RITSUMEIKAN

デジタル画像改ざん検出に関する研究の現状

デジタル・フォレンジック研究会　副会長
立命館大学　情報理工学部
上原　哲太郎
立命館大学大学院　情報理工学研究科
Songpon Teerakanok

デジタル・フォレンジック・コミュニティ2019 in 関西（2019/02/19）

画像の改ざんが極めて容易に

- Photoshopの「コンテンツに応じた塗り」「パッチツール」「スポット修正」など
  - https://helpx.adobe.com/jp/photoshop/using/content-aware-patch-move.html
  - https://helpx.adobe.com/jp/photoshop/using/content-aware-fill.html

次のような改ざんが問題に

消去

複製

置換

Gajanan K.Birajdar Vijay H.Mankar **Digital image forgery detection using passive techniques: A survey**

残念ながら学術界でも

京大

iPS研で論文不正　図でデータの捏造や改ざん

会員限定有料記事　毎日新聞 2018年1月22日 19時37分（最終更新 1月22日 23時25分）

社会一般 > 科学・技術 > 速報 > 社会 > 医療 > サイエンス >

所属する助教による論文の不正行為が判明し、謝罪会見で謝罪する京都大の（左から）山中伸弥iPS細胞研究所所長、湊長博副学長、山本克己副学長＝京都市左京区で2018年1月22日午後5時32分、小松雄介撮影

京都大（京都市）は22日、京大iPS細胞研究所の山水康平（やまみず・こうへい）・特定拠点助教（36）が昨年2月に発表したヒトのiPS細胞（人工多能性幹細胞）に関する論文で、データの捏造（ねつぞう）・改ざんがあったと発表した。論文を構成する図や補足図に計17カ所で捏造と改ざんがあり、論文の主張に沿うよう有利にデータが操作されていたという。京大は論文の撤回を申請しており、今後、関係者の処分を行う予定。他の研究や今後の研究には影響はないとしている。同研究所を含め、京大で論文の捏造が認定されたのは初めてという。

毎日新聞2018年1月22日

学術論文では
ねつ造・剽窃は
許されないが
単なる「加工」は
許容される
場合もあるので
判定はより難しい

我々の問題意識

- このような写真が刑事事件捜査や裁判の場に出てきても、気づくことは困難
- **自動的に**改ざんの可能性を検出する技術やツールの開発が今後重要ではないか？
- 一般にBlind Image Forgery Detection Passive Image Forgery Detectionと呼ばれる技術について調査

先行したサーベイ研究

- Hany Farid:
  Image Forgery Detection – A survey.
  IEEE Signal Processing Magazine, 26(2):16-25, 2009.
- Gajanan K.Birajdara, Vijay H.Mankarb:
  Digital image forgery detection using passive techniques: A survey.
  Digital Investigation, Vol.10, Issue 3, pp. 226-245, 2013.
- この2本のサーベイ論文を起点に技術を比較
- 本講演は一部は既発表だが未発表内容を含む
  - S.Teerakanok, T.Uehara: Digital Media Tampering Detection Techniques: An Overview, IEEE COMPSAC2017など

画像改ざんの大まかな分類

- Active Image Forgery Detection
  - あらかじめ電子透かしや署名を埋める（今回は扱わない）
- Blind Image Forgery Detection
  - 改ざんされた画像のみから改ざん検出
  - 複数画像合成 or 単一画像内での改ざん
    - 複数画像合成の方がより容易
  - 元画像データ or 印刷物など再加工のみ
    - 後者は一般にはかなり困難

どうやって改ざんを発見するか？

- **Photoshopの「コンテンツに応じた塗り」**

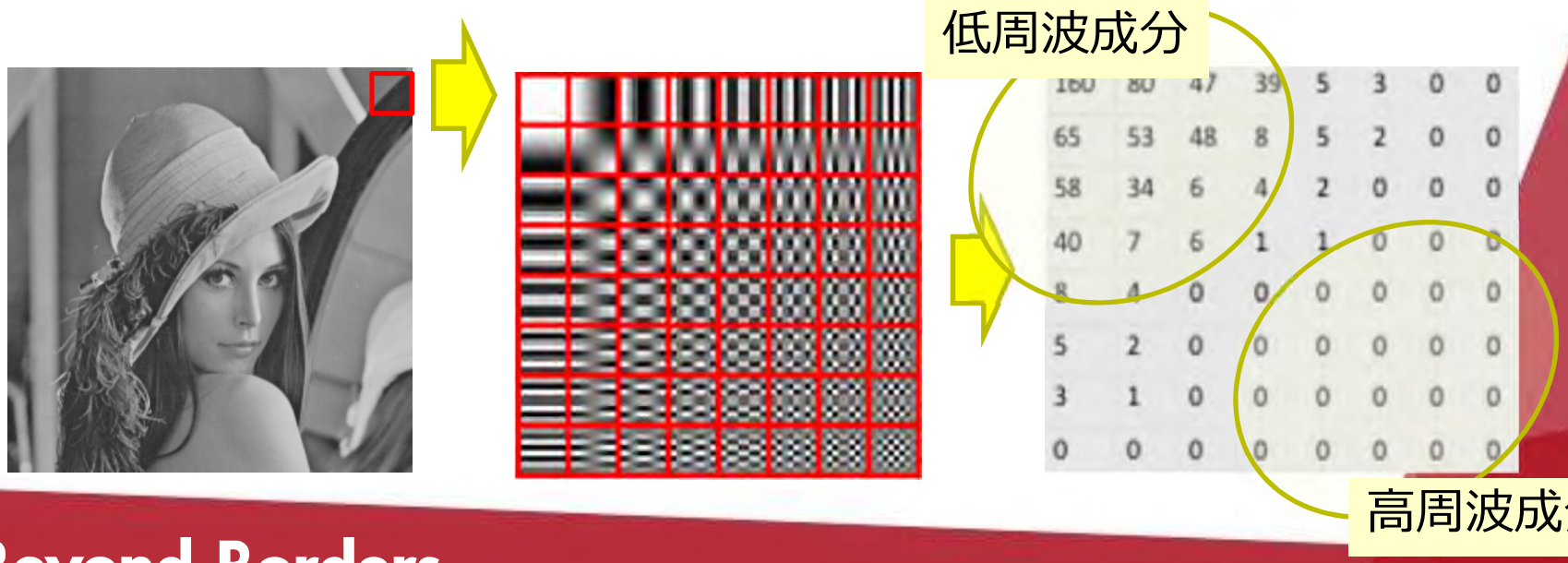
1. 修正で特徴量が変化する
2. 複製がある

改ざん検出の基本戦略

- 改ざんの結果「他とは違う」ことを検出
  - 修正部分は他の画像からの合成？
    - 特徴量がいろいろと違うはず
  - 修正部分は面的にJPEG再圧縮される？
    - 改ざん部分を面的に検出しやすい
  - 修正部分と周囲の間に補完処理が入る？
    - 改ざん部分が面的に検出しやすい
- 改ざんの際に「コピペ」することを検出
  - 同一画像が複数画面内に現れることを検索

