Digital Image Forensics

-Threats to the Integrity of Digital Media Content
-Digital Content Protection
-Digital Forensics

Hasna mp

Roll : 12

Threats to the Integrity of Digital Media Content

- **Digital images** are widely used in everyday communication, including social media, websites, newspapers, TV, and magazines.
- **Due to the large number of images shared online**, they are vulnerable to alterations and integrity attacks.
- **Easy-to-use image editing software** like Adobe Photoshop makes it simple to manipulate images,raising concerns about their authenticity.
- **Some image edits are harmless**, meant for improving visual quality, but others are used for deception.
- **Forgers manipulate images** to hide or change important details,often to spread false information or damage reputations.

- **Fake images spread quickly** through social media and messaging apps, sometimes causing serious consequences at a national level.
- **Digital images are not just for communication**—they also serve as legal evidence.
- **Protecting image authenticity** has become a big challenge today.
- **Examples of fake images** include face morphing attacks (used for identity theft)
- **A well-known case** was a fake image of former U.S. President Barack Obama watching Indian Prime Minister Narendra Modi’s lecture, which was proven false by forensic experts.

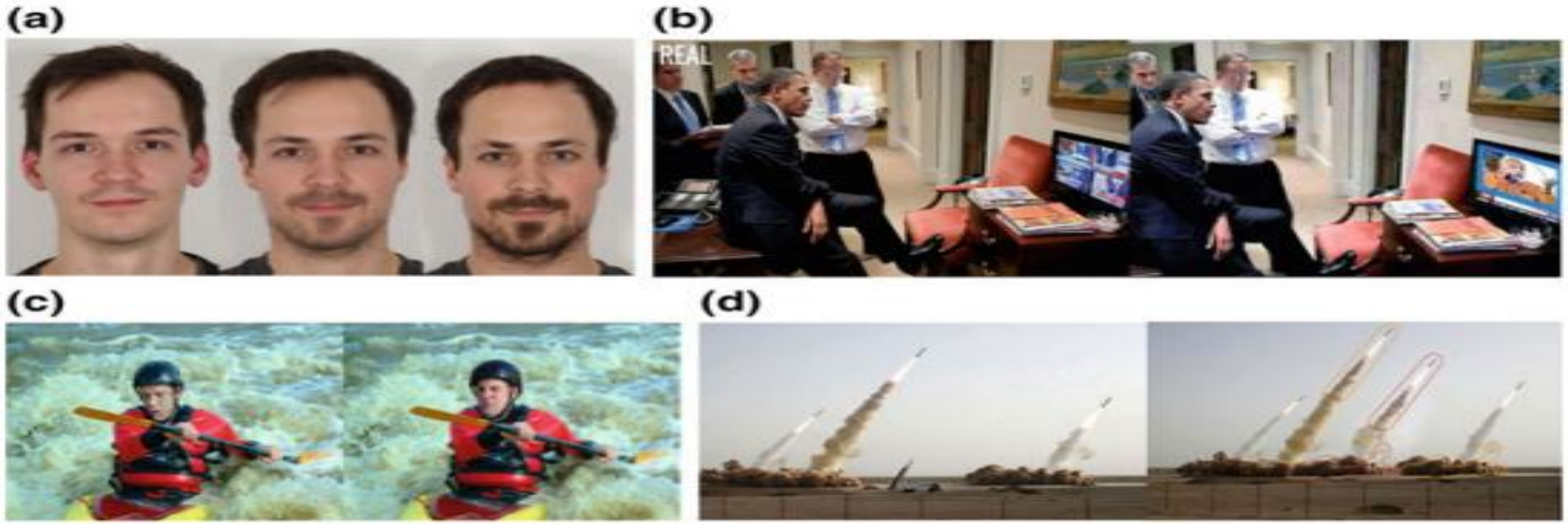

Fig. 1.1 Image forgery attack examples: **a** face morphing attack: left, right images are original, and center image is morphed. **b** Original image (left), forged image (right) [4]; **c** an original image (left) and a composite image (right), in which the head of another person was overlaid onto the shoulders of the original kayaker; **d** an image of an Iranian missile test taken in July 2008: original (left) and forged (right) [13]

Figure 1.1d shows both original and forged images (with more missiles reported in the forged image) of an Iranian missile test taken in July 2008 [13].

Digital Content Protection

- Cybercrime is increasing quickly, so people are trying to find better ways to protect digital content.
- Two common methods to protect digital content are **watermarking** and **steganography**.
- **Watermarking** adds a hidden mark to a picture or video to prove it's real.
- **Steganography** hides secret information inside an image or video to keep it safe.
- Many cameras today include built-in security features like watermarking and encryption.
- Adding these security features makes cameras more expensive.

Digital Forensics

- **Digital forensics** is like being a detective for digital pictures and videos.
- It helps find out **where a picture or video came from** and **if someone changed it**.
- It **does not** need any extra hidden information before checking for changes.
- This is called a **passive security method** because it doesn’t add anything beforehand.
- Digital forensics is **very useful but also tricky** because it works on already-made content.
- There are **two main jobs** in digital forensics:
    - **Finding out where an image came from** (source identification).
    - **Checking if an image has been changed** (forgery detection).

THANK YOU