技術解説

「顔認証技術と防犯カメラを中心とした事例紹介」

日本電気株式会社　第二官公ソリューション事業部

浜田　康志（左）
坂本　静生（右）

概要:

顔認証の性能は日々進化し、多くの場面で実用的な性能を発揮できるようになってきた。本論文では、米国国立標準技術研究所による顔認証ベンチマークテストの評価結果から、近年の顔認証の精度の向上について述べる。また、そのベンチマークテストで高い評価を得た当社の顔認証技術を用いた様々なソリューションから、防犯カメラに関連する三つの事例を紹介する。

1．はじめに

わたしたちは毎日の暮らしの中で、出会う人々が誰であるか日々認識しながら生活している。このようなひとの認識をコンピュータ上で実現することは、さまざまなマンマシンインタフェースの入り口として非常に重要である。ひとの認識には、旧来からの持ち物（IDカードなど）や記憶（パスワードなど）に基づく方法に加え、身体的あるいは行動的な特徴を直接利用するバイオメトリクスがあり、近年その利用が定着しつつある。

特に2001年9月11日に起きた米国同時多発テロがきっかけとなり、バイオメトリクスは社会的な重要性を大きく高めることとなった。これはカードの所持や、ID・パスワードの利用などによる本人の証明では、漏えい・偽造・なりすましを本質的に防ぐことができないためである。実際、19名の9.11ハイジャック犯は計62通の正規な州政府が発行した運転免許証を所持していた。これにより、米国に留まらず日本や世界各国において、パスポートや出入国管理でのバイオメトリクス応用が加速度的に進むこととなった。日本でも2014年夏に、羽田空港・成田空港において顔認証実証実験が行われるなど検討が進んでいる[1]。

バイオメトリクスでは指紋、虹彩、静脈や顔などさまざまな身体情報が使われる。なかでも顔による認証はひと同士のコミュニケーションに最も近い認証手段であり、セキュリティ以外のさまざまな目的にも顔認証技術を応用することができる。また、顔認証では汎用のカメラで撮影した顔画像で認証が可能である。これは、他の身体情報（モダリティ）のバイオメトリクスでは専用センサの操作をしばしば要求されることとは、大きく異なる点である。ほかにも顔認証は、利用者に特別な認証動作を強いる必要がないという大きなメリットもある。

当社は1989年に顔認証技術の研究開発を始め、1999年に顔認証システムを出荷して以来、多様なソリューションへと展開してきた。認証精度も継続して改善を重ねており、有力ベンダーが数多く参加する米国国立標準技術研究所（NIST: National Institute of Standards and Technology）主催の顔認証のベンチマークテストにおいて、2009年、2010年、2013年と参加したすべてのテストでトップ評価を獲得した。

本技術紹介では、米国国立標準技術研究所による顔認証ベンチマークテストの評価結果から、近年の顔認証の精度の向上について述べる。また、そのベンチマークテストで高い評価を得た当社の顔認証技術を用いた様々なソリューションから、三つの事例を紹介する。

2．顔認証の性能の動向

顔認証の性能は日々進化している。特に近年その精度は大きく向上し、多くの場面で実用的な性能を発揮できるようになってきた。顔認証の精度はベンチマークテストなどを通じて計測されるが、その中で特に代表的な米国の国立機関が実施するベンチマークテストの結果から顔認証の性能の動向について紹介する。

2001年の米国同時多発テロの後、米国は国土を守

るための重要な技術のひとつとしてバイオメトリクスを掲げ、同国立標準技術研究所に対してその技術評価及び調達等に必要な標準化を行うよう命じた。これを受けて、指紋や虹彩の他に顔の認証精度を評価する第三者ベンチマークテストが度々実施されている。現在、米国国立標準技術研究所（NIST: National Institute of Standards and Technology）が中心となってベンチマークテストを主催している。最近ではFRVT2013（Face Recognition Vendor Test 2013）が開催され、ベンダー各社に認証アルゴリズムを提出させ、ベンダーには評価用の画像を一切公開せずに技術レベルを評価する、いわゆるブラインドテストによって客観的かつ正確に評価する目的で実施された。米国国土安全保障省（DHS :Department of Homeland Security）、米連邦捜査局（FBI: Federal Bureau of Investigation）が支援する他、その評価は米国内だけに留まらず世界的にも信頼され高い注目を集めている。

