Powering
Trusted Identities

Informativo Técnico

Aplicação de leitores de impressão digital multiespectral no projeto UE2020

Tribunal Superior Eleitoral

SOBRE O DOCUMENTO

Este documento apresenta uma visão geral sobre tecnologias de captura de impressão digital, e em especial detalhes a tecnologia de ***Leitura De Impressão Digital Multiespectral***, suas vantagens, e na seção final, um conjunto de sugestões técnicas em atendimento ao chamado da AUDIÊNCIA PÚBLICA DA UE2020 nº 1/2019 PROCESSO Nº 2019.00.000006505-5, que permitiriam que este tipo de tecnologia venha a competir e contribuir com o projeto.

Sumário

VISÃO GERAL SOBRE MÉTODOS DE CAPTURA

Aquisição de digitais em dispositivos capacitivos

Nesta classe estão os sensores que detectam as perturbações de capacitância, geradas pelo toque do dedo sobre a superfície de silício do sensor para obter a imagem da impressão digital.

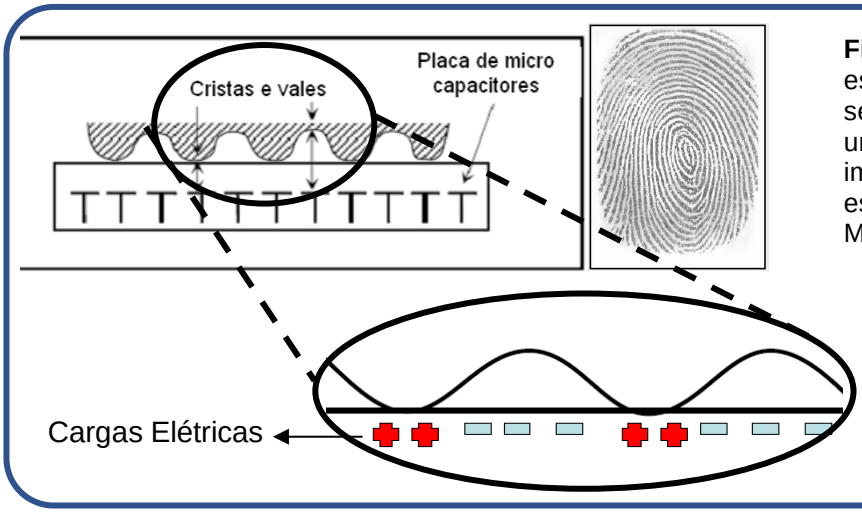


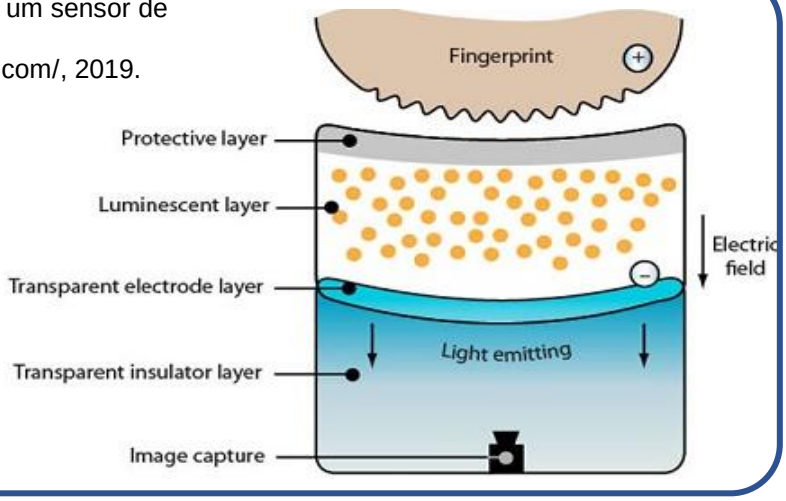
Figura – Modelo esquemático de um sensor capacitivo e um exemplo de imagem colhida por este sensor. Fonte: MODI, 2008.

Sensores Capacitivos não produzem distorções geométricas como sensores de passagem, mas são propensos a apresentar distorções devido à natureza elétrica da tecnologia que empregam. Uma descarga eletrostática pode afetar a imagem resultante dado que suas placas condutoras são sensíveis a esta condição. Também podem afetar o dispositivo ruídos oriundos da linha de energia elétrica de 60 Hz e internos do sensor.

Aquisição de digitais em dispositivos de eletroluminescência

Nesta classe estão os sensores que fazem a leitura da imagem da impressão digital através da captura da imagem fluorescente formada pelo contato da pele, eletricamente estimulada, com uma película de filme especial (LEF ou Light Emitting Film – Película Eletroluminescente, em tradução livre). De forma similar ao dispositivo capacitivo, as perturbações de eletricidade, geradas pela descarga de íons da pele sobre o filme, fazem a superfície da película brilhar. Uma câmera posicionada abaixo do filme captura a imagem formada, que depois de processada, forma o desenho imagem da impressão digital.

Figura – Modelo esquemático de um sensor de eletroluminescência.
Fonte: http://hozoorghiyab.blogfa.com/, 2019.



Aquisição de digitais em dispositivos Óticos

Os sensores agrupados nesta classificação se baseiam no fenômeno de detecção de luz espalhada (Frustated Total Intern Reflectance, FTIR) para obter o desenho da impressão digital, quando, através do toque do dedo sobre um prisma, se distorce o reflexo da fonte de luz interna sobre o sensor de imagem também interno (CCD).

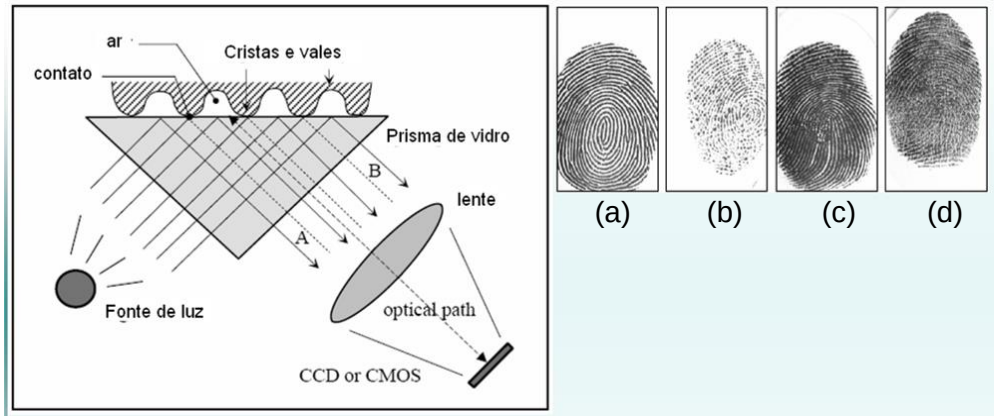


Figura – Modelo esquemático de um sensor ótico de prisma simples.
Ao lado, exemplos de imagens colhidas em condição (a) normal, (b) com dedo seco, (c) dedo úmido e (d) dedo idoso. Fonte: adaptado de MALTONI et al., 2009.

