

NEC の顔認証技術と応用事例

今岡 仁^{†1}

近年、テロリズムや ID 詐欺の世界的な増加に伴い、バイオメトリクス個人認証技術に関する必要性は年々高まっている。顔認証技術は、非撮影者が認証動作を必要としない点や、履歴として残された画像から本人特定が容易な点など、他のバイオメトリクス個人認証技術にはない優位性がある。筆者が所属する NEC では、2010 年に実施された米国国立標準技術研究所(NIST)のバイオメトリクス技術評価プログラム(Multiple Biometric Evaluation)において、実際の犯罪記録から抽出した 160 万人分の顔画像を用いた評価で 92% の 1 位検索率、他人受入率 0.1% 時の本人拒否率 0.3% という他の参加組織に比べて高い精度を達成した。本稿では、NEC の顔認証技術に関して概説し、NIST の評価結果と NEC の顔認証エンジンを使った応用事例を紹介する。

NEC's Face Recognition Technology and Applications

HITOSHI IMAOKA^{†1}

With the recent rise in terrorism and ID theft, the need for biometric personal authentication technology increases year by year. Face recognition technology has advantages not found in other biometric personal authentication technologies, e.g. the ease of identification of a person based on an image kept on file. A matched person now has no need to do anything in order to receive authentication. NEC participated in the Multiple Biometric Evaluation program, a biometrics technology evaluation program of the National Institute of Standards and Technology (NIST), USA, that was held in 2010. NEC achieved the highest recognition performance among the participating organizations, with the highest identification rate of 92% of 1.6 million persons and the lowest false non-match rate of 0.3% at a fixed false-match rate of 0.1%. This paper describes the face recognition technology developed by NEC and introduces the results of evaluation by NIST and actual cases of applications using NEC's face recognition technology.

1. はじめに

社会の電子化やオープンネットワーク化に伴い、本人認証を必要とする機会が益々増えてきている。我々の身の回りだけでも、コンピュータへのログイン、銀行 ATM でのキャッシュカードの利用、クレジットカードの利用、会社やマンションへの入退場など、その例として挙げることができる。通常、これらの場面で個人認証を行う場合には、パスワードや暗証番号などを利用する知識認証と呼ばれる方法、または磁気カードや IC カードを用いる所有物認証と呼ばれる方法が一般的である。しかし、これらの方法は、パスワードを忘れていたり、カードを盗まれたり、偽造されたりする危険性があり、十分な方法であるとはいえない。特に、知識認証は使用場面が増えたときに多くのパスワードを記憶しつづけることが困難である。

バイオメトリクス個人技術はその点、パスワードや暗証番号による認証方式とは異なり、忘れることがないという利点がある。これまで、バイオメトリクス認証には指紋や静脈や顔など、様々な特徴を使って認証する方式が提案されているが、顔認証特有の利点として、

- (1) 入力された顔が履歴として残るため、不正利用や誤認識した場合にその本人の特定が容易である。また、不正行為を事前に抑止する効果も期待できる

- (2) 遠隔から認証が可能である
 - (3) 非接触型の入力デバイスが使える
- ことが挙げられる。

本稿では、NEC の顔認証技術について説明する。次に、米国国立標準技術研究所(NIST)のバイオメトリクス技術評価プログラムにおける評価結果を紹介し、顔認証技術の応用事例を説明する。最後に、顔認証技術における今後の課題を示し、本稿をまとめる。

2. 顔認証技術の概要

顔認証処理の概要を図 1 に示す。まず、顔検出処理を行い、画像中の顔領域を決定する。次に、顔領域に対して、瞳中心、鼻下、口端などの顔の部品位置を求め、顔の大きさを正規化する。最後に、データベースに登録されている顔画像との照合を行い、類似度を算出する。得られた類似度を閾値処理することにより、登録人物と照合人物が同一か否かを判定する。以下に、処理毎に代表的な手法を紹介し、認証精度について説明する。

^{†1} 日本電気株式会社
NEC Corporation

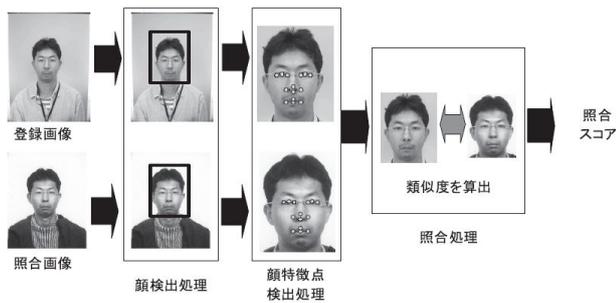


図 1 顔認証処理の概要
 Figure 1 Flow of Face Recognition

2.1 顔検出処理

顔検出を行う手法として、AdaBoost[1]、ニューラルネットワーク[2]、GLVQ[3]等を用いた手法が提案されている。入力画像における様々な顔の大きさや位置の違いに対応するために、テンプレートのサイズを一定にして、画像を一定の比率で縮小し、端から順にサーチする方法がとられている(図 2)。図中の矩形領域はテンプレート、矢印はサーチ順序を表す。テンプレート上の画像領域を抽出し、識別器を用いてその領域内の画像が顔か否かを判定する(図 3)。すべての領域について判定を行うことにより、画像中の顔領域を決定する。

