Análise Forense de Documentos Digitais

Prof. Dr. Anderson Rocha

anderson.rocha@ic.unicamp.br

http://www.ic.unicamp.br/~rocha

Reasoning for Complex Data (RECOD) Lab.
Institute of Computing, Unicamp

Av. Albert Einstein, 1251 – Cidade Universitária
CEP 13083-970 • Campinas/SP – Brasil

Spoofing em Biometria

Técnicas para Criação e Detecção

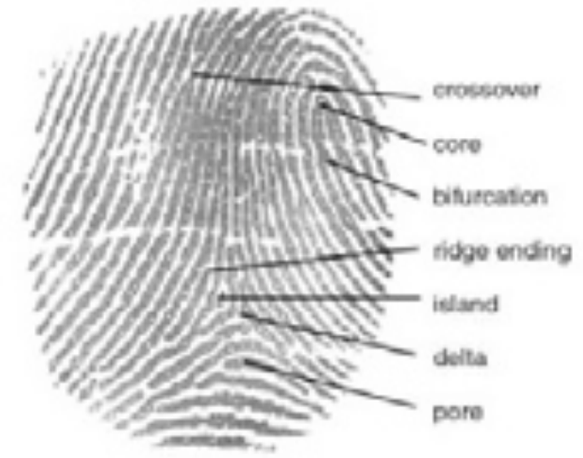
Organização

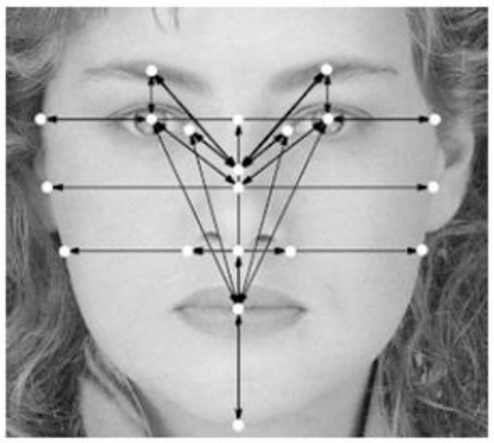
- Introdução
- Motivação
- Visão geral
  - Impressões digitais
  - Íris
  - Face
- Aprofundamento em solução anti-spoof para impressões digitais
- Aprofundamento em solução anti-spoof para face

Introdução

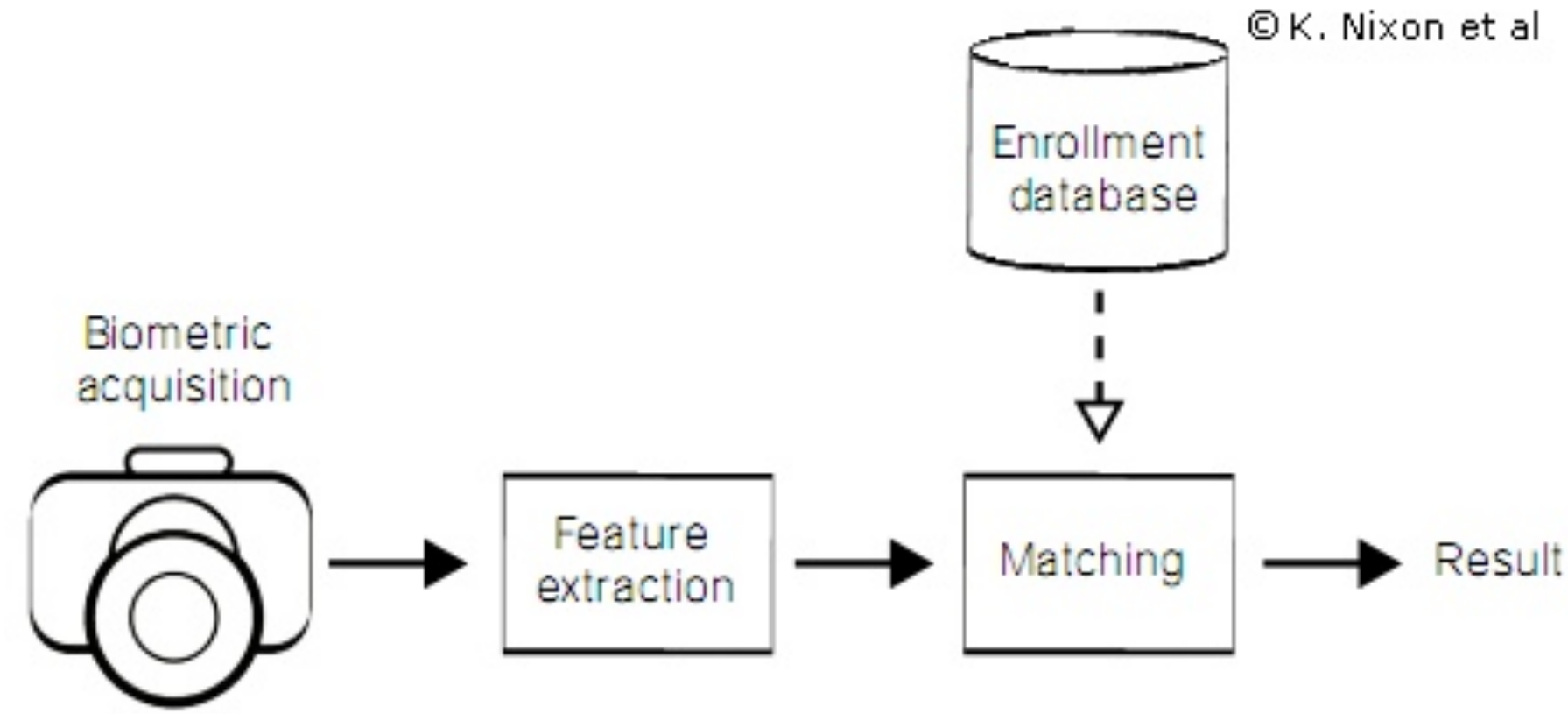
Introdução

- Biometria: é um método para identificação automática de uma pessoa, baseado em características físicas ou comportamentais
  - Impressões digitais
  - Íris
  - Face





Sistema biométrico



An example of how biometric data travels to obtain a result.

Motivação

Motivação

- Aumento no uso da Biometria
  [Thalheim et al. 2002] Impressão digital mais comum, reconhecimento facial mais aceitável; Reconhecimento de voz, de assinatura e jeito de digitar ainda pouco expressivo

- Muita pesquisa para otimizar a diferenciação entre humanos

- Pouca pesquisa (e recente) sobre a confiabilidade dos métodos, sobre como impedir ataques

Visão Geral

[Nixon et al. 2007]

Complementado com [Thalheim et al. 2002]

