AtlantTIC
Research Center for
Information & Communication Technologies

Homomorphic encryption and collaborative camera attribution

4rd BYMAT Conference
Bringing Young Mathematicians Together, *November 9-11, 2022*

Alberto Pedrouzo-Ulloa, *atlanTTic Research Center, Universidade de Vigo*
apedrouzo@gts.uvigo.es

Outline

- Introduction
- Camera attribution
- Fingerprints and privacy leakage
- Proposed collaborative framework
- Some example functionalities
- Conclusions

Introduction

Main motivations for this work

Motivations for collaboration

- The amount of multimedia content that law enforcement agencies (LEAs) must deal with in their investigations is ballooning.

Motivations for collaboration

- The amount of multimedia content that law enforcement agencies (LEAs) must deal with in their investigations is ballooning.



Motivations for collaboration

- The amount of multimedia content that law enforcement agencies (LEAs) must deal with in their investigations is ballooning.
- Collaboration between LEAs is becoming essential in a growing number of cases.

Motivations and obstacles for collaboration

- The amount of multimedia content that law enforcement agencies (LEAs) must deal with in their investigations is ballooning.
- Collaboration between LEAs is becoming essential in a growing number of cases.
- The exchange of multimedia is strongly limited by privacy and data protection laws.

LEAs and Image Forensics

- ***Camera attribution*** is a very relevant scenario for *collaboration among LEAs*



Camera attribution

Image forensics

Image camera device fingerprint

- PRNU (Photoresponse Non-Uniformity) is a specific **noise pattern inherent to digital imaging sensors**

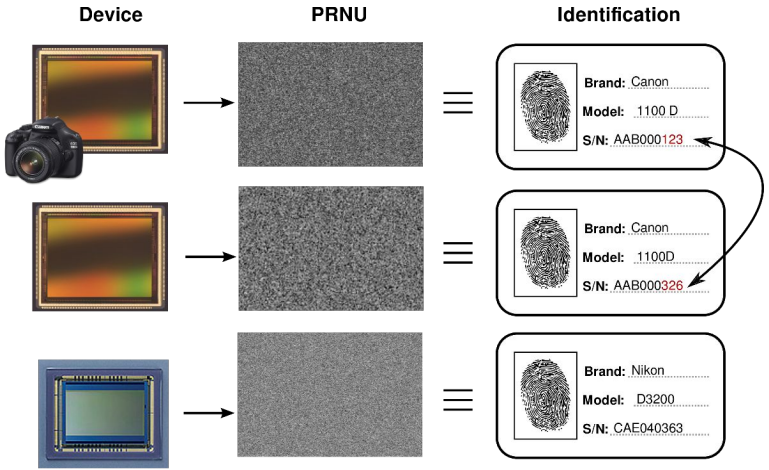


Image camera device fingerprint

- PRNU (Photoresponse Non-Uniformity) is a specific noise pattern inherent to digital imaging sensors
- Thanks to its random nature, the **PRNU acts as a fingerprint of the underlying device**

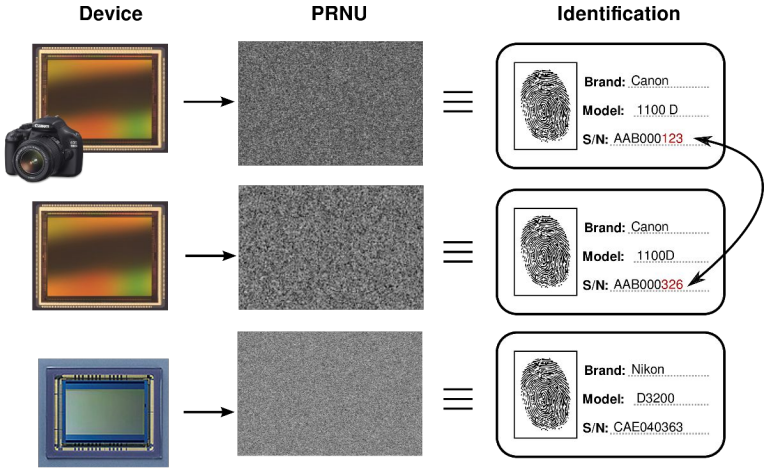
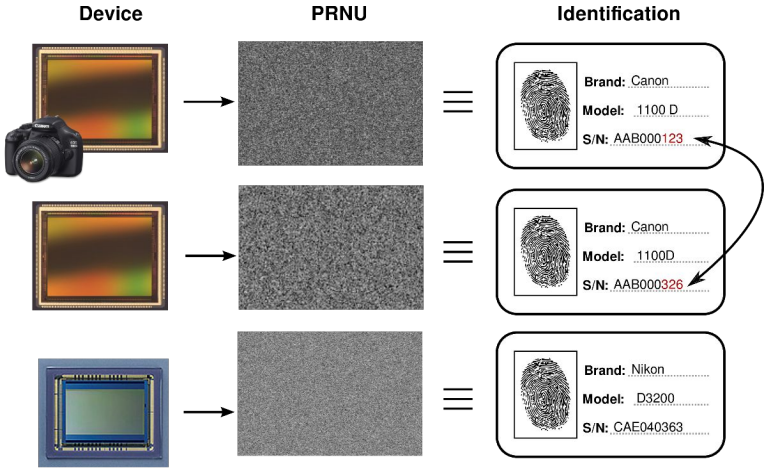


