低コスト住宅向け画像監視システム

Low-cost image monitoring system for home security

○ 丸山　哲裕，服部　公央亮，田口　亮，梅崎　太造(名工大)，保黒　政大(中部大)

Tetsuhiro MARUYAMA, Kosuke HATTORI, Ryo TAGUCHI, Taizo UMEZAKI, Nagoya Institute of Technology
Masahiro HOGURO, Chubu University

Key Words: Security, Image Processing, Low-cost

1. まえがき

近年，住宅等への侵入犯罪の増加[(1)]に伴い，警備サービス業者と契約して自宅のセキュリティを強化する人が増加している．しかしながら，監視カメラ等の機器を購入する初期費用や月々の利用料に高いコストが必要であり，一般家庭において容易に導入することは困難である．

そこで，本研究では画像処理により動体を検知し，WEBを介して検知情報を記載したメールを携帯電話へ送信する，安価な自己管理型セキュリティシステムの構築を提案する．PC，携帯電話，WEBカメラといった一般家庭が所有する，あるいは安価な機器を利用することで初期費用を抑える．さらに，画像処理による侵入者の自動検出により人件費をなくし，安価な利用料を実現する．侵入者の自動検出には差分処理および時系列処理により追跡する手法が多く提案されている[(2)(3)]．パターン認識による人検出技術を用いた手法も盛んに研究されているが[(4)(5)]，計算量のコストが大きい，学習パターンに依存するなどの短所もある．本システムはあらゆる住宅環境を対象とし，一般的スペックのPCでリアルタイムに動作することを目指すため，主に差分処理を用いて動体を検出する．

2. システム概要

本システムのサービス全体の概要をFig.1に示す．

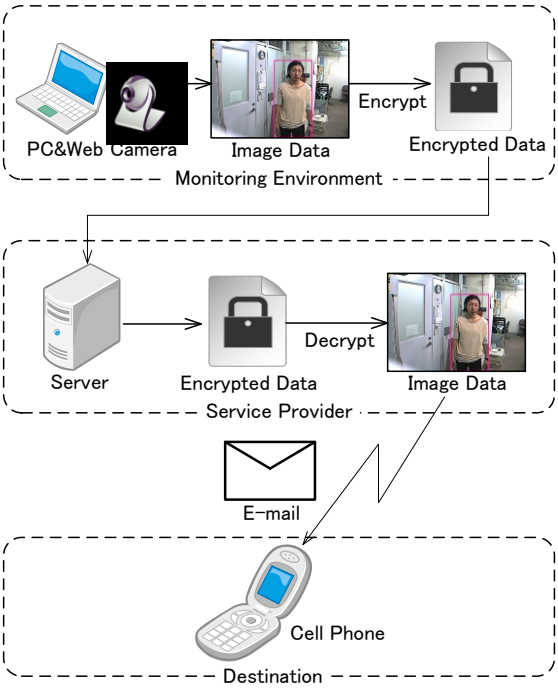


Fig.1　System outline

自宅に設置したWEBカメラから画像を取得し，画像処理により動体を検出する．侵入を検知した際にはメールにより外出先のユーザーへ通知する．メールには画像データを添付して自宅の状態を確認できるようにする．

メールを送信する際は，サービス事業者が運用しているサーバーを介してユーザーへ送信すると同時に，サーバーへ検知ログを保存する．これにより，ユーザーは専用のWEBページにて過去の検知ログを閲覧することが可能となる．画像データはプライバシー情報を含むため暗号化を施しサーバーへ送信し，またサーバーに保存する際も暗号化されたデータを保存する．