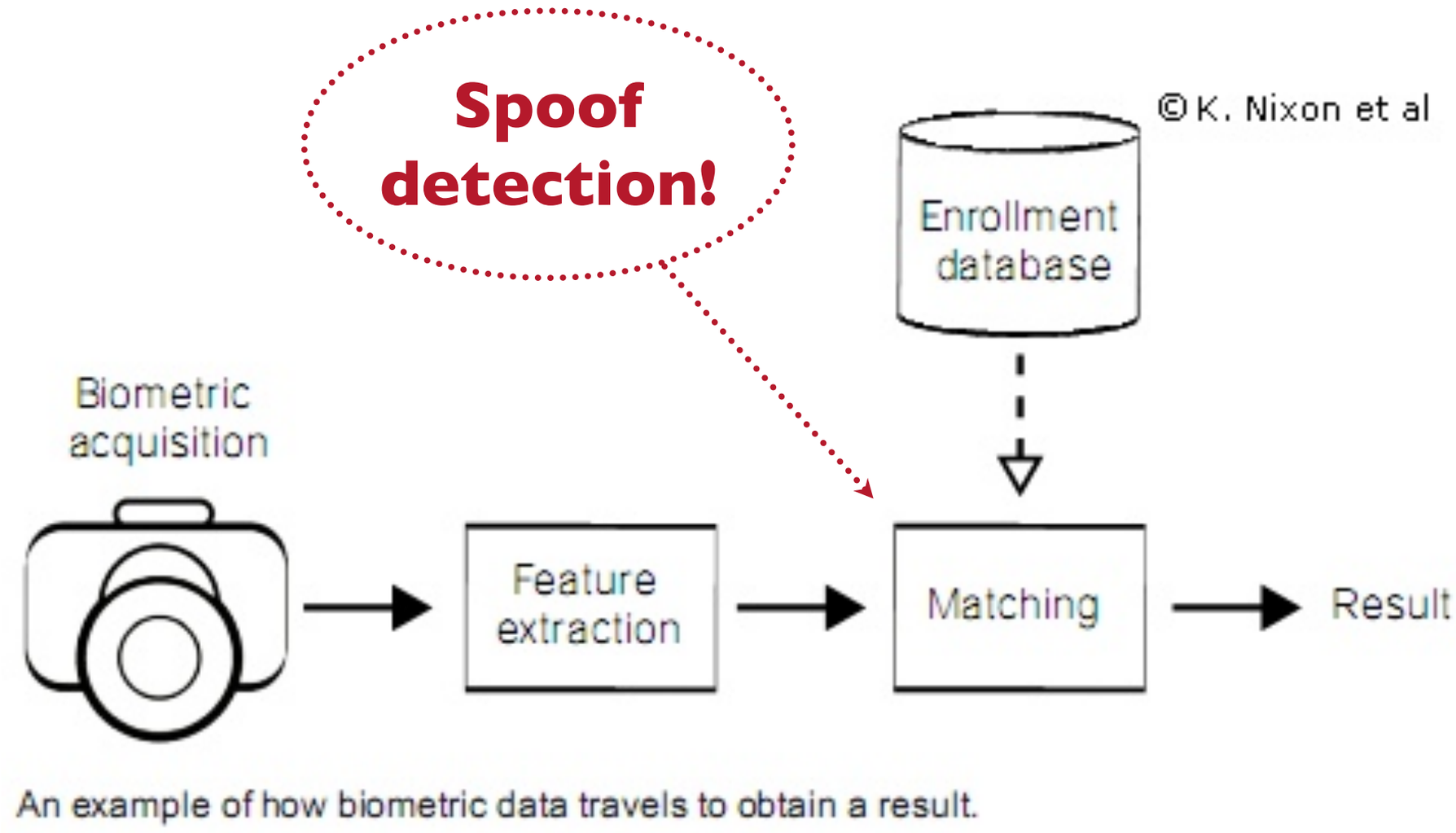
Ataques

- Podem visar esconder a própria identidade ou obter privilégios que outra pessoa possui
- Tipos:
  - Replay (sniffer na USB), Trojan (alterar o matcher ou o BD)
  - Spoof
    - Consiste em apresentar ao sensor um dado biométrico falso
    - Mais suscetível, pois todos tem acesso fácil a esta parte do processo
    - Pode ser um dedo de gelatina com uma impressão digital moldada, uma foto do rosto de alguém, uma lente de contato
    - O 1° ataque a um sistema de impressão digital data da década de 1920, por Alert Wehde, na penitenciária do Kansas

Detecção de Spoof

- Detectar se o dado biométrico realmente vem de uma pessoa viva. Pode:
  - utilizar os mesmos dados biométricos obtidos para identificação;
  - coletar mais dados no tempo;
  - ou precisar de hardware adicional

Sistema biométrico



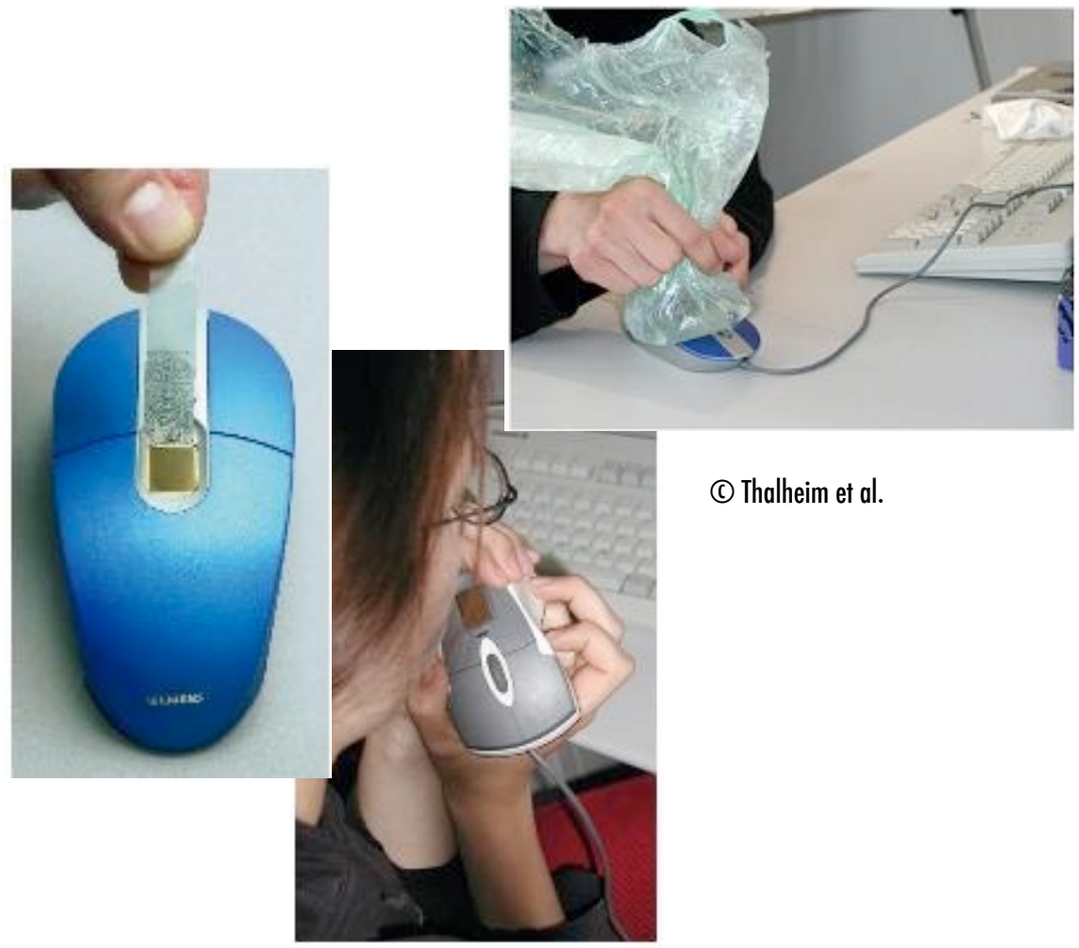
An example of how biometric data travels to obtain a result.

