the forgery in natural images?
- By what means one can approach fusion and reconstruction methods to spot the changes caused by forgery in document images?
- How to develop a unified method for detecting forgery which can adapt to multiple multimedia formats such as video, natural scene and document images?

SCOPE OF THE STUDY:

- Identifying altering or tampering content in document images, forging property, insurance, certificates and other vulnerable documents
- Unified system for forgery text detection in multiple multimedia formats .
- Saving the design, development, maintenance and integration cost.
- Based on the input from the text detection system.
- Limited to the forgery in text through copy-paste, insertion, alteration operations.
- Not the scope to detect the forgery at visual context level or general image forgery.
- Documents considered for this work is limited to PDF, Handwritten texts and printed text documents only.

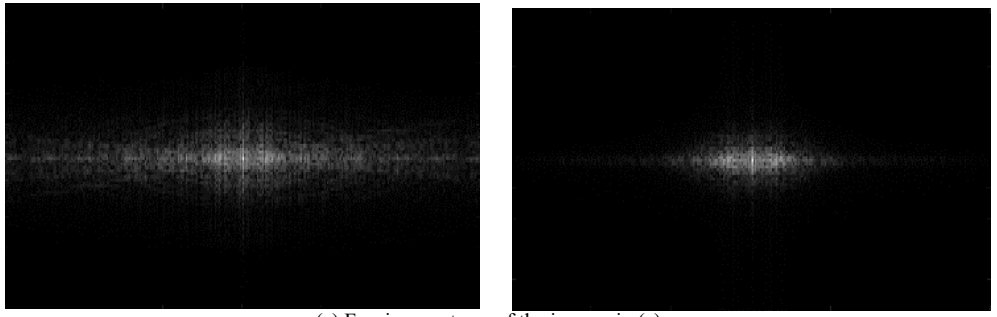
PROPOSED METHOD: DESIGN SCIENCE RESEARCH METHODOLOGY (DSRM)



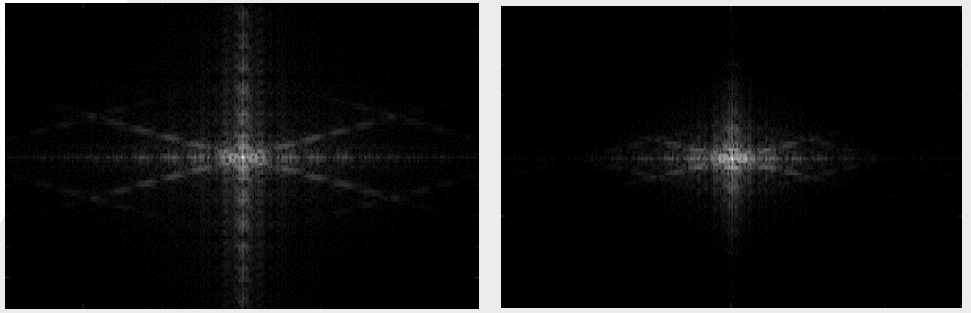
PRELIMINARY FINDINGS:

(a) Original and forged images for copy-paste operations.

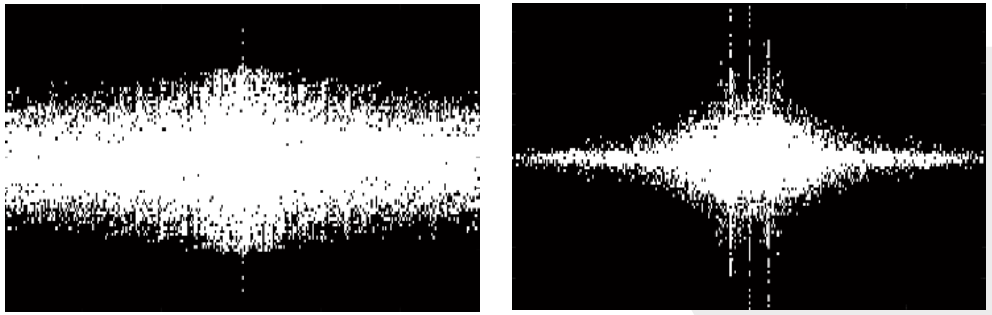
(b) Original and forged text images for insertion operation



