博士論文

監視カメラシステムにおける プライバシー保護の実現手法および システム構築手法の研究

A Study on Privacy Protection and Optimal Design for Monitoring Camera System

指導教官　北澤 仁志 教授

東京農工大学大学院 工学府
電子情報工学専攻

藪田 顕一

要旨

防犯や犯罪捜査，遠隔地の状況把握などを目的とした監視用カメラの設置は不可欠になっており，ますますその需要が増大していく傾向にある．カメラ撮影画像に対する研究は，行動識別や特徴分析などの画像解析，交通監視やマーケティングへの応用などが盛んである．それに比べ，撮影画像中の人物へのプライバシー保護や，監視カメラシステムの構築を対象とした研究はあまり報告が無い．報告数は少ないが，社会の安心安全を実現するために，欠かすことのできない重要な分野である．本論文では，撮影画像中に映りこんだ人物へのプライバシー保護，プライバシーを保護した画像が改竄されていないことの証明，最小のカメラ台数によって監視対象の空間を観測できる監視カメラ配置の最適化，という 3 点の研究テーマについて報告する．

まず，監視カメラにおけるプライバシー保護を実現する手法を提案する．監視カメラにおけるプライバシー保護は，移動物体を不可視化することと，移動物体の行動が判別できることを同時に満たすこととする．この定義に基づき，次の 3 点を満たす手法を提案する．(1) 撮影画像中の移動物体に適切な画像処理を施し特定を不可能にする．(2) オリジナルの移動物体は，暗号化により保護し，電子透かしにより JPEG 圧縮された出力画像に埋め込む．(3) 撮影時点までのフレームを用いてすべての処理を行う．提案手法を適用し出力した監視カメラ画像は，通常の JPEG ビューアを用いて閲覧すると移動物体領域が不可視化されている．そのため，撮影された人物のプライバシーが保護できる．一方，犯罪捜査や追跡などの用途では，特殊なビューアを使って，出力画像に埋め込まれたデータを抜き出し，復号して，オリジナルの移動物体を見ることができる．提案手法を実現するためのエンコーダとデコーダの構成方法を述べる．さらに，実験によりプライバシー保護と移動物体の特定が両立できることを示す．

次に，プライバシーを保護した画像の真正性を保障する手法を提案する．カメラにより撮影された人物のプライバシーを画像の不可視化により保護し，被写体の特定が必要な際にオリジナルの移動物体を復元する手法を提案した．ところが，復元画像の証拠能力は乏しいため，復元画像の真正性を証明できる方法が必要である．そこで，RSA 公開鍵暗号方式と電子署名を応用して，復元画像の真正性証明が可能な手法を提案する．撮影画像へ

の復元を必要とせず，また，不可視化のための画像処理により真正性が失われることがないため，真正性証明とプライバシー保護を両立できる．また，撮影画像の再構成に必要な暗号化データを，ハフマン符号化の特性を利用した電子透かしを用いて出力画像に埋め込むことで，ファイルサイズの増加が抑えられる．実験により，提案手法が，プライバシーが画像処理により保護できること，またそのときに画像の真正性が証明できること，出力データ量の増加を抑えていることを示す．

さらに，あるシーンから移動物体のフロー（シーン内の物体の移動経路）を，最小台数のカメラで検出するための，カメラの位置や向きと，視野角などのカメラ仕様を求める手法について述べる．移動物体のフロー解析は交通監視等に有用であるが，フロー検出のために観測空間全域を観測しようとすると，多数のカメラが必要になり，また，カメラ配置を求めるのに非常に時間がかかる．そこで，あらかじめフローの特定に必要な観測エリアを求め，カメラ台数と実行時間を削減する必要がある．まず，観測空間から出入り口，通路，分岐点，袋小路により構成されるグラフ構造を定める．次に，フローは観測空間の出入り口と，通路の少なくとも一端にある分岐点を観測することで特定できることを利用し，観測エリアを求める．次に，この観測エリアをカバーする最小台数のカメラ配置を集合被覆により求める．これにより，最小台数でフローを検出できるカメラ配置を求めることができる．実在のシーンをモデルとしたデータでの実験により，本手法が実行時間とカメラ台数の両面から，監視カメラシステムの構築に有効であることを示す．

目次

第 1 章

序論

防犯や犯罪捜査，遠隔地の状況把握などを目的とした監視用カメラの設置は不可欠になっており，ますますその需要が増大していく傾向にある．警視庁は，繁華街の防犯対策として，平成 14 年 2 月に新宿区歌舞伎町地区で「街頭防犯カメラシステム」の運用を開始し，これを皮切りに渋谷区宇田川町地区（平成 16 年 3 月運用開始），豊島区池袋地区（平成 16 年 3 月運用開始），台東区上野 2 丁目地区（平成 18 年 2 月運用開始），港区六本木地区（平成 19 年 3 月運用開始）と，導入の拡大を続けている [1]．これらの街頭防犯カメラシステムの導入地区では，犯罪認知件数の推移に減少傾向が見られ，監視カメラの設置が犯罪抑止に効果的であることを示している（114 ページ参考資料内，表 6.1 参照）．また，平成 21 年 1〜6 月までの間に 110 件の撮影データが警察署長に提出され，うち 63 件が事件の証拠資料として用いられるなど，犯罪の抑止のみならず，犯罪捜査への有用性も高い．警察庁だけでなく，各自治体や企業などによる監視カメラの設置も多く，日常生活において，街角や駐車場，店舗内，マンション内など，屋内外を問わず様々な環境で監視カメラを目にすることが多い．さらに，監視カメラの設置拡大は国内だけに見られる傾向ではなく，世界的にもその動きが伺える．監視カメラ大国とも呼ばれる世界有数の監視カメラ設置国のイギリスで，平成 18 年 9 月に国内の監視カメラに関する調査資料が報告された [2]．資料によると，イギリス国内には約 420 万台ものカメラが設置されており，1 人あたり 1 日平均 300 回は監視カメラに撮影されている，と報告されている．このような生活安全の確保を目的とした監視カメラの設置のみならず，観光地の様子をリアルタイムに眺める，現在の天気や道路状況を知る，などを目的とした市販のネットワークカメラを活用したライブカメラも数多く存在する．これらは WEB を通じて簡単に世界中の様々な場所の映像を得ることができる．ウェブカメラは，個人で設置することも容易であり，また，広帯域通信サービスの普及により動画像の通信が容易になったことなどもあり，非常に多くのライブカメラ映像がネットワーク上に存在する．

このように，様々な環境を映すカメラが多数存在することから，カメラにより撮影した

画像を対象とした，行動識別や特徴分析などの画像解析の研究や，交通監視やマーケティングに応用する研究などが盛んに行われ，報告も多く見受けられる．それらの研究に比べ，監視カメラシステムをどのように構築，運用するかといった研究はあまり報告が見当たらない．報告数は少ないが，プライバシーの侵害や管理，設置コストの削減などといった課題がある重要な分野であり，社会の安心安全を実現するためには，これらの研究も欠かすことができない．本論文では，撮影画像中に映りこんだ人物のプライバシー保護の実現，撮影画像のプライバシー保護と真正性証明の両立，最小のカメラ台数によって観測空間中の移動物体のフローを検出できる監視カメラ配置の最適化という 3 点の研究テーマから，監視カメラシステムの構築と運用について寄与することを目的とする．

■監視カメラ撮影画像におけるプライバシー保護の実現

監視カメラによって撮影された画像中には，監視対象となる人物や車などが映り，犯罪捜査などへ活用されている．その一方で，監視カメラは犯罪には無関係であったり，ただ通り過ぎるのみであったりといった監視や観測が不要な人物や物体も数多く撮影する．また，撮影画像中に映りこんだ人物にとって，自分たちが撮影された画像がどのように扱われるかが不明瞭である．一般的な監視カメラの運用では，撮影画像が監視カメラから画像蓄積サーバに送られ，一定期間保存されるシステムがよく見受けられるが，撮影画像がどの程度の期間保存されるのか，外部への情報漏えいへの対策がどのようになされているか，などといった懸念も生ずる．さらに，撮影画像がどのような場合に開示されるのか，開示されたときにどのような人物が閲覧するのか，といった点も明確に把握できない．つまり，本来なら監視下に置かれる必要のない人物が，いつの間にか監視され，また，自らの知らないうちにその情報が活用される，さらには，自らに落ち度がなくても自身の映った画像が広く流出するなどといった可能性にさらされているといえる．平成 15 年に「個人情報保護法」と通称される「個人情報の保護に関する法律」が施行されたことによる影響もあり，プライバシー問題に対しての反応は敏感になっており，監視カメラにおけるプライバシー侵害への対策が注目されている．

一般にはこの問題を避けるため，撮影画像をモニタできる人物を監視カメラの設置者や監視カメラを置く建物の管理者などに限定する，監視カメラの撮影範囲内に住宅や私有地などの私的空間が入らないようにする，映りこんだ私的空間には画像処理を施すなどといった，監視カメラ設置者との信頼関係による方法がとられる．しかしながら，これらの手法によって確実にプライバシー保護がされる確証はない．また，撮影者や管理者との間に十分な信頼が築かれていたとしても，情報の漏洩などの過失による，撮影画像の流出などの心配は避けられない．そのため，従来の信頼関係による方法ではない，技術的で確実なプライバシー保護手法の確立は重要な課題である．

従来の技術的な解決手法には，プライバシーを保護すべき物体の解像度を低下させ，判

別や特定を不可能にする非可逆な処理を用いた手法がある [3] [4]．これらの手法を適用した場合，プライバシー保護は実現できるが，犯罪捜査や追跡など証拠映像が必要となる際に撮影画像の証拠能力が不十分となり，本来の監視カメラとしての効果が損なわれてしまう．また，画像に特殊な符号化を用いる手法も提案されている [5]．この手法では，撮影画像にプライバシー保護処理を施した画像のみでなく，撮影画像そのものも表示することができる．しかし，画像の符号化に一般に使われる方法と異なるものを用いているため，プライバシー保護の有無にかかわらず画像の閲覧には特殊なシステムを使用する必要がある．そのため，設置コストや操作コストが高くなることが問題となる．

本論文では，この問題に対し，

- 撮影画像に画像処理を施して画像中の人物を不可視化し，特殊な符号化を用いずにプライバシーを保護する
- 移動物体の情報を暗号化して持つことで，犯罪捜査や追跡のときに撮影画像を再構成することを可能にする

といった，2 点から，プライバシー保護と監視の両立ができる手法を提案する．

■撮影画像へのプライバシー保護と真正性証明の両立

デジタル画像はアナログ画像に比べ，画像編集が容易であるため，撮影後の写真の色調やコントラストの補正，合成や切り取りといった加工処理などがよく行われる．これらの画像処理は多くの画像エディタで簡単に行えるため，一般にも広く浸透している．加工が容易であるという特徴から，デジタル画像は証拠能力に乏しく，撮影，出力した画像に改変が加えられていないことを証明できなければ，裁判などの司法の場で証拠として採用されないといった問題がある．プライバシー保護と監視の両立ができる手法も例外ではなく，プライバシーを保護した画像から撮影画像を再構成した画像が証拠として採用されるためには，撮影画像を再構成した画像が真正であることを示さなければならない．再構成画像が真正であることを証明できなければ，再構成された画像中の人物が実際に撮影されていたことが保証できない．

デジタル画像の真正性を証明する手法は様々なものが提案されている．田森らは，数論変換に基づく非耐性の電子透かしを埋め込み，攻撃を受けた際にはその透かしが壊れることを利用し，改竄検出を行う手法 [6] を提案した．杉村，西垣らは，公開鍵暗号とアルゴリズム公開型電子透かしを用いて画像の真正性が検証可能な手法 [7][8] を提案した．また，片山らはフラジャイル電子透かしを用いて携帯電話で実装可能な改竄検出手法 [9] を提案した．

これらの手法は撮影した画像そのものの真正性を証明する，もしくは改竄を検出するものであり，そのままプライバシー保護手法とともに用いると，プライバシー保護処理や再

構成処理を改竄攻撃と判別してしまう．そのため，プライバシー保護手法と組み合わせることができない．そこで，これらの真正性証明機能とプライバシー保護を両立する最も簡単な方法は，プライバシー保護を施した画像から完全に撮影画像に戻してから，前述の真正性証明手法を用いることである．しかし，撮影画像を完全に復元するためのデータが必要なため，撮影画像に対して出力ファイルサイズが大きくなる，また，撮影画像を再構成してからでないと真正性を証明できないため，無関係な人物のプライバシーも開示されることや，証明できる機関が限られてしまう，といった問題がある．そこで，撮影画像への再構成を伴わない，従来の真正性証明手法によらない真正性検証が必要である．

本論文では，この問題に対し，

- プライバシーの保護された画像から再構成される画像が，撮影画像に対し真正であることを，画像を再構成せずに示す
- RSA 公開鍵暗号方式を用いることで，アルゴリズムを公開できる真正性検証方法を示す
- 真正性検証情報と復元情報を出力ストリームに埋め込んでも，その符号長の増加を抑えられるような電子透かしを行う

といった，3 点から，プライバシーを保護した画像が改竄されていないことを証明する手法を提案する．

■最小カメラ台数によるカメラ配置の最適化

また，監視カメラシステムを構築するときに，どこにどのようなカメラを置くのが適当なのかを知りたいという要求がある．とにかく多数のカメラを設置すれば，ほとんどの場合観測したいシーンのすべてを監視カメラの撮影範囲内に収めることができる．しかし，多くの台数のカメラを設置すると，カメラそのもののコストが非常にかかる，撮影した画像をすべてモニタリングすることが困難，撮影画像の蓄積に大容量のストレージが多数必要，カメラのメンテナンスなどの管理にかかるコストが増大する，といった様々な問題が生じる．特に広大な環境を対象に構築しようとする場合，その環境が広大になればなるほどカメラは多く必要になるため，これらの問題が避けられない．そのため，観測目的を果たすことのできる，必要最小台数のカメラで監視カメラシステムを構築する手法が求められる．

一般には，監視カメラの設置場所に，店舗の出入り口や人通りの多いところ，オフィスビルのエレベーターホール，街頭での犯罪発生率の高い場所，などを選びそれらの場所に限定してカメラを置くことが多い．このように設置場所を決めようとすると，これらの場所は手動で決めなければならず，狭い店舗やマンションのロビーなどであればその決定は比較的容易であるが，ショッピングモールのような広い店舗や，多数のフロアを持つビ

ル，大学の敷地内，街の一区画などを対象とした場合，その位置を決めるのは困難である．さらに，撮影しなかった箇所があることによって監視性能が低下する可能性もある．そのため，与えられた観測シーンに対して監視性能を損なわないカメラの最適配置を自動的に求める手法が望まれる．

従来のカメラ配置の自動解法に関しては，Art Gallery Problem[10] が古くから知られている．この手法では，カメラセンサーは 360° 全方位，無限遠方までの視野を持っていると仮定し，さらにカメラの位置はシーンの外壁を示す多角形の角に限定されるとして，最適位置を求めるものである．しかし実際には，カメラセンサーの視野は方位，距離ともに限界があり，また設置位置も角に限らない．Nikolaidis らはカメラをセンサネットワークの一種として捉え，室内で活動するロボットへ情報を与えるものとして，室内のカメラ配置を解く手法を提案している [11]．室内で活動するロボットの軌跡を中心に監視重要度をマッピングし，あらかじめ指定したカメラ台数での最適なカメラ位置と向きを最急降下法により求める．この手法では最急降下法を用いているため，局所解に陥る可能性がある．Hörster らは狭い観測シーンでのカメラ最適配置問題を，複数のケースに分割し，線形計画法によりそれぞれを解いている [12]．この手法では，局所解に陥らず最適解が得られることが保証されるが，観測点とカメラ候補点をともに手動で配置するため，観測シーンが広大になるとそのコストが増大し，適用が困難になると考えられる．また，観測点やカメラ設置点の数がそれぞれ 100 個程度を超える場合には近似解法が必要としているため，狭い範囲の環境でなければ，最適解が得られる保証が無い．Murray らは広い観測シーンでのカメラ最適配置問題に対し文献 [13]，[14] において解決法を提案している．文献 [13] では観測シーンをメッシュで領域分割し観測点を置き，カメラ設置位置は手動で設定し，さらに，カメラから見える領域の組み合わせを集合被覆問題として解くことで，任意のカメラ台数に対して観測領域面積を最大化するカメラ配置を求める．また，文献 [14] では，位置を固定したカメラに対して，最適なパン・チルト・ズームパラメータを与える手法を述べている．しかし，ある空間や領域全体を観測したい場合のカメラ台数や位置，向きなどを求めるためには，自由度の高い設置位置の候補を与えること，つまり，カメラ位置も自動で設定できることが必要である．さらに，カメラパラメータと位置を同時に求めなければ最適解が得られない可能性がある．

本論文では，この問題に対し，

- 目的の観測シーンに進入してきた物体の移動経路を見落とすことなく検出できるカメラ配置を求める
- カメラ位置と向き，視野角や視野距離などのスペックを同時に考慮することで，最小のカメラ台数による最適配置を求める

といった，2 点から，最適カメラ配置を求める手法を提案する．

■本論文の構成

第 1 章では，研究背景と研究目的について述べた．まず，監視カメラが国内外を問わず多数設置されている現状と，これからも増加の一途をたどるであろうことを示した．さらに，個人のプライバシーへの関心が高まり，監視カメラの設置増加に伴ってプライバシーを保護する技術的な手法の確立が必要であること，また，多くの環境で監視カメラシステムを構築するためには，監視カメラの最適配置を自動的に求める手法が必要であることを述べ，本論文で対象とする問題，解決すべき課題を明らかにした．

第 2 章では，監視カメラによるプライバシー保護の技術的な実現手法とその構成法について述べる．まずは，監視カメラにおけるプライバシー保護を定義する．監視カメラでのプライバシー保護では，移動物体を特定する情報は隠蔽しながらも，どのような行動があったかは把握できる必要がある．そのため，物体と背景が分離できることが必要である．本論文では，監視カメラシステムを固定モニタリングカメラによって構成する．固定モニタリングカメラは，位置や向き，パン・チルト・ズームパラメータが固定されていることから，人や車が存在せず，さらに日照や照明などの撮影環境に変化がなければ常に一定の画像を撮影し続ける．この特徴を利用することで，プライバシーを保護する物体を撮影画像から抜き出すことができる．プライバシー保護の定義に基づき，監視カメラにおいて撮影した画像中の移動物体領域を，画像処理によって不可視化することで，移動物体のプライバシー保護を実現する．しかし，移動物体を不可視化したままでは犯罪捜査や追跡に用いることはできない．そこで，撮影画像を再構成するための復元情報を電子透かしにより出力ストリーム中に埋め込む．さらに，復元情報には暗号化を施しておき，撮影画像を再構成できる人物を制限する．このプライバシー保護と移動物体の特定，追跡を可能にする手法の構成法を，移動物体を不可視化する処理，復元情報の作成，復元情報の電子透かしによる埋め込みを中心に説明する．提案手法を適用した実験から，定義に従って移動物体のプライバシーが保護できること，移動物体を復元し撮影画像が再構成できることを示し，さらには，複数の人物が存在するときに特定の人物のみを復元しそのほかの人物はプライバシーを保護したままにできること，また，画像中の移動物体の大きさに対して提案手法が適用可能であるか，符号長がどのように変化するかを示す．

第 3 章では，真正性証明とプライバシー保護を両立できる手法について述べる．第 2 章で述べる手法により，撮影画像のプライバシー保護は可能である．しかし，再構成画像に表れた人物が，撮影画像中にも存在していたことを示せなければ，証拠としての有用性は低い．そこで，プライバシー保護された画像から再構成される画像が，真正であることを証明できる手法を提案し，手法の構成法を述べる．撮影画像を RSA 公開鍵暗号方式と電子証明を応用した方式で暗号化することによって，プライバシーを保護した画像を再構成せずに真正性が検証できる．この手法を実現するための，RSA 暗号を利用した復元用

データの生成方法，電子署名を利用した真正性検証用データの生成方法を述べる．また，出力ストリームの符号長を増加させずに，真正性検証用データや撮影画像復元用データを埋め込むための，ハフマン符号化の特徴に基づいた電子透かし方法を説明する．さらに，真正性を検証する手順と様々な改竄攻撃への耐性を示し，最後に実験から，移動物体のプライバシーを保護しても再構成画像の真正性が証明できることを示し，撮影画像中の移動物体の大きさと出力ストリームの符号長の関係性から手法の有効性を示す．

第 4 章では，監視カメラシステムを最小のカメラ台数で構築するための手法を述べる．監視カメラの配置を最適化する問題では，固定モニタカメラが常に同じ範囲を撮影することから，設置したカメラと観測範囲との関係が一意に定まる．カメラと観測範囲のすべての組み合わせから，目的とする観測範囲をカバーする最小台数のカメラ配置の組み合わせを選択することで，監視カメラの最適配置が求まる．しかし，カメラ位置と観測点を定める際に，特に広大なシーンを対象としてカメラ配置を求めようとする場合には，それらを手動で定めるのは困難である．また，観測シーン全体をカバーするカメラ配置の解法を用いるとカメラ配置は求まるが，非常に多くのカメラを必要とする，また，最適解を求めるのに長時間を要する，といった問題がある．そこで，まず，与えられた観測シーンを矩形領域で近似して，通路や分岐点からなるグラフ構造を定める方法を述べる．次に，グラフ構造と頂点被覆により，すべての移動物体の移動経路を捉えることのできる観測領域の求め方を説明する．さらに，求めた観測領域と，監視カメラを置ける位置や向き，カメラ仕様から，カメラ候補と観測領域との関係性を集合被覆問題に置き換え，最小カメラ台数での最適配置を求める手法を示す．実験では，手法の有用性を示すための仮想的なシーンと，実在する広大なシーンを対象に，観測シーン全体を観測する場合や，シーン中のすべての分岐点を観測する場合に比べて，短時間に少ない台数での最適配置が求まることから手法の有効性を示す．

最後に第 5 章で，本論文の成果についてまとめる．

第 2 章

Masking を用いたプライバシー保護手法

2.1 はじめに

本章では，監視カメラシステムにおけるプライバシー保護の技術的な実現手法について述べる．提案手法ではエンコーダ，デコーダが次に示す 6 点の条件を満たすことで，プライバシー保護と監視の両立を実現する．

1. **撮影画像中の移動物体に対し画像処理を行う**
   移動物体に画像処理によるモザイク化や透明化などの不可視化 (masking) を施すことでプライバシー保護を実現する．masking には非可逆な画像処理を用いるため，masking が施された画像 (**masked image**) を，画像処理のみによって撮影画像へ復元することはできない．
2. Masked image **は一般の** JPEG **ビューアで閲覧が可能**
   Masked image は，JPEG[15] ストリームとして出力する．JPEG 圧縮形式は圧縮率が高く，画像圧縮によく用いられる一般的なフォーマットである．監視カメラによって撮影を続けると，撮影画像は多量になり，そのデータサイズは膨大になる．そのため，長期間撮影した画像を無圧縮のまま保存することは現実的ではなく，圧縮して蓄積，保存する必要がある．また，保存された masked image は特別な操作やアプリケーションを必要とせず簡単に閲覧できることが望ましい．これは，被撮影者が，自身が撮影された画像を特別なアプリケーションや装置を利用，導入するころなく確認できることで，プライバシー保護への透明性が増すことや，監視画像のモニタリングを容易に行うことができるためである．

3. **撮影画像は特殊ビューアにより再構成が可能**

   犯罪捜査や追跡のためには，移動物体の特定が必要である．そのため，出力 JPEG ストリームから，撮影画像が再構成できなければならない．提案手法では，移動物体情報を用いて，撮影画像の再構成を可能とする．撮影画像の再構成，閲覧は，上記 2. の場合と異なり，監視カメラを設置する責任者，警察などの捜査を行う機関などといった，特定の人物や機関のみに限定する．そのため，一般のビューアとは別に撮影画像の再構成機能を持つ特殊なビューア (reconstructing viewer) を作成する．reconstructing viewer での撮影画像の再構成にはパスワードを必要とするため，reconstructing viewer を手に入れただけでは撮影画像を再構成できない．

4. **エンコーダは入力 1 フレームに対し 1 つのストリームを出力する**

   撮影画像を再構成するためには，masked image に対応する移動物体情報を，masked image と別のストリームで出力することが，最も簡単な実装方法である．しかし，この方法では出力ストリームと移動物体情報が正しく対応しているか，移動物体情報をまったく無関係の画像から引用していないかなど，両者のデータの整合性をとる必要が生じる．また，masked image を出力するための JPEG ストリームと，撮影画像を再構成するための移動物体情報との対応関係を保ったまま保存，管理する必要がある．そのため，単一のストリームを保存するのに比べ，データ紛失の可能性が高くなるなど，管理面の問題も生じる．よって，1 フレームの撮影画像から 1 つの JPEG ストリームのみを出力し，移動物体情報は JPEG ストリーム中に電子透かしを用いて埋め込んでおく．利用者は，masked image の表示や撮影画像の再構成の際に，デコーダに与えるデータ形式を意識しなくてよい．JPEG ビューアを用いれば masked image が閲覧でき，reconstructing viewer を用いれば画像が再構成できる．

5. **Reconstructing viewer では複数の移動物体から再構成する移動物体の選択が可能**

   撮影画像中に複数の移動物体が存在する場合，それらの物体から，注目する物体のみを復元して再構成画像を得られるようにする．全ての移動物体を一括して復元すると，注目する物体とともに撮影されただけの，本来プライバシー保護されているべき移動物体が特定・識別されてしまうことがある．そのため復元する移動物体が選択できるようにし，その他の移動物体はプライバシー保護された状態に保つ．

6. **エンコードは逐次的に行われる**

   撮影画像へのエンコードは，撮影時点までのフレームのみを用いて行われる．そのため，撮影と同時にエンコード，および JPEG ストリームの出力ができるので，エンコーディングを行いながらも，リアルタイムで監視を行うことができ，一時的にも撮影画像をそのまま保存することがないため，撮影画像が流出するリスクを避けられる．

2.2　監視カメラにおけるプライバシー保護

まず，本節では，監視カメラにおけるプライバシー保護の定義を述べる．本論文では，プライバシー保護は “ 被写体が誰であるか” を隠すことで満たすことができるとする．ここで，図 2.1(b)，図 2.2(b) はともに，(a) の撮影画像に画像処理を施し “被写体が誰であるか” を隠蔽した図である．しかし，本論文では，監視カメラにより撮影した画像へのプライバシー保護の実現を目的とするため，“ 被写体が何をしているか” まで隠してはならない．これは，図 2.2(b) に示すように，“ 被写体が何をしているか” を隠蔽してしまうと，何が起こったかを把握することができず，監視映像から問題の場面と問題ない場面を区別することができなくなり，有効な監視ができなくなるためである．図 2.1(b) からは，図 2.1(a) のようにボールを投げている人物 **A** を特定することはないが，誰かが何かを投げている，と言う行動を推測することができる．何が起こっているかを知ることで問題行動が発見できるため，監視の有効性が保たれる．本論文では，図 2.1(b) に示すように，移動物体などを不可視化することで，“被写体が誰であるか” を隠蔽する．さらに，形状を明らかにすることで “ 被写体が何をしているか” が把握できる画像を，プライバシー保護された画像とする．ここで，移動物体を不可視化し，その移動物体を特定する情報を隠蔽した画像を，本論文では masked image と呼ぶ．

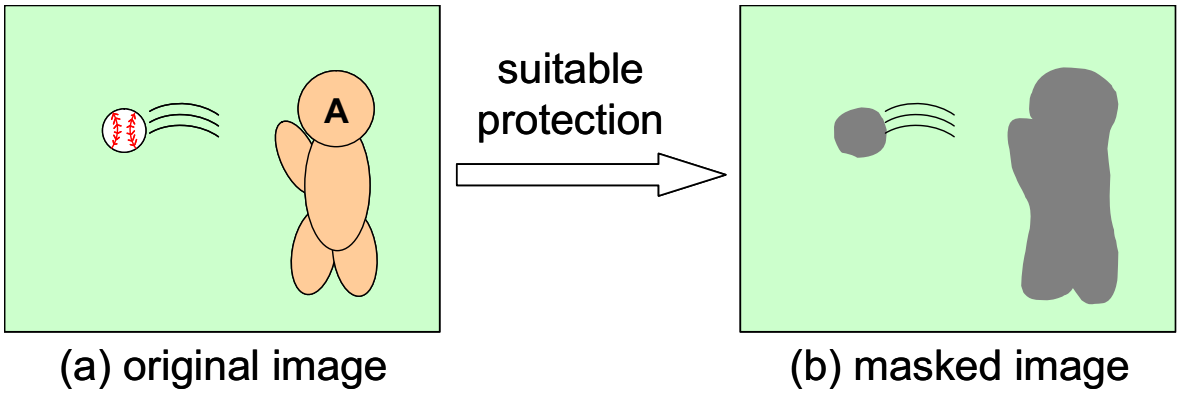


図 2.1 適切なプライバシー保護の例

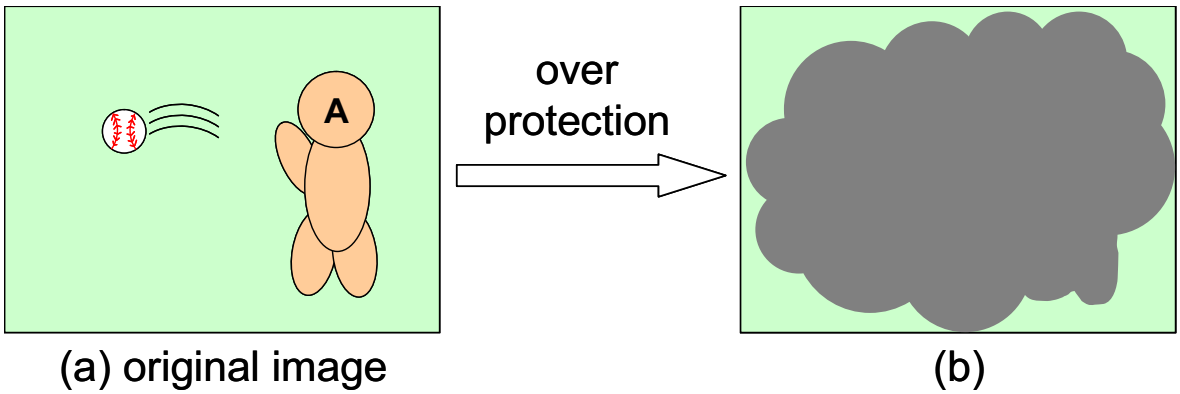


図 2.2 過剰なプライバシー保護の例

監視カメラにおけるプライバシー保護の実現には，撮影画像中の移動物体などの形状を知る必要がある．本論文は移動物体を前景領域，そのほかの領域を背景領域として撮影画像を 2 つの領域に分離する．移動物体の抽出には背景差分法 [16] [17] [18] [19]，フレーム間差分法 [20]，オプティカルフロー [21][22] などを用いることができる．この部分はいまだ研究途上であり，正確な移動物体の抽出のために研究を行っている [23][24][25][26]．本論文では監視カメラシステムを固定モニタリングカメラにより構築することを利用して，文献 [16] の背景差分法を利用して移動物体を抽出する．本節では背景差分法による固定モニタカメラ映像中の移動物体抽出手法の概要を述べる．

2.2.1　背景差分法による移動物体抽出

固定モニタリングカメラによる撮影では，移動物体が存在せずまた，撮影環境の変化がなければ，常に一定の画像が得られる．その一定で変化の無い画像を背景画像とし，撮影画像との差分をとることで，変化のあったピクセルを前景領域として取り出すことができる．しかし，実際にはノイズの影響や，照明条件の変動，環境光の揺らぎにより，同一ピクセルの輝度値はわずかに変化する．この変化に影響されずに移動物体領域を抽出する処理方法が必要である．

本論文では，次のように背景画像を作成し，移動物体を抽出する．

1. 初期背景画像の作成
2. Gauss 分布近似による背景画像の更新
3. 移動物体に関わるピクセルの抽出

初期背景画像の作成

まず，安定した移動物体の抽出，背景画像の更新のために初期背景画像を作成する．撮影開始から n フレーム目までは，移動物体を含まず，日照や照明変動などの撮影環境の変化が極めて小さい画像を撮影し，これらの画像から初期背景画像を作成する．時刻 $t(t = 1, 2, \ldots, n)$ フレーム目において，撮影画像の輝度値を $I(t)$ とすると，時刻 $t(t = 1, 2, \ldots, n)$ フレーム目における初期背景画像の輝度値 $B_I(t)$ は，式 (2.1) で表される．

$$B_I(t) = \frac{B_I(t-1) \times (t-1) + I(t)}{t} \quad (t = 1, 2, \ldots, n) \tag{2.1}$$

また，そのときの分散値 σ_I^2 を式 (2.2) で近似する．

$$\sigma_I^2(t) = \frac{\sigma_I^2(t-1) \times (t-1) + \{I(t) - B_I(t)\}^2}{t} \tag{2.2}$$

よって，n フレーム目の初期背景画像の輝度値 $B_I(n)$ および分散値 $\sigma_I^2(n)$ は，それぞれ式 (2.3)，式 (2.4) で表される．

$$B_I(n) = \frac{1}{n} \sum_{t=1}^{n} I(t) \tag{2.3}$$

$$\sigma_I^2(n) = \frac{1}{n} \sum_{t=1}^{n} \{I(t) - B_I(t)\}^2 \tag{2.4}$$

Gauss 分布近似による背景画像の作成と更新

撮影環境はわずかずつ変化していくため，その変化を背景画像に徐々に取り込んでいかなければ，撮影画像との差異が広がり移動物体の誤抽出を引き起こす．初期背景画像は一定期間の撮影画像の輝度値を平均して作成したが，以降は背景画像の輝度値の揺らぎが単一 Gauss 分布により近似できるものとして更新する．撮影画像の輝度値と，背景画像の輝度値を比較し，標準偏差を基準に背景領域の揺らぎの範囲内であるか，異なる物体が入力されたかを判別し，背景領域であるピクセルのみ背景画像を更新する．時刻 t において，撮影画素の輝度値を $I(t)$，背景画像の輝度値を $B_I(t)$，その Gauss 分布の標準偏差を $\sigma(t)$，として撮影画像を更新率 $\rho(0 < \rho < 1)$ で背景画像に取り込むとすると，更新後の背景画像の輝度値 $B_I(t+1)$ は式 (2.5) で表される．

$$B_I(t+1) = (1-\rho)B_I(t) + \rho I(t) \quad (t \geq n) \tag{2.5}$$

また，標準偏差 $\sigma_I(t+1)$ は式 (2.6) で近似する．

$$\sigma_I(t+1) = \sqrt{(1-\rho)\sigma_I^2(t) + \rho \{I(t) - B(t)_I\}^2} \quad (t \geq n) \tag{2.6}$$