Impressões digitais

“How To Fool a Fingerprint Security System As Easy As ABC”

Criação do Spoof

- Como funciona
  - Se baseia na posição de detalhes (*minutiae*), como terminações e bifurcações dos sulcos
    10 a 12 são suficientes para identificar unicamente uma pessoa
- Spoofs
  - Impressões latentes
    - Pó de grafite e fita adesiva
      quase 100% de eficácia
    - Respiração
      nem sempre funciona
    - Bolsa com água
      chega a funcionar com segurança máxima



© Thalheim et al.

Criação do Spoof

- Mais Spoofs

- Dedo artificial
  - Obter a impressão digital de alguém
    cooperativamente ou fotografando uma impressão latente contrastada
  - Moldá-la em material macio
    silicone, plástico, gelatina, argila, cera ou material para molde dental
- Dedo desmembrado

Sensores para impressões digitais

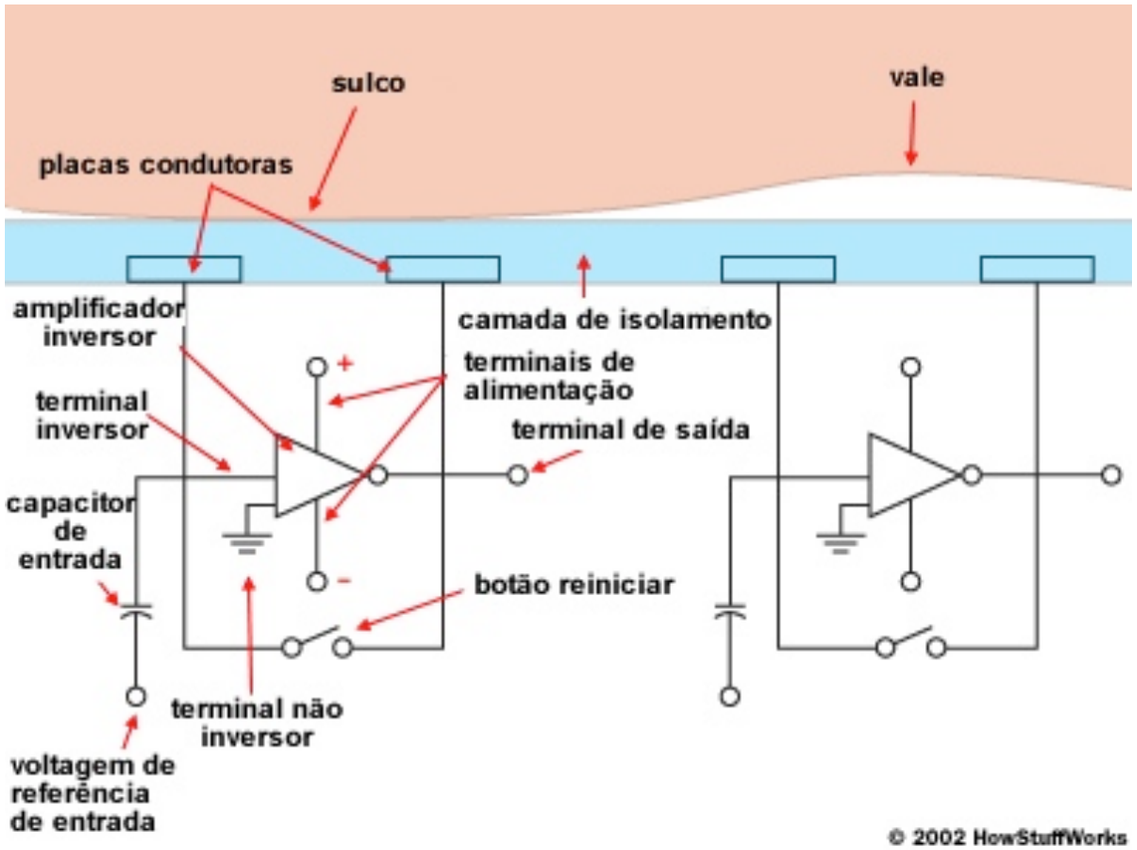
- **Ópticos**
  - **Total internal reflection (TIR):** Diferença de reflexão da luz nas cristas (em contato com o vidro) e sulcos (ar).
    - Ataques:
      - dedos artificiais de material com reflectância semelhante a da pele
      - Impressões digitais latentes
        [Thalheim et al. 2002] apenas com a fita adesiva, pó de grafite e luz
  - **Multispectral imaging (MSI):** Será detalhado mais adiante

Sensores para impressões digitais

- **Ultrasom:** Diferença de velocidade das ondas acústicas entre as cristas e o ar.
  - Ataques:
    - dedos artificiais de gelatina (mesmas características da pele em relação a eco)

Sensores para impressões digitais

- **Capacitivos:** Diferença de capacitância entre as células sob os sulcos ou cristas.
  - Ataques:
    - Impressões digitais latentes [Thalheim et al. 2002] Fácil!
    - Dedos artificiais de gelatina

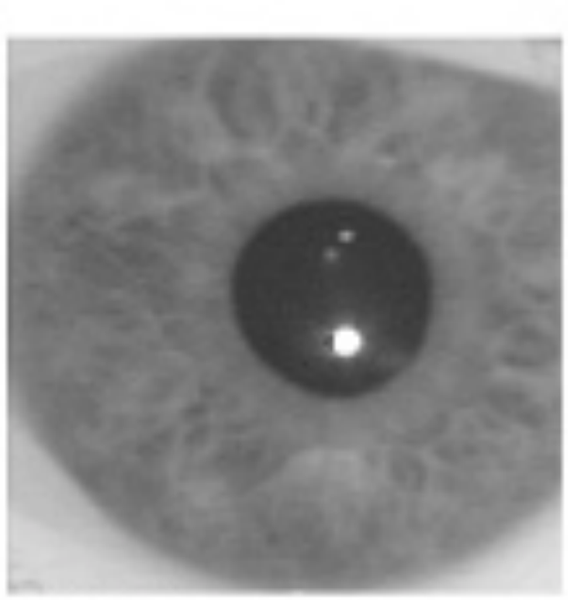


- **Térmicos:** Diferença de temperatura entre cristas (em contato com o vidro) e sulcos (ar).
  - Ataques:
    - Dedos artificiais de gelatina ou silicone [Thalheim et al. 2002] Bem mais dificil de enganar do que os ópticos e capacitivos

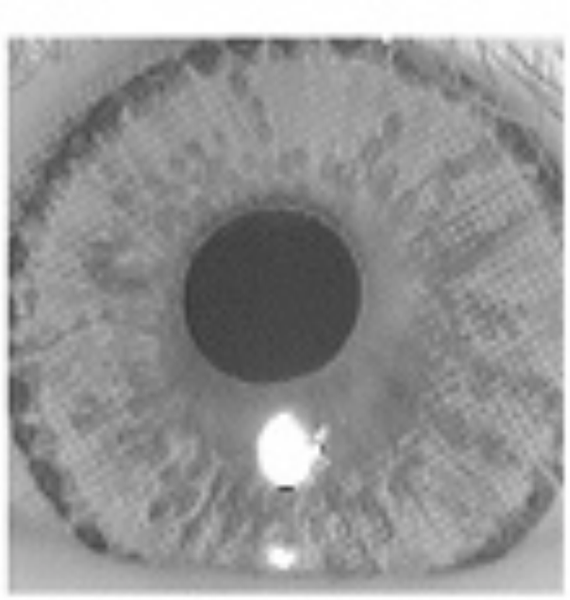
Detecção do Spoof

- Transpiração
  - Mudanças temporais na quantidade de suor presente na superfície do dedo
  - Obter várias imagens ao longo do tempo
  - Sensores capacitivos e ópticos
- Absorção da pele
  células vermelhas do sangue, hemoglobina, oxigênio
- Temperatura da pele
  Um spoof pode ser colocado num dedo real, mas parte da temperatura é dissipada
- Pulsação
  Varia de pessoa para pessoa, e de acordo com sua situação atual
- Outras possibilidades
  Resistência elétrica da pele, Detecção ultrasônica de estruturas dérmicas