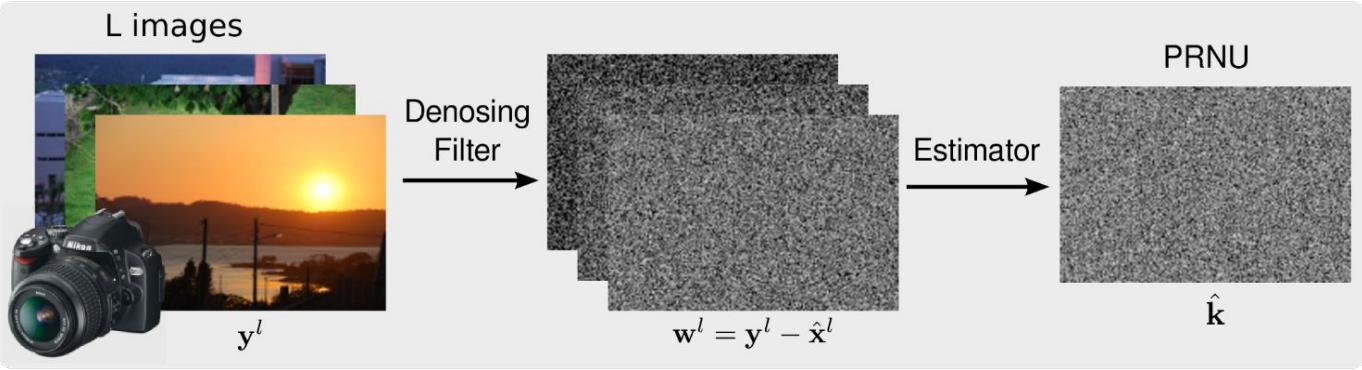
Image camera device fingerprint

- PRNU (Photoresponse Non-Uniformity) is a specific noise pattern inherent to digital imaging sensors
- Thanks to its random nature, the PRNU acts as a fingerprint of the underlying device
- Find immediate application in fighting against crimes involving depictions of minors.



