Vol.2015-DPS-162 No.43
Vol.2015-CSEC-68 No.43
2015/3/6

BloomFilter と Kinect を用いたプライバシーに考慮した屋内における迷子探索

矢島卓[†1]　宇田隆哉[†2]

近年，子供が巻き込まれる犯罪や事故が多発している．これらの犯罪や事故の多くは子供が親の目の届かない場所に居る時に起こりやすい．この様な事故や犯罪を防ぐために様々な迷子探索の研究・製品の開発がされている．しかし，既存の研究・製品は子供から目を離しやすいスーパーマーケットやデパートといった，Global Positioning System(GPS)の測位精度が低くなる屋内での利用に適していない．これに対し，不審者の捜索に使われている監視カメラを用いて類似する人物を映像から検索する技術は屋内であっても迷子探索に十分な効果が期待できる．しかし，これらのシステムは顔の情報を保存するため，プライバシーの問題があり，漏洩時にストーカー行為へ発展する懸念がある．また，人物を探索するための特徴情報と映像を保存するには大容量の記憶装置が必要になる．このような情報の格納先としてクラウドストレージが注目を集めているが，外部のクラウドストレージを利用すると管理者が異なるため，情報漏洩の懸念がある．そこで我々は，監視カメラの代わりに深度センサと RGB カメラを内蔵したデバイスである Kinect を用いて顔の特徴を利用しないプライバシーに考慮した屋内での迷子探索を提案した．私が提案した手法では人物を探索するのに用いる情報を Bloom Filter を用いてクラウドストレージに保存することで不正に閲覧された場合でも人物を特定することを困難にしている．また，撮影した映像は秘密分散法を用いてそれぞれの異なるクラウドストレージに保存される．秘密分散法を用いることでクラウドストレージの管理者が不正に映像を閲覧できないようにしている．

Lost Child Search Using BloomFilter and Kinect

TAKU YAJIMA[†1]　RYUYA UDA[†2]

In recent years, crime and accidents that children are caught are frequently. Many of these crimes and accidents are likely to occur when the child is in a place that is out of the reach of the parent of the eye. Has been the development of research and product in a variety of lost search in order to prevent such accidents and crimes. However, existing research and products, such as easy to supermarkets and department stores to release the eye from the children, not suitable for use in indoor positioning accuracy of Global Positioning System (GPS) is lowered. In contrast, a person of similar technology for searching from the image can be expected sufficient effect lost search even indoors using a surveillance camera that is used to search for a suspicious person. However, these systems for storing information of the face, there are privacy issues. There is a concern that development to stalking during leakage. Furthermore, the large-capacity storage device be required to save the feature information and the video for searching a person. The cloud storage as the storage destination of such information has attracted attention, but for the administrator to use the external cloud storage are different, there is a fear of information leakage. So we proposed a lost search in considering the privacy of not using the facial features using a device with a built-in depth sensor and RGB camera in place of the monitoring camera Kinect indoors. To the BloomFilter the information which can be used to search a person in this proposed method.I want to save this BloomFilter to cloud storage. And is it difficult to identify a person, even if the administrator has an illegal viewing.Also, images taken are stored in respective different cloud storage using a secret sharing scheme. Administrators cloud storage by using the secret sharing method is to prevent viewing illegally image.

1. はじめに

近年，子供が巻き込まれる犯罪や事故が多発している．警察庁の調べによると 13 歳未満の子供が被害者となった刑法犯の認知件数は，平成 25 年中は 2 万 6,939 件となっており[1]，これらの犯罪や事故の多くは子供が親の目の届かない場所に居る時に起こりやすい．この様な事故や犯罪を防ぐために様々な迷子探索の研究・製品の開発がされている[2][3][4][5][6][7][8][9][10]．しかし，既存の研究・製品は子供から目を離しやすいスーパーマーケットやデパートといった，Global Positioning System(GPS)の測位精度が低くなる屋内での利用に適していない．これに対し，不審者の捜索に使われている監視カメラを用いて類似する人物を映像から検索する技術は屋内であっても迷子探索に十分な効果が期待できる[11][12][13][14][15][16]．しかし，これらのシステムは顔の情報を保存するため，プライバシーの問題があり，漏洩時にストーカー行為へ発展する懸念がある．また，人物を探索するための特徴情報と映像を保存するには大容量の記憶装置が必要になる．このような情報の格納先としてクラウドストレージが注目を集めている．しかし，クラウドストレージの管理者はクラウドストレージに格納された情報を自由に閲覧できるため，情報漏洩の懸念がある．そこで私は，監視カメラの代わりに Kinect を用いて顔の特徴を利用しないプライバシーに考慮した屋内での迷子探索を提案する．