3. 動体検出処理

本研究では，一般家庭におけるPCの処理性能を考慮し，比較的計算量の少ない処理により動体を検出する．

3-1 初期背景生成

背景差分法で動体を検出するためには，背景を生成する必要がある．背景生成のために，まず式(1)により時刻 t におけるサイズNの画像 I_t よりフレーム間差分 d_t を得る．さらに式(2)によりフレーム間差分パワー P_t を求める．

$$d_t = |I_t - I_{t-1}| \tag{1}$$

$$P_t = 10\log_{10}\left(\frac{1}{N}\sum_{n=0}^{N} d_t(n)^2\right) \tag{2}$$

フレーム間差分パワー P_t を式(3)により閾値処理し，背景か否かを判定する．

$$Q_t = \begin{cases} 1, P_t \geq Th_p \\ 0, P_t < Th_p \end{cases} \tag{3}$$

ここで，Fig.2のように撮影環境により外乱の影響度合いが異なるために，動体が存在しない状況における P_t の値(オフセット)に差異があるため固定閾値で判定することは困難である．そこで，P_t の時系列情報を元にオフセットを求めて P_t より除去することを考える．

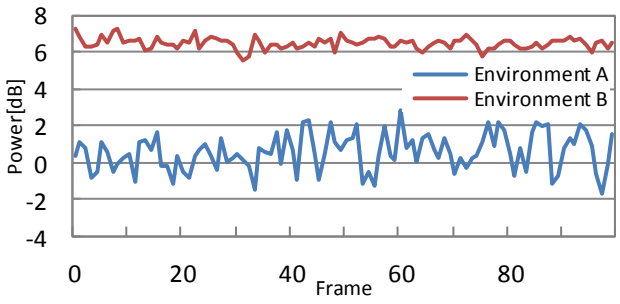


Fig.2　Power of frame difference in each environment

過去 M フレームにおける差分パワーの平均値 A_t との二乗誤差 E_t を式(4)，(5)により求める．二乗誤差 E_t が閾値以下のとき， A_t をオフセットとする．

$$A_t = \frac{1}{M}\sum_{m=0}^{M-1} P_{(t-m)} \tag{4}$$

$$E_t = \frac{1}{M}\sum_{m=0}^{M-1} \left(A_t - P_{(t-m)}\right)^2 \tag{5}$$

P_t からオフセットを除去したパワー P_t' を式(6)により求めて閾値処理により判定する． P_t' を Fig.3 に示す．

$$P_t' = P_t - A_t \tag{6}$$

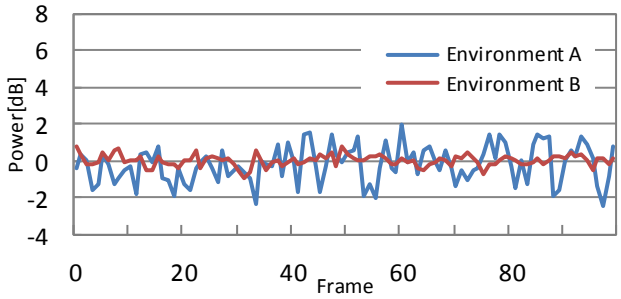


Fig.3　Offset removed from power of frame difference

背景と判定された画像 I_l を背景リストに追加し， L 枚取得したとき，式(7)により平均背景 I_B を生成する．

$$I_B = \frac{1}{L}\sum_{l=1}^{L} I_l \tag{7}$$

I_B を背景として背景差分法による動体領域検出を行う．

3-2 動体領域検出

動体領域を検出するために，まず式(8)により背景差分 D_t を得る．

$$D_t = \left| I_B - I_t \right| \tag{8}$$

D_t に対して $U \times V$ [pixel]の窓 W をシフト幅 s で走査し，窓内の水平方向，垂直方向それぞれの平均濃淡値 a_{Hor} ， a_{ver} を式(9)，(10)により求める(Fig.4)．

Fig.4　Candidate regions detection

$$a_{Hor}(h) = \frac{1}{U}\sum_{i=0}^{U} W(i,h) \tag{9}$$

$$a_{Ver}(w) = \frac{1}{V}\sum_{i=0}^{V} W(w,i) \tag{10}$$

平均濃淡値が閾値を越える範囲を動体候補領域とする．得られた候補領域 S における背景画像と現フレームとの類似度 R_{NCC} を式(11)により求める．

$$R_{NCC} = \frac{\sum_{i\in S}\sum_{j\in S} I_B(i,j) I_t(i,j)}{\sqrt{\sum_{i\in S}\sum_{j\in S} I_B(i,j)^2 + \sum_{i\in S}\sum_{j\in S} I_t(i,j)^2}} \tag{11}$$