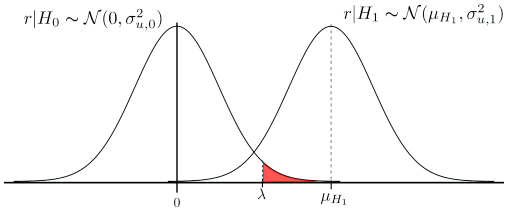
PRNU extraction

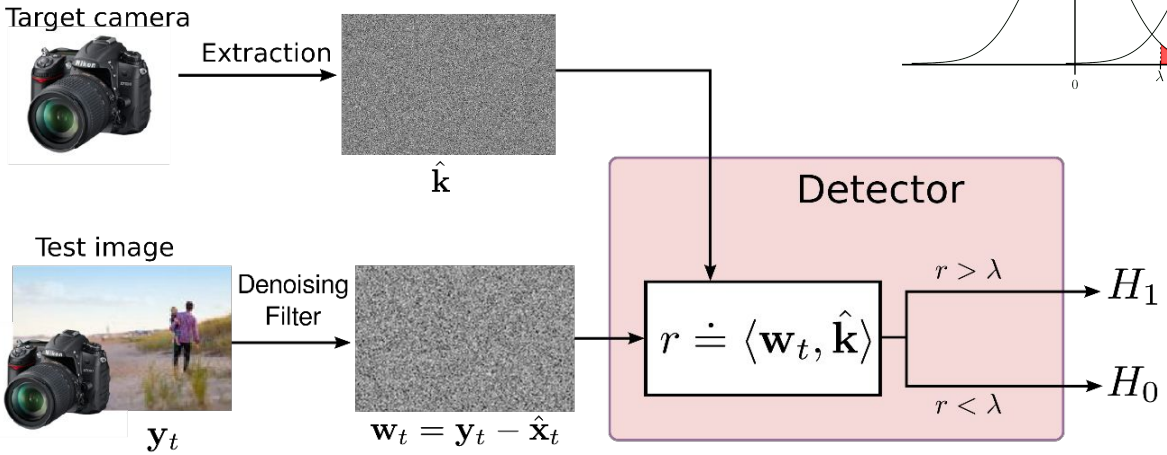
- Let $\{\boldsymbol{Y}^{(l)}\}_{l=1}^{L}$ be a set of L images taken with the same camera device
- The PRNU can be estimated by using the MLE: $\hat{\boldsymbol{K}} = \frac{\sum_{l=1}^{L} \boldsymbol{W}^{(l)} \circ \hat{\boldsymbol{X}}^{(l)}}{\sum_{l=1}^{L} \hat{\boldsymbol{X}} \circ \hat{\boldsymbol{X}}}$
- Where $\boldsymbol{W}^{(l)} = \boldsymbol{Y}^{(l)} - \hat{\boldsymbol{X}}^{(l)}$ and $\hat{\boldsymbol{X}}^{(l)}$ is the denoising of $\boldsymbol{Y}^{(l)}$



PRNU detection

- Given a test image $\boldsymbol{Y}$ with residue $\boldsymbol{W} = \boldsymbol{Y} - \hat{\boldsymbol{X}}$ and a PRNU estimate $\hat{\boldsymbol{K}}$ we define the statistic $u = \boldsymbol{W} \cdot \hat{\boldsymbol{K}}$





Fingerprints and privacy leakage

Fingerprints are not as random as they look like at first glance

Leakage in fingerprint estimates

- A number of images from the same device or camera model must be pooled together in order to extract fingerprints reliably.
- The images used to extract the fingerprints may be very sensitive (e.g., in child abuse cases)

Leakage in fingerprint estimates

- A number of images from the same device or camera model must be pooled together in order to extract fingerprints reliably.
- The images used to extract the fingerprints may be very sensitive (e.g., in child abuse cases)
- Some recent works have shown that camera fingerprints estimates can leak a considerable amount of information from the images used for extraction

Leakage in fingerprint estimates

- A number of images from the same device or camera model must be pooled together in order to extract fingerprints reliably.
- The images used to extract the fingerprints may be very sensitive (e.g., in child abuse cases)
- Some recent works have shown that camera fingerprints estimates can leak a considerable amount of information from the images used for extraction



Illustration taken from Fig. 3 in [1] (CC BY 4.0) / Cropped and rearranged from original

Proposed Collaborative Framework

Sharing without sharing

Federated framework

- A federated framework for fingerprint extraction/detection composed of:
  - **Data Owners:**

    LEAs or Forensic Institutions aiming at camera fingerprint extraction through collectively trained models.

  - **Aggregator Institution:**

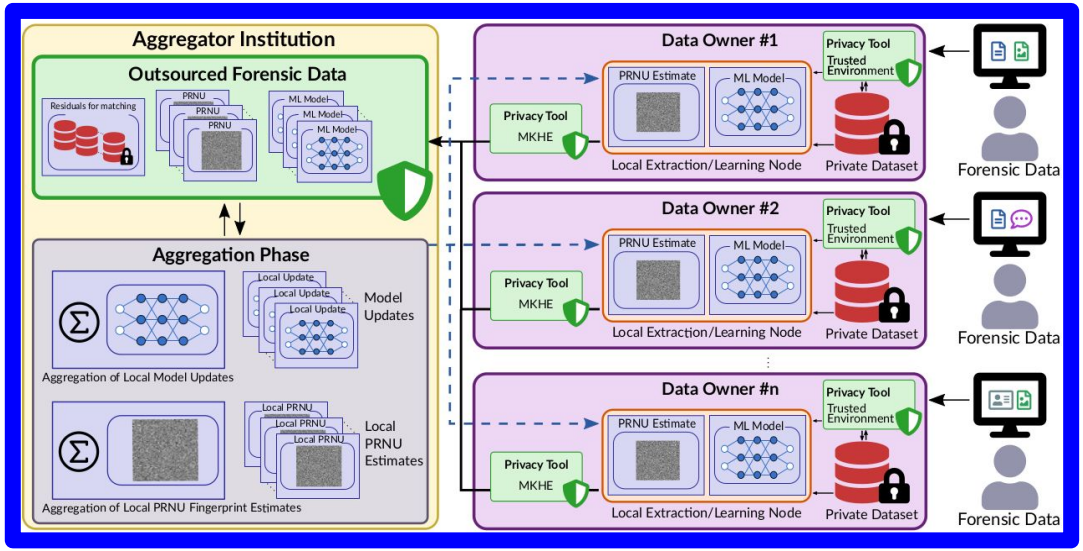
    A Data Owner, or larger organizations like Europol or Interpol.