†1 東京工科大学大学院バイオ・情報メディア学部
Graduate School of Bionics, Computer and Media Science ,Tokyo University of Technology

†2 東京工科大学コンピュータサイエンス学部
School of Computer Science ,Tokyo University of Technology

2. 既存研究

本章では，迷子探索と類似の人物探索の既存の研究・製品ついて記述する．

2.1 迷子探索の既存研究

GPS を用いた迷子探索では子供に GPS を搭載した携帯電話端末機器を持たせておき，子供が迷子になった時 WEB サイトから子供の居場所を調べることができる．GPS を使って現在位置を求める原理はまず，GPS 衛星が電波を発信した時刻と，受信した時刻の時間差に電波の伝播速度を掛けることで，その衛星からの距離を知ることが出来る．次に，この距離を 3 つ以上の異なる衛星について測定することで，地球上の現在位置を知ることが出来るという仕組みである．2 つから 3 つの衛星からの距離を測定できる場所では，経度と緯度を知ることができ，4 つの衛星からの距離を測定できる場所では，経度と緯度に加えて高度を割り出すことが出来る．しかし，上空からの電波であるため，屋内や地下など受信機の上部が遮られる環境では，電波が受信不能になり，測位出来ない事がある．また，ビル街などでは電波がビルによって屈折してしまうことで，正確な位置を求める事が出来なくなる可能性がある．そのため屋内での迷子探索に適していない．屋内の迷子探索を行う研究としてイオン株式会社と NTT ドコモの迷子探しサービス[2]がある．これは施設に子供連れで訪れた時に専用機器を貸し出し，子供が迷子になった場合に，i モードなどのインターネット接続サービスを利用して施設内のどのエリアにいるのかを確認できるサービスである．このサービスでは，施設内に設置された屋内基地局設備 InbuildingMobile CommunicatinSystem(IMCS)を用いて位置の取得を行っている．しかし，これらのサービスでは当然ながら事前に専用機器を子供に持たせなくてはならず，IMCS を導入していない施設では利用できない．

2.2 人物映像検索の既存研究

人物映像検索の研究として[11][12][13][14][15][16]がある．これらのシステムは監視カメラ等で録画した映像から，人物の年齢・性別・身長・衣類などの特徴に該当する人物を検索することができる．また，あらかじめ見つけたい人物の特徴を設定することで特定の人物をリアルタイムで検出可能である．これらのシステムは映像を録画し，顔のデータを抽出して記憶装置に保存するため，プライバシーの問題がある．

3. 提案概要と要素技術

本章では課題と提案概要を 3.1 節に，RGB の代わりに HSV を用いる理由を 3.2 節に，本提案手法の要素技術である秘密分散法を 3.3 節に，BloomFilter を 3.4 節に記述する．

3.1 課題と提案概要

既存の研究において第 1 に 2.2 節に記述したように，映像から人物を探索するシステムは，人物の特徴を記憶装置に保存する必要があるため，プライバシーの問題がある．また，第 2 に情報量と容量の増加から大容量の記憶装置が必要となる．これはクラウドサービスによって提供されるクラウドストレージを利用することで容易に解決が可能であるが，外部のサービスを利用することからクラウドストレージの管理者が不正な閲覧を行い，情報が漏洩する懸念がある．

本提案手法は迷子探索において本来監視カメラを設置する場所に Kinect を設置し，店内を撮影する．この時に人物が映った場合映った時間と場所，身長と衣類の上下の HSV 値を Bloom Filter を用いてクラウドストレージに保存する．また，撮影した映像は秘密分散法を用いてそれぞれの異なるクラウドストレージに保存される．迷子を探すユーザは携帯端末で迷子探索システムを使い子供の身長，衣類の HSV 値，入店時間を入力する．探索システムは入力された情報をもとに索引用の BloomFilter を生成し，クラウドストレージから類似する子供を探索する．類似する子供を発見した場合，探索システムは子供が最後に映った Kinect を特定してマップ情報と発見した場所をユーザの携帯端末に送信する．人物の特徴情報が BloomFilter を用いて暗号化されているため，クラウドストレージの管理者は不正に閲覧を行ったとしても個人の特定をできない．また，秘密分散法を用いることでクラウドストレージの管理者が不正に映像の閲覧をするのが困難になる．