Íris



Natural iris

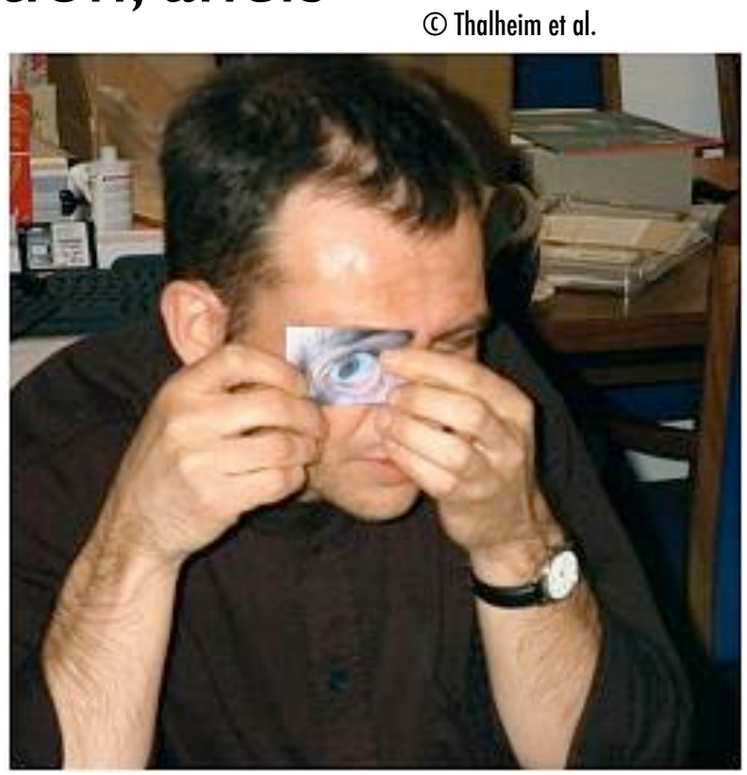


Fake iris printed on a contact lens

© Nixon et al

Criação do Spoof

- Como funciona
  - Se baseia na estrutura da área texturizada do olho em torno da pupila, usa luz infravermelha
  - Cria templates com Gabor decomposition, anéis concentricos.



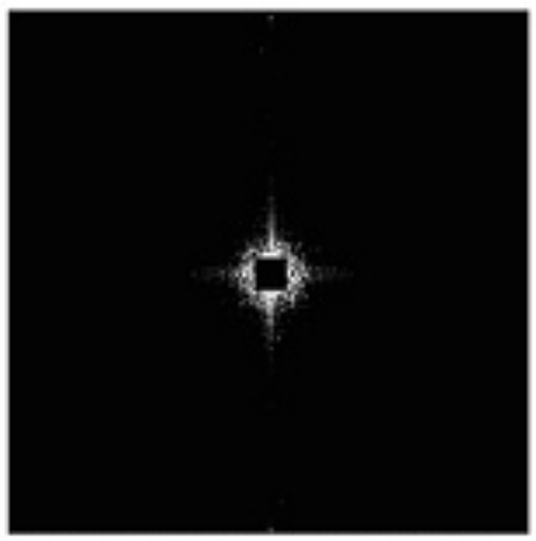
Criação do Spoof

- Spoofs
  - Foto ou vídeo do olho em alta qualidade [Thalheim et al. 2002] foto com impressora jato de tinta, 2400 x 1200 dpi, furo para a pupila
  - Padrões de íris impressos em lentes de contato
  - Íris artificiais tridimensionais ou com várias camadas

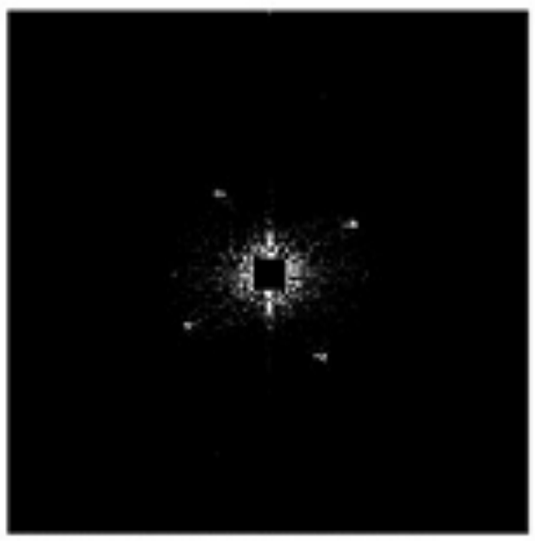
© Thalheim et al.

Detecção do Spoof

- Detectar movimentos involuntarios dos olhos (*hippus*), ou reação à luz, ou se pisca
- Desafio-resposta (piscar, mover para um lado)
- Análise de Fourier



2D Fourier spectrum of natural iris



2D Fourier spectrum of fake iris

© Nixon et al

Face

© Tan et al.

Criação do Spoof

- Como funciona
  - Tiram fotos em luz visível ou infravermelha.
  - O match se baseia em caracteristicas como a distância entre os olhos.
  - Podem ser 2D ou 3D.


© Thalheim et al.

- Spoofs
  - Foto impressa da pessoa
  - Vídeo da pessoa na tela de um notebook/celular
  - Modelos tridimensionais

Detecção do Spoof

- Movimentos involuntários do rosto, cabeca, piscar dos olhos
- Textura da pele, refração de acordo com o tipo de luz
- Reflexão da luz 2D *versus* 3D [Tan et al. 2010]
- Análise de Fourier da imagem
- Sensor tridimensional
- Desafio-resposta (piscar, sorrir, falar frases)

Reflexões [Thalheim et al. 2002]

- Os dispositivos testados não são para ambientes de segurança máxima, mas...
- Vale o custo X benefício, se são facilmente enganados?
- Os dispositivos biométricos já tem condições de substituir as senhas?

