プライバシー保護機能付き監視カメラシステムの真正性証明とデータ量削減手法

藪田　顕一†　　北澤　仁志†
†東京農工大学大学院工学府

1　まえがき

犯罪の抑止や遠隔地の状況把握のために，監視カメラが多数用いられている．しかし，監視カメラは監視不要な人物なども撮影してしまうため，画像の拡散などによるプライバシーの侵害という問題を抱えている．

筆者らはRSA公開鍵暗号方式を応用し，プライバシー保護と真正性証明機能を兼ね備えた固定カメラによる監視システム[1]を提案した．この手法では，1)移動物体に画像処理を施して識別を不可能にする，2)復元情報を電子透かしで埋め込む，3)撮影画像と復元画像間に，人が検知できる変化がないことを移動物体を復元せずに示し真正性を証明する，ことができる．

本報告では，復元情報をハフマン符号化の特徴に基づいて埋め込む手法を説明し，ファイルサイズを増加させずに真正性証明が可能であることを示す．

2　プライバシー保護と真正性証明機能を兼ね備えた監視システム

まず，プライバシー保護と真正性証明機能を兼ね備えた監視システムの概要を説明する．

図1は監視システムのフローである．まず，監視カメラにより撮影した画像を入力する．入力画像には，輝度のAC成分の最下位ビットを0にする前処理を施す．入力された画像から移動物体の抽出を行い，抽出された移動物体領域にプライバシ保護のための画像処理を行う．この画像処理をmasking，maskingされた画像をmasked imageと呼ぶ．本手法では，maskingには単一色による塗りつぶしを用いた．

また，RSA暗号と電子署名を応用して，撮影画像から復元用のデータと真正性検証用のデータを作成する．真正性検証用のデータは撮影画像を公開鍵で暗号化したストリームから得られるハッシュ値を，秘密鍵で暗号化したものである．これらのデータを電子透かしによりmasked imageに埋め込み出力する．

3　電子透かしによる復元データの埋め込み

本手法では，JPEG規定のAnnex Kによる標準テーブルのハフマン符号化の特徴に基づいた，符号量の変化を抑えた埋め込みを行う．ハフマン符号化された入力値は，(入力値とゼロランレングスにより決まるハフマン符合) + (付加ビット) の形で出力される．ハフマン符号が同一のグループ内であれば，入力値を変えても出力符号長は変わらない．そこで，輝度のAC成分を入力値(ac)により，$|ac| \geq 2$のグループと$|ac| \leq 1$のグループに分け，$|ac| \geq 2$のグループへ優先的に埋め込みを行う．式(1)は入力値acと埋め込みビットb，電子透かし後の係数$ac_{(w)}$の関係を表した式である．$sign$は入力値の正負を示す．

$$ac_{(w)} = sign \times \left(2\left\lfloor \frac{|ac|}{2} \right\rfloor + b\right) \quad (1)$$

埋め込み位置が不足する場合は$|ac| \leq 1$のグループへ埋め込む．このグループへの埋め込みはハフマン符号が変化するため，出力符号長が変化する．

4　復元画像の真正性検証

復元画像が，撮影画像を改竄したものでないことは次の6ステップで証明できる．1)masked imageから復元用データと真正性検証用データを抜き出す．2)真正性検証用データから，公開鍵を用いて，ハッシュ値を復号する．3)masked imageを公開鍵で暗号化する．4)復元用データを用いて，3のデータから撮影画像を暗号化したストリームを復元する．5)4のストリームからハッシュ値を計算する．6)2と5の手順で求めたハッシュ値の一致を検証する．ハッシュ値が一致すれば復元画像は真性である．

5　データ量増加を抑えた埋め込み実行例

図2は，プライバシー保護と復元の実行例である．図2(a)は監視カメラによる撮影画像，図2(b)は輝度のAC成分の最下位ビットを0とした画像である．2つの画像間にはPSNR=46.9[dB]と高い類似性がある．図2(c)はプライバシーを保護した画像である．図2(d)の復元画像は，(b)の画像と全く同一の画像に復元できている．

図3は，撮影画像(640×480[pixel])中に存在する移動物体の面積と，masking，電子透かしにより増減するデータサイズの関係を示したものである．maskingに単一色による塗りつぶしを用いているため，maskingされた領域ではJPEG圧縮効率が高くなる．そのため，移動物体のサイズが大きくなるに伴ってmaskingによる符号長削減効果が高くなる．一方，移動物体が大きくなると，復元データのサイズが増加するため，電子透かしによる符号長の増加が顕著になる．単一色での塗りつぶしによる減少に比べて，電子透かしによる増加の方が急峻であり，移動物体が35000[pixel]を超えるとすべての画像で電子透かしによる増分が上回る．また，本手法では，埋め込みデータのビット数が，masked imageの$|ac| \geq 2$となるAC成分より少ない場合には，

A Method of Data Reduction and Image Authentication for A Security and Privacy Protection Camera System
†Kenichi YABUTA　†Hitoshi KITAZAWA
†Department of Electrical and Electronic Engineering, Tokyo University of Agriculture and Technology