軽度の照明変動等が生じた場合と動体が進入した場合を比較すると前者の方が類似度 R_{NCC} は高くなる．そのため閾値を下回った候補領域は削除することで照明変動等により発生した誤検出の削減を図る．

残った候補領域のうち重なりあった領域を統合することで最終的な検出領域とする．Fig.5 に動体検出処理のフローを示す．

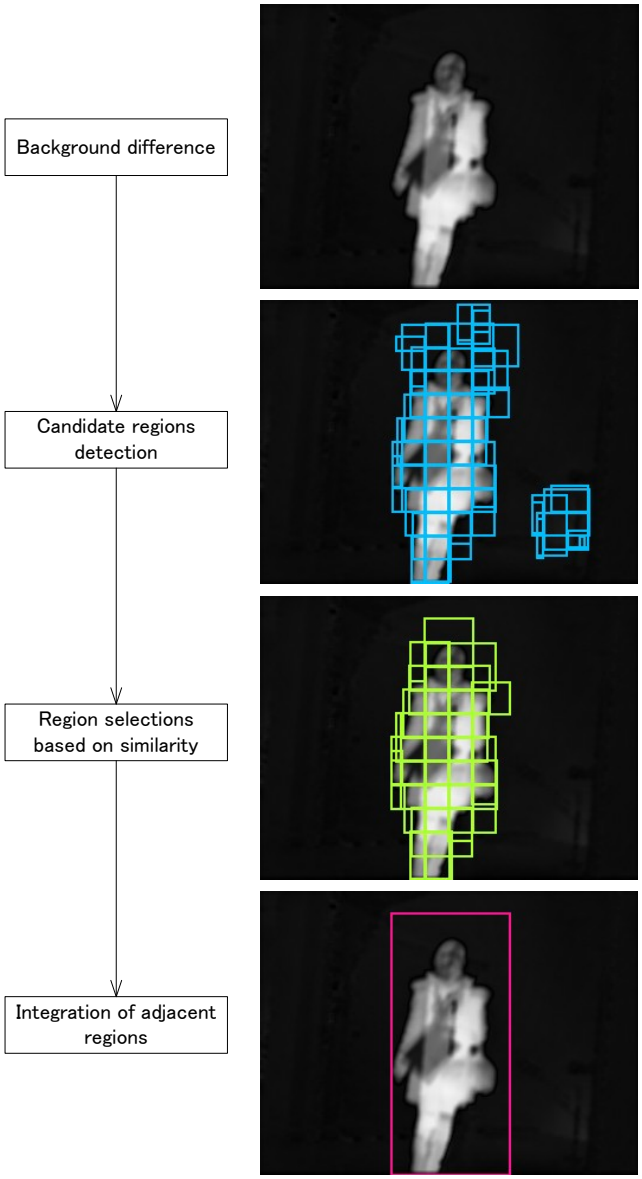


Fig.5　Motion regions detection flow

3-3 背景更新

経時変化や新たな静止物体の進入などが発生することで背景変化が生じる可能性がある．そのため背景を更新する必要がある．

背景は3-1節でも用いた過去 M フレームにおけるフレーム間差分パワーの二乗誤差 E_t が閾値以下のときに式(12)のように更新する．

$$I_B = (1-\alpha)I_B + \alpha I_t \qquad (12)$$

α は重みであり，ここでは 0.1 と設定した．

4. 画像送信タイミング

本システムでは 3 章に示した処理により動体を検出するが，一般に動体は連続した数フレームで検出されるため，そのすべてを送信するのは連続して大量のメールを受信することとなり煩わしい．そのため，連続して検出されたときはそのうち 1 枚の画像を送信することとする．連続した検出区間の最初のフレームには動体の一部のみが映っている場合が多いため，送信する画像としては不適当である．そのため，検出開始から T フレーム目を送信するものとする(ただし，検出区間が T フレーム以上のとき)．T の値は主観実験により 5 フレーム目と決定した(Fig.6)．