  - **End users:**

    Participating or other LEAs or Forensic institutions.

Federated framework

- A federated framework for fingerprint extraction/detection:
  - **Data Owners**
  - **Aggregator Institution**
  - **End users**

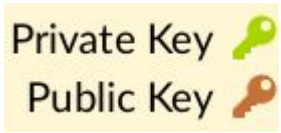


How to protect fingerprints during processing?

- Homomorphic Encryption

$$\left\{ \begin{array}{c} E(m_1) + E(m_2) = E(m_1 + m_2) \\ E(m_1) \cdot E(m_2) = E(m_1 \cdot m_2) \end{array} \right\}$$

- It enables to perform computation under encrypted data.
- Typically two keys are defined:



How to protect fingerprints during processing?

- Homomorphic Encryption

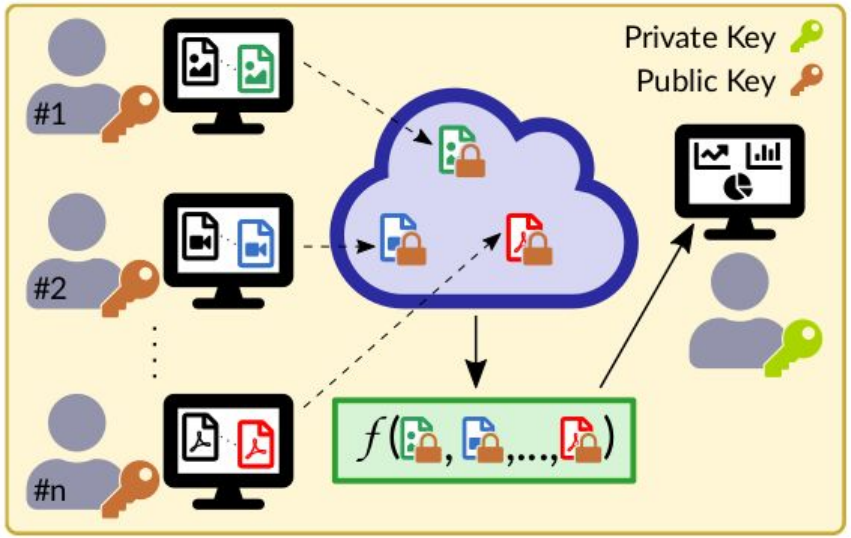
$$\left\{ \begin{array}{c} E(m_1) + E(m_2) = E(m_1 + m_2) \\ E(m_1) \cdot E(m_2) = E(m_1 \cdot m_2) \end{array} \right\}$$

- It enables to perform computation under encrypted data.
- Typically two keys are defined:

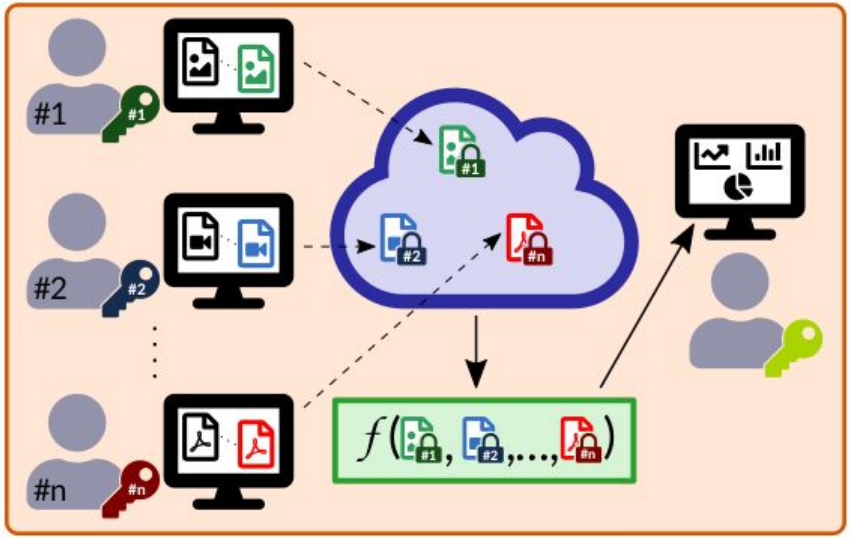


Single-key HE vs Multi-key HE

- Our scenario requires to incorporate multiple keys into HE.
  - Prevents decryption without permission of other participants.



