Fake Image and Video Detection

Midterm Presentation 2

Renesa Ray

University of Koblenz-Landau

renesa@uni-koblenz.de

Research Seminar
January 23, 2023

Presentation Overview

1. Introductory Flow
   - Situation
   - Complication
   - Question

2. Line of argumentation
   - Hierarchy of detection methods
   - Deep fake detection groupings

Situation

- Technologies such as DALL.E 2 [Mishkin, 2022], Gan-generated images, and Synthesia are utilized to create photo-realistic fake media which poses greater risks.
- We need to be able to distinguish authentic images from fake ones, as the forgery events are increasing.
- Currently, Microsoft's Video Authenticator tool [Kelion, 2020] works by trying to detect giveaway signs that an image has been artificially generated.
- Detection methods can vary according to the type of forgery used in the image or video.

Complication

- Early attempts of detection were based on handcrafted features obtained from artifacts and inconsistencies of the fake video synthesis process [Chang, 2009]
- Fakes have become complex which has been generated by the advancing AI technology stack, so hard to detect.
- So, DL-based techniques can be adopted, but these need an large amount of training data [Nguyen, 2022].
- Certain types of forgeries don't have enough data available, so block based methods could be useful instead[Ganguly, 2023].

Question

Dealing question

Need to do a SLR that gives us glimpse of what technology of detection can be used for varying types of forgery which enables us to know different detection methods.

