The 32nd Annual Conference of the Japanese Society for Artificial Intelligence, 2018

画像認識を用いた ATM セキュリティ強化

Security Reinforcement for ATM by Using Image Sensing

岸礼子[*1] Reiko Kishi　ファンチョンフィ[*1] Phan Trong Huy　山本一真[*1] Kazuma Yamamoto　増田誠[*1] Makoto Masuda

[*1] 沖電気工業株式会社 経営基盤本部 研究開発センター
Corporate Research and Development Center, Oki Electric Industry Co., Ltd.

ATM (Automated Teller Machine)-related crimes have been reported as serious problems overseas. One of such crimes is *skimming*: the act of installing skimming device on ATM to illegally copy information of cash cards or passwords. Detecting such illegal acts promptly is important since we can immediately prevent ATM-related crimes by automatically raising alarms and also reduce supervisor's monitoring burden. We have realized an anomaly behavior detection technique which finds not only suspicious devices but also detects actions of installing them. In this article, we discuss our proposed method which combines video feature extraction, ATM status acquisition and recognition. Compared to processing only image information, the proposed method proves to be more effective in recognizing anomaly behaviors from normal behaviors.

1. はじめに

海外では ATM（Automated Teller Machine）利用者のカード情報や暗証番号情報を盗み取るスキミング等の犯罪が深刻な問題となっている。このような犯罪を実行時に検知することは、その場での警報や通報による犯罪抑止や監視員の負担軽減につながるため重要である。しかし近年は犯罪装置の小型化が進み、ATM 外観からは犯罪装置の識別が困難となっている。そこで我々は犯罪装置だけでなくそれを取り付けている行為も検知する技術を実現した。

本稿では、動画像処理による異常行動検知手法に“ATM 状態把握”を組み合わせた ATM 異常行動検知手法を提案する。さらに模擬データを用いて提案手法の有効性を示す。

2. 動画像処理による異常行動検知手法

本章では、一般的な動画像処理による異常行動検知手法を紹介し、ATM へ応用する際の課題を述べる。

2.1 一般的な動画像処理による異常行動検知

動画像処理による異常行動検知手法は一般的に、“動画像特徴抽出”と“識別処理”が用いられる。

[南里 2005]は、動画像特徴に立体高次局所自己相関（CHLAC）を、識別処理には部分空間法を用いている。CHLAC は画素値を 2 値化した連続する 3 フレーム間の局所領域を 251 個のパターンに当てはめる手法である。異常行動が正常行動の中に混ざっても検知可能（加法性）で、かつ、検知性能は画像内の位置に依らない（位置不変性）という利点を持っている。部分空間法では、特徴空間上に正常行動の部分空間を構成し、入力フレームの特徴量とその部分空間との距離を異常度として扱っている。これにより、複数人歩行者の中での転倒動作を異常として検知し、手法の有効性を示している。

[弓場 2012]は、動画像特徴として Space-Time Patch（ST-Patch）、識別には Continuous Rank-Increase Measure（CRIM）を用いている。ST-Patch は、動画像の小領域内の濃度勾配値の統計量から求められる。勾配値は上下左右の画素に加え連続するフレーム間からも求めるため、特徴量は「見え」と「動き」の情報を併せ持っている。CRIM は、ST-Patch から計算できる非定常度の値で、この値が閾値を超えたときに異常とみなしている。ST-Patch と Real AdaBoost と呼ばれる機械学習手法によって人物領域検出を行い、Real AdaBoost の信頼度を用いて人物領域内の人の部分に重み付けを行った CRIM で異常検知を行っている。それによって、エスカレーターでの転倒を対象とした動的な背景下での異常行動検知手法を提案している。

その他にも異常行動検知に用いられる手法には、動画像特徴として、[林 2006]では Optical Flow、[Kobayashi 2012]では STACOG、[弓場 2012]では MHI などがあり、識別処理としては、Linear Discriminant Analysis（LDA）、Support Vector Machine（SVM）、Gaussian Mixture Models（GMM）などがある。

2.2 ATM 異常行動検知での課題

我々は動画像処理による異常行動検知を ATM に対する犯罪の検知に応用する。監視カメラは ATM の上部に設置し、手元の細かい動作がわかるように、操作部を中心に撮影する（図 1）。