3.2 HSV を用いる理由

衣類の色での探索は照明の明るさによって精度の低下が起こる[14]．ユーザ情報に登録する衣類の色の情報を RGB ではなく HSV にし，基準となる明度を決めておき照明の明るさの違う場合に明度の差を補正することで精度の低下を防ぐ．HSV とは色相(Hue)、彩度(Saturation)、明度(Value)の三つの成分からなる色空間のことであり，色相環の赤を 0°として，反時計まわりに緑の位置が 120°，青が 240°と色相を定められる人間から見て直感的に色を指定しやすいカラーモデルである．

3.3 秘密分散法

秘密分散法の手法の 1 つである（k, n）閾値法[17]は，秘密情報を n 個の分散情報に分散し，この分散情報から任意の k 個を収集すると秘密情報が復元できるが，k-1 個の分散情報を収集しても元の秘密情報に復元できない．秘密分散法は，その特長を生かして，主に暗号鍵などの管理に使われているが，データの保護にも利用されている．秘密分散して管理することで，一部の分散情報が紛失しても，情報が漏えいしないので機密性の確保ができ，また，残りの分散情報から復元が可能なため可用性の確保ができる．秘密分散法は計算量的安全性ではなく情報理論的安全性に基づいている．情報理論的安全性とは高性能の計算能力を有するコンピュータを持ってしても，公開情報から暗号文を復号することができないことをいう．

Vol.2015-DPS-162 No.43
Vol.2015-CSEC-68 No.43
2015/3/6

3.4 BloomFilter

BloomFilter とは，1970 年に Burton Howard Bloom により考案された，空間効率の良いデータ構造である．主に要素が集合に含まれているかどうかを検証するために使用される．BloomFilter は，mbit のビット配列であり，それぞれの要素が 0 又は 1 で表される．初期状態ではすべての要素が 0 であるが，データを追加する度にいずれかの要素が 1 となる．1 となる要素の位置は，追加するデータのハッシュ値で決まる．ある要素がその集合に含まれているかどうかを検証する際は，その集合によって生成される BloomFilter の，その要素のハッシュ値が示す位置のビットを調べる．それらのビットがすべて 1 である場合，要素は集合に含まれている可能性がある．そうでない場合，要素は集合に含まれていない．ただし，BloomFilter は偽陽性を持つため，要素が集合に含まれていないにも関わらず，含まれていると判断されることがある．これは，ハッシュ値の衝突によって引き起こされる．Bloom Filter における偽陽性の確率 r は式(1) によって求められる．ここで，m は BloomFilter のフィルタ長，n は集合に含まれる要素数，k は使用するハッシュ関数の数を表す．なお，Fan ら[18]によると，最も効率よくフィルタリングできる k は，式(2) で求められる．

$$r = \left(1 - \left(1 - \frac{1}{m}\right)^{kn}\right)^{k} \quad (1)$$

$$k = \left(\frac{m}{n}\right) ln2 \quad (2)$$

4. 提案手法

本章では，本提案手法の前提を 4.1 節に，想定環境を 4.2 節に，情報の格納方法を 4.3 節に，BloomFilter における近隣数値の判定法を 4.4 節に，迷子の探索方法を 4.5 節に，分散情報の収集手法を 4.6 節に記述する．

4.1 前提

本提案手法はショッピングモールなどの子供が迷子になりやすい屋内で利用される．子供がショッピングモールにいる間は服を着替えることはほとんどないため服の特徴が変化しないものとする．アプリケーションは利用する施設であれば簡単にいつでも使えるように QR cord でダウンロードできるようにしておく.Kinect の配置は Kinect の撮影範囲が約 $4m^2$であることから全体を撮影する様な配置にはできない．そのため図 1 の様に人が通路を出入りする時，必ず Kinect の前を通過する様に配置される．最後に撮影した Kinect がある通路に探索している人物がいるため全体を撮影していない場合でも迷子の探索を行うことができる．