2.2 顔部品位置検出処理

目や鼻の領域が他の領域に比べて暗いという性質を利用して、目や鼻の位置を検出する手法が容易に考えられる。しかしながら、照明変動や眉等の他の暗い領域の影響を受けやすいため、安定に特徴点を抽出することは容易でない。そこで、Elastic Bunch Graph Matching (EBGM)[4]や Active Appearance Model (AAM)[5]が用いられることが多い。EBGM では、顔パターン上に設定された幾つの特徴点(例えば、瞳中心、鼻先、口端など)を端点としたグラフ(図 4)により顔パターンを表現し、画像から抽出された特徴量とグラフの形状を用いて部品位置を決定する。それにより、得られた顔部品位置は顔の変形に対してロバストになっている。一方、AAM では、顔画像を低次元の部分空間で表現しているため、姿勢変動がある場合についても安定して位置を抽出することが可能である。

2.3 顔照合処理

顔照合処理では、正規化された登録画像と照合画像それぞれに対して特徴抽出を行う。正規化後の画像も、姿勢や表情の違いにより位置の違い、照明変動による輝度値の違いがあるため、識別するための個人性を残しつつ、変動成分を吸収するような特徴を利用するのが望ましい。次に施される識別処理では、主成分分析(Eigenface 法)[6]、判別分析(Fisherface 法)[7]等が知られている。顔認証研究の初期のころは、ノイズなどの成分を抑えて照合する Eigenface 法

が使われた。しかし、主成分分析では個人内の変動を考慮していないため、登録時と照合時の画像に違いがある場合には対応が難しい。Fisherface 法は、個人内変動と個人間変動の比を最大になるように学習するため、学習データとテストデータの分布が近い場合には有効である。これに対して、著者らは、照明・姿勢のように顔モデルで記述可能な変動と、経年変化のようなモデルで記述困難な変動に分け、記述可能な変動については画像を生成し、記述困難な変動については判別分析を用いる手法を提案している[8,9]。図 5 に顔形状モデルと照明モデルを用いて元画像から生成された姿勢変動画像と照明変動画像の例を示す。以上で述べたように、画像パタンの変動要因によって、モデルベースの手法と学習ベースの手法を上手く組み合わせることが重要である。

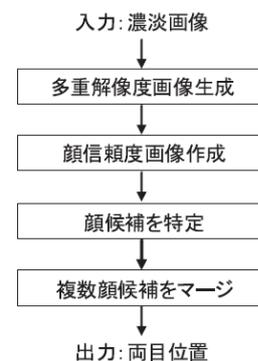


図 2 多重解像度画像を用いた顔検出
 Figure 2 Flow of face detection.



図 3 顔(上段)と顔以外(下段)の画像例
 Figure 3 Examples of face (upper row) and non-face (lower row) images.

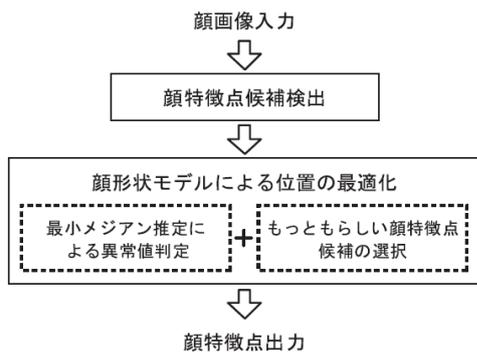


図4 顔部品位置検出処理の流れ
 Figure 4 Flow of face feature point detection.

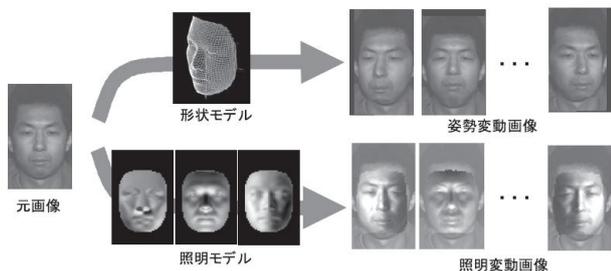


図5 姿勢変動画像と照明変動画像の例
 Figure 5 Example of a matching result.