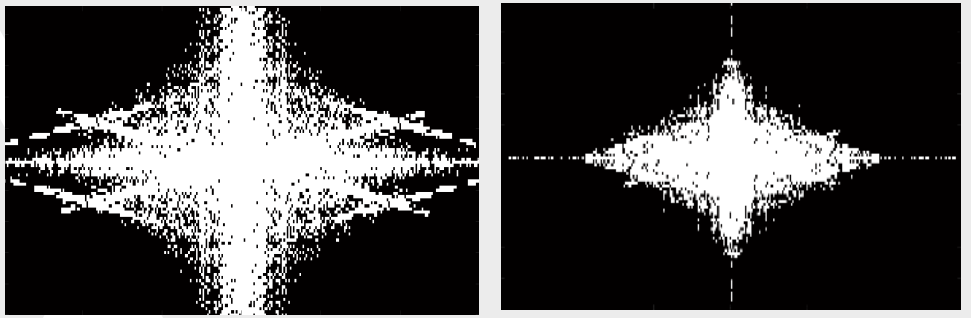
(c) Fourier spectrum of the images in (a).



(d) Fourier spectrum of the forged images in (b).



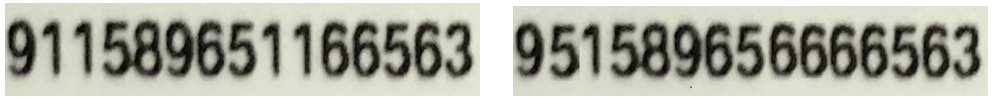
(e) Binary form for Fourier spectrum in (c)



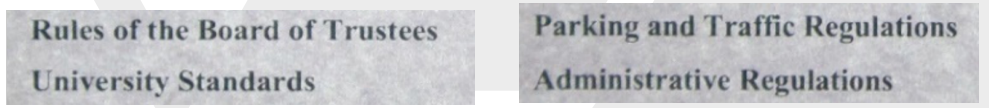
(f) Binary Fourier spectrum of forged images shown in (d)

Fig. 9. Examples of Brightness distribution and shape of the fourier spectrum for the original and forged text of different operations from video frames.

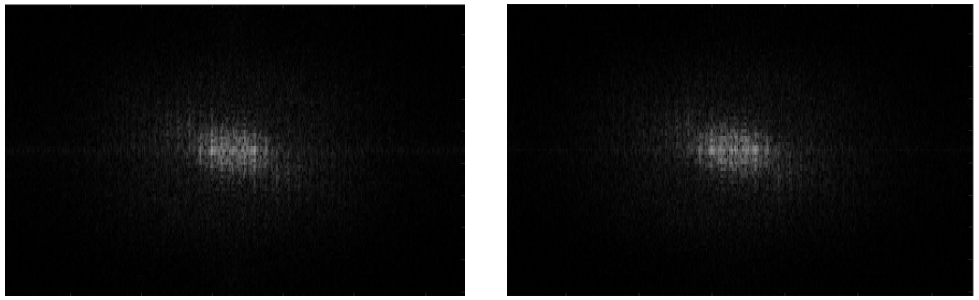
PRELIMINARY FINDINGS:



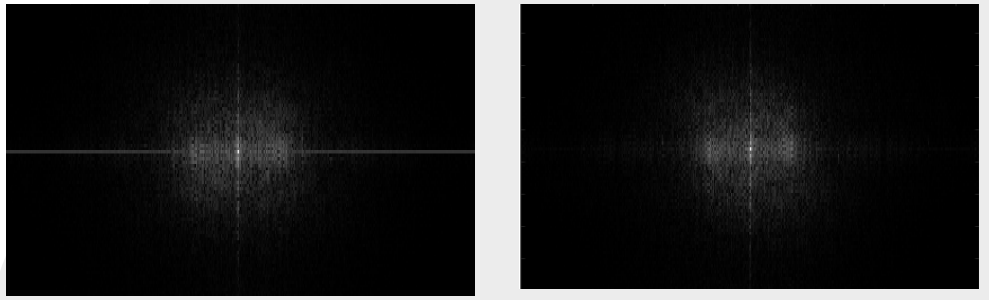
(a) Original and forged images in IMEI forgery images



