研究計画書
顔認識による個人へのアクセス：顔認識技術のネットワーク化の実現と評価

慶應義塾大学総合政策学部
自署:_____
希望プログラム: サイバーインフォマティクス(CI)
学籍番号:70835080
2012 年 5 月 24 日

概要

近年画像認識や顔認証技術の発展が目覚しく、対象の顔情報を捉えた画像データを元に世界中の人物が繋がるような世界の実現が射程に入った。そこで本研究では、顔認識に基づいたユーザ間のアクセス手法を具現化し、現状の顔認証技術をどこまでユーザ間のアクセスに用いる識別手法として用いられうるか評価し、顔認識を用いたアクセス手法が社会で用いられるようになった際にどの様な問題が発生しうるかの検証を行う。

1　はじめに

近年コンピュータの高性能化と画像認識の進化に伴い様々な応用や実用例が広がっている。その実例としてセキュリティーの分野では、顔認証を用いた電子端末のロック機能[8]や生体情報を利用したパスポートの実現が挙げられる[9]。大規模 SNS である Facebook では、Tag Suggestions と呼ばれるアップロードされが写真に顔認識技術を用いて、写真に写っているユーザのタグを自動的に追加する機構などを導入している[10]。また大規模なデータ処理に用いられている例としては、Agharwa ら[7]による画像共有サイトにアップロードされた大量の観光名所を捉えた画像データを元に、画像認識技術を用いたマッチングにより、都市レベルでの 3D モデルの生成を行なった実験が挙げられる。

これらの画像認識技術の成長により、カメラで撮影した対象との顔認識による接続対象の識別と直感的なアクセスの実現が射程に入った。顔認識による対象へのアクセスの実現には様々なメリットが存在する。既存のコンピュータ間の通信モデルでは、個々のユーザが相手のユーザ名、アドレス、Google[3]のような検索エンジンからの検索結果等の情報を元に、インターネットを介して接続を行なっていた。しかしこのモデルでは屋外などに居合わせたそれまで面識の無かった人物へのアクセスを行う事へのニーズを満たせなかった。また、スマートフォン間でのアクセスを行うサービスとして、GPS とユーザが端末に発生させた振動の情報をもとにマッチングを行い連絡先やファイルを交換する BUMP[4]というサービスが存在するが、この手法では相互のユーザが対象を認識しており、通信を行う意図を持っていなければならないという制約がある。

本研究で提唱するユーザと対象である人物の顔認識を利用したアクセス手法の実現は、これらの既存の手法の問題を解消し、人と人の顔認識を介した新たな繋がりかたのカタチの実現を期待出来る。私生活の観点からは、その場で知り合った人物と通信する為に端末へのアクセス手法の取得を実現出来る。さらに、未成熟で自身の両親のコンタクト等を記憶していない児童には、その児童の顔情報を親の端末へのアクセス手法と紐付けしておけば、迷子になってしまってもその児童を発見した店員や警察官がその児童の顔から本研究で提唱するシステムに問い合わせを行う事により容易に親へアクセスし、児童が現在どこにいるのかを伝えられる。なお商業的観点からすれば、店舗に頻繁に来客するユーザに対して、店内のカメラで捉えた客の顔などの情報を店舗の売上情報と紐付けし、客の顔で本システムへ問い合わせを行いアクセス手法を取得すれば、既存の買い物情報から特別なサービス情報の発信等の様々なユースケースの実現が期待出来る。

そこで本研究では、ユーザが相手の顔情報を元に対象人物の端末へのアクセス手法を取得するシステムを既存の画像認識技術を用いて実装し、現在の技術でこのアクセス手法を実用に耐えうるかどうかの検証を行い、その後にシステムの運用を行い、プライバシーなどの多面的な観点から、ユーザが本システムを利用して発生しうる問題を検証する。

2　コミュニケーションモデル

近年の高性能な携帯端末の普及により確立した

ユーザ間の端末を介したアクセス手法は、既存のパーソナルコンピュータ間のアクセス手法とは異なる要素技術と判断要素によって実現されている。本章ではユーザ間の端末を介したアクセス手法を、どの様な端末を対象としたものかという観点からそれぞれのアクセス手法をモデル化する。

2.1 パーソナルコンピュータを介したアクセス手法

スマートフォン等の高性能携帯端末が登場する以前のユーザ間のインターネットに接続した端末を利用したアクセス手法は、ユーザ名、ネットワークアドレス等の文字列で表せる情報を元に通信対象を識別し、実現されていた。