3. 米国国立標準技術研究所 NIST による認証性能評価結果

NIST では、顔認証技術に関する性能評価を 1993 年から数年おきに継続的に実施している。

NEC は 2010 年に実施された最新の評価プログラム Multiple Biometrics Evaluation[10]に参加し、犯罪記録から抽出した 160 万人の顔画像から 92% の 1 位検索率、ビザ申請時に使われた 180 万人の顔画像から 95% の 1 位検索率という高い検索精度を達成した。また、160 万人からの検索に必要な時間は、画像 1 枚当たり約 0.4 秒であり、高速に動作する。さらに、誤照合率(FAR が 0.1% での FRR)については、犯罪記録の顔画像に対しては 4%、ビザ申請顔画像に対しては 0.3% となった。特にビザ申請顔画像における誤照合率は、他の参加組織に比べてほぼ 1 桁高い性能を得ている。

4. 照合評価例

図 6 に照合結果例を示す。左側が照合画像で、右側が登録画像である。上段の照合画像と登録画像は同一人物の画像であり、下段の照合画像は異なる人物の画像である。照合スコアは中列に棒グラフで表わされ、閾値以上の場合には本人、閾値以下の場合には他人と判定されたことを意味している。上段の結果は、照合スコアが閾値よりも高い

め本人と判定され、下段の結果は照合スコアが閾値よりも低いため他人と判定されたことを示している。本例では上段の照合画像と登録画像では、約 23 年の経年変化があるが、正しく照合されていることが分かる。

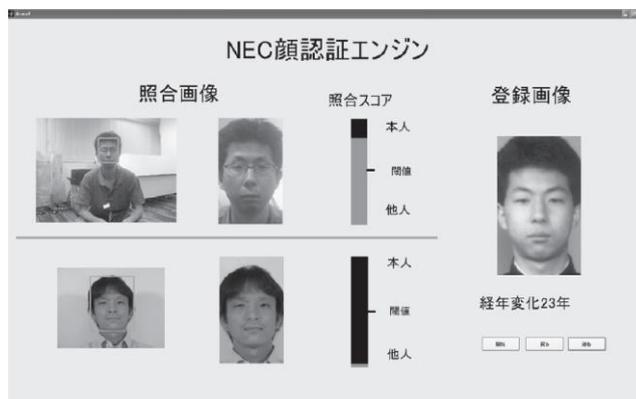


図6 照合評価例
 Figure 6 Example of a matching result.

5. 顔認証技術の応用事例

International Biometric Group の調べでは、2009 年のバイオメトリクス全体の市場は 34 億ドルであり、そのうち顔認証は 11.4% である[11]。5 年後の 2014 年には、バイオメトリクス市場は 94 億ドルに拡大すると予想されている。国内でも IC 旅券の発行が 2006 年 3 月から始まり、その中に顔画像情報が書き込まれた IC チップが入っている。また、外国人入国者に対しては、顔や指紋の個人識別情報の提供が義務づけられており、犯罪者リストとヒットした人物に対しては入国を拒否、身柄を拘束することができる。以下に、NEC での顔検出・顔照合エンジン「NeoFace®」を使った事例を紹介する[12]。

香港入国管理局では、出入国審査の際に自動車に乗車したまま顔認証を行い、自動的に本人識別を行う出入国ゲート管理システムを 2007 年より導入した[13]。香港では、全住民の ID カード化が実現しており、個人識別情報が登録されている。さらに、車ごとにドライバーが一对一で登録されており、車のナンバーからドライバーが特定できるため、出入国ゲート進入時に車のナンバーを識別し、ドライバーが特定できる。ドライバーが顔認証により本人であることが特定されると、出入国業務が完了しゲートが開かれる。本システムでは、非接触という顔認証の利点を生かし乗車したまま認証が行えるため、審査がスムーズに行える。

NEC アメリカと DataWorks Plus は 2012 年、ペンシルベニア州刑事司法コミュニティを支援するための顔認識ソリューションを提供した[14]。ペンシルベニア州司法ネットワーク (JNET) は、約 40,000 人の警察官やペンシルベニア州の刑事司法の専門家に情報を提供しており、800 以上の貢献法執行機関や他州事務所でも利用されている。JNET

顔認識システムは、ペンシルベニア州の刑事司法の専門家が 350 万件の顔画像データから、1 対 1 または 1 対多の検索によって個人を特定したり、発見したりすることができる。これまで、JNET の顔画像検索は、殺人、強盗、強盗、詐欺や ID 窃盗など多数の例を解決する上で役立っている。