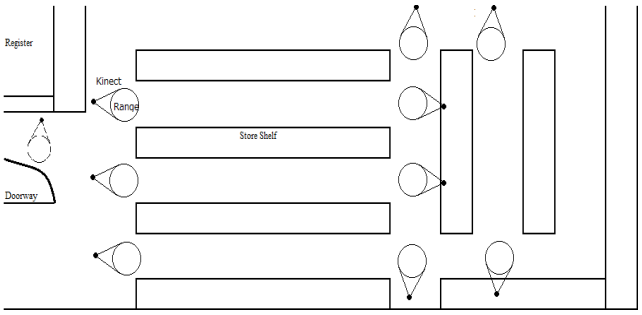

図 1　Kinect の配置

4.2 探索システムの想定環境

図 2 は探索システムの想定環境であり，各エンティティは下記のとおりとなる．

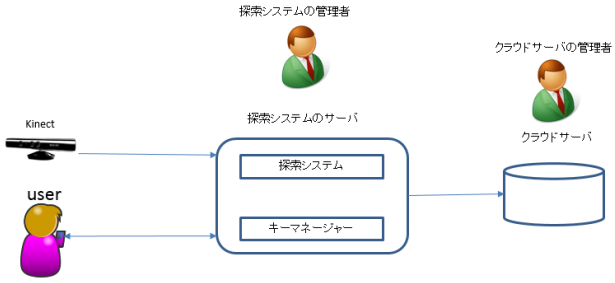

図 2　探索システムの想定環境

4.2.1 探索システムのサーバ

探索システムのサーバ（以下 SS_S）は本提案手法の探索システムが動作するサーバであり，各ショッピングモール等のサーバである. SS_S はネットワーク経由でユーザにサービスの提供を行う. SS_S 内のキーマネージャは暗号鍵の生成と管理を行う．キーマネージャで生成される暗号Key_S_nは一定周期で更新され，更新には現在の暗号鍵のハッシュ値を求め，得られたハッシュ値を次の暗号鍵Key_S_{n+1}とする．添字の n は生成されている暗号鍵のハッシュ回数を示している．キーマネージャの管理は SS_S の管理者（以下 SS_S_A）が行う．また，キーマネージャで生成された暗号鍵は SS_S_A のみが扱える．

4.2.2 探索システムの管理者

SS_S の管理権限を持つ. またキーマネージャの操作権限を持つ.

4.2.3 クラウドストレージ

クラウドストレージ（以下CS_m）は探索システムにより生成されたデータと映像の格納を行う外部のサービスであり，CS_mの管理者（以下CS_A_m）に管理される．本提案手法では複数の異なるクラウドストレージを利用し，添字の m は利用しているクラウドストレージの数を示している．

4.2.4 クラウドストレージの管理者

CS_A_mはそれぞれの異なるCS_mの管理者であり，CS_mに保存されるデータの管理権限を持つ．また，CS_A_mはCS_mと同

Vol.2015-DPS-162 No.43
Vol.2015-CSEC-68 No.43
2015/3/6

じ数だけ存在する．

4.2.5 Kinect

Kinect はマイクロソフトから販売されたジェスチャーによって操作ができる．カメラ，深度センサ，マルチアレイマイクロフォンから構成される．ゲームデバイスであり，本提案手法においてショッピングモールの監視カメラの代わりに複数台設置される．監視カメラの変わりに設置される理由としてカメラからの距離を測定し，人物の身長が測定できる深度センサのあるカメラが必要であり，Kinect は深度センサとカメラがあり安価である．撮影した映像は SS_S に送信される．それぞれの Kinect には個体を識別する必要があるためK_aを振っておく．添え字 a は施設の Kinect の数を示している．