Multispectral Imaging em impressões digitais

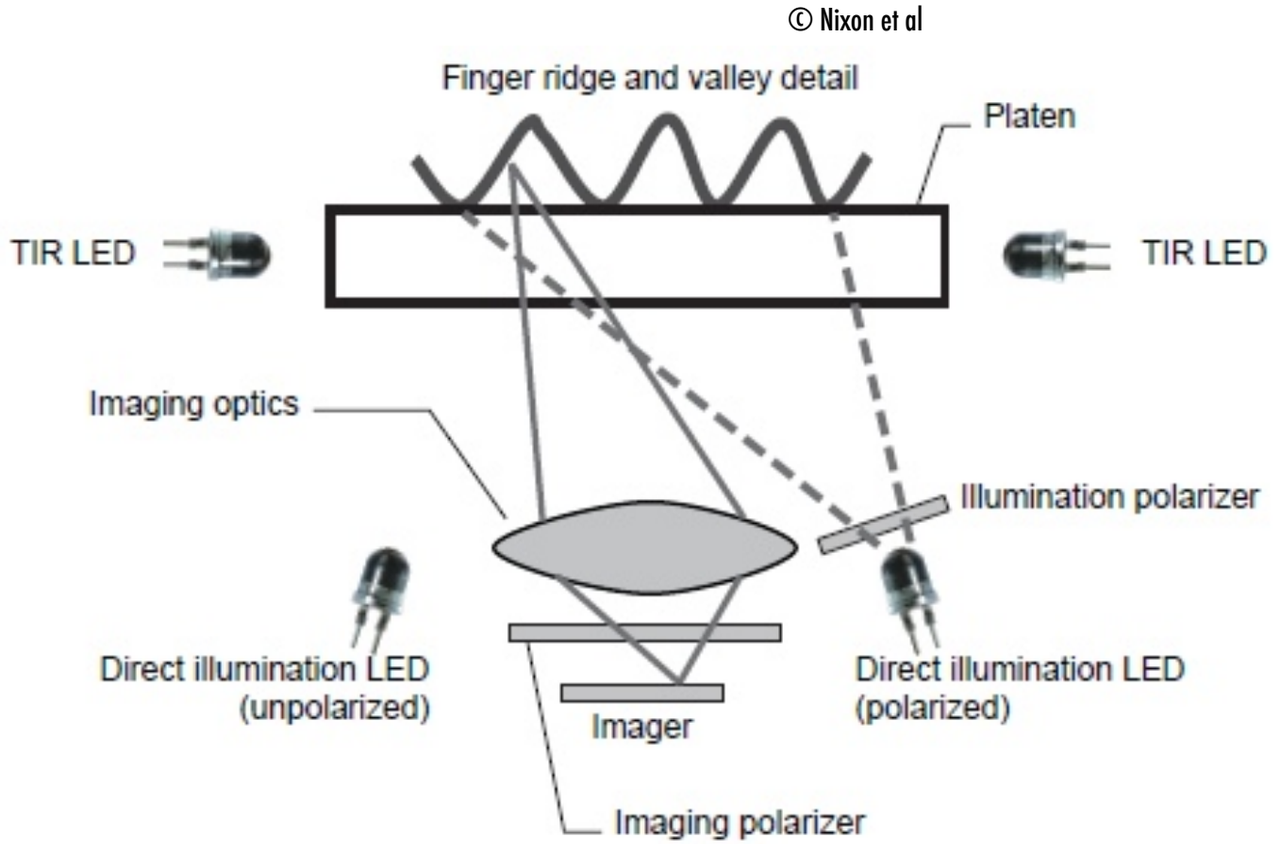
[Nixon et al. 2007]

Sensor

- Sensor de impressões digitais baseado em MSI, produzido pela Lumidigm – J110
- Configurado para obter imagens da superfície e subsuperfície do dedo em várias condições ópticas.
- Características ópticas da subsuperfície discriminam entre peles verdadeiras e falsas
- Combinação possibilita obter dados biométricos sob diversas condições fisiológicas e ambientais.
  Luz ambiente forte, umidade, pouco contato entre o dedo e o sensor, pele seca

Princípios de Operação

- Imagens capturadas sob características diferentes: informações diferentes e complementares.
- Frequências de luz diferentes: penetram a pele em diferentes profundidades.
- Polarizações diferentes: mudam o grau de contribuição das características da superfície e subsuperfície da pele na imagem.
- Orientações de luz diferentes: mudam o local e a intensidade com que características da superfície são acentuadas.



Teste de Spoof

- 3 sensores, 118 voluntários entre 18 e 80 anos
- Visitas ao longo de 3 semanas, não foram instruídos a lavar as mãos ou tratar os dedos previamente.
- Total de 49 tipos de spoof: Latex, silicone, massa de modelar, argila, borracha, cola, resina, gelatina e fita foram utilizadas em várias cores, concentrações e espessuras.
- Um total de 17.454 imagens foram coletadas de dedos reais e 27.486 imagens falsas. Para cada classe de spoof, entre 40 e 1940 amostras foram coletadas, sendo os spoofs transparentes os que mais tiveram amostras.
- Cada imagem foi processada utilizando wavelets para a extração de características baseadas nas informações espectrais e de textura disponíveis. 8 características foram utilizadas para classificação.

Teste de Spoof

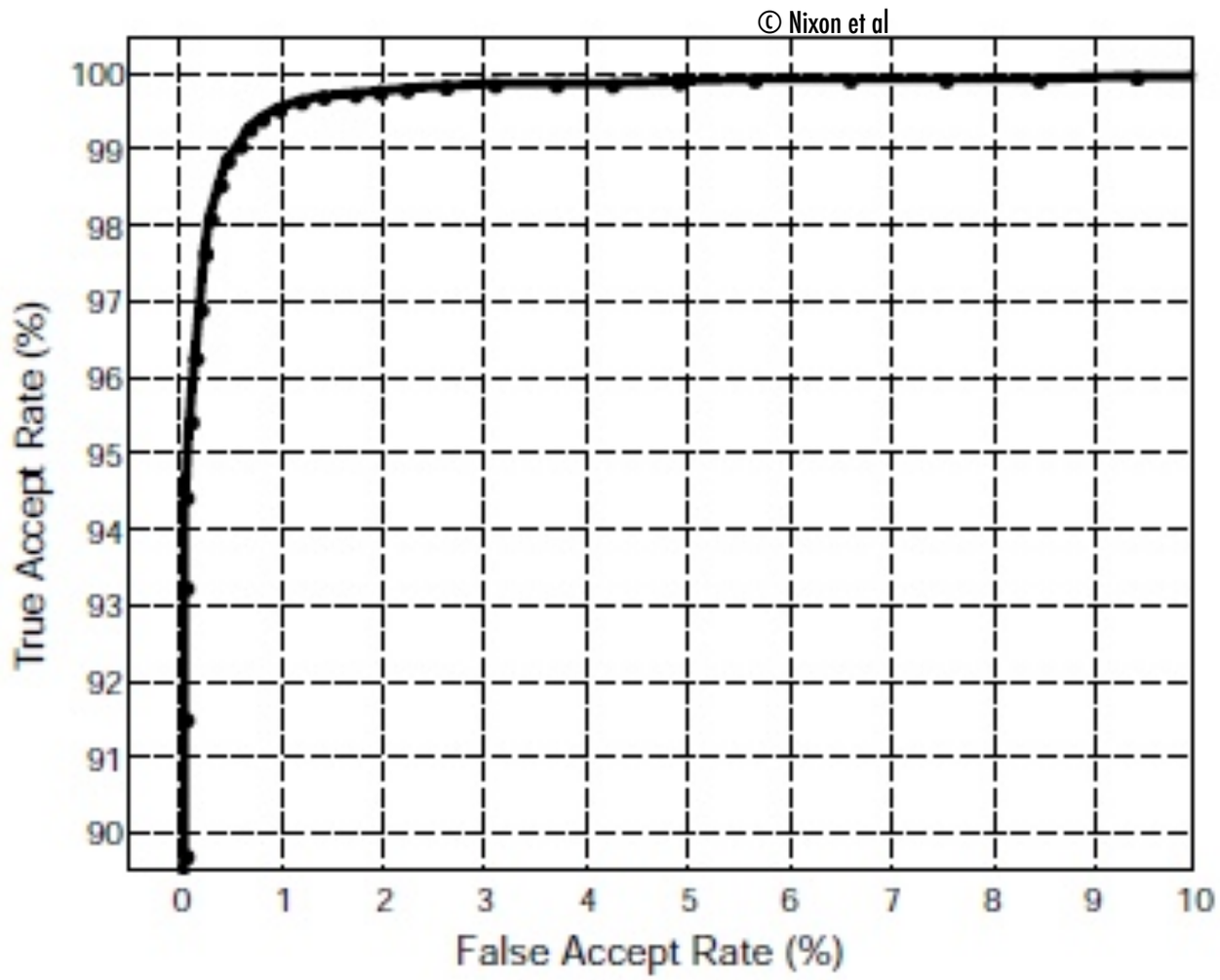
- Para calcular o trade-off do erro entre Verdadeiro Positivo e Falso Positivo, foram utilizadas as médias das distâncias euclidianas para as classes de pessoa e spoof.