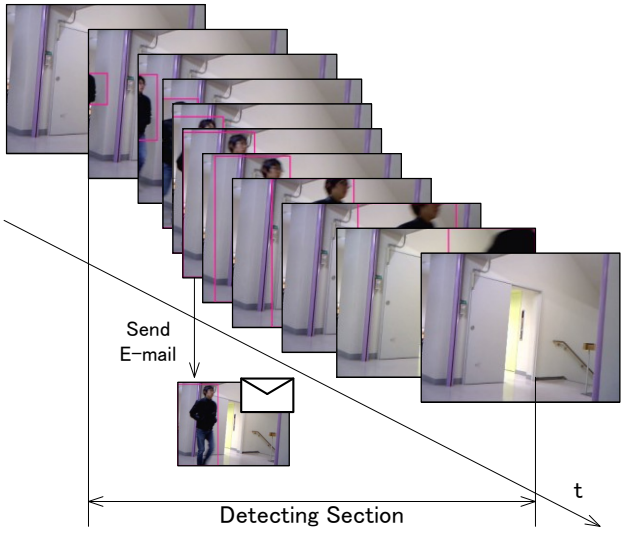


Fig.6　Selection of image to send

5. 情報セキュリティ

本システムは通信を用いるため，ユーザーの個人情報が外部に漏出しないように設計する必要がある．本システムではログイン時における通信と動体検知時の画像データ送信の 2 箇所で通信を行う．

5-1 ログイン時

本システムではログイン時に，ユーザー認証と鍵生成を行う．Fig.7 にそのフローを示す．

まず，ユーザー認証について説明する．本システムでは，利用する際にユーザー登録を必要とすることを想定する．

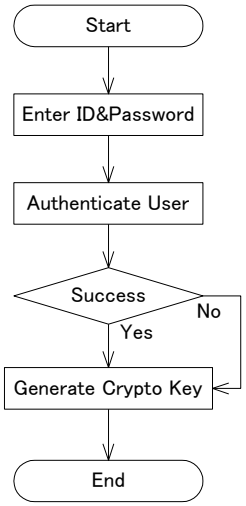


Fig.7　Login flow

また，それに伴いシステムの利用時にはユーザー認証が求められる．認証にはパスワードを必要とするが，認証における通信時にパスワードが外部へ漏洩することを防ぐ必要があるため，チャレンジ/レスポンス方式を認証に用いる(Fig.8)．これにより，外部へパスワードが漏洩することなく，セキュアに認証することが可能である．

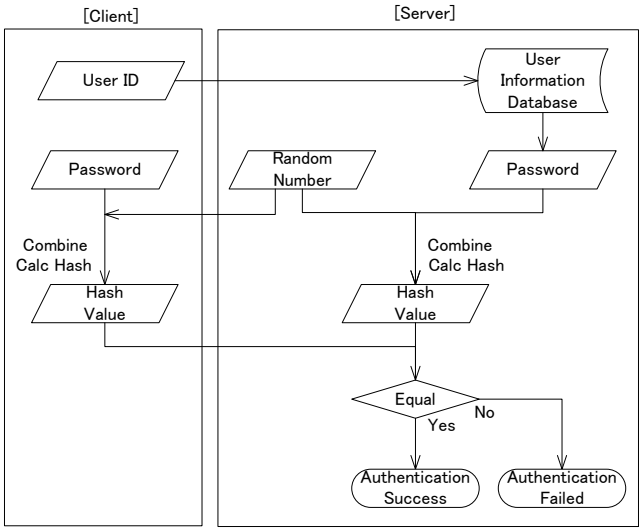


Fig.8　Challege/Response authentication

次に鍵生成について説明する．ログイン時には後述する画像データ送信時に用いる暗号鍵を生成する必要がある．本システムでは共通鍵による暗号化を行うため，Diffie-Hellman の鍵交換アルゴリズムを用いることで，外部に漏洩することなく共通鍵をユーザーとサーバーで共有することができる(Fig.9)．