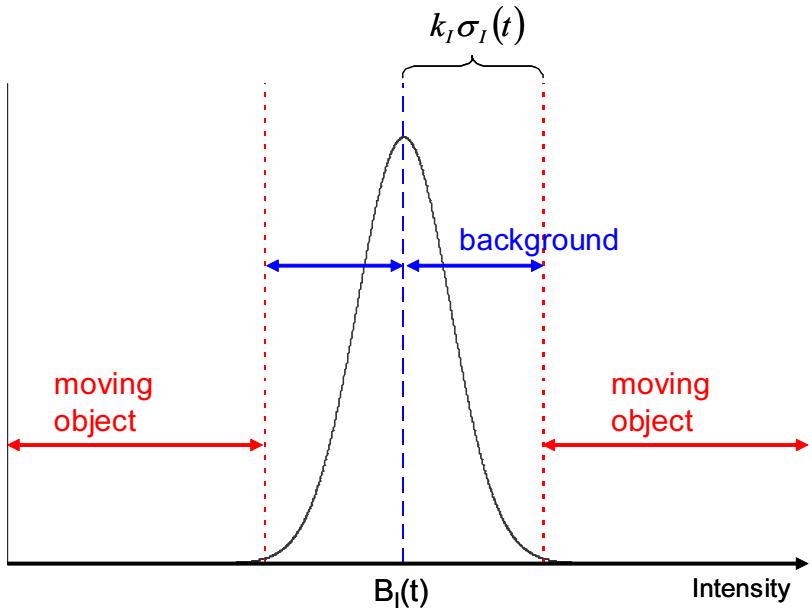


図 2.3 Gauss 分布近似によるピクセルの判別

各フレームにおける移動物体に関わるピクセルの抽出

各ピクセルが移動物体に関わるものであるかは，図 2.3 のように Gauss 分布近似によって判別する．

フレーム t における撮影画像の輝度値 $I(t)$ と背景画像の輝度値 $B_I(t)$ および，分散値 $\sigma_I(t)$ が式 (2.7) を満たすとき，そのピクセルを移動物体関わるピクセルとして抽出する．また，式 (2.8) をみたすときは背景であるとして，背景更新に用いる．

$$|B_I(t) - I(t)| > k_I\sigma_I(t) \tag{2.7}$$
$$|B_I(t) - I(t)| \leq k_I\sigma_I(t) \tag{2.8}$$

提案手法では，ここで抽出された移動物体領域を，プライバシー保護が必要な領域であるとして扱う．

2.3 Masking によるプライバシー保護の構成

プライバシー保護と監視の両立を実現する手法の全体の構成と概要について説明する．提案手法のシステムは，プライバシー保護の処理などを行うエンコード部と，移動物体の復元に基づき撮影画像を再構成するデコード部の，2 つに大きく分けることができる．エンコード部の構成を図 2.4 に，デコード部の構成を図 2.5 に示す．

エンコード部では，まず，監視カメラにより画像を撮影する．第 2.2 節に述べたように，監視カメラには固定モニタカメラを用いる．次に，撮影画像を移動物体領域と背景領域に分離するため，背景差分法による移動物体抽出を行う．抽出した移動物体には時系的な追跡であるトラッキング [27] を行い，抽出移動物体に固有のオブジェクト番号をつける．前フレームより継続して存在する移動物体には前フレームの物体と同一のオブジェクト番号を継続して付与し，現フレームで新規に出現した移動物体には新たなオブジェクト番号を付与する．移動物体の類似性は，移動物体の高さ，幅，面積，移動速度などの特徴から計算される．次に，撮影画像，撮影画像から抽出された移動物体，抽出された移動物体のオブジェクト番号の 3 種を用いて，エンコーダにより masked image を作成する．エンコーダの詳細な構成は第 2.4 節で述べる．作成された masked image は単一の JPEG ビットストリームとして出力され，保存・送信される．

保存・送信された JPEG ビットストリームは 2 種類のデコーダによってデコードできる．一般に用いられる JPEG ビューアやブラウザである normal viewer によってデコードした際には，masked image が表示される．Masked image は移動物体が不可視化されているため，第 2.2 節で述べたように，画像中の物体のプライバシーを保護したままモニタリングできる．提案手法のために作成された reconstructing viewer を用いてデコードすると，移動物体を復元して撮影画像を再構成した画像が表示される．この画像からは移動物体の特定が可能であるため，犯罪捜査や追跡に使用できる．Reconstructing viewer によるデコーディングは第 2.5 節で説明する．

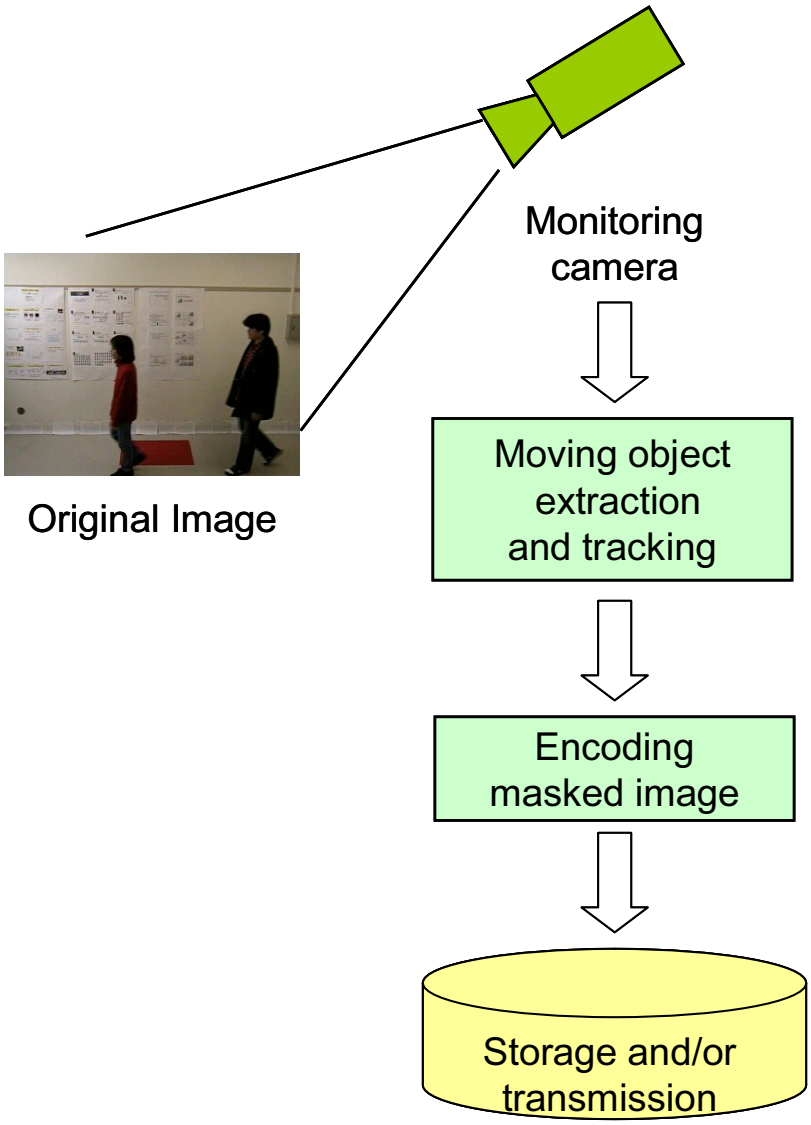


図 2.4 提案手法の構成（エンコード部）

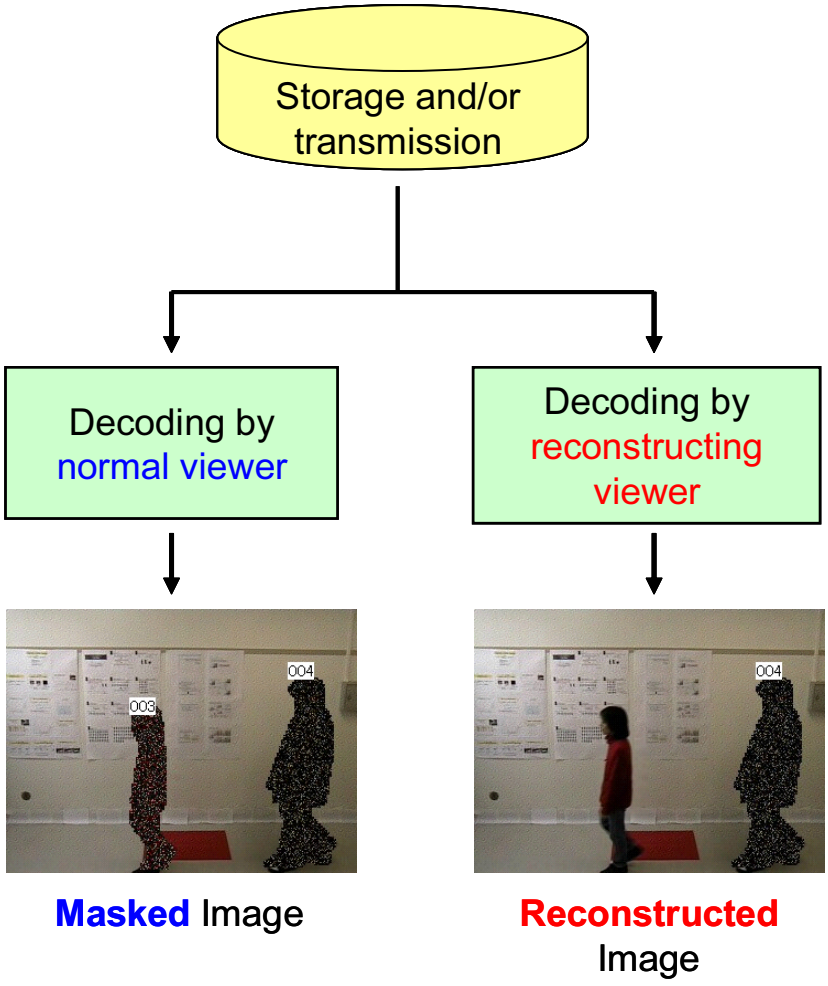


図 2.5 提案手法の構成（デコード部）

2.4　エンコーダの構成

図 2.6 はエンコーダの構成を示したものである．図中の (a)masking，(b)AES 暗号化，(c) 電子透かしについては，それぞれ第 2.4.1 節，第 2.4.2 節，第 2.4.3 節で詳細に述べる．

エンコーダは撮影画像，撮影画像から抽出した移動物体，抽出した移動物体のオブジェクト番号の 3 つをそれぞれ入力とする．移動物体とオブジェクト番号はそれぞれ移動物体ごとに個別に処理する．

まず，移動物体に対する処理について説明する．移動物体は各物体ごとに離散コサイン変換 (DCT)，量子化 (Quantization)，ジグザグスキャン (Zigzag scan)，ハフマン符号化 (Huffman coding) を行い，符号化移動物体 (coded moving object) を作成する．これは各移動物体にそれぞれ JPEG 圧縮を行い，そのヘッダーを除いた処理と等価である．次に，符号化移動物体を AES(Advanced Encryption Standard)[28] により暗号化し，暗号化ストリーム (encrypted stream) を作成する．このとき，AES に用いるパスワードは移動物体に割り振られたオブジェクト番号を元に生成する．最後に，暗号化ストリームは電子透かし処理に送られる．

次に撮影画像の処理について説明する．撮影画像は masking によって masked image に変換される．masked image は DCT，量子化，ジグザグスキャンによって処理される．ここで行う量子化では，移動物体画像へ用いた量子化テーブルと異なるものを用いることができる．異なる量子化テーブルを用いることで masked image と再構成される移動物体の圧縮率を変えることができるため，masked image のみを高圧縮して，出力 JPEG ストリームの符号長を削減することなどができる．この量子化 DCT 係数に移動物体の処理によって作成した暗号化ストリームを電子透かしにより埋め込む．埋め込みの後，量子化 DCT 係数列はハフマン符号化によって符号化され，最後にヘッダーを付与して JPEG ビットストリームが出力される．

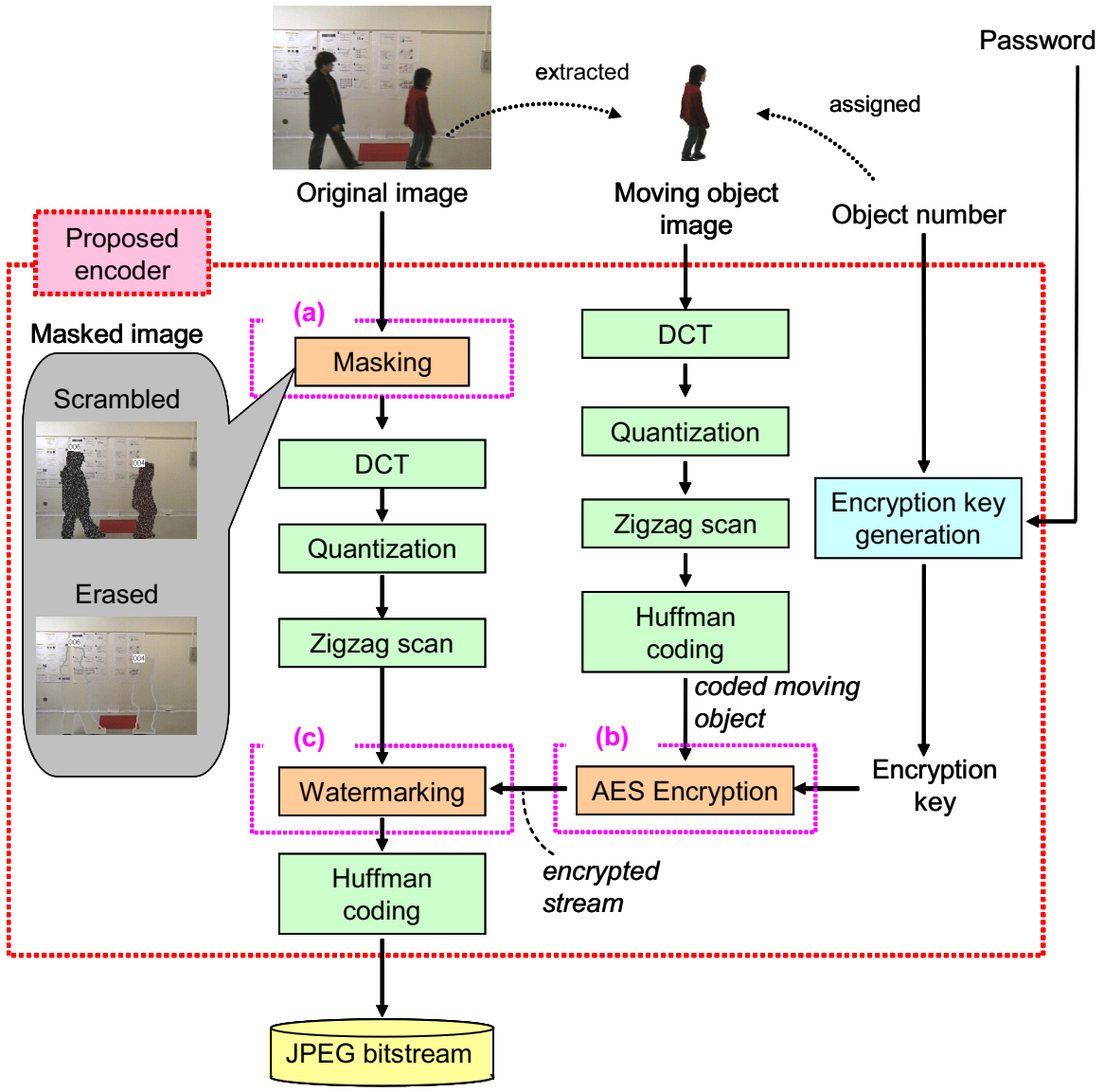


図 2.6 エンコーダの構成

2.4.1 (a) Masked Image の作成

本節では，図 2.6(a) の masking について説明する．masking には図 2.7 に示す Scrambling，Erasing，Defocusing，Mosaicing の 4 種の画像処理を用いた．図 2.7 の上段は人物にそれぞれの masking を行った結果，下段はそれぞれを適用した際の各ピクセルの変化を模式的に示したものである．いずれの masking された画像も人物を特定することができないことがわかる．以下に，それぞれの masking についての詳細を述べる．

■Scrambling

移動物体領域中の全ピクセルをランダムに，移動物体領域内部に存在するいずれかのピクセルで置き換えることにより，擬似スクランブル画像を生成する手法である．置き換えに用いる乱数列は重複を許すため，撮影画像の移動物体領域内部と Scrambling 後の移動物体領域内部が同一のピクセル集合で構成されることは保証されない．そのため，Scrambling された画像にピクセル入れ換えを施しても撮影画像は復元されない．Scrambling は masking された物体の形状が判別しやすい，また，移動物体中の一部分（例として車のナンバープレート，人物の顔領域など）に限定して masking を行う場合に，図 2.7 に示した 4 つの手法の中で，最も自然に表示できる，という利点がある．

■Erasing

撮影画像の移動物体領域内のピクセルを，背景画像の同座標のピクセルに置き換えることにより，移動物体を透明化する手法である．背景画像への置き換えのみでは物体形状が明確でなく，“被写体が何をしているか” を認識できないため，移動物体領域のエッジを画像内に書き込むことで，移動物体の形状を表示する．Erasing を用いると，masked image 上では移動物体の形状のみしか分からず，色情報や顔情報などはまったく認識できないため，4 種類の masking のうち最も強固なプライバシー保護を行う手法といえる．

■Defocusing

撮影画像の移動物体中のピクセルの R, G, B 値それぞれを近接ピクセルの平均値に置き換えることで，ピントボケした（フォーカスをはずした）画像を生成する手法である．x 座標 i，y 座標 j のピクセルを Defocusing する場合，座標 (i, j) を中心とした $(2X + 1) \times (2Y + 1)$ 個のピクセルの平均値でピクセル (i, j) を置換する．式 (2.9) は Defocusing 処理を示す．ここで，M_{ij} は masked image の x 座標 i，y 座標 j の R, G, B 値，I_{rs} は入力画像の x 座標 r，y 座標 s の R, G, B 値をそれぞれ表す．式 (2.9) は R, G, B の値に対する計算いずれか一つを表している．実際には R, G, B 各色にこの計算を行

わなければならない.

$$M_{ij} = \frac{\sum_{r=-X}^{X} \sum_{s=-Y}^{Y} I_{i+r,j+s}}{(2X+1) \times (2Y+1)} \tag{2.9}$$

Defocusing を用いた場合，色情報のほとんどは開示され，ある程度までは移動物体を識別することが可能である.

■Mosaicing

撮影画像の移動物体中のピクセルを含むブロックを作成し，そのブロック内の全ピクセルの R, G, B 値をそれぞれブロック内の平均値に置き換えることで，モザイクをかけたような画像を生成する手法である．ブロックサイズを $(2X+1) \times (2Y+1)$，ブロックの中心座標を (mx, my) として Mosaicing を行う場合，式 (2.10) となる．ここで，M_{ij} は masked image の x 座標 i，y 座標 j の R, G, B 値，I_{rs} は入力画像の x 座標 r，y 座標 s の R, G, B 値をそれぞれ表す.

$$\begin{aligned} M_{mx-X,my-Y} = M_{mx-X+1,my-Y} = \cdots = M_{mx+X,my+Y} \\ = \frac{\sum_{r=-X}^{X} \sum_{s=-Y}^{Y} I_{mx+r,my+s}}{(2X+1) \times (2Y+1)} \end{aligned} \tag{2.10}$$

式 (2.10) は R, G, B の値に対する計算いずれか一つを表している．実際には R, G, B 各色にこの計算を行わなければならない．Mosaicing を用いた場合も，Defocusing と同様色情報のほとんどは開示されるが，形状がブロック化されるため移動物体は Defocusing より識別が難しい.

Masking には上記の処理から任意のものを選んで行うことが可能である．移動物体がおおまかにどのような色をしているかを示したい場合には，Scrambling や Defocusing, Mosaicing が適しており，移動物体の形状以外の一切の情報を隠したい場合には Erasing を用いるのが適切である.

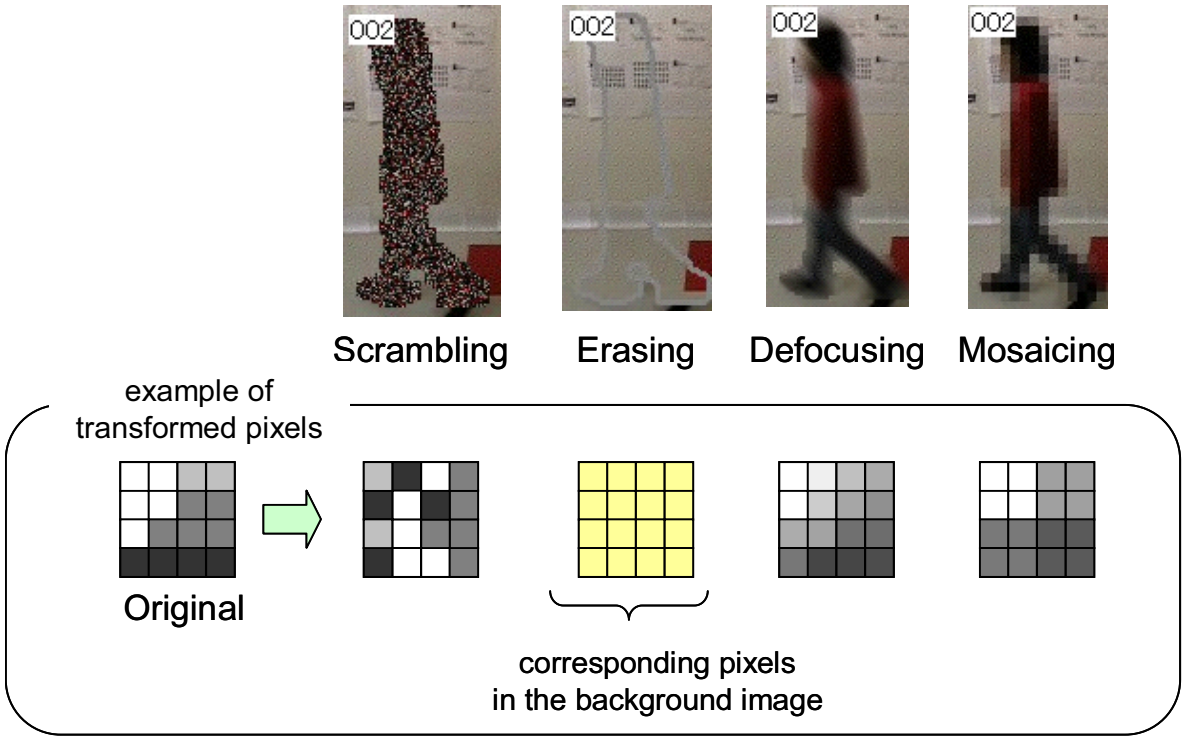


図 2.7 masking 手法 (Scrambling，Erasing，Defocusing，Mosaicing) の比較

2.4.2 (b) 移動物体情報の暗号化

本節では図 2.6(b) の AES 暗号化について説明する．第 2.4.1 節では，通常ビューアを用いた際に表示する，masked image の作成について述べたが，reconstructing viewer を用いた際には移動物体を復元し，撮影画像を再構成して表示する必要がある．そのため，移動物体情報を保存する必要があるが，特定の人物以外が移動物体を復元できないように暗号化する．また，オブジェクト番号をもとにそれぞれの物体に個別の暗号鍵を割り当て，注目する物体だけ復元できるデータ構造を作成する．暗号化は物体ごとに行うが，第 2.4.3 節に述べる，電子透かしプロセスへ送る際には，暗号化データをひとつのストリームに結合する．

移動物体情報暗号化フロー

図 2.8 は AES 暗号化の処理フローを示したものである．撮影画像から抽出された移動物体は，暗号化の前にあらかじめ DCT，量子化，ジグザグスキャン，ハフマン符号化により符号化移動物体に変換されている（第 2.4 節）．ここで，符号化移動物体は 16×16 ピクセルのブロック単位で作成しておく．16×16 ピクセルは，JPEG 圧縮の単位である MCU(Minimum Coded Unit) のサイズと同じである．通常の JPEG 圧縮では，ジグザグスキャンまでは MCU 単位で行うが，ハフマン符号化は画像全体で行う．符号化移動物体の作成ではハフマン符号化も MCU 単位で行う．

オブジェクト k の移動物体画像から生成した符号化移動物体を “coded moving object k” とする．また，coded moving object k の符号長を N_k とする．各 coded moving object は次に示す 3 ステップで埋め込みデータに変換される．

Step 1:

Coded moving object はオブジェクト 1 つに付き，1 本のストリームとして与えられる．電子透かしにより masked image に埋め込む際には全オブジェクトに対して 1 本のストリームに結合するため，結合されたストリームを，再びオブジェクトごとに戻せるように，coded moving object の前後に識別子を挿入する．それぞれの識別子は，JEPG ヘッダーと同じ長さの 2 バイトコードの中から，自由に使える組み合わせのものを用いる．

Step 2:

Coded moving object を AES により暗号化する．ここで，AES は 16 バイト単位での暗号化であるため，coded moving object と識別子をあわせた符号長が 16 バイトの倍数ではない場合，coded moving object 終端の識別子の後ろに適当な長さ

のダミーコードを挿入し，16 バイトの倍数にそろえる．coded moving object k の識別子，ダミーコードを含む最終的な符号長 L_k は次の式で表される．

$$L_k = N_k + 4 + D_k \equiv 0 \ (mod 16)$$

ここで，D_k は coded moving object k に付加するダミーコードの符号長を示す．AES の暗号化鍵は各移動物体のオブジェクト番号を元に，それぞれのオブジェクト固有のものを生成する．AES の暗号化鍵長は 16 バイト，24 バイト，32 バイトの 3 種から選択できる．提案手法では 24 バイト長の鍵を用い，前半 22 バイトをパスワード，後半 2 バイトを対応するオブジェクト番号として，鍵を生成する．暗号化は各移動物体ごとに個別に行い，ここではオブジェクトの個数分の暗号化データを生成する．

Step 3:

すべての暗号化ストリームを単純に並べて結合し，1 本の暗号化ストリームを作る．暗号化ストリームは第 2.4.3 節で，masked image 中に電子透かしによって埋め込まれる．

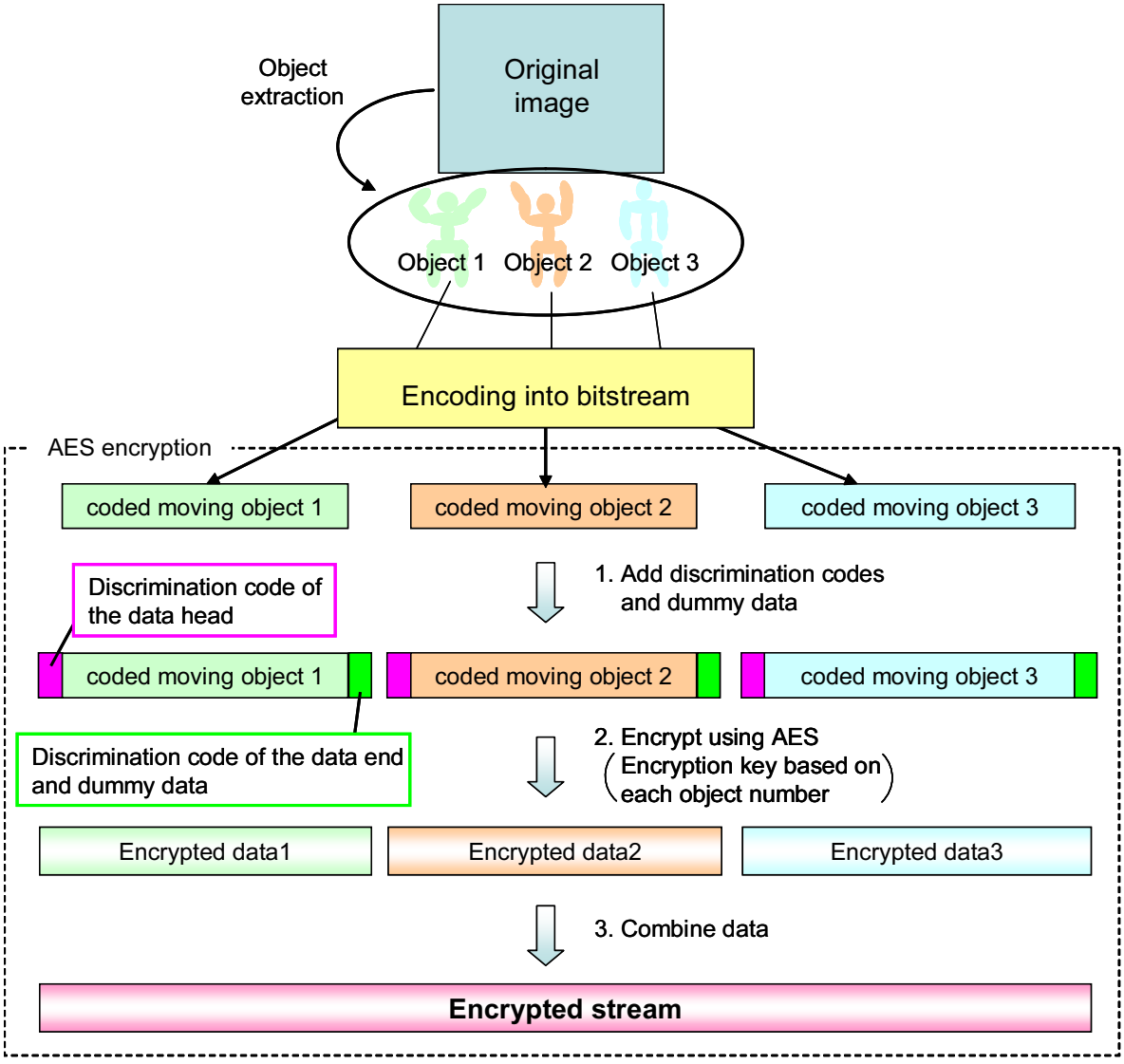


図 2.8 符号化移動物体からの暗号化ストリームの生成

2.4.3 (c) 電子透かしによる移動物体情報の埋め込み

電子透かしに用いる DCT 係数位置

本節では図 2.6(c) の電子透かしについて説明する．前節で作成した暗号化ストリームを電子透かしによって masked image 内に埋め込む．図 2.6(a) で masking された masked image は，標準の JPEG 圧縮処理と同様に DCT，量子化されている．本章での電子透かしは，masked image の量子化 DCT 係数の最下位ビット (LSB: least significant bit) を埋め込むデータのビット値で置換する方式を用いる．図 2.9 は電子透かしに用いる量子化 DCT 係数の位置を示したものである．図中の左上 1 番の係数は DC 成分を表し，残りの 63 個の係数は AC 成分を表す．AC 成分は左上にあるほど低周波成分を表し，右下にいくほど高周波成分を表す．提案手法では，人間の視覚特性と JPEG 圧縮の特性から優先的に用いる係数位置を決定した．電子透かしには中間周波数帯を優先的に使用し，暗号化ストリームが長くなるにつれ，高周波数帯へ埋め込んでいく．また，低周波数帯は電子透かしには用いない．人間は低周波数帯の係数変化に敏感であり，わずかな変化でも画像に現

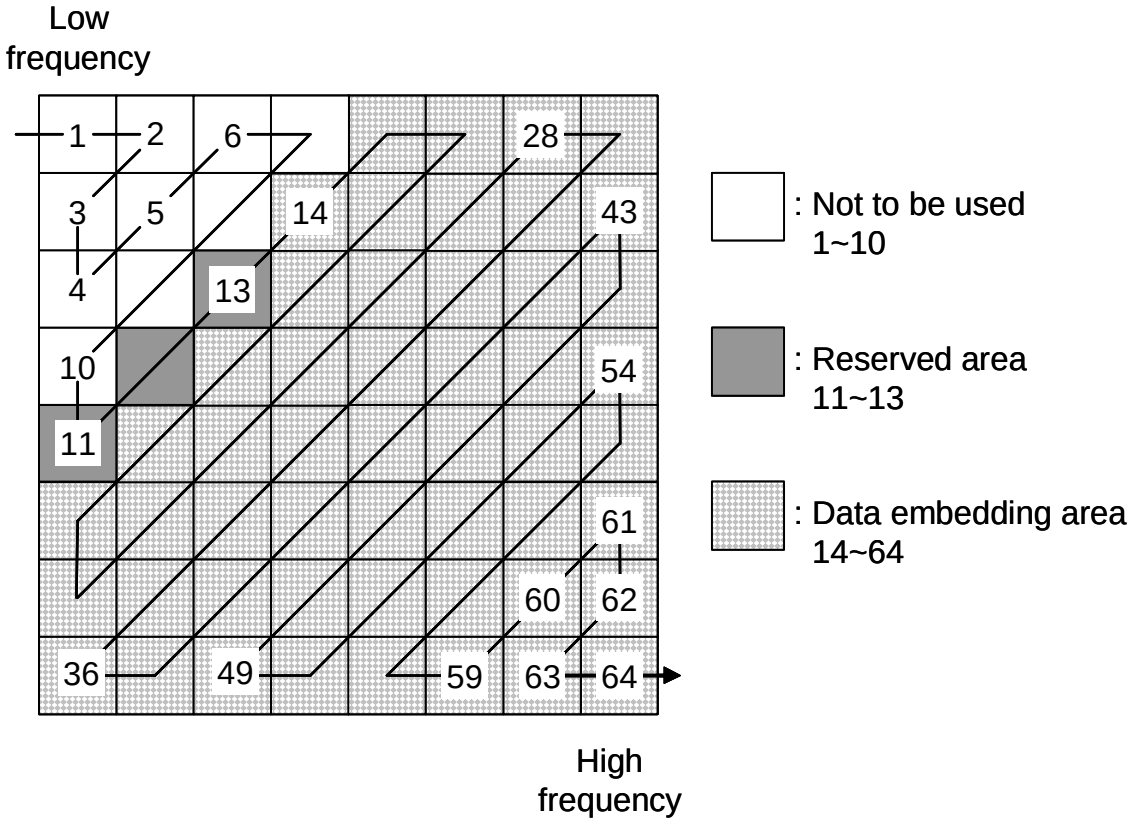


図 2.9 電子透かしで埋め込みに用いる DCT 係数位置

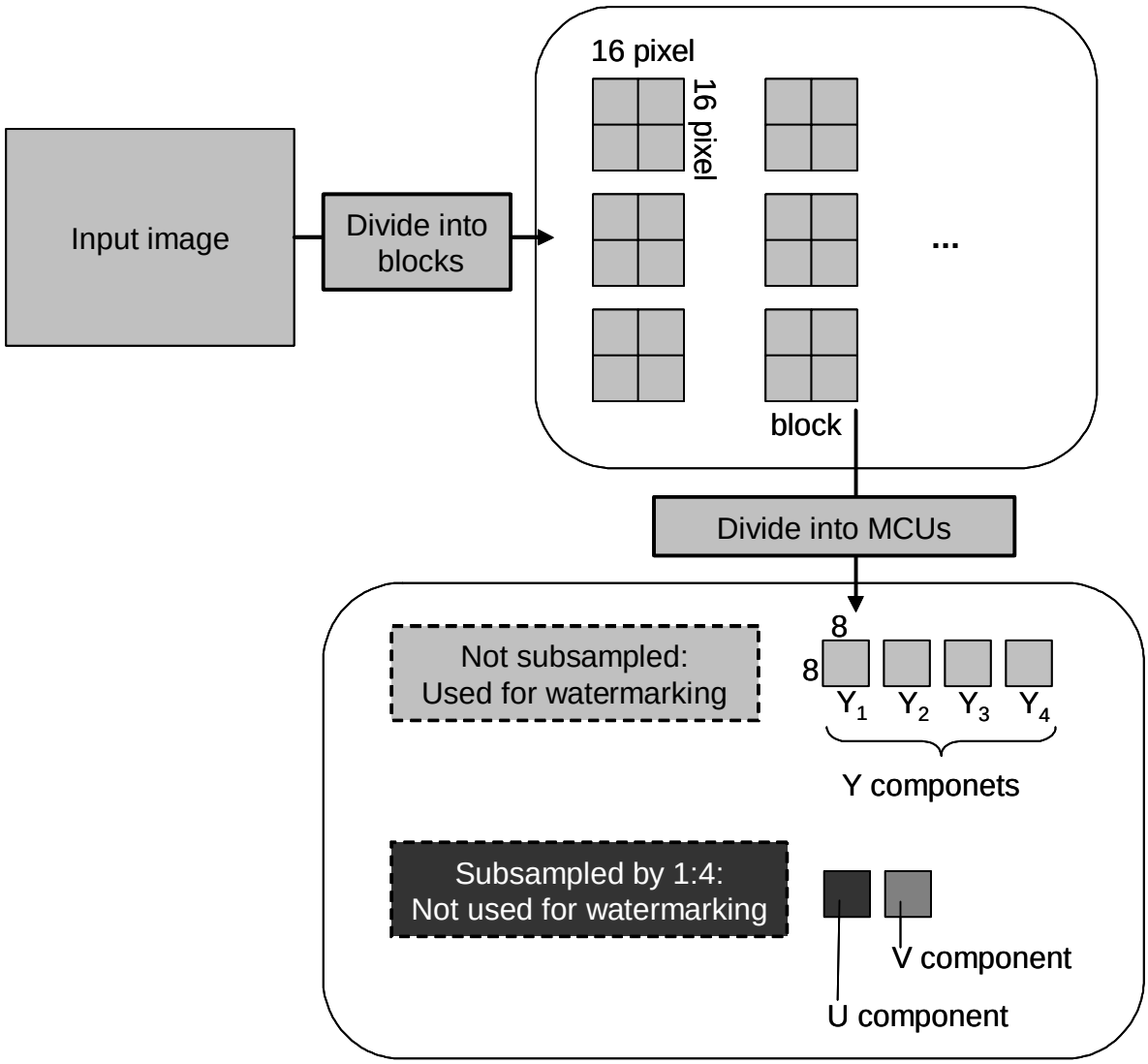


図 2.10 画像の MCU への分割と電子透かしに用いる成分の選択．輝度成分のみを埋め込みに用い，色差成分は用いない．

れる影響に気づきやすい．逆に，高周波数帯の変化には鈍く，多少の変化があっても気づきにくい．JPEG 圧縮ではその性質を利用し，低周波数帯には低圧縮，高周波数帯には高圧縮をかけるように設計されているため，高周波数帯では量子化後の係数を微小に変化させたとしても，逆量子化を行うと変化が大きく表れ，画像に表れる影響が目立ちやすい．そのため，DCT 係数の値を変化させたときに最も画像上の影響が小さいのは中間周波数領域となる．

図 2.11 電子透かしに YUV 全成分を用いた場合と Y 成分のみを用いた場合の比較.