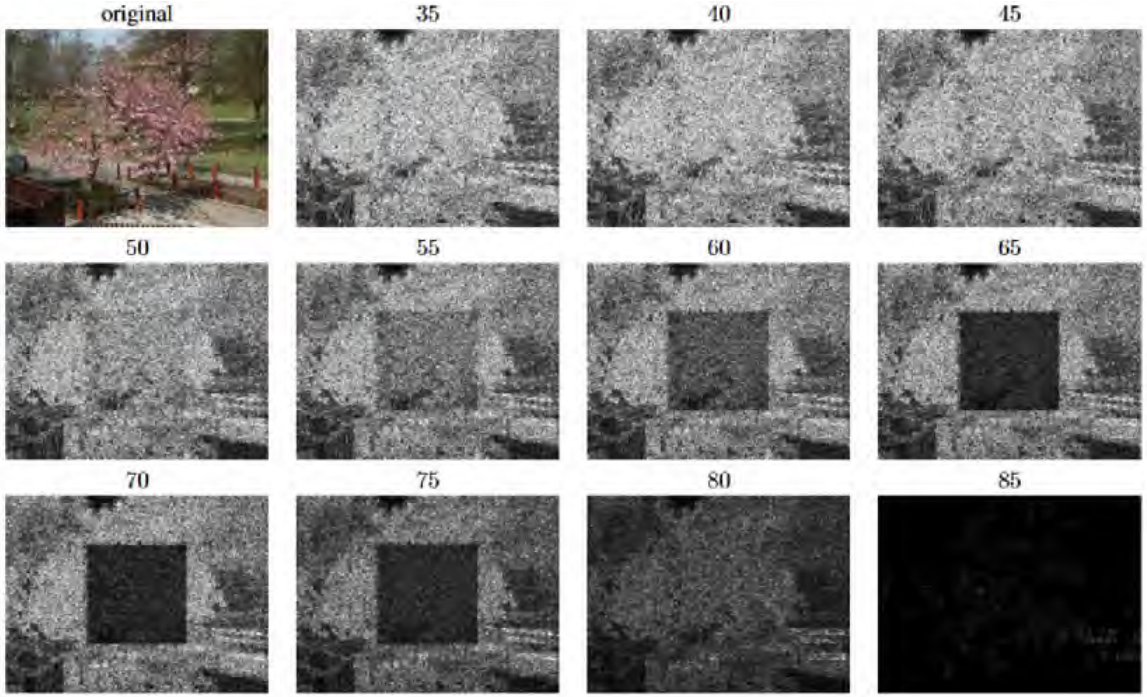
JPEGにおける離散コサイン変換

- カラーの時はRGB→YC_BC_R変換
- 画像を8x8のマクロブロックに分割
- 各ブロックを離散コサイン変換
  - 縦横とも画像を波の重ね合わせで表現
- 量子化処理した後、高周波成分を切り捨て



Media Qualityパラメータ≒圧縮率が違うことを検出

- 例えばH.Faridの”JPEG Ghost”

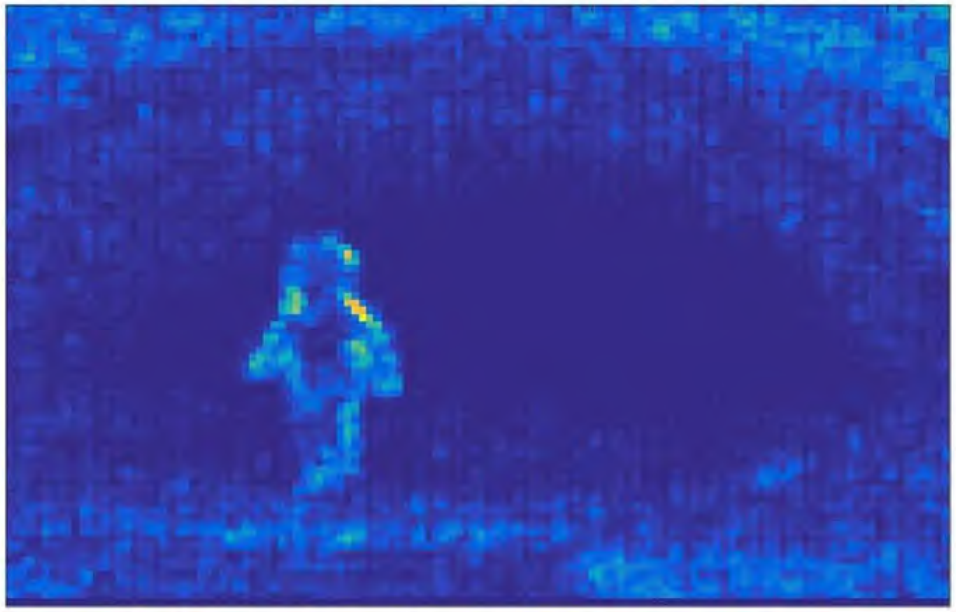


圧縮率が
違う部分が
画像処理で
浮かび上がる

H. Farid, ”Exposing digital forgeries from JPEG ghosts,” IEEE Trans. Inf. Forensics Secur., vol. 4, no. 1, 2009, pp. 154-160.

圧縮率の違いから何が分かるか？

a) Original Tampered Image

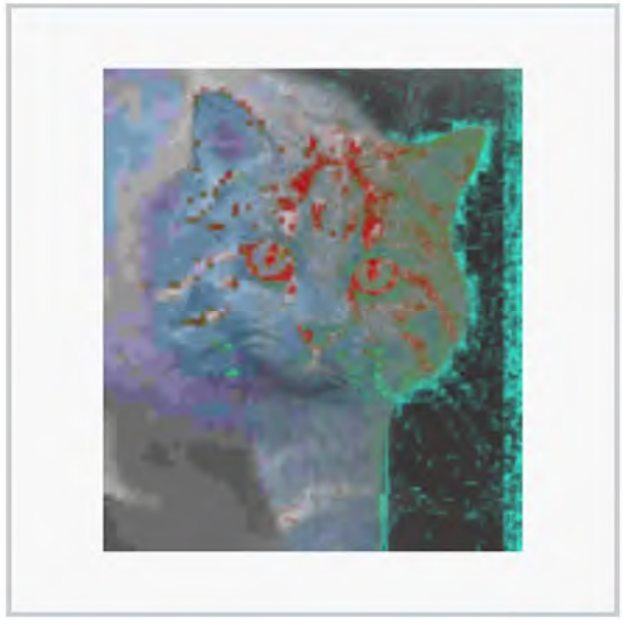


b) Detection using JPEG's quantization processes

人が見れば分かるが…

Error Level Analysis (From Wikipedia)





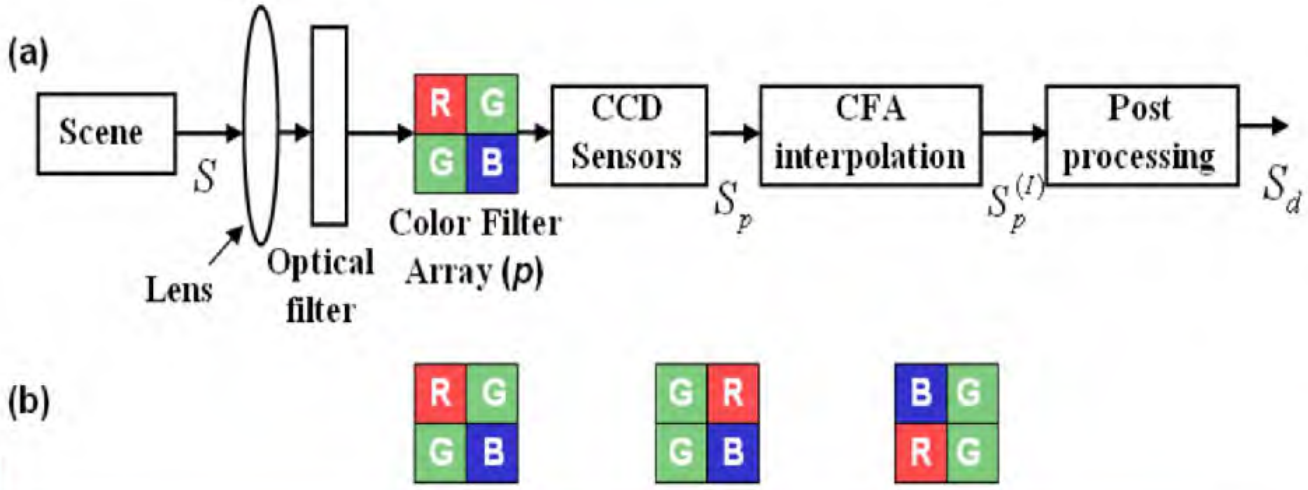
- 画像をある圧縮率で再圧縮して引き算

ELAは量子化ノイズを浮かび上がらせる

圧縮率が高いとノイズは消えやすい
高画質のところはノイズが残る

カメラのカラーフィルタ

- 撮像素子は1つの点は1つの色しか認識していない（カラーフィルタに依存）
- フィルタはColor Filter Array(CFA)と呼ばれ機種によって異なることがある
- CFAを推定する研究



A. Swaminathan, M. Wu, and K. J. R. Liu, Nonintrusive component forensics of visual sensors using output images, IEEE Trans. Inf. Forensics and Secur., vol. 2, no. 1, 2007