WEB を用いた通信は、ほぼすべての情報通信端末が物理的に移動せず、その所属するネットワークが固定的に決められていた年代のアクセス手法の最たるものだ。企業、マスメディア、教育、動画メディア、個人利用などの多くの人間が様々な場面で WEB を用いてアクセスを行なっている。WEB を用いたアクセスでは、主にブラウザと呼ばれるアプリケーションを利用し、直接相手の端末のネットワークアドレスを指定しアクセスを行うか、Google 等の検索エンジンを用いて文字列情報を元に相手の端末のネットワークアドレスを調べた上でアクセスを行う。

一般的な端末間の相互的なアクセス手法で、近年個人で所有することが一般的となった携帯端末でも利用されている電子メールシステムは、ユーザ名とホスト名を元に DNS サーバに名前解決の問い合わせを行い、メールサーバであるホストのネットワークアドレスを取得し、そのホストに向けてメッセージを送信する。なおそのメッセージは宛先に含まれているユーザがメッセージ受信の為にメールサーバへ接続を行った際に初めてそのメッセージを送信した側と宛先であるユーザとの通信は成立する。

Skype[1]は、マイクロソフト社が提供している P2P コミュニケーションサービスである。Skype のシステムでは、ユーザのステータス等のデータをスーパーノードと呼ばれる固定ネットワークアドレスを持ち、高い計算能力を持ったユーザの端末に P2P 技術を用いて分散し、ログインの為に行う通信等を本社のサーバとの通信により行う構成となっている。Skype ユーザが新たな通信対象へアクセスする際は、ユーザ名、メールアドレス、氏名のいずれかを元にスーパーノードに問い合わせを行い、相手に承認要求を送信し、承認を経てアクセスを行う。[2]

上部に記した主にパーソナルコンピュータ間で使われるアクセス手法は、相手の端末のネットワークアドレスを直接指定するか、相手がサービスなどに登録している個人情報やユーザ名などの文字列で表される情報を元にアクセスを行う。しかし、これらの手法では、アクセス要求を発行する前に接続相手のネットワークアドレスやユーザ名などの識別子を口頭や他の手法などで取得する必要がある。この手順の必要性は、ユーザに手数を強いる事により、対象へのアクセスにあたってユーザが接続を行う際の直感性と利便性を犠牲にしている。

2.2 スマートフォン間のアクセス手法

個人が所有するスマートフォン同士でのコミュニケーションでは、既存のデスクトップコンピュータ等で利用されているユーザ名やアドレスに基づく接続や検索とは異なり、センサ等の技術によって成立している。本項では主流である BUMP[4]というサービスの技術とその性質について説明する。

BUMP は、極至近距離に存在するスマートフォン間のアクセス手法を提供するサービスである。このサービスでは、通信を望んでいるユーザ達が、それぞれの端末上で BUMP アプリを起動し、お互いの端末を軽く接触させる。接触を加速度センサにより探知した BUMP アプリは、接触の発生時間、GPS により取得された位置情報、接触時の加速度センサのデータを元にサーバに問い合わせを行う。サーバは、それらの端末の時間、位置情報、加速度センサーのデータを元に端末のマッチングを行い、アプリケーション上で接続相手の簡易プロフィールを示し、ユーザに接続を承認するかを問い合わせ、承認を経た後にアクセスを行えるようになる。

2.3 既存のスマートフォン間のアクセス手法の問題

しかし前項に記載したスマートフォン間で利用される接続手法にも問題がある。BUMP は極近距離で通信端末を接触させねばならず、利用場面が限定され、サーバによる端末のマッチング手法の問題で数 Km 離れた異なるユーザと接続してしまうケースもある。[5]なお、端末を介した通信手法として BUMP は、通信を行いたいユーザ双方の端末に GPS システム、加速度センサ、そして衝突に耐えられる強度を必要とする。このシステムの設計上の制限は、ユーザがアクセス出来る相手ユーザの端末を厳しく限定してしまう。ユーザが抱えるその場に存在する人物の端末へアクセスを行いたいという要求を満たすには端末の仕様への制