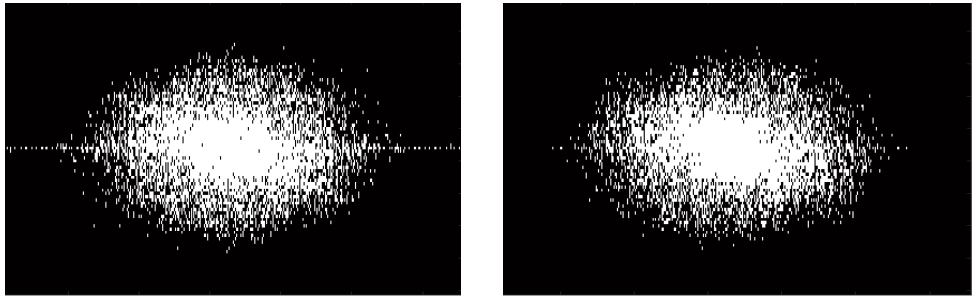
(b) Original and Altered document images



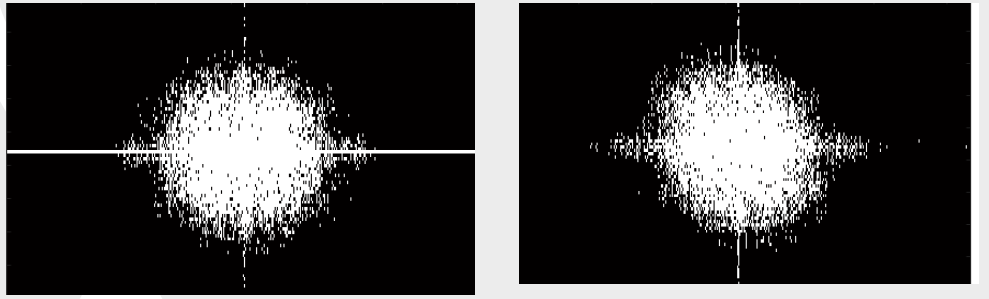
(c) Fourier spectrum of the images in (a).



(d) Fourier spectrum of the forged images in (b).



(e) Binary form for Fourier spectrum in (c)



(f) Binary Fourier spectrum of forged images shown in (d)

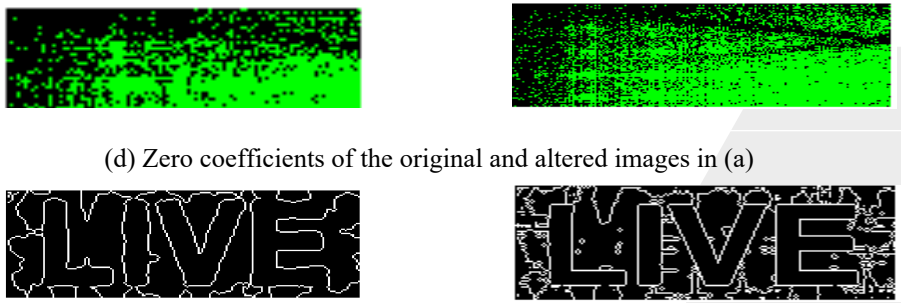
Fig. 10. Examples of Brightness distribution and shape of the fourier spectrum for the original and forged text of different operations from video frames.

PRELIMINARY FINDINGS:

(a) Original image and forged inserted image

(b) Positive DCT coefficients of the original and altered images in (a)

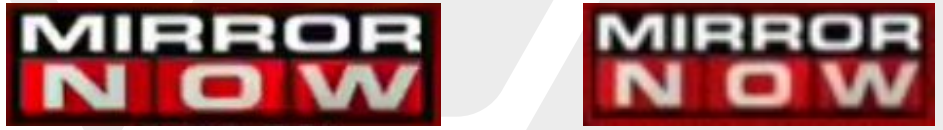
(c) Negative DCT coefficients of the original and altered images in (a).



(d) Zero coefficients of the original and altered images in (a)

(e) The results of fusion operation on Positive and negative coefficients IDCT with Laplacian filter

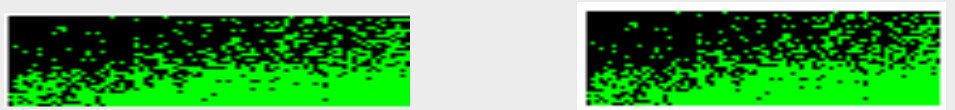
Fig. 11. The illustration of Positive, negative and zero coefficient distributions and final fusing output of the positive and negative DCT coefficients



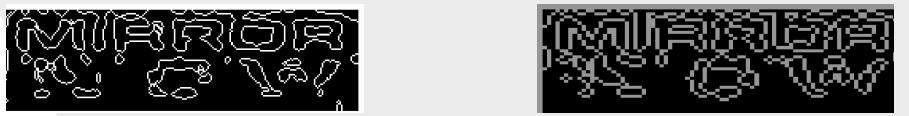
(a) Original image and forged copy-paste images

(b) Positive DCT coefficients of the original and altered images in (a)

(c) Negative DCT coefficients of the original and altered images in (a).