電子透かしに用いる YUV 成分の選択

すでに述べたとおり電子透かしはデコードした画像の画質変化を引き起こす．同時に，もともと 0 値であった係数に 1 を埋め込んだ場合，ゼロランレングスの減少から圧縮効率も低下させてしまう．これらの影響は埋め込みに用いられる MCU の選び方によって変わる．ここでは，電子透かしの影響を抑えるための埋め込み成分の選択法を示す．

提案手法では JPEG 圧縮に 4:2:0 フォーマットを用いている．4:2:0 フォーマットでは，人間の視覚が色差成分のピクセル間変化を感じにくいことから，色差成分である UV 成分を共に 1:4 にサンプリングする．輝度成分である Y 成分はサンプリングされず，16×16 ピクセルのブロックから，8×8 の Y 成分が 4 個得られる．よって，図 2.10 に示すように，1 ブロックは 4 個の Y 成分と 1 個ずつの UV 成分の計 6 個のブロックに分けられる．さらに，色差成分と輝度成分には異なる量子化テーブルを用いることが可能であり，変化を感じにくい色差成分には輝度成分に比べ強い圧縮をかける．

ここで，電子透かしに用いる成分の違いによる影響を調べるため，YUV 成分全てを用いて電子透かしを行った場合と，サンプリングのされていない Y 成分のみに電子透かしを用いた場合の比較を示す．図 2.11 は原画像と，原画像の YUV 成分すべてに電子透かしを行った画像，原画像の Y 成分のみに電子透かしを行った画像，それぞれの画像の同一位置のブロックを抜き出したものである．なお，電子透かしを行った画像には，同じ埋め込みデータを同じ符号長埋め込んだ．YUV 成分全てを用いた場合，画像中に虹模様のようなノイズが発生していることがわかる．一方，Y 成分のみでは画像上に凹凸があるようなノイズが発生している．主観的な評価ではあるが，色成分に変化のある虹模様のノイズの方が目立ちやすいと感じられる．次に，表 2.1 に埋め込み後のブロックの原画像ブロックに対する PSNR(Peak Signal to Noise Ratio) と，埋め込み後ブロックの符号長を

表 2.1 PSNR とデータサイズの比較.

	PSNRs [dB]	Data length [KB]
YUV components	33.02	19.83
Only Y component	36.40	18.56

示す．画像サイズが $X \times Y$ である画像 I，J 間の PSNR の計算は式 (2.11) によった．

$$PSNR = 20 \times \log 10 \left(\frac{255}{\sqrt{\frac{\sum_{x=0}^{X} \sum_{y=0}^{Y} (I_{xy} - J_{xy})^2}{X \times Y \times 3}}} \right) \tag{2.11}$$

ここで，I_{xy} は画像 I の座標 (x, y) の R，G，B 値，J_{xy} は画像 J の座標 (x, y) の R，G，B 値を示す．

UV 成分を含めて電子透かしを用いる場合，Y 成分のみへの電子透かしに比べその影響が強く出ていることが示されている．これは，UV 成分があらかじめサブサンプリングされていることや，量子化の際に強い圧縮をかけゼロランレングスを多く生成するためと考えられる．よって提案手法では UV 成分を除き，Y 成分のみに電子透かしを用いることで, 圧縮効率の低下, 画質の劣化を抑える．このとき, 画像サイズを 320×240 ピクセルとすると, 埋め込みに用いることのできる MCU は, $320/16 \times 240/16 \times 4 = 300 \times 4 = 1200$ 個となる．

Masked image への埋め込み

電子透かしによるノイズが画像の局所に現れないよう，図 2.12 に示すように画像全体に均一に暗号化ストリームを埋め込む．Masked image が m 個の MCU を持つとき，まず，1 番目の MCU の 14 番目の DCT 係数の LSB を，暗号化ストリームの 1 番目のビットと置換する．次に，2 番目の MCU の 14 番目の DCT 係数の LSB を，暗号化ストリームの 2 番目のビットと置換する．同様にして，m 番目の MCU の 14 番目の DCT 係数の LSB は，暗号化ストリームの m 番目のビットと置換する．暗号化ストリームの符号長を L として，$L > m$ である場合，1 番目の MCU の $15(= 14 + 1)$ 番目の DCT 係数の LSB を，暗号化ストリームの $(m + 1)$ 番目のビットと置換する．したがって，$(j + 1)$ 番目の MCU の $(i + 14)$ 番目の DCT 係数の LSB は, 暗号化ストリームの $(i \times m + j + 1)$ 番目のビットと置換する．ここで，i は DCT 係数位置から 14 を引いたもの $(i = 0, 1, \ldots, 50)$,

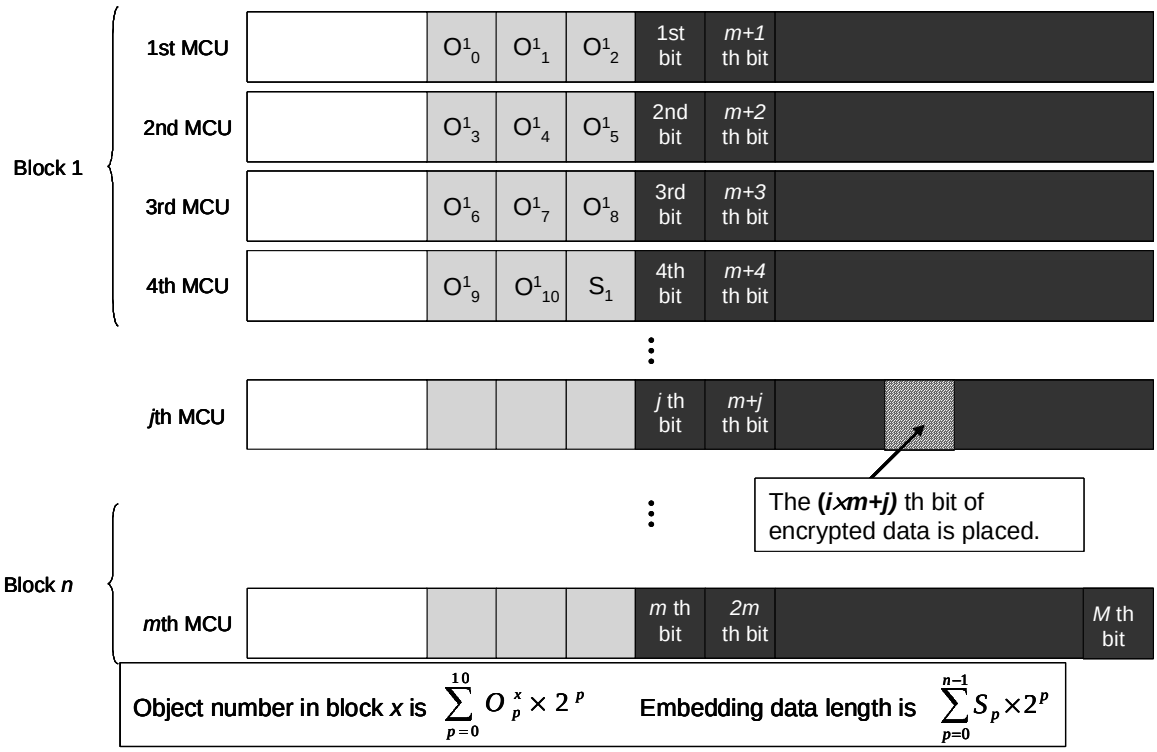


図 2.12 暗号化ストリームの DCT 係数への埋め込み手順

j は MCU の番号 $(j = 0, 1, \ldots, m-1)$ をそれぞれ示す．

埋め込み可能な係数のすべての LSB の個数を M 個とする．暗号化ストリームの符号長 L が $L > M$ であり，すべての LSB の個数を超える場合，埋め込み可能な係数の最下位から 2 ビット目 (2nd LSB) に埋め込む．このとき，1 番目の MCU の 14 番目の DCT 係数の 2nd LSB を，暗号化ストリームの $(M+1)$ 番目のビットと置換する．

デコーダにより，撮影画像を再構成するためには物体位置や，暗号化ストリームの符号長を知る必要がある．そこで，これらの情報は暗号化ストリームとは別に，図 2.9 に示す，DCT 係数の 11-13 番目の reserved area に埋め込む．オブジェクト番号は 16×16 ピクセルのブロック内の 4 つの MCU に図 2.12 に示すように埋め込む．各ブロックのオブジェクト番号は図 2.13 に示すように決定する．1 つのブロック内に複数のオブジェクトが存在する場合，ブロック内のピクセル数が最も多いオブジェクトの番号を割り当てる．いずれのオブジェクトもブロック中に存在しない場合にはオブジェクト番号 0 を割り当てる．1 つのブロック内の reserved area は 12 ビットあるが，そのうちの 11 ビットをオブジェクト番号に用いる．ブロック x のオブジェクト番号は，次の式で得ることができる．

$$\sum_{p=0}^{10} O_p^x \times 2^p$$

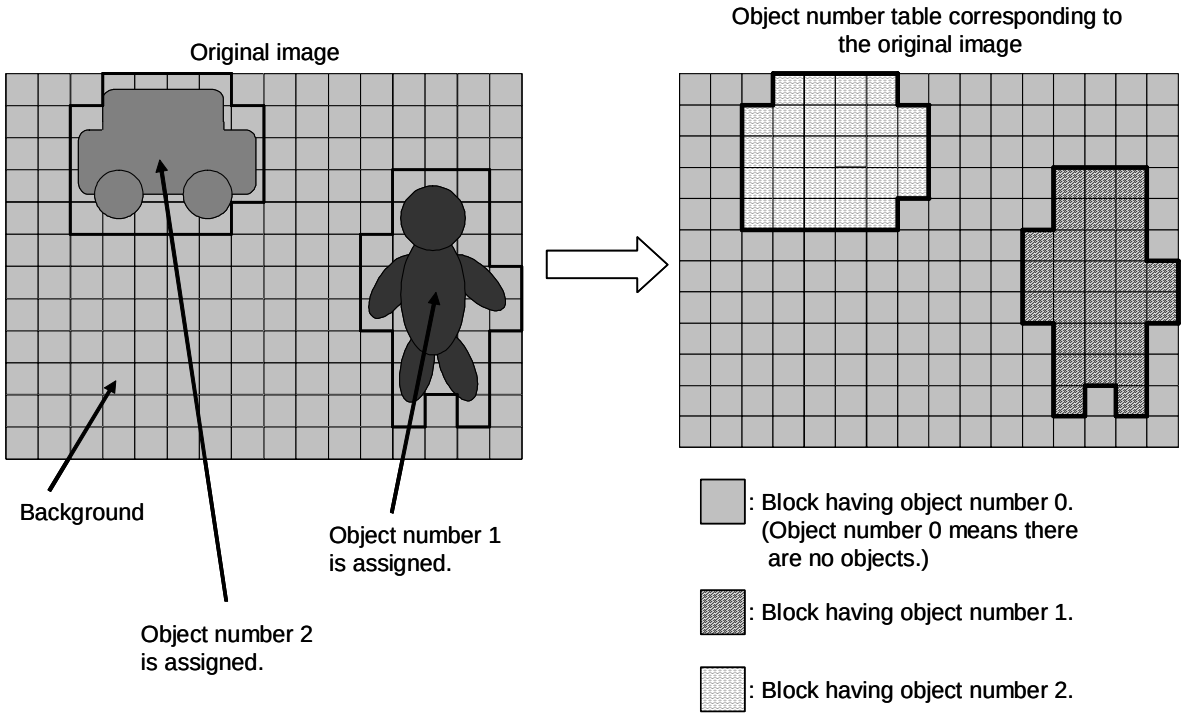


図 2.13 各ブロックのオブジェクト番号の決定

ここで，p は reserved area 内の埋め込み位置，O_p^x はブロック x 内の位置 p に埋め込まれたビット値を示す．

Reserved area の 12 ビットの残り 1 ビットは暗号化ストリームの符号長を表すのに用いる．暗号化ストリームの符号長は次の式で得ることができる．

$$\sum_{q=1}^{n} S_q \times 2^{q-1}$$

ここで，n は 16×16 ブロックの番号，S_q はブロック q に埋め込まれたビット値を示す．オブジェクト番号，暗号化ストリームの符号長をどのように用いるかは，第 2.5 節で説明する．

2.5　デコーダの構成

本節では reconstructing viewer による撮影画像の再構成について説明する．Masking される前の移動物体を表示するためには, JPEG ストリームを reconstructing viewer でデコードする．Reconstructing viewer に適切なパスワードを投入することで，エンコーダで暗号化され埋め込まれた移動物体を復元することができる．図 2.14 は reconstructing viewer による再構成のフローを示したものである．

なお，JPEG ストリームを normal viewer によってデコードすると，masked image が得られる．masked image へのデコードは JPEG フォーマットに基づく処理であるため，本論文では詳しい説明は省略する．

電子透かしによって埋め込まれた移動物体情報の抜き出し

JPEG ストリームから撮影画像を再構成するには，埋め込んだ暗号化ストリームを抜き出すことが必要である．まず，JPEG ストリームを標準の JPEG デコード処理と同様に，ハフマン復号し，量子化 DCT 係数に変換する．第 2.4.3 節に述べたように，量子化 DCT 係数には暗号化ストリームが埋め込まれている．そこで，次のように暗号化ストリームを抜き出す．まずは，各ブロックの reserved area に埋め込まれた暗号化ストリームの符号長を抜き出し，符号長を得る．次に，1 番目の MCU の 14 番目の DCT 係数の LSB を抜き出し，暗号化ストリームの 1 番目のビットを得る．さらに，2 番目の MCU の 14 番目の DCT 係数の LSB を抜き出し，暗号化ストリームの 2 番目のビットを得る．このようにして，$(j+1)$ 番目の MCU の $(i+14)$ 番目の DCT 係数の LSB から，暗号化ストリームの $(i \times m + j + 1)$ 番目のビットを得る．抜き出した，暗号化ストリームの符号長が，あらかじめ得た符号長に達したとき，量子化 DCT 係数からの抜き出しを終える．

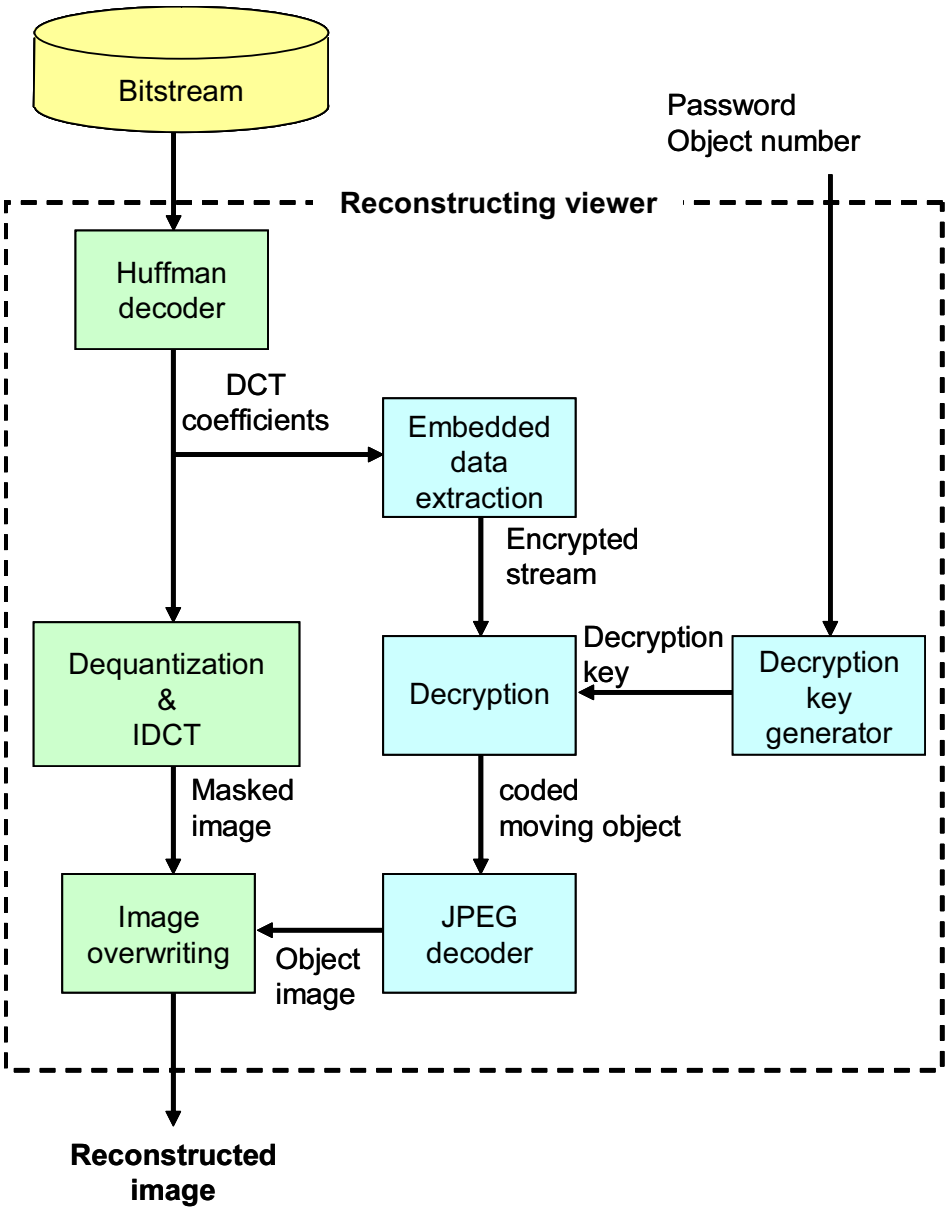


図 2.14 reconstructing viewer の構成

移動物体情報の復号

複数の移動物体のなかから，特定の移動物体のみを復元する方法を述べる．図 2.15 は復元の手順を示している．量子化 DCT 係数から抜き出した暗号化ストリームは複数の移動物体を暗号化したデータが連結している．ここでオブジェクト番号 k の物体を復元したい場合，第 2.4.2 節で coded moving object k を暗号化した鍵に対応する復号鍵を用いることで，目的の k 番目の物体のみを復元できる．物体 k に対応した復号鍵により暗号化ストリームを復号すると，coded moving object k と前後の識別子のみが正確に復元され，そのほかの coded moving object は鍵が異なるため復元できない．そこで，正確に復号できた識別子にはさまれたデータを取り出すことで，目的の coded moving object だけが得られる．

再構成画像の出力

抜き出した object data は JPEG デコーダにより移動物体画像にデコードできる．ここでは，移動物体画像を masked image の適切な位置に上書きし，撮影画像を再構成する．Masked image は JPEG ストリームを標準の JPEG デコーディングに則り処理をして作る．JPEG ストリームの各 16×16 ピクセルのブロックには電子透かしにより，オブジェクト番号が埋め込まれている．Coded moving object k から復元した移動物体画像を，masked image のオブジェクト番号 k を持つブロックに上書きする．これにより，オブジェクト番号 k を持つ物体のみを復元し，他の物体は masking されたままの再構成画像を作ることができる．この再構成画像では，目的の物体をもともとの撮影画像と同様に特定することでき，同時に，そのほかの物体はプライバシーを保護したままである．

また，すべての，もしくは複数の物体を復元した再構成画像が必要な場合には，coded moving object の復号を繰り返すことで，複数の物体を復元できる．

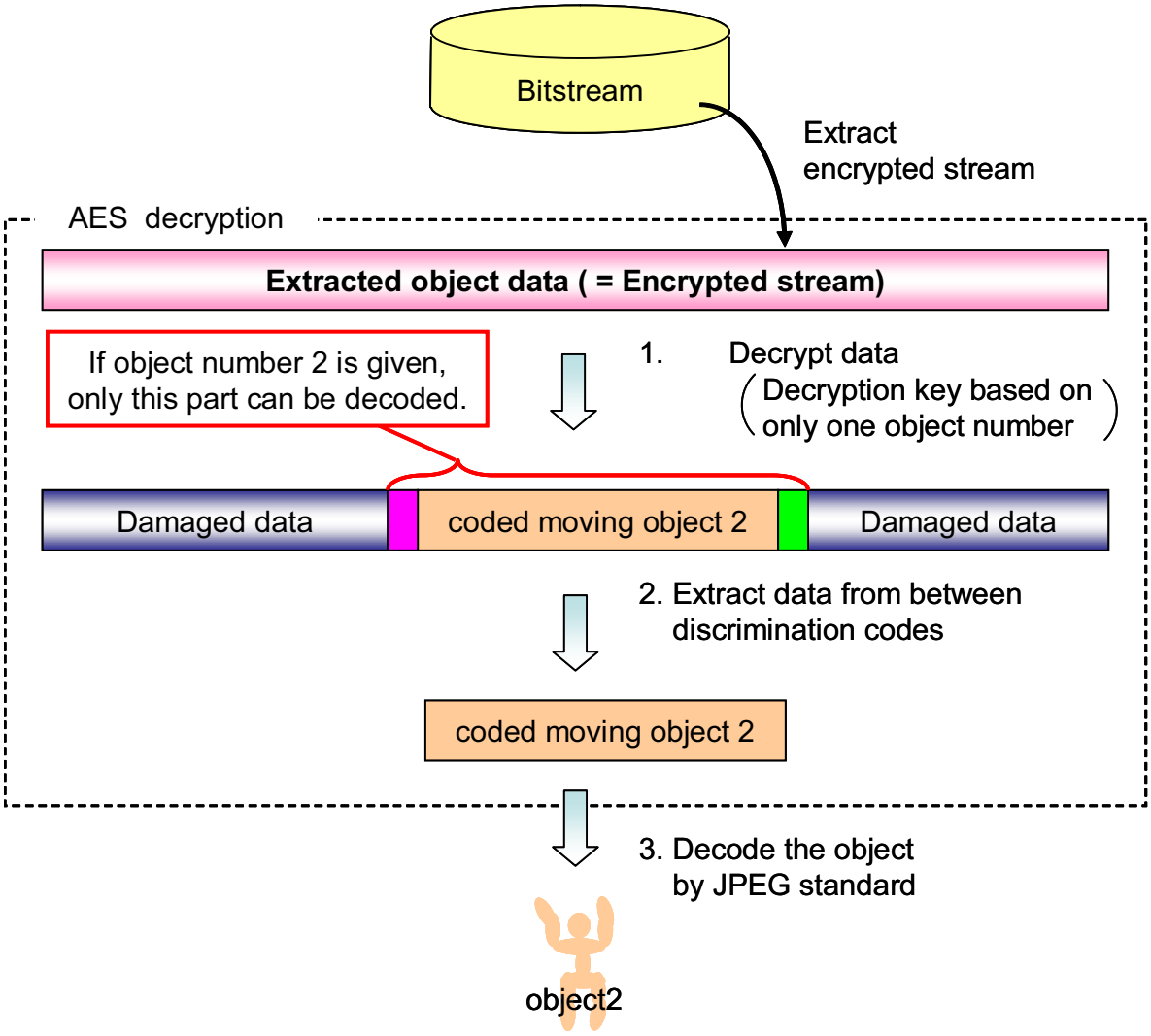


図 2.15 暗号化ストリームからの移動物体の復元

2.6 実験結果

本節では提案手法の実験結果と考察を示す．まず，第 2.6.1 節において，提案手法において masked image を作成し，撮影画像を再構成した結果を示す．また，同一人物を連続的に復元した結果も示す．第 2.6.2 節では，撮影画像中に存在する移動物体の大きさが変化するに伴って，埋め込む暗号化ストリームの符号長がどのように変わるかを示す．また，移動物体がどの程度の大きさ以内であれば本手法が適用できるかを示す．第 2.6.3 節では，移動物体の大きさの変化に応じて，出力 JPEG ストリームの符号長がどのように変化するかを示す．

なお，本章の実験で用いる撮影画像シーケンスは画像サイズ 320×240 ピクセル，ビット深度 24[bits/pixel] のものを用いた．

2.6.1 Reconstructing Viewer による移動物体の再構成

まず，提案手法によりエンコードした JPEG ストリームを normal viewer，reconstructing viewer のそれぞれによりデコードした結果を示す．撮影画像は 3 人の人物が存在するものを用いた．移動物体への masking には scrambling と erasing の 2 つを用いた．また，再構成画像は，それぞれ異なる人物を復元した画像を示す．

図 2.16 は撮影画像と masked image，再構成画像を示したものである．図 2.16(b)，(c) はエンコーダにより出力された JPEG ストリームを normal viewer でよりデコードして得られた masked image である．それぞれ，移動物体は scrambling，erasing されそれぞれの物体が誰であるかを特定することはできない．しかし，どちらの masked image も物体の形状がはっきりしているため，そこに 3 人の人物がいることがはっきりわかる．次に，reconstructing viewer を用いて移動物体を復元した結果を示す．図 2.16(d) は，オブジェクト番号 006 番の人物を復元するためのパスワードを，reconstructing viewer に投入して再構成した画像である．オブジェクト番号 006 番が割り当てられた左端の人物のみが復元されていることがわかる．同様に，図 2.16(e) は，オブジェクト番号 004 番の人物を復元した再構成画像である．画面中央の人物のみが復元されている．このように，提案手法は注目する物体のみを復元しながらも，そのほかの物体のプライバシーを保護したままにすることができる．また，図 2.17 は車を含む画像に提案手法を適用した結果である．人物以外の物体も同様に masking によるプライバシー保護が適用できることが示されている．

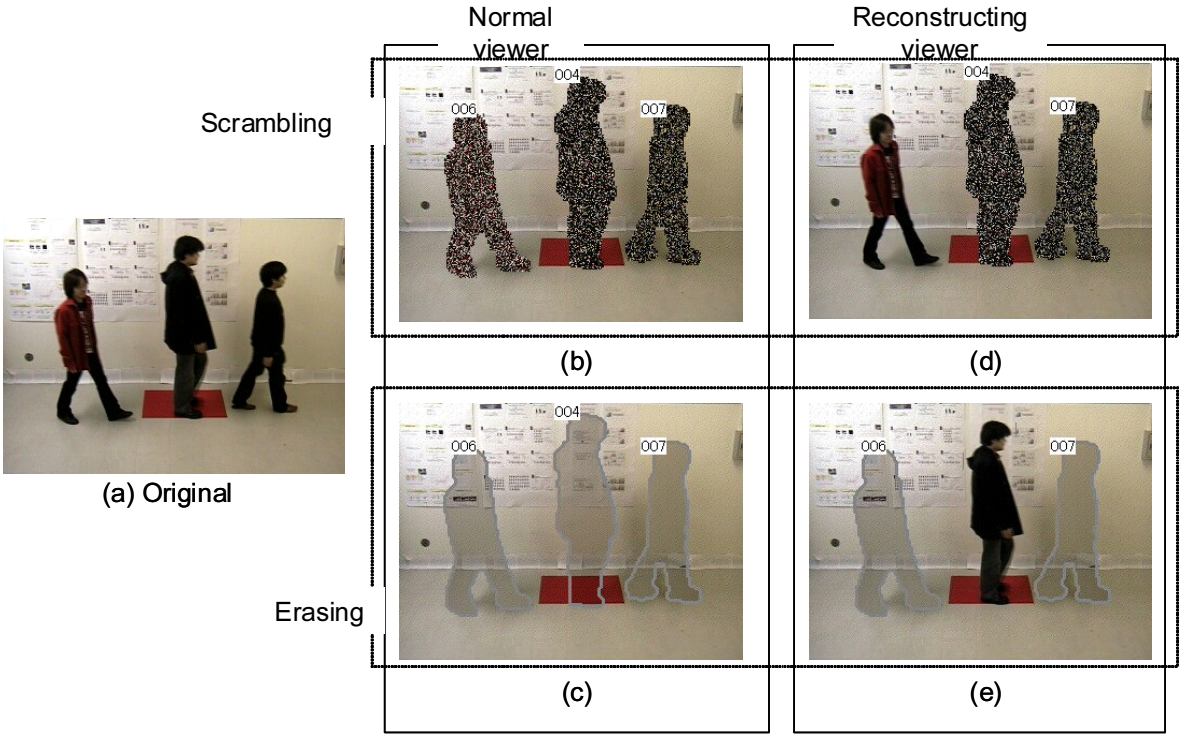


図 2.16 提案手法の適用結果．(a) 撮影画像，(b) Scrambling による masked image，(c) Erasing による masked image，(d) 図 (b) 中の 006 番の人物を復元した再構成画像，(e) 図 (c) 中の 004 番の人物を復元した再構成画像

次に，PSNR を指標として，提案手法を評価する．PSNR の算出には式 (2.11) を用いた．図 2.16，2.17 ともに，入力画像と，すべてのオブジェクトを復元した再構成画像間の，PSNR を求めた．それぞれの PSNR は 32.63[dB] および，31.70[dB] であり，これらの値はともに，“移動物体が誰，何であるか” や，“何が起こった画像であるか” が十分に判断できる画質であるといえる．

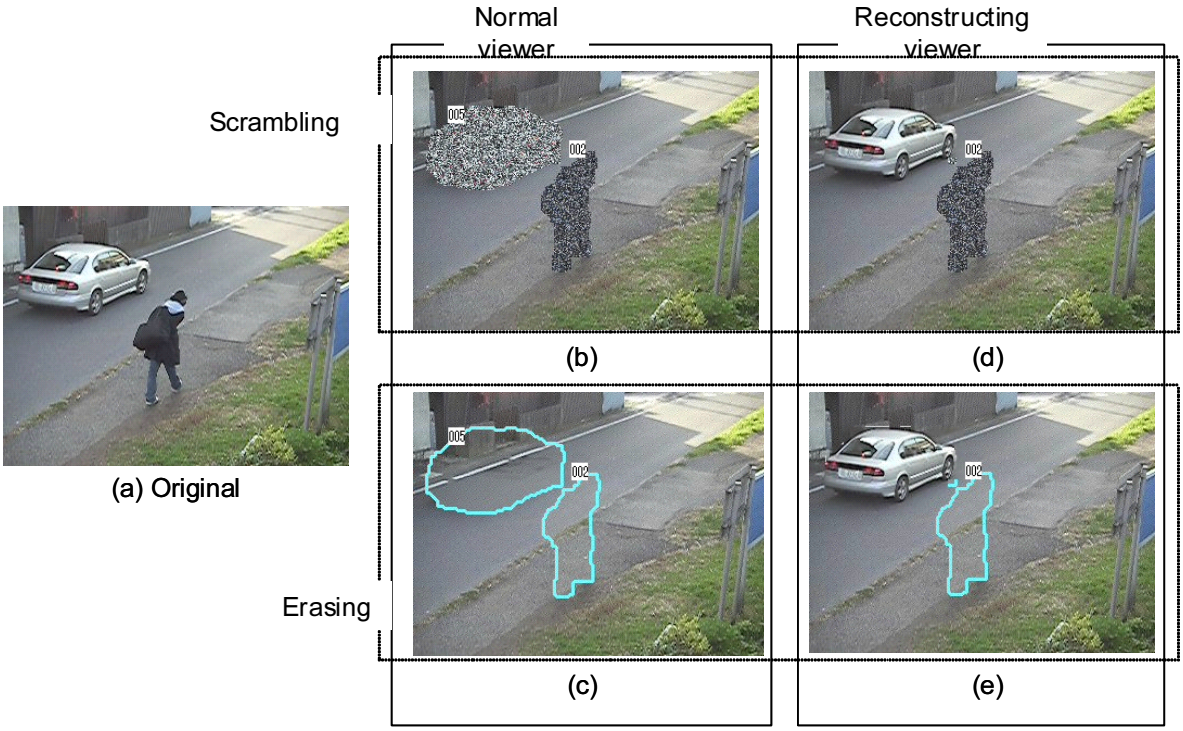


図 2.17 車を含んだ撮影データへの適用結果

同一移動物体の連続処理

ここでは連続的に入力される画像シーケンス中の同一移動物体を連続して復元した結果を示す．撮影画像は室内で二人の人物が左右に往復するシーンを撮影したものである．全 117 フレーム，その中で移動物体を含む画像は 78 フレームである．その中で 25〜63 フレーム目の masked image と再構成画像を 1 フレーム置きに計 20 枚ずつ示す．図 2.18 は normal viewer を用いて，出力ビットストリームを masked image としてデコードした画像である．図 2.19 は reconstructing-viewer を用いて，オブジェクト番号 001 番の人物を復元した再構成画像である．25〜37 フレーム目までは目的の人物しかシーン中に存在しないため，再構成画像中の移動物体は復元されたものだけである．39〜51 フレーム目には目的の人物と，プライバシーを保護したままにしたいもう一人の人物（オブジェクト番号 002 番）の二人が存在する．このときの再構成画像では左側の人物のみが復元されており，右側の人物は masking されたまま保たれている．また，残りの 53〜63 フレーム目ではオブジェクト番号 001 番が付与された移動物体がシーン中に存在しないため，再構成画像と masked image は同一の画像となっている．

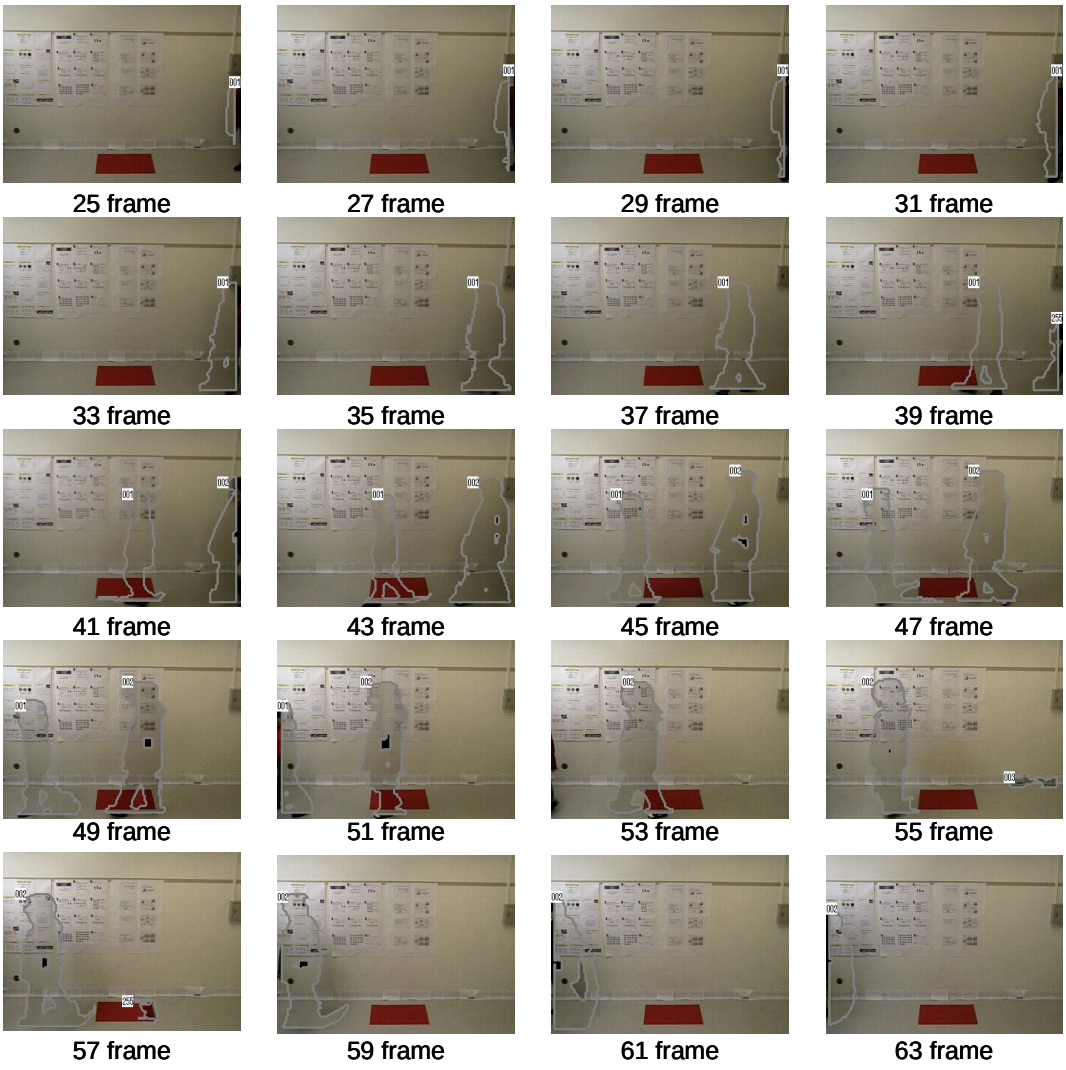


図 2.18 撮影画像を連続処理したときの masked image.