4.2.6 User

User は本提案手法の探索システムの利用者である．

4.2.7 $Customer_s$

$Customer_s$は Kinect に撮影された顧客であり，添字の s は撮影された顧客の数を示している．また，User も顧客に含む．

4.3 映像と BloomFilter の記録

図 3 は探索システムが映像と BloomFilter をクラウドストレージに格納するまでの流れである．各エンティティは下記のとおりとなる．

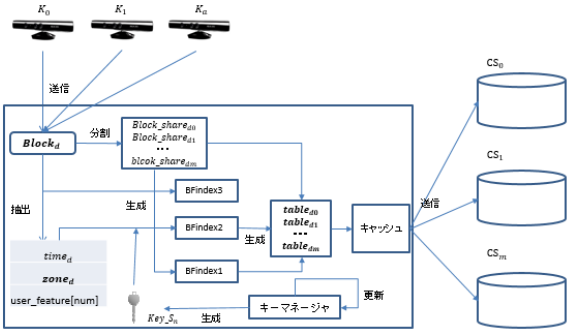

図 3　映像と BloomFilter の格納

4.3.1 $Block_d$

$Block_d$は映像を t 秒毎に圧縮したもの．添字の d は$Block_d$の番号を示している．

4.3.2 $time_d$

$time_d$は$Block_d$が撮影された時刻である．

4.3.3 $zone_d$

$zone_d$は$Block_d$を撮影した Kinect であり，$zone_d$の値はK_aとなる．

4.3.4 num

num は$Block_d$内に映った人物の総数であり，同一人物が同じ$Block_d$内で再度映った場合はカウントしない．

4.3.5 $user\_feature_{num}$

$user_feature_{num}$は$Block_d$に映った人物の特徴をまとめた構造体であり，$height_d$, $color\_top\_h_d$, $color\_top\_s_d$, $color\_top\_v_d$, $color\_bottom\_h_d$, $color\_bottom\_s_d$, $color_bottom_v_d$で構成される．$height_d$は$Block_d$に映った人物の身長である．$color\_top\_h_d$, $color\_top\_s_d$, $color_top_v_d$は$Block_d$に映った人物が着用している衣類の上半身部分の HSV の各値である．同様に，$color\_bottom\_h_d$, $color\_bottom\_s_d$, $color_bottom_v_d$は衣類の下半身部分の HSV の各値となる．

4.3.6 $Block\_share_{dm}$

$Block_share_{dm}$は秘密分散法の一つである(k,m)閾値法を用いて$Block_d$を単独では意味の無い断片に分割したものであり，添え字の m は$Block_d$を分割した総数であり，データの保存先となるCS_mの総数である．この$Block_share_{dm}$から任意の k 個を集めると，元の$Block_d$を復元できる．一方，任意の k-1 個の$Block_share_{dm}$を集めても，元の情報は全くわからない．また，一部の$Block_share_{dm}$が紛失，漏洩しても機密性の確保ができ，残りの$Block_share_{dm}$から復元が可能なため可用性の確保ができる．(k,m)閾値法の原理を(2, 3)閾値で説明する．傾き a をランダムに決定し，$Block_d$を y 切片とする(3)式の直線から，任意の 3 点(x1, y1)，(x2, y2)，(x3, y3)を選択し，これを$Block_share_{dm}$とする．

$$y = ax + Block_d \tag{3}$$

これにより，2 つの$Block_share_{dm}$で$Block_d$を復元でき，1 つの$Block_share_{dm}$では$Block_d$を復元できない仕組みが実現する．なお，k≧3 の場合は，(k-1)次曲線を利用する．CS_A_mは$Block_d$を閲覧するには$Block_share_{dm}$を k 個集めなければならず，管理者の違う他のCS_mを探査し，各々のCS_A_mが結託して不正を行わないとならないため困難である．

4.3.7 BFindex1

$Block\_share_{dm}$，$time_d$，$zone_d$，$height_d$の 4 つの属性がデータベース登録用の要素として生成される．各々の登録要素はKey_S_nを鍵に k 個のハッシュ関数$Hash_k$を適用される．算出された k 個のハッシュ値の bit 列が 1 の BloomFilter が生成され，生成された BloomFilter の論理和が BFindex1 である．算出されたハッシュ値が重複した場合，重複した bit 列を 1 にするために論理和が用いられる．また，$height_d$は num の値が 2 以上の場合，num の数値ぶんの異なる登録用の要素が生成される．各々の登録要素を X とし，Key_S_nを鍵に k 個のハッシュ関数$Hash_k$を適用し，算出されたハッシュ値をHX_{kn}とすると(4)の式でHX_{kn}を求めることができる．添字の k は適用しているハッシュ関数の番号であり，添字 n は利用している暗号鍵の番号である．BFindex1 の生成例を図 4 に示す．

$$HX_{kn} = Hash_k(X \| Key\_S_n) \tag{4}$$

Vol.2015-DPS-162 No.43
Vol.2015-CSEC-68 No.43
2015/3/6

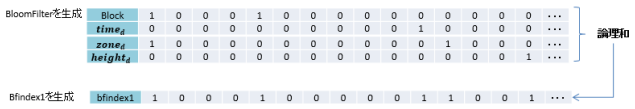

図 4　BFindex1 の生成例

4.3.8 BFindex2

BFindex2 は$Block_share_{dm}$, $color\_top\_h_d$, $color\_top\_s_d$, $color\_top\_v_d$, $color\_bottom\_h_d$, $color\_bottom\_s_d$, $color_bottom_v_d$の 7 つの属性から BFindex1 と同様にして生成された BloomFilter である.

4.3.9 BFindex3

$Block_share_{d(m+1)}$をKey_S_nと連接して k 個のハッシュ関数$Hash_k$適用する. 算出された k 個のハッシュ値の bit 列が 1 の BloomFilter が BFindex3 である. また, $Block_share_{dm}$の添え字 m が n となる時は m を 0 として BFindex3 を生成する.

