Universidade do Minho
Escola de Engenharia

Tecnologias Biométricas: aplicação no Controlo de Acesso a Sistemas de Informação

Sumário pormenorizado da lição de síntese

Prova de Agregação no ramo de conhecimento de

Tecnologias e Sistemas de Informação

submetida à

Universidade do Minho

por

Henrique Manuel Dinis dos Santos

Maio de 2013

Conteúdo

Índice de figuras

1. Introdução

A lição cujo sumário pormenorizado é apresentado neste relatório intitula-se "Tecnologias Biométricas: aplicação no Controlo de Acesso a Sistemas de Informação". A lição enquadra-se num módulo de ensino subordinado ao tema "Controlo de Acesso e Autenticação", a lecionar no âmbito da Unidade Curricular UC "Engenharia da Segurança dos Sistemas de Informação", de carácter opcional, que integra o plano de estudos de diversos cursos de pós-graduação, no âmbito das Tecnologias de Sistemas de Informação (TSI), integrados na oferta formativa do Departamento de Sistemas de Informação, da Universidade do Minho[1].

A UC é apresentada de forma mais detalhada no relatório intitulado "Engenharia da Segurança dos Sistemas de Informação: Relatório da Unidade Curricular", onde estão sintetizados os aspectos científicos, pedagógicos e profissionais, fundamentais da área e que, juntamente com este relatório, constitui um requisito exigido aos candidatos ao título de Agregado.

Para além do sumário pormenorizado da lição, este relatório inclui o seu enquadramento na UC e no módulo de ensino em que se insere e ainda uma descrição dos seus objectivos específicos e o conteúdo.

2. Enquadramento da lição

Nesta secção é descrito o enquadramento da lição, quer ao nível da UC, quer ao nível do módulo de ensino. Esse enquadramento é relevante uma vez que a natureza e as características funcionais da UC limitam, naturalmente, as decisões relativas aos objetivos, conteúdos e até mesmo métodos de avaliação a utilizar. O enquadramento é feito a dois níveis por forma a realçar devidamente esses condicionalismos.

2.1. A UC de Engenharia da Segurança dos Sistemas de Informação

A UC Engenharia da Segurança de Sistemas de Informação tem carácter opcional e integra o plano de estudos de diversos cursos de pós-graduação, tal como referido em (Santos 2013). A UC encontra-se instanciada no 2º semestre do plano dos cursos de Mestrado em Engenharia e Gestão de Sistemas de Informação (MEGSI)[2], Mestrado em Sistemas de Informação (MSI) e Mestrado em Serviços de Informação (MServInf). O regime de escolaridade prevê 3 horas de

[1] A oferta formativa em TSI está sintetizada em TSI@UMINHO (http://tsiuminho.dsi.uminho.pt/home)

[2] Aquando da realização deste relatório decorria o processo de transição da Licenciatura em Tecnologias e Sistemas de Informação (LTSI) para o Mestrado Integrado em Engenharia e Gestão de Sistemas de Informação (MIEGSI). Desse processo resultará a fusão do MEGSI no MIEGSI. No que respeita à UC descrita neste relatório essa transformação não teve qualquer impacto, para além da alteração da designação do curso, uma vez que continua com o mesmo enquadramento, quer temporal quer programático.

contacto semanal (um total de 45 horas no semestre), que tipicamente são distribuídas por um período teórico de 1 hora e um período teórico-prático de 2h. Os objetivos gerais desta UC são:

- Desenvolver o conhecimento essencial sobre diversas tecnologias de segurança da informação, assim como as respetivas competências técnicas necessárias à sua correta implementação, o que no conjunto é fundamental para permitir um envolvimento consciente e efetivo na elaboração e implementação de um processo de Gestão da Segurança da Informação; e
- Alertar os alunos para as questões relacionadas com a temática da Segurança da Informação no contexto atual do "Ciberespaço".

Estes objetivos têm natureza complementar, procurando fomentar o conhecimento e a respectiva experiência prática, para cada tópico. Esta complementaridade é considerada essencial dada a natureza dos saberes envolvidos. De uma forma mais específica, os resultados de aprendizagem (RA) desta UC estão indicados na Listagem 1

Na perspetiva das competências de natureza mais prática é evidente a enfâse colocada na componente de segurança em redes. Esta opção não pretende valorizar a componente tecnológica da Segurança da Informação, face às questões de âmbito organizacional e de gestão. No entanto, recorda-se aqui que esta UC pode ser (e desejavelmente será) antecedida de uma outra UC, também opcional, com enfoque nesses aspetos. Esse facto justificou uma orientação mais objetiva para os RA definidos nesta UC.

a) Reconhecer a importância de uma cultura de segurança relativamente à utilização dos Sistemas de Informação.
b) Conhecer os aspectos técnicos das Tecnologias de Informação e Comunicações (TIC) e que mais as expõem a riscos de segurança.
c) Reconhecer as principais ameaças e a forma típica como os ataques são efectuados.
d) Analisar vulnerabilidades em Sistemas de Informação.
e) Planear uma estratégia de segurança para um Sistema de Informação baseada num modelo de gestão do risco (ênfase nas redes de computadores).
f) Implementar e controlar tecnologias de segurança, no contexto de uma política de segurança para Sistemas de Informação.
g) Utilizar ferramentas de auditoria e análise da segurança em computadores e redes
h) Reconhecer o papel das normas na Segurança da Informação e em particular o da família de normas ISO/IEC 27000.

Listagem 1 - Resultados de aprendizagem para a UC ESSI

Não existe um mapeamento direto entre os objetivos, ou os RA, e os diversos módulos lecionados na UC – ver detalhes em (Santos 2013). Com efeito, e exceptuando parcialmente os dois primeiros RA, a maioria dos módulos estão orientados às tecnologias de segurança e promovem, para cada módulo, um subconjunto dos RA, com ênfase no conhecimento fundamental e na utilização prática da tecnologia, assim como na sua integração em políticas de segurança. Esta organização é patente na estrutura curricular que, a partir da terceira semana e ao longo de 11 semanas, tipicamente dedica duas ou três semanas a cada uma das

tecnologias em estudo. No contexto deste relatório, a lição apresentada debruça-se sobre as tecnologias biométricas e corresponde à segunda parte do módulo dedicado ao estudo das tecnologias de Controlo de Acesso, onde o enfoque são as técnicas de autenticação dos utilizadores.

2.2.O módulo Controlo de Acesso e Autenticação

De acordo com o plano apresentado em (Santos 2013), a leccionação do módulo Controlo de Acesso e Autenticação ocorre nas semanas 6 e 7 da UC. Este módulo estrutura-se de forma a promover essencialmente os RA a), e) e f) (ver Listagem 1), naturalmente no âmbito do controlo de acesso. Com efeito, após a frequência deste módulo, os alunos deverão ser capazes de reconhecer a importância do controlo de acessos, construir um modelo de suporte e escolher as melhores tecnologias para a sua implementação, dando especial atenção à problemática da autenticação dos utilizadores, onde as tecnologias biométricas serão alvo de uma abordagem dedicada e mais detalhada.

Os conteúdos a abordar neste módulo encontram-se sintetizados na Listagem 2. A primeira parte introduz os fundamentos do Controlo de Acesso, realçando as três funções básicas – Autorização, Autenticação e Auditoria. São ainda apresentados e discutidos diversos modelos e protocolos. Na segunda parte é abordada a questão da autenticação, inicialmente numa perspetiva da autenticação entre máquinas, apresentando e discutindo as principais técnicas, bem como as suas vantagens e limitações. Na última parte é discutida a problemática da autenticação dos utilizadores, discutindo as diversas alternativas e analisando em mais detalhe aspetos funcionais e não funcionais das tecnologias biométricas, o que será naturalmente mais detalhado no capítulo seguinte deste relatório.

