中国科学院大学
University of Chinese Academy of Sciences

Asymmetric Feature Generation and Matching in Images

Zhipeng Cao, Master's Candidate

Academy of Mathematics and Systems Science, Chinese Academy of Sciences

数系天地
勤笃求真

中国科学院数学与系统科学研究院
Academy of Mathematics and Systems Science
Chinese Academy of Sciences

01.10.2025, Beijing, China

Problem Background

Consider a real-life scenario: Can we match individuals from two sets of similar images?

Figure: The Same Twin from Different Perspectives

- For strangers, it is **difficult** to match individuals in the two images.
- For their family members, it is **easy to identify** the corresponding individuals at a glance.

Asymmetric Feature Matching Problem

- How to generate a set of images that appear similar to attackers but can be matched by defenders?
  - Unlike traditional feature point matching, pre-trained models are often sufficient for image feature matching in most cases.(SIFT,deep learning...)
  - Asymmetric features.

Applications: Current UAV navigation and control algorithms rely on GPS signals and cannot achieve local positioning.

Problem Formulation and Solution

First, consider only two perspectives and generate data from a single original image A. The first perspective data is given by:

$$D_1 = A + \Delta_1 + w_1, \ldots, D_m = A + \Delta_m + w_m,$$

and the second perspective data is given by:

$$E_1 = A + \Delta_1 + \zeta_1, \ldots, E_m = A + \Delta_m + \zeta_m.$$

Can we derive the optimal linear transformation F to facilitate matching of the original image set?

Difficult for Attackers to Match

The goal is to minimize the maximum difference between perturbations:

$$\min_{F, \Delta_1, \ldots, \Delta_m} \max_{i \neq j} ||\Delta_i - \Delta_j||.$$

Easy for Defenders with Knowledge of the Transformation Matrix

For defenders who know the transformation matrix F, the following condition ensures correct matching:

$$\forall i \neq j, ||B_i - C_i||_F < ||B_i - C_j||_F,$$

which implies:

$$||F(w_i - \zeta_i)||_F < ||F(\Delta_i - \Delta_j) + F(w_i - \zeta_j)||_F,$$

and further:

$$||F(w_i - \zeta_i)||_F + ||F(w_i - \zeta_j)||_F < ||F(\Delta_i - \Delta_j)||_F.$$

Thank You!