Hierarchy of detection methods

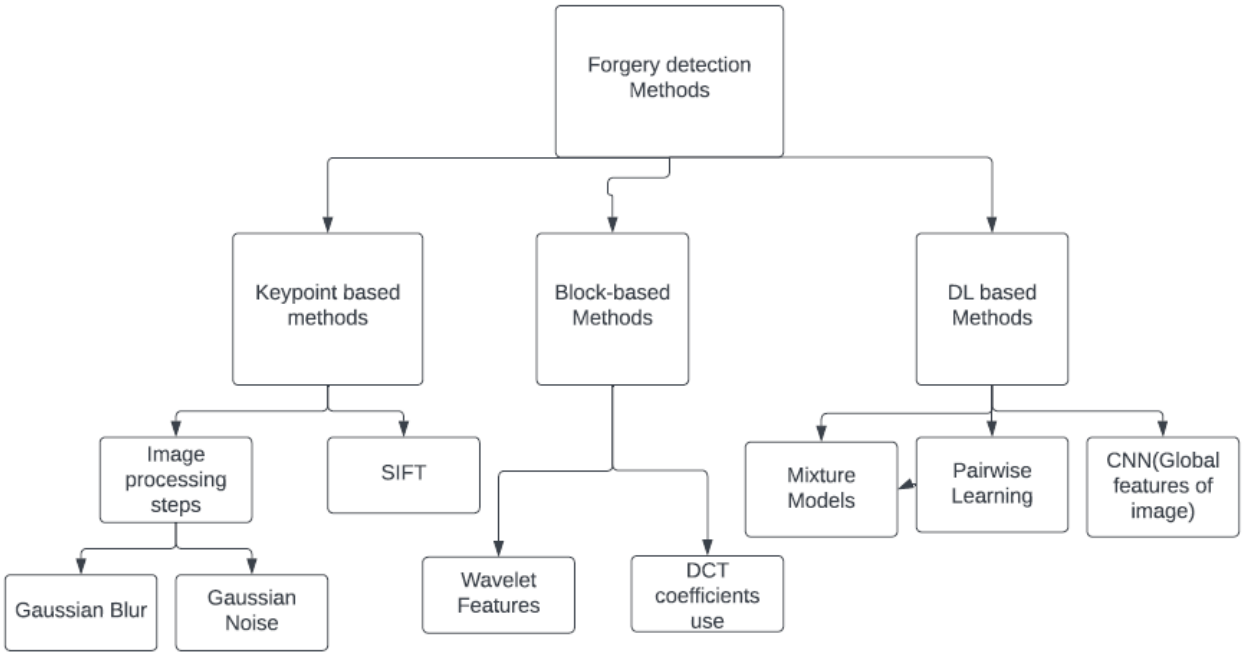

Figure: Characteristics of detection methods

Deepfake detection groupings

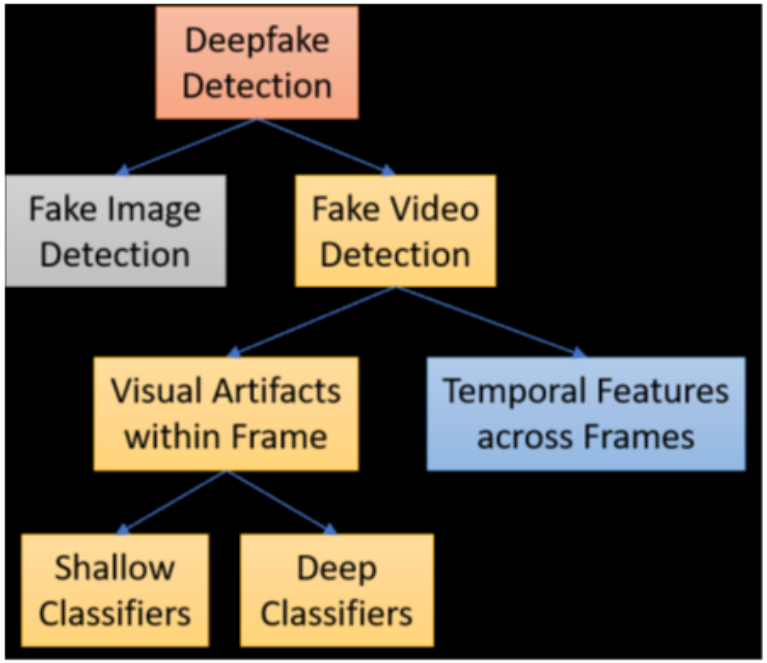

Figure: Categories of detected methods using deep learning methods[Nguyen, 2022]

Final set of resources

75 resources are finalized

References

Kelion, Leo (2020)
Deepfake detection tool unveiled by Microsoft
BBC News

Mishkin, Pamela and Ahmad, Lama and Brundage, Miles and Krueger, Gretchen and Sastry, Girish (2022)
DALL·E 2 Preview - Risks and Limitations
https://github.com/openai/dalle-2-preview/blob/main/system-card.md

Zandi, Mohsen and Mahmoudi-Aznaveh, Ahmad and Talebpour, Alireza (2016)
Iterative copy-move forgery detection based on a new interest point detector
IEEE Transactions on Information Forensics and Security.

Nguyen, Thanh Thi and Nguyen, Quoc Viet Hung and Nguyen, Dung Tien and Nguyen, Duc Thanh and Huynh-The, Thien and Nahavandi, Saeid and Nguyen, Thanh Tam and Pham, Quoc-Viet and Nguyen, Cuong M (2022)
Deep learning for deepfakes creation and detection: A survey
Computer Vision and Image Understanding (223), 1077–3142.

References continued..


Chang, Hsuan T and Hsu, Chih-Chung and Yeh, Chia-Hung and Shen, Day-Fann (2009)
Image authentication with tampering localization based on watermark embedding in wavelet domain
Optical Engineering 48,0577002.


Ganguly, Sagnik and Mandal, Sanmit and Malakar, Samir and Sarkar, Ram (2023)
Copy-move forgery detection using local tetra pattern-based texture descriptor
Multimedia Tools and Applications (pp. 1-22).


Hsu, Chih-Chung and Zhuang, Yi-Xiu and Lee, Chia-Yen (2020)
Deep fake image detection based on pairwise learning
Applied Sciences 10(1), 370.


Liu, Baoping and Liu, Bo and Ding, Ming and Zhu, Tianqing and Yu, Xin(2023)
TI2Net: Temporal Identity Inconsistency Network for Deepfake Detection
Proceedings of the IEEE/CVF Winter Conference on Applications of Computer Vision (pp. 4691-4700).

The End

THANK YOU