

〈研究発表〉

画像解析型侵入検知システム

藤原 伸行¹⁾, 秋元 淳一郎²⁾

(株)明電舎 基礎技術開発部 (〒410-8588 沼津市東間門字上中溝 515, E-mail: fujiwara-n@mb.meidensha.co.jp)¹⁾
 (株)明電舎 ITソリューション推進室 (〒141-6029 東京都品川区大崎 2-1-1, E-mail: akimoto-j@mb.meidensha.co.jp)²⁾

概要

上水道施設等のライフラインには、近年のセキュリティ意識向上やテロ対策として、各種フェンスセンサが設置されて来ている。しかしながら、フェンスセンサだけでは、既に構内に入ってしまった侵入者や毒物・爆発物の投げ込みには無力である。一方、浄水場等には監視カメラが配備されており、職員が監視モニターで広く構内を監視できる場合も多い。ここでは監視カメラの画像を処理し、職員の代わりにIT機器で侵入者等を自動検知する「画像解析型侵入検知システム」を紹介する。本システムは昼夜を問わず高い検知率と耐環境性を有し、屋外監視に適したものとなっている。

キーワード: 侵入検知, 監視カメラ, 画像解析, セキュリティ, 浄水場

1. はじめに

近年のセキュリティ意識向上やテロ対策として、重要施設の監視においては、Fig.1 に示すような赤外線ビームや開閉検知センサ等の物理的なセンサ情報を用いる手法¹⁾が適用されており、上水道施設等のライフラインには、各種フェンスセンサが設置されて来ている。しかしながら、フェンスセンサだけでは、既に構内に入ってしまった侵入者や毒物・爆発物の投げ込みには無

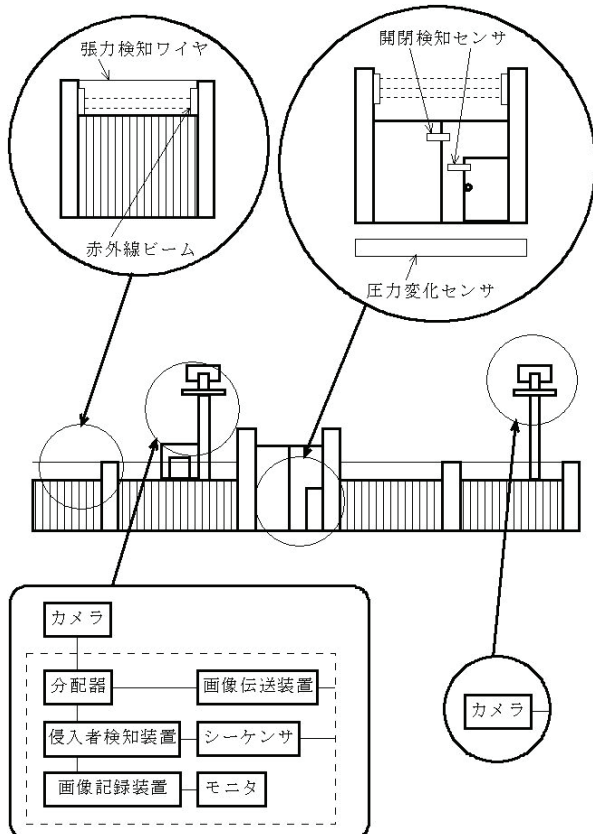


Fig.1: Sensors for Observation

力である。別の監視手段として、浄水場等の重要施設には多くの監視カメラが配備されている。これは Fig.2 に示すような監視カメラの画像を監視員が集中管理室のモニターにより視認監視する手法である。これは広い監視範囲を常時監視することができるが、多くの監視モニターを少数の監視員が一度に監視するため監視員の負担が大きいといった問題がある。そこで、監視カメラの画像を処理し自動的に侵入者を検知する装置の導入が期待されている。