1. Controlo de Acesso
   - 1.1. Fundamentos do Controlo de Acesso
   - 1.2. Modelos e protocolos
2. Autenticação
   - 2.1. Autenticação por *keyword*
   - 2.2. Autenticação baseada no endereço
   - 2.3. Autenticação baseada em criptografia
3. Autenticação dos utilizadores
   - 3.1. *Passwords* em maior detalhe
   - 3.2. *Tokens* em maior detalhe
   - 3.3. Biometria em maior detalhe

Listagem 2 - Conteúdos programáticos do módulo Controlo de Acesso e Autenticação

Como suporte bibliográfico fundamental a estes conteúdos, são indicados os documentos que constam na Listagem 3. Como preparação para o módulo é solicitada aos alunos a leitura das referências 2, 4, 6 e 10 – ver Listagem 3. Para além desta lista bibliográfica são ainda fornecidos apontadores para alguns *sites* com informação relevante, nomeadamente:

- Biometrics Research Homepage at MSU (http://biometrics.cse.msu.edu/index.html)
- The Biometric Consortium (http://www.biometrics.org/index.htm)

- NIST Biometrical Portal (http://www.nist.gov/biometrics-portal.cfm)

1. Kaufman, C., Perlman, R. and Speciner, M. *Network Security: Private Communication in a Public World*. Prentice Hall PTR, Upper Saddle River, NJ 07458, 2002. (cap. 9)
2. **Jain, A. K., Ross, A. and Prabhakar, S., *An introduction to biometric recognition*, Circuits and Systems for Video Technology, IEEE Transactions on, 14, 1, 4-20, 2004.**
3. Bishop, M., *Introduction to Computer Security*, Prentice Hall PTR, 2004. (cap. 3 a 7).
4. **Sandhu, R. S. and P. Samarati, *Access control: Principles and practice*. IEEE Communications Magazine 32(9): 40-49, 1994**
5. Sandhu, R. S., E. J. Coyne, et al., *Role based access control models*. Computer 29(2): 38-47, 1996.
6. **Dunstone, T. and Yager, N., *Biometric System and Data Analysis: design, evaluation and data mining*, Springer, 2010**.
7. Maltoni, D. et. all, *Biometric Systems: Technology, Design and Performance Evaluation*, Springer, 2005
8. Jain, A. K., *Biometrics: Personal Identification in Networked Society*, Kluwer Academic Publishers, 1999
9. Delac, K. and Grgic, M., *A survey of biometric recognition methods*. 46th International Symposium Electronics in Marine, ELMAR-2004.
10. **Magalhães, P. S., *Estudo dos padrões de digitação e sua aplicação na autenticação biométrica*, Master Thesis, Departamento de Sistemas de Informação, Universidade do Minho, 2005**.
11. Rashed, A. and Santos, H., *Multimodal Biometrics and Multilayered IDM for Secure Authentication*, in Global Security, Safety, and Sustainability. vol. 92, S. Tenreiro de Magalhães, et al., Eds., ed: Springer Berlin Heidelberg, pp. 87-95, 2010.
12. Strebe, M., *Network Security Foundations: Technology Fundamentals for IT Success*, Sybex, 2004. (cap. 3)

Listagem 3 - Bibliografia indicada para o módulo

As duas sessões previstas para a leccionação deste módulo incluem as seguintes atividades:

- Exposição (na primeira sessão) dos fundamentos do Controlo de Acesso, acompanhado com alguns exemplos práticos que ilustram a aplicação do modelo Bell-LaPadula e Clark-Wilson e a sua exploração em ambientes reais.
- Elaboração de um trabalho prático em grupo sobre a aplicação de um modelo de Controlo de Acesso; este trabalho tem um tempo de realização previsto de oito horas, quatro das quais correspondem a trabalho autónomo; o trabalho é entregue antes da segunda sessão, sendo aí discutido em grupo.
- Exposição (na segunda sessão) dos conceitos fundamentais das biometrias, realçando as suas virtudes, bem como os problemas de avaliação, tecnológicos e de aceitação; a discussão em aula é promovida com a apresentação de casos de estudo da implementação de tecnologias biométricas ilustrando a possível preparação de ensaios sobre o tema (este é considerado um tópico com excelentes condições para preparação do ensaio final usado na avaliação da UC).

3. Descrição da lição

A lição aqui descrita corresponde então à segunda sessão do módulo "Controlo de Acessos e Autenticação", sumariamente apresentado na secção anterior. Esta segunda sessão compreende um período de cerca de duas horas de aula, abrangendo, para além da exposição dos fundamentos, as atividades complementares de discussão e interação com os alunos, assim como a discussão do trabalho prático para avaliação deste módulo. Por esse motivo, esta lição não segue exatamente o mesmo alinhamento da aula real, atendendo à diferença do contexto das provas de agregação, procurando aqui focar os mesmos assuntos, mas aprofundando alguns aspetos fundamentais e de interdisciplinaridade.

Nesta lição serão abordadas as tecnologias biométricas e a sua utilização como mecanismo de autenticação, no contexto do Controlo de Acesso. Os objetivos específicos da lição são os seguintes:

- Reconhecer as aplicações gerais das tecnologias biométricas, assim como as propriedades fundamentais de uma biometria
- Compreender as vantagens de uma taxinomia multidimensional para biometrias
- Descrever a arquitetura típica de um sistema biométrico, assim como as funções e modo de operação de cada um dos seus componentes
- Parametrizar a função de decisão de um sistema biométrico em função da precisão desejada
- Compreender a problemática da avaliação do desempenho de uma biometria
- Discutir a segurança de um sistema biométrico, nas suas diversas dimensões

Esta lista de objetivos é ambiciosa e alguns deles, para serem atingidos na sua plenitude, carecem de alguns pressupostos que, na prática, nem sempre estarão presentes. Por exemplo, a capacidade para parametrizar corretamente uma função de decisão obriga ao domínio de alguns modelos estatísticos. Sendo suposto que nesta fase da sua formação os alunos possuem esse conhecimento, a verdade revela que nem sempre isso se verifica. O mesmo acontece na discussão da segurança de um sistema biométrico, que exige algumas competências desenvolvidas noutros módulos desta UC. Mais uma vez, eventuais lacunas irão dificultar a progressão desejada dos alunos. De notar que esta reflexão é realizada com os alunos, sempre que tal se revela necessário, o que resulta num conjunto de recomendações específicas com o objetivo de ultrapassar aquelas limitações.

Do ponto de vista do sumário, esta lição é estruturada segundo os tópicos apresentados na Listagem 4. A apresentação da lição será feita com o recurso a um conjunto de *slides* desenvolvidos com o PowerPoint.

- Introdução às biometrias
- Características biológicas, propriedades e requisitos das biometrias
- Exemplos de biometrias (estabelecidas e em investigação)
- Taxonomia multidimensional
- Sistemas biométricos
    - Arquitetura típica de um sistema biométrico
    - Modos de operação
    - Funções de similaridade
- Precisão e avaliação
    - Tipos de avaliação
    - Instrumentos de avaliação do desempenho
- Escalabilidade e segurança
- Exemplos de aplicação

Listagem 4 - Sumário da lição

4. Sumário pormenorizado

Mais de um século decorreu desde a proposta de Alphonse Bertillon para um sistema de identificação baseado na medição de algumas características do corpo humano. O objetivo era a caracterização e identificação de criminosos, mas efetivamente Bertillon criou o primeiro laboratório de antropometria e o processo de registo de identificação que ficou conhecido como o sistema de Bertillon[3]. A evolução desse conceito rapidamente revelou a necessidade de utilizar características mais eficazes (o sistema original baseava-se apenas em medidas das dimensões físicas do corpo humano), emergindo a impressão digital como uma solução promissora. Um pouco por todo o mundo diversas agências governamentais promoveram estudos científicos e o desenvolvimento de métodos mais eficazes para capturar, processar, registar e comparar impressões digitais. No entanto, apenas na segunda metade do século XX apareceu o primeiro AFIS (*Automatic Fingerprint Identification System*), orientado para a identificação no âmbito da investigação criminal (Maltoni, Maio et al. 2009). Outras técnicas mereceram uma elevada atenção, com particular realce para o reconhecimento facial, cuja facilidade de aplicação ficou definitivamente ligada à proliferação de dispositivos de captura de imagens. Hoje em dia estas técnicas são amplamente usadas em aeroportos pelos serviços de controlo de fronteiras, com base nos passaportes, o que promoveu ainda mais a sua investigação (Zhao, Chellappa et al. 2003).