Os sensores ópticos introduzem distorções características de sua tecnologia. As bordas das imagens das impressões digitais capturadas podem apresentar a tendência de ficarem turvas, ou podem se apresentar de maneira desfocada devido à instalação de lentes e suas curvaturas. Um fenômeno chamado Distorção Trapezoidal também é observado em imagens de impressões digitais capturadas de sensores ópticos, devido à desigualdade de caminhos ópticos entre cada ponto da impressão digital e a lente do sensor (IGAKI et al., 1992). O nível de contraste em imagens de impressões digitais resultantes também é afetado por esta tecnologia podendo apresentar zonas de sombra na imagem devido à luz direta incidindo sobre o sensor.

O método de captura multiespectral

Este tipo de sensor captura várias imagens da impressão digital, cada uma usando diferentes comprimentos de onda luminosa, em diferentes orientações e polarizações. Cada comprimento e polarização de luz projetado sobre o dedo reflete em uma diferente subcamada da epiderme e da derme, onde cada imagem forma uma diferente perspectiva de uma mesma impressão digital. Uma vez que, por questões morfológicas, todas estas perspectivas guardam entre si o mesmo padrão de desenho de linhas e vales da camada externa, é possível combinar estas imagens através de um algoritmo e obter uma fidedigna representação da imagem da impressão digital.

O ponto forte desta tecnologia é que, diferente das outras tecnologias apresentadas acima, este tipo de tecnologia não depende do contato da epiderme com a superfície do prisma para que uma imagem da impressão digital seja formada e obtida, apresentando vantagens nítidas em duas situações:

- Quando existe a presença de obstáculos, tais como umidade, líquidos ou oleosidade, e outros elementos que acabam entrado em contato involuntário com a prisma junto com o dedo, o que acaba por gerar, na imagem da impressão digital obtido, artefatos que não fazem parte do desenho de vales e cristas, distorcendo o seu real desenho.
- Dedos secos ou com a impressão digital desgastada por trabalho manual intenso, comum em cirurgiões e pedreiros e professores, que não tem uma camada externa nitidamente definida pra tocar o prisma de captura e gerar uma imagem

Assim, por conta destas características que este é considerado o método de captura de impressão digital mais robusto quando são consideradas condições adversas de uso, como ambientes com iluminação direta solar ou presença de umidade (BONDA, FAKOUFAR, 2009) (ROWE, NIXON, 2005) (ROWE, NIXON, BUTLER, 2007).

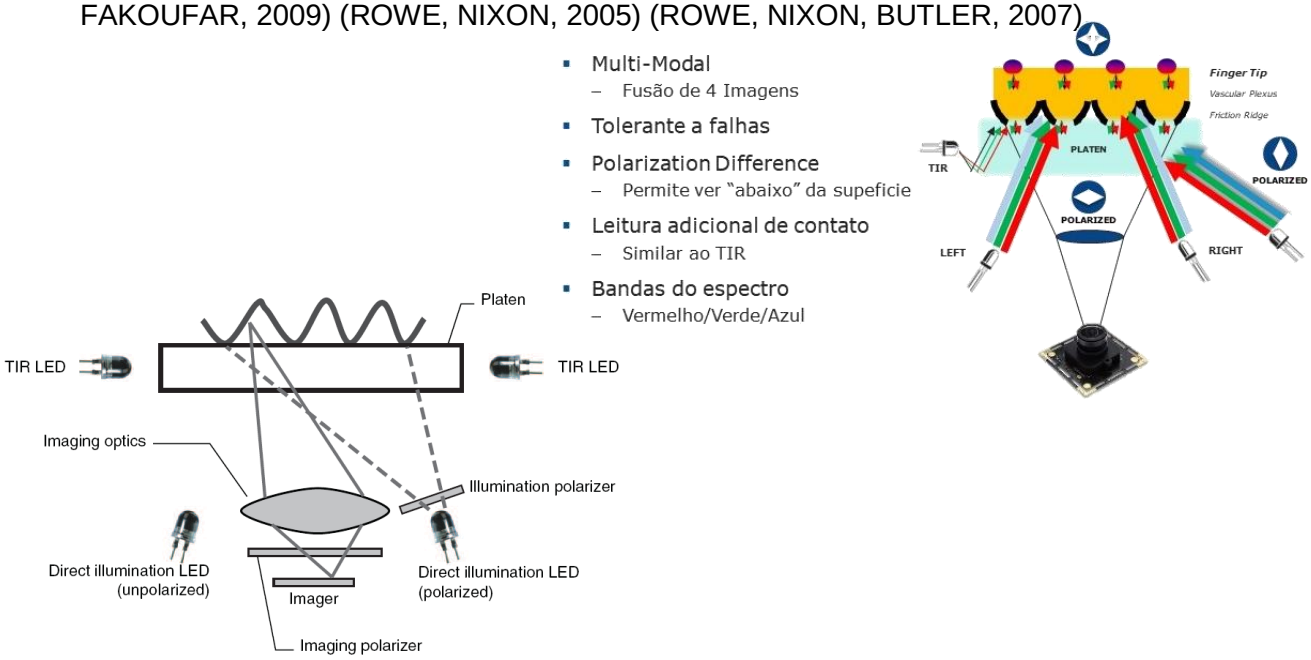


Figura - Modelos esquemáticos de um sensor de captura multiespectral. Fonte: adaptado de ROWE, R. K.; NIXON, K. A.. 2005.