本稿では、監視カメラの画像を処理し侵入者等を自動検知する、画像解析型侵入検知システムを紹介する。本システムは昼夜を問わず高い検知率と低い誤検知率を有し、屋外監視に適したものとなっている。

2. 侵入検知システムの構成

我々は受変電設備の監視を主な対象として監視カメラ画像による画像監視システムを開発して来た³⁾。このシステムは監視カメラのアナログ画像をそのまま監視モニターへ出力するものではなく、画像伝送端末と呼ばれる画像変換装置と、画像配信サーバと呼ばれる画像の管理と配信を行う装置を用意し、監視カメラの画像を画像伝送端末で一旦受け、画像伝送端末から通信回線を用いて画像配信サーバへ送り、画像配信サーバから要

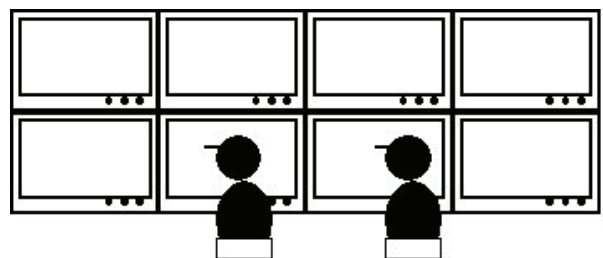


Fig.2: Example of a guard box

求に応じてクライアントPCへ画像を配信するものである。Fig.3にこのシステムの概念図を示す。

ここで監視カメラ画像から侵入者を自動的に検知する侵入検知システムの構成について考える。従来から用いられている構成は、監視カメラ画像を直接侵入検知装置へ入力する方法である。この構成は監視カメラと侵入検知装置のみによって侵入者を自動検知するシステムを基本的に構成でき、小規模な監視システムとしては安価な構成を実現できる。しかしながら、大規模な監視システムを構築する場合は、監視箇所それぞれに侵入検知装置を設置する必要があり、逆にコスト高となってしまう。さらに、テロ対策を考慮した場合は、侵入検知装置や画像蓄積を担う装置等、監視システムとして重要な装置が各所に分散している構成は、安全管理運用上好ましくない。そこで我々は、侵入検知装置にもクライアントPCと同様に画像配信サーバからネットワーク経由で画像を受け取る機能を持たせ、複数箇所の監視カメラ画像を処理して自動的に侵入者検知を行う「検知サーバ」として構成する手法を採用した。検知サーバの操作画面をFig.4に示す。検知サーバは1台で同時に4chまでの監視カメラ画像を処理し、1chにつき最大で16個の侵入物を7.5[fps]の処理速度で同時に検知することができる。

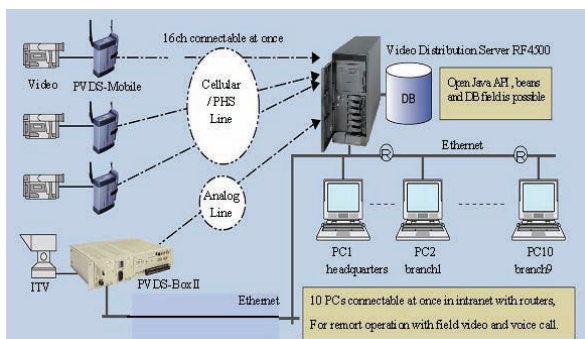


Fig.3: Image delivery system



Fig.4: a display of the detection server

侵入検知システムの構成をFig.5に示す。このシステムでは機能別に処理を担当する装置を用意し、それぞれを個別にLANへ接続してネットワーク経由で情報の授受を行う構成となっている。このため、クライアントパソコンとメッセージ出力用パソコンは事務所へ、画像配信サーバと検知サーバは計算機室へ設置する等、レイアウトをユーザ側が自由に設定することが可能で、各装置を機能別に適所へ設置することができる。つまり、監視システムの核となる画像配信サーバと検知サーバを安全な場所へ集約でき、被監視箇所には工業用監視カメラと、ディスクレスな小型低発熱広温度範囲動作対応の画像伝送端末、および、小型通信装置を堅牢な盤収納して設置すれば良く、厳重な保安体制を要する箇所を削減出来る。