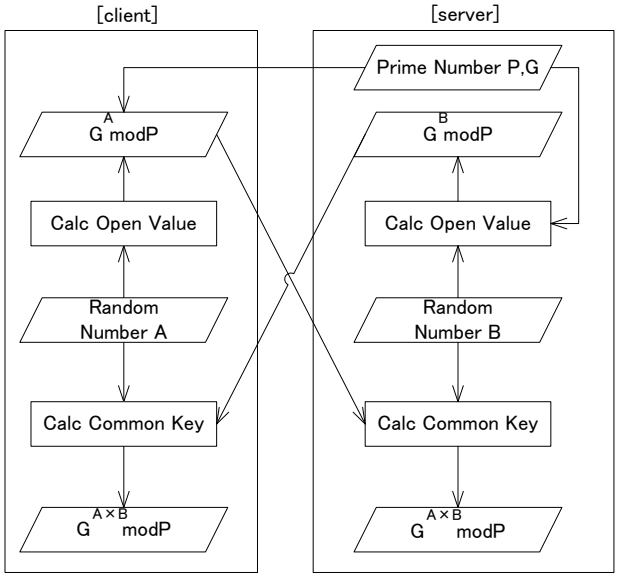


Fig.9　Diffie-Hellman key exchange

5-2 画像データ送信時

動体を検知した際，そのとき得られる画像データをサーバーへ送信する．このとき，画像データはプライバシーに関わる情報を含む可能性が高い．通信中において，第三者によってデータが盗聴されるのを防ぐため，本システムでは画像データを暗号化する．暗号化には対称暗号方式の 1

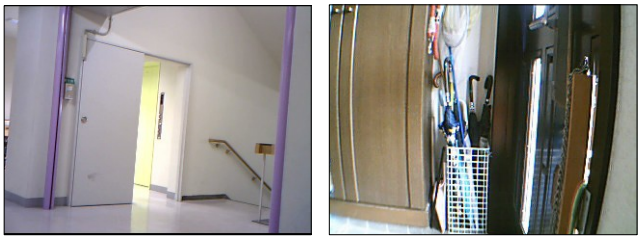
つである AES を用い, 暗号鍵にはログイン時に作成した共通鍵を用いる.

6. 評価実験

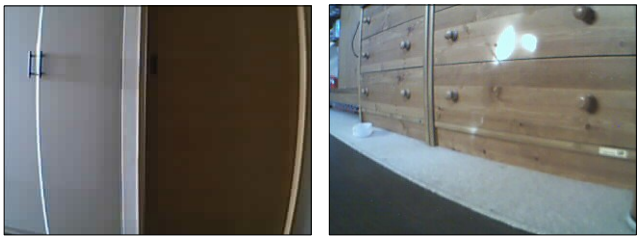
本システムの検出精度とユーザビリティについて評価実験を行った.

6-1 検出処理の精度評価

動体検出処理の精度を検証した. 実験対象は Fig.10 に示す 4 環境におけるカメラ映像である. 目視により動体が存在するシーンを決定し, 検出されたシーンとの比較により性能を評価する. 各実験データの録画時間と動体存在シーン数を Table 1 に示す.



