

SmartLook: Bloqueador de aplicativos *open source* dinâmico por meio de reconhecimento de íris

Pamella Baranoski Clos
IFPR

Instituto Federal do Paraná
Quedas do Iguaçu, Brasil
pamellabaranoski@gmail.com

Flávio Endrigo Cechim
IFPR

Instituto Federal do Paraná
Quedas do Iguaçu, Brasil
flavio.cechim@ifpr.edu.br

Alexandre Peres Arias
IFPR

Instituto Federal do Paraná
Quedas do Iguaçu, Brasil
alexandre.arias@ifpr.edu.br

Odair Moreira de Souza
IFPR

Instituto Federal do Paraná
Cascavel, Brasil
odair.desouza@ifpr.edu.br

Abstract — *The security of personal data has been indispensable with the advance of technology and the Internet. This advance has also given rise to methods for data breaches and invasions, particularly for the capture of information that is stored in the cloud. Currently, there are some ways to ensure the security of information, from the simplest, such as encrypted passwords, two-factor authentication, to the most complex, such as facial recognition, digital and iris. In this context, in order to increase digital security, the aim of this work is to protect sensitive data by recognizing the human iris using the computer graphics high-pass filter technique, which highlights prominent areas of the images, through an access blocker application. For the development of the blocking application with iris recognition we use the Sobel and Scharr function algorithms available in the OpenCV package, the Python programming language, for the development of the Dart and Flutter applications. Thus, at the end of the work, there is an application developed for smartphones, allowing the user to select applications installed on the device to apply security and access control through iris recognition.*

keywords: *Information Security, Iris recognition and openCV.*

Resumo — *A segurança dos dados pessoais tornou-se indispensável com o avanço da tecnologia e da Internet. Com esse avanço surgiram também métodos para violação de dados e invasão, principalmente para captura das informações armazenadas na nuvem. Atualmente, existem algumas maneiras para garantir a segurança da informação, desde as mais simples, tais como senhas criptografadas, autenticação em dois fatores, até as mais complexas, como o reconhecimento facial, digital e de íris. Neste contexto, visando o aumento da segurança digital, o principal objetivo deste trabalho é proteger os dados sensíveis, por meio do reconhecimento da íris humana utilizando a técnica de filtros de passagem-alta de computação gráfica, que evidenciam áreas de destaque das imagens, via um aplicativo bloqueador de acesso. Para o desenvolvimento do aplicativo bloqueador com reconhecimento de íris utiliza-se os algoritmos das funções de Sobel e Scharr disponíveis no pacote OpenCV, a linguagem de programação Python, no desenvolvimento do aplicativo dart e flutter. Ao final do trabalho, obtém-se uma aplicação desenvolvida para smartphones, permitindo a seleção de aplicativos instalados no aparelho para aplicar a segurança e acesso via reconhecimento de uma íris.*

Palavras-chave: *Segurança da Informação; Reconhecimento de íris e openCV.*

I. INTRODUÇÃO

Desde o surgimento da Internet a sociedade busca maneiras de proteger os dados que circulam pelas redes [1]. Com o aumento da geração de informação em formato digital, tem sido questionada a importância de se ter garantido a sua disponibilização e preservação por longos períodos de tempo [2].

No Brasil em meados de 2018 entrou em vigor a Lei Geral de Proteção de Dados (LGPD), lei nº 13.709/2018, que visa a segurança de dados digitais. Foi promulgada para proteger os direitos fundamentais de liberdade e privacidade e a livre formação da personalidade de cada indivíduo. Esta lei visa o tratamento de dados pessoais dispostos em meio físico ou digital, feito por pessoa física ou jurídica, de direito público ou privado, englobando um amplo conjunto de operações que podem ocorrer em meios manuais ou digitais [3].

Em conjunto com a LGPD foram instituídos alguns meios para garantir a proteção de dados, tais como, a criação de senhas fortes, uso de antivírus e a inserção de webcam e microfones para reconhecimentos. Alguns métodos envolvem tecnologia avançada e um grau de complexidade recorrente que é necessário para atender a expectativa do usuário, como a biometria digital e o reconhecimento de íris.

Em 1936 Frank Burch levantou a teoria de que a textura da íris humana possuía características suficientes para que fosse instituída como um meio de reconhecimento de um indivíduo. John Daugman, foi o pesquisador do laboratório de computação da Universidade de Cambridge (UK) responsável por desenvolver o primeiro algoritmo para executar o reconhecimento de pessoa, isso por meio das junções das características da íris humana [4].