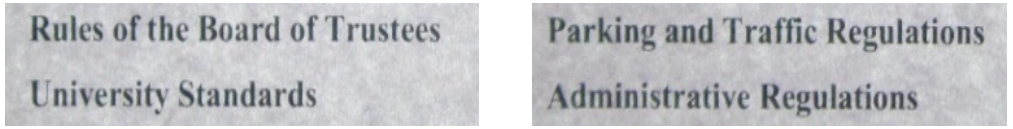
(d) Zero coefficients of the original and altered images in (a)



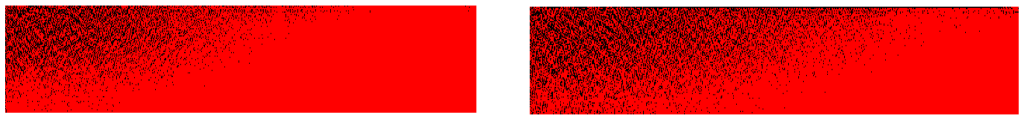
(e) The results of fusion operation on Positive and negative coefficients IDCT with Laplacian filter

Fig. 12. The illustration of Positive, negative and zero coefficient distributions and final fusing output of the positive and negative DCT coefficients

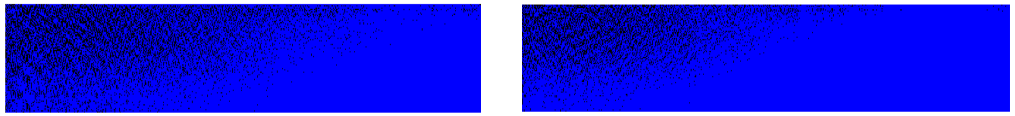
PRELIMINARY FINDINGS:



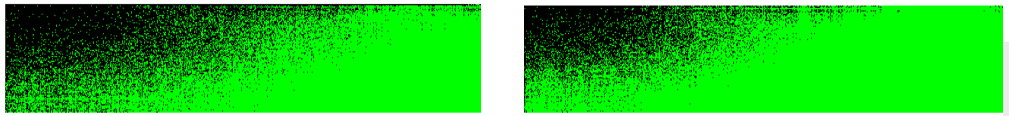
(a) Original image and Altered documents images



(b) Positive DCT coefficients of the original and altered images in (a)



(c) Negative DCT coefficients of the original and altered images in (a).

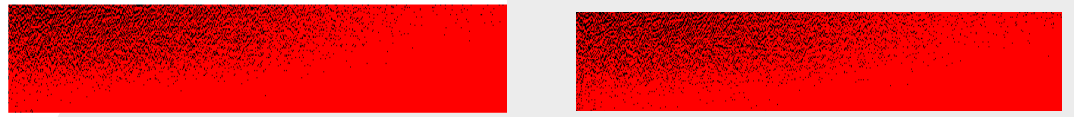


(d) Zero coefficients of the original and altered images in (a)

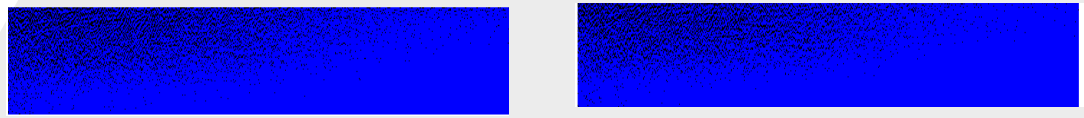
(e) The results of fusion operation on Positive and negative coefficients IDCT with Laplacian filter

Fig. 13. The illustration of Positive, negative and zero coefficient distributions and final fusing output of the positive and negative DCT coefficients

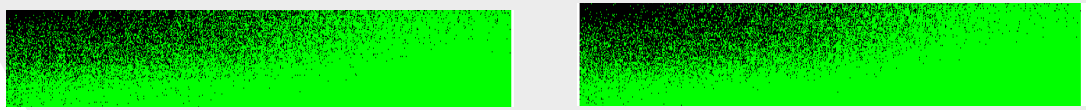
(a) Original image and Altered IMEI images