図 2.19 撮影画像を連続処理したときの再構成画像．オブジェクト番号 001 番の人物を再構成した．

2.6.2 撮影画像中の移動物体の大きさと埋め込み限界の考察

本節では暗号化ストリームの符号長と画像中の移動物体の大きさとの関係を示す．また，この関係性から，電子透かしに LSB のみを用いた場合，および，2nd LSB まで用いた場合に，どの程度の大きさの移動物体まで提案手法を適用できるのかを示す．図 2.20 は横軸を撮影画像中に移動物体が占める割合，縦軸を暗号化ストリームの符号長として，その関係性を示したグラフである．ここで，暗号化ストリームを作る際の移動物体画像の量子化には，低圧縮用量子化テーブル *Low*（表 2.2）と高圧縮用量子化テーブル *High*（表 2.3）の 2 種類を用いた．低圧縮用量子化テーブル *Low* は，第 2.6.1 節において masked image の圧縮に用いたものと同一の量子化テーブル，高圧縮用量子化テーブル *High* は量子化テーブル *Low* よりも高い圧縮率の量子化テーブルである．用いた画像シーケンスは，複数の移動物体を含む様々なシーンのものを用いた．フレーム数は全部で 999 である．図 2.20 の水平な 2 本の線はそれぞれ，電子透かしに LSB のみを用いた際に埋め込める最大符号長，電子透かしに 2nd LSB まで用いた際に埋め込める最大符号長を示している．本実験では，電子透かしに用いるブロックを $320/16 \times 240/16 \times 4 = 1200$ 個としている．したがって，埋め込める限界となる符号長は，LSB のみを用いた場合では $1200 \times (64 - 14 + 1) = 61200[\text{bit}] = 7650\text{byte}$，2nd LSB まで用いた場合は $61200 \times 2 = 122400[\text{bit}] = 15300\text{byte}$ である．

このグラフより，埋め込める移動物体の最大の大きさが推測できる．移動物体の大きさが画面の 40% 以内である場合には，移動物体画像の圧縮に低圧縮用量子化テーブル *Low* を用いても，LSB にすべての暗号化ストリームを埋め込むことができた．移動物体の大きさが画面の 40% を超えた場合には，電子透かしに 2nd LSB まで用いるか，移動物体画像を高圧縮用量子化テーブル *High* で圧縮する必要がある．さらに，移動物体の大きさが 85% を超える場合には，移動物体画像を高圧縮用量子化テーブル *High* で圧縮し，さらに電子透かしに 2nd LSB まで用いなければ暗号化データをすべて埋め込むことはできない．本実験結果より，移動物体画像に高圧縮をかけ，埋め込み係数を拡大することで，画面全体を移動物体が占める場合にも，提案手法が適用できることが示された．

ここで，第 2.6.1 節で示した提案手法の実行例，図 2.16，図 2.17 において，移動物体が画面を占める割合は，それぞれすべての移動物体の大きさをあわせても 39% と 20% である．そのため，これらの例ではすべての移動物体を低圧縮用量子化テーブル *Low* で圧縮し，暗号化ストリームを LSB のみを用いることで埋め込むことができる．

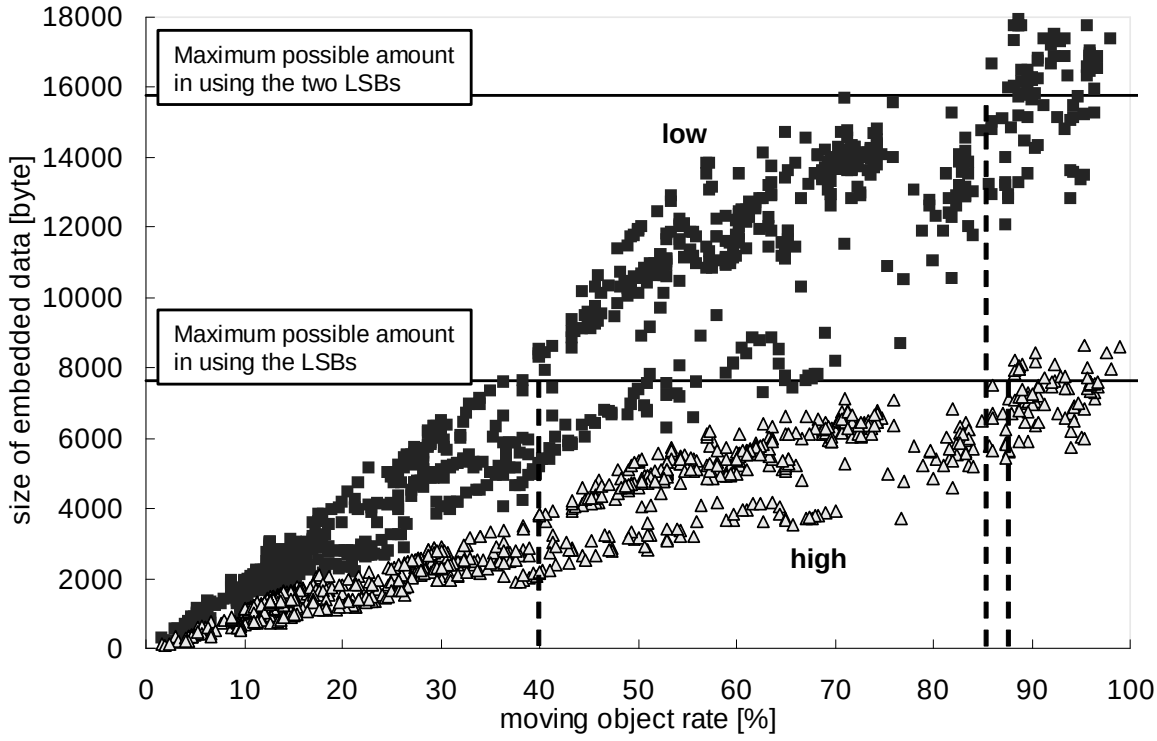


図 2.20 撮影画像中に存在する移動物体の大きさと暗号化ストリームの符号量の関係．移動物体画像は低圧縮 (Low) もしくは高圧縮 (High) のいずれかで量子化されたものを示す．画像中には電子透かしに LSB のみを用いた場合，2nd LSB を用いた場合の最大の埋め込み量を示している．

表 2.2 低圧縮用量子化テーブル *Low*

3	2	2	3	5	8	10	12
2	2	3	4	5	12	12	11
3	3	3	5	8	11	14	11
3	3	4	6	10	17	16	12
4	4	7	11	14	22	21	15
5	7	11	13	16	21	23	18
10	13	16	17	21	24	24	20
14	18	19	20	22	20	21	20

(a) Y component

3	4	5	9	20	20	20	20
4	4	5	13	20	20	20	20
5	5	11	20	20	20	20	20
9	13	20	20	20	20	20	20
20	20	20	20	20	20	20	20
20	20	20	20	20	20	20	20
20	20	20	20	20	20	20	20
20	20	20	20	20	20	20	20

(b) U and V component

表 2.3 高圧縮用量子化テーブル *High*

13	9	8	13	19	32	41	49
10	10	11	15	21	46	48	44
11	10	13	19	32	46	55	45
11	14	18	23	41	70	64	50
14	18	30	45	54	87	82	62
19	28	44	51	65	83	90	74
39	51	62	70	82	97	96	81
58	74	76	78	90	80	82	79

(a) Y component

14	14	19	38	79	79	79	79
14	17	21	53	79	79	79	79
19	21	45	79	79	79	79	79
38	53	79	79	79	79	79	79
79	79	79	79	79	79	79	79
79	79	79	79	79	79	79	79
79	79	79	79	79	79	79	79
79	79	79	79	79	79	79	79

(b) U and V component

2.6.3　Masked Image の符号長の変化

本節では，出力 JPEG ストリームの符号長と画像中の移動物体の大きさとの関係を示す．図 2.21 は，横軸を，前節と同様に，撮影画像中に移動物体が占める割合，縦軸を出力 JPEG ストリームの符号長と撮影画像の符号長の比率として，その関係性を示したグラフである．撮影画像の符号長は画像サイズ $X \times Y$ ピクセル，ビット深度 B[bits/pixels] としたとき，$X \times Y \times B$[bits] で求めることができる．本章の実験では，撮影画像は 320×240 ピクセル，ビット深度 24[bits/pixels] であるため，その符号長は 1843200[bit]=225[Kbyte] である．出力 JPEG ストリームを作成する際の量子化は，masked image の圧縮には量子化テーブル *Low* のみ，移動物体画像には，量子化テーブル *Low*，*High* の 2 種類を用いた．図 2.21 の Low，High の表記は，移動物体画像の量子化に適用した量子化テーブルの種類を示している．実験に用いた画像シーケンスは第 2.6.2 節で用いたものと同一のもの，999 フレームを用いる．

画像中に存在する移動物体が小さく，おおよそ 10% 程度までの場合，移動物体画像の圧縮にどちらの量子化テーブルを使っても，あまり符号長の違いはなく，符号長の比率はおおよそ 0.05 ～ 0.09 である．移動物体の占める割合が画面中の 25% 程度におさまる場合，移動物体画像の量子化に量子化テーブル *Low* を用いても，符号長の比率が 0.10 を超えない．移動物体が大きくなるにつれて，量子化テーブル *Low* を用いた場合の符号長の増加が顕著になるが，移動物体が画面のほとんどを覆っても，その比率は 0.20 を超えることが無い．提案手法は，出力ストリームに多量のデータを埋め込むが，十分な画像圧縮効果が保たれている．

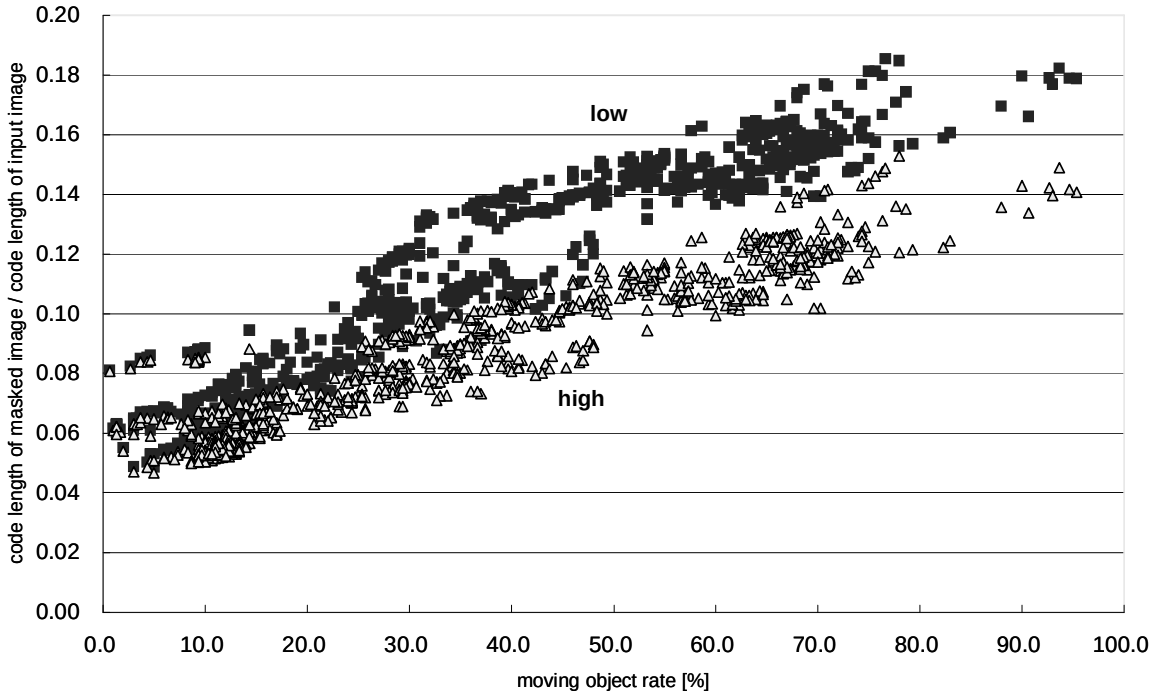


図 2.21 撮影画像中の移動物体の大きさと出力 JPEG ストリームの符号長の関係

2.7　本章のまとめ

本章では，固定モニタカメラにより構成される監視カメラシステムにおける，撮影画像中の移動物体に対するプライバシー保護手法を提案した．撮影画像から背景差分法により抽出した移動物体領域を画像処理により識別不能とした．さらに，物体を識別するため，もともとの移動物体画像を，出力ビットストリーム内に電子透かしを使って埋め込むことにより，撮影画像の再構成を可能にした．提案手法では，抽出移動物体をトラッキングし，その情報を用いることで移動物体を個別に処理することでき，複数の人物から特定の人物を選んで復元したり，複数フレーム間で注目する人物のみを連続して復元できる．これにより，たまたま注目物体と同時に画面内に映り込んでしまった監視不要の物体が，注目物体とともに復元されることを避けることができ，再構成画像の上でもプライバシー保護を損なうことがない．電子透かしによって暗号化ストリームを出力 JPEG ストリームに埋め込んだため，外部からデータを与えずに出力 JPEG ストリームのみで移動物体を再構成できた．電子透かしを用いるため，適用可能な移動物体の大きさに限界があることや，出力 JPEG ストリームの圧縮効率の大幅な低下，が考えられるが，第 2.6 節の実験の結果，画面全体を移動物体が覆っていても，移動物体情報がすべて埋め込めること，出力 JPEG ストリーム中に限界まで暗号化ストリームを埋め込んでも，圧縮率は 0.20 より悪くならないことが示された．実行例で適用した，複数の人物が十分に認識，識別できる程度の大きさで映っていた画像では，画像中の移動物体が占める割合は約 40% であり，このときの圧縮率は 0.08 ～ 0.14 程度であった．これより，提案手法は監視カメラシステムにおけるプライバシー保護と，移動物体の追跡を両立する手法として有効であるといえる．

第 3 章

真正性証明とプライバシー保護を両立する手法

3.1 はじめに

前章では，監視カメラでのプライバシー保護を実現する技術的な手法について述べた．撮影画像内に映りこんだ移動物体を masking して，プライバシーを保護した．さらに，犯罪捜査などのために，オリジナルの移動物体を復元し撮影画像を再構成することで，被撮影者の特定を可能にした．ここで，再構成画像が法廷や犯罪捜査などの場で証拠能力を確保するには，撮影画像に対して改竄あるいは合成されたものではないことを示さなければならない，という課題がある．そこで本章では，移動物体を masking したままで，再構成して得られる画像が撮影画像に対して真正であることを証明する手法を提案する．

提案手法では，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両立する．撮影画像と再構成画像間に人が検知できる変化がないことを，公開鍵を用いて暗号化した画像ストリームを使って，移動物体を復元せずに検証する．RSA 公開鍵暗号方式を用いているため，真正性検証のアルゴリズムと公開鍵を公開することで，誰にでも真正性の検証が行える．この検証は移動物体を復元することなく実行できるため，秘密鍵を知る管理者のみならず，秘密鍵を知らないユーザでも画像真正性を検証でき，さらに，プライバシーが公開されない．提案手法は，前章に述べた手法と同様に，出力 JPEG ストリーム中に画像復元情報と真正性検証情報を埋め込む．このとき，電子透かしによる埋め込み係数位置をあらかじめ固定せず，ハフマン符号化の特性に基づき選択的に用いることで，符号量の増加を抑える．

3.2　移動物体の復元を必要としない真正性証明手法

本節では提案手法の構成について説明する．図 3.1 は提案手法のフローである．提案手法は（a）入力部，（b）プライバシー保護部，（c）真正性証明部，（d）画像出力部の 4 つにより構成される．以下，各構成部のアルゴリズムを詳細に説明する．

3.2.1　（a）入力部

前章では監視カメラから入力される画像形式はビット深度 24[bits/pixel] のものとしたが，本章の提案手法では，撮影画像は監視カメラにより JPEG 圧縮されるものとする．真正性証明とプライバシー保護機能を備えた監視カメラシステムを実現するため，監視カメラには AES などの暗号化機能 [29][30] が組み込まれ，撮影された画像は JPEG 圧縮された後，必ず暗号化されて出力されるものとする．提案システム（authentication and privacy protection system）は復号機能を持ち，監視カメラから入力された暗号化 JPEG ストリームを JPEG ストリームへ復号してから以降の処理を行う．監視カメラと提案システムは秘匿された共通鍵を持ち，監視カメラの出力を不正に取得し撮影画像を流出させることや，提案システムへ直接改竄画像を入力することを防ぎ，監視カメラで撮影した画像のみが提案システムへ入力されることを保障する．復号された JPEG ストリームにハフマン復号を行い，量子化 DCT 係数に変換する．量子化 DCT 係数は（b）プライバシー保護部，（c）真正性証明部，（d）画像出力部のそれぞれに送られる．

3.2.2　（b）プライバシー保護部

プライバシー保護部では，移動物体の抽出と物体の masking を行う．まず，入力部から送られた量子化 DCT 係数に逆量子化，逆 DCT を行いピクセル単位の画像データに変換する．次に，入力画像から移動物体の抽出を行う．移動物体の抽出には前章と同様に背景差分法を用いた．

抽出した移動物体に masking を行う．本章では，図 2.7 に示した 4 手法 (Scrambling, Erasing，Defocusing，Mosaicing) とは異なり，移動物体全体を単一色で塗りつぶして masking する．背景差分により移動物体領域判別された領域内の全ピクセルを，明るさと視覚的な自然さを考慮して $(R, G, B) = (171, 172, 163)$ で置換した．JPEG 圧縮では同一の色が連続している場合には，圧縮効率が高くなるため，単一色で塗りつぶすと符号長の減少が期待できる．masking された画像を 16×16 ピクセルのブロックに分割する．その中で，masking を行ったピクセルを含むブロックのみ，DCT，量子化を行い，再び量子化 DCT 係数に変換する．変換したブロックの量子化 DCT 係数により構成される，

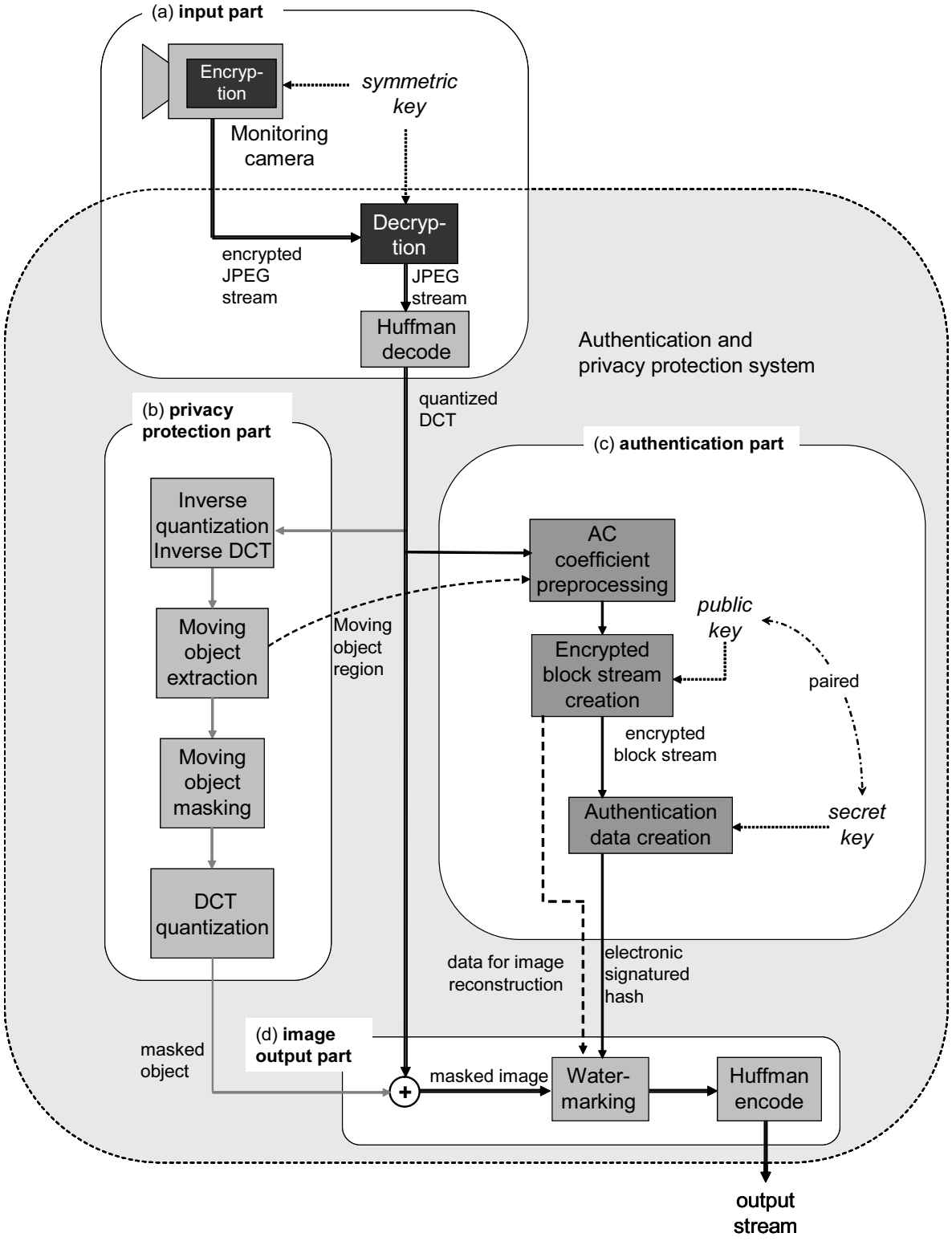

(a) input part
Encryp-tion
symmetric key
Monitoring camera
Decryp-tion
encrypted JPEG stream
JPEG stream
Huffman decode
Authentication and privacy protection system
quantized DCT
(b) privacy protection part
(c) authentication part
Inverse quantization Inverse DCT
AC coefficient preprocessing
public key
Moving object extraction
Moving object region
Encrypted block stream creation
paired
encrypted block stream
Moving object masking
Authentication data creation
secret key
DCT quantization
data for image reconstruction
electronic signatured hash
(d) image output part
masked object
masked image
Water-marking
Huffman encode
output stream

図 3.1 システムフロー

masking された移動物体画像 (masked object) を（d）画像出力部に送る．また，移動物体抽出処理により得られた，移動物体領域の情報 (moving object region) は (c) 真正性証明部で再び使う．

3.2.3 （c）真正性証明部

真正性証明部では，再構成画像の真正性を証明するために用いる真正性検証用データと，masked image から撮影画像を再構成する際に使う撮影画像復元用データを作成する．

DCT 係数の前処理と暗号化ブロックストリームの生成

まず，暗号化ブロックストリームの生成の説明で用いる用語を説明する．量子化 DCT 係数によって構成される撮影画像を，16 × 16 ピクセルのブロックに分割したものを，ブロックストリーム (block stream) と呼ぶ．また，ブロックストリームをそれぞれ公開鍵によって暗号化したものを，暗号化ブロックストリーム (encrypted block stream) と呼ぶ．

次に，暗号化ブロックストリームの生成方法について述べる．図 3.2 は暗号化ブロックストリームの生成手順を示したものである．まず，(a) 入力部より得た撮影画像から，ブロックストリームを生成する．撮影画像の量子化 DCT 係数を，輝度 (Y) 成分と色差 (UV) 成分に分け，さらに輝度成分を DC 成分と AC 成分に分ける．色差成分のすべての係数と，輝度成分の DC 成分はその値のまま変更せず，輝度成分の AC 成分のみを式 (3.1) により変更する．

$$ac\prime = \begin{cases} sign \times 2 \left\lfloor \frac{|ac|}{2} \right\rfloor & \text{移動物体を含まないブロック} \\ ac & \text{移動物体を含むブロック} \end{cases} \tag{3.1}$$

ここで，ac は AC 成分の値，$sign$ は AC 成分の正負を表す．また，$\lfloor x \rfloor$ は x を超えない最大の整数を示す．ブロック中の移動物体の有無は，(b) プライバシー保護部での移動物体の抽出結果により判別する．第 3.2.4 節の「電子透かしによる埋め込み」において，出力ストリームの量子化 DCT 係数には，真正性検証用データと撮影画像復元用データを電子透かしにより埋め込む．そのため係数の変化が生じるが，あらかじめ式 (3.1) により前処理を行うと，電子透かし後も同じ処理を行うことで，同一の量子化 DCT 係数に戻すことができる．この AC 成分の変更による画像の変化はわずかであり，人が検知できるほどの変化は起こらない．式 (3.1) による輝度成分の AC 成分の変換の後，量子化 DCT 係数を JPEG の圧縮単位である 16 × 16 ピクセルのブロックに分割し，ブロックストリームを作る．次に，それぞれのブロックストリームを公開鍵を用いて RSA 暗号化する．これにより，暗号化ブロックストリームが生成できる．いずれのブロックストリームも同一の

公開鍵を使って，暗号化ブロックストリームに暗号化する．

撮影画像から得られる全ての暗号化ブロックストリームを，真正性検証用データの作成プロセスに送る．また，移動物体を含むブロックは撮影画像復元用データ (data for image reconstruction) として，（d）画像出力部の電子透かしプロセスへ送る．

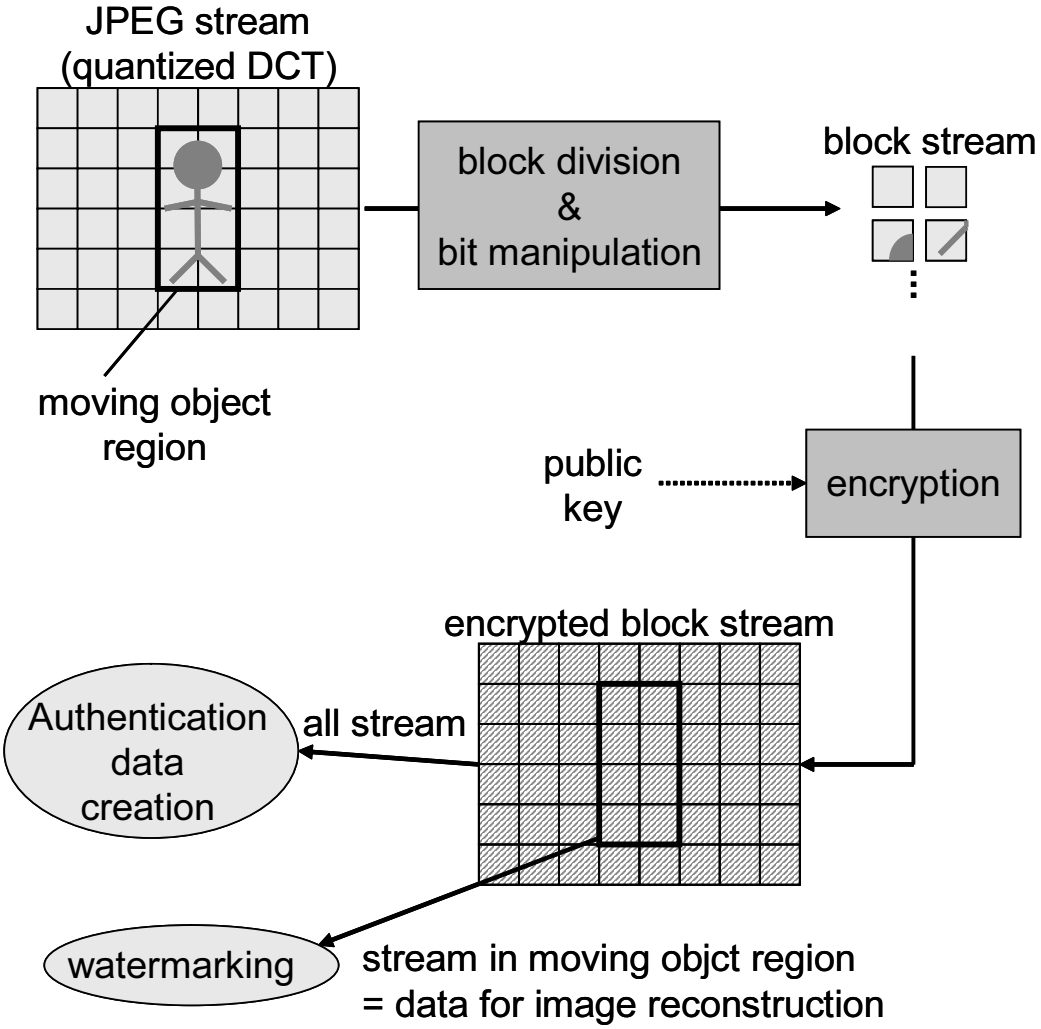


図 3.2 暗号化ブロックストリームの生成

真正性検証用データの作成

次に，暗号化ブロックストリームを用いて，画像真正性の証明に用いる検証用のデータを作成する．

まず，ブロックごとに生成した暗号化ブロックストリームを結合し，一本のストリームにまとめる．次に，ハッシュ関数を用いて結合したストリームからハッシュ値を計算する．このハッシュ値に電子署名し，署名文を真正性検証用データ (electronic signatured hash) とする．真正性検証用データは，撮影画像復元用データと同様に（d）画像出力部の電子透かしプロセスへ送られる．署名文の作成に用いる鍵は，ブロックストリームから暗号化ブロックストリームへ暗号化した際に用いた公開鍵と対になる秘密鍵を用いる．RSA 公開鍵暗号方式は，公開鍵と暗号鍵を逆に使い，署名を作成できる性質を持つ．ただし，一般の公開鍵暗号方式では，必ずしもこの性質は保障されない．

3.2.4 （d）画像出力部

画像出力部には，(a) 入力部から撮影画像の量子化 DCT 係数，(b) プライバシー保護部から masked object，(c) 真正性証明部から撮影画像復元用データと真正性検証用データ，がそれぞれ入力される．これらの入力を使い，画像出力部では masked image の作成と，masked image への電子透かしによるデータ埋め込みを行う．

Masked image の作成

(a) 入力部から送られた，量子化 DCT 係数のうち移動物体を含むブロックのすべての係数を，(b) プライバシー保護部で作成した，移動物体を masking したブロックの量子化 DCT 係数 (masked object) で置き換え，masked image を作成する．移動物体を含まないブロックは監視カメラから入力された撮影画像の JPEG の量子化 DCT 係数のまま残す．

電子透かしによる真正性検証データと撮影画像復元データの埋め込み

masked image の量子化 DCT 係数を輝度成分と色差成分に分割する．さらに輝度成分を，DC 成分と AC 成分に分割する．埋め込みには，第 2.4.3 節での，埋め込みに用いる成分と画質や符号長に与える影響の議論に基づき，輝度成分の AC 成分のみを用いる．

提案手法では，JPEG 圧縮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ることのできる埋め込み係数選択方法を用いる．ハフマン符号化はハフマンテーブルに従って行われる．ここで，ハフマンテーブルは，圧縮対象の画像を変換した量子化 DCT 係数がとる値の出現頻度を元に，最適なものを決めることができる．しかし，画像ごとに最適

表 3.1 ゼロランレングスが 0 の場合のハフマンテーブル．付加ビットの先頭 S は入力値が正のとき 1，負のとき 0 となる．また，x は入力値に応じて 0 か 1 が決まることを示す．

入力値の絶対値	ハフマン符号	付加ビット
512 ∼ 1023	1111111110000011	Sxxxxxxxxx
256 ∼ 511	1111111110000010	Sxxxxxxxx
128 ∼ 255	1111110110	Sxxxxxxx
64 ∼ 127	11111000	Sxxxxxx
32 ∼ 63	1111000	Sxxxxx
16 ∼ 31	11010	Sxxxx
8 ∼ 15	1011	Sxxx
4 ∼ 7	100	Sxx
2,3	01	Sx
1	00	S