Devido ao fato de ser um reconhecimento que utiliza uma parte do corpo humano, atribui-se ao método uma certa confiança, visto que nem mesmo gêmeos idênticos possuem linhagens de padrões iguais na íris. Segundo Hakon Jonsson, gêmeos monozigóticos possuem uma diferença genômica que percorre em média 5,2 mutações de desenvolvimento precoce, deste modo dois irmãos gêmeos podem utilizar a segurança via reconhecimento da íris [5].

A escolha da íris humana como recorrência biométrica é em consequência da ausência do contato físico, visando

higiene e a impossibilidade da mutação da íris [6], visto que é protegida pela córnea, ou seja, por toda a vida o indivíduo terá o mesmo padrão de íris, considerando condições de saúde normais.

Nesse contexto, o principal objetivo deste trabalho é executar o reconhecimento da íris humana por meio da técnica de filtros de passagem-alta de computação gráfica, que evidenciam áreas de destaque das imagens para um aplicativo bloqueador de acesso à informação. Para ampliar a utilização deste aplicativo, ele está sendo disponibilizado em licença livre, desenvolvido com ferramentas e algoritmos de código aberto, tornando-o de fácil acesso. Até o momento ele visa a utilização exclusivamente em *smartphones* com câmera para realizar a captura da íris.

II. RECONHECIMENTO BIOMÉTRICO E O RECONHECIMENTO DA ÍRIS

O reconhecimento biométrico consiste na atribuição de Identificadores (ID) para dobras presentes nos dedos dos pés e das mãos. Essas dobras podem ser observadas entre as camadas da pele humana. Na camada intermediária, denominada derme, encontram-se as elevações e as papilas dérmicas que são responsáveis pela digital.

Ao examinar a camada das papilas dérmicas, nota-se variações de cristas que garantem a unicidade de cada pessoa. Essas cristas podem possuir irregularidades, as minúcias, ou chamados pontos característicos. Sendo assim, esses pontos podem ser utilizados no reconhecimento das características de cada indivíduo [4].

Para realizar o reconhecimento, as imagens são capturadas a partir de softwares específicos para segmentar os detalhes e aumentar a precisão do algoritmo. também, é possível utilizar-se de filtros para aumentar a renderização da imagem. Na sequência a imagem é tratada com um processo de binarização, transformando as cores das imagens em preto e branco, fazendo assim uma grande matriz de 0 e 1 [6].

A biometria digital possui uma semelhança notável com a técnica de reconhecimento de íris, principalmente no modo pelo qual os dois reconhecimentos tratam os pontos-chaves de cada indivíduo, extraíndo as informações de partes físicas do ser humano e transformando-as em códigos para utilização no processamento de reconhecimento [4].

A íris é estruturada por um tecido que é composto por trabéculas (rede de filamentos cruzados) e está situada entre a área da córnea e o cristalino [7]. Conforme apresentado na Fig. 1, a superfície é considerada plana e possui no estroma (tecido localizado na circunferência interna) músculos que são responsáveis por dilatar e contrair a pupila. A principal função da íris é controlar a quantidade de luz que entra no olho e é semelhante ao processo que ocorre em uma câmera fotográfica.

A íris tem uma estrutura única variando de pessoa para pessoa, inclusive entre o olho esquerdo e o olho direito. Assim como a impressão digital ela possui padrões únicos. A íris pode ser empregada como um método de

reconhecimento humano devido aos fatores que garantem sua estrutura única e a proteção fornecida pela córnea, tendo em questão o fato de servir como uma película de proteção contra agentes externos [10].

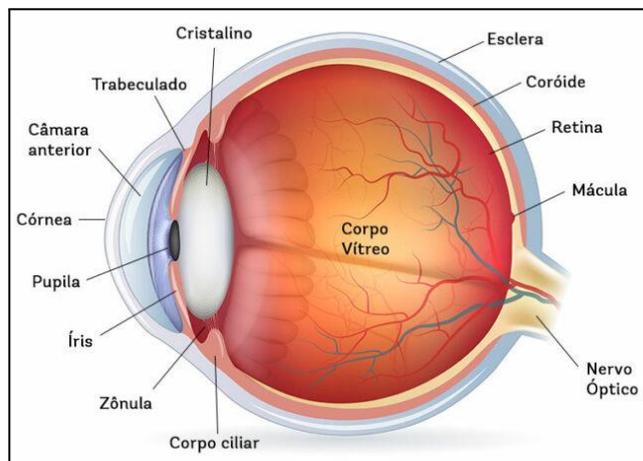


Fig. 1. Representação das estruturas que formam o olho. Fonte: www.hosergipe.com.br/blog/conheca-a-estrutura-dos-nossos-olhos/

A forma única da íris é explicada pela quantidade de pontos localizados na superfície, tais como seus anéis, estrias, manchas e coroas. De maneira geral, os algoritmos extraem esses pontos e transforma-os em códigos, que são usados posteriormente para o reconhecimento da íris [6].

