

ICS 07.140
CCS A 92



**NATIONAL STANDARD OF THE
PEOPLE'S REPUBLIC OF CHINA**

GB/T 45429-2025

**Forensic sciences - Forged video and image of a person -
General rules for examination**

法庭科学 伪造人像 检验通则

Issued on: February 28, 2025

Implemented on: June 1, 2025

**Issued by: State Administration for Market Regulation;
Standardization Administration of the PRC**

Table of Contents

- 1 Scope
- 2 Normative references
- 3 Terms and definitions
 - 3.1 forged video and image of a person
 - 3.2 digital media
 - 3.3 Deepfake
 - 3.4 adversarial attack
 - 3.5 presentation attack

1 Scope

This document defines the terminology and classification of forged portraits in the field of forensic science, and specifies the testing equipment, testing procedures, and testing methods for forged portraits.

Content and appraisal opinion categories describe the basic methods of forged portrait inspection.

This document is applicable to forged portrait detection in the field of forensic science.

2 Normative references

GB/T 45428

GB/T 45430

GB/T 45432

GB/T 45433

3 Terms and definitions

For the purposes of this document, the terms and definitions defined in GA/T 120 and the following apply.

3.1 forged video and image of a person

Fake portraits created using a variety of technical means.

Note. This includes tampered portraits, deep fake portraits, adversarial attack portraits, and

presentation of attack portraits, etc.

3.2 digital media

A video image created or captured digitally and composed of a series of pixels.

3.3 Deepfake

Technical methods that use deep learning, virtual reality, and other generative synthetic algorithms to create fake digital media.

3.4 adversarial attack

An attack that intentionally adds subtle perturbations to the input video image to evade face detection or produce false identity verification results. means.

3.5 presentation attack

Presenting a false image of a person in the form of a paper photo, electronic photo, video, mask, head model or other physical medium for the purpose of deceiving An attack vector designed to mislead an observer or an authentication system.