Semantic Forensics

Digital Image Processing |Electronics and Communication Engineering
Indian Institute of Information Technology, Nagpur

*Scan QR to know more

Semantic Forensics

Semantic forensics is the application of Digital Image processing (DIP) techniques and machine learning algorithms to detect and analyze fraudulent or malicious intent in digital communications. It involves the analysis of written or spoken text to identify patterns and characteristics that are indicative of deception, manipulation, or other malicious activities.

Semantic forensics can be used in various fields, including law enforcement, intelligence, cybersecurity, and social media analysis. For example, it can be used to detect fake news, online propaganda, and hate speech. It can also be used to identify and track individuals or groups engaged in criminal or terrorist activities.

Overall, semantic forensics provides a powerful tool for detecting and mitigating the risks associated with digital communications, helping to safeguard individuals, organizations, and society as a whole.

Introduction

Semantic forensics is becoming increasingly important in digital communications, as it provides tools and techniques for identifying the authenticity and context of media content, including images, videos, and audio recordings.

Image processing plays a crucial role in semantic forensics by providing tools to analyze and understand visual information in digital media. Semantic forensics involves identifying the authenticity and context of media content, including images, videos, and audio recordings. Image processing techniques can be used to extract features from images, such as color, texture, and shape, which can then be used to identify the source of an image or to detect whether an image has been manipulated.

Background

Here is a high-level flowchart of the semantic forensics process :

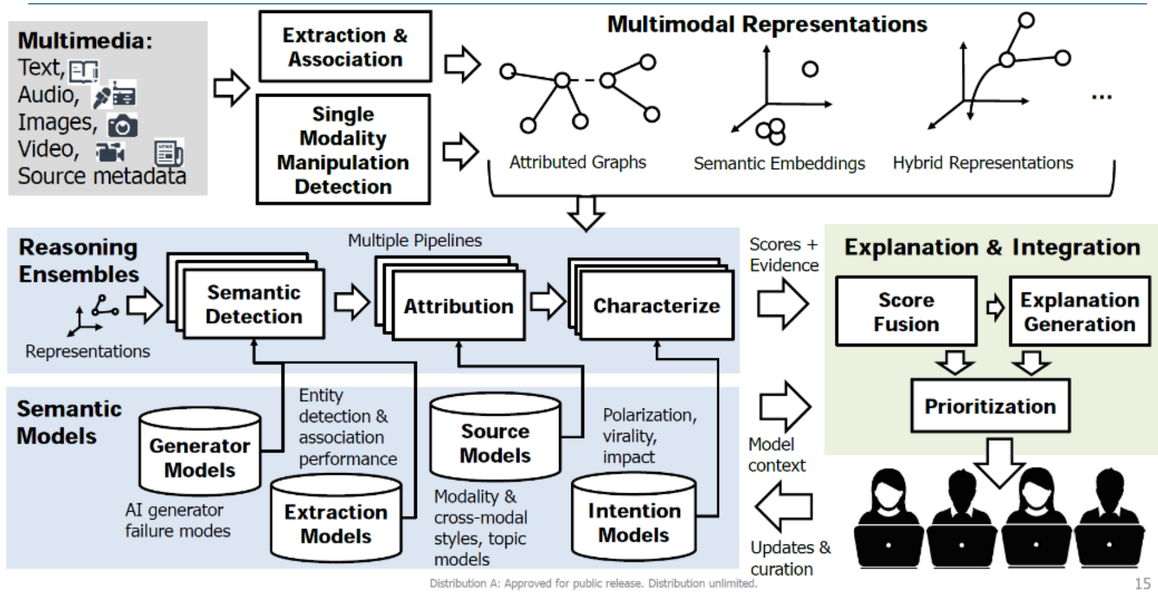

Fig 1 – Flowchart

	Desired Capability	Today	SemaFor
Detection	Automatically detect semantic generation/manipulation errors	Limited	**Yes**
	Detect manipulations across multiple modalities and assets	Limited	**Yes**
	Robust to many manipulation algorithms	Fragile	**Highly robust**
	Increased adversary effort needed to fool detection algorithms	Some	**Significant**
Attribution	Automatically confirm source or author	Limited	**Yes**
	Automatically identify unique source fingerprints	No	**Yes**
	Explain authorship inconsistencies	No	**Yes**
Characterization	Automatically characterize manipulation intent or impact	No	**Yes**
	Provide evidence and explanation for manipulation intent	No	**Yes**
	Correctly prioritize generated/manipulated media for review	No	**Yes**

Table 1 - Current vs Desired Capability for Synthetic Media Detection

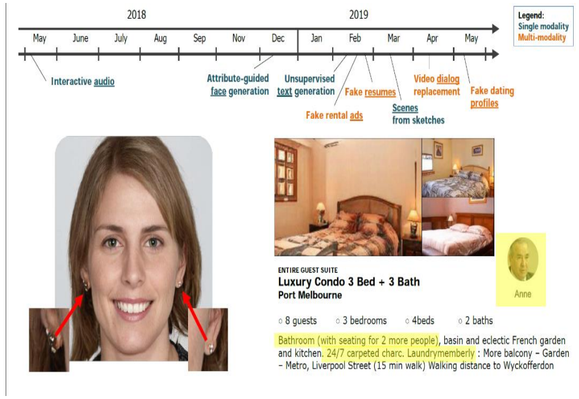

Fig 2 - Incredible Pace of Synthetic Media Generation

Result

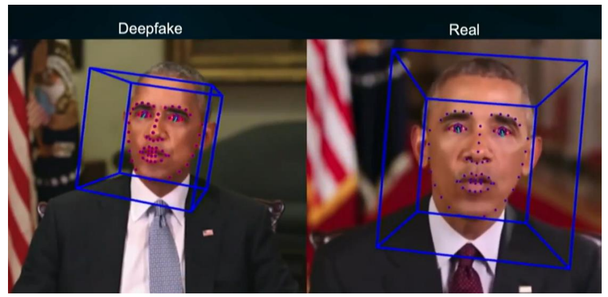

Fig 4 – A Semantic Tool in action on a clip of a Deep Fake from former US President Obama that was created by the actor Jordan Peel

Advantages

1. Can detect sophisticated forms of manipulation, such as deepfakes and text-based disinformation
2. Can provide a more nuanced understanding of the authenticity and context of media content, rather than just a binary "true/false" determination.
3. Can analyze the context and meaning of content, not just the technical properties

Limitations

1. **Resource-intensive**: The computational and resource requirements for semantic forensics can be high, especially for large volumes of data.
2. **Privacy concerns**: Semantic forensics may involve the analysis of personal or sensitive information, raising privacy concerns and ethical considerations.

References

1. https://www.darpa.mil/program/semantic-forensics
2. https://www.darpa.mil/attachments/SemanticForensics-IndustryDay-2019-08-12a.pdf