Numa outra perspetiva, a evolução tecnológica, com o consequente aumento da dependência do ser humano relativamente aos meios de processamento e comunicação da informação, trouxe um conjunto de novos requisitos particularmente críticos, relacionados com o controlo

[3] Ver http://criminaljustice.state.ny.us/ojis/history/bert_sys.htm, visitado em Outubro, de 2012.

de acesso. Efetivamente, uma parte substancial das falhas de segurança informática ocorrem, direta ou indiretamente, de falhas de controlo de acesso, nomeadamente derivadas do uso inapropriado do método de autenticação mais divulgado, as palavras-chave (Richardson 2011).

Desde sempre o uso de palavras-chave foi considerado como um risco considerável para a segurança da informação, permitindo diversos tipos de ataques, desde ataques por "força bruta", passando por ataques por ludibriação dos utilizadores, até ataques que permitem contornar o mecanismo de autenticação (Neumann 1994). No entanto, o uso desta técnica de autenticação é simultaneamente considerado muito conveniente pela maioria dos utilizadores e, a menos de aplicações mais críticas, os utilizadores demonstram uma clara preferência pela sua utilização (Jones, Antón et al. 2007). Mas à medida que a sociedade vai aderindo a novos e variados serviços no âmbito da Internet, alguns envolvendo informação privada ou coletiva de elevado valor, os riscos vão aumentando, exigindo métodos de autenticação bastante mais eficazes (Vijayan 2012), (Matthews 2012) e (Jakobsson, Chow et al. 2012).

É neste contexto que as biometrias merecem uma atenção mais cuidada. O termo biometria deriva dos termos gregos *bio* (vida) e *metron* (medida), estando atualmente associado a uma classe de métodos e técnicas destinadas a utilizar representações digitais de características físicas ou comportamentais de utilizadores, com vista à sua identificação e/ou autenticação (Magalhães and Santos 2003). Apesar de diferentes no seu objetivo e nos processos associados, as funções de identificação e autenticação de seres humanos partilham alguns atributos que efetivamente são garantidos pela grande maioria das técnicas biométricas, muito embora algumas delas, pela sua natureza e forma de implementação, se adeqúem melhor a uma ou outra função – refira-se, no entanto, que a identificação, pela sua essência, carece sempre da utilização de algum tipo de biometria.

Ao longo das últimas décadas e à medida que a tecnologia foi evoluindo, permitindo o desenvolvimento de sensores mais precisos e mais baratos, as técnicas biométricas têm vindo a ser aplicadas a um leque considerável de características humanas, quer fisiológicas, quer comportamentais. Adicionalmente, diversas técnicas informáticas tem vindo a ser utilizadas no processamento biométrico, em especial no âmbito da verificação de padrões, conferindo a este domínio um estatuto próprio em termos de investigação e desenvolvimento (Jain, Ross et al. 2004).

4.1.Propriedades e características

A definição de biometria apresentada anteriormente, por si só, permitiria utilizar um leque bem alargado de características fisiológicas ou comportamentais dos seres humanos. No entanto, o objetivo da sua utilização (identificação e autenticação), bem como o universo dos utilizadores envolvidos, limitam esse espectro ao impor um conjunto de restrições, habitualmente referidas como propriedades fundamentais do universo dos utilizadores visados (Jain, Ross et al. 2004):

- Universalidade – a característica deve existir em todos os sujeitos;
- Diferenciação – quaisquer dois sujeitos devem poder ser distinguidos (particularmente importante na identificação, com menor relevância na autenticação);

- Continuidade – a característica deve ser suficientemente invariante durante um determinado período de tempo e no contexto de um determinado critério de comparação; e
- Mensurabilidade – a característica deve ser passível de processamento quantitativo, em tempo útil.

Para além destas propriedades fundamentais, um sistema biométrico prático e útil deverá ainda cumprir um conjunto de requisitos, incluindo:

- Desempenho – em particular relativamente à precisão, o tempo exigido no processamento e os recursos exigidos;
- Aceitação – qualquer tecnologia que se revela demasiadamente intrusiva será, naturalmente, rejeitada pelos utilizadores, o que dificultará ou mesmo impedirá, a sua implementação; e
- Resistência – na ótica das ameaças e ataques a que um sistema deste género estará exposto, é muito importante refletir, *a priori*, sobre a dificuldade em contornar o sistema usando métodos fraudulentos.

Diferentes sistemas biométricos satisfazem cada uma das propriedades atrás enunciadas em graus diferentes, existindo a necessidade de planear cuidadosamente o projeto biométrico, em função do cenário real, por forma a não comprometer o seu funcionamento. Por exemplo, supondo que se pretende implementar um projeto de identificação a nível nacional, será necessário escolher uma biometria que satisfaça, sobretudo, as propriedades da universalidade e da diferenciação – caso alguma delas não se verifique, por definição, não haverá a possibilidade de identificar alguns sujeitos, o que viola claramente o principal objetivo. Adicionalmente, na prática será necessário recolher vários milhões de biometrias, o que poderá exigir recursos e tempo consideráveis (ou mesmo proibitivos). Finalmente, mas não menos importante, a adição de novos utilizadores pode sempre criar novos problemas de precisão, que as avaliações prévias não permitiram prever. Em suma, o conjunto de dificuldades que se coloca a um projeto desta natureza, dada o seu factor de escala, transforma-o num desafio bastante complexo (Jarosz and Fondeur 2005). No contexto do exemplo referido é interessante estudar alguns casos de insucesso, como seja a tentativa de implementação de um cartão de identidade nacional no Reino Unido (Martin 2012) – onde os fatores de ordem pessoal (privacidade) se revelaram muito importantes - assim como alguns casos de sucesso, pelo menos parcial, como sejam os do Bangladesh, Malásia, Índia e Paquistão (Islam, Baniamin et al. 2012), (Reddy 2011) e (Ho and Eswaran 2011).

Mesmo com várias limitações, a lista de características fisiológicas e comportamentais que podem ser usadas em sistemas biométricos é bastante extensa. Uma questão óbvia que se pode colocar nesta altura é saber qual a melhor biometria, em função das propriedades fundamentais. Mas, ao trabalhar as diferentes dimensões e em diferentes contextos, rapidamente verificamos que tal desiderato está bastante longe de poder ser atingido, não havendo nenhuma biometria que satisfaça cabalmente todas as propriedades (Wayman, Jain et al. 2005) e (Hong, Yun et al. 2005).

Algumas das características biométricas, como sejam a impressão digital e o reconhecimento facial, foram já alvo de diversos estudos, encontrando-se numa fase de amadurecimento que

permite a sua utilização em aplicações reais. Mas outras, como seja a dinâmica de digitação em um teclado (*Keystroke Dynamics*), encontram-se ainda em um estágio de estudo e desenvolvimento. Na Listagem 5 é apresentada uma relação de características biométricas em ambas as fases de amadurecimento (Delac and Grgic 2004). Uma nota particular deve ser dada para o caso dos estudos que envolvem aplicações multidimensionais, que procuram ultrapassar algumas limitações dos sistemas biométricos isolados (como será discutido posteriormente), combinando duas ou mais biometrias. Embora em rigor não se trate de uma nova biometria, a análise é similar o que justifica a sua inclusão nesta lista (Cimato, Gamassi et al. 2006).