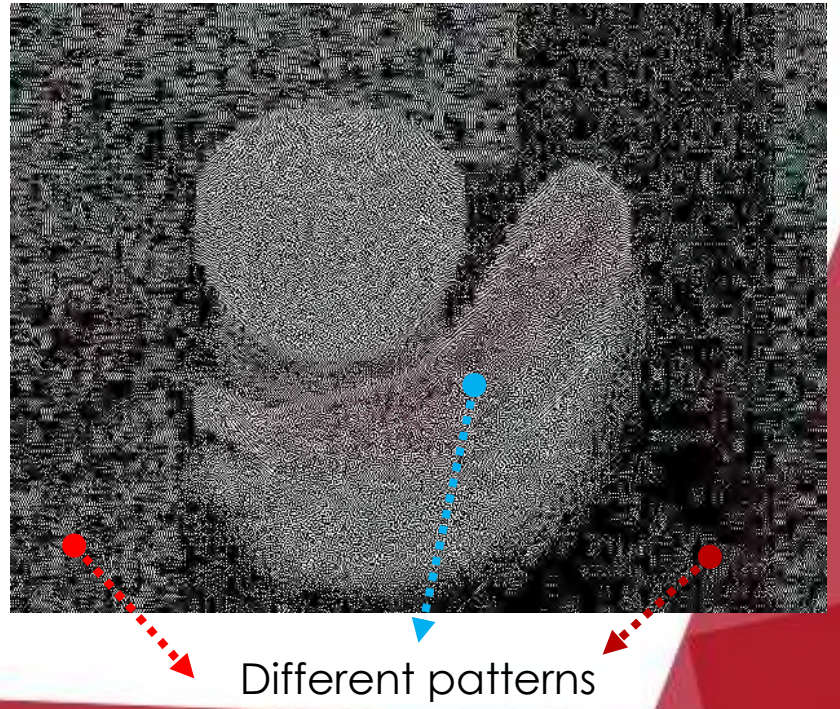
補完処理がパターンを生む

CFAの差やマクロブロックのアラインのずれ、
JPEG処理プログラムの細かなアルゴリズム差…

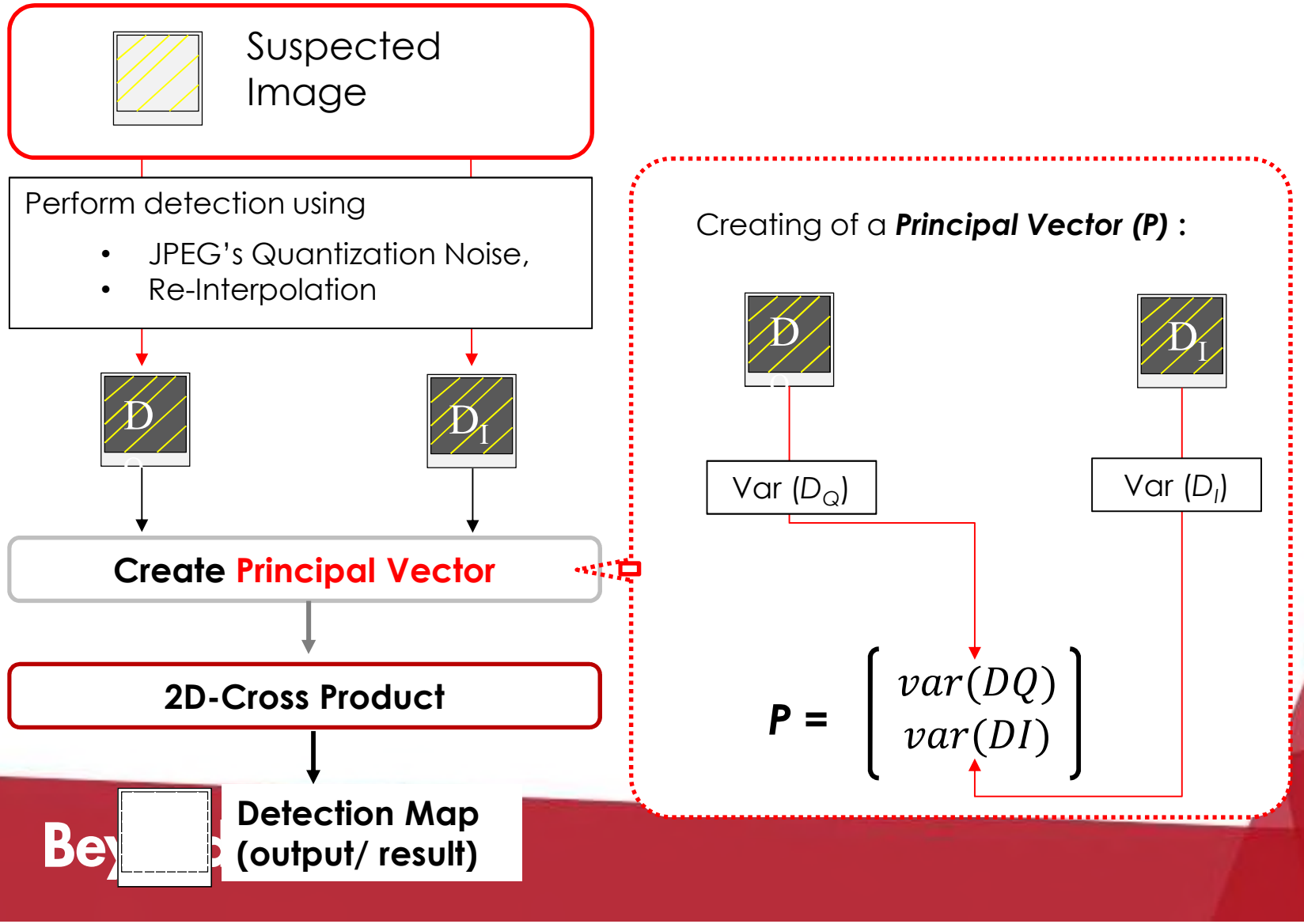
Original Tampered Image

Source: CASIA TIDE V2.0

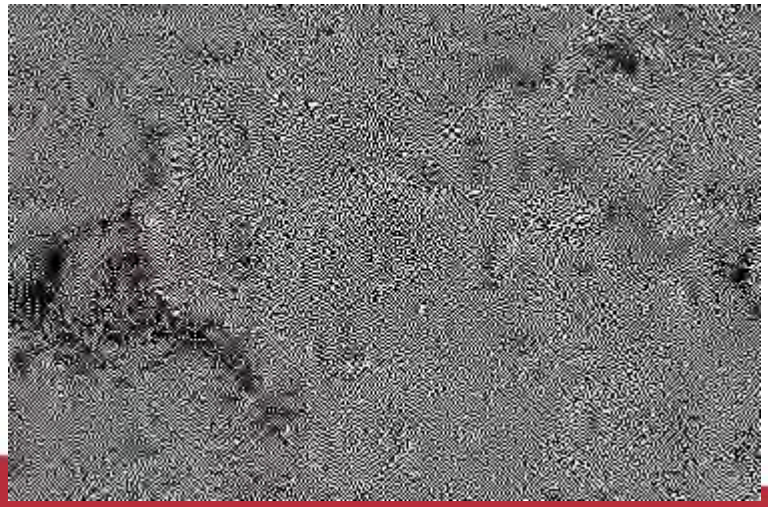
Detection Result

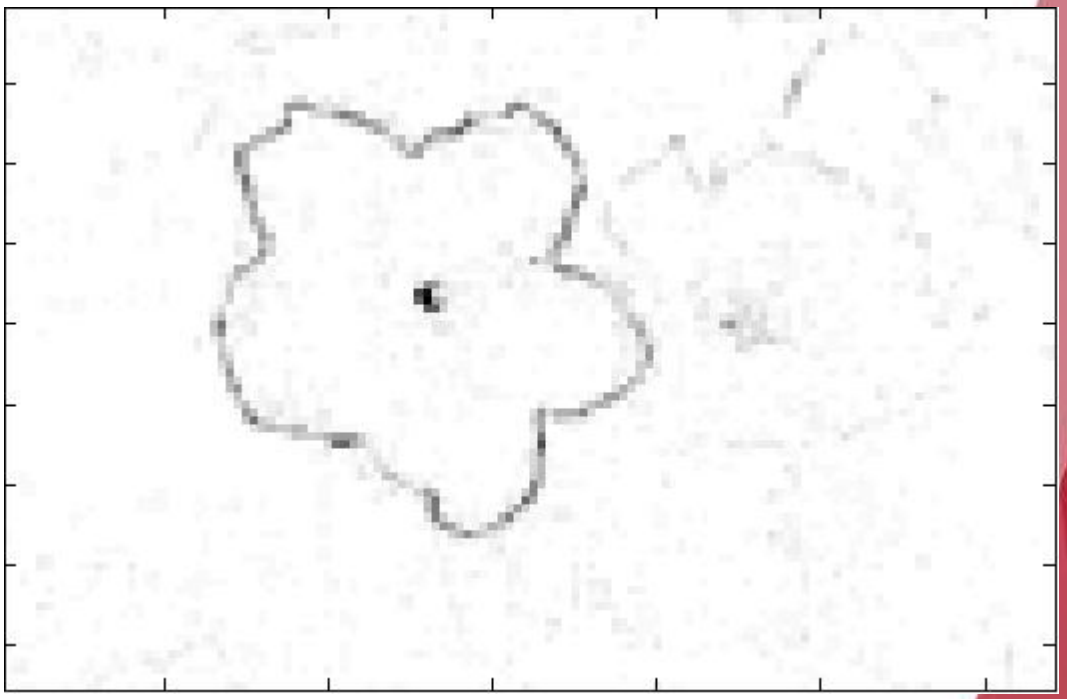


我々はこれらを組み合わせる研究



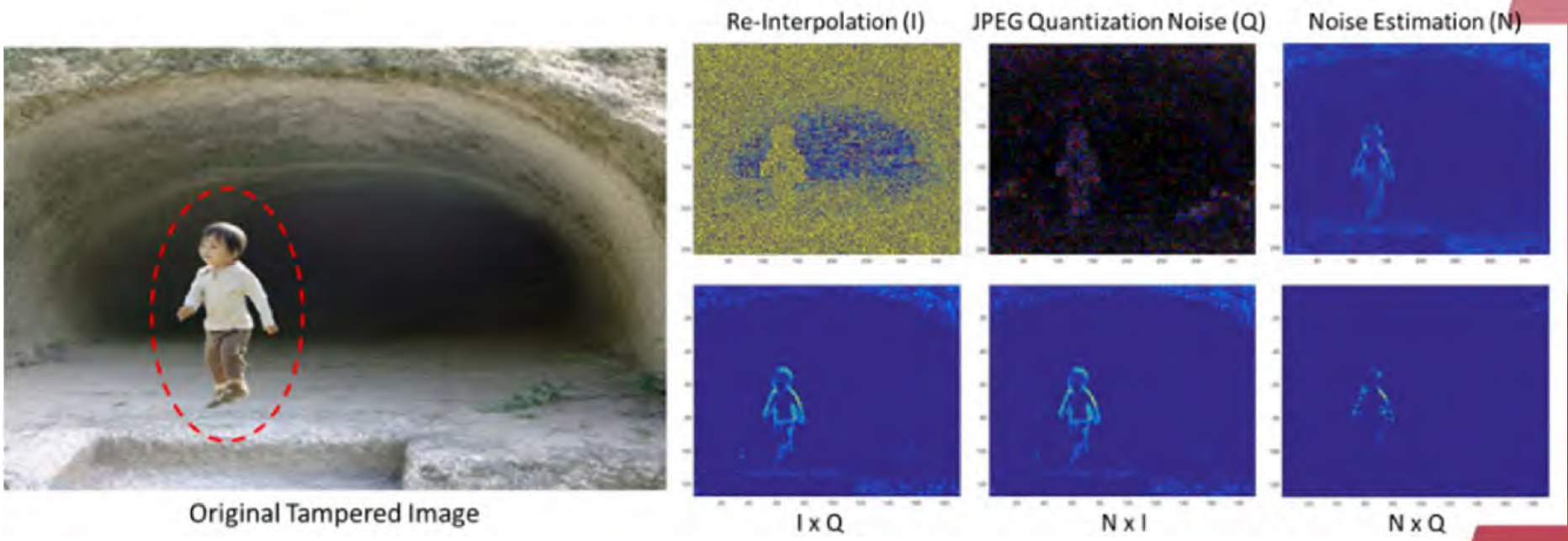
うまくいく例





A Comparison between **enhanced detection result** (right) and **non-enhanced results** (left)