III. MATERIAIS E MÉTODOS

Para executar o reconhecimento da íris, este trabalho visa a utilização de estágios segmentados no qual cada um tem uma determinada responsabilidade. Segundo Reillo [3], os sistemas de identificação biométricos são compostos por três etapas: (i) Captura de imagem; (ii) Processamento dos dados da imagem; e, (iii) Extração de características próprias do usuário.

A. Captura de imagens

A captura da imagem é a parte crucial e minuciosa de todo o conjunto de processamento. Se resume na entrada da imagem que é tratada com filtros, para que o resultado seja retornado corretamente, e comparada com uma imagem já existente no aplicativo. Nessa etapa é necessário atenção e precisão, visto que para maior eficiência do sistema de identificação da íris, uma baixa luminosidade acaba interferindo diretamente no resultado [4].

As imagens capturadas não precisam ser totalmente nítidas, de modo que este trabalho é para o uso em dispositivos móveis. Em ambos os momentos, no cadastro da íris e para desbloquear um aplicativo escolhido, as imagens serão submetidas ao processamento e os resultados retornados serão comparados.

B. Processamento dos dados da imagem

As imagens são submetidas a um processamento utilizando algoritmos que implementam a técnica de evidenciamento de gradientes de imagem, essa técnica

consiste em aplicar filtros para dar destaque às regiões de alto contraste da imagem. Os algoritmos das funções de *Sobel* e *Scharr* estão disponíveis na linguagem de programação Python no pacote *OpenCV* [8].

O *OpenCV* é uma biblioteca nativa que pode ser encontrada em Python e permite realizar operações de processamento de imagens, como aplicação de filtros e mudança de orientação utilizando cálculos matemáticos e funções para retorno de informações.

A região da imagem que possui uma cor mais clara é a área de transição de uma cor para outra, semelhante a um filtro negativo. Esse tipo de filtro é utilizado em algoritmos de reconhecimento de objetos. Os operadores convolucionais permitem evidenciar os gradientes, utilizam argumentos específicos para os cálculos. Os gradientes são utilizados para encontrar a detecção de bordas e para revelar informações estruturais dos objetos pertencentes à imagem [9].

A primeira etapa consiste em calcular o gradiente da imagem submetida, na qual cada pixel da imagem em escala de cinza utiliza o gradiente para evidenciar a mudança de intensidade dos pixels para determinada direção e orientação.

Para encontrar os componentes estruturais da imagem é necessário encontrar e marcar as seguintes orientações: norte, sul, leste e oeste, que estão subjacentes ao centro da imagem. Esses quatro valores que retornam são utilizados para o cálculo da mudança vertical de x e y da imagem, eles são calculados conforme as Equações (1) e (2) [10]:

$$G_y = I(x, y + 1) - I(x, y - 1) \quad (1)$$

$$G_x = I(x + 1, y) - I(x - 1, y) \quad (2)$$

Em seguida, calcula-se a aproximação do *Sobel* e *Scharr* para o gradiente obtido. O método *Sobel/Scharr* utiliza os seguintes parâmetros, conforme o Cód. 1.

```
int    ddepth (profundidade)
int    dx,
int    dy,
int    ksize = 3 (tamanho)
double scale = 1 (escala)
double delta = 0 (delta)
int    borderType = BORDER_DEFAULT
```

Cód. 1 Estrutura e parâmetros da função Sobel.

Ao fim do processamento da aplicação dos filtros, o algoritmo retorna uma matriz com os valores evidenciados. A próxima etapa é fazer a comparação da imagem cadastrada e processada anteriormente.

C. Extração de características do usuário

Ao utilizar da recorrência do processamento que retorna uma matriz com características da imagem, a matriz é armazenada em um banco de dados para realizar o bloqueio dinâmico.

Desta maneira o usuário deve escolher quais aplicativos deseja iniciar utilizando o reconhecimento da íris. O

bloqueio se torna dinâmico, visto que toda vez que é aplicado pode solicitar ou não a foto da íris. Isso se deve à tela de configurações, onde o usuário pode optar por salvar/atualizar a íris e realizar as suas preferências.