図1は2010年に実施されたベンチマークテストから、年々改善される認証精度を図示したものである[2]。横軸は、誤合致率（FMR:他人同士の顔画像が誤って合致してしまう率）が0.1%水準となる条件での誤非合致率（FNMR:本人の顔画像が誤って合致しない率）、縦軸はベンチマークテスト名称を示す。1990年代初期の評価では誤非合致率は80%近くあった。しかし約10年で約20%まで大幅に性能が改善された。そしてそれから約10年、2010年のベンチマークテストでは性能はさらに改善され、当社の顔認証技術が参加ベンダーの中で最高精度となる0.3%を実現した。このように近年の顔認証技術の劇的な発展により、多くの場面で実用的な性能を発揮できるようになった。

また、最新のFRVT2013の評価結果のひとつとして、図2に16万人からの識別処理結果を示す[3]。横軸は識別処理にかかった時間の中央値、縦軸は識別しようとした本人が一位にならなかった確率であり、左下に近いほど高速かつ高精度であることを示している。参加者は複数のアルゴリズムの提出が認められており、グラフ上で当社はEで始まる文字列が割り当てられている。当社の識別処理時間及び一位識別失敗率は、他の参加者に比較して約半分以下であることがわかる。このように大規模な人数の中から人を高速に識別する能力も、実用的な性能を発揮できるようになった。