VANTAGENS OBSERVADAS NA CAPTURA MULTIESPECTRAL

Imagens obtidas em condições adversas

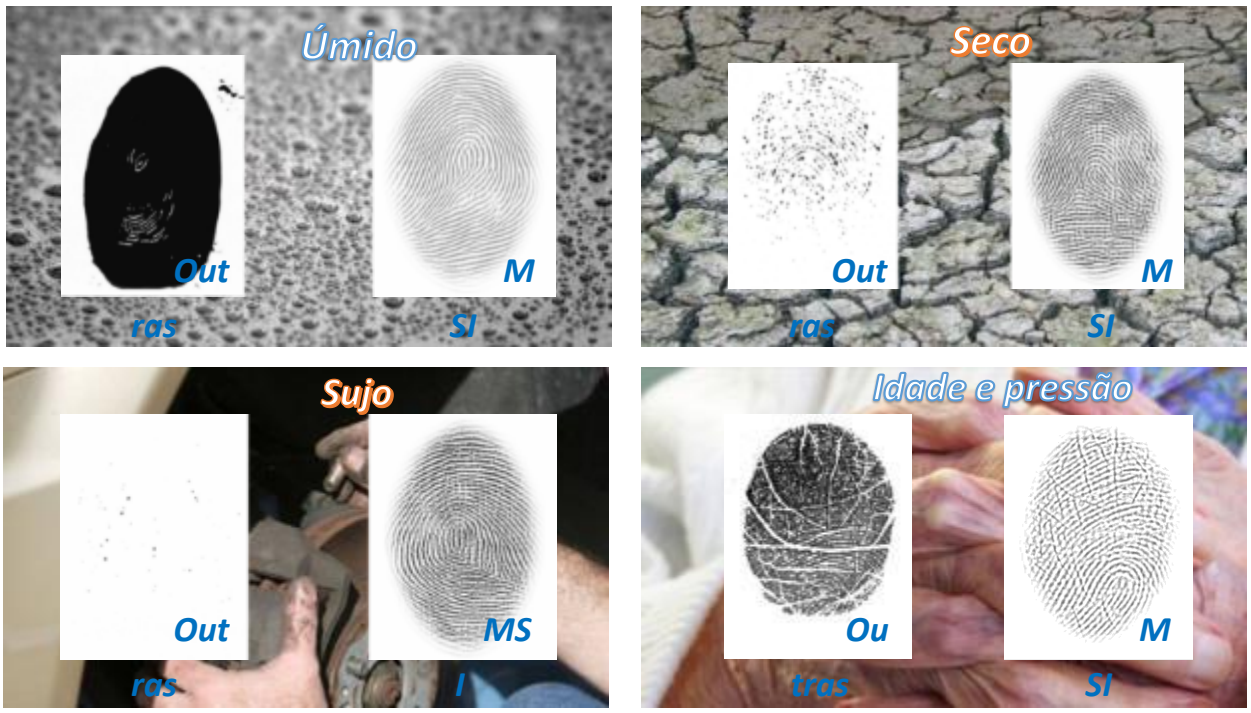
Por não depender do contato da impressão digital com uma superfície, isto é, não depender apenas do relevo externo da impressão digital para obter seu desenho, a captura multiespectral apresenta vantagens sobre outros métodos, particularmente em condições adversas (BONDA, K.; FAKOURFAR, H.. “Performance of Fingerprint Recognition System in Maritime Environment.” 2009. https://docplayer.net/21649987-Abstract-1-introduction-1-1-methodology.html) ou de pessoas com condições de pele especiais (https://www.youtube.com/watch?v=9iSgbFii4-M).

Em geral, tecnologias de contato apresentam grande dificuldade em capturar imagens nas seguintes situações:

- **Dedos secos ou com pele ressecada:** dedos secos ou ressecados tendem a apresentar uma pele mais rígida. Esta rigidez não permite o contato da pele de maneira consistente com o prisma, gerando imagens incompletas da impressão digital.
- **Dedos úmidos, ou sensor úmido:** dedos úmidos, ou umidade presente no prisma acabam gerando ou ampliando as áreas de contato da pele com o sensor, gerando imagens em que é impossível discernir o que é uma linha e o que é a presença do liquido. Em um estudo considerando dedos enrugados por umidade. KRISHNASAMY, P.; BELONGIE, S.; KRIEGMAN, D; 2011 apontam que leitores ótico não são capazes de executar a leitura de impressões digitais nestas condições e apontam como saída adequada o emprego de leitores multiespectrais.
- **Dedos sujos**: a presença de determinados tipos de sujeira, como óleos hidratantes ou de protetores solares, assim como a umidade, gera imagens com artefatos adicionais a impressão digital, criados pela presença do liquido.
- **Pessoas de idade avançada:** a pele, com o avanço da idade, perde na camada mais externa, parte de sua consistência, se tornando mais maleável. Nestas condições, ao tocar o sensor, a imagem das linhas fica prejudicada, pois ficam menos evidentes as diferenças entre vales e sulcos da digital.
- **Pressão dos dedos:** Uma outra vantagem de sensores MSI é que a pressão exercida pelo usuário tem pouca interferência sobre o resultado da captura. A impressão digital é colhida de toda a área de captura mesmo quando o dedo não entra em contato com todo o prisma, garantindo que as áreas de interesse da digital (as que tem as minúcias ao redor do núcleo) estarão presentes.

Comparativo de captura de imagens

A figura abaixo mostra comparativos de imagens entre sensores de toque e sensores multiespectrais:



Detecção de Ataques de Apresentação (popular Liveness ou detecção de vida)

Em decorrência da quantidade e qualidade de informações obtidas por um sensor multiespectral, equipamentos baseados nesta técnica se apresentam especialmente preparados para a missão de diferenciar uma tentativa fraudulenta de verificação de uma tentativa feita pelo indivíduo correto. Por exemplo, discriminar a cópia do dedo de um eleitor, feita em silicone para o dedo real do eleitor.

Sensores multiespectrais são particularmente bem-sucedidos nesta tarefa pois contam com uma quantidade de informações das estruturas do dedo (presentes na sub-camadas da pele) para identificar materiais diferentes do tecido pele humana viva.

Não por coincidência esta foi a tecnologia adotada pela totalidade dos bancos brasileiros em seus caixas eletrônicos.

A capacidade de detecção de dedos falsos (detecção de ataques de apresentação) foi comprovada pelo reconhecido e renomado laboratório iBeta, credenciado pelo NIST, em um teste seguindo o padrão ISO 30107-3, tendo sido certificado com nível de 100% de acerto.

Na plataforma de teste, voluntários se cadastraram previamente e se autenticaram três vezes com sucesso para garantir seu efetivo cadastro. Na seuqência ataques de apresentação (PAs) foram tentados por cinco vezes cada. A cada tentativa realizada, o aplicativo forneceria um índice de qualidade de impressões digitais, uma pontuação de

atividade e uma pontuação de correspondência (match), além da exibição em tempo real da imagem obtida. Ao final do teste, os voluntários retornaram e se autenticaram mais três vezes com sucesso para verificar se o aplicativo de reconhecimento de impressões digitais ainda era capaz de reconhecer o usuário genuíno.

O iBeta não conseguiu obter acesso em nenhuma das tentativas de ataques (PAs) garantindo uma taxa de sucesso global de Apresentação de Ataque (PA) de 0%, o que equivale à taxa de correspondência de apresentação de ataque de imposição total combinada (IAMPR) de 0%. **Ou seja, um teste 100% bem-sucedido.**

Alta interoperabilidade com sistemas tradicionais e legados de impressão digital

Embora utilize uma técnica única para obter uma impressão digital, o resultado de sua leitura é 100% compatível e comparável com impressões digitais obtidas por outros métodos. Uma digital obtida em um sensor multiespectral pode tranquilamente ser comparada com bases de dados capturadas em sensores rolados ou batidos do tipo ótico e de eletroluminescência (como os presentes nas bases de dados do TSE, do Banco Itaú e da Polícia Federal).

A tecnologia produz imagens seguindo todos os padrões de mercado como a ISO/IEC 19794-4:2011 Information technology — Biometric data interchange formats — Part 4: Finger image data, e com o formato WSQ do FBI. A Lumidigm tem seu algoritmo de compactação certificado pelo FBI.