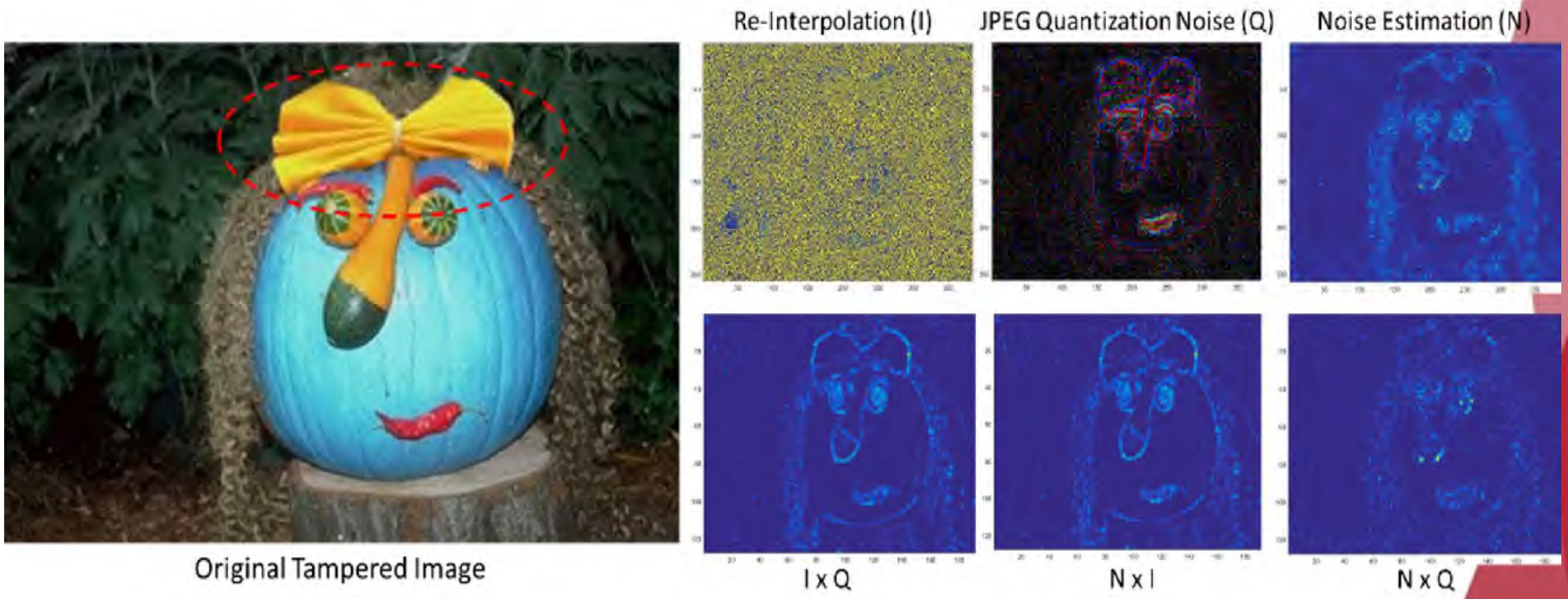
これもうまくいった



Source: CASIA TIDE V2.0

Note.
I = Interpolation based detection technique
Q = JPEG's Quantization & Compression noise based techniques
N = Image Noise Estimation technique

失敗例もある



Source: CASIA TIDE V2.0

Note.
I = Interpolation based detection technique
Q = JPEG's Quantization & Compression noise based techniques
N = Image Noise Estimation technique