6. 今後の課題

本稿では顔認証技術に関する最近の動向を解説した。次に、顔認証技術が更に普及するために克服しなければならない課題を示す。

(1) 顔画像パターン変動による識別性能の問題

顔認証はある程度離れた距離からでも撮影が可能であるため利便性が高い反面、照明や姿勢など撮影環境の変動を受け易い。照明変動については、屋外で撮影された画像など大きな性能劣化要因と考えられてきた。しかし、2009 年に実施された NIST の評価では、屋外を含む照明変動が大きな画像群に対して、誤照合率は NEC が 2%、米 L1 社が 7%であり、克服されつつある課題であると考えている [15]。一方、姿勢変動については、同時に行われた NIST の評価において、大きく性能低下することが報告されている。例えば、横顔を多く含む静止画像照合のテストでは、誤照合率は約 80%である。また、Web 上に掲載された画像を収集した斜め向きの顔など非正面の顔を多く含む画像データベース LFW DB(Labeled Faces in the Wild)[16]では、EER(FAR と FRR が等しい点)が約 7%である。非正面での顔認証は今後の課題であり、今後の改良が期待される領域である。

(2) 非協力型認証に対する応用

顔認証は他のバイオメトリクスと異なり、離れた場所からでも識別しやすい特徴を使っているのが利点である。本稿では主に正面を向いて認証する協力型の認証について説明してきたが、顔認証はビデオ中に写っている人物を自動で検索するような非協力型の認証にも利用することができる。非協力型認証の場合、一般に正面を向いていないため、(1)で述べた姿勢変動による識別性能低下の影響が大きい。また、画面上に写った顔が小さいため、個人識別するための十分な解像度の画像が得られない場合も多い。さらに、動画の場合には、カメラ前を横切る時間が短いため、処理速度の高速性が要求される。すなわち、非協力型の認証に利用するためには、姿勢変動や画質低下に対する頑強性と、リアルタイムに処理ができる高速性の両方を兼ね備えている必要がある。今後は、これらの技術が開発されることを期待する。

7. まとめ

本稿では顔認証技術の概要と応用事例、今後の課題について述べた。今後、姿勢変動がある場合や量けた画像に対する認証性能が改善されることで、顔認証技術は加速度的

に普及していくことが期待される。

参考文献

- 1) P. Viola and M. Jones: "Rapid Object Detection Using a Boosted Cascade of Simple Features," Proc. IEEE Conf. Computer Vision and Pattern Recognition, pp.511-518 (2001)
- 2) H. A. Rowley, S. Baluja, and T. Kanade: "Neural network-based face detection" IEEE Trans. Pattern Anal. & Mach. Intell., 20, pp.23-38 (1998).
- 3) A.Sato, H. Imaoka, T. Suzuki and T. Hosoi: "Advances in Face Detection and Recognition Technologies", NEC J Adv Technol, 2, pp28-34 (2005)
- 4) L. Wiskott, J. Fellous, N. Krüger and C. Malsburg: "Face recognition by elastic bunch graph matching", IEEE Trans. Pattern Anal. & Mach. Intell., 19, pp. 775-779 (1997)
- 5) T. F. Cootes, G. J. Edwards and C. J. Taylor: "Active appearance models", Proc. of 5th European Conference on Computer Vision, 2, Springer, pp. 484-498 (1998)
- 6) M.A.Turk and A.P.Pentland: "Face recognition using eigenfaces", Proc. IEEE Conf. Computer Vision and Pattern Recognition, pp.586-591 (1991)
- 7) P.N. Belhumeur, J.P. Hespanha, and D.J. Kriegman: "Eigenfaces vs. Fisherfaces: Recognition using Class Specific Linear Projection", IEEE Trans. Pattern Anal. & Mach. Intell., 19, pp.711-720(1997)
- 8) 今岡仁,佐藤敦: "判別分析と摂動画像法を用いた顔照合アルゴリズム",FIT2005 pp.31-32(2005)
- 9) 井上晃,坂本静生,佐藤敦: "部分領域マッチングと摂動空間法を用いた顔照合",画像センシングシンポジウム, 2, pp.555-560 (2003)
- 10) http://biometrics.nist.gov/cs_links/face/mbe/MBE_2_D_face_report_NISTIR_7709.pdf
- 11) "Biometrics Market and Industry Report 2009-2014", International Biometric Group 2008
- 12) <http://www.nec.co.jp/soft/neoface/product/neoface.html>
- 13) <http://www.nec.co.jp/press/ja/0707/1901.html>
- 14) <http://www.necam.com/about/read.cfm?ID=1d9578c1-b6e0-415b-ae3d-8fb8bbd2a288>
- 15) P. J. Phillips: "MBGC Still Face Challenge Version 2 Preliminary Results", MBGC Workshop (2009)
- 16) <http://vis-www.cs.umass.edu/lfw>