- Verdadeiro Positivo: 99.5%

- Falso Positivo: 0.9%.

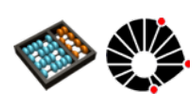
- Nesse ponto muitos tipos de spoof nunca eram aceitos e nenhum caso de spoof tinha uma taxa de falso positivo maior que 15%.

- Detecção de spoof robusta em sensores MSI com mínimo impacto para o usuário genuíno.



Face Liveness Detection from a Single Image with Sparse Low Rank Bilinear Discriminative Model

[Tan et al. 2010]



Face Liveness Detection

- A idéia
- Uma face humana real – 3D
- Face em uma foto – 2D
- A rugosidade de uma face real é diferente da de uma foto.

Face Liveness Detection

- O Modelo
  - Duas imagens: $I_t(x, y)$, de uma face humana real, e $I_f(x, y)$ de uma face impostora. Qual a diferença delas?
- Suposição de reflectância Lambertiana
  - Superfície da face é modelada como um reflector difuso ideal.
  - De acordo com a lei do cosseno de Lambert, a intensidade de uma imagem de face é descrita como:

$$I(x, y) = f_c(x, y)\rho(x, y)A_{light}\cos\theta$$

Onde $f_c(x, y)$ depende da câmera, A_{light} é a intensidade da luz e $\rho(x, y)$ representa a reflectância da superfície.

Face Liveness Detection

- $\cos\theta = n \times s$ é o ângulo entre a normal e o raio de luz.
- $A_{light}(n \cdot s) \triangleq \mu(x, y)$ é a iluminância da imagem.
- Sendo $f_c(x, y)$ constante, as imagens real e impostora podem ser descritas como:

$$I_t(x, y) = \rho_t(x, y)\mu_t(x, y),$$
$$I_f(x, y) = \rho_f(x, y)\mu_f(x, y).$$

- Sob as mesmas condições de iluminação, a diferença entre as imagens é obtida comparando as propriedades de superfície, reflectância e normal.

Face Liveness Detection

- É possível estimar os valores para $\rho(x, y)$ e $\mu(x, y)$ através de uma série de amostras.
- Método baseado em Variational Retinex
  - Primeiro se estima a iluminância, para depois estimar a reflectância.
  - O método Logarithmic Total Variation (LTV) é usado para estimar a iluminância, através da fórmula

$$\mu = \min \int_{image} \| \nabla \mu \|^1 + \ddot{e} \mid I - \mu \mid$$

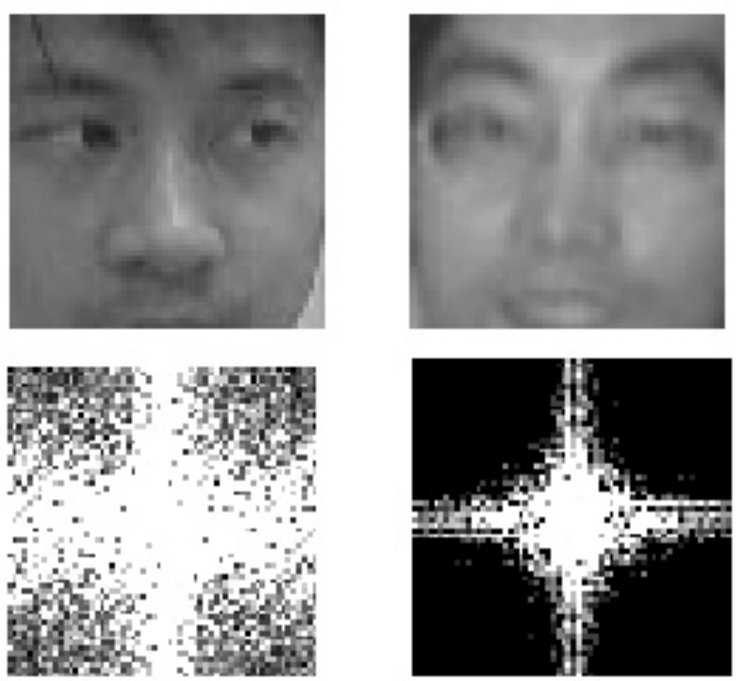
λ é um parâmetro de fidelidade de dados (utilizado 0.5 no paper)

  - Tendo μ pode-se estimar ρ com a fórmula de Land Retinex:

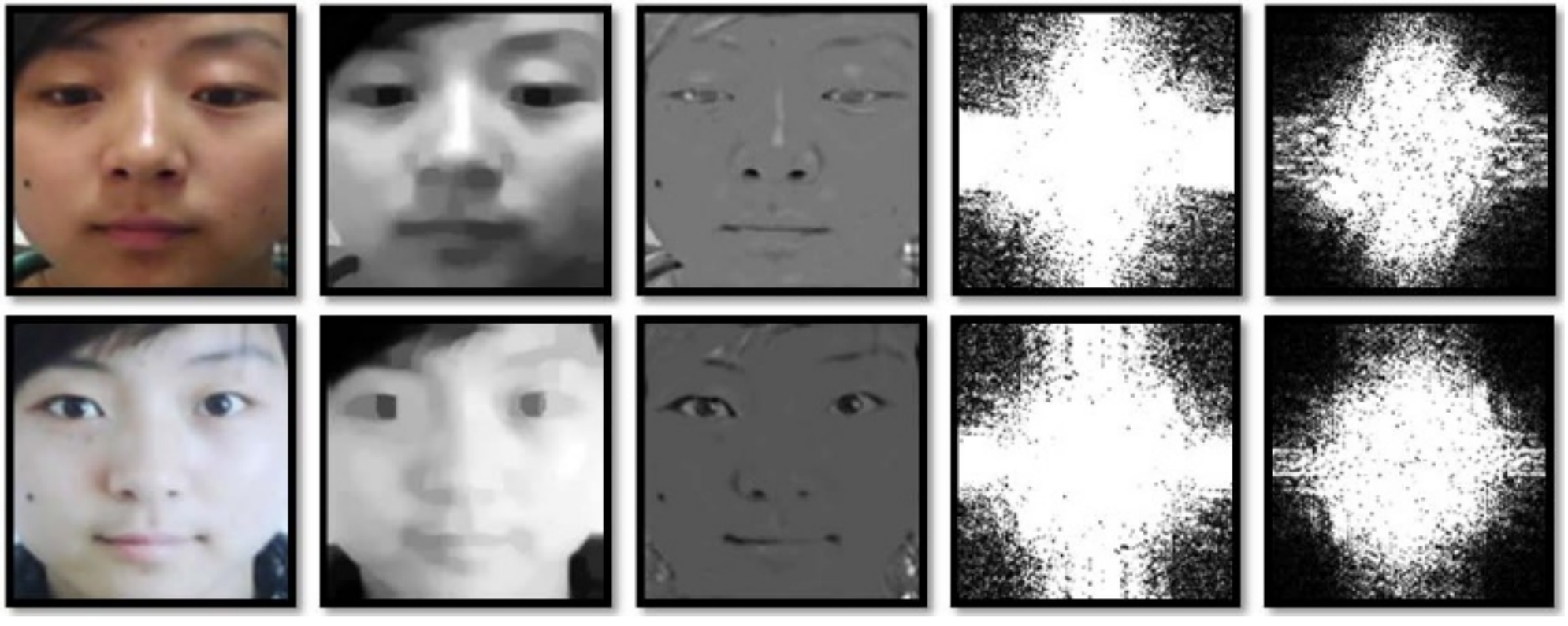
$$\log(\rho(x, y)) = \log(I(x, y) + 1) - \log(\mu(x, y) + 1)$$

