

Development of an efficient steganalysis framework for uncovering hidden data in digital media.

[www.uncoverproject.eu](http://www.uncoverproject.eu)

Coordination: Royal Military Academy, Belgium email: [office@uncoverproject.eu](mailto:office@uncoverproject.eu)

## ILLICIT USES OF STEGANOGRAPHY

- Hidden communication between criminals/terrorists
- Cyber espionage, information leakage
- Malware (hiding code, CC-server addresses)
- Hiding criminal activities (e.g. child pornography)

## STATUS IN LAW ENFORCEMENT

Use of commercially available tools

- ➔ Slow, no indication of confidence, limited detection
- ➔ State-of-the-art?

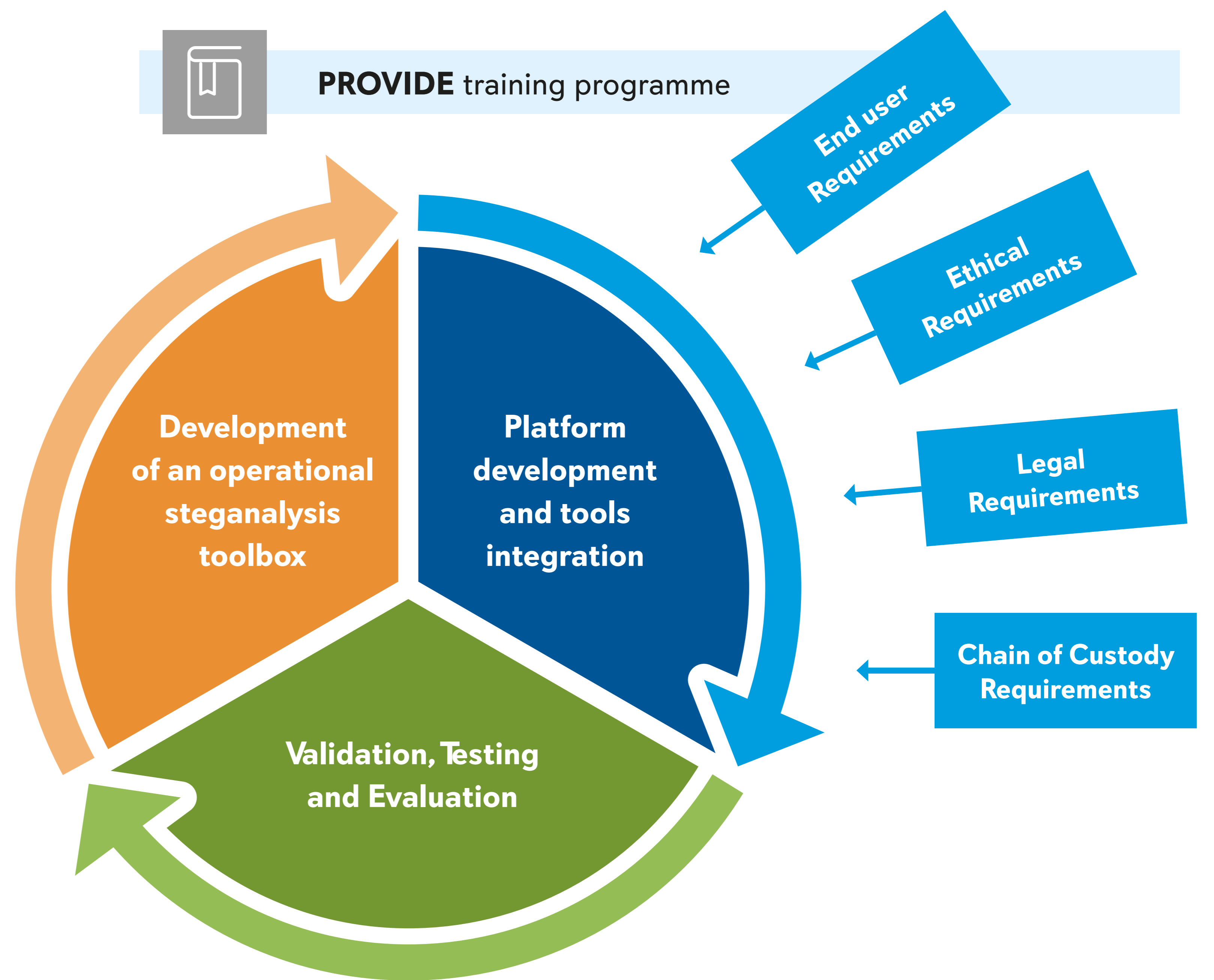
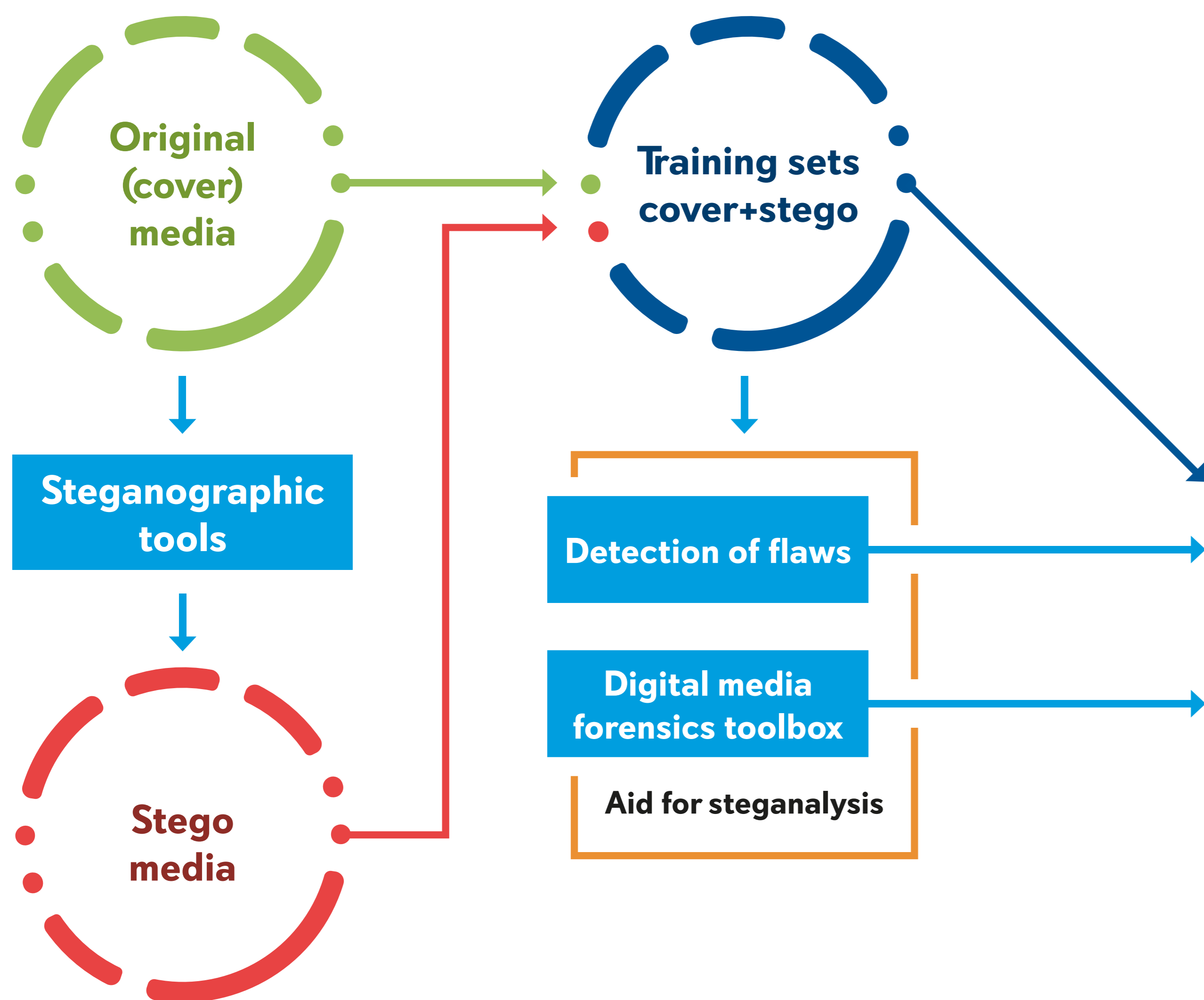
## OBJECTIVES OF UNCOVER