Convém detalhar ainda um aspeto dos sistemas biométricos multidimensionais, relacionado com o nível a que é feita a agregação da informação biométrica. Assim, ao nível mais baixo (da extração), os dados biométricos são diretamente agregados, gerando um novo padrão – o sistema tem que lidar apenas com um padrão, ficando mais simples, mas perde-se a possibilidade de valorizar mais ou menos cada uma das biometrias adquiridas. A um nível mais elevado (decisão) pode-se usar a informação resultante da verificação de cada uma das biometrias individualmente – neste caso apenas se tem em conta o resultado binário (aceita/rejeita) de cada uma das biometrias em questão. Num nível de maior detalhe (da comparação) pode-se usar o valor de verosimilhança de cada umas das biometrias individuais que possibilita uma decisão com mais informação embora, como é óbvio, com maior complexidade (Jain and Ross 2002).

Biometrias estabelecidas	**Biometrias em investigação**
• Voz • Termogramas infravermelhos: análise facial e padrão das veias da mão • Impressão digital • Geometria da mão • Assinatura • Face • Iris • Retina	• Dinâmica de Digitação *(Keystrokes dynamics*) • Locomoção • Odor • Orelha • Eletrocardiograma • DNA • Multidimensionais (*multimodal*)

Listagem 5 – Características biométricas estabelecidas e em investigação

4.2.Taxonomia

De uma simples análise das características biométricas, resulta com alguma naturalidade uma divisão em duas grandes classes: biometrias fisiológicas; e biometrias comportamentais. As primeiras estão associadas a característica de natureza fisiológica do individuo, como seja a impressão digital, as diferentes características dos olhos (retina e íris), a geometria da mão, a geometria dos vasos sanguíneos, diversas características da face, a forma das orelhas, o ADN, ou mesmo o odor. A grande maioria destas características permanece bastante estável no tempo, com a exceção da face que pode ser facilmente modificada (simples máscara). Já a segunda classe de biometrias depende fortemente de comportamentos apreendidos ao longo da vida e é condicionada por todos os fatores que influenciam a própria aprendizagem e a evolução. Inclui-se nesta classe a assinatura, a dinâmica de digitação, a forma de utilização do rato, a forma de caminhar e a voz – na verdade a voz apresenta características

comportamentais e fisiológicas, podendo estar numa ou noutra classe dependendo exatamente do que é medido (Jain, Ross et al. 2004).

Mas esta divisão em duas classes não evidencia alguns aspetos que podem ser importantes para algumas aplicações. Por exemplo, quando se estudam biometrias com algum foco na utilização, pode ser importante distinguir o modo como a biometria é aplicada: de modo furtivo, ou de modo colaborativo. Esta classificação reflete até que ponto o utilizador está intencionalmente envolvido no processo de verificação. Como é natural, as biometrias que operam em modo furtivo serão bastante mais toleradas pelo utilizador, sendo ainda mais resistentes às utilizações fraudulentas, pois o utilizador não sabe à partida, quando é que a captura e verificação são realizadas. Esta diferença pode ser fundamental para a aceitação de um sistema biométrico (Magalhães, Kenneth et al. 2008). A Figura 1 mostra um mapa com as principais técnicas biométricas já referidas, divididas pelos quadrantes definidos pelas duas dimensões de classificação descritas.

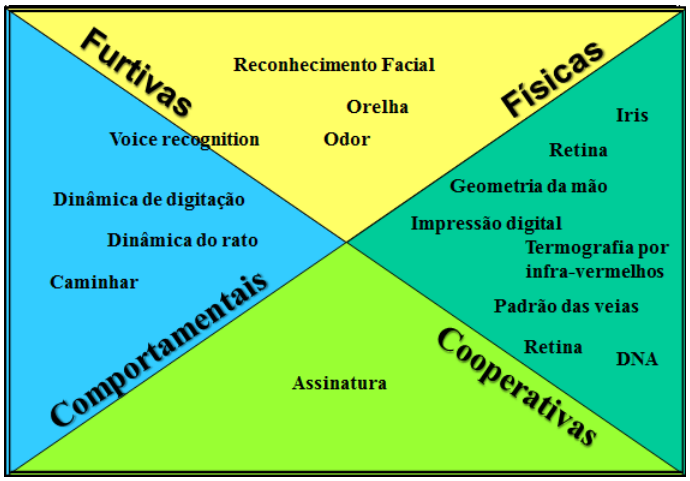


Figura 1 - Taxonomia para biometrias

Outras classificações são possíveis, procurando explorar outras perspectivas, ou simplesmente procurando detalhar mais as características específicas de uma dada classe. É o caso da taxonomia proposta por Yampolskiy, que detalha bastante mais as biometrias comportamentais, expondo aspetos como sejam a origem da interação – distinguindo as interações com os computadores, das interações com outros dispositivos/sistemas –, ou ainda a natureza do comportamento – motora, quando o comportamento a medir está associado a algum tipo de movimento muscular, ou não motora, no caso contrário (Yampolskiy and Govindaraju 2010).

4.3.Sistemas biométricos

Independente das características a serem medidas, um sistema biométrico pode ser visto como um sistema de reconhecimento de padrões, que opera sobre um conjunto de dados recolhidos de um ou mais indivíduos, confrontando-os com padrões previamente armazenados num repositório (Jain, Ross et al. 2004). Ao nível mais baixo encontramos muitas semelhanças com um sistema de processamento de sinal, com sinais a uma, duas ou três dimensões, eventualmente com mais do que um sinal em simultâneo, conforme a natureza dos sensores em causa (Wayman, Jain et al. 2005).

Dependendo da fase e do contexto de aplicação um sistema biométrico estará a operar em um de três modos: modo de registo (*enrollment*); modo de verificação; e modo de identificação (Jain, Ross et al. 2004). No primeiro modo procede-se à recolha, validação e armazenamento de um ou mais padrões associados a cada indivíduo (ver Figura 2). No modo de verificação, também designado por modo de reconhecimento positivo (ver Figura 3), o sistema irá capturar uma biometria, juntamente com algum tipo de identificação do indivíduo (nome de utilizador, por exemplo), a qual vai servir para selecionar um padrão da base de dados e que será comparado com o padrão capturado. O resultado será um determinado nível de verificação (*match*) que, em função de algum limite previamente estabelecido (*threshold*), irá determinar se a verificação tem sucesso ou não (ou seja, se o indivíduo foi ou não autenticado). No modo de identificação não existe a indexação prévia à base de dados (ver Figura 4), sendo o padrão recolhido comparado com todos os existentes na base dados. Dessas comparações resulta uma lista ordenada, com os padrões que mais se aproximam daquele que foi capturado. Normalmente é pré configurada a dimensão da lista e/ou o limite mínimo do resultado das comparações, para que cada padrão da base de dados possa ser considerado como uma potencial identificação.

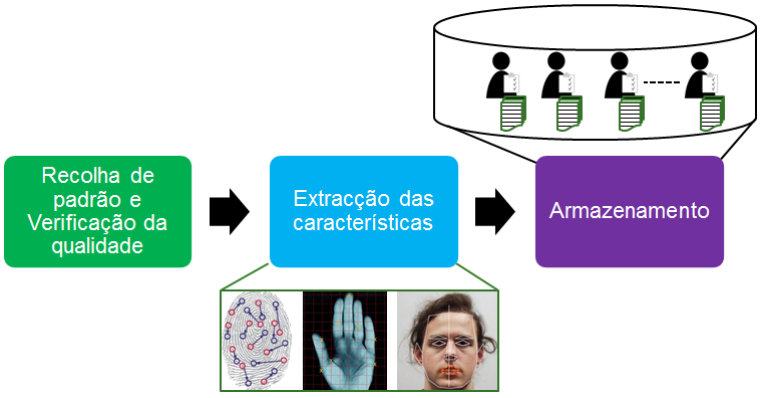


Figura 2 – Sistema biométrico no modo de registo (*enrollement*)