限は少なくなければならない。

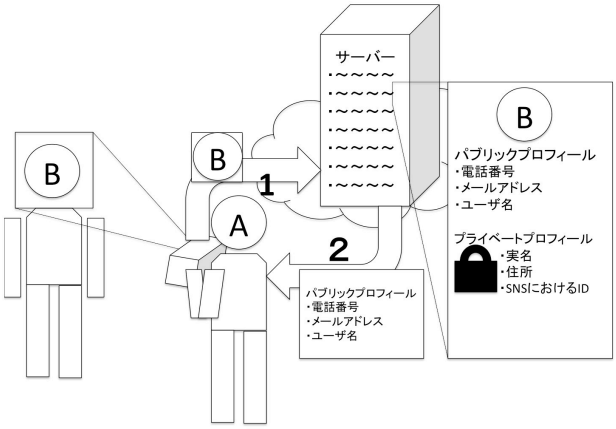
3　問題提起とアプローチ

直感的でユーザフレンドリーなユーザ間の端末を介したアクセス手法を実現するには幾つかの要件が存在する。一つはユーザにアクセスしたい対象などに関する文字列情報の入力を必要としないこと。二つにユーザの利便性を損なうようなジェスチャーを要求したり、端末の仕様に関する制限を強いないこと。そして三つにセンサの不精確さ、攻撃者の操作によりシステムが誤認し、ユーザの個人情報が第三者に漏れることが無いことである。

そのため、本研究では多くの携帯端末にカメラが搭載されており、ラップトップ等にも WEB カメラ等を容易に接続できる点とユーザがアクセスしたい相手を視覚により認識する点に着目した顔認識を利用したアクセス手法を提唱する。

本研究で提唱するシステムはサーバクライアント型サービスであり、ユーザが他のユーザへのアクセスを求める際、その対象の顔写真を撮影するなどして取得し、サーバに問い合わせを行う。サーバから相手に承認要求が送信され、相手ユーザから承認を経てアクセスは実現される。画像解析による顔認識とコンタクトの保存と送信をサーバで担う。そして、ユーザが操作する端末上のクライアントアプリケーションにより、ユーザの求める通信対象の顔写真のサーバへの送信、アクセスを求められているユーザ側で承認操作を行う。

本システムへの問い合わせ時の動作を下の図に



表した。

図に存在するユーザ A がユーザ B に対し電子端末を介してアクセスを行いたいと望んだと仮定する。その際

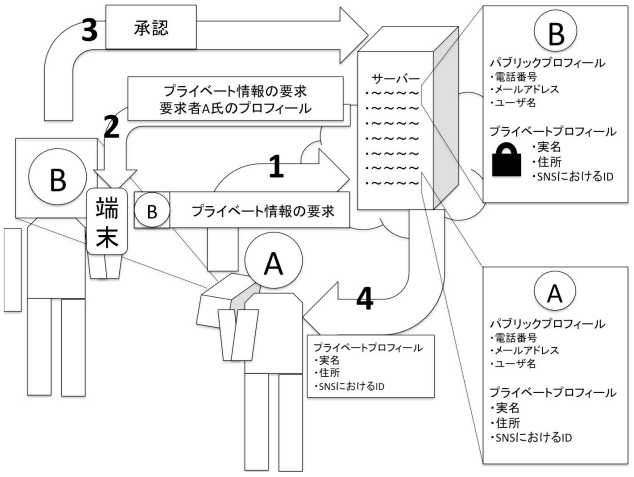
・A は B の顔を撮影し、顔情報を元にサーバへ問い合わせを行う

・サーバは、B のユーザ情報を顔認識により引き出す

・A に対して公開設定されているパブリックプロフィールを送信する

・得られたアクセス手法を元に A は B へアクセスを行う事が出来るようになる

なお顔の情報というものは、一人の人物に対して固有である。しかしながら人物が他者と電子端末を介してコミュニケーションを行う時にはプライバシーのポリシー、どういった通信手段を使うか等の相手とどういったつきあい方をしたいかに左右される要素が多くある。例えばある人物が商業上の理由により顧客や取引先と電子端末を介して連絡を取り続ける必要が発生したとする。そうした場合、彼は当システムを介して、連絡先を相手が自身の連絡先を取得出来るようにしておく必要がある。しかしながら、プライベートでユーザの知り合いと SNS でのユーザ名等のアクセス手法を顔の情報を元にやりとりしており、システムがユーザの多面性に関する配慮に欠けていたら相手に仕事外でのプライベートなアクセス手法や情報が漏れてしまう事になる。そこで本システムでは、ユーザが自身のどの情報を公開し、どのアクセス手法を非公開にするかを設定出来る機構を搭載する。ユーザ A がユーザ B の非公開に設定されているアクセス手法を取得して通信を行う際に発生する手順を下の図に示す。