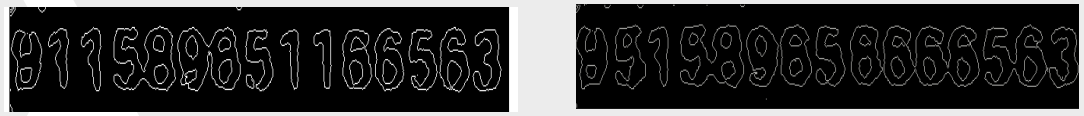
(b) Positive DCT coefficients of the original and altered images in (a)



(c) Negative DCT coefficients of the original and altered images in (a).



(d) Zero coefficients of the original and altered images in (a)



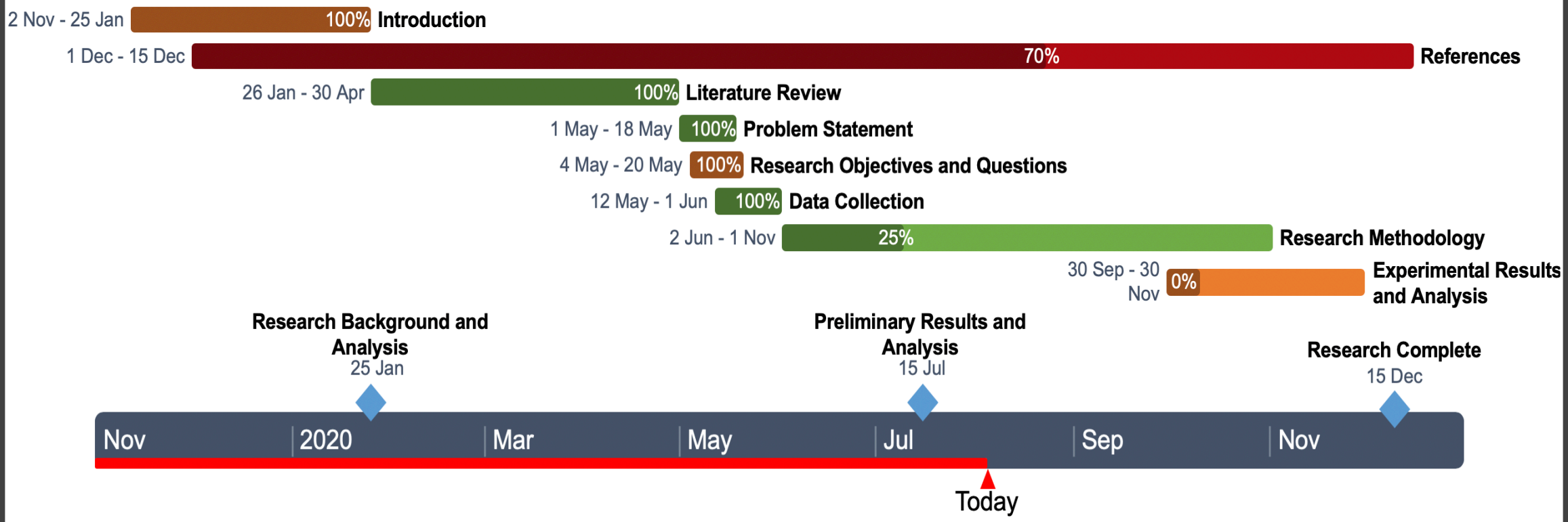
(e) The results of fusion operation on Positive and negative coefficients IDCT with Laplacian filter

Fig. 14. The illustration of Positive, negative and zero coefficient distributions and final fusing output of the positive and negative DCT coefficients

SIGNIFICANCE OF THE WORK:

- Great impact in the field of forensics and its applications.
- Detecting forged information in sensitive applications, such as news media, military and law enforcement videos, handwriting verification/authentication, etc.
- Beneficial in real-world application area like payment receipt, banking cheques and property documents etc.
- Help in Reducing the frauds and crime rates.
- The future scope in areas such as forensic investigation, criminal investigation, surveillance systems, intelligence system, sports, legal services, medical imaging and journalist.

Forged Text Detection method in Video, Natural Scene and Document Images



PROGRESS OF THE WORK:




Questions?




Thank you!