4.3.10 $table_{dm}$

$table_{dm}$は$Block_share_{dm}$, BFindex1, BFindex2, BFindex3 を要素に持ち, $Block_d$毎に m 個生成されるデータの集合である. m は$Block_share_{dm}$が生成された数と等しくなる. 同一の$Block_d$から生成された m 個の$Block_share_{dm}$のハッシュ値はそれぞれの値が異なるため BFindex1 と BFindex2 の値は毎回異なる. しかし, 人物の特徴のハッシュ値は同一のため, 悪意あるCS_A_mにCS_mに保存されている BFindex1 や BFindex2 を改竄されたとしても, 他方のCS_mと比較することで FalsePositive が増える可能性はあるが, False Negative が増える可能性はなくなる. 本提案手法では$zone_d$のハッシュ値は暗号鍵Key_S_nが更新されるまで同じ値になり, 連続してCS_mに保存した場合CS_A_mにビットパターンから$zone_d$の推測される恐れがある. そのため, 生成された m 個の$table_{dm}$を SS_S にキャッシュし, キャッシュデータの容量が設定された値以上になった時点で, キャッシュされている$table_{dm}$をランダムに異なるCS_mに分散し保存する. それぞれのCS_mに複数の Kinect が撮影した$time_d$の違う映像が同時に保存されるため, CS_A_i は$zone_d$の推測が困難になる.

4.4 近い数値の登録要素の生成

BloomFilter を用いた場合, 近隣の数値を判断することはできないため, $height_d$, $color\_top\_h_d$, $color\_top\_s_d$, $color\_top\_v_d$, $color\_bottom\_h_d$, $color\_bottom\_s_d$, $color_bottom_v_d$はデータベースに格納された値と検索時の値が僅かでも違う場合検索できなくなる. しかし, 先行研究[19]において数値を一定間隔で分割し各領域にバケット番号を振り, 該当するバケットの名前を属性名と合わせ語とすることで数値の大小を判定する手法が提案されている. 本提案手法では大小ではなく近い数値が必要なため, 入力された数値に該当するバケット番号には「バケット番号:eq」として, 入力された数値の該当するバケット番号の±1 には「バケット番号:ne」とする. 「バケット番号:eq」, 「バケット番号+1:ne」, 「バケット番号-1:ne」の 3 つ登録要素が生成される. そのため$height_d$, $color\_top\_h_d$, $color\_top\_s_d$, $color\_top\_v_d$, $color\_bottom\_h_d$, $color\_bottom\_s_d$, $color_bottom_v_d$は生成された 3 つの登録要素をもつ. なお HSV 値の H だけは 0 から 360 の範囲があり, 0 と 360 は同じ色相となるため隣接していることとなる. そのため H の値を 15 の間隔で分割し, 入力された数値に該当するバケット番号が 0 の場合「バケット 24:ne」と「バケット 1:ne」となる. $height_d$のバケット番号を Hei とし di 番まで用意する. di は分割する回数であり, di の最大値を大きくするほど語検出が減少する. $color_top_h_d$のバケット番号を TH, $color_top_s_d$のバケット番号を TS, $color_top_v_d$のバケット番号を TV, $color_bottom_h_d$のバケット番号を BH, $color_bottom_s_d$のバケット番号を BS, $color_bottom_v_d$のバケット番号を BV として, それぞれ di 番まで用意する. 図 5 に近い数値の登録要素の生成例を示す.

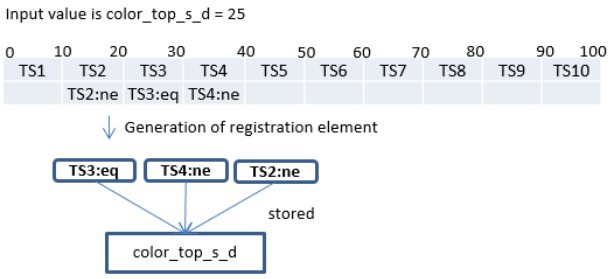

図 5　近い数値の登録要素の生成例

4.5 探索手法

User は携帯端末のアプリケーションを使い探索する人物の入店した時間, 身長, 衣類の上下の HSV 値を入力する. 探索システムが入力された入店した時間から現在の時間までの$time_d$を bt 個生成する. bt は入店時間から現在の時間までの間に$Block_d$を生成した数である. また探索システムがK_a個の$zone_d$を生成する. BFindex1_s はメタデータの bt 個の中の 1 つの$time_d$, K_a 個の中の 1 つの$zone_d$と$height_d$をKey_S_nと連接して k 個のハッシュ関数$Hash_k$に適用しハッシュ値を算出し, 算出された k 個のハッシュ値の bit 列が 1 の BloomFilter が生成され, 生成された BloomFilter の論理和である. 算出されたハッシュ値が重複した場合, 重複した bit 列を 1 にするために論理和が用いられる. BFindex2_s は$color_top_h_d$, $color\_top\_s_d$, $color\_top\_v_d$, $color\_bottom\_h_d$, $color\_bottom\_s_d$, $color_bottom_v_d$をKey_S_nと連接して k 個のハッシュ関数$Hash_k$に適用しハッシュ値を算出し, 算出された k 個のハッシュ値の bit 列が 1 の BloomFilter が生成され, 生成された BloomFilter の論理和である. 探索システムは BFindex1_s と BFindex1 を比較する. BFindex1_s のビット列が 1 となる箇所の全てが BFin