A が B と公開されているアクセス手法ではなく、ユーザ B が相手を限定して運用しているアクセス手法を通じて通信したいと認識したとする。

・A は B の顔情報と共に限定的に公開しているプライベートプロフィールへの取得要求を発行する

・サーバは顔認識を行い、B に対して A のパブリックプロフィール情報と共に A から B へのアクセス要求を転送する

・B は、A から受けたアクセス要求に対して承認

するか、否認するかを選択する
・承認を選択した場合、サーバからAに対してBのプライベートプロフィールが送信される。
これらの過程を経てユーザAはユーザBと限定的にユーザBが公開しているアクセス手法で通信を行う事が出来るようになる。

また本研究で提唱している顔認識による個人へのアクセス手法の提供は、日常生活を送る上で最低限必要な言語コミュニケーション能力を兼ね備えていない幼児が迷子になった際等に大変大きな貢献が可能である。大規模なショッピングセンターなどの商業施設、人通りの多い公共交通施設などで迷子が発生したとする。その際、その幼児の顔情報が本研究で提唱する顔認識サーバに親へのアクセス手法などと共に登録されていたとする。すると迷子を発見した警察官や商業施設の従業員は迷子の顔写真を撮り、顔認識サーバへ接続し迷子になった幼児の親へのアクセス手法を取得し、彼らに子供が今どの辺りにいるのかを伝えて回収するように伝える事が可能となる。これは、既存の人物間の電子端末を介した電話番号、メールアドレス、ユーザ名などの文字列情報を元にしたアクセス手法では実現できないアクセス手法である。

4　顔認識システムの実現に伴い発生しうる問題点

このシステムは、既存のアクセス手法では解決出来無かった問題を解決しうる可能性を示している。しかしながら本研究で提唱するシステムには幾つかの難解な問題が発生する可能性を伴っている。本章では想定される幾つかの問題とどのような対処法を検討しているかを記載する。

4.1　登録されている人物の顔情報とそのアカウントを運用しているユーザの同一性の担保

本システムでは、顔写真とアクセス手法を紐付けする事を想定している。その様なプライバシーの観点から見てセンシティブな情報を扱う以上、ユーザがそれらの情報を承認する相手ユーザが、アクセスしたいと思った実社会の人間と同一である事をシステムが担保、もしくはユーザが判断しやすくなる機構を用意しなければならない。想定している手法は、アカウント名等が重複、もしくは似たものが登録されていたり、顔認識で複数のユーザがマッチングされたケースを想定して全てのアカウントに対して固有の数値で表現されるID を発行し、実空間でユーザ達がアカウントとユーザの同一性を確認する手法を用意しておくこと。また、簡易なチャット機能をクライアントアプリケーションに用意してコミュニケーションを承認前に行い確認を行う事である。

4.2　攻撃者による偽装アカウント作成

偽装アカウントによる個人情報の抜き出しは Facebook 等の SNS で問題として危惧されている攻撃である。[11]本システムに対して攻撃者が、インターネットから取得した特定の人物の個人情報等と共にアカウントを当システムに対して作成すれば、当システムを利用するユーザが不正にアカウントを作成した人物に誤って承認を行い、個人情報を露見してしまう可能性が存在する。この問題への対策としてシステムは、アカウント作成に辺りユーザに対して多数の視点から撮影した顔情報を要求する。それにより攻撃者が本システムへと他人を装いアカウントを作成するのを困難にする。本システムで採用する予定であるアカウント作成におけるユーザへの多視点からの顔情報の要求はこの偽装アカウント問題に対する解決手法となる事が期待出来る。

5　研究要素と修士での活動予定

本研究が提唱するシステムは、いくつかの構成要素の実装を経て実現する。また研究としてそれらの要素に対して多面的な評価が必要となる。下記に実装と評価に関する項目を記す。

5.1　データベース

本システムではユーザの顔情報、コミュニケーションソフトウェアでの ID やメールアドレスなどのユーザへのアクセス手法、そしてどのユーザ間で通信手法を相互的に交換しあったかを記録するデータベースを実装する。

5.2　顔認識サーバ

本研究では、ユーザからの問い合わせに利用される画像データを対象ユーザが本システムのデータベースに登録している顔情報と比較した際、縮尺、向き、明暗が異なるケースが存在するものと想定する。また、多くのユーザが本システムを利用すれば、それに合わせてユーザからの問い合わせに対してマッチングを行うための計算処理コストも比例して大きくなる。そのため問い合わせをされた顔情報に対するマッチングにあたり、どの様なアルゴリズムを用いるのが最適なのかを検討する。

