# Análise da viabilidade de Reconhecimento Facial e Autenticação em aplicações mobile

**Júlio Sérgio Quadros dos Santos, Vanessa Lago Machado, José Antônio Oliveira de Figueiredo**

[1]Instituto Federal de Educação, Ciência e Tecnologia Sul-Rio-Grandense Campus Passo Fundo

Estrada Perimetral Leste, 150 - Passo Fundo - RS - Brasil
CEP: 99064-440

julioquadros@gmail.com,
{vanessa.machado,jose.figueiredo}@passofundo.ifsul.edu.br

***Abstract.*** *This paper verifies technologies based on eigenface method, and describes how technological evolution has been providing more efficient use forms of face recognition and identification systems. The objective of this work is to identify the main tools available, and to verify the feasibility of using this to perform authentication.*

***Resumo.*** *Este artigo identifica as tecnologias baseadas no método eigenface e descreve como a evolução da tecnologia vem proporcionando formas mais eficazes de utilização dos sistemas de reconhecimento e identificação facial. Assim, o objetivo deste trabalho é identificar as principais ferramentas disponibilizadas, bem como verificar a viabilidade do uso dessas para realização de autenticação.*

## 1. Introdução

A identificação facial computadorizada tem se tornado uma ferramenta em importantes setores tecnológicos, por se tratar de um método de identificação biométrica não intrusivo. Dentre suas características, destaca-se a não necessidade de colaboração da pessoa que está sendo analisada, sendo assim utilizada no controle de acesso.

Com a utilização do reconhecimento facial, as pessoas que transitam podem ser identificadas pelo sistema de reconhecimento integrado com as câmeras, sem a necessidade de interação das pessoas com os sistemas. Assim, o presente trabalho tem como objetivo identificar as principais tecnologias utilizadas para reconhecimento facial e analisar a viabilidade da utilização de tal tecnologia para realização de autenticação em aplicações mobile.

O artigo encontra-se organizado como segue: Na Seção 2 é apresentado o estado da arte em relação às técnicas de reconhecimento facial; na Seção 3 é apresentada a metodologia utilizada para realização dos testes; na Seção 4 são apresentados os resultados obtidos; e na Seção 5 são realizadas algumas considerações finais.

## 2. Estado da Arte

O primeiro sistema automatizado de reconhecimento facial foi desenvolvido por Takeo Kanade, em sua tese de doutorado em 1973. Contudo, devido à baixa capacidade de processamento de um grande número de imagens, o trabalho se mostrou inviável. Em 1990 Kirby e Sirovich retomaram o trabalho em um sistema de representação de baixa dimen- são [Datta et al. 2015]. Atualmente, verifica-se que o termo "reconhecimento facial" pode ser utilizado em dois contextos: verificação e identificação. Assim, a verificação trata da comparação de face 1:1 (um para um), enquanto a identificação realiza a comparação de faces 1:N (um para muitos).

Em 2000, Pentland e Chouodhury [Pentland e Choudhury 2000] afirmaram que no futuro os computadores teriam mais interações com os seres humanos do que os próprios seres humanos entre si, e que os principais elementos para a interação de forma inteligente seriam o reconhecimento facial e o reconhecimento de expressões.

Essa tecnologia vem apresentando crescimento, tal fato deve-se às inúmeras implementações de sistemas de reconhecimento e identificação facial na área de segurança pública. Segundo Datta et Al. [Datta et al. 2015], verificação e identificação facial é um métodos não intrusivo para reconhecimento das pessoas, sendo assim, esse método de biometria é utilizado em vários sistemas de segurança, auxiliando na solução de diversos casos policiais, por exemplo.

O algoritmo de reconhecimento facial com melhores indicações de uso é o método *eigenface*. A Agência de Defesa dos Estados Unidos estabeleceu, em 1993, o programa *face recognition technology* (Feret), no qual foram identificados quatro algoritmos apropriados para o projeto, que, depois de analisados, foram escolhidos três algoritmos com maior confiabilidade, todos baseados no método *eigenface* [Pentland and Choudhury 2000]. Dessa forma, esse é o método de reconhecimento facial utilizado amplamente pelos algoritmos relacionados.