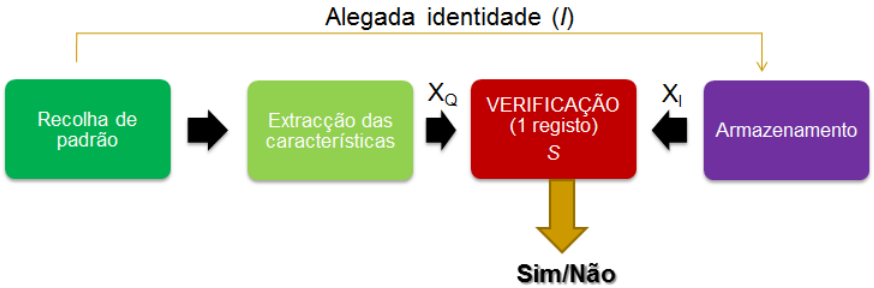


Figura 3 - Sistema biométrico no modo de verificação

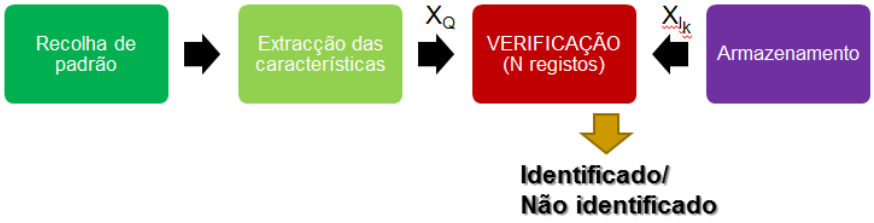


Figura 4 - Sistema biométrico no modo de identificação

A identificação é uma função crítica nas aplicações que fazem reconhecimento negativo (o indivíduo não indica a sua identidade), onde o objetivo é descobrir se um individuo efetivamente é quem ele nega ser – isto é, ele nega pertencer a um dado grupo, o que a identificação vai, ou não, validar. No entanto, também é possível usar a identificação em aplicações de reconhecimento positivo – por exemplo, para detetar se um individuo faz parte de uma lista de procurados, por exemplo. De notar que o reconhecimento positivo, à semelhança da autenticação, pode ser feito por diversas outras técnicas, mas o reconhecimento negativo apenas pode ser feito recorrendo a biometrias (Wayman 2001).

Independentemente do modo de funcionamento, um sistema biométrico deve compreender um conjunto de blocos essências. Um primeiro bloco que inclui o sensor biométrico, captura dados em bruto, estando tipicamente associado a algum tipo de algoritmo destinado a avaliar a qualidade intrínseca dos dados – particularmente crítico na fase de registo. Por exemplo, no caso de um AFIS, o sensor tem que ser capaz de recolher um número mínimo de pontos singulares de uma impressão digital, sem o qual não se considera dispor de um padrão biométrico útil – caso tal não aconteça, normalmente o indivíduo é solicitado a repetir o processo, mas um número limitado de vezes, findo o qual se considera ser impossível o registo (*Fail to Enroll* - FTE). No caso das biometrias que utilizam imagens digitais, o sensor é uma vulgar câmera de vídeo ou fotográfica e o processo de recolha partilha algoritmos com qualquer outra aplicação de processamento de imagem, nomeadamente para fazer a segmentação da imagem (e.g., delimitar a face numa imagem). Existe uma diversidade enorme de sensores desenvolvidos para dar resposta às necessidades das aplicações biométricas, mas por razões económicas ou devido à complexidade do processo de extração de padrões que permitam uma implementação eficiente de um sistema biométrico, a sua vulgarização está longe de ser conseguida (Ratha and Govindaraju 2008).

O bloco seguinte consiste na extração das características relevantes e a construção do padrão biométrico propriamente dito. O padrão obtido depende muito da técnica utilizada e da biometria em causa, sendo necessário estudar e avaliar cuidadosamente, para o conjunto de indivíduos alvo, as variáveis mais relevantes e que permitam atingir o máximo desempenho (Dunstone and Yager 2010). O domínio das variáveis a utilizar é consideravelmente elevado, existindo algumas técnicas no âmbito do reconhecimento de padrões que procuram identificar o conjunto mínimo de variáveis que são mais representativas das singularidades dos dados apresentados – apenas como exemplo dessas técnicas, refira-se a Análise Discriminante Linear (Ye and Ji 2010) e os filtros de Gabor (Krishna, Balasubramanian et al. 2010), ambos com resultados interessantes no reconhecimento facial, e *Rough Sets*, técnica utilizada com sucesso para determinar os casos particulares da dinâmica de digitação (Revett, Magalhães et al. 2005). De notar que o algoritmo usado nesta fase é determinante no sucesso da aplicação

biométrica, não sendo de estranhar que, frequentemente, os algoritmos utilizados sejam proprietários. Finalmente, neste bloco é também possível executar algum tipo de aferição sobre a qualidade do padrão obtido, podendo ocorrer uma rejeição e a consequente falha de aquisição (um eventual FTE, no caso da função de registo).

O terceiro bloco consiste essencialmente no algoritmo de verificação cuja finalidade depende da utilização. No caso da autenticação, assumindo que X_Q é o padrão a testar, I é o índice na base de dados e X_I o respetivo padrão armazenado, a decisão é binária (w_1 ou w_2), com base no valor (*score*) devolvido pela função de similaridade S e comparando-o com um dado limite t. O processo é descrito pela seguinte equação:

$$(I,\ X_Q) \in \begin{cases} w_1 & if\ S(X_Q, X_I) \geq t, \\ w_2 & otherwise, \end{cases}$$

Equação 1 - operação de decisão na Autenticação

Já no caso da identificação, assumindo novamente que X_Q é o padrão a testar, o resultado será a lista dos N padrões X_{I_K} extraídos da base de dados, que produzem o maior valor resultante da aplicação da função de similaridade S, desde que esse valor seja superior a um dado limite t. O processo é descrito pela seguinte equação (onde I_{n+1} representa o conjunto dos padrões que não geram resultados superiores ao limite t):

$$(X_Q) \in \begin{cases} I_K & if\ \max\limits_K \{S(X_Q, X_{I_K})\} \geq t,\ K = 1,2,\dots,N, \\ I_{N+1} & otherwise, \end{cases}$$

Equação 2 - Operação de decisão na Identificação

No caso da verificação é ainda possível não definir nenhum valor limite, extraindo-se, nesse caso, a lista dos N padrões que produzem o melhor resultado de comparação.

Como se pode observar, num caso ou no outro existem dois parâmetros críticos: a função de similaridade S e o limte t (*threshold*) – menos relevante, no caso da identificação. Seja por questões físicas, seja por questões comportamentais, a função $S(X_Q, X_I)$ irá produzir resultados diferentes fruto da variação (aleatória) dos padrões biométricos X_Q e X_I. Dessa forma, o limite t deverá ser escolhido por forma a permitir minimizar o impacto negativo das variações da função de similaridade, na decisão. Apenas estudos alargados com o universo dos indivíduos alvo (o que se pode revelar uma tarefa bastante onerosa) poderão conduzir a uma boa definição da função de similaridade e do valor limite. Mais à frente será feita uma análise mais detalhada sobre os erros de decisão e o seu impacto.

O último bloco que interessa discutir é o que faz o armazenamento dos padrões biométricos. Muito embora a sua função seja facilmente compreendida, há, contudo, algumas questões importantes a referir, sobretudo relacionadas com os formatos e a natureza da informação a armazenar. Começando por este último aspeto, é desejável armazenar não apenas o padrão biométrico em si, mas também informação relacionada com a qualidade do padrão (erros, valores de similaridade obtidos, características dos sensores, contexto, etc.) e, como é óbvio, informação sobre a identidade do proprietário de cada padrão, sendo que cada utilizador

poderá ter vários padrões associados. Adicionalmente poderá considerar-se útil armazenar os dados em bruto que deram origem ao padrão, com vista à possibilidade de recalcular o padrão, eventualmente na sequência de uma optimização do algoritmo de extração do padrão, ou ainda com vista ao estudo comparativo de algoritmos de geração de padrões. Aliás, é exatamente sob esta última perspetiva que estão disponíveis diversas Bases de Dados internacionalmente reconhecidas, como seja a FERET (*Face Recognition Technology*)[4], a Multi-PIE da Universidade de Cornegie Mellon[5], a CASIA, as bases de dados de impressões digitais mantidas pelo NIST[6], entre muitas outras que, frequentemente, são usadas para concursos internacionais que procuram estimular a investigação e desenvolvimento na área das biometrias (Flynn 2008) – o *site* Biometrics Ideal Test[7] mantém uma lista atualizada de algumas das bases de dados mais utilizadas.