5.3　アクセス手法としての顔認識の精度と性能の評価

本研究で提唱するシステムの実現には、まずコンタクトやプロフィールなどのプライバシーの観

点からして重要な情報をインターネットを介してやりとりする事をユーザが同意するに値する顔認識の精度をもたなければならない。また、本システムを具現化し、多くの人物に実際に利用してもらい、このシステムが社会にもたらしうるインパクトを検証するには、大規模なユーザの顔情報を収集しつつ、どれほどの実行時間でマッチングを行えるかを検証する必要がある。アクセス手法として普及した BUMP のマッチングに要する実行時間が 9.4 秒から 37.8 秒である事から、[5]それに近い数値を目標として顔認識サーバの応答速度の最適化を精度の保持と並行して行い、現状の技術でどこまでの性能を発揮出来るかを検証する。

5.4　新しい人物間の繋がりを実現するアーキテクチャとして

本研究で提唱するシステムでは、第三章で紹介した迷子問題のような、既存のアクセス手法では解決出来ないような問題を解決出来る可能性を示している。しかしその一方で、ユーザの顔情報がユーザ自らが感知していない所で公開されていて、それを元にユーザ自信が関わりを持ちたくない見知らぬ他者から承認要求を受けたり、悪意を持った攻撃者が偽装してユーザのコンタクト情報、個人情報を取得しようとする可能性等が想定される。本システムの具現化によって観測されうる社会へのインパクト、そして発生しうる新たな問題に対する解決法の模索に取り組む予定である。

6　これまでの活動

私は学部２年次より、村井研究室に所属している。研究室では 、マイクロコンピュータや FPGA 等のプラットフォームなどのクロスコンパイルを必要とするハードウェア環境で開発経験を会得し、ハードウェアでの開発にまつわる問題や仕組みを理解し、解決するためにプログラムや回路の開発を行なってきた。

３年次よりネットワーク機器の内部遅延測定器の開発を FPGA で行なっており、その過程で Ethernet や IP などのレイヤー２やレイヤー３のネットワーク技術への知識を会得し、大局的な観点から既存のコンピュータの OS や IO に関する根本的な処理応答速度等の問題と原因の一端を理解した。

7　志望理由

政策・メディア研究科が所在する湘南藤沢キャンパスは開設時からインターネットを導入してから、構内全域への無線 LAN の導入、学生へのスマートフォン所持の推奨、講義での SNS の利用など様々な先進的な取り組みを行なっている。その為、顔認識を利用した新たなユーザ間のアクセス手法を提唱する本研究の遂行、そしてシステムの導入と実験を行うには大変理想的な環境と言える。

なお、村井研究室のファカルティーや学生は、研究成果や技術を社会へどのように還元できるか、そしてその際にどの様な新たな問題が発生しうるかを想像しながら研究活動を行なっている。そのため既存技術を応用して新たな価値を社会に還元しようと目論んでいる本研究を行うのに大変適した環境だと言える。また、彼らからの指導や研究に関する意見は、本研究の推進に際し非常に有益であると思われる。

以上の理由から私は政策・メディア研究科への進学を強く希望する。

参考文献

[1] Skype www.skype.com

[2] デジタルアドバンテージ＋海津 智宏 ネットワーク管理者のための Skype 入門　第 2 回　Skype の通信メカニズム http://www.atmarkit.co.jp/fwin2k/experiments/skype02/skype02_01.html

[3] Google http://www.google.com

[4] BUMP http://bu.mp/

[5] Studer, A., and Passaro, T., and Bauer, L. Don't Bump, Shake on It: the exploitation of a popular accelerometer-based smart phone exchange and its secure replacement http://dl.acm.org/citation.cfm?id=2076780

[6] Lowe, D. Distinctive Image features from scale-invariant keypoints. Int.J.Comput. Vis. 60,2 (2004), 91-110, http://www.cs.ubc.ca/~lowe/papers/ijcv04.pdf

[7] Agarwal, S. Building Rome in a Day. Communications of ACM. 54,10 (2011), 105-112, http://dl.acm.org/citation.cfm?id=2001293

[8] Anil, R. pam-face-authentication http://code.google.com/p/pam-face-authentication

[9] 外務省. IC 旅券の発行を開始しました http://www.mofa.go.jp/mofaj/toko/passport/ic.html

[10] The Facebook Blog. Making Photo Tagging Easier https://www.facebook.com/blog/blog.php?post=467145887130

[11] Stein, T., Chen, E., Mangla, K. Facebook Immune System. http://research.microsoft.com/en-us/projects/ldg/a10-stein.pdf