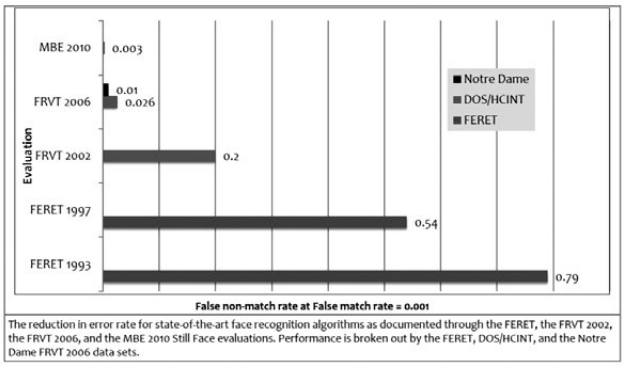

図１　顔認証の精度改善（文献［2］より引用）

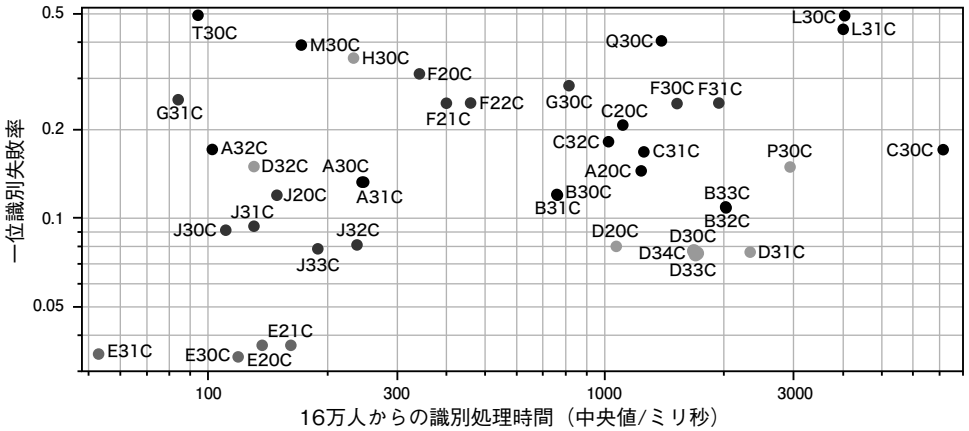

図２　16万人からの識別実験結果（文献［3］より引用）
NECの結果にはEから始まる文字列が割り当てられている。

3. 顔認証ソフトウェア「NeoFace」とその活用事例

当社では顔認証アプリケーションのコアとなる顔検出/顔照合ソフトウェア開発キット「NeoFace」と、この開発キットを利用したアプリケーションを提供している。NeoFaceは、開発に必要なSDKライブラリ、及び開発した顔認証アプリケーションの実行に必要なランタイムライブラリをそれぞれ提供しており、WindowsやLinuxが搭載されたPCやサーバなどの環境に対応している。また、前節で紹介したベンチマークテストで好成績を収めた認証アルゴリズムを取り入れることで、高精度の顔認証を実現している。

当社の顔認証技術は大まかに、画像の中から顔が存在する領域を検出する顔検出技術と、検出した二つの顔を互いに比較して類似度を求める顔照合技術の二種の技術で構成される(図3)。

顔の検出は、画像の端から順に顔らしい領域を探索する処理が基本となる。そのため計算量は比較的大きくなる傾向にあり、処理速度と検出精度を高いレベルでバランスさせることが必要である。この課題を解決するために、当社では独自のパターン認識手法である、最小分類誤りに基づく一般化学習ベクトル量子化法を用いている。この手法は、同じく大量の文書から文字を読み取るOCRなどでも実績を上げている。

顔の照合は、顔検出で得られた二枚の顔画像を比較して類似度を算出する。目や鼻の凹凸や傾きを始めとした様々な特徴量の中から、あらかじめ非常に多数の顔画像を利用して個人を識別するために最適な特徴量を学習しておく。これらの選択された特徴量により、経年変化などの認証精度に悪影響を及ぼすとされてきた要因に頑健な個人識別を実現できる(多元特徴識別法)。

このふたつの機能を組み合わせることでさまざまな顔認証ソリューションを実現することができる。以下に事例の一部を紹介する。

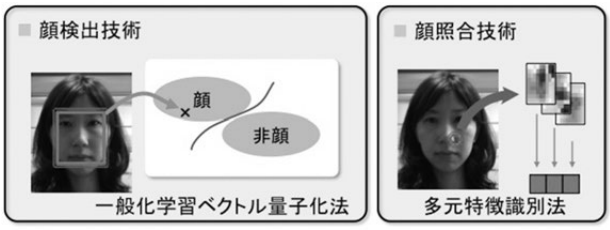

図3　NEC の顔認証技術

◆シカゴ警察 犯罪者検索システム

シカゴ警察ではNeoFaceを用いて、過去の犯罪者の顔画像を検索するシステムを構築している。登録された顔は450万人にのぼる大規模なものである。

2013年、シカゴ近郊の電車内で拳銃を突きつけ携帯電話を強奪し逃走した人物の顔画像を、シカゴ交通局の電車車両内に設置された防犯カメラが捉えた。シカゴ警察で顔画像を照会したところ、犯人と思しき人物が一位で検索された(図4)。その後、目撃者による確認や証拠の収集などの捜査により容疑者が逮捕され、2014年に裁判所で懲役刑が言い渡された。この事件は、米国において初の顔認証技術による逮捕事例として報道された[4]。

このようにベンチマークテストなどだけではなく実際のシステムでも、数百万人規模のデータベースからの検索で高い精度を発揮している。

日本国内では2015年7月に新幹線内で焼身自殺が発生したことを受け、2016年春より新幹線車両内での防犯カメラの機能変更あるいは新たな設置が順次進んでいる[5]。私鉄での防犯カメラ設置が進んでおり[6]、日本でも撮影された映像のさらなる活用が期待される。

図4　シカゴ列車強盗犯の被疑者写真（左）と列車内で撮影された監視映像（右）

◆ボストンマラソン爆弾テロ事件の顔画像評価

2013年4月15日に開催されたボストンマラソンで爆弾テロ事件が発生した。ミシガン州立大学はこの捜査に、顔認証技術が有効だったのではないかと考えて、評価実験を行った。フロリダ ピネラスカントリーから提供を受けた100万人の被疑者画像に犯人の画像を混ぜ込んで識別を実施した。米国国立標準技術研究所で2010年に実施されたベンチマークテスト、MBE 2010 (Multiple Biometric Evaluation)[2]に提供しトップを獲得した当社製品NeoFaceが評価に利用された。