Vol.2015-DPS-162 No.43
Vol.2015-CSEC-68 No.43
2015/3/6

dex1 のビット列が 1 なら BFindex2_s を生成する.探索システムは BFindex2_s と BFindex2 を比較する． BFindex2_s のビット列が 1 となる箇所の全てが BFindex2 のビット列が 1 なら類似する人物がその場所にいるため，マップ情報と K inect の位置と撮影された時間を User の携帯端末に送信する．BFindex1_s のビット列が 1 となる箇所のうち一つでも BFindex1 のビット列が 0 なら，$time_d$と$zone_d$の値を変更した BFindex1_s を生成する．これを bt×K_a回繰り返す．探索システムは全パターンの比較を行い，一致しなかったなら，User の携帯端末に一致しなかった事を送信する．図 6 に探索システムの流れを示す.

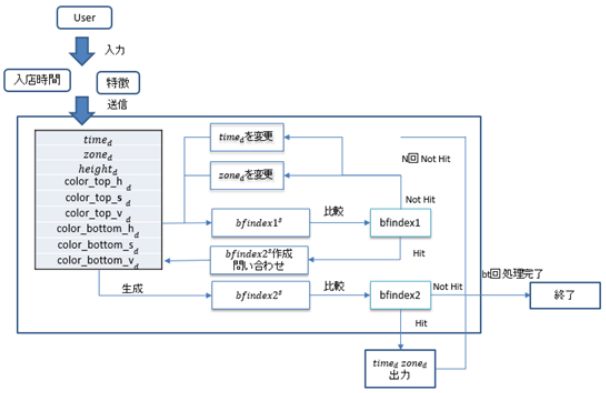

図 6　探索システムの流れ

4.6 分散情報の収集

$Block_d$を閲覧するためには異なるクラウドストレージに保存されている$Block_share_{dm}$から任意の k 個を集めると，元の$Block_d$を復元できる．復元する$Block_d$の share を収集するために 4.3.9 項の BFindex3 を用いる．$Block_share_{dm}$とKey_S_nのハッシュ値で BloomFilter を作成し BFindex3 と比較する．生成した BloomFilter のビット列が 1 となる箇所の全てが BFindex3 のビット列が 1 なら，一致した$table_{dm}$の$Block_share_{dm}$を用いて同じ処理を繰り返す．これを n 回繰り返した$table_{dm}$の$Block_share_{dm}$とKey_S_nのハッシュ値で生成した BloomFilter と始めに作成した BloomFilter が同一の場合，収集された share は同一の d であるため$Block_d$が復元できる．図 7 に分散情報の収集の流れを示す.

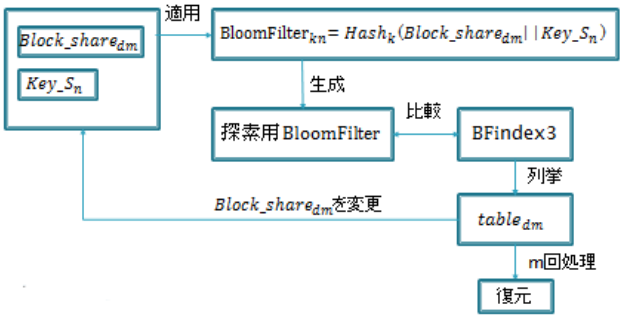

図 7　分散情報の収集

5. 考察

4.6 節に記述した収集方法は，分散された情報の一部が紛失した場合，次の分散情報を探索するための BloomFilter を生成できなくなり，$Block_d$が復元できなくなる．これは，閾値法の特徴である可用性の確保ができていないことになる．これに対して，BFindex3 を生成するのに用いる$Block_share_{d(m+1)}$を$Block_share_{d(m+2)}$に変更した BFindex4 を生成し，BFindex3 を用いて収集中に途切れた場合 BFindex 4 を用いることで紛失した分散情報の探索ができるようになると考える．しかし，クラウドストレージの管理者に与える情報と記録する容量が増加するため，トレードオフの関係である.