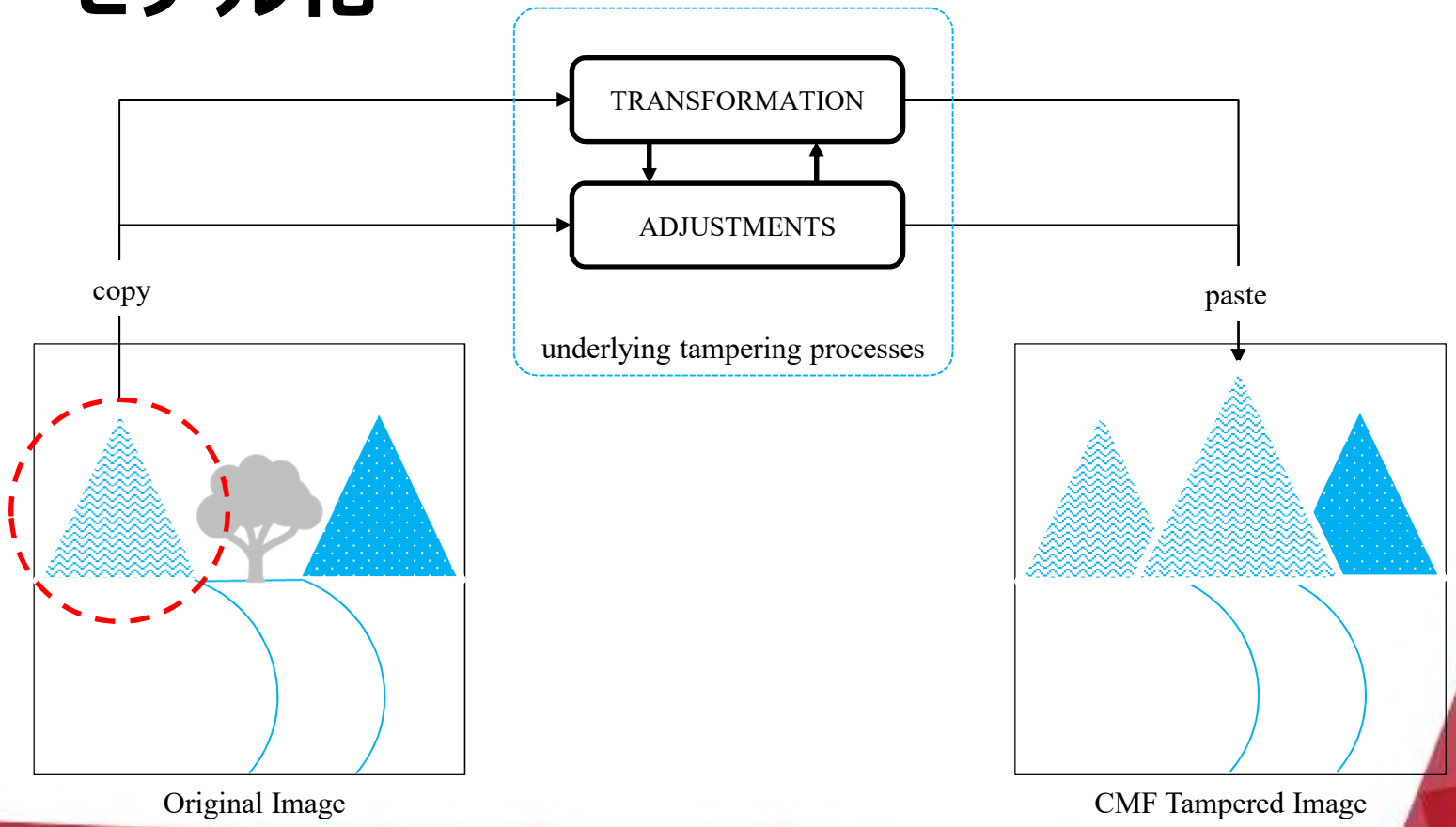
FAILED

「コピペ」の検出の課題

- Copy&Move Forgery (CMF)
- 単なるデーター致では済まない
  - 切り取り・拡大縮小・回転・変形等が組み合わされるため単純比較できない
- 計算量がどうしても多い
- 誤検出がそれなりに発生する
  - 同一パターンの繰り返し画像は大変
    - 例：レンガのカベ