Por outro lado, não devemos esquecer que, pela sua natureza, a informação contida numa base de dados biométricos é sensível e tem carácter privado, pelo que deve ser armazenada recorrendo a técnicas de cifra, que garantam a sua proteção. O mesmo tipo de cuidado deve ser assumido quando se consideram operações de transferências desses dados, ou a sua utilização para fins científicos, podendo ser necessário remover toda a informação de identidade para garantir a privacidade (Dunstone and Yager 2010). Por tudo isto, as técnicas e formatos a utilizar no armazenamento e nas transações que envolvem informação biométrica têm vindo a merecer uma atenção redobrada, mormente por parte de diversos organismos de normalização.

4.4.Normalização das biometrias

Dado o crescente interesse pelas tecnologias biométricas e muito especialmente a natureza global das várias aplicações em causa, quer ao nível nacional quer ao nível internacional é natural emergir uma preocupação crescente com questões de interoperabilidade. Muitas dessas questões criam expectativas sobre o aparecimento de enquadramentos comuns que permitam um melhor entendimento relativamente à eficiência e eficácia das diversas soluções. Este tipo de enquadramento sugere a criação de normas.

Não menosprezando vários esforços de normalização que foram surgindo desde a introdução dos primeiros sistemas biométricos (sobretudo AFIS e a sua aplicação forense), uma maior pressão sobre estas questões é bem mais evidente a partir dos primeiros anos do século XXI, em grande parte devido ao aumento em número e perigosidade de incidentes direta ou indiretamente relacionados com a Segurança dos Sistemas de Informação e o seu efeito de globalização. Um impulso considerável nesse sentido foi dado com a criação, em Junho de 2002, da subcomissão SC 37, dedicada às biometrias, no âmbito do comité técnico conjunto ISO/IEC JTC1 – Joint Technical Committee 1 da International Organization for Standardization (ISO) e da International Electrotechnical Commission (IEC). Rapidamente a SC 37 desenvolveu diversas normas relativas a interfaces e formatos de dados para biometrias da impressão

[4] O programa FERET foi promovido pelo Departamento de Defesa dos Estados Unidos e o National Institute of Standards and Technology (NIST), para estimular a investigação sobre reconhecimento facial - http://www.frvt.org/FERET/default.htm
[5] http://www.multipie.org/
[6] http://srdata.nist.gov/gateway/gateway?keyword=fingerprint
[7] http://biometrics.idealtest.org/

digital, íris e face. No entanto, muitos outros tipos de biometrias carecem de idêntico esforço, sendo evidente que esta subcomissão é uma das mais ativas dentro do ISO/IEC JTC1.

Mas existem outros esforços importantes que devem ser acompanhados, dado o seu potencial impacto. A Figura 5 mostra as principais organizações envolvidas nesse processo – mais detalhes são apresentados em (Deravi 2008). Em particular importa realçar, para além das organizações de normalização, a existência de um consórcio, BioAPI[8] (indiretamente suportado por o NIST e a NSA – National Security Agency – através do Biometric Consortium[9]), cujo principal objetivo tem sido o desenvolvimento de um importante interface genérico de alto nível, para aplicações e serviços de tecnologias biométricas. Atualmente na versão 2.0, esta especificação foi acompanhada pelas principais organizações de normalização, que produziram normas em conformidade, ANSI e ISO (M1 ANSI INCITS 358-2002 e ISO/IEC 19784).

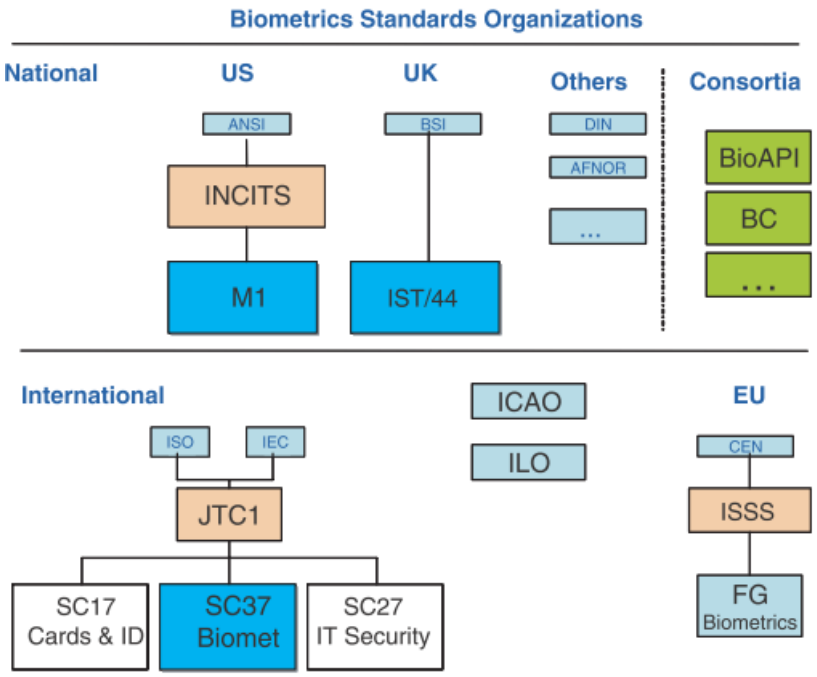


Figura 5 – Organizações de normalização de biometrias (Deravi 2008)

Aquele consórcio promoveu ainda um outro importante projeto de normalização, designado por Common Biometrics Exchange File Format e a sua extensão Common Biometrics Exchange Formats Framework, hoje reconhecido pela sigla CBEFF. À semelhança da especificação BioAPI, a especificação CBEFF foi igualmente transformada em normas ANSI e ISO (M1 ANSI INCITS 398-2005 e ISO/IEC 19785). Como se deduz facilmente, estas normas são determinantes na garantia da interoperabilidade entre sistemas biométricos.

Para além deste importante envolvimento comum, o comité M1 (equivalente Americano ao SC 37) desde cedo esteve particularmente ativo na normalização ao nível dos formatos dos dados biométricos, sobretudo impressão digital, face, íris, assinatura e geometria da mão, refletindo naturalmente as preocupações centrais do NIST. Idênticas preocupações aparecem num conjunto de normas relacionadas com a interoperabilidade de aplicações biométricas no

[8] BioAPI Consortium, http://www.bioapi.org/index.asp
[9] Biometric Consortium (BC), http://www.biometrics.org/

controlo de acesso em fronteiras, nos transportes, na defesa, no comércio e serviços de finanças (Dunstone and Yager 2010). Mais recentemente o SC 37 tem vindo a acompanhar esse esforço com a criação da família de normas ISO/IEC 19794 (Deravi 2008). No que respeita ao teste e relatórios de desempenho, ambas as organizações revelam preocupação, mantendo grupos de trabalho a desenvolver as famílias de normas M1 ANSI INCITS 409 e ISO/IEC 19795.

Dada a orgânica do JTC 1 é ainda de salientar o envolvimento de outras subcomissões no esforço de normalização de biometrias. Em particular a SC 17 (*Cards and personal identification*) que coopera com a SC 37 na normalização sobre a utilização de biometrias em *smartcards*, mantendo um grupo de trabalho (WG11) exatamente nesse tema. Também a SC 27 (*IT Security techniques*) evidencia alguma sobreposição com a SC 37, sobretudo na avaliação da segurança (aplicação a biometrias) e nos conceitos fundamentais de Segurança da Informação, em geral, que são da competência da SC 27 (Ryan 2009).

Esta síntese não aborda todos os esforços de normalização, nem todas as organizações envolvidas (as referências indicadas fornecem mais detalhes), mas procura indicar os principais vetores de evolução associados às principais preocupações de normalização e que, de forma mais ou menos coerente, traçam o caminho que se espera seguir ao nível da adopção desta importante tecnologia de autenticação e identificação.