Além disso, a interoperabilidade da tecnologia multiespectral foi posta a prova em 2008, quando a OIT (Organização Internacional do Trabalho ou ILO) organizou e conduziu um teste (CAMPBELL; MADDEN; 2009) onde cruzou efetivamente a captura de impressões digitais feitas em diversos sensores, independentemente de sua certificação junto ao FBI, o que incluiu a participação de sensores baseados em capturas multiespectral outros óticos e outros capacitivos.

Nos resultados apresentados, de fato a interoperabilidade pode ser observada de forma consistente entre a maioria dos sensores.

Mas é na página 45 do relatório sobre os resultados que a resposta sobre a interoperabilidade de sensores Multiespectrais foi dada de forma categórica:

> *"… shows that the new Product H* is actually one of the best performing interoperable products."*
>
> *(… mostra que o novo produto H é, na verdade, um dos produtos com melhor desempenho para interoperabilidade.)*
>
> *"…product H* turns out to be one of the two best performing products."*
>
> *(…o produto H apareceu com um dos dois melhores produtos em termos de desempenho para interoperabilidade)*

**** Produto H é a referência usada para o leitor multiespectral utilizado no teste***

Casos de Sucesso do emprego de leitura multiespectral

Bancos Brasileiros

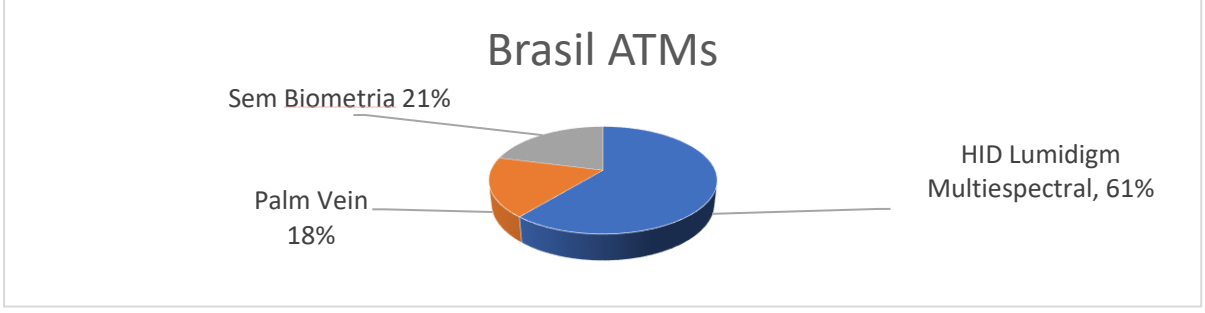
Bancos brasileiros são pioneiros no mundo na adoção de biometria em caixas eletrônicos. Embora um grande banco não tenha adotado a modalidade de impressão digital, esta foi a escolha de todos os demais bancos brasileiros que o fizeram.

Embora a forma de cadastramento de cada um tenha características particulares, e utilizem sensores de diversos tipos, TODOS SEM EXCEÇÂO adotam a tecnologia de leitura multiespectral Lumidigm em seus caixas eletrônicos com comprovado sucesso e nenhum registro de fraude em mais de 8 anos de aplicação.

Esta escolha se apresenta de forma natural e confirma as vantagens apresentadas acima para este tipo de leitura de impressão digital.

Importante lembrar que, em algumas destas instituições os primeiros dispositivos estão em operação desde 2011, sem nenhum processo de limpeza ou cuidado especial, em variadas condições de ambiente.

Bank	ATMs Biométricos	Usuários cadastrados (Milhões)	Transações mensais (Milhões)	Transações por ano (Milhões)	Biometric ATM Market Share
Banco ITAU	24.745	37	165	1.980	13,38%
CAIXA Economica Federal	25.000	25	60	720	13,51%
Banco do Brasil	32.000	20	80	960	17,30%
Banco Santander	14.000	10	20	240	7,57%
Banco Mercantil	500	2	5	60	0,27%
Tecban - Banco 24 horas	22.000		10	120	11,89%
BRB Banco de Brasilia	659	1	5	60	0,36%
BANRISUL	900	2	5	60	0,49%
BANPARA	451	1	3	36	0,24%
Banco BMG		1			
COAMO Agroindustrial Cooperativa		1			
CrediSis Sistema de Credito Corp.		1			
TOTAL	**120.255**	**98**	**353**	**4.236**	**65,01%**



SUGESTÕES DE MUDANÇA PARA O TERMO DE REFERÊNCIA DA UE2020

A HID Global é hoje o maior fabricante de leitores biométricos do mundo, englobando marcas reconhecidas de leitores de impressão digital tais como

- ***Digital Persona*** (já em uso em diversos modelos de urna)
- ***Crossmatch*** (em uso em diversos Detrans pelo Brasil, cadastramento do Passaporte, etc)
- ***Lumidigm*** (presentes em mais de 170 mil ATM e terminais lotéricos, única marca aprovada pelos bancos brasileiros)

Em virtude da publicação da Audiência pública para o projeto das urnas modelo UE 2020 gostaríamos de parabenizar a equipe técnica do TSE, que de forma brilhante elencou as diferentes tecnologias de leitura da impressão digital que poderão ser empregadas nas urnas.

Assim, na posição de fabricante com uma vasta linha de dispositivos prontos para atender o projeto UE2020 de diferentes formas, apresentamos nas próximas seções deste documento argumentos para reforçar nossa indicação do uso da tecnologia multiespectral da nossa linha ***Lumidigm***, além de sugestões para a especificação e pontuação das tecnologias que podem reforçar a especificação.

Motivações para mudanças

O processo de votação é reconhecido pela sua agilidade e simplicidade. A biometria, assim como aconteceu nos caixas eletrônicos, deve permitir melhora na experiência do usuário cidadão, o mesmo tempo que eleva a segurança do sistema.

Com vista neste objetivo entendemos que a aplicação de leitores multiespectrais são a solução mais adequada frente as opções de mercado.

Agilidade na autenticação

Por não dependerem do contato físico com as áreas de leitura, sensores multiespectrais apresentam clara tendência a manter constante o tempo para a captura de uma digital.

A consequência desta qualidade é que, mesmo os eventos de falha de autenticação tomam pouco tempo do processo. Diferente de outros sensores, que na presença de situações adversas (como dedos secos, húmidos, ou na presença de sujeira) aumenta consideravelmente o tempo de captura, sensores multiespectrais raramente se desviam de seu tempo médio. Esta característica, por si só, já fornece recurso de redução no tempo do processo de autenticação, tendo notável impacto em filas.

Captura em condições adversas

A capacidade de ler digitais em condições adversas beneficia o processo ao evitar que condições ambientais (como o ambiente seco da região do planalto central, a umidade da região amazônica, ou a grande presença de protetor solar nas mãos de eleitores das regiões litorâneas) tenham impacto no tempo de atendimento durante o dia.