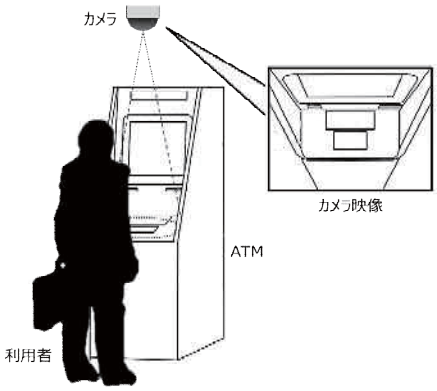

図 1: 撮影イメージ

連絡先: 岸礼子, 沖電気工業株式会社 経営基盤本部 研究開発センター, 埼玉県蕨市中央 1-16-8, kishi422@oki.com

「引き出し」「預け入れ」などの ATM に対する通常操作が正常行動となる。正常行動は動作速度に個人差があり、さらに端末上に手を置く・持ち物を持つなど操作以外の動作が含まれる。また、異常行動はカードを挿入口へ差し込むふりをして犯罪装置を設置するなど、正常行動に似せた犯罪行動が起こり得る。このように正常行動と異常行動に多様性があるため動画像処理のみでの識別は十分な精度を期待できない。

3. 提案手法

我々は "ATM 状態把握"を導入し、動画像特徴量抽出と ATM 状態把握および識別処理による異常行動検知手法を提案する。本手法は異常検知辞書を作成する学習フェーズと、異常検知辞書を用いて異常行動を検知する検知フェーズに分かれる。本章では、"ATM 状態把握"の概要、学習フェーズと検知フェーズについてそれぞれ説明する。

3.1 ATM 状態把握

"ATM 状態把握"とは、「無人状態」「暗証番号入力状態」などといった ATM の取引状態(以下、ATM 状態)を把握することである。ATM 状態把握により、起こり得る正常行動を限定できることが大きな利点である。図 2 のように、無人状態から利用者が取引を行って立去るまでには ATM 状態は多様に変化する。例えば「暗証番号入力状態」では暗証番号キーに対する動作が発生するが、それ以外の ATM 状態時に暗証番号キー周辺に動作があれば警戒する必要がある。「近接状態」は取引開始前または終了後のことである。そのため ATM 操作のような複雑な動きは起こらないはずであり、複雑な動作がある場合には警戒する必要がある。このように、ATM 状態把握によって起こり得る動作を絞ることで、異常行動検知の識別性能の向上が可能になる。

ATM 状態は、ATM 自体から通知される内部状態の情報を用いて把握する。

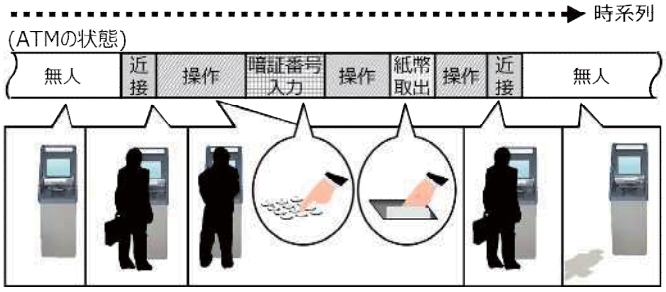

図 2:ATM 状態が変化していく例

3.2 学習フェーズ

学習フェーズでは、正常行動のみを用いて機械学習を行い ATM 状態毎の異常検知辞書を生成する。

図 3 に提案手法の流れを示す。まず、カメラから映像を取得し、フレームごとに正規化画像を生成し、特徴量を抽出する。ATM 状態把握では、入力フレームに対応する ATM 状態を取得しておく。その後、ATM 状態ごとに蓄積しておいた特徴量に対して、機械学習を用いて ATM 状態毎の異常検知辞書を生成する。

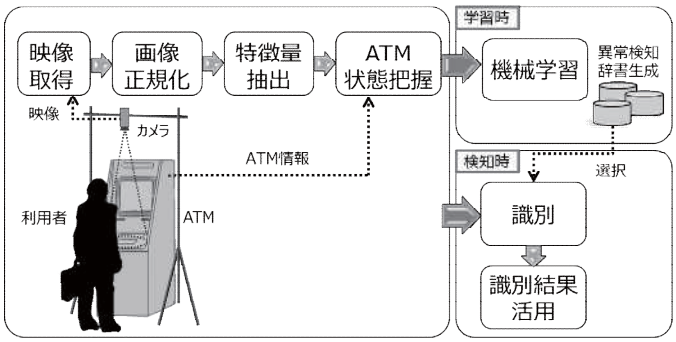

図 3:提案手法の流れ

3.3 検知フェーズ

検知フェーズでは、入力フレーム毎に正常／異常を判定する。

映像取得から ATM 状態把握までは、学習フェーズと共通の処理となる。入力フレームと同じ ATM 状態時の特徴量から生成した異常検知辞書を選択して識別処理を行い、正常／異常を判定する。識別結果活用では、結果が異常だった場合にのみアラーム発報、ATM 画面へのメッセージ表示、監視センターや ATM 管理者への通知・通報などを行う。