**IMPROVE** existing methods

**IMPLEMENT** Platform

**DEMONSTRATE** with real life cases

**PROVIDE** training programme

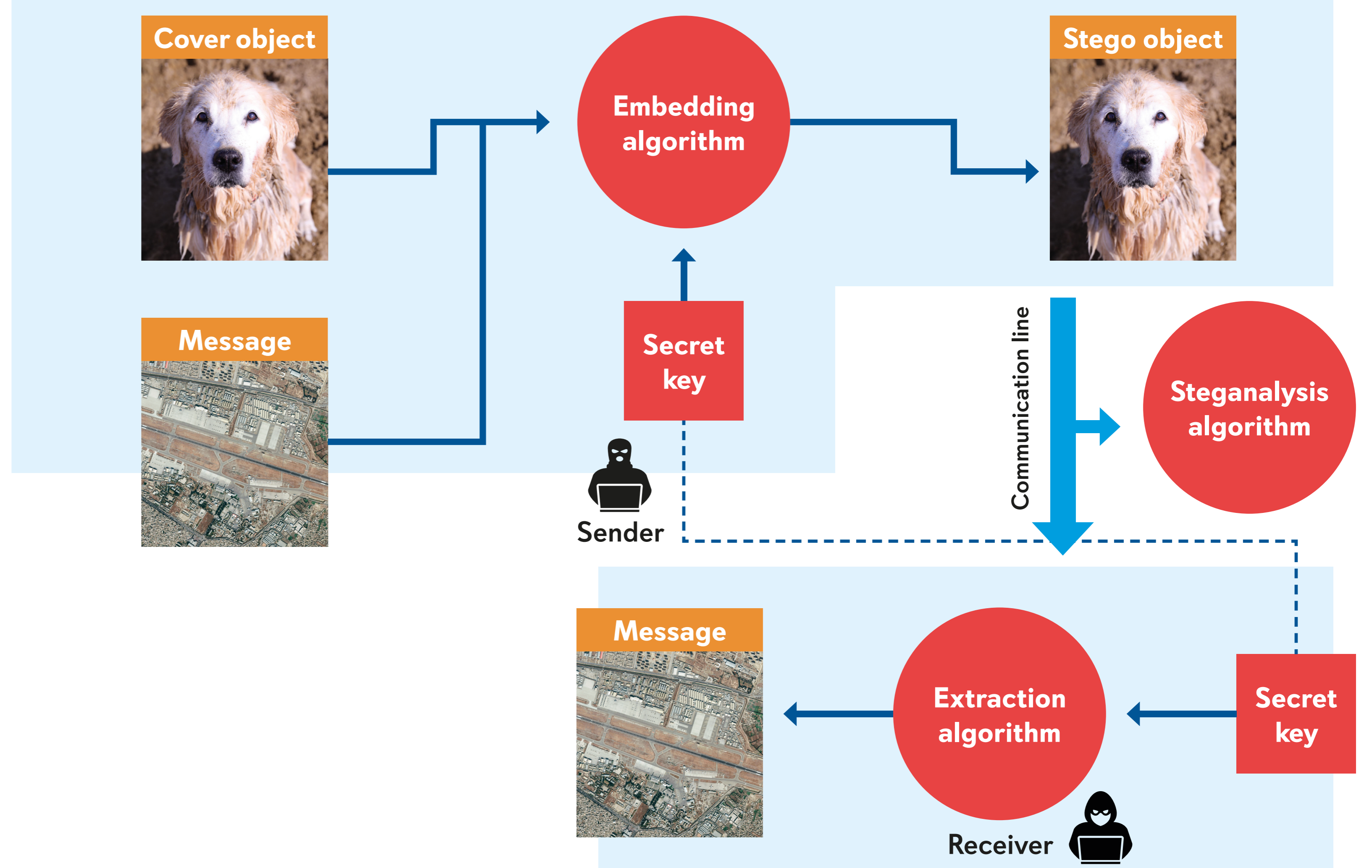


## WHAT IS STEGANOGRAPHY?

Cryptography	Steganography
„CRYPTOS“ = hidden ➔ hidden message/writing	„STEGANOS“ = covered ➔ concealed message/writing
Hides message <b>MEANING</b>	Hides message <b>PRESENCE</b>

Both words stem from Greek "grafien" (graphy) = writing

## HOW DOES IT WORK?



Want to know more about UNCOVER?



SCAN ME



This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 101021687.