テーブルを求めるのは処理時間を要する．そのため，JPEG 規定の Annex K による標準テーブルを用いることが多い．提案手法では，この Annex K による標準テーブルを用いた上で，符号量の変化が生じない係数を，埋め込み位置に選ぶ．表 3.1 は AC 成分に対するハフマンテーブルの一部を示したものである．ただし，表 3.1 はゼロランレングスが 0 の場合，つまり，入力値の直前に連続した 0 値が無い場合のものを示している．また，表中の付加ビットの項は，S が入力値の正負により，正のとき 1，負のとき 0 を示すことを示し，x は入力値に応じた値をとることを示す．

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．例えば，入力値が 10，ゼロランレングスが 0 である場合には，表 3.1 より入力値が 8 ∼ 15 のグループに属するため，ハフマン符号が 1011 となり，付加ビットは 10 を 2 進数表記した 1010 となる．よって，10111010 と符号化される．ハフマン符号は，それぞれが固有であり，重複するパターンが無いように選ばれている．そのため，ハフマン復号の際には，ビット単位でストリームを読み込むと，いずれかのハフマン符号が該当し，そのハフマン符号を元に付加ビットを取り出すと一意に係数値が復号できる．この例では，前半 4 ビットの 1011 が，ゼロランレングス 0 の入力値が 8 ∼ 15 であるグループを示すハフマン符号であることがわかり，さらにその後ろに長さ 4 ビットの付加ビットが続くことがわかるため，1010 を 10 進数に直した 10 を得ることができる．

ここで，入力値を，ハフマン符号が同一グループ内の他の値に変更しても，付加ビット

が変化するだけで，ハフマン符号化後の符号長は変化しない．入力値の正負を変えないとすると，入力値が 2 を超える場合には，符号長を変化させずに付加ビットを変更することができる．AC 成分の入力値を ac として，ac のとる値により，係数を $|ac| \geq 2$ のグループと $|ac| \leq 1$ のグループに分け，$|ac| \geq 2$ のグループの係数へ優先的に埋め込みを行う．しかし，符号長の変化はなくても，画像へデコードすると画質への影響は生じる．そのため，付加ビットを大きく変更すると画質に許容できない劣化が生じる．画像の変化を抑えるため，変更は最下位ビットのみとする．式 (3.2) は入力値 ac と埋め込みビット $b(\in 0, 1)$，電子透かし後の係数 $ac_{(w)}$ の関係を表した式である．

$$ac_{(w)} = sign \times \left(2 \left\lfloor \frac{|ac|}{2} \right\rfloor + b \right) \tag{3.2}$$

また，$|ac| \geq 2$ のグループの全ての係数を用いても，埋め込みデータが残っている場合，$|ac| \leq 1$ のグループへ残りを埋め込む．このグループへの埋め込みも式 (3.2) を用いる．しかし，$ac = 0$ と $|ac| = 1$ の間で入力値が変化すると，ハフマン符号や付加ビットの長さが変化し，$|ac| \geq 2$ のグループへの埋め込みと異なり符号長が変化する．

JPEG 圧縮は，高周波帯域で計数値に 0 が連続することが多く，AnneX K の標準化テーブルでは，ゼロランレングスを高い圧縮効率で圧縮できようになっている．表 3.2 は，ゼロランレングスが 5 のとき，つまり，入力値の前に連続した 0 が 5 個ある場合のハフマン符号である．入力値が $\{0, 0, 0, 0, 0, 4\}$ であるとき，ハフマン符号 1111111110011110 であるため出力符号は 11111111110011110100 の 19 ビットとなる．ここに $\{1, 1, 1, 1, 1, 0\}$ を埋め込むと入力値が $\{1, 1, 1, 1, 1, 4\}$ となり，ゼロランレングス 0 入力値 1 の出力符号は 001，ゼロランレングス 0 入力値 4 の出力符号は 100100 であるため，出力符号は 001001001001001100100 の 21 ビットとなる．また，逆に入力値 $\{1, 1, 1, 1, 1, 4\}$ に $\{0, 0, 0, 0, 0, 0\}$ を埋め込むと，出力符号長は 21 ビットから 19 ビットに減少する．このように $ac = 0$ の係数に $b = 1$ を埋め込む，もしくは $|ac| = 1$ の係数に $b = 0$ を埋め込むと，符号長が変化する．もともと量子化 DCT 係数の値は 1 より 0 をとることが多いため，$|ac| \leq 1$ のグループへの埋め込みを行うと，係数値が 0 から 1 になることによって，ほとんどの場合で符号長が増大する．

この手法を用いたときの限界となる埋め込みデータ量は画像サイズに依存し，例えば 640×480 ピクセルの画像では約 37[Kbyte] まで埋め込むことができる．JPEG ファイルの符号長は圧縮率や画像の性質により変化するが，実験的に監視カメラにより撮影した 640×480 ピクセルの画像はおおよそ $100 \sim 75$[Kbyte] 程度である．この場合，画像中の $1/3 \sim 1/2$ を移動物体が占めても，全てのデータを埋め込むことができる．埋め込みデータ量が限界量を超えると，この電子透かし法では出力ストリームに全てのデータを埋め込むことができない．しかし，限界を超える大きさの移動物体が抽出されるのは，カメラの

表 3.2 ゼロランレングスが 5 の場合のハフマンテーブル．入力値に対する付加ビットは表 3.1 と同値．

入力値の絶対値	ハフマン符号
512 ∼ 1023	1111111110100101
256 ∼ 511	1111111110100100
128 ∼ 255	1111111110100011
64 ∼ 127	1111111110100010
32 ∼ 63	1111111110100001
16 ∼ 31	1111111110100000
8 ∼ 15	1111111110011111
4 ∼ 7	1111111110011110
2,3	11111110111
1	1111010

目の前を障害物が横切る場合や，急激な日照変動が起こった場合などであり，通常の監視下ではほとんど起こらないものである．また，起こったとしても，その masked image は画像の大半の領域が masking されたものであり，図 2.2（c）に示したような，何が起こったか判別できない監視として有効性のない画像である．そこで，埋め込みデータ量が限界量を超える場合には，暗号化ストリームを直接出力し，masked image の出力はスキップする．暗号化ストリームを出力しているため，第 3.3.3 節に示す手順を踏むことで，撮影画像の再構成は可能である．

ハフマン符号化と出力

電子透かし埋め込み後の係数を，表 3.1，表 3.2 に示す標準のハフマンテーブルを用いて符号化する．最後に，ヘッダーを付加し，これを JPEG ストリームとして出力する．前章での出力と同様に標準の JPEG フォーマットに従ってストリームを出力しているため，一般の JPEG ビューアを用いることで masked image が閲覧できる．

3.3　真正性の検証と撮影画像の再構成

本節では，移動物体を撮影画像に戻さずに，出力 JPEG ストリームから再構成される画像が，改竄されていない真正な画像であることを証明する手順を示す．さらに，撮影画像を再構成する手順を示す．

3.3.1　真正性の検証

図 3.3 は真正性検証手順を示したものである．真正性検証は次の 6 ステップからなる．

Step1: **電子透かしにより埋め込んだデータの抽出**

まず，電子透かしにより埋め込まれた撮影画像復元用データ (data for reconstruction) と，真正性検証用データ (electronic signatured hash) を抜き出す．撮影画像復元用データと真正性検証用データは，第 3.2.4 節に示した係数に埋め込まれている．そのため，JPEG ストリームをハフマン復号し，輝度成分の AC 成分を $|ac| \geq 2$ のグループと $|ac| \leq 1$ のグループに分ける．$|ac| \geq 2$ のグループに属する係数の最下位ビットを取り出し，次に $|ac| \leq 1$ のグループに属する係数の最下位ビットを取り出すことで，埋め込んだデータをすべて抜き出すことができる．ハッシュ値は長さが固定であるため，真正性検証用データ，撮影画像復元用データの順に埋め込んでおくことで，抜き出したデータを簡単に分離できる．

Step2: **真正性検証用データからのハッシュ値への復元**

抜き出したデータのうち，真正性検証用データをハッシュ値に戻す．真正性検証用データは，結合した暗号化ブロックストリームから得られたハッシュ値を，秘密鍵で変換したものである．そこで，真正性検証用データに公開鍵を用いて再変換すると，ハッシュ値に戻すことができる．

Step3: masked image **からの暗号化ブロックストリームの生成**

次に，masked image から第 3.2.3 節に示した手順で暗号化ブロックストリームを生成する．Masked image を 16×16 ピクセルのブロックに分割し，式 (3.1) を用いて輝度成分の AC 成分係数を処理してブロックストリームを作る．次に，ブロックストリームを公開鍵により暗号化する．ただし，DCT での再変換による係数値の変化を避けるため，実際には，出力 JPEG ストリームをハフマン復号した量子化 DCT 係数から，暗号化ブロックストリームを生成する．

暗号化ブロックストリームを生成するアルゴリズムは公開されており，また，暗号化に用いる鍵は公開鍵であることから，誰でも masked image から暗号化ブロックストリームを生成できる．

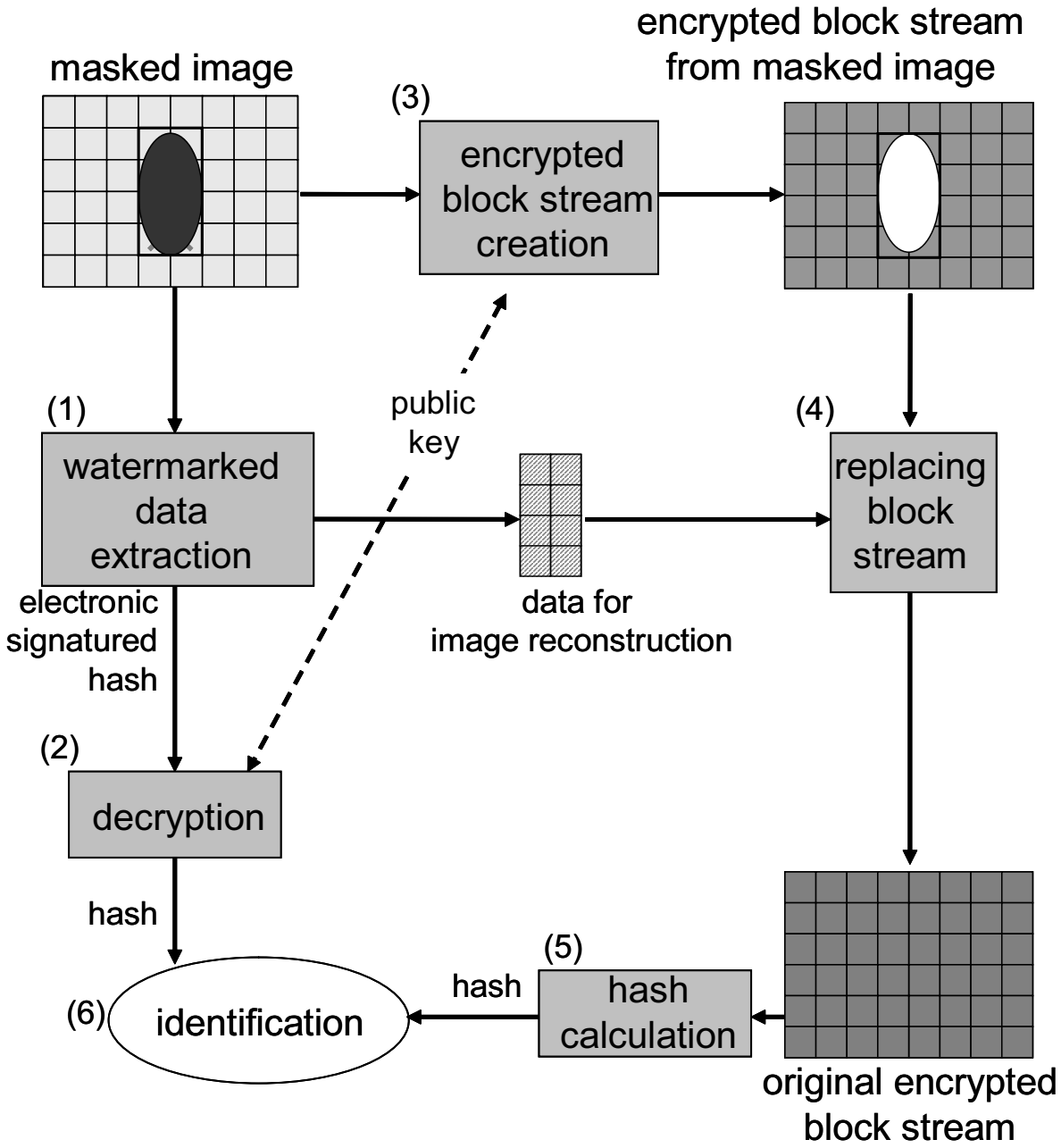


図 3.3 真正性検証手順

Step4: **暗号化ブロックストリームの復元**

Step3 で得られた，masked image から生成した暗号化ブロックストリームは，移動物体に masking した影響で，移動物体を含むブロックで撮影画像から生成したものと異なる．そこで，撮影画像から作られる暗号化ブロックストリームに戻すため，step1 で抽出した撮影画像復元用データで移動物体を含むブロックの暗号化ブロックストリームを置換する．

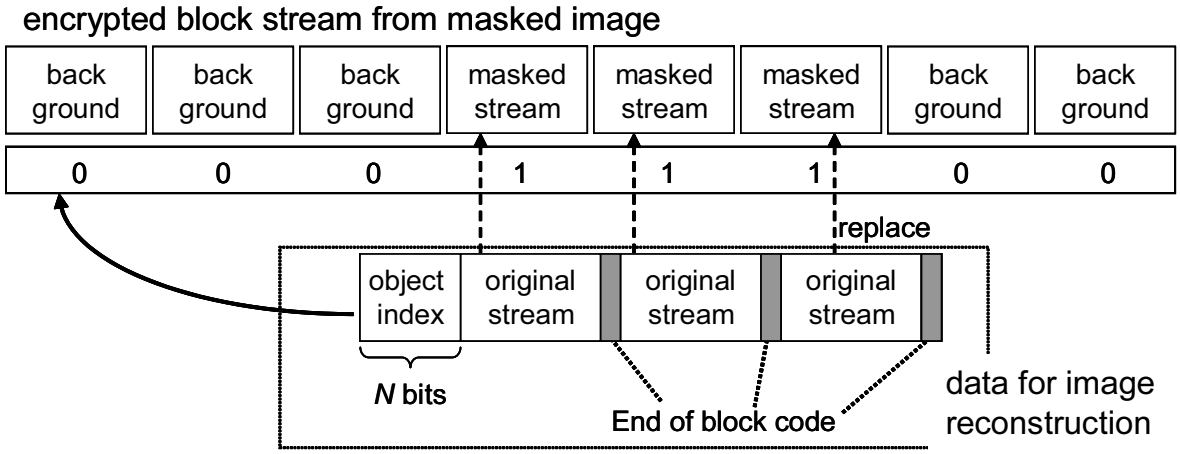


図 3.4 撮影画像復元用データの構造

図 3.4 は撮影画像復元用データの構造を示したものである．撮影画像復元用データの先頭には移動物体を含むブロックをさす object index がある．これは各ブロックを 1 次元スキャンし，移動物体が存在すれば 1，背景であれば 0，つまり masking するブロックに 1，masking しないブロックに 0，を割り当てたブロック数 N のビット長を持つデータである．Object index が 1 を指すブロックを，撮影画像復元用データの暗号化ブロックストリームで先頭から順に置換する．暗号化ブロックストリームは，あらかじめブロック単位に分割できるようにブロックごとの切れ目を示す 2 バイトコード (0xFFD9) を挟み込んでおく．第 2.4.2 節の識別子と同様に，JEPG ヘッダーと同じ長さの 2 バイトコードの中から，自由に使える組み合わせのものを選んだ．

このようにして作った暗号化ブロックストリームは，改竄などの攻撃が加えられていなければ，第 3.2.3 節において作成した暗号化ブロックストリームと，1 ビットの違いもなく同一である．つまり，秘密鍵によって復号すると撮影画像を再構成できる，暗号化ストリームである．

Step5: **暗号化ブロックストリームからのハッシュ値の算出**

Step4 で復元した暗号化ブロックストリームからハッシュを計算する．ここでのハッシュの計算は第 3.2.3 節で用いたハッシュ関数による．

Step6: **ハッシュ値の比較**

Step5 で計算したハッシュ値と，step2 で復元したハッシュ値とが一致すれば，カメラで撮影した画像と復元して得られた画像とは，式 (3.1) で変更した量子化 DCT 係数の最下位ビットを除き完全に同一であり，人が検知できるような違いは存在しない．つまり，画像が真正であり，改竄や合成がされていないことが保証される．

3.3.2 改竄への耐性

提案手法の改竄攻撃への耐性を示す．3 種類の攻撃を想定し，それぞれに対して提案手法が頑健であることを示す．まず，masked image を改竄し，一般の JPEG ビューアで出力できる画像を改竄する攻撃．次に，撮影画像復元用データを改竄し，再構成した画像に表れる人物などの移動物体を別なものに変更する攻撃．最後に，真正性検証用データを改竄し，masked image や撮影画像復元用データの改竄を行ったうえで，その画像が真正であるかのように見せかける攻撃．

1．masked image の改竄

Masked image に直接画像処理を行った場合には，第 3.3.1 節の step4 で暗号化ブロックストリームを復元しても，撮影画像と同一の暗号化ブロックストリームにならない．そのため，真正性検証用データから復元したハッシュ値と，暗号化ブロックストリームから計算したハッシュ値とが一致せず，改竄された真正でないものと判別できる．

2．撮影画像復元用データの改竄

暗号化ブロックストリームは，ブロックストリームを公開鍵で暗号化したものである．ブロックストリームおよび，暗号化ブロックストリームの生成手順は，真正性検証手順で用いるため，公開されている．そのため，任意の画像から同じフォーマットのデータを作ることが可能である．悪意を持った人物が，本来，撮影画像中に存在しない人物の画像から，偽の暗号化ブロックストリームを作成し，本来の撮影画像復元用データと置き換えることも考えられる．この場合，**1．**の改竄攻撃と同様に，step4 で撮影画像と同一の暗号化ブロックストリームが復元できない．そのため，ハッシュ値が一致せず，改竄と判別できる．

3．真正性検証用データの改竄

Masked image や撮影画像復元用データを改竄した上で，改竄画像から得られるハッシュ値から，偽の真正性検証用データを作成し，本来の真正性検証用データと置き換えようとする場合を考える．真正性検証用データは step2 で公開鍵によって，ハッシュ値に復号される．つまり，真正性検証プロセスを通過できる，偽の真正性検証用データを作るには，改竄画像のハッシュ値を秘密鍵で変換しなければならない．よって，公開鍵から秘密鍵の推測は非常に困難であり，偽の真正性検証用データを作ることはできない．

1．，**2．**の改竄への耐性はハッシュの強度に依存し，**3．**の改竄は，RSA 公開鍵暗号方式の強度に依存する．また，提案手法は，ハッシュと公開鍵暗号方式以外には改竄耐性に関

わる要因を持たない．ハッシュの強度，RSA 暗号化の強度ともに十分なものが報告されているため [31]，本手法は実用に耐えうる十分な攻撃耐性を持つ．

3.3.3 撮影画像の再構成

Masked image から撮影画像を再構成する手順を示す．

第 3.3.1 節の真正性検証の手順 step3,4 によって，撮影画像から得られるものと同一の暗号化ブロックストリームを復元する．この暗号化ブロックストリームから，秘密鍵用いて，ブロックストリームを復号する．これらのブロックストリームは監視カメラによる撮影画像の量子化 DCT 係数を 16×16 ピクセルのブロックに分割したものである．よって，ブロックストリームに標準 JPEG デコードと同じく，逆量子化，IDCT，RGB 変換を行うことで撮影画像に戻すことができる．

なお，暗号化ブロックストリームからブロックストリームへの復号には秘密鍵を用いるため，秘密鍵を知る特定の人物や機関以外には，撮影画像を再構成することはできない．

3.4 実行例と考察

3.4.1 実データによる実行例

まず，提案手法を実データに適用した結果を示す．図 3.5（a）が撮影画像で，画像サイズは 640 × 480 ピクセルである．図 3.5（b）は撮影画像に式 (3.1) による前処理を行い，輝度の AC 成分の最下位ビットを 0 とした画像である．図 3.5（a），（b）間の PSNR は 46.9[dB] と高い類似性を持ち，目視で違いを見つけるのは困難なほど，前処理の適用による画像の変化は少ない．図 3.5（c）は出力 JPEG ストリームを JPEG デコードした masked image である．画面右側にいる人物が単一色で塗りつぶされ，特定や識別が不可能なことがわかる．特定はできないが，図 2.1（b）に示したように適切なプライバシー保護処理が施されているため，人物の形状は認識でき，そこに誰かが立っていることがわかる．図 3.5（d）は秘密鍵を用いて，出力 JPEG ストリームから撮影画像を再構成した画像である．図 3.5（b）と図 3.5（d）には 1 ビットも違いは無く，完全に同一の画像に復元できている．

従来法による真正性の証明手法とプライバシー保護を併用する場合には，図 3.5（d）に示す再構成した画像を用いなければ真正性を検証できない．そのため，真正性を検証するときには被撮影者のプライバシーが開示されるという問題が生じる．さらに，プライバシー情報にアクセスすることを許される特定の機関でのみしか，真正性の検証ができないという問題がある．提案手法は，図 3.5（c）の masked image を用いて，人物を特定できる情報を隠したまま画像の真正性が検証できる．そのため，従来法と異なり，真正性検証にともなってプライバシーを開示することがなく，誰にでも真正性が検証できる．

(a) input image

(b) preprocessed image

(c) masked image

(d) reconstruct image

図 3.5 実データへの実行結果

3.4.2 出力 JPEG ストリームの符号長の考察

次に，提案手法を用いた場合の出力 JPEG ストリームの符号長について考察する．

masking，電子透かしによる符号長への影響

表 3.3 は，提案手法を適用した撮影データの全フレーム数，移動物体を含むフレーム数，入力 JPEG ストリームの符号長，出力 JPEG ストリームの符号長を，それぞれ示したものである．撮影データは，data1 が屋内を撮影したもの，data2，data3 がそれぞれ屋外の異なる環境を撮影したものである．Data1 は図 3.5 に示したものを含む画像シーケンスである．Data2 は長時間撮影の画像シーケンス，data3 は data2 とは異なる長時間撮影の画像シーケンスから移動物体を含む区間を抜粋して作成したものである．また，画像サイズはそれぞれ，data1，data2 が 640×480 ピクセル，data3 が 320×240 ピクセルである．

表 3.3 より，data1，data2 の出力 JPEG ストリームの符号長はわずかではあるが，入力 JPEG ストリームの符号長よりも小さい値を示している．提案手法の出力ストリームの符号長は，第 3.2.2 節に述べた masking と，第 3.2.4 節に述べた電子透かしにより，増減が決まる．masking は移動物体領域を単一色で塗りつぶすため，その領域で JPEG 圧縮効率が高くなりファイルサイズが減少する．また，電子透かしではファイルサイズが増

表 3.3 屋内外の撮影データに対する実行結果

	フレーム数	移動物体を含むフレーム数	入力ストリーム符号長 [MB]	出力ストリーム符号長 [MB]
data1	510	492	25.30	24.89
data2	3,000	224	208.44	208.32
data3	3,339	2,538	34.25	35.68

表 3.4 Masking による符号長の減分と，電子透かしによる符号長の増分

	入力ファイルサイズ [MB]	masking による減分 [MB]	電子透かしによる増分 [MB]	出力ファイルサイズ [MB]
data1	25.30	2.08	1.67	24.89
data2	208.44	0.34	0.22	208.32
data3	34.25	0.90	2.33	35.68

加する．

そこで，表 3.4 にそれぞれのデータの，masking による符号長の減分と電子透かしによる符号長の増分を示す．Masking においては，移動物体が画面内に占める割合が大きければ，単一色で塗りつぶす領域が大きくなり符号長が減少する．一方，移動物体が大きいと，撮影画像を復元するために埋め込むデータが大きくなり，masked image の $|ac| \geq 2$ となるグループの AC 成分にすべてのデータを埋め込めなくなり，符号長の増加に繋がる．移動物体が，$|ac| \geq 2$ となる AC 成分を持つ係数に，すべて埋め込める大きさの範囲で最大となるとき，出力ストリームの符号長の減少幅は最大となる．Data1，data2 では，移動物体を埋め込むときに，$|ac| \geq 2$ となるグループの AC 成分の係数に，データの大半を埋め込むことができるフレームが多かったこと，などから，出力 JPEG ストリームの符号長が入力に対し減少していると考えられる．

移動物体の大きさと符号長

ここでは，画像 1 フレームごとに，移動物体の大きさと，符号長の変化との関係を示す．図 3.6(a) は data3 から一部の区間を抜き出し，各フレームの入力ストリームの符号長 (input data size)，出力ストリームの符号長 (output data size)，移動物体を含む 16×16 ピクセルのブロックの数 (number of object block) を示したものである．入力ストリームの符号長は灰色の実線，出力ストリームの符号長は黒色の実線，移動物体を含むブロック数は灰色の破線で示す．また，符号長は左軸，ブロック数は右軸に対応している．図に示すように，移動物体の入力がない場合 (1 から 15 フレーム付近，91 フレーム以降) は入力，出力ストリームの符号長は等しく，ブロック数が 30 個以下程度の小さな移動物体が入力された場合 (21 から 31 フレーム付近，45 から 91 フレーム付近) には，出力ストリームの符号長が入力ストリームの符号長に対して減少していることがわかる．しかし，移動物体を含むブロック数が大きい 31 から 41 フレーム付近では，出力ストリームの符号長が増加している．図 3.6(a) から得られる，移動物体が小さい場合には符号長が減少し，大きい場合には符号長が増加するという結果は，第 3.4.2 節での推察と一致する．

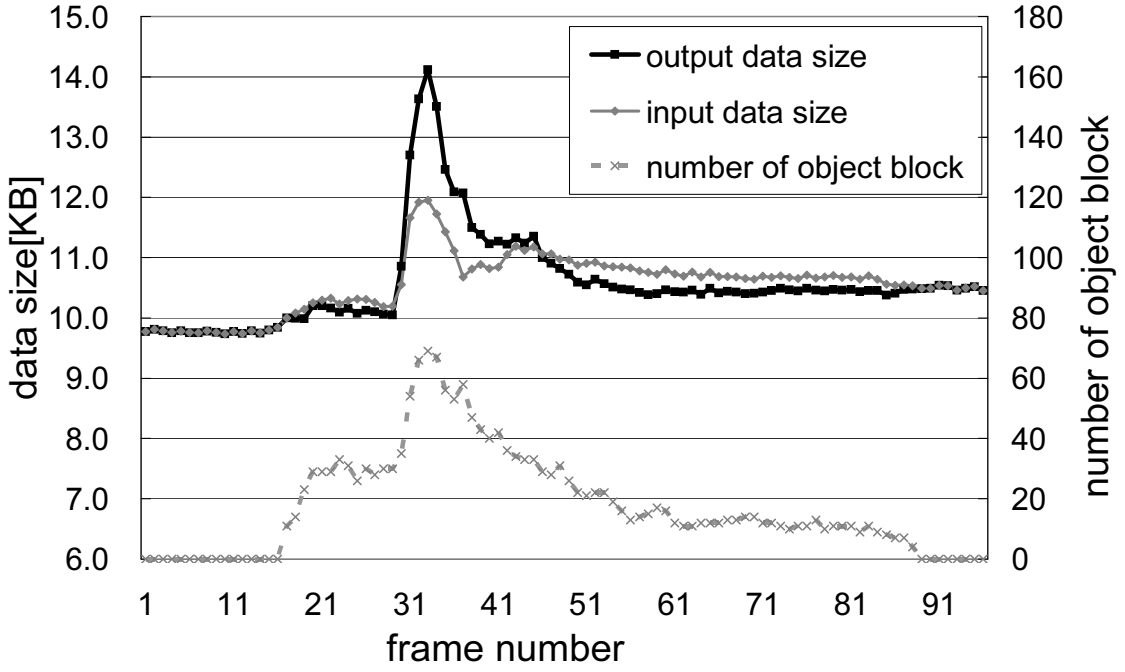
さらに詳細に，移動物体を含むブロック数と符号長の増減の関係性を調べる．図 3.6(b) は移動物体を含むブロック数と，電子透かしで埋め込む量の関係を示したグラフである．黒塗りの点は出力ストリームの符号長が入力を上回らないフレーム，白抜きの点は 31 から 41 フレーム目のように，出力ストリームの符号長が入力ストリームの符号長に対し増加しているフレームを示す．図から，移動物体を含むブロック数が 30 から 35 個を超えると，出力ストリームの符号長が増加していることがわかる．data3 で用いた画像のサイズは 320×240 ピクセルであり，ブロックサイズは全部と 300 個なる．つまり，出力ストリームの符号長が入力に対して増加していないのは，移動物体が全ブロック数の約 1 割程度に収まる場合である．$|ac| \geq 2$ となる AC 成分の数は撮影シーンや圧縮強度に強く依存

するため，定量的に示すことはできないが，data3 の撮影シーンでは画面の 1 割程度の大きさの移動物体であれば，その符号長は $|ac| \geq 2$ である AC 成分の個数以内であると推測できる．また，白抜きの点から下方向に伸びる垂線は，出力ストリームの符号長の増加量を示している．移動物体を含むブロック数が多くなるにつれ，出力ストリームの符号長の増加量が増すのは，$|ac| \leq 1$ である AC 成分へデータを埋め込むと出力の符号長が増加するという推論と一致する．しかし，いずれの場合も，電子透かしによって埋め込むデータ量よりも，少ない増加量であることがわかる．従来法による真正性証明を適用するために撮影画像を完全に復元する場合には，埋め込みデータをそのまま保存する必要があり，出力ストリームの符号長の増加量と埋め込みデータ量は等しくなる．そのため，提案手法では，data3 の入力に対して，1 フレームあたり最大で約 3KB ほど，符号量を少なくすることができた．また，いずれのフレームでも，符号長の増加量が，埋め込みデータ量を上回ることはなかった．つまり，すべてのフレームにおいて，従来法より出力ストリームの符号長を削減できた．

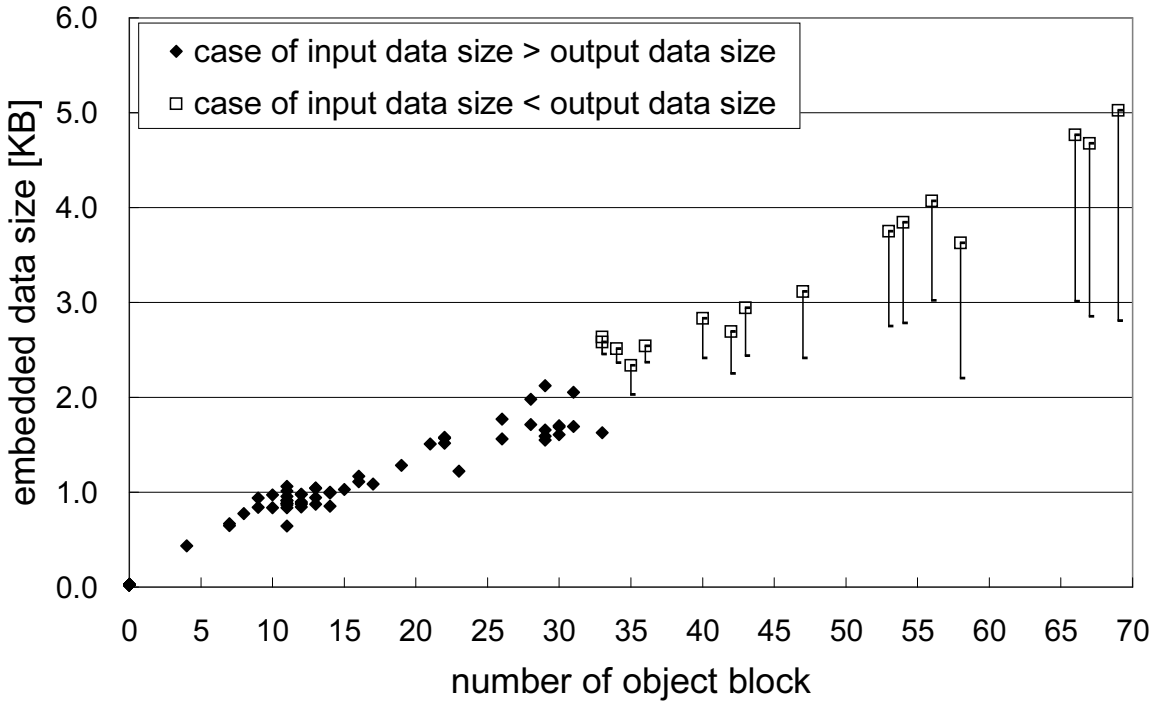
符号長の増減と masked image

次に，出力ストリームの符号長が増加しないフレームと増加するフレームを出力画像と共に比較する．図 3.7 はそれぞれの出力を示したものである．28 フレーム目の画像では，出力ストリームの符号長は減少しているが，33 フレーム目の画像では，符号長が増加している．それぞれの画像の移動物体を含むブロック数に注目すると，28 フレーム目の画像では 30 個であるのに対し，33 フレーム目の画像では，移動物体が複数存在することもあり，ブロック数が増加し 69 個となっている．

最後に，図 3.8 に出力ストリームの符号長が入力ストリームの符号長に対して増加しない場合の再構成画像と masked image を，data1 と data2 のそれぞれから 1 枚ずつ示す．図に示すように，電子透かしによって出力ストリームの符号長が増加しない程度の大きさの移動物体であっても，十分に，masked image での移動物体の形状の識別や，再構成画像での被写体の特定が可能であることがわかる．



(a) the size of input data and output data



(b) number of object block with respect to embedded data size

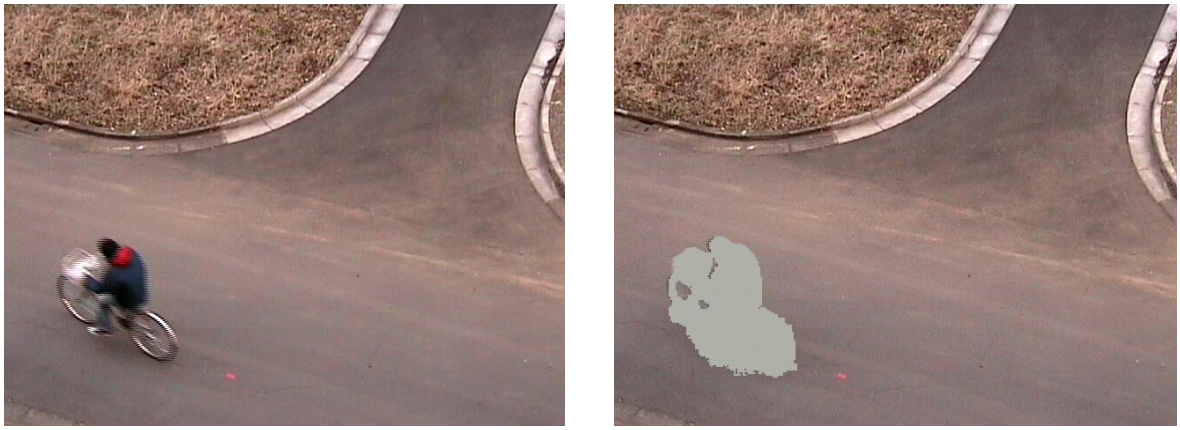
図 3.6 入力および出力ストリームの符号長と移動物体の大きさ

(a) 出力ファイルサイズが
減少した場合　（第28フレーム）
(a) output data size is reduced
(frame 28)
object block: 30
input data size: 10430[byte]
output data size: 10307[byte]