4.5.Precisão e avaliação

Formulação do problema

Um sistema biométrico ideal, para além das características já enunciadas, daria uma resposta exata quando solicitado a verificar a identidade de um indivíduo, através de um padrão biométrico que lhe tenha sido recolhido. Pelo menos tão exata quanto a resposta à introdução da palavra-chave correta, realizada pelo seu legítimo possuidor. Mas ao contrário do que acontece com a verificação de uma palavra-chave, um sistema biométrico raramente decide com base em dois padrões exatamente iguais. Saber até que ponto essa diferença pode constituir um obstáculo à utilização do sistema é o principal objetivo da avaliação do desempenho, relativamente à precisão. De uma forma geral podemos considerar três tipos de avaliação (Gamassi, Lazzaroni et al. 2005) e (Mansfield and Wayman 2002):

- Tecnológica – carece de uma base dados bem caracterizada, como todos os seus elementos perfeitamente definidos e, se possível, normalizada; será um processo repetível, com o objetivo principal de avaliar algoritmos;
- Operacional – usa bases de dados obtidas em tempo real; o ambiente da recolha de dados e das experiências não é facilmente duplicável e tem por principal objetivo fazer uma avaliação do sistema; e
- Cenário – consiste numa avaliação ao sistema num contexto real (ou numa sua simulação), com um protótipo completo; os dados podem ser reutilizados se a recolha for controlada.

Todas estas formas de avaliação ocupam um lugar relevante ao longo da vida de um projeto biométrico. A avaliação tecnológica está tipicamente mais ligada ao processo de desenvolvimento, enquanto a avaliação de cenários antecede habitualmente a implementação num ambiente concreto e a avaliação operacional visa uma análise sistémica, que

normalmente é relevante na fase de prototipagem do sistema. Contudo, convém realçar que a principal diferença entre os três tipos de avaliação reside nos dados utilizados, já que as ferramentas são fundamentalmente as mesmas. A abordagem assumida neste módulo está orientada para a avaliação operacional.

De uma forma genérica, na avaliação aqui em questão estamos fundamentalmente perante dois tipos de erros: a falsa aceitação; e a falsa rejeição. Conhecer a natureza e avaliar esses erros é fundamental para definir a precisão de um sistema biométrico. Contudo, como já foi referido os dados disponíveis no desenvolvimento, teste e avaliação habitualmente não conseguem reproduzir fielmente a população alvo (sobretudo em aplicações de larga escala), o que se traduz no facto de a precisão de um sistema biométrico nunca poder ser determinada com rigor e de uma forma definitiva – a não ser em aplicações de âmbito local, com uma população muito reduzida (Newman 2009).

O problema da precisão é muito mais crítico no caso da identificação, já que no caso da autenticação os erros podem ser mais tolerados. Não obstante, dada a criticidade da função de controlo de acesso e a sua dependência de uma autenticação forte, é importante conhecer este aspeto de um sistema biométrico e em particular os métodos de avaliação e análise utilizados. Assim, a reflexão feita nesta secção recai sobretudo na autenticação, ou verificação da identidade, mas salientado, quando for pertinente, os aspetos comuns com a função de identificação. Na essência, a análise da precisão feita aqui e salvo indicação em contrário, segue o enquadramento descrito em (Dunstone and Yager 2010).

Atendendo à natureza aleatória das variáveis que influenciam o processo de captura de biometrias (desde fatores psicomotores até fatores ambientais), assim como o tipo de problema em estudo – o ponto de partida é uma afirmação de identidade, sobre a qual é necessário tomar uma decisão discreta, aceitar ou rejeitar, associada a uma probabilidade de tomar a decisão errada – a teoria estatística é o campo da matemática que habitualmente é usado. Mais propriamente, a sua área designada por Teste de Hipóteses (*Hypothesis Testing*), cuja formulação serve perfeitamente o problema em questão.

O método em questão exige a seguinte formulação. Começa-se por identificar a chamada hipótese nula (H_0), que se presume ser verdadeira, a menos que existam evidências do contrário. Se tal acontecer, então existirá uma hipótese alternativa (H_1) que será aceite. No caso da verificação biométrica as hipóteses referem-se à afirmação de identidade e são as seguintes:

- H_0: a afirmação de identidade é verdadeira (legítimo); ou seja, os dois padrões biométricos a comparar foram obtidos das mesmas características, do mesmo indivíduo
- H_1: a afirmação de identidade é falsa (impostor); ou seja, o padrão biométrico apresentado não corresponde ao padrão de referência armazenado

O objetivo do sistema de verificação será então aceitar ou rejeitar H_0, com base na informação disponível (teste estatístico), que tipicamente é uma grandeza escalar e que no caso do sistema biométrico não é mais do que o valor de similaridade (S) anteriormente descrito.

Parâmetros de avaliação

Iremos agora assumir que conseguimos obter de alguma forma (possivelmente a partir de um grupo de teste, representativo) a função de densidade de probabilidades dos resultados da função de similaridade, para ambas as hipóteses, i.e., para amostras dos utilizadores legítimos e dos impostores. A Figura 6 ilustra o que poderíamos esperar como resultado. Os utilizadores legítimos obtêm valores de S mais elevados, mas possivelmente distribuídos numa gama maior de valores, enquanto os impostores obtém concentrações mais elevadas, para valores de S mais baixos. A mesma figura mostra ainda o valor do limite τ definido para a função de decisão e que, naturalmente, será a origem dos erros de decisão.

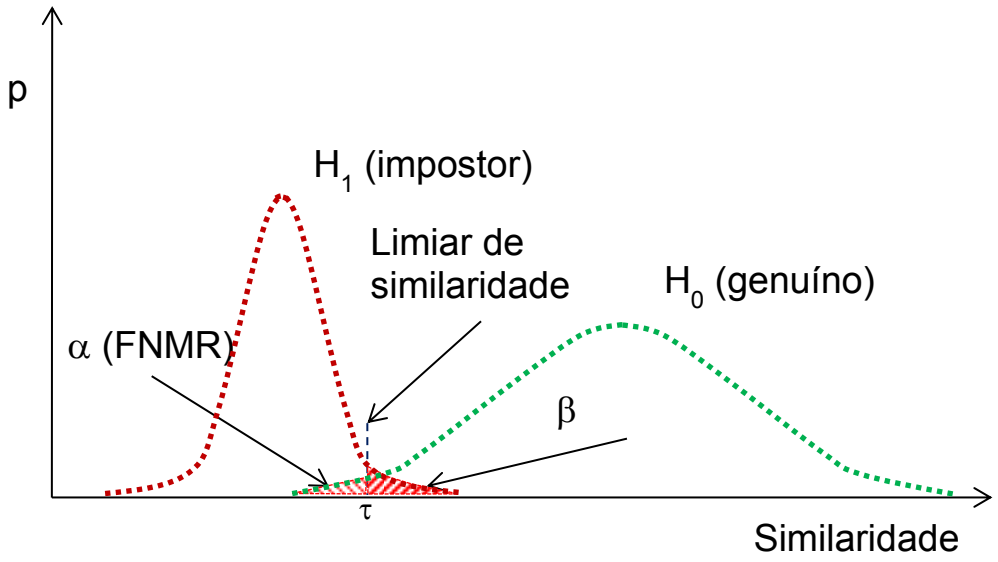


Figura 6 – Exemplo de possíveis funções de densidade de probabilidades para as amostras de um utilizador legítimo e dos impostores