本提案手法に用いる Kinect は深度センサとカメラがあり安価である．しかし，技術は日進月歩であり，より高性能かつ安価なデバイスが誕生した場合そちらに変更する必要がある.

6. おわりに

本論文では，監視カメラの代わりに Kinect を用いて顔の特徴を利用しないプライバシーに考慮した屋内での迷子探索を提案した．本手法ではクラウドストレージに記録する映像は秘密分散法により正規の手段以外での閲覧は困難である．また，記録される人物の特徴が BloomFilter を用いて記録されるため，個人の特定も困難となっている．この BloomFilter は探索システムのサーバでキャッシュし，ランダムにクラウドストレージに記録するため，クラウドストレージの管理者による統計攻撃に耐性を得ている．以上より我々の提案した手法はプライバシーを保護しつつ迷子を探索するのに有用と考える.

参考文献

1)　平成 26 年警察白書,
http://www.npa.go.jp/hakusyo/h26/ (2015/1/7)
2)　イオン株式会社，株式会社エヌ・ティ・ティ・ドコモ: 迷子探しサービス,
http://www.npa.go.jp/hakusyo/h23/honbun/index.html (2012/6/30).
3)　レーダー機能付きアラーム PWS-KF1W 迷子探します,
http://www.princeton.co.jp/product/securitypc/pwskf1w.html
(2012/6/30).
4)　KDDI 株式会社: 安心ナビ,
http://www.au.kddi.com/anshin/index.htm (2012/6/30).
5)　株式会社 N・T・T・ドコモ: イマドコサーチ,
http://www.mydocomo.com/web/useful/imadoco/index.html(2012/6/30)
6)　セコム株式会社:ココセコム,
http://www.855756.com/ (2012/7/4)
7)　ソフトバンクグループ:位置ナビ,
http://mb.softbank.jp/mb/service/3G/ichinavi/ (2012/7/4)
8)　西村 康孝，田坂 和之，吉原 貴仁: 音波を使った携帯通信端末間の方向推定方式，電子情報通信学会論文誌 B, Vol.J95-B , No.11, pp.1404-1413, (2012)
9)　岡田 延昭，山下 邦弘，三浦 元喜，羽山 徹彩，國藤 進: 迷子防止のための振動による位置関係情報提示装置の提案-カンジルホウイ-，第六回知識創造支援システムシンポジウム, pp113-118, (2009)
10)　田中 良志，手塚 伸，宮田 宙和，宇田 隆哉: 拡張現実によ

る迷子探索システムの提案, 一般社団法人電子情報通信学会, 暗号と情報セキュリティシンポジウム(SCIS) , 4D1-3, (2011).
11) 日本電気株式会社: 自然な言葉で入力された服や顔の情報をもとに 大量の映像から特定の人物を発見できる,人物検索技術, http://www.nec.co.jp/press/ja/0911/0404.html (2012/7/3).
12) ALSOK: カメラ映像から特定の人物を捜すシステム, http://www.alsok.co.jp/company/news/news_release_details.htm?alpc_news.news_detail[id]=1111 (2012/7/3).
13) 日立国際電気:類似顔画像検索, www.hitachi-kokusai.co.jp/products/camera/isnex/imagesearch.html (2012/7/3).
14) 由雄 宏明, 松川 隆行: 顔・着衣特徴による高速人物検索, panasonic technical journal Vol,54 No,4 Jan,(2009).
15) 松尾 賢治, 橋本 真幸, 小池 淳: 類似顔検索のための異なる人物間の顔類似度算出, 電子情報通信学会論文誌 D , Vol.J92-D, No.8, pp.1383-1392, (2009).
16) 松原 大輔, 廣池 敦, 影広 達彦: 疎分散カメラ環境における類似画像検索を用いた人物追跡, 電子情報通信学会技術研究報告, PRMU, パターン認識・メディア理解, 110(330), pp25-30, (2010)
17) A.Shamir: How to share a secret,Communications of the ACM, Vol.22, No.11, pp.612-613, (1979).
18) L. Fan, P. Cao, J. Almeida, A. Z. Broder, :Summary cache: A scalable wide-areaWeb cache sharing protocol, IEEE/ACM, Transactions on Networking, vol. 8, no. 3, pp 281-293, (2000).
19) 新井 裕子, 渡辺 知恵美：データベースアウトソーシングにおけるプライバ シ保護に考慮した範囲検索法, 電子情報通信学会第 19 回データ工学ワークショップ, C1-1（2008）.