As duas tabelas abaixo mostram a taxa de erro de autenticação (FRR) para vários sensores na presença das seguintes situações: presença de umidade no sensor (Water), presença de sujeira moderada (como terra, ou loção hidratante ou protetor solar), ambiente com excesso de iluminação (muito comum próximo a janelas ou muito próximo e abaixo de iluminação artificial), excesso de pressão no dedo pelo usuário, ou baixa pressão.

		Average real world performance	Water	Dirt	Bright Ambient Light	High finger pressure	Low finger pressure	Acetone (dry finger)
Lumidigm	Multispectral	1.58 (1)	0.00 (1)	2.56 (1)	5.33 (3)	0.00 (1)	0.00 (1)	1.58 (3)
Futronic	Optical	28.01 (2)	0.00 (1)	81.81 (6)	31.42 (5)	1.28 (3)	45.33 (2)	8.19 (5)
Sagem CBM	Optical	36.85 (3)	83.33 (5)	79.71 (5)	0.00 (1)	2.56 (4)	52.30 (3)	3.17 (4)
Identix	Optical	39.49 (5)	74.66 (3)	98.48 (10)	2.66 (2)	0.00 (1)	61.11 (4)	0.00 (1)
Sagem MSO	Optical	40.08 (4)	90.66 (6)	33.33 (2)	50.00 (9)	3.84 (5)	62.66 (5)	0.00 (1)
UPEK	Capacitive	45.04 (6)	NA (9)	67.24 (3)	36.00 (6)	40.90 (9)	91.66 (8)	34.42 (8)
SecuGen	Optical	53.14 (7)	94.44 (8)	94.80 (8)	6.66 (4)	7.69 (6)	81.94 (7)	33.33 (7)
Authentec	Radio frequency	60.73 (8)	NA (9)	76.62 (4)	45.94 (8)	53.16 (10)	98.66 (10)	90.00 (10)
Cross Match	Optical	66.59 (9)	79.72 (4)	95.23 (9)	100.00 (10)	17.94 (7)	73.33 (6)	33.33 (6)
TesTech	Electro-optical	66.60 (10)	91.66 (7)	86.95 (7)	36.11 (7)	27.27 (8)	93.84 (9)	63.79 (9)

Results are FRR rates (%) at an FAR of 0.01% (1 in 10,000). Performance ranks are in parentheses. September 2008
Water results for some sensors are marked NA (not available) because those sensors do not work in water.

		Average real world performance	Water	Dirt	Bright Ambient Light	High finger pressure	Low finger pressure	Acetone (dry finger)
Lumidigm	Multispectral	1.79 (1)	0.00 (1)	3.84 (1)	5.30 (4)	0.00 (1)	0.00 (1)	1.58 (3)
Futronic	Optical	27.74 (2)	0.00 (1)	81.81 (6)	31.42 (7)	0.00 (1)	46.66 (2)	6.55 (5)
Sagem CBM	Optical	36.10 (3)	81.94 (5)	79.71 (5)	1.33 (2)	1.28 (5)	50.76 (3)	1.58 (3)
Identix	Optical	38.13 (5)	69.33 (3)	98.48 (10)	2.66 (3)	0.00 (1)	58.33 (4)	0.00 (1)
Sagem MSO	Optical	39.08 (4)	100.00 (8)	21.79 (2)	50.00 (9)	0.00 (1)	62.66 (5)	0.00 (1)
UPEK	Capacitive	45.04 (6)	NA (9)	67.24 (3)	36.00 (8)	40.90 (9)	91.66 (8)	34.42 (8)
SecuGen	Optical	45.34 (7)	81.94 (6)	94.80 (8)	0.00 (1)	1.28 (5)	75.00 (7)	19.04 (6)
Authentec	Radio frequency	52.08 (8)	NA (9)	71.42 (4)	18.91 (5)	45.56 (10)	98.24 (10)	78.33 (10)
Cross Match	Optical	63.00 (9)	74.32 (4)	95.23 (9)	100.00 (10)	8.97 (7)	69.33 (6)	30.15 (7)
TesTech	Electro-optical	64.50 (10)	91.66 (7)	86.36 (7)	30.55 (6)	25.97 (8)	93.84 (9)	58.62 (9)

Results are FRR rates (%) at an FAR of 0.01% (1 in 10,000). Performance ranks are in parentheses. September 2008
Water results for some sensors are marked NA (not available) because those sensors do not work in water.

Os testes foram conduzidos no laboratório da própria Lumidgm com uma amostra de aproximadamente 25 pessoas, mostram respectivamente o resultado após 1 e 3 tentativas de autenticação por pessoa. É possível notar de forma clara a diferença de desempenho, evidenciando o benefício da tecnologia.

Sugerimos mais à frente um protocolo de teste que permite a execução de teste similar para o processo de qualificação das propostas de urna eletrônica.

Capacidade de discriminação de dedos falsos (PAD – detecção de ataques de apresentação)

A possibilidade do uso de uma biometria forjada em um leitor biométrico abre porta para diversos ataques, que podem comprometer não só a segurança da urna eletrônica e a inviolabilidade do voto, mas toda a imagem do processo de votação, ainda que os ataques tenham limitação de escalabilidade.

A aplicação de leitura multiespectral de impressões digitais é a mitigação mais eficaz para este risco, funcionando como um seguro contra futuras ameaças à segurança e à imagem da urna.

Capacidade de leitura de imagens além da impressão digital (voto em trânsito)

Sensores multiespectrais fazem a captura de toda e qualquer imagem presente na região próxima a lente ou prisma de captura. Isto permite que, de forma disruptiva, imagens de códigos de barras 2D (tipo QR code) sejam lidos e processados pelo sensor, quando programado para tal.

Uma aplicação desta capacidade hipotética, já experimentada em laboratório, é a leitura do *template* do eleitor a partir de um QR code gerado e apresentado na tela de um celular, de forma totalmente off-line. Após a leitura do QR code, o sensor descodifica o *template* do eleitor, pede que este apresente sua biometria e confirma sua identidade, realizando o voto de forma segura.