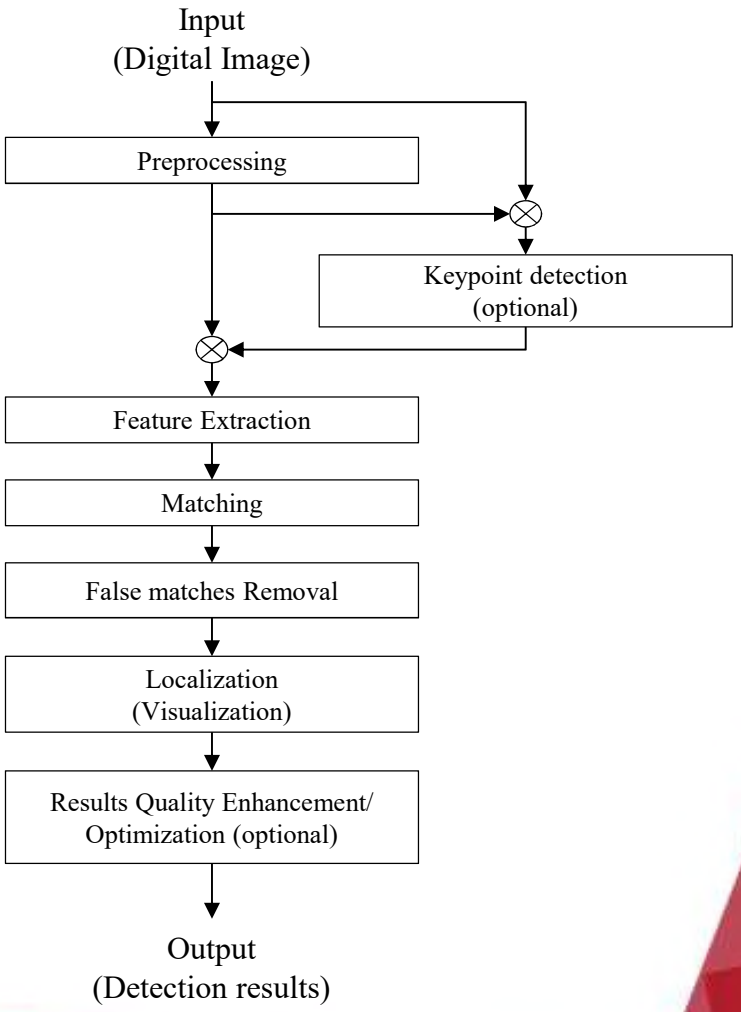
我々が行ったサーベイ

- モデル化

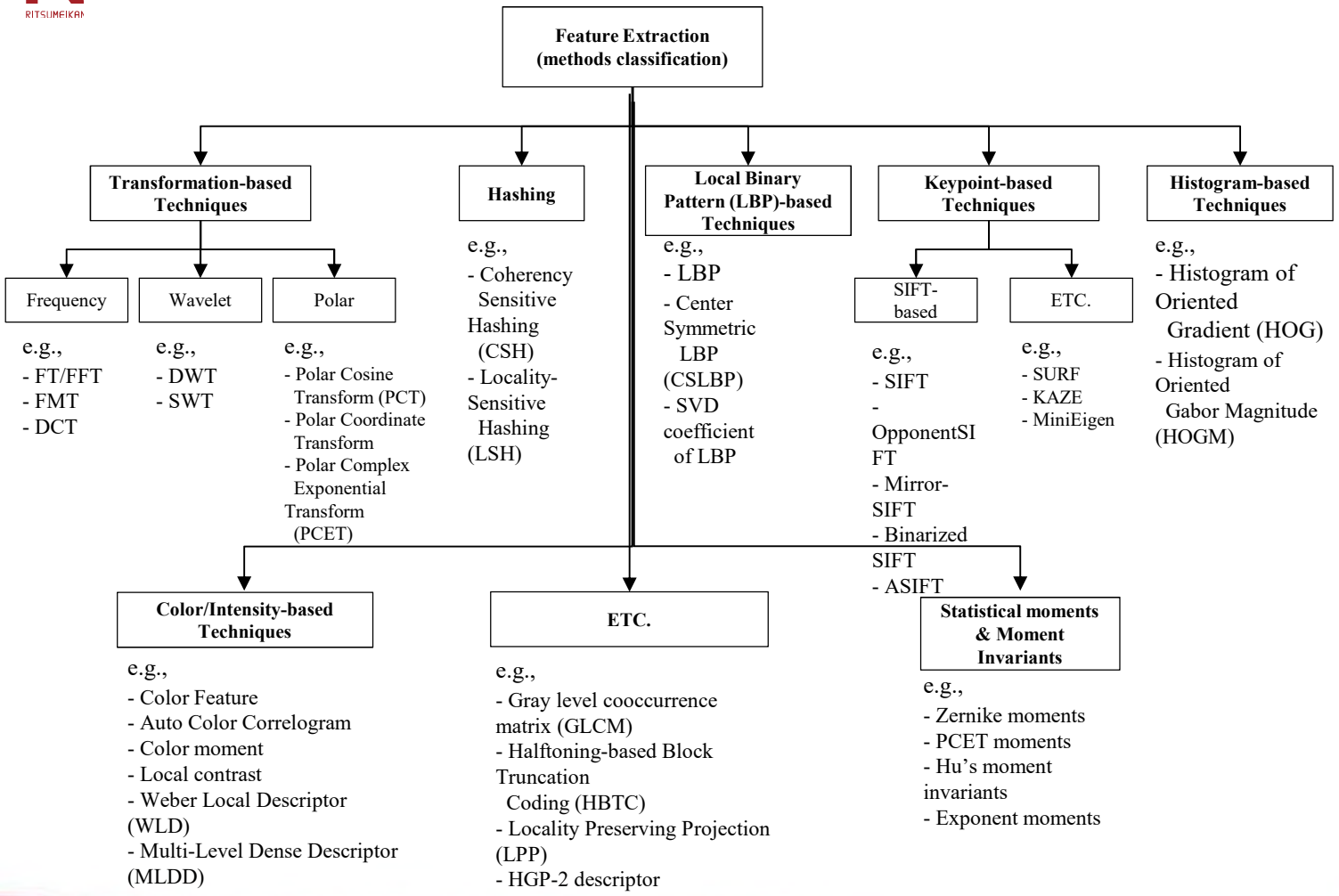


処理を分類

- 前処理
- 特徴点検出
- 特徴量測定
- 一致判定
- 誤検出除去
- 可視化
- 結果の強調

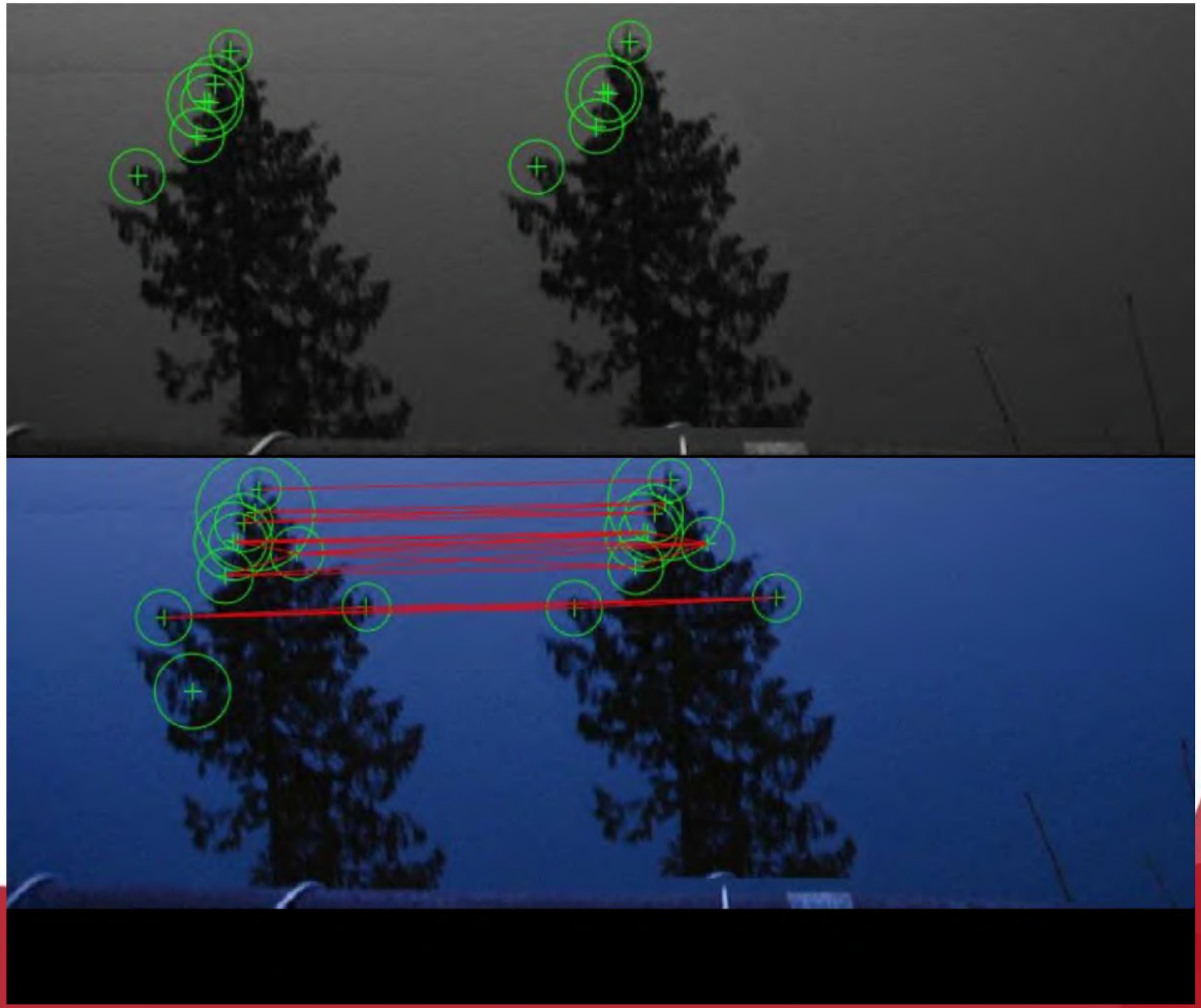


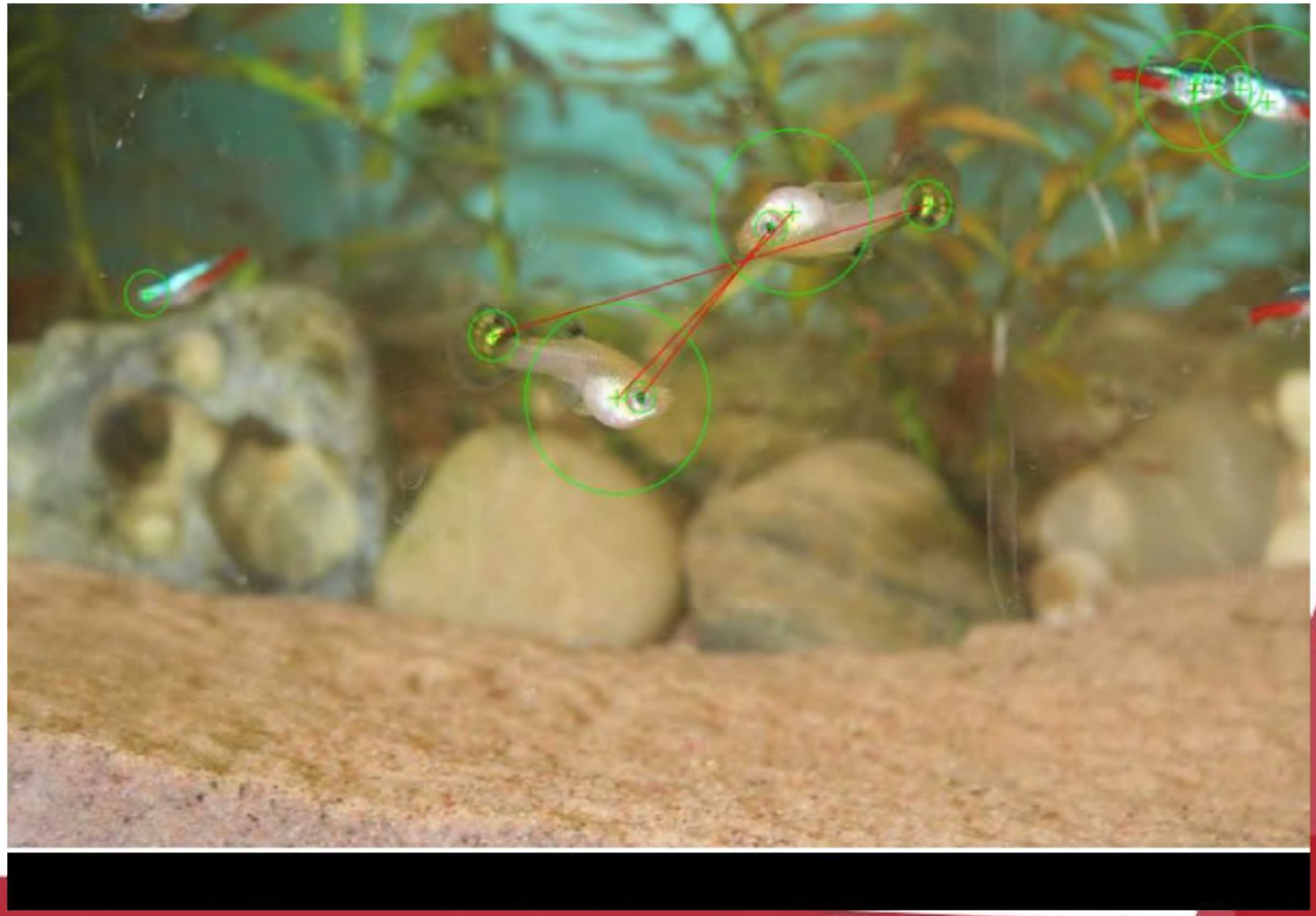
特徴量算出だけでも大量の研究



特徴点検出と特徴量算出
(Keypoint detection and Feature extraction)