(a) Environment A (b) Environment B



(c) Environment C (d) Environment D

Fig.10 Recording environments

Table 1 Video details

Environment	Time	Motion scene number
A	12 [min]	33
B	24 [h]	91
C	25 [h]	3
D	25 [h]	38

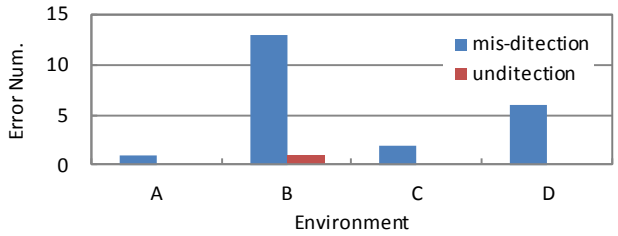


Fig.11 Detection process errors

各データの誤検出数, 未検出数を Fig.11 に示す. 未検出はほぼ発生せず, ほとんどの動体存在シーンを検出することができた. しかしながら, いくつかのシーンで誤検出が発生した. 日出時や, 日光の照射角度の変化に伴なう窓や戸などからの光の差し込み等により急激な輝度変化が生じる場合に多くの誤検出が発生していることを確認した. なお, 実験データには在宅時に撮影したものもあり, 室内灯の点消灯時に検出が発生したが, 不在時の住宅においては侵入者の存在なしにはあり得ないため検出成功とした. 今後, テクスチャの比較, 平均輝度を用いた画像全体の輝度正規化などにより検出精度の改善を目指す.

6-2 ユーザビリティの評価

本システムの操作性, 機能性について 15 名の被験者に対するアンケートを行い, 主観評価を調査した. “かなり悪い”, “悪い”, “やや悪い”, “普通”, “やや良い”, “良い”, “かなり良い” の 7 段階で評価する. 得られた評価結果を集計し, 系列カテゴリー法により解析することで, 順位尺度から正規化された 0～6 (悪～良)の比率尺度に変換する. 解析結果を Table 2 に示す.

Table 2 Subjective assessment of system

Genre	Item	Evaluation
Operativeness	Login	5.4
	Sarting detection	5.4
	Option settings	5.2
	Log viewer for PC	5.4
	Log viewer for cell phone	4.4
Functionality	Option Settings	5.2
	Log viewer for PC	5.6
	Log viewer for cell phone	4.4

評価の低い項目として操作性, 機能性ともに携帯電話用ログ閲覧ページとオプション設定が挙げられる. 携帯電話用ログ閲覧ページは簡易的なものであるため, 操作性, 機能性ともに低評価であると考えられる. オプション設定については設定画面がやや煩雑でわかりにくいために操作性に, その他に設定したい項目があるために機能性に低い評価がなされたものと考えている. 今後, より直感的に操作可能なインターフェースの提供により改善を目指す.

7. まとめ

不在時の住宅における動体を検知し, WEB を介して携帯電話へ通知するシステムを開発した. 現状としていくつかのシーンで誤検出が発生するため, 今後検出処理について改善を図る必要がある. また, あらゆる住宅環境で高精度な検出を実現するために, より多くの環境における実験を行っていく. 被験者を対象に, それぞれの環境における本システムの評価を調査した結果, 全体的に良い評価を得られたが, 十分な評価が得られていない項目も存在し, 多機能化を進めるとともに, より直感的なインターフェースを提供することで操作性についても今後改善していく.

参考文献

(1) 警察庁統計, “平成 19 年の犯罪情勢”.
(2) 島田 竜也, 柳下 達也, 河口 尚広, 熊谷 拓哉, 内藤 恵介, 山田 博三, 森 晃徳, “屋内侵入者検知システムの開発”, 信学技報. PRMU, vol.102, No.531, pp.87-92, 2002.
(3) 羽下 哲司, 八木 康史, “時空間動き特徴に着目した屋外侵入者監視技術に関する研究”, 情報処理学会研究報告. CVIM, Vol.2006, No.51, pp.259-274, 2006.
(4) 舘俊太, 武藤佳恭, “3 層ニューラルネットワークと変形テンプレート法による動画像の人物検出”, 情報処理学会論文誌. 数理モデル化と応用, Vol.44, No.SIG_14, pp. 48-56, 2003.
(5) 山内悠嗣, 藤吉弘亘, 山下隆義, “Boosting に基づく特徴量の共起表現による人検出”, 第 11 回画像の認識・理解シンポジウム(MIRU2008), pp. 180-187, 2008.