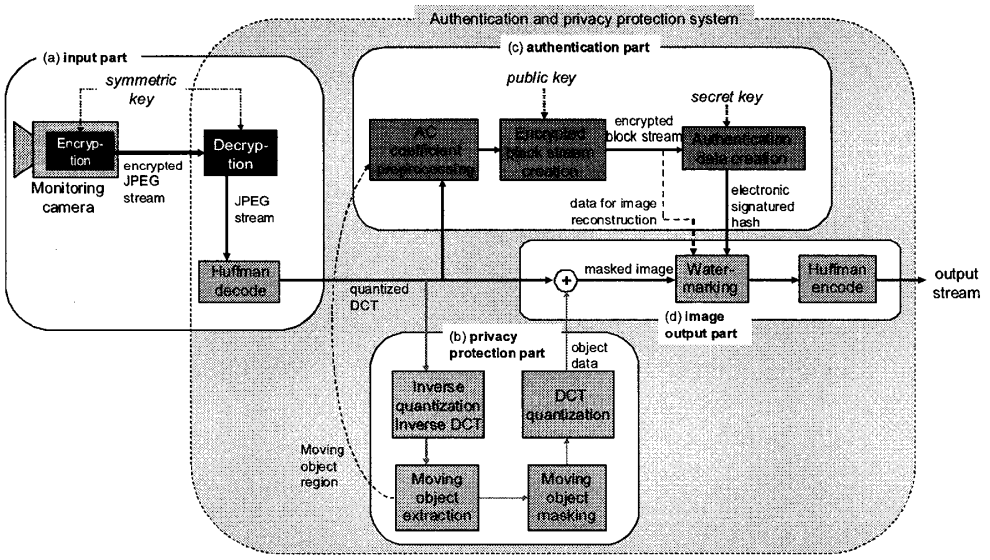

図 1: システムフロー

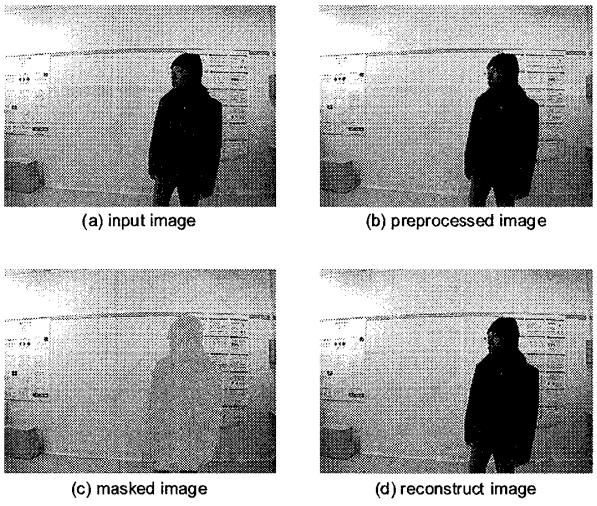

図 2: プライバシー保護と復元の実行例

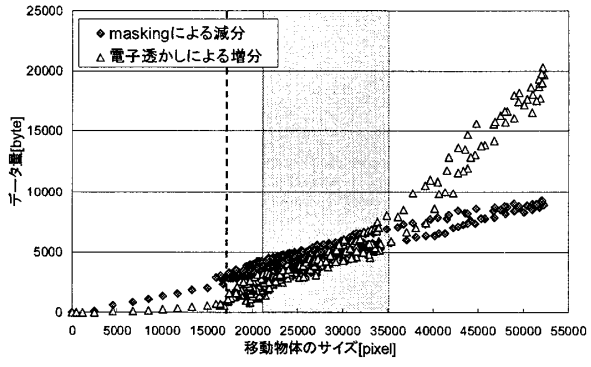

図 3: 移動物体の大きさと masking による減分，および電子透かしによる増分

出力データ量は増加しない．そのため，17000[pixel] 程度までは，電子透かしによる増加はほとんどない．

図 4 は，電子透かしに利用する係数位置の選択方法による，出力データ量の違いを示したものである．横軸は入力のデータ量，縦軸は出力のデータ量を示している．係数の選択方法は，$|ac| \geq 2$ となる係数を優先して用いる提案手法，係数位置を固定する方法，ランダムに選択する方法の 3 種を用いた．図中の破線の下側にプロットされた点は，入力データより出力データが小さいことを示している．提案手法は多くの画像でデータ量を削減出来ている．

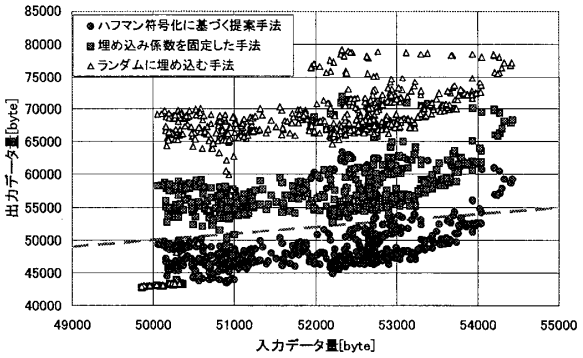

図 4: 電子透かし位置選択方法による比較

6 むすび

本報告では，プライバシー保護機能付き監視カメラシステムの真正性証明とデータ量削減手法を提案した．RSA 公開鍵暗号方式と電子署名を応用することで，プライバシー保護と真正性証明を両立した．また，ハフマン符号化の特徴に基づく電子透かしを用いて復元用データを埋め込んだことで，画面 1 割程度の移動物体であれば符号長が増加しない効果が得られた．

参考文献

[1] 藪田顕一, 北澤仁志. 真正性証明とプライバシ保護を両立する監視カメラシステム. 画像電子学会誌, Vol. 38, No. 5, pp. 694–702, Sep. 2009.