3.侵入者の検知

施設への侵入者の行動パターンとしては、施設外部から施設へ接近し、施設との境界を乗り越えて施設へ侵入するケースが一般的である。また、施設へ侵入する前に施設周囲を徘徊し、施設状況や侵入経路の調査を行う事も少なくない。このため、施設への侵入者の監視においては、施設を隔てるフェンス、壁といった境界近傍を徘徊する不審者の状態を検知することが重要である。そこで我々は、画像上において監視する範囲(これを「検知領域」と呼ぶ)を設定し、検知領域へ侵入した不審者を追跡すると共に、検知領域の中で施設を隔てる境界に仮想的な線を設置し(これを「侵入禁止線」と呼ぶ)、その侵入禁止線を囲む矩形の検査範囲を設けて検査範囲に入る不審者の状態を検出した。この時の不審者の状態として、単に検知領域へ入ったものを「検知」、施設を隔てる侵入禁止線の接近側領域に在るものを「警戒」、侵入禁止線の侵入側領域に在るものを「警報」、更に検知領域から居なくなった不審者を「消失」とした(Fig.6)。このように、施設を隔てる境界近傍

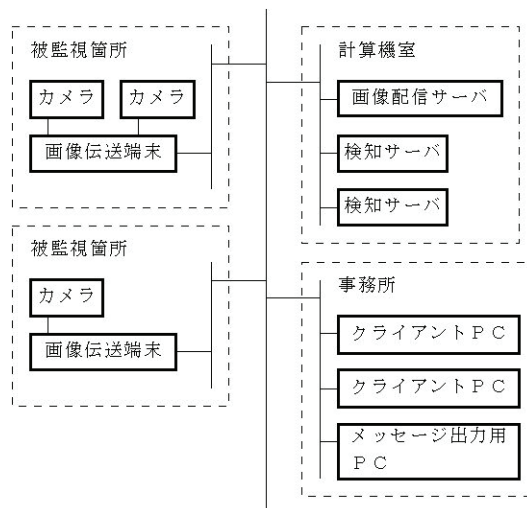


Fig.5: System configuration

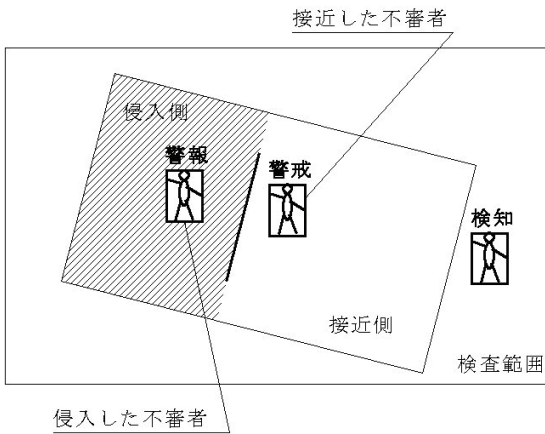


Fig.6: Action of intruders by the borderline

の不審者の状態を幾つか持つことで、検知した不審者が施設に対して現在どのような状態にあるかを把握し、不審者が接近した場合は注意を、侵入した場合は警告を発生し警備員が出動する等、不審者のそれぞれの状態に応じた適切な対応が可能となる。検査範囲に入った不審者を検出する方法としては、後述する局所領域の時間相関変化を用いた。