Para avaliação dos resultados da identificação ou verificação utiliza-se o *threshold*, o qual trata-se de um índice de similaridade que varia de zero a um, nesse caso, quanto mais próximo de um, maiores as similaridades entre as faces. Contudo, a definição do *threshold* interfere nos falsos positivos e falsos positivos que o sistema poderá gerar, dessa forma o *threshold* ideal é aquele com o menor custo de erro médio por reconhecimento. Para isso utiliza-se a fórmula do F1 Score, a qual se refere à média ponderada ente a precisão e a proporção de eventos positivos corretamente previstos [Ruiter 2015].

De acordo com Taigman [Taigman et al. 2014], as taxas de erro na identificação de face tiveram um declínio nos últimos 20 anos, em três principais magnitudes: detecção, alinhamento e verificação de faces. Contudo, apesar dos avanços, esses sistemas têm demonstrado sensibilidade a vários fatores, como a incidência de luz, expressões faciais, oclusão e o envelhecimento. Além disso, a utilização de alinhamento facial ainda é um desafio, pois depende de normalização dos dados para geração da face em um formato que possa ser comparado com dados a serem identificados.

Por outro lado, verifica-se que diversas empresas vêm desenvolvendo sistemas sofisticados para utilização em controle de fronteiras e sistemas inteligentes de controle biométrico. Ainda, gigantes da tecnologia como Microsoft, Google, IBM e Facebook já

possuem, dentro de uma gama de pesquisas, projetos em nível avançado para reconhecimento facial, os quais já encontram-se à disposição dos usuários.

A Microsoft disponibiliza uma plataforma de infraestrutura em nuvem (Microsoft Azure), a qual possui serviços no formato de contratação de recursos com pagamento pela utilização, permitindo que sejam utilizados recursos de forma elástica e escalável, possibilitando a contratação de recursos conforme as necessidades específicas. Além disso, o sistema permite diversificadas análises das faces reconhecidas nas imagens, possibilitando também a comparação entre duas fotos para verificação se essas referem-se à mesma pessoa, incluindo a capacidade de avaliar os níveis de emoção, e identificar a idade e o gênero da pessoa, a qual a face foi identificada na foto.

A empresa Google disponibiliza uma *Application Programming Interface* (API) - traduzido como Interface de Programação de Aplicativos - chamada de Google Vision, que realiza o serviço de identificação facial. A tecnologia possui uma ampla documentação, com códigos fonte atualizados. Dentre suas características ela possui capacidade de reconhecimento de faces, com relativa facilidade, porém não realiza verificação.

Outro sistema disponível é o BioId, desenvolvido pela empresa que leva o mesmo nome, o qual possui recursos avançados, permitindo que sejam obtidos maiores índices de confiabilidade, o que garante que não sejam utilizadas fotos de outros usuários, isso é possível solicitando que a pessoa efetue movimentos durante o processo de autenticação. Porém, o serviço possui limitações de uso para testes com período definido pela empresa, fazendo com que o desenvolvimento possa depender da disponibilização de recursos financeiros para a efetiva conclusão dos testes.

## 3. Metodologia

O trabalho desenvolvido conta com a utilização da API de reconhecimento facial desenvolvida pela Microsoft, utilizada para fins de comparação de imagens, que permite sua utilização para fins de autenticação. Nesse contexto, verifica-se, em trabalhos relacionados, que o Android 4.0 *Ice Cream Sandwich*, lançado em 2011, possui entre suas novidades o desbloqueio por reconhecimento facial [Gonçalves e Toledo 2013]. Contudo, o intuito do presente trabalho visa a verificação de viabilidade de autenticação para aplicativos desenvolvidos e não para o sistema operacional do smartphone.

Para isso, dentre as opções de tecnologias de reconhecimento facial, destaca-se os serviços da Microsoft, Google e da empresa especializada em autenticação BioID. Assim, a opção pela utilização da Microsoft, como estudo de caso, tem como justificativa a disponibilização do serviço de forma gratuita para desenvolvedores, além da documentação com exemplos, o que facilita a implementação dos testes. A empresa Google oferece o serviço de identificação facial para testes gratuitamente, porém, a API Vision disponibilizada não apresenta a funcionalidade de comparar faces, tornando inviável a utilização da tecnologia como sistema de autenticação.