(b) 出力ファイルサイズが
増加した場合　（第33フレーム）
(b) output data size is increased
(frame 33)
object block: 69
input data size: 12240[byte]
output data size: 14458[byte]

図 3.7 data3 の masked image とファイルサイズ

(a) images from data1（640x480）



(b) images from data2（320x240）

図 3.8 符号長の増大しない場合の masked image と再構成画像

3.4.3 実行時間

本節では，提案手法の実行時間について述べる．表 3.5 は各データセットを用いた場合のフレームレートを示したものである．フレームレートは移動物体の存在するフレームのみから算出した．提案手法は画像サイズに計算コストが依存するため，640 × 480 ピクセルの data1, data2 では，320 × 240 ピクセルの data3 の場合に比べ，フレームレートが低くなっている．また，いずれの場合も動画撮影のフルレートである 30 frame/sec を下回るが，監視カメラではフレームレートを落として撮影・保存することが多く，5 frame/sec は監視カメラの撮影レートとしては支障のない値と言える．

表 3.5 提案手法のフレームレート

	フレームレート [frame/sec]
data1	5.70
data2	4.85
data3	11.39

3.5　本章のまとめ

本章では，RSA 公開鍵暗号方式と電子透かしを用いた，撮影画像の真正性証明と被撮影者のプライバシー保護を同時に実現する手法を提案した．撮影画像を再構成してからでないと真正性が検証できない従来法と異なり，提案手法では再構成した画像を必要とせずに，移動物体を特定する情報を隠蔽した画像から真正性が証明できる．また，撮影画像復元用データを埋め込む電子透かしにおいて，係数の値から埋め込み位置を選ぶことにより，移動物体が大きすぎない限りファイルサイズが増加しない効果が得られた．特に，実験に用いたデータのうち 640×480 ピクセルのデータでは，出力ファイルサイズを入力ファイルサイズより小さくすることができた．一方，出力ファイルサイズが増加した 320×240 ピクセルのデータでは，各フレームを検証した結果，入力される物体が画面の 1 割に収まる場合には，ファイルサイズが増加しないことを示した．また，移動物体の大きさが画面の 1 割であっても，masked image や再構成画像において，十分移動物体の特徴である人物の顔や形状などを表すことを示した．さらに，データセット全体ではなく個々のフレームでは，ファイルサイズが増加するフレームであっても，撮影画像を完全に復元するためすべてのデータを損失無く保存する従来法に比べて，ファイルサイズが減少することを示した．これらの特徴から，住宅街など人物の往来が多くない環境では，通常の JPEG による撮影とほぼ変わらない，もしくは小さいファイルサイズで保存することができ，提案手法は住宅街などでの監視カメラの運用に適応性の高い手法であると言える．また，実行時間に関しては 640×480 ピクセルの画像を用いた場合には約 5 frame/sec と，監視用途には支障の無い実行速度が得られた．

第 4 章

監視カメラの最適配置手法

4.1 まえがき

前章までは，監視カメラによる撮影画像中の人物に対するプライバシー保護について述べた．このような監視カメラにより撮影した画像の取り扱いが重要な課題であるように，どのような場所を撮影するようにどれだけのカメラをどこに置くのが適切か，という構築方法も重要な課題である．本章では，固定モニタカメラによって構成される監視カメラシステムにおける，監視カメラの自動配置問題について述べる．固定モニタカメラは，カメラ位置，カメラ向き，視野角，視野距離が一定であるため，観測できる領域が一意に定まる．そのため，目的の観測シーンを観測するためにはどのようなカメラを，どこに，何台置けばよいか，という最適なカメラ配置を一意に求めることができる．観測シーンを複数の離散的な観測点で近似し，さらにカメラを設置できる場所を指定することで，設置するカメラと観測点の観測・非観測の関係を求める．この関係を集合被覆問題へ置き換えて解くことで，厳密な最適カメラ配置を求めることができる．

ここで，カメラ配置最適化問題は，その性質がカメラ位置と観測点の設定方法に大きく依存し，最適化されたカメラの台数や最適解を得るまでの時間を大きく左右する．そのため，これらをどのように設定するかは本問題の重要な課題となる．一般に見受けられるカメラ位置と観測点の設定方法には次のような方法がある．

一点一点を手動で設定する方法

カメラ位置の設定において，電源ケーブルと電源供給源の距離関係や，カメラを据え付ける金具の関係などでカメラを設置できる位置が限定される場合には，この方法がよく用いられる．

観測点の設定においては，建物の出入り口を見張る場合や，店舗内の注目商品のある棚付近を観測するなど，あらかじめ注目すべき点が決まっており，それ以外の場

所は観測されなくてもかまわない場合に用いられる．

このように，観測シーンの形状以外に，あらかじめ多くの制約が与えられている場合には有用である．点数が少ない場合には簡単に設定できる方法ではあるが，注目箇所が非常に多い，もしくは大きな観測シーンを対象とするなど，設定できる候補位置が多くなる場合には，すべてを手動で設定するコストは非常に高くなる．また，カメラ位置に制限がなく自由度が高い，注目箇所が広場などの点ではなく領域で表されるような場合には，設定が難しい．

観測シーンをグリッドで細分して得られた点上に自動設定する方法

カメラ位置の設定においては，候補位置が多くなればなるほどカメラが最適な位置に近づくことができるため，カメラ台数の削減に繋がる．

観測点の設定においては，一定間隔おきに観測点を設定できるため，観測シーン全体を撮影したい場合に適している．

この方法はグリッド間隔に大きく依存する．グリッド間隔を細かくすればするほど，カメラ位置，観測点の点数が非常に多くなるため最適な解に近づく．また，見落としや死角の発生を防げる，といった利点がある．しかし，その分最適カメラ配置の求解が困難になり，解が得られる保障がなくなる，また，解が得られたとしても求解までに長時間を要する．逆に，グリッド間隔を荒くすることによって，カメラ位置と観測点を減らせば求解までの時間は短くなるが，カメラ台数の増加や，見落としや死角が発生する．

エリアを手動で指定し，エリア内にグリッド分割やランダム配置により設定する方法

前二つの方法の中間に当たる方法である．一点一点を手動で指定するのではなくカメラ位置や観測点を設定できる領域を指定する．さらに，その領域内部をグリッド分割やランダムに選択して候補点や観測点を配置する．あらかじめ，シーン中の観測が必要な領域やカメラを置ける領域が決まっている場合には，一点一点を手動で設定する場合に比べ，設定に関するコストを低く抑えられる．また，観測シーン全体ではなく一定の範囲内を分割するので，設定する点数の増加も抑えられる．そのため，全体を観測する場合に比べ，短時間で解が求まる．しかし，エリア指定は手動で行わねばならないため，観測シーンが広大になるとそのコストが無視できなくなる．

実際のシーン，特に街中などの広い空間を対象として最適カメラ配置を決定するには，(1) 観測に多数のカメラが必要となる，(2) 解くのに非常に長い処理時間がかかる，という 2 つの問題点がある．(1) の問題を解決するには，シーン全域の観測でなく，観測位置を限定する必要がある．さらに，観測点を配置できるエリアを手動ではなく，与えられたシーンの形状から自動決定できれば，広い空間であっても手動操作のコストを削減でき

る．本章では，シーン中の移動物体のフローを検出するためのカメラ配置が求まることを目的とし，通路のグラフ構造に基づいて，観測すべき位置（観測エリア）を頂点被覆を用いて決定する．次に，得られた観測エリアについて集合被覆を解くことで，巨大なシーンであっても集合被覆問題の規模を小さくできるため（2）の問題点が解決できる．

4.2　観測シーンからのグラフ構造抽出と観測エリアの決定

4.2.1　フロー検出問題のモデル化

本節では，シーン内の物体のフロー（移動経路）検出問題をモデル化する．まず，観測シーンに対し以下の 2 点を仮定する．

- シーン内では通行可能な区域と，通行不可能な障害物が明確に区別され，障害物は視界を遮るものとする
- 明示された出入り口でのみシーン内外の移動が可能

次に，グラフ構造を取り出すために観測シーンを出入り口，通路，分岐点，袋小路の 4 つの構成要素に分解する．これらの構成要素の特徴を以下に示す．

出入り口

出入り口は外から観測シーン内へ入場，もしくは観測シーンから外へ退場できる唯一の箇所である．以降に示す，通路，分岐点，袋小路は自動的に抽出するが，出入り口のみは観測シーンとともに手動で与える．

通路

通路はその幅や形状によらず，分岐することなく両端の地点をつなぐものとする．図 4.1 は通路に分類するものとしないものの例である．図中の青色の破線は上下の地点を結ぶルートを示したものである．図 4.1(a) は，途中で幅が変化したり曲がりくねったりしたシーン形状の例であるが，上下の地点を分岐することなくつないでいるため，通路に分類する．図 4.1(b) は，入退場できる箇所を 2 つ持つ広間や通路の例である．この例でも上下の地点を結ぶには破線の結び方のみであるため，通路に分類する．図 4.1(c) は，一見すると通路のようであるが，中央付近に存在する障害物のため，上下の結び方が，左側を通るもの，右側を通るもの，と 2 種類存在する．この例は，内部に分岐を持つため，一つの通路には分類せず複数の通路と分岐点に細分する．

分岐点

分岐点は通路が 3 本以上交差する箇所とする．しかし，自由形状のシーンに対して厳密に分岐点の位置を定めることは非常に困難である．そのため，本章では観測シーンを矩形領域の集合で近似できるものとして，分岐点を定める．ある矩形領域が，3 つ以上の異なる矩形領域と接続あるいは重なり合う場合，その矩形領域の中心を分岐点とする．

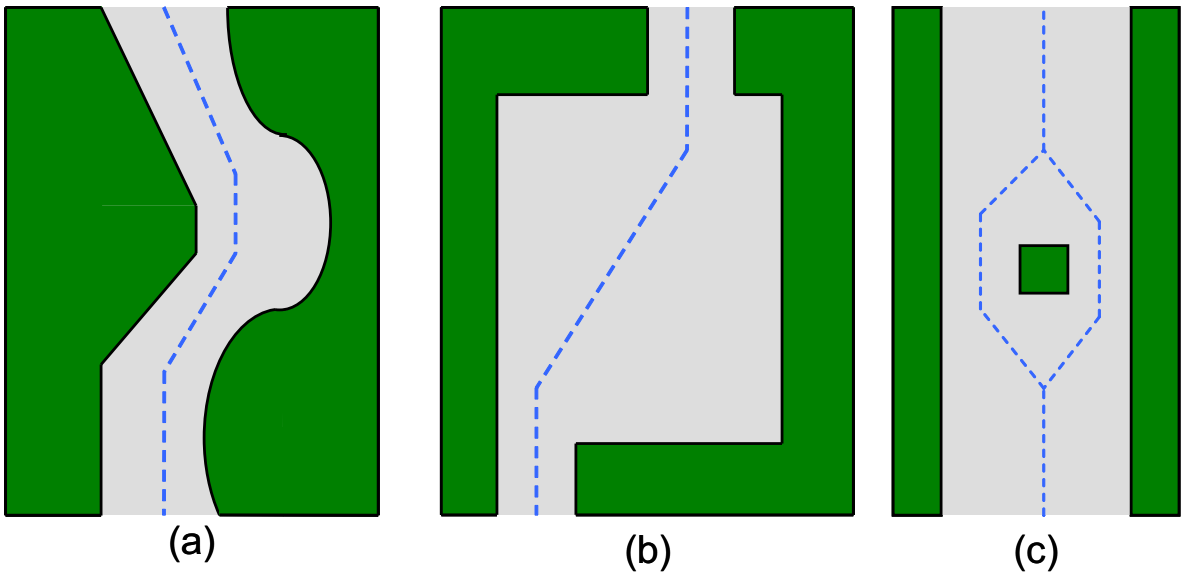


図 4.1 ひとつの通路に分類するシーン形状 (a)(b) と，ひとつの通路に分類しないシーン形状 (c).

袋小路

袋小路はある一本の通路の終端が他のいずれの通路にもつながらない箇所とする．

提案手法では，“出入り口から物体が進入し，通路や分岐点を通過して，出入り口から退出するという一連の動き” をフローと定義する．シーンに現れた全ての物体に対してフローを特定できる観測モデルを示す．まず，フローの定義より，物体の進入，退出を監視しなければならない．そのため，全ての出入り口を観測する．次に，シーンの仮定より，通路を通る物体は必ずどちらかの端に現れる．つまり，通路の両端の分岐点や袋小路を観測すれば，通路の中間を観測しなくても物体がどの通路を通過したか（通り抜けたか）がわかる．本論文では通路を途中で引き返すような動きは考慮せず，通路を他端まで通り抜ける動きをフローとして検出する．

ここで，通路の通過を検出するのであれば通路のいずれか一端に当たる分岐点を観測すれば十分である．図 4.2 は通路の一端の観測からフローを復元した例である．図中の S と T は出入り口，A, B, C, D, X, Y, Z は分岐点，そのうち A, B, C, D は観測した分岐点，X, Y, Z は観測必須でない分岐点とする．また，W は観測必須でない袋小路を示す．また，グレーの円内の矢印は観測された物体の動きを示し，細線は観測を元に復元したフロー，破線は通過しなかった通路を示す．図 4.2 は S からシーンに進入し，$S \rightarrow A \rightarrow Y \rightarrow C \rightarrow D \rightarrow Z \rightarrow B \rightarrow X \rightarrow T$ という経路をたどり T から退出したフローの例である．ここで，AC 間にある分岐点 Y は観測されていないが，図に示す観測のみから $A \rightarrow Y$，$Y \rightarrow C$ が復元できる．まず，A で下方向の通路への動きが観測され

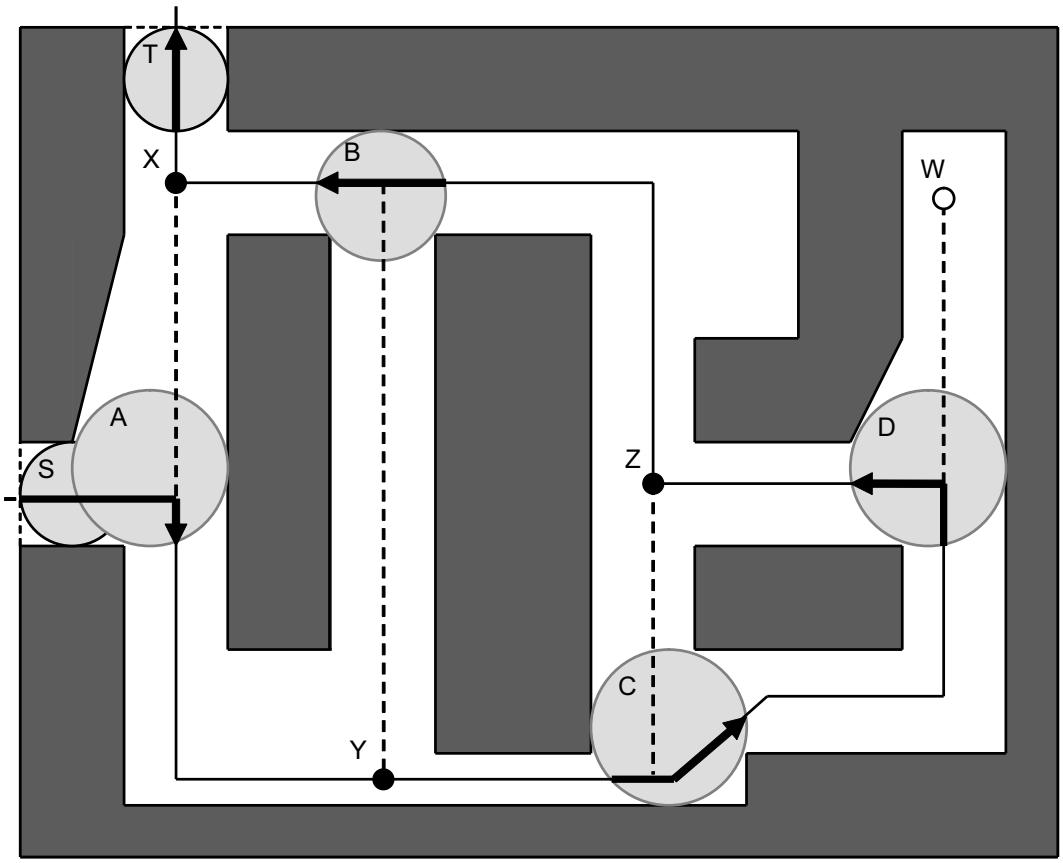


図 4.2 観測された物体とフローの復元．図中の矢印は観測された物体の動き，細線はそれを元に復元したフロー，破線は通過しなかった通路を示す．

ているため，物体はこの通路の終端 Y に到達する．これより $A \to Y$ を復元できる．次に，C で左方向の通路からの動きが観測されているため，物体はこの通路の始端 Y から来たことがわかる．これより $Y \to C$ を復元できる．また，仮に $Y \to B$ という経路をたどったとすると，B において下方向の通路からの動きが観測されるはずである．しかし，実際には右方向の通路からの動きしか観測されておらず，この物体は $Y \to B$ の経路をたどっていないことが明らかである．よって，Y を観測しなくても，$A \to Y \to C$ という一連の動きを復元できる．このように，全ての通路に対していずれか一端を観測することでシーン内の全ての分岐点間をどのような経路で移動したかを特定することができる．

そこで，本手法ではシーン内の通路を枝 E，分岐点と袋小路を頂点 V_b，出入り口を頂点 V_g とするグラフ $G(V, E)(V = V_b \cup V_g)$ を作成する．グラフ G から，全ての出入り口の集合 V_g と，枝の少なくとも一端の頂点 $\acute{V}_b$ からなる，頂点集合 $\acute{V}(\acute{V} = \acute{V}_b \cup V_g)$ を観測する問題として本問題を解く．

4.2.2 観測シーンの領域分割とグラフ構造の抽出

本節では観測シーンからのグラフ構造抽出について説明する．図 4.3 は入力された観測シーンからグラフ構造を抽出する手順を示している．

Step1: **矩形領域集合への近似**

まず，入力されたシーン（図 4.3(a)）を間隔 $2l$ の等間隔メッシュで分割し，複数の矩形領域の集合として扱う（図 4.3(b)）．メッシュの間隔 $2l$ は，観測シーン中の通路を見逃すことの無いように，観測シーン中の最も細い通路幅以下に設定する．メッシュ分割された領域の中心点 (x, y) が障害物の外にあればそこには面積 $2l \times 2l$ の小領域 $r^1_{(x,y)}$ があるとする．中心が障害物内部に入り込んでいる場合，その領域は計算の対象からはずす．このとき最大幅 l の死角が発生する可能性がある．しかし，幅 l を観測対象に合わせ適切に設定することで，対象の見落としを防ぐことができる．例えば，車を対象とする場合には $l \leq 1[m]$，人を対象とする場合には $l \leq 50[cm]$ とすれば，カメラにまったく映らずに通り抜けることは困難であり，十分であると考えられる．

Step2: **階層構造の抽出**

次に，矩形領域の集合から階層構造を抽出する．図 4.4(a) に示すように点 P を頂点にもつ 4 つの領域（$r^{h-1}_{(x-l,y-l)}, r^{h-1}_{(x+l,y-l)}, r^{h-1}_{(x-l,y+l)}, r^{h-1}_{(x+l,y+l)}$）が全て存在する場合，1 つ上の階層に点 P を中心とする小領域 $r^h_{(x,y)}$ を作成する．ここで，座標 (x, y) 階層 $h(h = 1, 2, \ldots)$ の位置に小領域が存在するとき $r^h_{(x,y)} = 1$，存在しなければ $r^h_{(x,y)} = 0$ として，領域作成プロセスを論理式で表現すると式 (4.1) となる．

$$r^h_{(x,y)} = r^{h-1}_{(x-l,y-l)} \ \ and \ \ r^{h-1}_{(x-l,y+l)} \ \ and \ \ r^{h-1}_{(x+l,y-l)} \ \ and \ \ r^{h-1}_{(x+l,y+l)} \tag{4.1}$$

このプロセスを新しい小領域が作成されなくなるまで繰り返す．図 4.3(c) は，図 4.3(a) の観測シーンから階層構造を抽出した結果である．

Step3: **グラフ頂点の検出**

次に，階層構造からグラフ G の頂点 V を検出する．図 4.4(b) に示すように点 Q を中心とする小領域 $r^h_{(x,y)}$ の上位階層に，点 Q を頂点に持つ小領域が 1 つも存在しない場合，小領域 $r^h_{(x,y)}$ の中心 (x, y) はグラフ G の頂点とする．ここで，小領域 $r^h_{(x,y)}$ の中心がグラフ G の頂点であるとき $n^h_{(x,y)} = 1$，頂点でないとき $n^h_{(x,y)} = 0$ として，ノード検出プロセスを論理式に表すと式 (4.2) となる．

$$n^h_{(x,y)} = 1 - \left(r^{h+1}_{(x-l,y-l)} \ \ or \ \ r^{h+1}_{(x-l,y+l)} \ \ or \ \ r^{h+1}_{(x+l,y-l)} \ \ or \ \ r^{h+1}_{(x+l,y+l)} \right) \tag{4.2}$$

また，出入り口に隣接する領域もグラフ G の頂点に加える．第 4.2.1 節で述べたよ

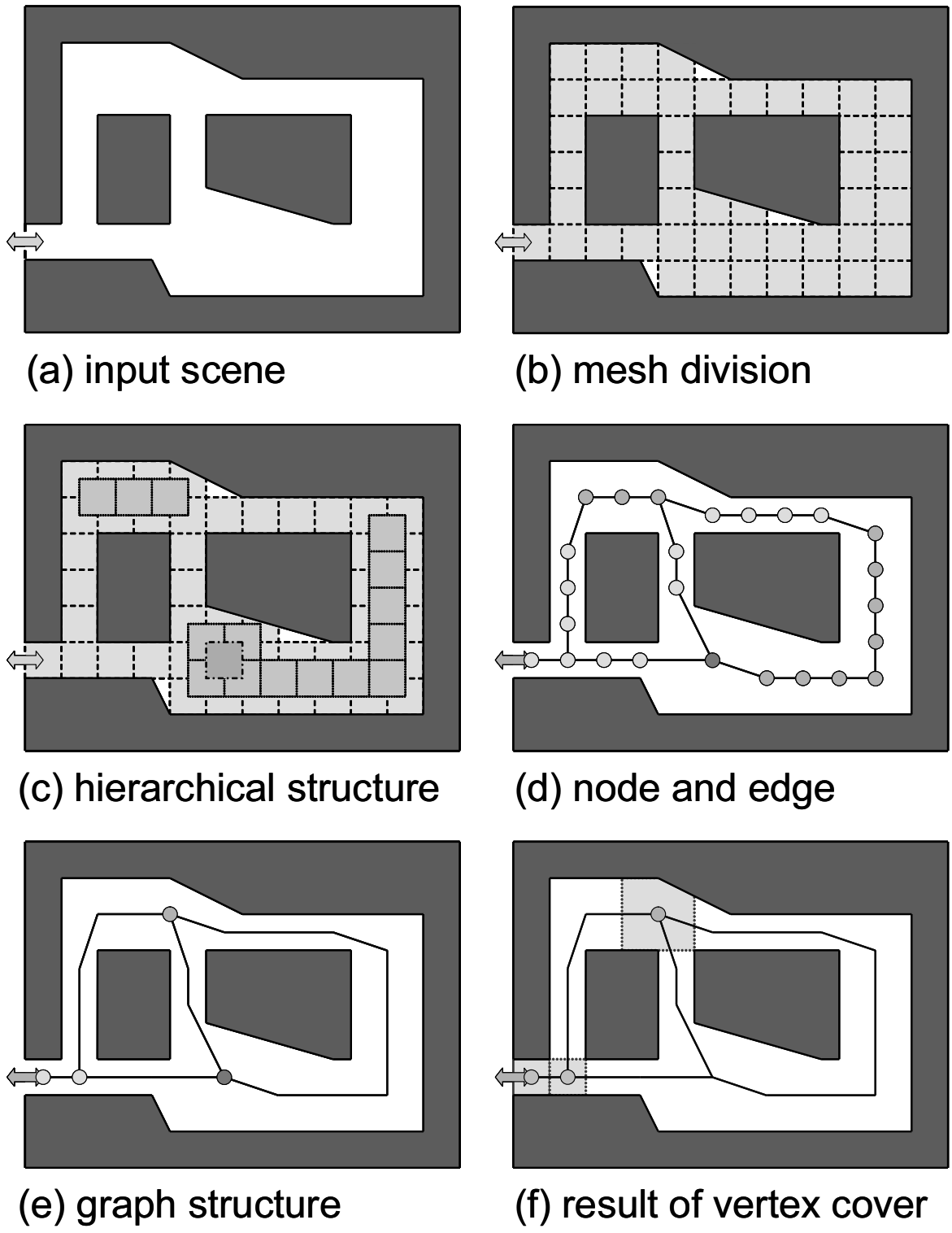


図 4.3 観測シーンとグラフ構造

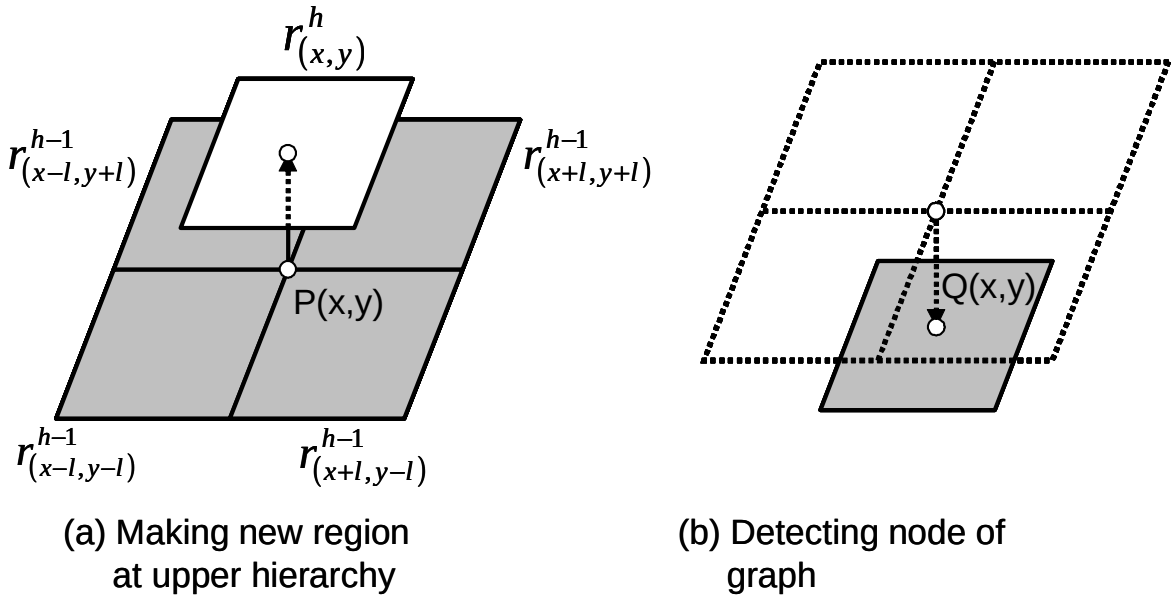


図 4.4 階層構造と領域作成，ノード検出

うに，観測シーンの出入り口は手動で与える．図 4.3 中の矢印は出入り口を表している．小領域 $r^{h_g}_{(x_g,y_g)}$ が出入り口に隣接するとき，$n^{h_g}_{(x_g,y_g)} = 1$ とする．

Step4: **グラフ頂点の接続**

最後に，図 4.3(d) に示すように，小領域の隣接関係に基づき各頂点を接続し，グラフ構造を取り出す．Step3 でのグラフ頂点は，階層構造の頂点を取り出したものであるため，接続する枝が 2 本の頂点が多数存在する．しかし，分岐点は枝が 3 本以上接続する頂点であり，接続する枝が 2 本である頂点は実際には通路の一部を表すため，グラフから取り除く．図 4.3(e) は，通路中の頂点を取り除いた最終的なグラフ G を示している．残った頂点が $n^{h}_{(x,y)} = 1$ であるとき，(x, y) を中心とする面積 $2lh \times 2lh$ の領域を，その頂点の持つ観測エリアとする．

4.2.3 頂点被覆問題に基づく観測エリアの決定

前節で取り出したグラフ $G(V,E)$ より頂点被覆問題を用いて全ての枝 E のいずれか一端をカバーする頂点集合 $\acute{V}$ を求める（図 4.3(f)）．頂点集合 $\acute{V}$ は複数存在するが，提案手法ではその中で，観測エリア面積の和が最小のものを求める．以下に，頂点集合 $\acute{V}$ を求める線形制約式を示す．

$$
\begin{aligned}
s &= \text{グラフ } G \text{ の頂点}, \quad s \in V \\
t &= \text{グラフ } G \text{ の枝}, \quad t \in E \\
y_s &= \begin{cases} 1 & \text{頂点 } s \text{ がカバーされる場合} \\ 0 & \text{上記以外} \end{cases} \\
a_s &= \text{頂点 } s \text{ に対応する観測エリアの面積}
\end{aligned}
$$

Minimize

$$
Z = \sum_{s \in V} a_s y_s \tag{4.3}
$$

Subject to:

$$
y_u + y_v \quad \geq 1 \quad e_t = (u,v) \in E \quad \forall t \tag{4.4}
$$

$$
y_s \in \{0,1\} \, \forall s \in V_b \tag{4.5}
$$

$$
y_s \quad = 1 \quad \forall s \in V_g \tag{4.6}
$$

ここで，$e_t = (u,v)$ は枝 e_t の両端の頂点がそれぞれ，頂点 u と頂点 v であることを示す．

式 (4.5) はシーンの分岐点の観測，非観測が選択されることを示し，式 (4.6) はシーンの出入り口は必ず観測されることを示す．式 (4.4) はグラフ $G(V,E)$ の枝 $e_t \in E$ の端点に当たる頂点 u,v の少なくとも一方はカバーされる必要があることを示す．これをグラフ G 内の全ての枝 E に対して満たすときの合計面積最小の観測エリアを式 (4.3) により求める．式 (4.3) では a_s は頂点 s に対応する観測エリアの面積を示し，選択された領域の合計面積を最小化する目的関数を表す．

4.3 最適カメラ配置の決定

4.3.1 カメラ設置点と観測点の設定

観測シーンの形状に基づき，カメラ設置点を設定し，また，前節で求めた合計面積最小の観測エリアに基づき，観測点を設定する．

まず，カメラ設置点は観測シーン全域をメッシュ分割し，得られた領域の中心点とする．ただし，中心点が障害物の内部に入り込んでいるものは除く．なお，メッシュ分割は第 4.2.2 節でのメッシュ分割に用いた間隔 $2l$ のメッシュとはと異なる間隔のものを用いることができる．次に，観測点は第 4.2.3 節により求めた観測エリア内に等間隔で置いた点とする．観測点を置く間隔は任意であるが，観測点を置く間隔により，観測領域内部に観測点同士の隙間に死角が発生する可能性がある．そのため，観測点の間隔分だけ見落とす領域が発生することがある．第 4.2.2 節で述べた観測シーンを小領域に分割する場合と同様に，この間隔を建物内なら人物，屋外なら車が通り抜けないだけの狭さに設定し，物体の見落としを防ぐ．

4.3.2 カメラ候補

設置するカメラは位置（設置点），方向，カメラ仕様（視野角，視野距離）のパラメータにより決まる．パラメータの異なる個々のカメラを “カメラ候補” と呼ぶ．カメラ候補は使用可能な複数のカメラの視野角と視野距離，およびカメラ設置位置のグリッド間隔，向きの角度刻みを与えることにより，すべての組み合わせを自動生成する．

次に，自動生成されたカメラ候補から撮影可能な観測点を求める．図 4.5 は，カメラ候補 C_i の撮影範囲と，その内部にある観測点 O_j を示している．図中のカメラ候補 C_i が観測可能な点はこの 5 点である．このカメラ候補と撮影可能な観測点を，すべてのカメラ候補に対して求める．ただし，カメラ候補の観測可能な範囲内の観測点であっても，図 4.6 のように，カメラ候補と観測点を結ぶ線分が，いずれかの障害物と交わる場合は観測できない．また，いずれの観測点も観測範囲内にもたないカメラ候補は，次節の集合被覆問題には用いず，あらかじめ取り除いておく．

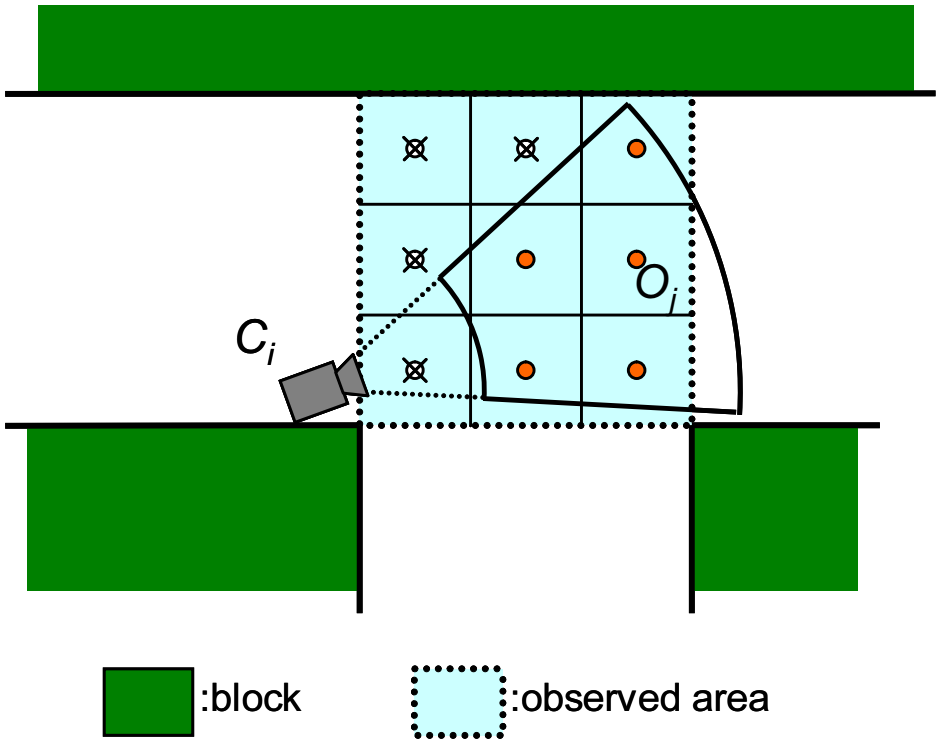


図 4.5 カメラ候補から観測可能な観測点

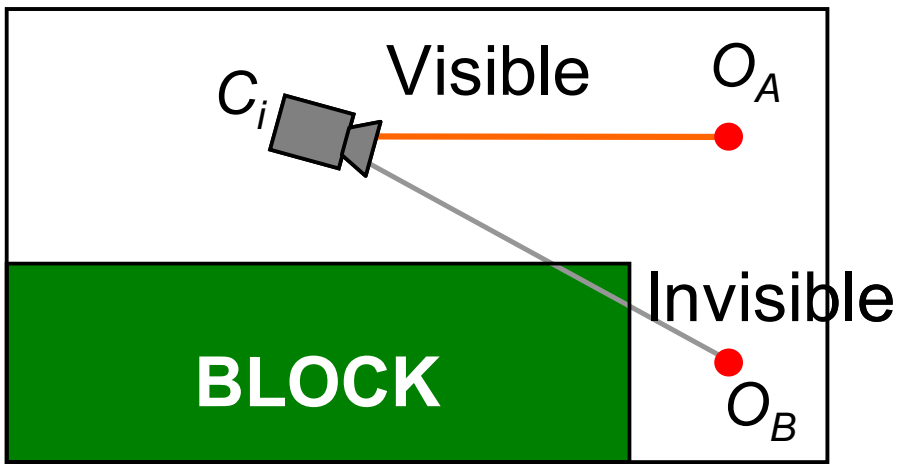


図 4.6 カメラ候補と観測点の間に障害物がある場合

4.3.3 集合被覆問題に基づくカメラ配置の最適化

第 4.3.2 節で求めたカメラ候補と観測点の関係から，最小台数で全ての観測点をカバーする最適カメラ配置を集合被覆問題により求める．以下にカメラ最適配置を求めるための線形制約式を示す．

$$
\begin{aligned}
C_i &= \text{カメラ候補}, \quad i = 1, 2, \ldots, n \\
O_j &= \text{観測点}, \quad j = 1, 2, \ldots, m \\
x_i &= \begin{cases} 1 & \text{カメラ候補 } C_i \text{ を設置する場合} \\ 0 & \text{上記以外} \end{cases} \\
p_{ij} &= \begin{cases} 1 & \text{カメラ候補 } C_i \text{ が} \\ & \text{観測点 } O_j \text{ を観測可能な場合} \\ 0 & \text{上記以外} \end{cases}
\end{aligned}
$$