***(capacidade potencial do sensor, sujeita a configuração de software especial).**

Sobre a classificação de sensores do FBI e padrão PIV

O FBI, de forma a orientar a adoção de leitores de impressão digital de forma clara, classifica dispositivos pelo tamanho de sua área de captura. Sensores de captura da impressão digital para captura de apenas um dedo podem se enquadrar em uma de três categorias: FAP 10, FAP 20 e FAP 30, onde quanto maior o FAP maior a área de captura. Embora a certificações PIV não se aplique totalmente a sensores multiespectrais, estes apresentam áreas similares, conforme a tabela abaixo:

		Sensor FAP 30	Sensor Multiespectral Linha V	Sensor FAP 20	Sensor Multiespectral Linha M	Senso FAP 10
Área de Captura	Cm	2,54 X 2,03	2,79 x 1,77	2,03 X 1,52	1,74 x 1,39	1,65 X 1,27
	Pol.	1,0” X 0,8”	1,1” X 0,7”	0,8” X 0.6”	0,68” X 0,55”	0,65” x 0,5”

Já o padrão FIPS 201-PIV apresenta uma série de definições para equipamentos de Verificação de Identidade Pessoal, dentre os quais alguns voltados para sensores biométricos e, mais especificamente, para garantir a interoperabilidade entre equipamentos de diferentes fornecedores. Esta interoperabilidade, no entanto, é garantida apenas de forma implícita, dentro do entendimento razoável de que se uma impressão digital foi capturada numa determinada proporção de tamanho, ela pode ser comparada com outra nas mesmas condições. É a ÚNICA classe de especificações que não exige que o equipamento seja fisicamente enviado ao NIST para certificação, sendo requisitadas apenas as imagens produzidas pelo sensor. Assim, não existe nenhuma relação direta entre a certificação e o produto especifico fornecido.

O que de fato acontece é que tal certificado, embora relevante, não garante de fato uma boa coleta, mas apenas que se o sensor conseguiu coletar uma impressão digital, ela terá a proporção esperada.

No mais, pelas suas características de funcionamento, não é possível tecnicamente aplicar o processo de certificação PIV ao processo multiespectral, pois para obter a imagem final da digital o sensor multiespectral combina 12 imagens diferentes, um processamento vedado pelas regras do PIV. No mais, todas as regras e dimensões dos sensores PIV são respeitadas pelos sensores multiespectrais, de forma a garantir interoperabilidade (conforme atestada por diversos casos de uso e testes apresentados neste documento).

SUGESTÕES ADICIONAIS PARA O EDITAL

Nas seções a seguir, apresentamos sugestões de alterações para o Termo de Referência da UE2020, sempre precedidas pelas razões técnicas que as justificam.

Sugestão 1 – área de captura para sensores multiespectrais

Das razões para a mudança

Entendemos que a exigência na urna de sensores com áreas de captura maior, como FAP 30 ou até 40, reflete a preocupação do TSE em aumentar a performance da autenticação, de forma a evitar falhas de reconhecimento, decisão que encontra amplo amparo na literatura acadêmica relacionada ao assunto.

Os estudos conhecidos mostram claramente que existe um relevante e considerável ganho de performance entre imagens geradas em um sensor de área FAP 10 contra um de área FAP 20.

NO ENTANTO.

Os ganhos que se observam entre sensores de área FAP 20, comparados com os de área FAP 30 são muito mais modestos, como pode-se observar no gráfico a seguir.

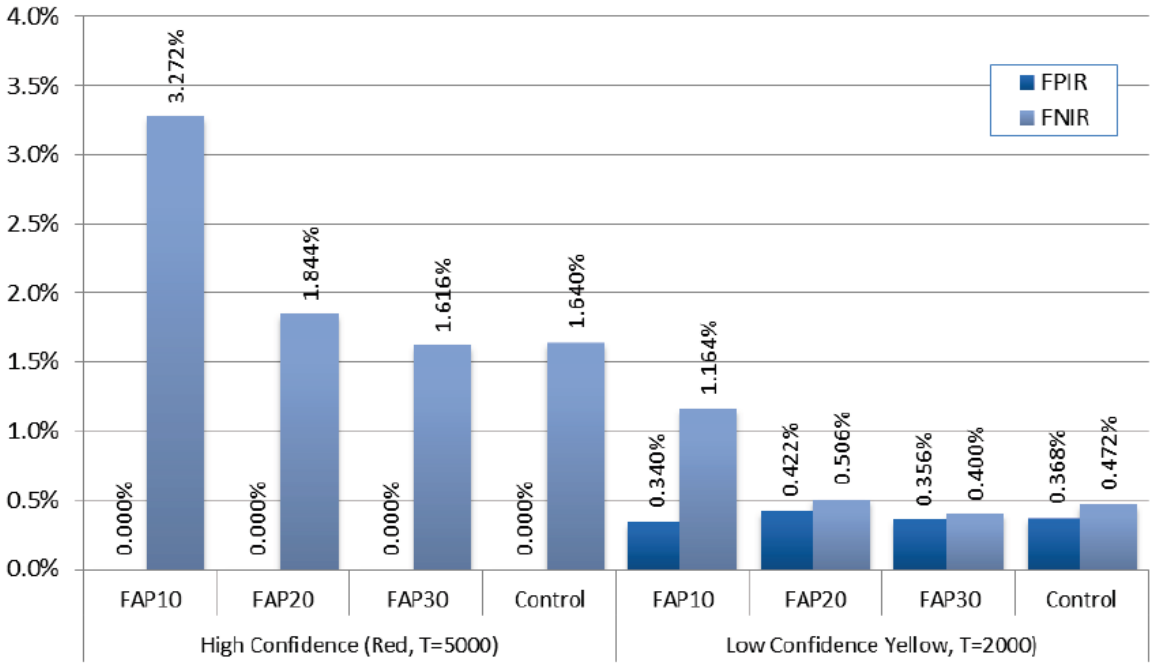
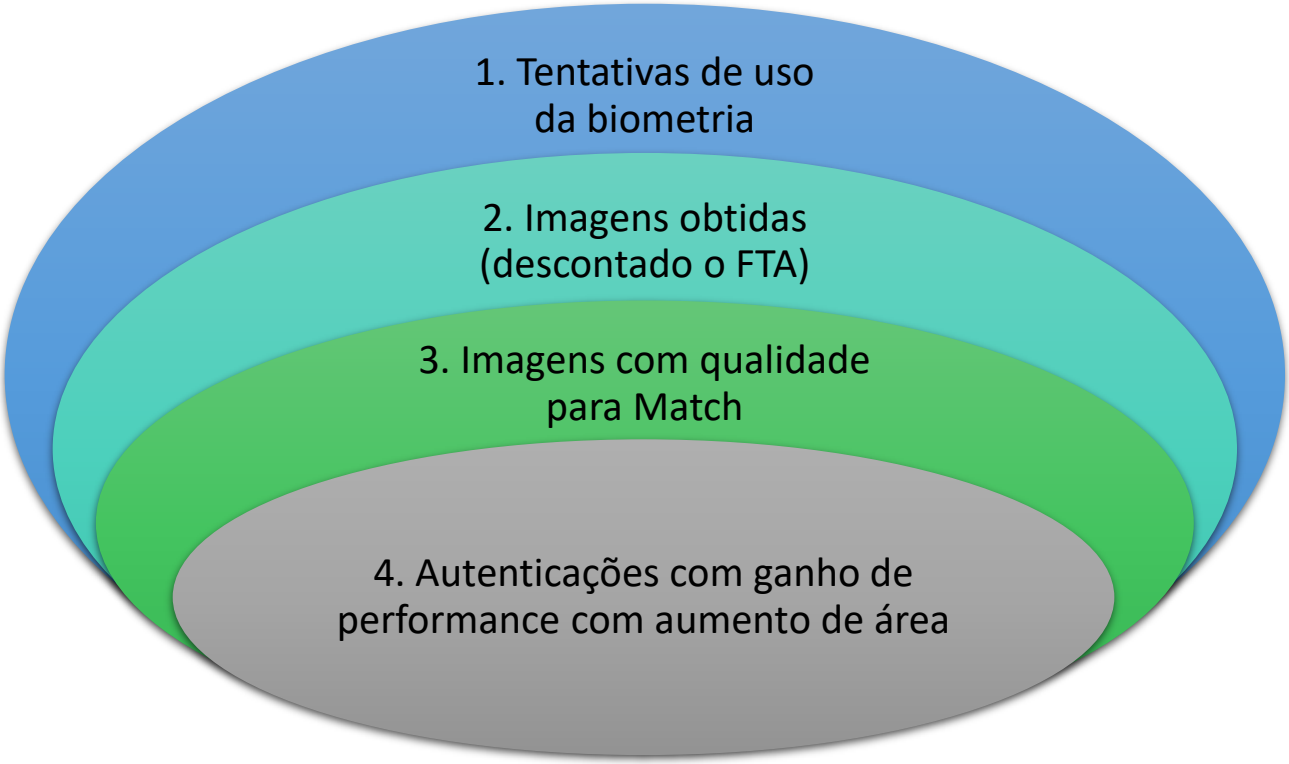