- コーナー検出：角となる点を探す
  - Harrisのコーナー検出法
  - Laplacian of Gaussian (LoG)
    Difference of Gaussian (DoG)
- 不要な特徴点を削除
- 特徴点を基準に特徴量を算出
- 特徴量の対応を探すことにより
  CMFの痕跡を探す





特徴量の算出法
Feature Extraction

- 変形（移動・回転・拡大縮小）の検出
  - 極コサイン変換（Polar Cosine Transform）
  - Fourier-Mellin変換
  - 高速Fourier変換（FFT）
  - 定常ウェーブレット変換（SWT）
  - 離散コサイン変換（DCT）
- ハッシュ値の算出
  - 「似たような画像は似た値になる」
    ハッシュ関数を用いて特徴量を算出
    N.Krawetz: Perceptual Hash (Ave. Hashなど)
    X.Bi: Coherency Sensitive Hash
    など

Perceptual Hash

- Average Hash
  - 画像を8bitのグレイスケール化
  - 8x8画像に圧縮し、明るさの平均値を得る
  - 8x8領域が平均より明るいか暗いかの64bit値
- Perceptive Hash
  - 8x8グレー画像をDCTにかけたもの


00001101…

特徴量の算出法（続）

- Local Binary Pattern (LBP)
  - He, Wangらによる画像の繰り返しパターンを検出するためのアルゴリズム
  - 各点の8近傍点との類似度を8つの0,1で表してパターン化し特徴量とする
  - 単独では用いられないが他との組み合わせで特徴点マッチングに使われることがある

SIFT
（Scale-Invariant Feature Transform）

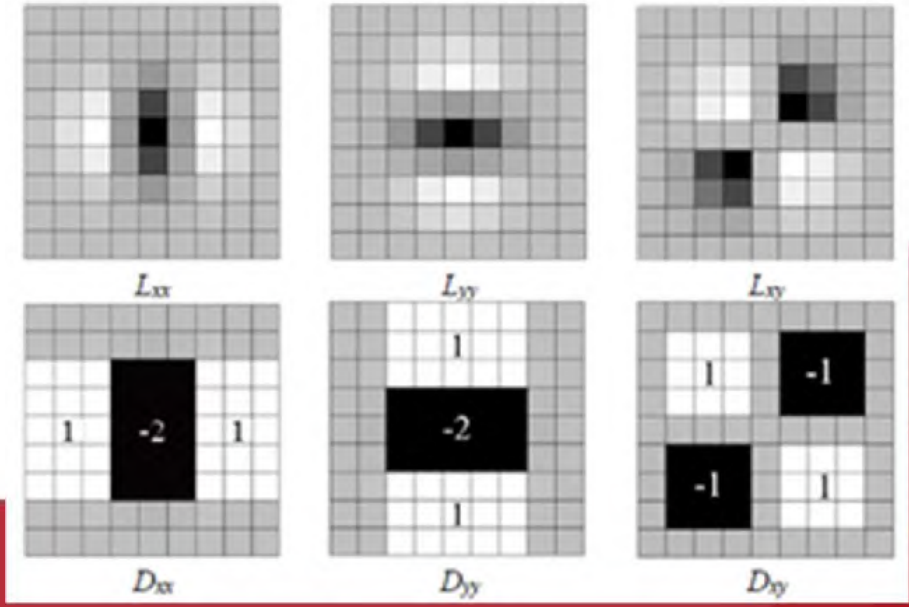
- British Columbia U. David Loweが2004年に論文化
- 2段階の処理
  - 特徴点（≒コーナー点）検出
    - スケール処理、特徴量算出
    - 特徴点を探すため、Difference of Gaussian （DoG）を利用
    - 特徴点を絞り込み処理
  - 特徴量記述
    - 特徴点の周りの点の特徴から向きを算出
    - 特徴点の周りの点やブロックの勾配から128個の値からなる特徴量を算出

Difference of Gaussian（DoG）

- 特徴点検出にはLoGが有効であることは知られていた（Linderburg, 94）が計算コストが高い
- それをDoGに置き換えることで高速化

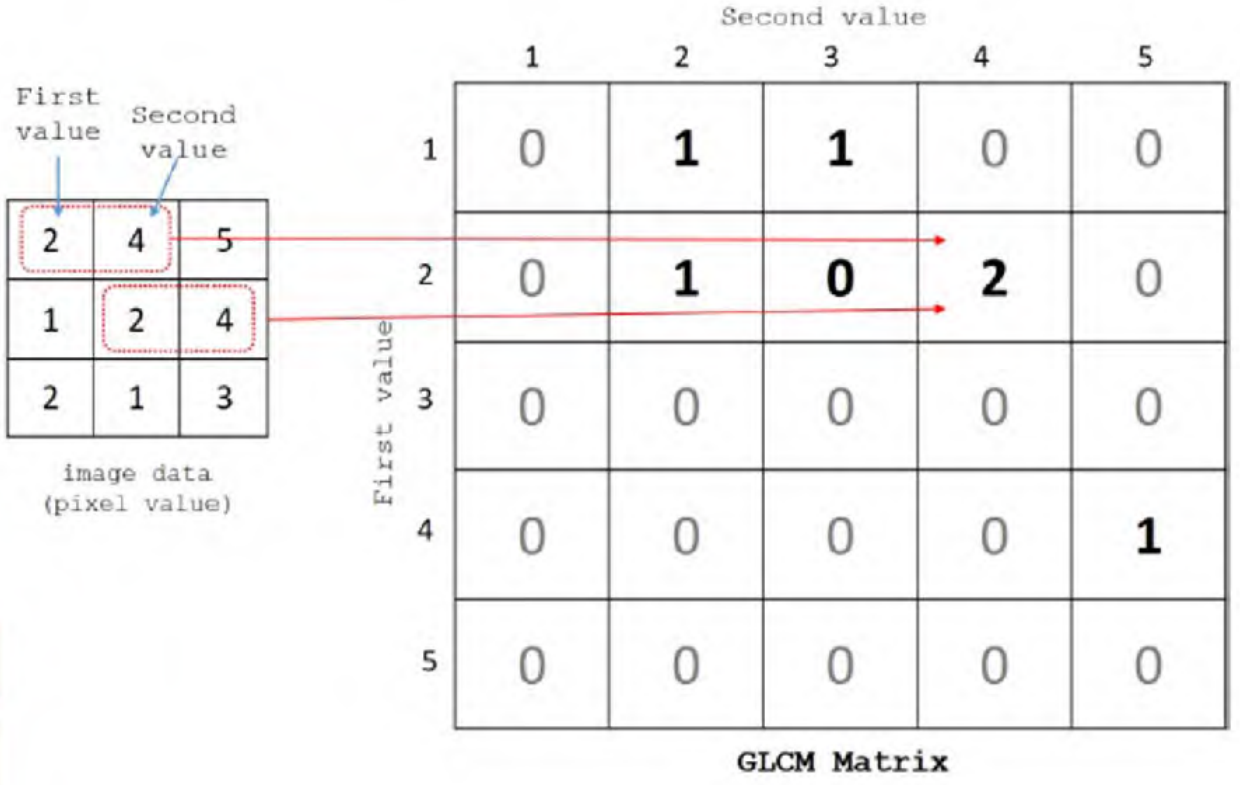
SURF
（Speeded-Up Robust Features）

- SIFTの遅さを補う提案
  Bay, H., Tuytelaars, T. and Van Gool, Lらによる（2006)
- DoGの代わりにBox Filterで近似
- 精度が落ちる