Minimize

$$
Z = \sum_{i=1}^{n} x_i \tag{4.7}
$$

Subject to:

$$
\sum_{i=1}^{n} p_{ij} x_i \quad \geq 1 \quad \forall j \tag{4.8}
$$

$$
x_i \in \{0, 1\} \, \forall i \tag{4.9}
$$

$$
p_{ij} \in \{0, 1\} \, \forall ij \tag{4.10}
$$

ここで，カメラ候補数 i の最大値 n はすべてのカメラ位置，カメラ方向，カメラ仕様の組み合わせにより決まる．式 (4.8) において p_{ij} はカメラ候補 C_i が観測点 O_j を観測可能であることを表すため，すべての観測点 O_j において式 (4.8) を満たすことで観測エリア内をもらさず観測することができる．この制約の下，式 (4.7) によりカメラ台数を最小化する．

4.4　実験結果

本節では，本実験のために作成した仮想的な観測シーンと，実在の環境を元に作成した観測シーンに，提案手法を適用し，カメラ台数と実行時間から提案手法の有効性を示す．

まず，本実験に用いたカメラの視野角と視野距離，カメラ候補設置時の角度刻みを表 4.1 に示す．本実験では視野角 45° の標準的なカメラと，より遠方を撮影可能な視野角 15° のカメラ，より広角な撮影が可能な視野角 75° のカメラの 3 種を用いた．

これら 3 種のカメラの撮影範囲は，図 4.7 に示す解像度 N，視野角 θ，視野距離 l の関係を用いて決定した．まず，視野角 45° のカメラ 2 を基準とし，カメラ 2 において $l_2 = 12.0$[m] 先で撮影可能な解像度を N_2[pixel/m] とした．解像度 N_2 を撮影画像の判別に最低限必要な解像度とし，それぞれ視野角 $\theta_1 = 15°, \theta_3 = 75°$ のカメラにおける，解像度 N_1, N_3 が N_2 と等しくなる視野距離 l_1, l_3 を式 (4.11) から求めた．

$$\frac{l_2}{N_2} \tan\frac{\theta_2}{2} = \frac{l_{1\ or\ 3}}{N_{1\ or\ 3}} \tan\frac{\theta_{1\ or\ 3}}{2} \tag{4.11}$$

また，カメラに物体が接近しすぎると，物体の一部しか撮影できないなどにより十分な撮影ができないため，全てのカメラにおいて，それぞれカメラから視野距離 l の 10% 未満にある範囲は，観測できないとした．カメラ候補の向きを決める角度刻みは，カメラの視野角をもとに，カメラ 1，カメラ 2，カメラ 3 でそれぞれ 15°，15°，30° とした．

表 4.1 各カメラの視野角と視野距離

	visual angle [deg]	visual distance [m]	angle step [deg]
camera 1	15	3.8–37.8	15
camera 2	45	1.2–12.0	15
camera 3	75	0.6–6.5	30

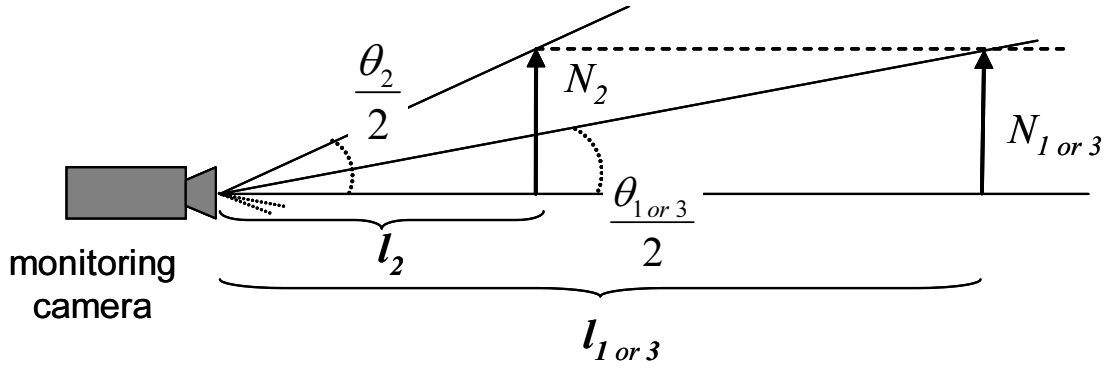


図 4.7 カメラ仕様の決定．N：解像度，θ：視野角，l：視野距離．

4.4.1　仮想シーンによる実験

まず，仮想的な観測シーンに対して，観測シーン全域を観測する場合，提案手法と同様にグラフ構造を定めすべての分岐点を観測した場合，提案手法により分岐点から第 4.2.2 節に述べた方法で分岐点を削減してから最適カメラ配置を求めた場合，の 3 種の手法を適用した結果を示す．

図 4.8 は本実験のために作成した仮想的な観測シーンである．仮想シーンのサイズは 120[m]×100[m] である．図の通路中にある線分は取り出したグラフ構造，外周上にある 7 つの矢印は出入り口をそれぞれ示している．領域分割のグリッド間隔を 2.0[m]，観測点間隔を 0.4[m]，カメラ候補設置のグリッド間隔を 1.0[m] として実験を行った．

表 4.2 に実験結果を示す．実験はシーン全域を観測した場合（Whole scene），グラフ G の全ての頂点にあたるエリアを観測した場合（Every vertex），頂点被覆を用いて観測エリアを削減した提案手法（Vertex cover）の 3 種類を行った．表には観測点の数（Observed points），カメラ候補数（Camera candidates），得られた最小カメラ台数（Placed cameras），実行時間（Processing time）を示す．Whole scene の実験による結

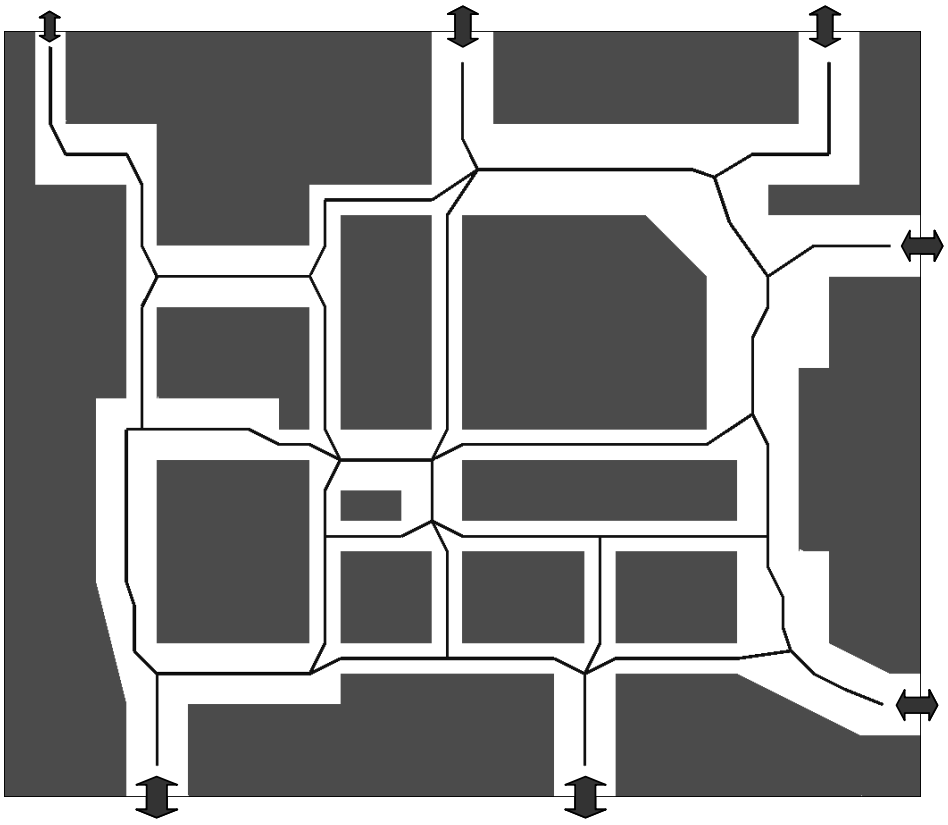


図 4.8 実験に用いる仮想シーン

表 4.2 仮想シーンによる実験結果.

	Observed points	Camera candidates	Placed cameras	Processing time [sec]
Whole scene	27110	185241	(60)	(100070.90)
Every vertex	12000	128571	36	43497.50
Vertex cover	7100	86007	29	252.58
grid interval of region segmentation				2.0 [m]
grid interval of observed point				0.4 [m]
grid interval of camera candidate				1.0 [m]

果の () 内の数値は最適解ではなく，一定時間で計算を打ち切った近似解であることを示している．実験に用いた PC は，Core 2 Duo 3.00GHz, RAM 4GB である．また，頂点被覆と集合被覆の解法には整数線形計画問題のソルバーである CPLEX[32] を用いた．実行時間は，集合被覆問題の求解にかかった時間のみの比較を示している．

表 4.2 より，観測シーン全域を観測するための最適カメラ配置は，100000[sec] 以上計算しても収束せず，100070.90[sec] の時点での近似解から得られるカメラ台数は 60 台である．観測エリアをグラフ G の頂点 V，つまりシーン中の分岐点と出入り口に限定すると，43497.50[sec] で最適解が求まり，そのカメラ台数は 36 台である．これらの手法に比べ，提案手法を用いて合計面積最小の観測エリアの組み合わせをあらかじめ選んでから，最適カメラ配置を求めると，最適解の収束にかかる時間は 252.58[sec] と非常に短時間であることがわかる．また，必要カメラ台数は 29 台と，観測シーン全域を観測する場合の台数に比べて半分以下の台数である．提案手法では，最適カメラ配置を求めるための集合被覆問題のほかに，合計面積最小の分岐点集合を求めるための頂点被覆問題も解いている．頂点被覆問題の求解に要する時間は 0.148[sec] と集合被覆問題を解く時間に比べて非常に短い．集合被覆問題，頂点被覆問題それぞれの求解に要する時間を合わせても，観測シーン全域やすべての分岐点を観測するカメラ配置を求める問題に比べ非常に短時間で厳密解が求まっている．

それぞれの手法で得られた最適カメラ配置を図 4.9 に示す．図中の矢印は設置されたカメラの位置と向き，視野角を示し，通路中の薄いグレーはカメラにより観測される領域，(b) と (c) の通路中の黒枠は観測エリアを示す．

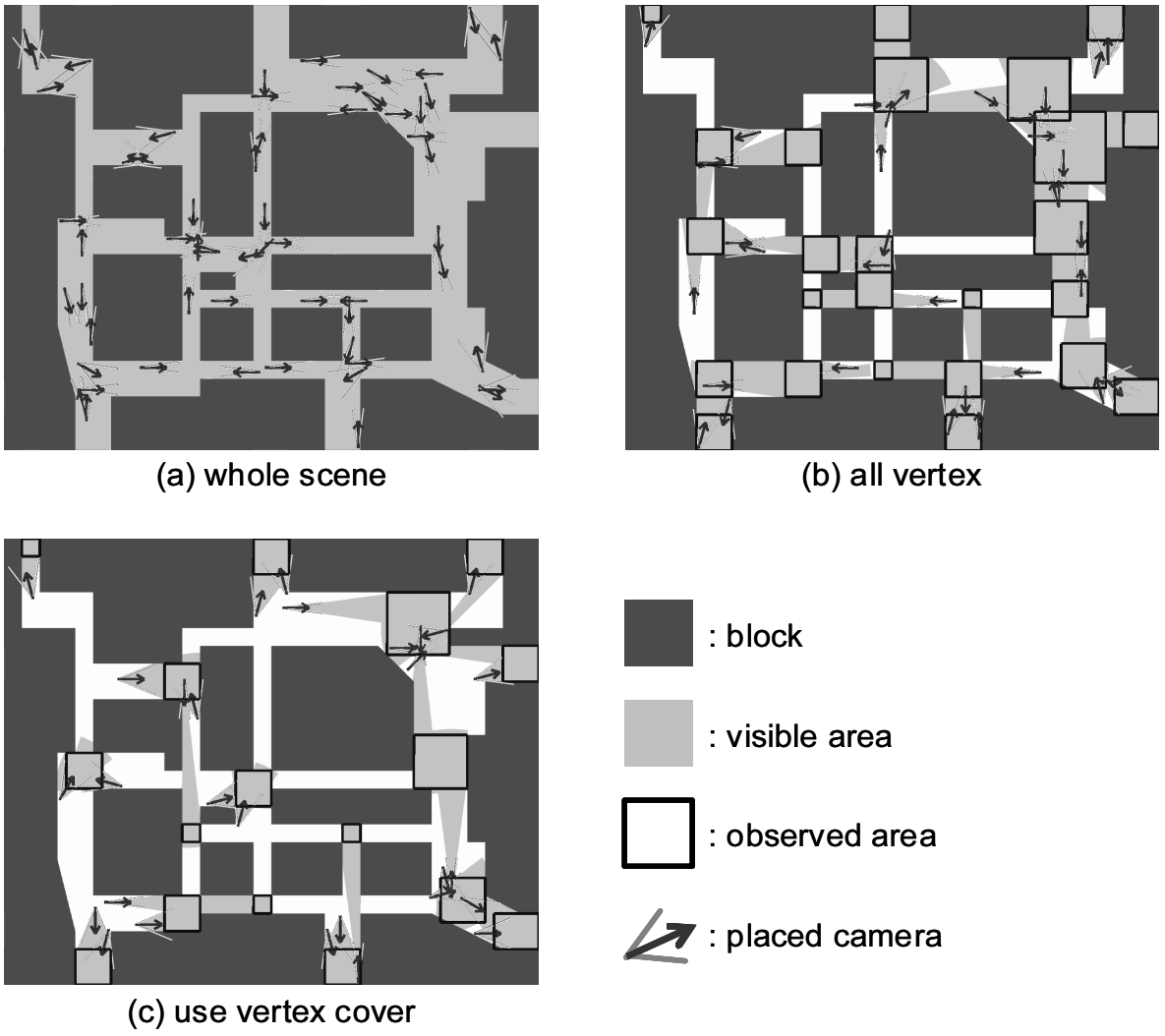


図 4.9 仮想シーンにおける実験結果．(a) 観測シーン全域を観測した場合，(b) 分岐点，出入り口のみを観測した場合，(c) 頂点被覆により観測エリアを最小化する提案手法.

4.4.2 実シーンによる実験

提案手法を含む第 4.4.1 節の 3 種の手法を，実シーンへ適用した結果を示す．実験に用いた観測シーンデータは，学内の通路と建物をモデルとしたものと，街の一区画をモデルとしたものの 2 種類を用いた．大きさはそれぞれ 420[m]×350[m]，1050[m]×400[m] と，仮想シーンよりも巨大な観測シーンである．両データとも，領域分割のグリッド間隔を 1.0[m]，観測点間隔は 0.5[m] とした．ただし，観測シーン全域を観測する場合 (Whole scene) では，観測点間隔を 0.5[m] とすると近似解の求解も困難になるため，3.0[m] に緩めた．カメラ候補設置のグリッドは学内モデルのデータでは 0.5[m]，街モデルのデータでは 1.0[m] とした．

学内をモデルとした観測シーンでの実験結果を示す．表 4.3 は表 4.2 と同様に 3 種の解法を用いたときの，観測点の数，カメラ候補数，必要カメラ数，実行時間を示したものである．図 4.8 よりも巨大な実シーンを用いたことで，観測点の数とカメラ候補数が増大している．提案手法を用いると，784.45[sec] と短時間に最適解が求まった．提案手法の条件は，全領域観測の場合に比べ，観測点，カメラ候補点ともに細かく計算しているが，全領域観測よりも非常に短時間に，かつ，少ない台数で解が求まった．また，頂点被覆の求解に要した時間も 0.00586[sec] と非常に短時間である．提案手法を用いた場合，必要カメラ台数は 33 台と，仮想シーンと同様に，シーン全域観測，全分岐点観測に比べて少ない

表 4.3 学内をモデルとした実シーンによるカメラ配置最適化の実行結果.

	Observed points	Camera candidates	Placed cameras	Processing time [sec]
Whole scene	2287	1635738	(143)	(100018.24)
Every vertex	10748	830874	53	4909.71
Vertex cover	6004	496496	33	784.45
grid interval of region segmentation				1.0 [m]
grid interval of observed point				0.5 [m]
(in the case of observing whole scene				3.0 [m])
grid interval of camera candidate				0.5 [m]

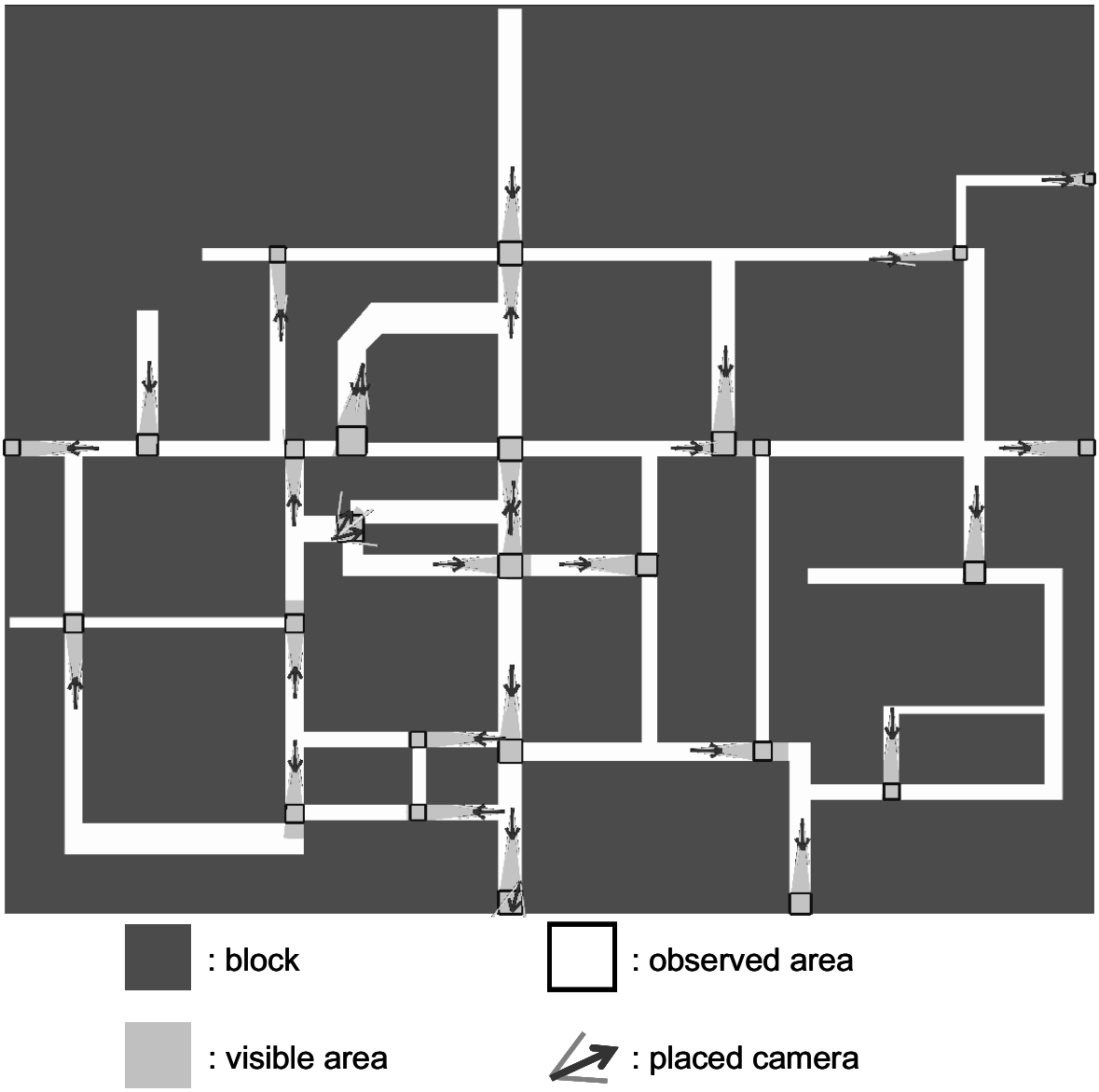


図 4.10 学内をモデルとした実シーンに対して提案手法により求めた最適カメラ配置.
カメラ台数は 33 台，求解までの時間は 784.45[sec].

台数である.

学内をモデルとした実シーンでの最適カメラ配置を，提案手法により求めたものを図 4.10 に，すべての分岐点を観測するものを図 4.11 に，シーン全域を観測するものを図 4.12 に，それぞれ示す.

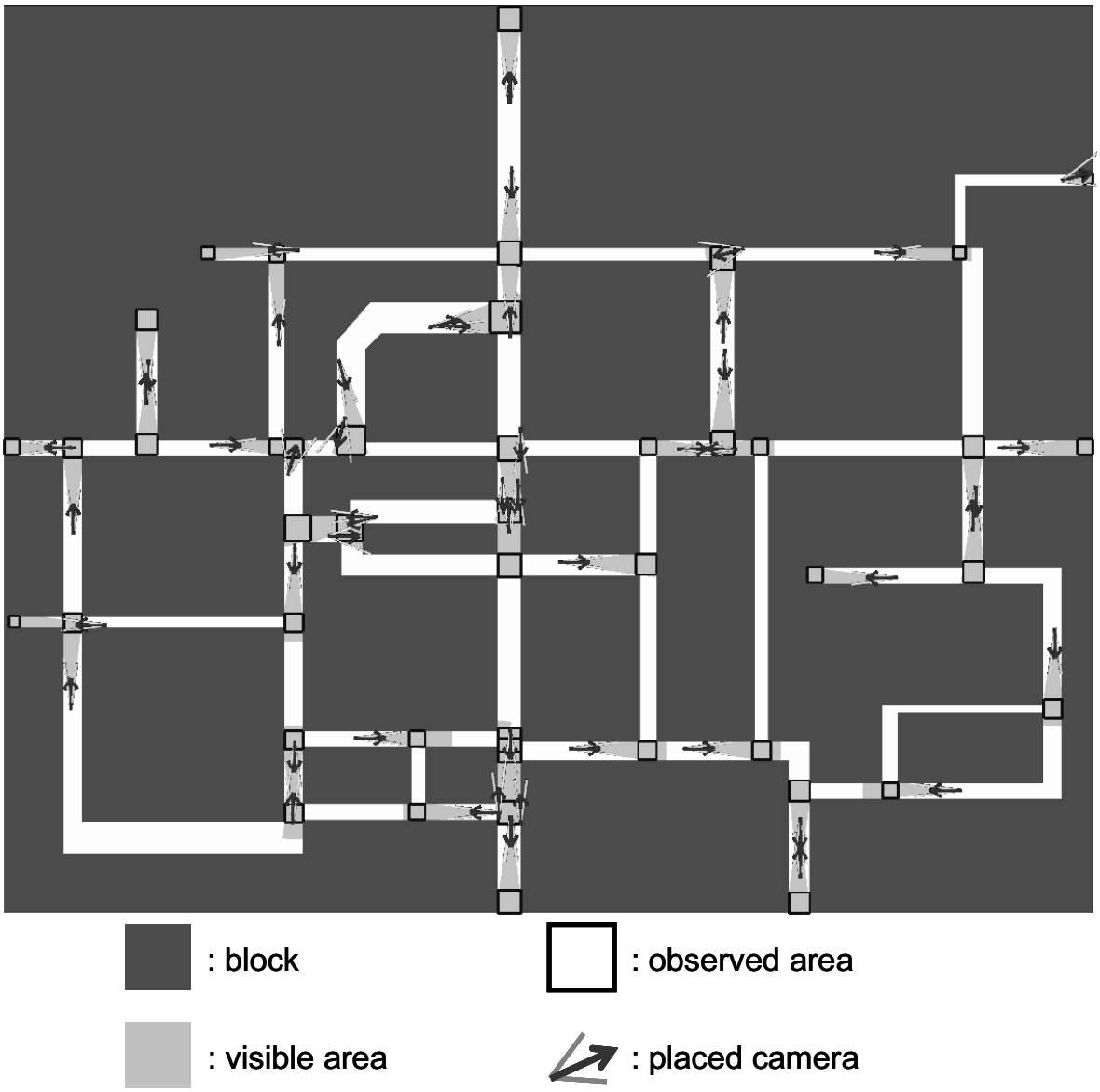


図 4.11 学内をモデルとした実シーンに対して全分岐点を観測する最適カメラ配置.
カメラ台数は 53 台，求解までの時間は 4909.71[sec].

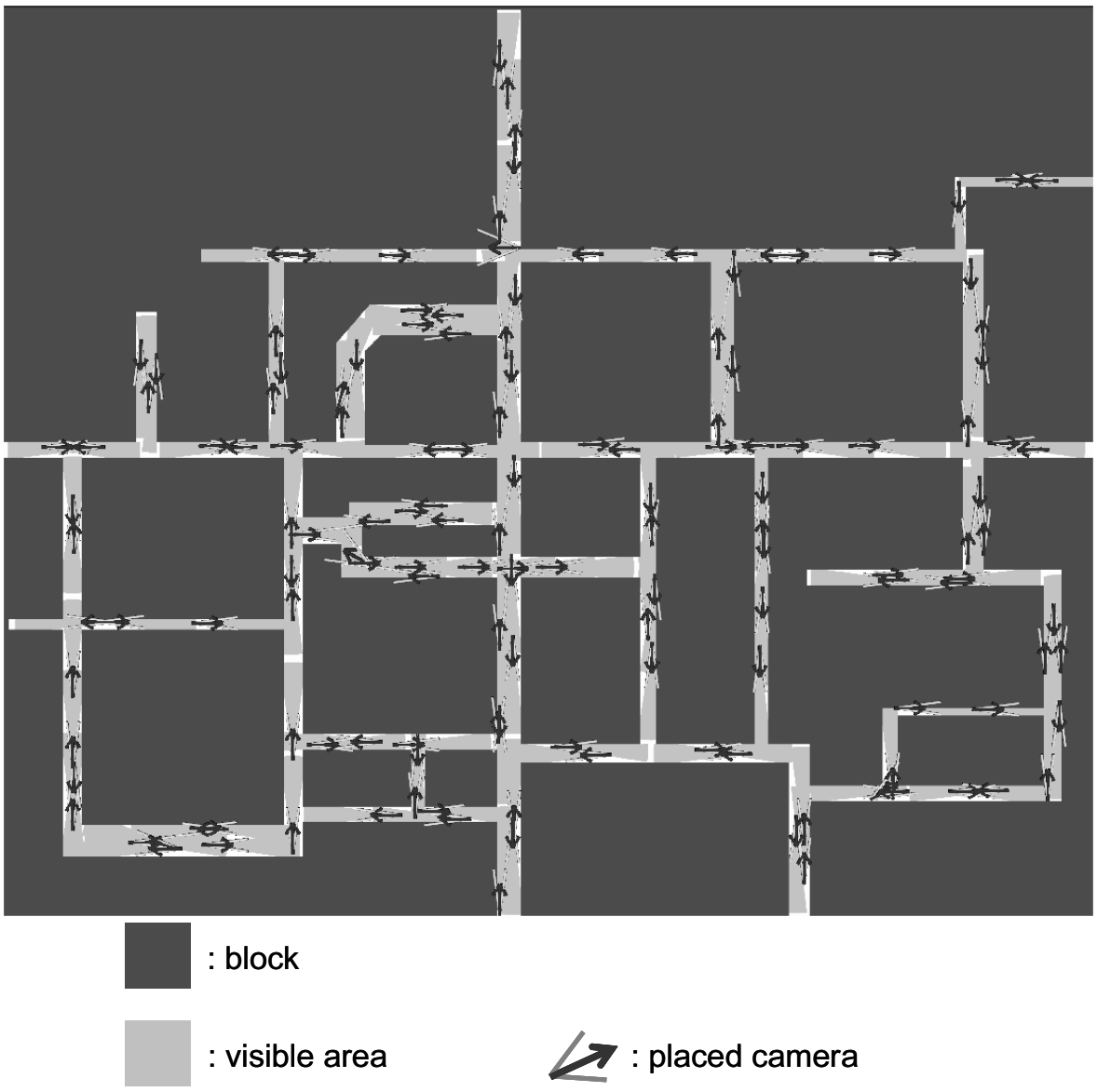


図 4.12 学内をモデルとした実シーンに対してシーン全域を観測する最適カメラ配置.
カメラ台数は 143 台（近似解），実行を 100018.24[sec] で打ち切った.

表 4.4 街の一区画をモデルとした実シーンによるカメラ配置最適化の実行結果.

	Observed points	Camera candidates	Placed cameras	Processing time [sec]
Whole scene	7117	1089166	(454)	(100018.77)
Every vertex	23884	495120	123	687.37
Vertex cover	15540	303642	81	334.68
grid interval of region segmentation				1.0 [m]
grid interval of observed point				0.5 [m]
(in the case of observing whole scene				3.0 [m])
grid interval of camera candidate				1.0 [m]

最後に，街の一区画をモデルとした観測シーンでの実験結果を示す．表 4.4 も，学内をモデルとした観測シーンの場合と同様に，3 種の解法を用いたときの，観測点の数，カメラ候補数，必要カメラ数，実行時間を示している．学内をモデルとした場合よりも，さらに巨大な観測シーンを用いたが，提案手法による最適解の求解に要した時間は 334.68[sec] であり，仮想シーン，学内モデルシーンを用いた場合と同様に短時間である．頂点被覆の求解に要した時間も同様に，0.0491[sec] と短い．また，カメラ台数も 3 種の解法の中で提案手法が最も少ない．

街の一区画をモデルとした実シーンでの最適カメラ配置を，提案手法により求めたものを図 4.13 に，すべての分岐点を観測するものを図 4.14 に，シーン全域を観測するものを図 4.15 に，それぞれ示す．

これらの結果より，提案手法はいずれの観測シーンにおいても，短時間に少ない台数での最適カメラ配置を求めるのに有効であるといえる．提案手法は，最適カメラ配置を集合被覆問題により求める前に，あらかじめ観測シーンから観測エリアを限定することで，短時間に最適解を求めやすい集合被覆問題に帰着させることができると考えられる．特に，観測シーンが巨大になり，分岐点間の距離がカメラの視野距離を超える場合には，その効果がよく現れる．また，頂点被覆問題も，集合被覆問題の求解に比べて，無視できる程度の時間で解を得ることができるため，提案手法は巨大なシーンのカメラ配置問題に対して有効な手法といえる．

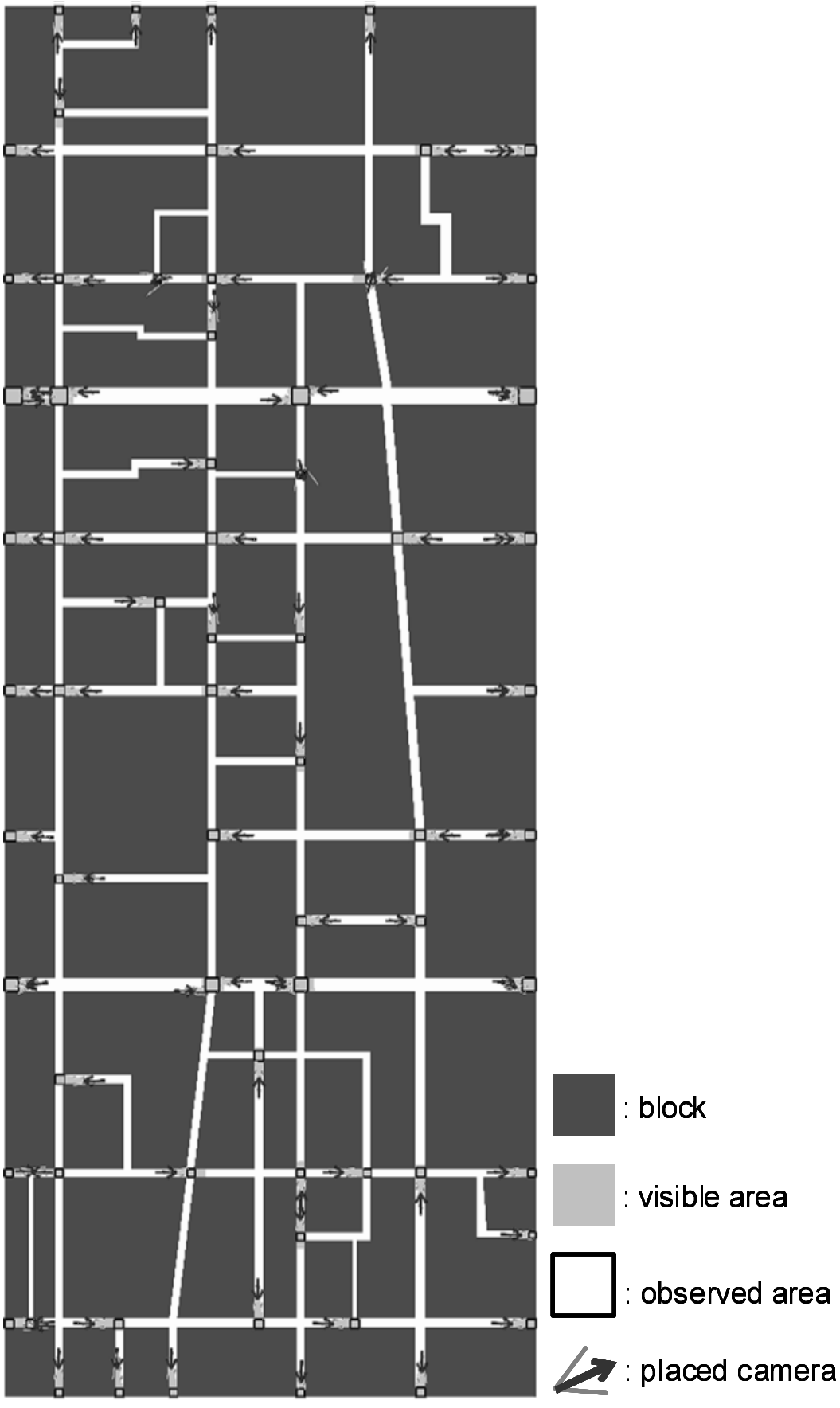


図 4.13 街の一区画をモデルとした実シーンに対して提案手法により求めた最適カメラ配置.
カメラ台数は 81 台，求解までの時間は 334.68[sec].