Figura – Comparativo do resultado do Matcher de acordo com a área da captura da imagem do estudo NIST.IR.7950 (ORANDI, S. 2014)

Mais importante, os estudos que tratam do tema, como o NIST.IR.7950 (ORANDI, et al., 2014), não levam em consideração dois outros aspectos fundamentais, de grande importância e relevância na usabilidade e experiência do usuário: a Taxa de Erro de Aquisição (FTA), que representa a quantidade de vezes em o sensor não conseguiu sequer obter uma impressão digital de uma pessoa, e a qualidade da imagem obtida.

Estes dois aspectos estão diretamente ligados entre si, e intimamente relacionados a tecnologia de captura empregada pelo sensor. São vários os fatores que podem levar um sensor a apresentar uma falha de aquisição ou que, quando não causam uma falha de aquisição, fazem com que o sensor obtenha uma imagem de qualidade ruim. Dependendo da tecnologia de captura, vários são os fatores relacionados a falhas de aquisição, como por exemplo:

- Umidade do ar muito baixa (deixando a pele seca) ou muito alta (deixando pele e prisma de leitores úmidos e demasia)
- Iluminação ambiente excessiva
- Condições especificas de pele (secura, oleosidade, umidade, consistência)
- Presença de sujeira, protetor solar, pomadas e afins nas pontas dos dedos



A figura acima ilustra (desconsiderando proporcionalidade) o tema: a área 1 representa todas as pessoas que irão tentar se autenticar em uma urna. Este ponto, inclusive, é onde se concentra a primeira questão de perda de tempo para autenticação. Dependendo das condições do usuário, do ambiente e da tecnologia, o usuário eleitor tem que despender considerável esforço para conseguir que sua digital seja capturada. A área 2 representa então a quantidades de imagens obtidas após este esforço inicial. A área 3 traz a próxima questão relevante: dentre as imagens obtidas, apenas uma parte realmente apresentará qualidade suficiente para que seja feito o reconhecimento dos padrões de cristas, vales e minúcias. Por fim, a área 4 representa quantas das autenticações realmente se beneficiarão de uma área maior de captura.

Assim, o que se pretende concluir aqui é que, embora a área seja um fator importante no processo de autenticação de impressões digitais, outros fatores contribuem

consideravelmente para uma melhor performance, e devem ser igualmente observados e pesados.

Acima destas considerações, cabe acrescentar que sensores de área de captura menor tem custos muito menores, em especial quando se considera o emprego de tecnologia multiespectral. Considerando o volume de 180 mil unidades, é possível estimar uma economia de vários milhões de dólares, apenas pela adoção de uma área de captura menor, sem que isso represente abrir mão de um avanço na performance de biometria de autenticação na urna.

Proposta de mudança

Sugerimos que para sensores multiespectrais além da a área mínima de captura de 2,794 x 1,77 centímetros (ou 1,1 x 0,7 polegadas), com contabilização de 10 pontos seja aberta uma opção mais econômica com área 1,74 x 1,39 centímetros (ou 0,68” X 0,55” polegadas).

Sugerimos para o item 182.2 do documento *Anexo II – Especificação Técnica - Hardware* a seguinte redação:

182.2. Caso multiespectral, a área de aquisição pode ter as medidas retangulares de, no mínimo, 0,68 polegadas no eixo vertical e, no mínimo, 0,55 polegadas no eixo horizontal ou, caso elíptica, com medidas do eixo maior com, no mínimo, 1,1 polegadas e eixo menor com, no mínimo, 0,7 polegadas;

Outras sugestões de mudança

Sugestões 2 - Criptografia

A criptografia é sem dúvida elemento crítico da segurança da urna e deve ser tomada no nível mais confiável possível. Assim, entendemos que existe espaço para uma melhor definição do que se entenderá por criptografia do tipo PRONTA (Dispositivo que implementa o canal seguro já integrado ao próprio leitor biométrico a partir de um projeto já existente e empregado em outros equipamentos também de maneira integrada).

Uma primeira medida é garantir que os algoritmos empregados na criptografia das informações foram implementados da forma correta. O NIST tem um programa gratuito de certificação, onde qualquer interessado pode validar sua implementação. Uma vez inscrito, o interessado recebe um pacote de informações (criptografadas) que deve ser processado da maneira correta e então devolvido para o NIST para checagem. Caso esteja dentro dos padrões, o NIST certifica o algoritmo. Importante considerar que nenhum código fonte é compartilhado com o NIST ou o governo americano.
(https://csrc.nist.gov/projects/cryptographic-algorithm-validation-program)

Desta forma sugerimos a adição de itens pontuáveis conforme abaixo:

- Apresentar certificação da aderência dos algoritmos ao nível 2 da FIPS, tem seu algoritmo listado como aprovado no site do NIST.

Sugestão 3 - Detecção de ataques de apresentação (popular *Liveness*)

A detecção de ataques de apresentação está ligada diretamente a sensação de segurança da população. Ainda que um ataque deste tipo tenha um alcance uma aplicabilidade contida, um eventual ataque bem-sucedido (facilmente aplicável em sensores óticos e de eletroluminescência) e compartilhado em redes sociais pode minara imagem da urna e do processo de votação.