D. Bloqueio dinâmico de aplicativos

Na Fig 2, apresenta-se o fluxo de processamento do aplicativo como um todo, tendo início no cadastro de uma íris dentro do App *SmartLook*. Após o cadastro, o usuário opta por quais dos aplicativos existentes em seu smartphone deseja proteger com o método de reconhecimento. Quando o determinado aplicativo for aberto, solicita-se uma foto para realizar a comparação, onde o algoritmo recebe e aplica os filtros, retornando um vetor com as características da imagem. Após o processamento, o aplicativo realiza a comparação entre as imagens e permite o acesso caso os dados sejam iguais.

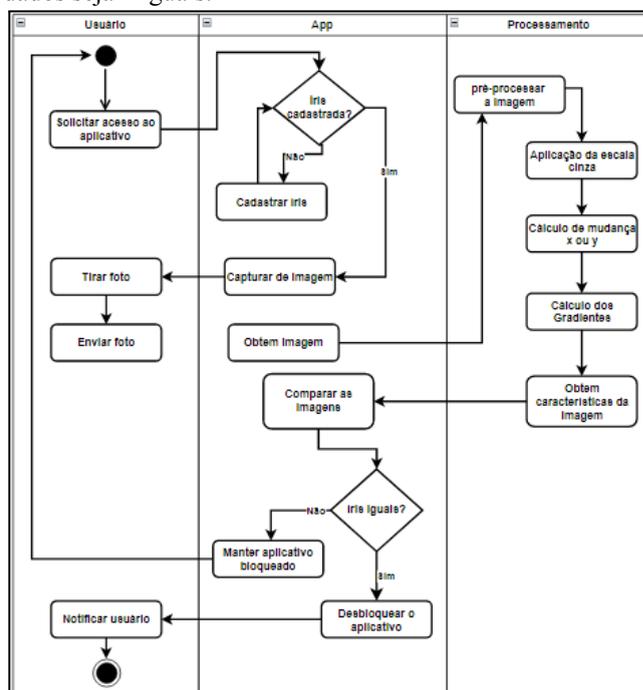


Fig. 2. Fluxo do processamento do aplicativo SmartLook.

O desenvolvimento do aplicativo está sendo em Dart [11] e Flutter [12], sua utilização até o momento para aparelhos smartphones que possuem uma câmera, para realizar a captura da imagem.

IV. RESULTADOS PARCIAIS E DISCUSSÕES

Observa-se na Fig. 3(a) a tela inicial do aplicativo, na Fig. 3(b) são exibidos os aplicativos instalados no dispositivo e que foram adicionados ao bloqueador. Na Fig. 3(c) apresenta-se a tela de configuração do bloqueador, onde é possível alterar a íris cadastrada, e então a câmera será aberta para obter a foto e opções de salvar os dados, realizar a alteração do idioma, verificar e gerenciar as preferências de privacidade, além da opção de visualização da íris cadastrada no aplicativo e a de reconhecimento após a inicialização do dispositivo.

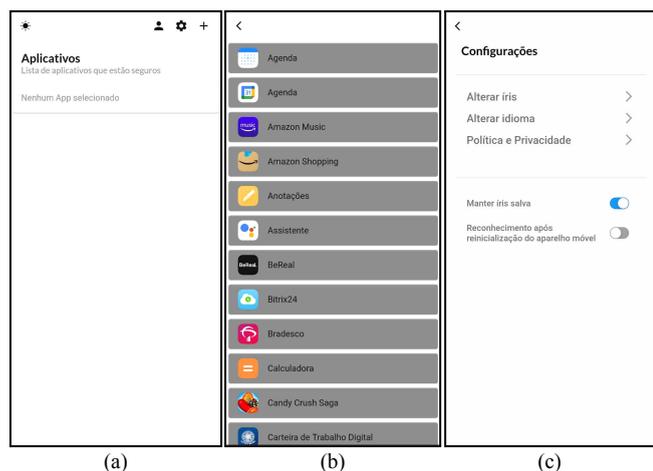


Fig. 3. Telas do bloqueador via reconhecimento de íris.

Na Fig. 4, apresenta-se uma das saídas dos dados do algoritmo de processamento na qual a foto é submetida à adição dos filtros três vezes e os valores das imagens são retornados para realizar a comparação.