4. 局所領域時間相関変化による侵入検知

画像の状態判定を行う手法として時間的に変化する画像の相関値の時間変化パターンである時間相関を用いる。これは Fig.7 に示すように監視カメラから入力した画像を矩形の小領域に分割し、一つ一つの小領域について、背景画像と対応する小領域との相関計算を一定時間毎にサンプリングされる画像に対して繰り返し計算し、この変化を記録して得られる相関値の時間変化パターンをもとに小領域ごとに変化の有無を判定する方法である²⁾。本システムではこの手法により画像上の変化を検出する。各小領域での相関計算には屋外での明るさ変化を考慮して、次式に示す正規化相関を用いた。

$$M(i, j) = \frac{\sum_{k=1}^K \sum_{l=1}^L P(i+k, j+l) \cdot Q(i+k, j+l)}{\sqrt{\sum_{k=1}^K \sum_{l=1}^L P(i+k, j+l)^2} \sqrt{\sum_{k=1}^K \sum_{l=1}^L Q(i+k, j+l)^2}} \dots (1)$$

$M(i, j)$: 相関値
 $P(k, l)$: 背景画像の画素(k, l)の輝度値
 $Q(k, l)$: 現在画像の画素(k, l)の輝度値

Fig.8 は、ある小領域について背景画像との相関値を計算した結果の時間変化(図の実線)と、小領域内各画素の輝度の二乗平均平方根(図の点線)の時間変化をグラフにしたものである。相関値の時間変化は次の3つの区間に大分される。A区間:相関値の変動が大きく

小領域上に動きがある、B区間:相関値が1に近く変動も少ないため小領域は背景と変わらない、C区間:相関値の変動が小さいが相関値自体が小さく小領域上に静止障害物がある。本システムでは不審者を検出するため、A, C区間に当る時間相関変化を持つ小領域を変化の存在する点(これを「変化点」と呼ぶ)として検出、さらに、隣合う変化点を連結し、塊として抽出して、この塊を監視画像内に存在する不審者として検出した。

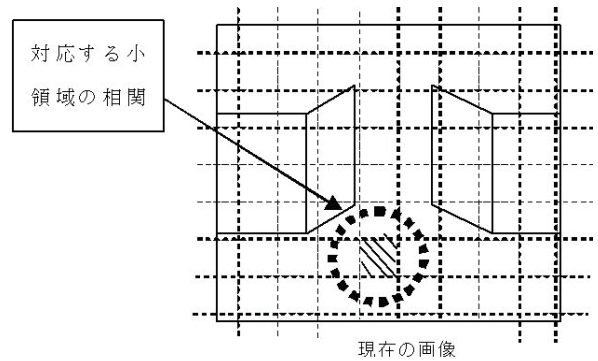


Fig.7: Segmented local windows of the camera image

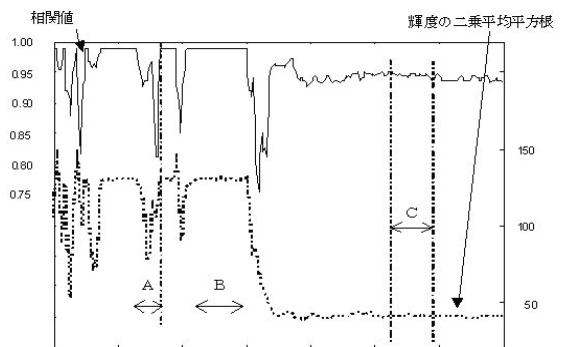


Fig.8: Fluctuations of time correlations of one window

5. 屋外監視カメラ画像による侵入検知実験

侵入検知システムにより、屋外監視カメラの画像から侵入者を検知した事例を紹介する。

Fig.9 は約15[m]の高さに設置された監視カメラから施設内の通路を見下ろした画像から通行者を検知した例である。施設内の広い区域を監視する場合は、この程度の高さに監視カメラが設置されることが多い。この例では、画像上において手前から1/3付近の通路を横切るように侵入禁止線を設置し、手前側を侵入側に、奥側を接近側に設定した。Fig10 は高感度の監視カメラにより夜間の施設内の広場を見下ろした画像から不審者を検知した例である。監視システムにおいて夜間の監視は重要である。夜間監視に用いられるカメラとしては赤外線カメラ、および高感度カメラがあるが、今回は高感度カメラの画像を用いた。