4. 評価

提案手法の有効性を確認するための実験を行った。本章では、従来手法(動画像特徴抽出と識別処理)と提案手法(動画像特徴抽出と ATM 状態把握および識別処理)でそれぞれ異常行動検知を行い、結果を比較する。

4.1 処理概要

従来手法と提案手法の間で"ATM 状態把握"に関わる処理以外は共通である。映像をフレームレート 10fps で取得し、画像正規化で 640×480 pixel にリサイズする。動画像特徴には細かい動きに対応できる ST-Patch を使用し、識別処理には一般的に用いられる部分空間法を用いた。入力フレームの特徴量と正常行動の部分空間との距離を異常度として算出し、異常度が閾値を超えた場合に「異常」と判定する。

4.2 評価データ

社内で模擬環境を構築し、実際に ATM に対する動作の映像を取得した。被験者として社員 149 名を集めて撮影し、正常行動データと異常行動データを生成した。正常行動データは、ATM の通常の取引を撮影したものとなる。通常の取引の中には、左手の操作、手を置く動作、紙幣を数える動作など特徴のある動きを意図的に含んでいる。異常行動データは、一般に知られている犯罪事例を元にしてシナリオを作り、犯罪行動を真似た動きを演じることで生成した。学習データと検知データにはそれぞれ以下を用いた。

- 学習データ:
  正常行動　約 800 動作(約 60 万フレーム)
- 検知データ:
  未学習の正常行動　約 240 動作
  異常行動　32 動作

ここでの異常行動は、カード挿入口に犯罪装置を取り付ける行為である。犯罪装置は厚紙などで模式的に製作したもので、カード挿入口を覆う様に取り付けられる。

4.3 評価方法と結果

本稿では、動作単位で評価を行う。各動作の中で一度でも異常と判定されたフレームがあればその動作を「異常」とし、そうでない場合は「正常」とする。評価指標には、Equal Error Rate（EER）を用いる。EER は、正常行動の誤検知率と異常行動の未検知率が等しくなるときのエラー率である。

従来手法は EER が 8.3% となった。正常行動に含まれているカードの入れ直しをする動作が高い異常値となったことが原因として挙げられる。一方、“ATM 状態把握”を導入した提案手法では EER が 0.0% となり、正常行動と異常行動を全て正しく識別できた。従来手法は、多様な正常行動を一つの部分空間にするのに対し、本手法は ATM 状態毎に起こり得る正常行動を学習するため、従来手法で見られた誤検知・未検知が改善されたと考えられる。

表 1：評価結果

	従来手法	提案手法
EER	**8.3 %**	**0.0 %**

5. おわりに

我々は、犯罪装置取付けなどの犯罪行動の検知が可能な異常行動検知技術を実現した。動画像特徴量抽出と ATM 状態把握および識別処理を組み合わせた手法を提案し、動画像処理のみでは識別できなかった正常行動と異常行動に対して結果が改善されることを確認した。本技術は ATM 操作に不慣れな人の戸惑い検知への応用も期待できる。

本評価データは疑似環境データでの評価のため、実環境データでの検証が必要である。

参考文献

[南里 2005] 南里卓也, 大津展之: 複数人動画像からの異常動作検出, 情報処理学会論文誌, vol.45, no.SIG_15, pp.43-50, 2005.

[弓場 2012] 弓場竜, 村井泰裕, 藤吉弘亘: 時空間特徴の統計的学習を用いた異常行動検知, 電子情報通信学会論文誌, vol.J95-D,no.6,pp.1369-1379,2012.

[林 2006] 林健太郎, 羽下哲司, 関真規人, 笹川耕一: 映像監視における人物位置行動の検出技術, 情報処理学会論文誌, vol.47, no.SIG_9, pp.12-19, 2006.

[Kobayashi 2012] Kobayashi, T., Otsu, N., : Motion recognition using local auto-correlation of space–time gradient, Pattern Recognition Letters, vol.33,no.9,pp.1188-1195,2012.

[弓場 2012] 弓場竜, 縣禎輝, 藤吉弘亘: 回帰推定による欠損距離画像の動作特徴量補正法, 電子情報通信学会技術研究報告, 信学技報, 2012.