現場で撮影された犯人のうちのひとりの画像（図5左端）で照会したところ、SNSから収集された本人の顔画像を最も類似した画像として得ることができた（図5左から二つめ）。この報告を受け、米国では顔認証技術の応用が真剣に議論されるようになっている。

日本では2020年に東京オリンピック・パラリンピック大会が開催されることが決まっており、テロ発生の脅威が高まっていると考えられる。テロ対策にはさまざまな手法が考えられるが、そのうちのひとつとして顔認証は有効に機能するものと思われる。

図５　ボストンマラソン爆弾テロ事件の顔画像識別実験結果
左端が照会画像、三つの画像は 100 万人の中から類似度が最も高い３枚（文献 [7] から引用）

◆セーブ・ザ・メモリープロジェクト

2011年3月11日に起きた東日本大震災は、日本に大きな爪痕を残した。多くの人が亡くなり、残された人々も財産だけでなく家族や友人を失った。そうした中、株式会社リコーは復興事業として、「セーブ・ザ・メモリープロジェクト」を進めている。

このプロジェクトは、被災地で見つかり地方自治体や多くのボランティアの努力で回収・洗浄された貴重な写真を、持ち主のかたへ届ける活動である。しかし、目視で一枚一枚写真を探すのは大変な労力が必要である。

そこで、写真を探しに訪れたかたの顔を撮影し、NeoFaceによって被災地で見つけられた40万枚にのぼる写真から検索することによって、その方や、家族や友人と一緒の写真をより効率的に発見し、思い出とともに持ち帰ることが可能となった。

このように一般的なスナップショットを対象とした顔認証も使われてきており、今後実フィールドでのますます広がっていくものと思われる。

4．おわりに

本論文では、米国国立標準技術研究所による顔認証ベンチマークテストの評価結果から、近年の顔認証の精度が劇的に向上し、多くの場面で実用的な性能を発揮できるようになりつつあることを紹介した。また、そのベンチマークテストで高い評価を得た当社の顔認証技術を用いた様々なソリューションから、三つの事例を紹介した。

当社は今後も世界トップのバイオメトリック技術を通して、安全・安心で公平な社会の実現に貢献する。

■参考文献

[1] 坂本静生, “羽田空港・成田空港における顔認証自動化ゲート実験,”情報処理学会情報規格調査会, 情報技術標準, No.104, pp.5-8 (2014).
https://www.itscj.ipsj.or.jp/hasshin_joho/hj_newsletter/NL104-w.pdf

[2] P. J. Grother, G. W. Quinn and P. J. Phillips, “Report on the Evaluation of 2D Still-Image Face Recognition Algorithms,” NIST Interagency Report 7709 (2011).

[3] P. Grother and M. Ngan, “Face Recognition Vendor Test (FRVT) – Performance of Face Identification Algorithms –,” NIST Interagency Report 8009 (2014).

[4] “顔認証分析、はじめて列車強盗を逮捕する,” Wired (2014).
http://wired.jp/2014/06/11/first-robber-caught-via-facial-recognition/

[5] “新幹線の防犯カメラ、客室でも常時録画へ 2016年春から順次,” the Huffington Post (2016).
http://www.huffingtonpost.jp/2015/09/09/shinkansen-camera-recording_n_8108782.html

[6] “東急全車両で車両内防犯カメラの設置を推進します,” 東京急行電鉄株式会社 (2016).
http://www.tokyu.co.jp/company/news/list/?id=2401

[7] J. C. Klontz, A. K. Jain, “A Case Study of Automated Face Recognition: The Boston Marathon Bombings Suspects,” Computer, Vol.46, No.11, pp.91-94 (2013).