Face Liveness Detection

- Método baseado em Diferença de Gaussianas (DoG)
- Analisa o espectro 2D de Fourier: frequências muito altas são ruidosas, utilizar as médias-altas
- Para manter o máximo de detalhes possível sem introduzir ruído ou aliasing, nesse trabalho são usadas gaussianas interna de $\sigma_0 = 0.5$ e externa de $\sigma_1 = 1.0$.



© Li et al.



© Tan et al.

- Linha superior: Imagens reais, Linha inferior: Imagens recapturadas
- Da esquerda para a direita:
  - 1) Imagem original;
  - 2) Imagem μ estimada com LTV; 3) Imagem ρ estimada com LTV
  - 4) Espectro de Fourier centralizado da imagem original; 5) Espectro de Fourier centralizado da imagem filtrada com DoG

- A Classificação
  - Treinado diretamente com as amostras, sem mais extrações de características.
- Sparse Logistic Regression
  - Seja $\mathbf{x} \in \Re^n$ uma amostra e $y \in \{-1,1\}$ a classe binária associada: Imagem falsa = +1, verdadeira = -1.
  - O modelo de regressão logística é dado por:

$$\text{Prob}(y \mid \mathbf{x}) = \frac{1}{1 + \exp(-y(\mathbf{w}^T \mathbf{x} + b))}$$

  - $\text{Prob}(y \mid \mathbf{x})$ é a probabilidade condicional da classe $y = 1$, dada uma amostra $\mathbf{x}$, $\mathbf{w} \in \Re^n$ é um vetor de pesos, $b \in \Re$ e é a intersecção.

Face Liveness Detection

- Sendo um conjunto de *m* dados de treinamento, $\{\mathbf{x}_i, y_i\}_{i=1}^{m}$ a função de probabilidade associada é definida como

$$\prod_{i=1}^{m} \text{Prob}(y_i \mid \mathbf{x}_i)$$

- O negativo do logaritmo da função de probabilidade é chamado de perda logística, e perda logística média é definida como:

$$\text{loss}(w,b) = -\frac{1}{m}\log\prod_{i=1}^{m}\text{Prob}(y_i \mid \mathbf{x}_i)$$

$$= \frac{1}{\text{m}}\sum_{i=1}^{m}\log(1+\exp(-y_i(\mathbf{w}^T\mathbf{x}_i + b)))$$

- Podemos determinar **w** e *b* minimizando a média de perda logística.

Face Liveness Detection

- Sparse Low Rank Bilinear Logistic Regression
  - Opera sobre a representação bi-dimensional das imagens, para explorar as suas propriedades espaciais.
  - Objetivo é aprender um matriz de projeção de posto baixo. – Número de linhas ou colunas linearmente independentes é baixo.
- Non Linear Model via Empirical Mapping
  - Transforma o mapeamento definido sobre as amostras de treinamento num espaço de características.
  - Usa SVM probabilístico, Relevance Vector Machine e Import Vector Machine

Face Liveness Detection

- Experimentos
  - Fotos de alta definição com uma câmera Canon, de modo que a face ocupa 2/3 da área da foto.
  - Impressão das fotos em papel fotográfico e em papel A4 70g. Fotos tiradas das fotografias impressas.
  - 

© Tan et al

Face Liveness Detection

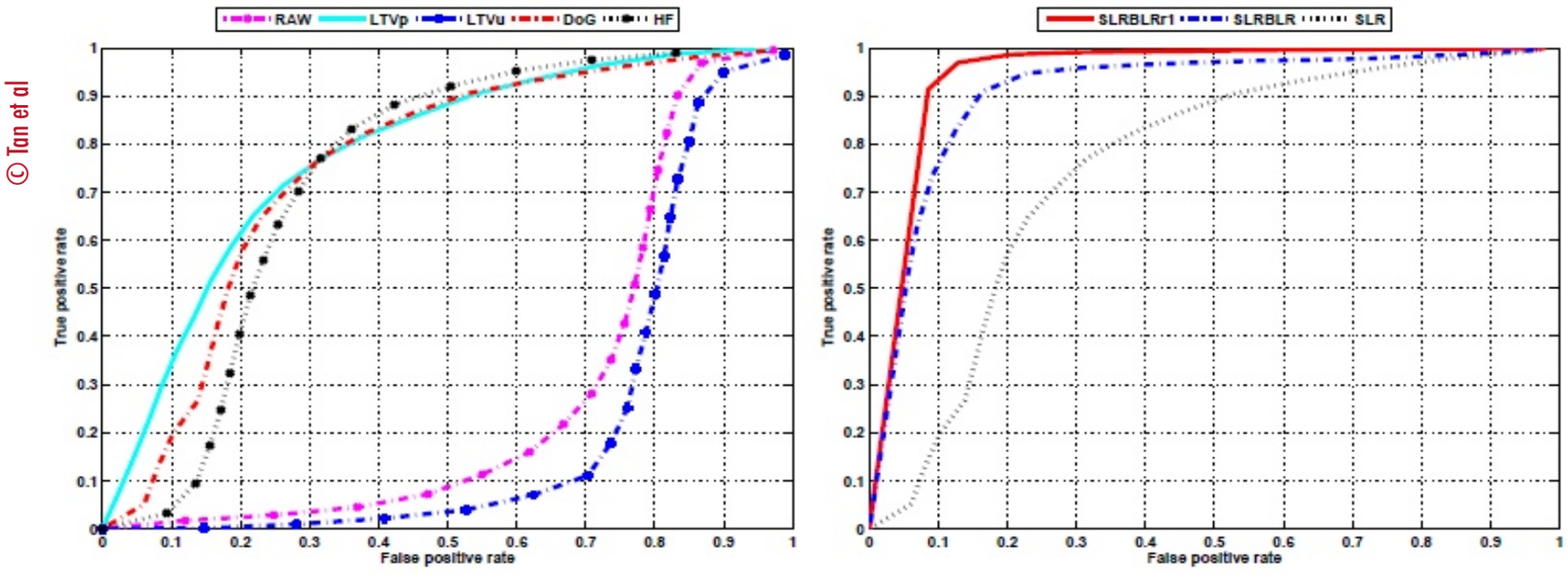
- Experimentos

	Session1	session2	session3	Total
Training Set				
Client	889	854	0	1,743
Imposter	855	893	0	1,748
Total	1,744	1,747	0	3,491
Test Set				
Client	0	0	3,362	3,362
Imposter	0	0	5,761	5,761
Total	0	0	9,123	9,123

- Normalização geométrica: detecção de face e corte, rotação e escala para fixar as posições dos centros dos olhos. Imagens fixadas em 64x64 pixels e conversão para escala de cinza de 8 bits.