Fig.9: Example of detection at an avenue

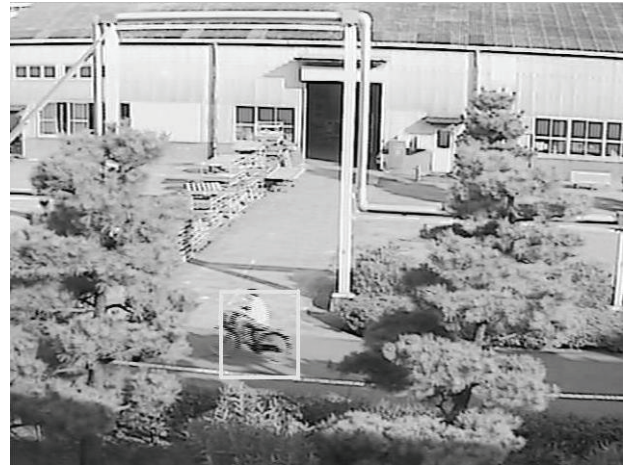


Fig.11: Example of a output by detection system



Fig.10: Example of detection at a park in night

侵入検知システムの性能を評価するため、監視カメラの画像を目視検査した結果と、侵入検知システムが検知出力を発生した結果との比較を行った。侵入検知システムの検知出力例を Fig.11 に示す。これは、約10[m]の高さに設置された監視カメラから施設内の通路を撮影したもので、監視範囲内に監視する通路と共に、並木や低木が入っている。また、監視している通路には、人物はもちろん自転車、自動車、フォークリフトといった様々な通過物が存在する。検知結果を Table.1 に示す。今回の実験結果では、全体で94件の通過物が発生し、この内91件を侵入検知システムにより自動検知することができた。検知率としては97%と高い検知率を達成した。未検知となった通過物は高速で通り過ぎる自転車2件と自動車1件であった。今回の実験では通路手前に大きな並木が2本立っており、通過物の見える範囲が短いことが未検知の大きな要因と考えられる。また、並木や低木が風で揺れる、朝夕の急激な日照変化等の環境変化が昼夜を通して発生した。これらの環境変化に対しては、低木の揺れへの検知出力1件であった。これらの結果から、侵入検知システムの高い検知率と耐環境性が確認できた。

Table.1: Experimental result of detection

項目	目視	侵入検知	検知率
人	52	52	100%
自転車	25	23	92%
車	11	10	91%
トラック	3	3	100%
フォークリフト	3	3	100%
計	94	91	97%

6. まとめ

上水道施設等ライフラインへのセキュリティの一環として導入が期待される、画像解析型侵入検知システムを紹介した。このシステムは、監視カメラの画像を処理し、職員の代わりにIT機器で侵入者等を自動検知するシステムである。本稿では、画像解析型侵入検知システムの構成、検知方法について説明した。また、各種監視カメラへ侵入検知システムを適用した事例、および、目視検査と侵入検知システムの検知出力との比較による性能評価試験結果を示した。本システムは昼夜を問わず高い検知率と耐環境性を有し、屋外監視に適したものとなっている。

[参考文献]

- 1) 増田：セキュリティサービスにおける認識・理解技術への期待, 電子情報通信学会技術報告書 PRMU 97-54, pp49-55, 1997
- 2) 庭川, 藤原, 恩田：監視カメラ映像から抽出する動きベクトルと局所領域時間相関変化を用いた通用門の出入状況監視, 電気学会 C 部門誌, Vol.123, No.7, pp1292-1297, 2003
- 3) 秋元：受変電設備に於ける画像中継配信システムの応用－現場状況ライブ配信と遠隔指揮－, 平成 15 年電気学会放電・開閉保護・高電圧合同研究会資料, ED-03-202, SP-03-124, HV-03-117, pp111-114, 2003