Single key



Multiple keys

High-level federated framework workflow

- All involved Data Owners generate individual secret and a collective public keys.
- Each Data Owner encrypts its data to be outsourced under a collective public key.
- One of the entities will be in charge of computing a particular functionality *f*.
- All involved parties collaboratively decrypt the output.

High-level federated framework workflow

- All involved Data Owners generate individual secret and a collective public keys.
- Each Data Owner encrypts its data to be outsourced under a collective public key.
- One of the entities will be in charge of computing a particular functionality *f*.
- All involved parties collaboratively decrypt the output.

High-level federated framework workflow

- All involved Data Owners generate individual secret and a collective public keys.
- Each Data Owner encrypts its data to be outsourced under a collective public key.
- One of the entities will be in charge of computing a particular functionality *f*.
- All involved parties collaboratively decrypt the output.

High-level federated framework workflow

- All involved Data Owners generate individual secret and a collective public keys.
- Each Data Owner encrypts its data to be outsourced under a collective public key.
- One of the entities will be in charge of computing a particular functionality *f*.
- All involved parties collaboratively decrypt the output.

Some example functionalities

What can we compute together?

Some examples of useful functionalities

- Aggregation of local PRNU estimates.
  - The functionality *f* is implemented with a homomorphic addition, followed by a division after decryption.

- Fingerprint matching.
  - The functionality *f* corresponds with a set of homomorphic scalar products among encrypted fingerprint estimates.

Some examples of useful functionalities

- Aggregation of local PRNU estimates.
  - The functionality *f* is implemented with a homomorphic addition, followed by a division after decryption.

- Fingerprint matching.
  - The functionality *f* corresponds with a set of homomorphic scalar products among encrypted fingerprint estimates.

Implementation runtimes

Is this practical?

Implementation runtimes

- Aggregation and matching functionalities implemented with Lattigo v3.0.4.
  - Parameters: {T = 2 16 + 1, bfv.PN12QP109} and {T = 3 · 2 30 + 1, bfv.PN13QP218}.
  - Evaluation runtimes were conducted multi-threaded on an Intel Core i7-4510U @2.00GHz x 4 with 7.7GB.
  - The rest of primitives were conducted singled-threaded.

64 parties + Cloud fingerprint 1024 X 1024	**CKG + RKG + RTG (Cloud + Parties)**	**Encryption**	**Evaluation**	**CKS (Cloud + Parties)**	**Decryption**
Aggregation	2 *ms* + 716 *us*	826 *ms*	689 *ms*	594 *ms* + 735 *ms*	173 *ms*
Matching	227 *ms* + 98 *ms*	1.13 *s*	65 *s*	775 *ms* + 483 *ms*	166 *ms*

Implementation runtimes

- Aggregation and matching functionalities implemented with Lattigo v3.0.4.
  - Parameters: {T = 2 16 + 1, bfv.PN12QP109} and {T = 3 · 2 30 + 1, bfv.PN13QP218}.
  - Evaluation runtimes were conducted multi-threaded on an Intel Core i7-4510U @2.00GHz x 4 with 7.7GB.
  - The rest of primitives were conducted singled-threaded.

64 parties + Cloud fingerprint 1024 X 1024	**CKG + RKG + RTG (Cloud + Parties)**	**Encryption**	**Evaluation**	**CKS (Cloud + Parties)**	**Decryption**
Aggregation	2 *ms* + 716 *us*	826 *ms*	689 *ms*	594 *ms* + 735 *ms*	173 *ms*
Matching	227 *ms* + 98 *ms*	1.13 *s*	65 *s*	775 *ms* + 483 *ms*	166 *ms*

Conclusions

A very brief summary

Conclusions

- We introduced a novel collaborative framework for secure camera attribution.
- Estimated fingerprints can leak information of the images used for estimation.
  - Encryption to protect fingerprints is fundamental.
  - Multi-key homomorphic encryption mitigates c*ollusion attacks between aggregator and data owners*.
- Our framework works for several functionalities.
  - We evaluated fingerprint aggregation and matching across encrypted databases.

Thanks for your attention!