Desta forma sugerimos a adição, no documento Anexo I – Descrição de Produtos e Serviços – UE2020, sob item 45.5.1.b.4, do seguinte texto:

b.4) Apresentar funcionalidade de Detecção de Ataque de Apresentação que permita descriminar dedos reais de dedos sintéticos e que apresente, ao menos:

b.4.1) Relatório de teste de conformidade ISO 30107-3 realizado por laboratório credenciado (iBeta, Nist) mostrando resistência de 100% de acerto na detecção de ataques, pelo menos no nível 1 da norma OU

b.4.2) Sistema de Detecção de Ataque de Apresentação PAD, comprovado por apresentação de atestado de capacidade técnica
Pontuação: 10 pontos

Sugerimos também, alternativamente ao relatório, esta característica seja avaliada nos testes do modelo de qualificação, acrescentando seção ao documento *Anexo Ia – Testes Complementares para Avaliação Modelo de Engenharia* na seguinte forma:

D.5 – Teste de Detecção de ataque de apresentação

146. (N>5) voluntários se cadastraram previamente e se autenticaram três vezes com sucesso para garantir seu efetivo cadastro.

147. Na sequência ataques de apresentação (PAs) com réplicas sintéticas dos dedos dos voluntários (de cola, papel e silicone, por exemplo) são tentados por cinco vezes cada.

148. A cada tentativa realizada, o aplicativo fornece um índice de qualidade de impressões digitais, uma pontuação de atividade e uma pontuação de correspondência (match), além da exibição em tempo real da imagem obtida.

149. Durante e/ou no final do teste, os voluntários retornaram e se autenticam mais vezes com sucesso para verificar que o aplicativo de reconhecimento de impressões digitais continua capaz de reconhece-los.

150. O fornecedor pode indicar um dos voluntários e intervir por uma única vez para orientação do uso e posicionamento do dedo, podendo também apontar eventual desvio evidente do posicionamento do dedo (sendo aquela tentativa descartada do teste).

Sugestão 4 – Avaliar Usabilidade vs. Interferência de condições adversas (umidade, sujeira, etc.)

Entendemos, dentre todas as questões apresentadas, que a usabilidade, em especial frente a condições adversas, é uma das questões mais críticas e com maior impacto para a experiência do voto e qualidade do processo de votação. Conforme pode ser observado na tabela da página 11, a diferença entre tecnologias em situações mais adversas é fator preponderante na usabilidade da biometria.

Sugerimos que capturas em condições adversas, que podem ser fator com grande impacto no atendimento ao cidadão, sejam avaliadas e pontuadas, acrescentando seção ao documento *Anexo Ia – Testes Complementares para Avaliação Modelo de Engenharia* , roteiro de teste na seguinte forma:

D.6 – Teste de Detecção de ataque de apresentação

151. (N>20) voluntários se cadastraram previamente através de uma tentativa com o sensor em condições normais.

152. Os voluntários realizam, de forma revezada, 3 tentativas de autenticação sem nenhum elemento de interferência no sensor.

153. Um elemento de interferência (como água borrifada, loção hidratante e protetor solar, maquiagem) é introduzido de forma moderada sobre o sensor e novas rodadas de tentativas de autenticação, são feitas por três vezes de forma revezada, entre os voluntários.

154. Para cada um dos elementos de interferência é realizada uma rodada de tentativas de autenticação, seguidas então por uma rodada em que usuários irão fazer forte pressão sobre o sensor, e depois uma rodada pousando o dedo levemente sobre o sensor.

155. Caso o sensor não apresente mudanças significativas de tempo na captura, e não seja observada Falhas de Aquisição (FTA, quando o leitor simplesmente não consegue sequer obter uma imagem da digital) ou Autenticação (FRR), a urna poderia auferir pontuação de qualidade de 20 pontos.

Sugerimos também a apresentação de atestado de capacidade técnica que demonstre a que os leitores foram aplicados com sucesso (>= 98%) em processo de autenticação de usuários, com as seguintes características:

a) uso "não assistido", isto é, que ocorre sem assistência/supervisão de terceiros;

b) podem eventualmente se encontrar em áreas expostas e abertas, sujeito as diversas condições de umidade e luminosidade presentes no território nacional;

c) os leitores podem eventualmente estar expostos ao público de forma constante, sujeito as diversas condições de uso adversas impostas por usuários;

d) os leitores não recebem nenhum procedimento de limpeza especial;

e) seu uso é inclusivo, e não diferencia clientes do banco por etnia, idade ou qualquer outra variável;

Sugestão 5 - Leitura Superficial vs. de Subcamadas

A capacidade de leitura de camadas da impressão digital além da camada externa está diretamente ligada a capacidade de leitura em situações adversas e discriminação de “dedos falsos” (PAD).

Sugerimos requisitar esta capacidade do leitor, oferecendo 10 pontos por esta capacidade.

Esta capacidade pode facilmente ser averiguada com um teste simples na presença de um plástico transparente, ou mesmo uma luva cirúrgica: sensores multiespectrais podem obter uma impressão digital através de uma camada destes materiais sem dificuldade.

REFERENCIAS TÉCNICAS

CAMPBELL, J. ; MADDEN, M. J.. **ILO Seafarers' Identity Documents**

Biometric Interoperability Test (ISBIT-4) Report. INTERNATIONAL LABOUR OFFICE (ILO). Janeiro de 2009. Acessado em 2019 em: https://www.ilo.org/global/standards/subjects-covered-by-international-labour-standards/seafarers/WCMS_191708/lang--en/index.htm

BONDA, K.; FAKOURFAR, H.. "**Performance of Fingerprint Recognition System in Maritime Environment.**" 2009. https://docplayer.net/21649987-Abstract-1-introduction-1-1-methodology.html

KRISHNASAMY, P.; BELONGIE, S.; KRIEGMAN, D.. "**Wet Fingerprint Recognition: Challenges and Opportunities**". 2011. IEEE / University of California, San Diego.

ORANDI, S. et al.. **NIST.IR.7950 - Examination of the Impact of Fingerprint Spatial Area Loss on Matcher Performance in Various Mobile Identification Scenarios.** Março de 2014. NIST. http://dx.doi.org/10.6028/NIST.IR.7950

ROWE, R.K.; NIXON, K.A.; BUTLER, P.W.. **Multispectral fingerprint image acquisition,** in Advances in Biometrics: Sensors, Algorithms and Systems, Springer, London, páginas. 3–24, 2007.

ROWE R.K. et al.. **Robust Fingerprint Acquisition: A Comparative Performance Study,** in Proc. SPIE Conf. on Biometric Technology for Human Identification IV, 2007a.

ROWE, R. K.; NIXON, K. A.. **Fingerprint Enhancement Using a Multispectral Sensor** , in Proc. SPIE Conf. on Biometric Technology for Human Identification II, Vol. 5779, 2005.

Editais de referência

Edital Banco do Brasil: **PREGÃO ELETRÔNICO Nº 2016/06675 (7421)**, DISEC/CESUP LICITAÇÕES SÃO PAULO

Edital Caixa Econômica Federal: **PREGÃO ELETRÔNICO Nº 009/5307-2018**, GECOT