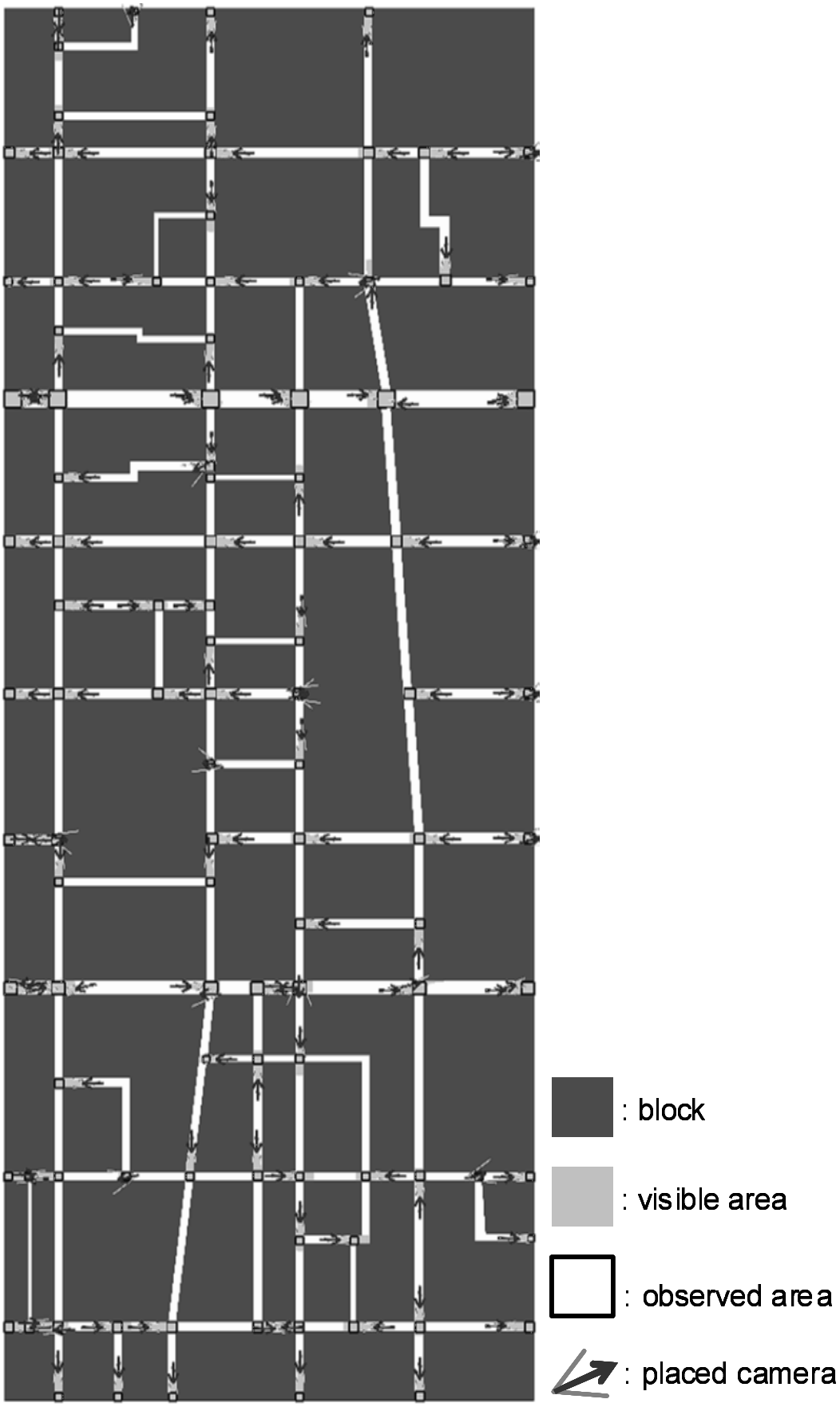


図 4.14 街の一区画をモデルとした実シーンに対して全分岐点を観測する最適カメラ配置.
カメラ台数は 123 台，求解までの時間は 687.37[sec].

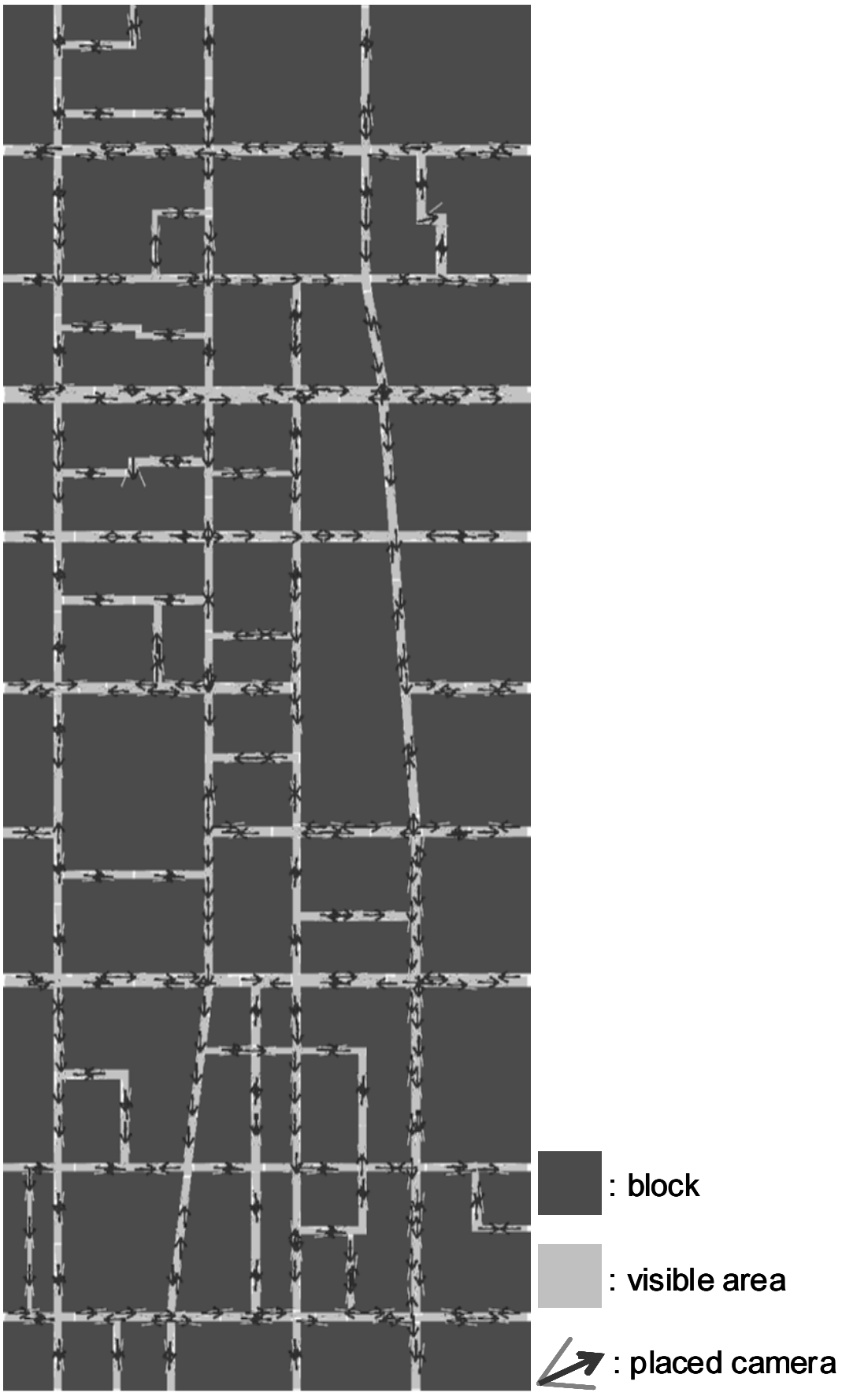


図 4.15 街の一区画をモデルとした実シーンに対してシーン全域を観測する最適カメラ配置.
カメラ台数は 454 台（近似解），実行を 100018.77[sec] で打ち切った.

4.5 本章のまとめ

本章では，監視カメラの自動配置問題において，観測シーンのグラフ構造から最小台数の最適カメラ配置を導く手法を述べた．監視カメラの自動配置に関する従来の手法では，解を得るのに非常に時間がかかることや，多数のカメラが必要となる，観測点やカメラ位置を手動で決める必要がある，局所解に陥るなどといった問題がある．提案手法では，物体のシーン内での移動経路を示すフローを特定できる，という観測問題のモデル化から，観測シーンの分岐点を観測すればよいことを示した．また，頂点被覆問題と集合被覆問題の 2 ステップの解法により上記の問題を解決した．まず，観測シーンが矩形領域で近似できることを仮定して，出入り口，通路，分岐点，袋小路の 4 つの構成要素に分解することで，グラフ構造を定めた．すべての通路間の移動を検出するには，通路の少なくとも一端が観測されていればいいことを利用して，定めたグラフ構造から，分岐点の組み合わせを取り出した．分岐点の組み合わせは多数存在するため，観測面積を最小化するように，合計面積が最小になる分岐点の組み合わせを頂点被覆により求めた．次に，頂点被覆により求めた分岐点の組み合わせから，観測エリアを求め，エリア内全てを観測できる最小台数のカメラ配置を集合被覆により求めた．実験結果から，シーン全域を観測するカメラ配置を得る解法に比べ，提案手法は処理時間の短縮，カメラ台数の削減が実現できることを示した．また，提案手法は，カメラ位置，カメラ向き，視野角視野距離のカメラ仕様からあらゆる組み合わせのカメラ候補を自動生成するため，集合被覆の規模が巨大になるが，2 ステップの解法を採用したため，短時間で最適解を得られることを示した．実験では，提案手法は実際に存在する環境をモデルとした実シーンでの実験においても，処理時間の削減，カメラ台数の削減といった効果があり，監視カメラの自動最適配置法として有効であることが示された．

第 5 章

結論

本論文では，監視カメラシステムにおけるプライバシー保護の実現と，システム構築についてまとめた．従来の監視カメラなどを対象とした研究は，撮影画像からの特徴量抽出や画像解析などに基づく，ITS やマーケッティングへの応用などを中心に行われてきた．一方で，安心安全社会の構築に不可欠な課題でありながらも，カメラに映る人物のプライバシー保護の実現や，システム構築の最適化を目指す研究は，報告が少ない．そこで，本論文では，監視カメラによって撮影した画像中に存在する，人物や物体への画像処理により不可視化する，プライバシー保護手法を提案した．提案手法は，不可視化され特定不可能になった物体を，電子透かしによって出力画像に埋め込んだ情報を元に復元し撮影画像を再構成できる．この提案により，プライバシー保護と，移動物体の特定や追跡との両立を可能にした．次に，プライバシー保護された画像から再構成した画像中の人物が，改竄や合成されたものではなく，もともとの撮影画像中に実在したことを証明しなければならない．そこで，この再構成画像が撮影画像に対して真正であることを証明できる機能を備えた，プライバシー保護手法を提案した．さらに，目的の観測シーンに進入する，すべての移動物体の移動経路を見落とすことなく観測できる，最小台数のカメラ配置の最適化法を提案し，監視カメラシステムの構築方法について述べた．

第 2 章では，監視カメラによって撮影した画像中の，人物や物体へのプライバシー保護手法を述べた．監視カメラを対象にプライバシー保護を実現するため，撮影画像中の人物の特定を不可能にしながらも，物体の形状はそのまま残すことで，行動の推測や異常行動の発見ができるようにした．従来の画面全体を覆い隠す処理と異なり，物体形状が明確なため，プライバシー保護と行動の把握を両立でき，監視目的に支障をきたさない．物体形状を残すために，背景差分法を用いて撮影画像を移動物体と背景領域に分離し，移動物体のみを画像処理によって不可視化した．さらに，犯罪捜査などに応用するため，撮影画像の復元情報を電子透かしにより，出力ストリーム中に埋め込んだ．提案手法では，抽出移動物体をトラッキングし，その情報に基づいて物体固有の暗号鍵を割り当てた．そのた

め，画像中に複数の人物が存在しても，目的の人物のみを復元しながらも，その他の人物はプライバシー保護されたままできる．また，複数のフレーム間で注目する人物のみを，連続的に復元する処理が可能である．これにより，たまたま注目物体と同時に画面内に映り込んでしまった，監視不要の移動物体が注目物体とともに復元されることが避けられる．電子透かしを用いて暗号化ストリームを埋め込むため，適用可能な移動物体の大きさに限界があること，出力 JPEG ストリームの圧縮効率の低下，といった問題が推測される．これに対し，実験から，画面全体を覆う大きさの移動物体であっても，提案手法が適用可能であることを示した．また，移動物体が大きくなるにつれて出力 JPEG ストリームの符号長は長くなるが，JPEG 圧縮による符号長削減の効果が保たれていることを示した．

第 3 章では，真正性証明機能を備えたプライバシー保護手法を提案した．RSA 公開鍵暗号方式と電子証明を応用し，プライバシーを保護した画像から再構成した撮影画像が，もともとの撮影画像に対して真正であり，改竄や合成された画像でないことを証明する手法である．従来の真正性証明手法は，プライバシー保護のための画像処理を，改竄と判別してしまう．そのため，従来法を活用するためには，撮影画像の復元情報や真正性を証明する情報を，画像と別に保存しておき，撮影画像へ完全に再構成してから真正性を検証しなければならない．この方法では，出力されたデータの符号長の総計がもともとの撮影画像より増大することや，撮影画像を再構成してからでないと真正性が検証できない，という問題点を抱えている．提案手法では撮影画像への再構成を必要とせずに，移動物体のプライバシーを保護したままで真正性が証明できる．撮影画像を復元してからでないと真正性が検証できない従来法と異なり，改竄された画像から，被撮影者のプライバシーが開示されることを防ぐことができる．また，撮影画像復元用データを埋め込む電子透かしにおいて，ハフマン符号化の特性を利用して，係数の値から埋め込み位置を選ぶことにより，出力ストリームの符号長増加を抑えた．実データを用いた実験により，撮影画像を再構成せずに，プライバシー保護をしたまま，再構成画像の真正性が証明できることを示した．また，移動物体の大きさと出力 JPEG ストリームの符号長の関係を示し，一定の大きさの移動物体までは，出力符号長が減少することを示した．出力符号長が増加しない移動物体の大きさでも，プライバシー保護画像からは物体の形状，再構成画像からは物体を特定するための顔領域などが十分に認識できることを示した．また，実行時間に関して，動画撮影のフルレートは下回るものの，監視用途には支障の無い速度であった．提案手法における，改竄攻撃への耐性は，RSA 公開鍵暗号方式やハッシュ計算の強度にのみに依存する．これらは十分な強度を持つため，提案手法は十分実用できる頑健性を持つ．さらに，これらの研究の進展により，より強固な耐性を持つ手法が提案されれば，それに伴い提案手法の耐性も高くすることができる．今後の課題として，実行速度をフルレート，ハーフレートに近づけるための高速化があげられる．RSA 公開鍵暗号方式の計算には時間がか

かるため，共通鍵暗号を組み合わせて利用することで，RSA 暗号化の計算回数を抑える方法が考えられる．

第 4 章では，監視カメラの自動配置問題において，観測シーンのグラフ構造から最小台数の最適カメラ配置を求める手法を述べた．従来のカメラ自動配置手法では，対象となる環境が，狭い空間であったり，観測位置やカメラ候補位置などが限定的なものであることが多い．そのため，これらの手法を，街中などの広い空間に適用しても，解を得られる確証がない．さらに，解を得られたとしても求解までに非常に時間がかかることや，カメラ台数が膨大になるといった問題がある．対象となる空間が広い場合，空間全体ではなく観測が必須な領域をあらかじめ定め，限定する方法が有効である．従来手法では，観測必須な領域を定めるには手動での操作がほとんどである．広大な空間に，領域を手動設定するのはコストが高く，自動的に領域を限定できることが必要である．提案手法では，物体のシーン内での移動経路を示すフローを特定できる，という観測問題のモデル化から，観測シーンの分岐点を観測すればよいことを示した．まず，観測シーンから，観測必須な領域を定めた．分岐点は，観測シーンの形が決まれば，そのグラフ構造を元に，自動的に取り出すことができる．与えられた観測シーンが矩形領域で近似できることを仮定し，出入り口，通路，分岐点，袋小路の 4 つの構成要素に分解することで，グラフ構造を定めた．フローの特定は，すべての通路について，少なくともどちらかの一端が観測されていれば可能であることを利用して，分岐点の組み合わせを取り出した．この条件を満たす分岐点の組み合わせは，一つの観測シーンに多数存在する．そのため，その中で合計面積が最小となる組み合わせを頂点被覆により決定した．次に，カメラ位置，カメラ向き，視野角視野距離のカメラ仕様からあらゆる組み合わせのカメラ候補を自動生成し，これらのカメラから観測できる領域を求めた．頂点被覆により求めた分岐点に基づき観測エリアを作り，エリア内全てを観測できる最小台数のカメラ配置を，カメラ候補と，その可視性から，集合被覆により求めた．学内や街の一区画などの，実在する環境をモデルに作成したシーンを対象に，実験を行なった．実験より，シーン全域を観測する場合や，すべての分岐点を観場合に比べ，提案手法はカメラ台数が削減でき，さらに，実行時間を短縮できた．提案手法は，カメラ候補の数が多く集合被覆の規模が巨大になるが，観測領域を決めるための頂点被覆，カメラ最適配置を求めるための集合被覆の 2 ステップの解法により最適化するため，短時間に解を得やすい集合被覆問題に帰着することができる．今後の課題として，移動カメラやロボット搭載カメラでの巡回警備問題への拡張が挙げられる．

序論に述べたとおり，監視カメラの設置が防犯や犯罪捜査での実績をあげている．そのため，これからも治安向上や状況把握のために，監視カメラは増え続けて行くと考えられる．イギリスでの例を見ても，監視カメラの設置が進んだ社会では，自分自身が撮影されることは避けられない．また，同時に，自分が設置した監視カメラが，誰かのプライバシーを侵害してしまうことも十分起こりうる．つまり，安心や安全のための監視カメラ

が，新たな加害や被害を生む可能性を持っている．そのため，プライバシー保護機能と真正性証明機能を兼ね備えた監視カメラシステムはこれから注目されていく研究であろう．また，監視カメラを設置するとき，無尽蔵に多くのカメラを設置と，構築や管理のコストがかさみ十分な費用対効果が得られない．最小のカメラ台数で効率的にシーン内の人物を観測できる監視カメラシステムを，手動での煩雑な操作を必要とせずに構築する提案手法は，これからの社会に貢献するであろう．本論文にて提案した，監視カメラにおけるプライバシー保護の実現とシステムの構築手法が，これからの社会の安心性や利便性の向上の一助となれば幸いである．

謝辞

本研究を行う貴重な機会を与えてくださり，懇切なる御指導と御鞭撻を賜りました，東京農工大学工学部電気電子工学科教授 北澤仁志先生に，心より深謝いたします．

“Privacy Protection by Masking Moving Objects for Security Cameras” の研究，論文投稿にあたり画像処理，信号処理の御指導，英語論文の構成に関する多くの助言を頂きました東京農工大学工学部電気電子工学科准教授 田中聡久先生に深く感謝いたします．

本論文の審査過程において，快く副査を引き受けてくださりました，東京農工大学工学部電気電子工学科教授 関根優年先生，涌井伸二先生，東京農工大学工学部情報工学科教授 中森眞理雄先生，東京農工大学工学部電気電子工学科准教授 清水昭伸先生に感謝いたします．

多くの御議論，御助言をしていただきました助教 富岡洋一先生，技術職員 梅澤淳先生に感謝いたします．

移動物体抽出手法の研究や英語論文の執筆に惜しみない協力をしてくださった東京農工大学工学府電子情報工学専攻 李竹氏，“移動物体のフロー検出のためのカメラ配置最適化” の研究，論文投稿にあたり協力してくださった東京農工大学工学府電気電子工学専攻 高良惇氏をはじめ，ゼミでの闊達な議論や多くの助言をいただいた北澤研究室のメンバーに感謝いたします．

参考文献

[1] “街頭防犯カメラシステム：警視庁,” http://www.keishicho.metro.tokyo.jp/seian/gaitoukamera/gaitoukamera.htm.

[2] イギリス情報委員会 (InfomationCommissioner) 委託，“監視社会に関する報告書 (a report on the surveillance society),” http://www.ico.gov.uk/upload/documents/library/data_protection/practical_application/surveillance_society_full_report_2006.pdf，2006.

[3] I. Kitahara, K. Kogure, and N. Hagita, “Stealth vision for protecting privacy,” in Proc. of 17th International Conference on Pattern Recognition (ICPR 2004), vol.4, pp.404–407, 2004.

[4] J. Wickramasuriya, M. Alhazzazi, M. Datt, S. Mehrotra, and N. Venkatasubramanian, “Privacy-protecting video surveillance,” in Proc. SPIE, vol.5671, pp.64–75, San Jose, CA, USA, Feb. 2005.

[5] A. Senior, S. Pankanti, A. Hampapur, L. Brown, Y.L. Tian, and A. Ekin, “Blinkering surveillance: Enabling video privacy through computer vision,” Technical Report RC22886 (W0308-109), IBM Technical Paper, Aug. 2003.

[6] 田森秀明，青木直史，山本強，“数論変換による脆弱型電子透かしを用いた改ざん位置検出法,” 電子情報通信学会論文誌 (A)，vol.J86-A，no.8，pp.872–879，2003.

[7] 黒田圭一，西垣正勝，曽我正和，田窪昭夫，“公開鍵暗号を用いたアルゴリズム公開型電子透かし,” 2002 年暗号と情報セキュリティシンポジウム予稿集，pp.763–768，2002.

[8] 科学技術振興機構 西垣正勝，黒田圭一，杉本友幸，曽我正和，“電子透かし埋め込みシステム・電子透かし検証システム,” 特許開 2005-039686，2003.7.18.

[9] 片山淳，北原亮，川村春美，小池秀樹，“アルゴリズム公開型フラジャイル電子透かし カメラ付携帯電話機への実装,” 映像情報メディア学会技術報告，vol.33，no.8，pp.9–12，2009.

[10] J. O’Rourke, Art Gallery Theorems and Algorithms, Oxford University Press,

1987.

[11] S. Nikolaidis, R. Ueda, A. Hayashi, and T. Arai, “Optimal camera placement considering mobile robot trajectory,” in Proc. of the 2008 IEEE International Conference on Robotics and Biomimetics (ROBIO2008), pp.1393–1396, Bangkok, Thailand, 2008.

[12] E. Hörster, and R. Lienhart, “On the optimal placement of multiple visual sensors,” in Proc. of the 4th ACM international workshop on Video surveillance and sensor networks (VSSN ’06), pp.111–120, Santa Barbara, CA, USA, 2006.

[13] A.T. Murray, K. Kim, J.W. Davis, R. Machiraju, and R.E. Parent, “Coverage optimization to support security monitoring,” Computers, Environment and Urban Systems, vol.31, no.2, pp.133–147, 2007.

[14] F. Janoos, R. Machiraju, R. Parent, J.W. Davis, and A. Murray, “Sensor configuration for coverage optimization for surveillance applications,” in Proc. SPIE Conference on Videometrics IX, vol.6491, p.649105, San Jose, CA, USA, 2007.

[15] W.B. Pennebaker, and J.L. Mitchell, JPEG: still image data compression standard, Springer, 1993.

[16] C. Stauffer, and W.E.L. Grimson, “Adaptive background mixture models for real-time tracking,” in Proc. CVPR ’99, vol.2, pp.246–252, Fort Colins, CO, USA, Jun. 1999.

[17] A. Lipton, H. Fujiyoshi, and R.S. Patil, “Moving target detection and classification from real-time video,” in Proc. IEEE WACV ’98, Nov. 1998.

[18] W.E.L. Grimson, C. Stauffer, R.A. Romano, and L. Lee, “Using adaptive tracking to classify and monitor activities in a site,” in Proc. CVPR ’98, pp.22–29, Santa Barbara, CA, USA, Jun. 1998.

[19] R. Collins, A. Lipton, T. Kanade, H. Fujiyoshi, D. Duggins, Y. Tsin, D. Tolliver, N. Enomoto, and O. Hasegawa, “A system for video surveillance and monitoring,” Technical Report CMU-RI-TR-00-12, Robotics Institute, Carnegie Mellon University, Pittsburgh, PA, USA, May. 2000.

[20] P. Rosin, and T. Ellis, “Image difference threshold strategis and shadow detection,” in Proc. of the British Machine Vision Conference, pp.347–256, 1995.

[21] B.K.P. Horn, and B.G. Schunck, “Determining optical flow,” ARTIFICAL INTELLIGENCE, vol.17, pp.185–203, 1981.

[22] J.Y. Bouguet, “Pyramidal implementation of the lucas kanade feature tracker description of the algorithm,” Intel Corporation Microprocessor Research Labs. OpenCV Documents, 1999.

[23] Z. Li, K. Yabuta, and H. Kitazawa, “Exclusive block matching for moving object extraction and tracking,” IEICE Trance. Inf. & Syst. (条件付き採録).

[24] Z. Li, K. Yabuta, and H. Kitazawa, “A new method for moving object extraction and tracking based on the exclusive block matching,” in Proc. of The 3rd Pacific-Rim Symposium on Image and Video Technology (PSIVT 2009), pp.249–260, Jan. 2009.

[25] 北澤仁志，李竹，藪田顕一，“排他的ブロックマッチングによる移動物体の抽出と追跡,” 電子情報通信学会技術研究報告，信号処理，SIP2008-9 (EI2008-9)，vol.108, no.3，pp.49–54，Apr. 2008.

[26] 李竹, 藪田顕一, 北澤仁志, “排他的ブロックマッチングによる移動カメラ映像中の目標物の探索,” FIT2008 第 7 回情報科学技術フォーラム, H-020，pp.103–104，Sep. 2008.

[27] C.J. Veenman, M.J. Reinders, and E. Backer, “Resolving motion correspondence for densely moving points,” IEEE Transactions on Pattern Analysis and Machine Intelligence, vol.23, no.1, pp.54–72, 2001.

[28] “Announcing the advanced encryption standard AES,” `http://csrc.nist.gov/publications/fips/fips197/fips-197.pdf`.

[29] 小暮正道，松田博，“ハードウェアによる des 暗号化・復号化技術の実現,” OMRON TECHNICS，vol.43，no.3，pp.293–298，2003.

[30] 松田博，“ハードウェアによる aes 次世代暗号技術の実現,” OMRON TECHNICS，vol.43，no.3，pp.299–303，2003.

[31] 情報処理振興事業協会，通信放送機構，“暗号技術評価報告書 (2002 年度版) cryptec report 2002,” ，Mar. 2003.

[32] “IBM ILOG CPLEX,” `http://www-01.ibm.com/software/integration/optimization/cplex/`, 2009.

[33] B. Korte，J. Vygen 著，浅野孝夫，平田富夫，小野孝男，浅野泰仁訳，組み合わせ最適化 理論とアルゴリズム，シュプリンガー・フェアラーク東京，東京，2005.

[34] 伊理正夫，白川功，梶谷洋司，篠田庄司，演習グラフ理論 基礎と応用，コロナ社，東京，1983.

研究業績

■原著論文

(1) Kenichi Yabuta, Hitoshi Kitazawa and Toshihisa Tanaka, “ Privacy protection by masking moving objects for security cameras,” IEICE Trans. Fundamentals, vol.E92-A, no.3, pp.919–927, Mar. 2009.

(2) 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.

(3) 藪田 顕一，高良 惇，北澤 仁志，“ 移動物体のフロー検出のためのカメラ配置最適化,” 電子情報通信学会論文誌 (A)，vol.J93-A, no.3, Mar. 2010.（掲載予定）

■査読付国際会議

(1) Kenichi Yabuta, Hitoshi Kitazawa and Toshihisa Tanaka, “ A new concept of security camera monitoring with privacy protection by masking moving objects,” in Proc. of the 2005 Pacific-Rim Conference on Multimedia (PCM 2005), Proc. SPIE 3768 of Lecture Notes in Computer Science, pp.831–842, Jeju, Korea, Nov. 2005.

(2) Kenichi Yabuta, Hitoshi Kitazawa and Toshihisa Tanaka, “ A new concept of real-time security camera monitoring with privacy protection by masking moving objects,” in Proc. of Electronic Imaging 2006, vol.6063, p.60630, San Jose, California, USA, Jan. 2006.

(3) Kenichi Yabuta and Hitoshi Kitazawa, “ Optimum camera placement considering camera specification for security monitoring,” in Proc. of 2008 IEEE International Symposium on Circuits and Systems (ISCAS 2008), pp.2114–2117, Seattle, WA, USA, May. 2008.

■国内査読無会議

(1) 藪田 顕一，北澤 仁志，田中 聡久，“ プライバシー保護と被写体の識別を両立させる固定モニタカメラ映像処理手法,” 電子情報通信学会技術研究報告, 信号処理, SIP2005-3 (IE2005-3), vol.105, no.29, pp.13–18, 機械振興会館, 東京, Apr. 2005.

(2) 藪田 顕一，北澤 仁志，田中 聡久，“ プライバシ保護と物体の識別を両立する固定モニタカメラ映像処理手法,” 第 8 回 DSPS 教育者会議 予稿集, pp.63–66，東京工業大学大岡山キャンパス, 東京, Aug. 2006.

(3) 藪田 顕一，北澤 仁志，田中 聡久，“ プライバシ保護と物体の識別を両立するための動画像処理手法の検討,” 情報処理学会 第 69 回全国大会, 4P-6，東京，Mar. 2007.

(4) 藪田 顕一，北澤 仁志，田中 聡久，“ プライバシ保護のための動画像処理におけるフレーム間相関の利用,” 電子情報通信学会技術研究報告, 信号処理, SIP2007-1 (IE2007-1), vol.107, no.22, pp.1–6, 機械振興会館, 東京, Apr. 2007.

(5) 高良 惇，藪田 顕一，北澤 仁志，“ 集合被覆問題に基づくモニタカメラの最適配置手法,” 画像電子学会 第 36 回年次大会 S3-3, Jun. 2008.

(6) 高良 惇，藪田 顕一，北澤仁志，“ 複数カメラでの観測や接続コストを考慮したモニタカメラの最適配置,” 2009 年映像情報メディア学会年次大会, 4-10, Aug. 2009.

(7) 藪田 顕一，北澤 仁志，“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,” 情報処理学会 創立 50 周年記念（第 72 回）全国大会, 2010.

■解説

(1) 北澤 仁志，藪田 顕一，“ 映像要約とプライバシー保護機能を備えたモニタカメラシステム,” 月刊自動認識, 日本工業出版, vol.22, no.11, pp.40–42, Sep. 2009.

(2) 北澤 仁志，藪田 顕一，“ 真正性証明とプライバシー保護システムを両立する監視カメラシステム,” 画像ラボ, 日本工業出版, Jun. 2009. (掲載予定)

■特許

(1) “ 映像変更装置、変更映像フレームのデータ構造、映像復元装置、映像変更方法、映像復元方法、映像変更プログラムおよび映像復元プログラム”
発明者：北澤 仁志，田中 聡久，藪田 顕一
出願人：国立大学法人東京農工大学
特願 2005-301072
特開 2007-110571

■関連論文

(1) Zhu Li, Kenichi Yabuta, and Hitoshi Kitazawa, “ Exclusive block matching for moving object extraction and tracking,” IEICE Trance. Inf. & Syst. (条件付き採録)

(2) Zhu Li, Kenichi Yabuta, and Hitoshi Kitazawa, “ A new method for moving object extraction and tracking based on the exclusive block matching,” in Proc. of The 3rd Pacific-Rim Symposium on Image and Video Technology (PSIVT 2009), pp.249–260, Jan. 2009.

(3) 北澤 仁志, 李 竹, 藪田 顕一, “ 排他的ブロックマッチングによる移動物体の抽出と追跡,” 電子情報通信学会技術研究報告, 信号処理, SIP2008-9 (EI2008-9), vol.108, no.3, pp.49–54, Apr. 2008.

(4) 李 竹, 藪田 顕一, 北澤 仁志, “ 排他的ブロックマッチングによる移動カメラ映像中の目標物の探索,” FIT2008 第 7 回情報科学技術フォーラム, H-020, pp.103–104, Sep. 2008.

参考資料

■警視庁公表の街頭防犯カメラシステム整備地区における犯罪認知件数の推移

表 6.1 は，警視庁が公表している街頭防犯カメラシステムを設置した歌舞伎町地区，宇田川町地区，池袋地区，上野 2 丁目地区，六本木地区，それぞれの犯罪認知件数の推移である．いずれの地区も設置前年からの件数を示しており，平成 13 年〜平成 20 年は年間の件数，さらに平成 20 年と平成 21 年は 1〜6 月の上半期の件数を示している．表内の () 内の数値は路上犯罪の認知件数を示している．犯罪認知件数の推移は，監視カメラの設置が犯罪抑止に効果的であることを示している．

表 6.1 街頭防犯カメラシステム整備地区の刑法犯認知件数.

地区	平成 13 年	平成 14 年	平成 15 年	平成 16 年	平成 17 年
運用開始日	年間	年間	年間	年間	年間
歌舞伎町	1,865	2,103	2,249	2,042	1,513
平成 14 年 2 月	(634)	(571)	(703)	(541)	(458)
宇田川町			1,722	1,405	1,322
平成 16 年 3 月			(280)	(233)	(227)
池袋			3,233	2,936	2,702
平成 16 年 3 月			(1,111)	(1,011)	(862)
上野 2 丁目					505
平成 18 年 2 月					(145)

地区	平成 18 年	平成 19 年		平成 20 年	平成 21 年
運用開始日	年間	年間	年間	1〜6 月	1〜6 月
歌舞伎町	1,686	1,815	1,694	829	918
平成 14 年 2 月	(479)	(487)	(487)	(219)	(221)
宇田川町	1,252	1,194	1,110	585	400
平成 16 年 3 月	(219)	(161)	(112)	(59)	(47)
池袋	2,252	2,501	2,234	1,086	1,051
平成 16 年 3 月	(852)	(746)	(562)	(261)	(241)
上野 2 丁目	411	411	449	205	226
平成 18 年 2 月	(151)	(139)	(160)	(68)	(71)

地区	平成 18 年	平成 19 年		平成 20 年	平成 21 年
運用開始日	年間	年間	年間	1〜6 月	1〜6 月
六本木	1,231	1,057	929	444	473
平成 19 年 3 月	(301)	(218)	(231)	(109)	(121)