Dessa forma, o presente trabalho consiste em analisar a viabilidade do uso da tecnologia de reconhecimento facial para autenticação em aplicativos mobiles. Para isso, foi utilizado como teste um dispositivo Asus Zenfone 5 com Android 5.0 com acesso a câmera e o Android Studio 2.3, ferramenta de desenvolvimento para a plataforma

Android, rodando em sistema operacional macOS Sierra 10.12.4, além da API de Reconhecimento Facial da Microsoft (Microsoft Azure).

Para o desenvolvimento da aplicação de referência, foram utilizados exemplos de códigos da Microsoft disponibilizados na plataforma do Github[28], em que a funcionalidade adequada para o sistema de autenticação é a de verificação de similaridades entre a face identificada em duas imagens, sendo uma imagem obtida por meio de um arquivo salvo no dispositivo e a outra obtida pelo uso da câmera do dispositivo. A tecnologia da Microsoft possibilita a obtenção do *threshold*, o qual por referencia a API considera como similares as faces quando o índice é maior ou igual a 0.5 (50%). Contudo, esse grau de similaridade permite que seja definido o índice de confiabilidade na imagem obtida, para que seja utilizada como autenticação.

## 4. Resultados Obtidos

O exemplo de código utilizado demonstra o uso da tecnologia para as funcionalidades de detecção de face, verificação de faces, agrupamento de faces, identificação de faces similares e funcionalidades de identificação de faces.

Para fins de teste foi realizada a identificação de similaridades entre duas faces, em que duas imagens em momentos distintos foram analisadas, sendo fotos tiradas em ambientes com diferentes incidências de iluminação, conforme Figura 1. O resultado apresentado indica o nível de similaridade de 0.75 (75%). Logo, considerando as métricas padrões da API, verifica-se que os resultados obtidos podem ser considerados satisfatórios.


Figura 1. Identificação de similaridades entre duas faces, obtidas por meio da API da Microsoft Azure (Dos autores).

## 5. Considerações Finais

Neste artigo foram apresentadas as principais tecnologias de reconhecimento facial e as possibilidades dessa para verificação e reconhecimento facial. Além disso, foram pesquisados fornecedores de APIs e exemplos de como podem ser utilizados os serviços de forma simplificada, possibilitando posteriores implementações. Assim, a utilização da API disponibilizada pela Microsoft mostrou-se eficiente, e atrelada a definição do

[28] https://github.com/microsoft/cognitive-Face-Android

*threshold* ideal pode ser utilizada como ferramenta para autenticação em aplicações mobile.

Entretanto, apesar das técnicas de reconhecimento facial tratarem de uma tecnologia promissora, a utilização do serviço de reconhecimento facial depende da utilização de APIs disponibilizadas por empresas de tecnologia. Essa dependência de poucos fornecedores pode ser considerada um aspecto negativo, em virtude da possibilidade de mudanças nas políticas de utilização ou termos comerciais, que possam ser adotadas pelos fornecedores.

Por fim, verifica-se a possibilidade, como trabalho futuro, de implementação do serviço de autenticação por reconhecimento facial para aplicações mobile.

## Referências

Datta, A. K., Datta, M., and Banerjee, P. K. (2015). *Face Detection and Recognition: Theory and Practice*. CRC Press.

Gonçalves, L. G. d. S. and Toledo, L. d. C. (2013). Protótipo de aplicativo para propaganda mobile em android.

Pentland, A. and Choudhury, T. (2000). Face recognition for smart environments. *IEEE Computer*, 33(2):50–55.

Ruiter, A. d. (2015). Performance measures in azure ml: Accuracy, precision, recall and f1 score.

Taigman, Y., Yang, M., Ranzato, M., and Wolf, L. (2014). Deepface: Closing the gap to human-level performance in face verification. In *Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition*, pages 1701–1708.