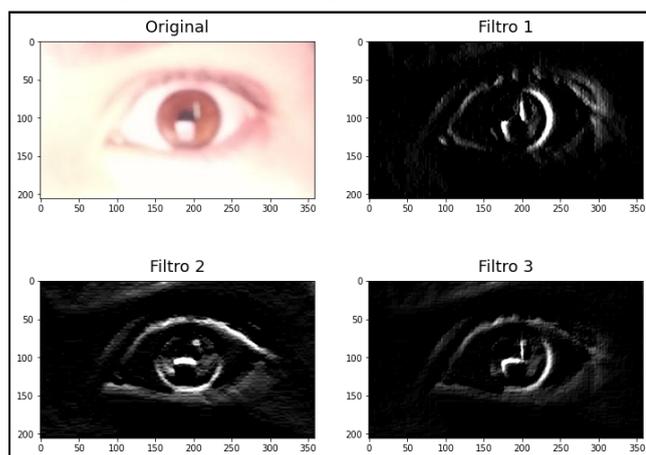


Fig. 4. Representação das estruturas que formam o olho em escala.

Na aplicação dos filtros os valores retornados são enviados ao aplicativo para realizar o fluxo de processos, fazendo a comparação entre a imagem cadastrada e a imagem que foi capturada e processada, validando o acesso ao aplicativo protegido.

Com o aumento da preocupação por proteção online, muitos usuários buscam por métodos que supram suas necessidades, onde muitas vezes, optam por algo que não seja pago e que não seja uma fraude.

Tendo ciência dessas demandas, ao fim da execução deste trabalho, o resultado será de um aplicativo sem custos, de fácil usabilidade e que realize o evidenciamento de características de imagens de íris, e consequentemente, sua comparação.

V. CONSIDERAÇÕES FINAIS

Considera-se que ao final do desenvolvimento do projeto o aplicativo será capaz de realizar a aplicação de filtros de

gradiente sobre a imagem e fazer a comparação para permitir ou não o bloqueio dinâmico de aplicativos.

Ressalta-se que este projeto, visa a política do software livre *open source*, estando disponibilizado no GitHub Link: <https://github.com/PamellaClos/SmartLook->, a modo que espera-se novas contribuições da comunidade tecnológica, para sua evolução.

REFERÊNCIAS

- [1] M. A. ARELLANO, "Preservação de documentos digitais". *Ciência da Informação*, v. 33, n. 2, pp. 15-27, 2004.
- [2] J. M. F ALMEIDA, "Breve história da Internet". 2005. Disponível em: <http://repositorium.sdum.uminho.pt/bitstream/1822/3396/1/INTERNET.pdf>. Acesso em: 22 out. 2022.
- [3] "Lei Geral de Proteção de Dados Pessoais" (LGPD). Disponível em: <https://www.gov.br/cidadania/pt-br/aceso-a-informacao/oi/oi>. Acesso em: 22 out. 2022.
- [4] R. M. COSTA, "Uma nova abordagem para reconhecimento biométrico baseado em características dinâmicas da íris humana." 2009. Tese (Doutorado em Processamento de Sinais de Instrumentação) - Escola de Engenharia de São Carlos, University of São Paulo, São Carlos, 2010. Acesso em: 22 out. 2022.
- [5] H. et al JONSSON, "Differences between germline genomes of monozygotic twins." *Nature genetics*, v. 53, n. 1, pp. 27-34, 2021.
- [6] R. C MAZI, DAL PINO JÚNIOR, A. "Identificação Biométrica através da impressão digital usando Redes Neurais Artificiais". *Anais do XIV ENCITA*, pp. 19-22, 2008.
- [7] C. Q. et al PICA, "Aperfeiçoamento e avaliação de sistema para quantificação da glicemia através de análises de imagens da íris humana." 2002.
- [8] C. R CASTELANO, "Estudo comparativo da transformada wavelet no reconhecimento de padrões da íris humana." 2006. Dissertação (Mestrado em Engenharia Elétrica) - Escola de Engenharia de São Carlos, University of São Paulo, São Carlos, 2006. doi:10.11606/D.18.2006.tde-30112006-134736. Acesso em: 22 out. 2022.
- [9] "OpenCV: Image Filtering." Disponível em: <https://docs.opencv.org/4.x/>. Acesso em: 22 out. 2022.
- [10] "OpenCV:." Disponível em: <https://opencv.org/about/>. Acesso em: 17 out. 2022.
- [11] C. Buckett, *Dart in action*. Shelter Island, NY: Manning, 2013.
- [12] Flutter - Build apps for any screen. Disponível em: <https://flutter.dev/>. Acesso em: 24 out. 2022.