Face Liveness Detection

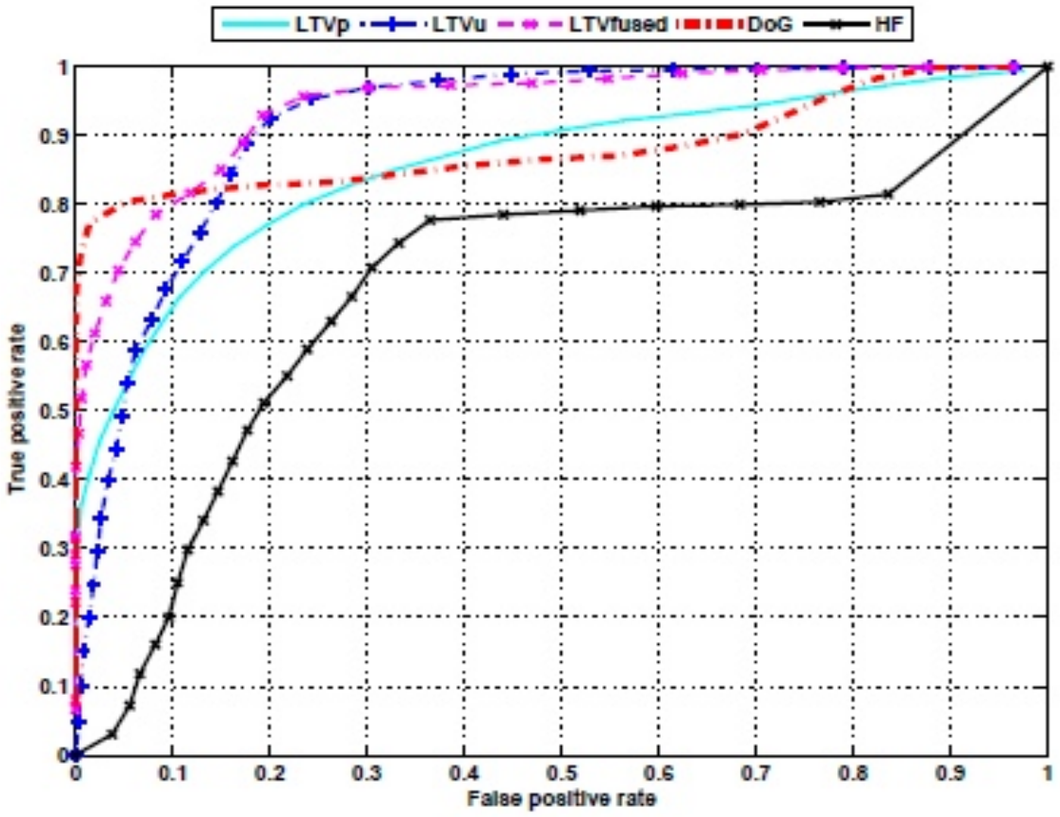
- Resultados
  - Sparse linear logistic regression
  - RAW: Imagem Original; LTVp: Imagem ρ estimada com LTV; LTVu: Imagem μ estimada com LTV; DoG: Imagem com filtro DoG; HF: Filtro em 1/3 das mais altas frequências.

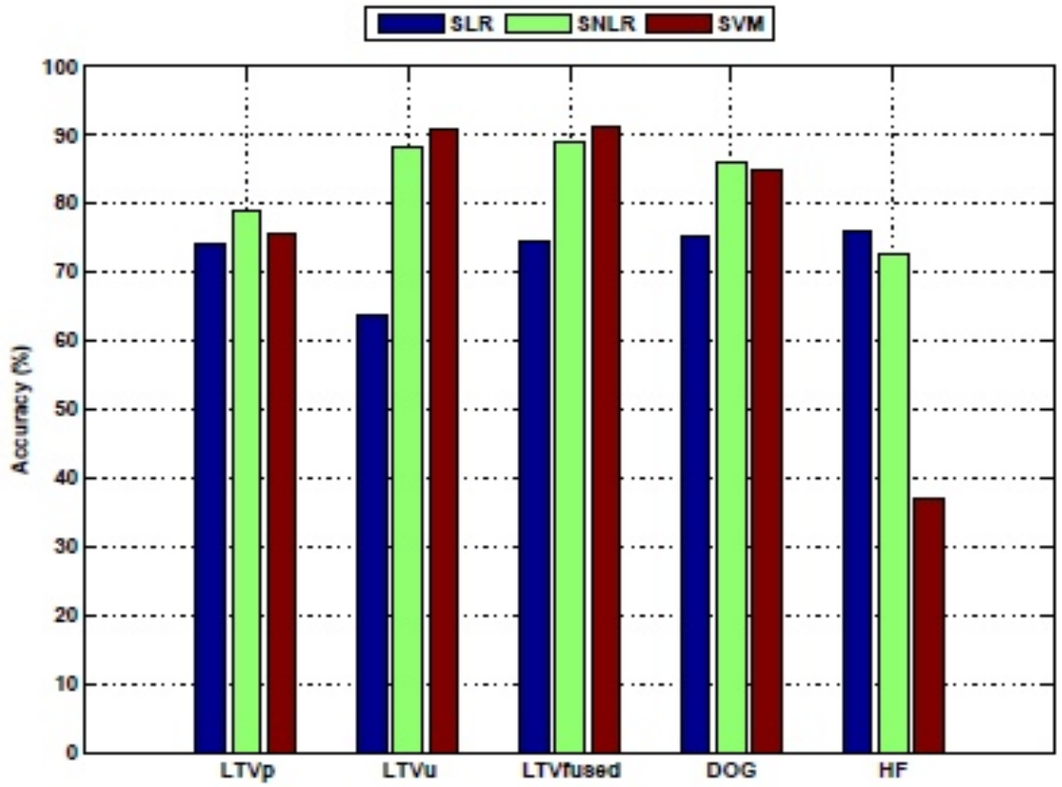


© Tan et al

Face Liveness Detection

- Resultados
  - Sparse nonlinear logistic regression e comparação





© Tan et al

Conclusões

Conclusões

- Jogo de gato e rato: novas técnicas de detecção, novos ataques
- São necessárias pesquisas, independentes dos fabricantes, para medir a segurança e apontar falhas
- Há vários métodos anti-spoof que parecem promissores, como o MSI da Lumidigm para impressões digitais e o [Tan et al. 2010] para face, mas só com testes no mundo real podemos afirmar

Referências

Referências

- **[Nixon et al. 2007]** Kristin Adair Nixon, Valerio Aimale, and Robert K. Rowe. Spoof detection schemes. White paper, LumidigmInc., 2007.

- **[Thalheim et al. 2002]** L. Thalheim, J. Krissler, P.-M. Ziegler; Body Check: Biometric Access Protection Devices and their Programs Put to the Test. Heise Online. November 2002

- **[Tan et al. 2010]** Tan, X.; Li, Y.; Liu, J.; Jiang, L.: Face Liveness Detection from A Single Image with Sparse Low Rank Bilinear Discriminative Model. In European Conference on Computer Vision (2010)

- **[Li et al. 2004]** Jiangwei Li , Yunhong Wang , Tieniu Tan , A. K. Jain: Live face detection based on the analysis of Fourier spectra. In Biometric Technology for Human Identification (2004)

Obrigado!