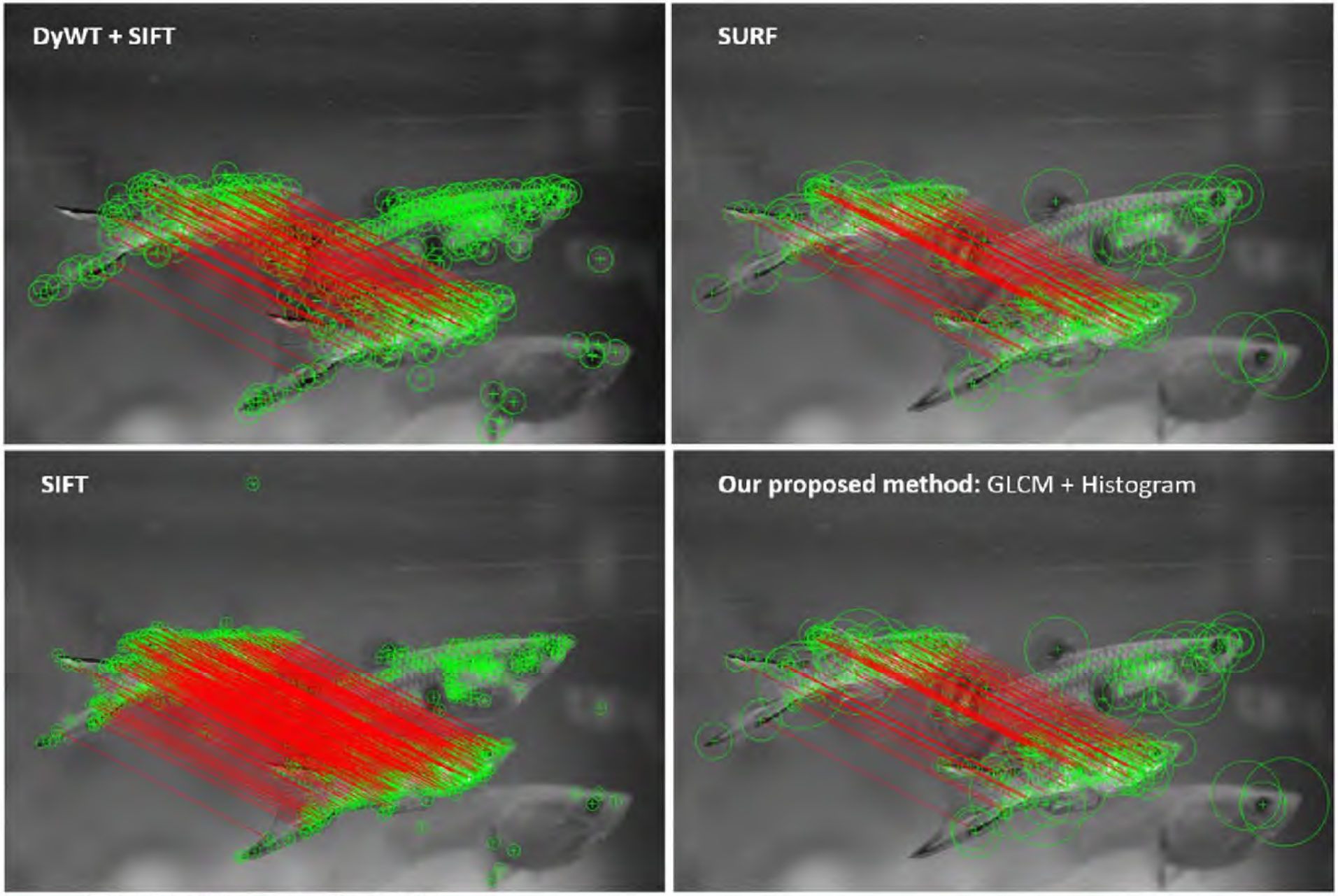
我々の手法

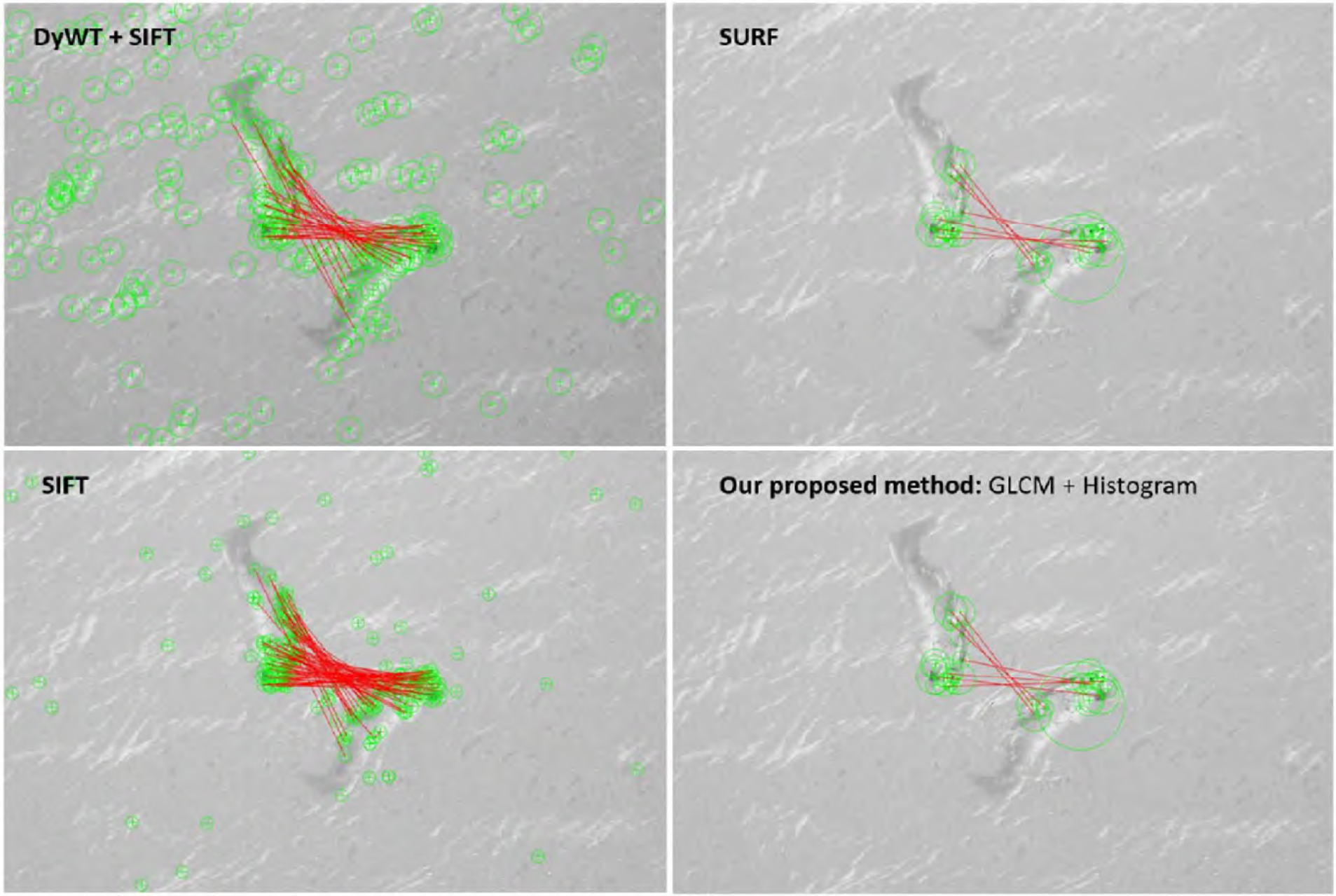
- MohanaiahらによるGLCMを活用
  Gray-Level Co-Occurrence Matrix



GLCMをさらに活用して…

- GLCMを特徴点の周り4点について積算
- この値にさらに2つの特徴量を得る
  - Shijinらによるコントラストに基づく特徴量
  - 特徴量の周囲の点と特徴点との明るさの差を64個のビンに分けた場合のヒストグラム
- これらから特徴量を得て比較する


DyWT + SIFT
SURF
SIFT
Our proposed method: GLCM + Histogram


DyWT + SIFT
SURF
SIFT
Our proposed method: GLCM + Histogram

現状の結果

- SURFとSIFTの中間程度の精度を
  SURFの3倍、SIFTの2.5分の1の時間で

Table 1 Performance using F_1 and accuracy (ACC) score

Methods	p	r	F_1	ACC	Time
SIFT	0.63	0.71	0.65	94.68	7.92
DyWT+SIFT [20]	0.48	0.41	0.43	90.06	1.71
SURF [19]	0.57	0.59	0.55	89.64	0.81
Our approach	0.72	0.60	0.64	92.36	2.98

ほかの特徴量

- ヒストグラムに基づく特徴量
  - SIFTにおける特徴点の「方向」決定など
  - Leeらによる
    histogram of oriented gradient (HOG),
    hist. of oriented Gabor magnitude（HOGM）.
- 色や輝度に基づく特徴量
- 統計的な積率（モーメント）に基づくもの
- そのほか

残念ながら決定打はまだない

- SIFT, SURFという2つの特徴点検出アルゴリズムが比較的性能が良いがFalse positiveが避けられない
  - 我々はSURFより少し遅いがSIFT程度の精度が出る手法を提案中
- CMFの候補が出ても現状ではまだ人の判定が必要で自動化は遠いのでまだまだ研究が必要