Estamos então perante dois tipos de erro de decisão que, segundo a formulação adoptada, são designados por erros do Tipo I e erros doTipo II. Os erros do Tipo I correspondem aos casos em que H_0 é verdadeira (linha a verde na Figura 6), mas por se verificar que $S < \tau$ é tomada a decisão de rejeitar – este erro é também designado por **FNM** (*False Non-Match*) ou **FR** (*False Rejection*), ou ainda **FN** (*False Negative*). Os erros do Tipo II correspondem aos casos em que H_0 é falsa (o que nos leva a assumir que H_1 é verdadeira), mas a decisão é aceitar, uma vez que $S \geq \tau$ – este erro é também designado por **FM** (*False Match*), ou **FA** (*False Accept*), ou ainda **FP** (*False Positive*). As probabilidades de ocorrência de um FNM e de um FM podem ser calculadas também a partir das funções de densidade de probabilidades, correspondendo às áreas representadas a sombreado na Figura 6, sendo designadas por FNMR (*FNM Rate*) e FMR (*FM Rate*) e dadas pelas seguintes expressões:

$$\boldsymbol{\alpha} = \int_{-\infty}^{\tau} \boldsymbol{f_{H_0}(S)ds}$$

$$\boldsymbol{\beta} = \int_{\tau}^{+\infty} \boldsymbol{f_{H_1}(S)ds}$$

Equação 3 - Determinação de FNMR e FMR

Como se pode facilmente observar, para um determinado sistema biométrico os valores de FMNR e FMR dependem fundamentalmente do limiar de decisão τ, o qual pode ser mesmo utilizado de forma dinâmica para ajustar o funcionamento do sistema. Baixando o valor de τ baixamos o valor de FNMR, mas aumentamos o valor de FMR, o que normalmente não é bom para uma aplicação de verificação. Mas já o poderá ser para uma aplicação de investigação forense, na qual se pretende que todos os possíveis indivíduos sejam considerados. Por outro lado, aumentando o valor de τ diminuímos o FMR, tornando o sistema mais imune a falsas verificações, mas pagando com isso o preço de uma menor usabilidade, dado o aumento dos erros de autenticação dos utilizadores legítimos, traduzido no aumento do valor de FNMR. Essa relação encontra-se sumariamente ilustrada na Figura 7, que mostra um exemplo de uma curva **DET** (*Detection Error Trade-off*). Um objetivo prático interessante será encontrar o valor de τ que permita operar com o mesmo valor de FNMR e FMR ($\alpha = \beta$), ponto esse que é referido habitualmente por **EER** (*Equal Error Rate*).

O valor EER é uma forma prática e simples de resumir, num único indicador, o desempenho de um sistema biométrico. No entanto, é preciso ter em conta que este indicador esconde muitos detalhes do desempenho e que, na grande maioria dos casos e por razões práticas, um sistema biométrico não irá operar na zona definida por este indicador. Em suma, pelo facto de uma dado sistema A ter um EER inferior ao de um sistema B, não implica que, em determinada aplicação, A tenha um melhor desempenho do que B.

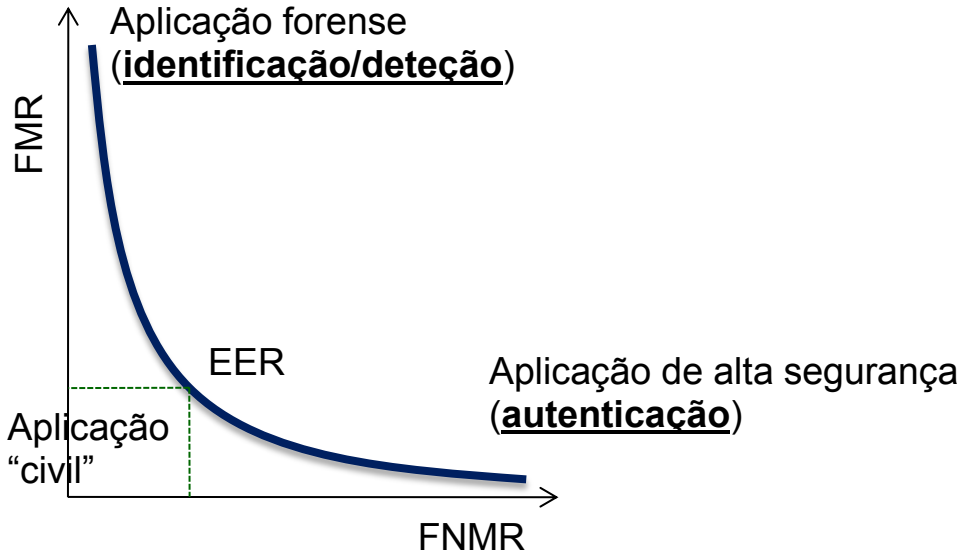


Figura 7 – Exemplo de uma curva DET (*Detection Error Trade-off*), que relaciona FNMR com FMR

De forma complementar e inspirando-nos em problemas similares, sobretudo na área do diagnóstico clínico, é ainda frequente deduzir outros indicadores de desempenho (Bewick, Cheek et al. 2004) e (Ratha and Govindaraju 2008). Vamos assumir que **M** (*Match*) expressa o número total de tentativas legítimas (idealmente seria número total de aceitações), **NM** (*Non-Match*) o número total de tentativas impostoras, **TM** (*True Match*) representa o número de vezes em que a decisão é aceitar sendo H_0 verdadeira ($TM = M - FNM$), **TNM** (*True Non-Match*) representa o número de vezes em que a decisão é rejeitar sendo H_0 falsa ($TNM =$

$NM - FM$). Os valores TM e TNM expressos em razões do total de, respetivamente, M e NM, assumem um significado especial:

$$TMR = TM/M = 1 - FNMR \quad \text{Usado para expressar a sensibilidade}$$

$$TNMR = TNM/NM = 1 - FMR \quad \text{Usado para expressar a especificidade}$$

Equação 4 – Expressões para o cálculo da Sensibilidade e Especificidade

Adicionalmente, TM e TNM são ainda usados para expressar a precisão, da seguinte forma (razão entre as decisões corretas sobre o total das decisões tomadas):

$$ACC = \frac{(TM + TNM)}{(M + NM)}$$

Equação 5 - Expressão para o cálculo da Precisão

De notar que o número de utilizadores e o número de atacantes não são considerados separadamente nestes indicadores, o que pode originar uma análise distorcida (e.g., um sistemas pode evidenciar uma especificidade muito elevada, porque o número de atacantes é baixo). Uma forma de contornar essa limitação é apresentar todos os valores relacionados numa tabela de confusão, como a que é apresentada na Figura 8.

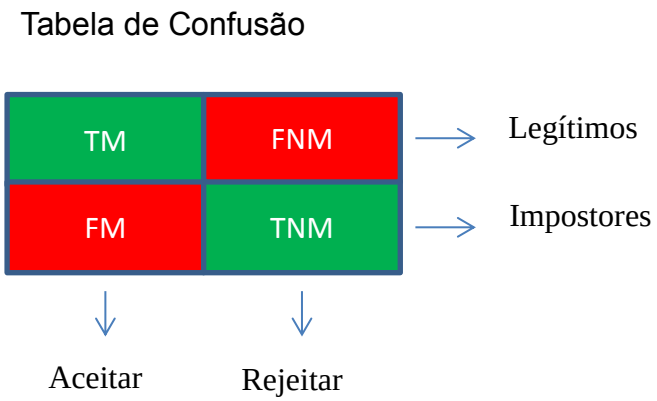


Figura 8 – Tabela de Confusão para mapear valores da decisão

As curvas ROC

Uma forma simples de resumir graficamente o desempenho de um sistema biométrico é através de curvas ROC (*Receiver Operating Characteristics*). Estas curvas (à semelhança das curvas DET acima referidas) evidenciam o impacto que o valor do limiar τ tem nos erros de operação, mas neste caso relacionando a taxa de falsos positivos (FMR) com a sensibilidade, ou taxa de verificação que, de acordo com a Equação 4, é determinada por $1 - FNMR$. Ou seja, uma curva ROC mostra o balanceamento estabelecido entre os benefícios (verdadeiros positivos) e o custo (falsos positivos), que podemos esperar obter quando tentamos ajustar o valor do limiar (Fawcett 2006). A Figura 9 mostra um exemplo de uma curva ROC.

Porque normalmente interessa analisar variações de valores muito pequenos de FMR, é vulgar utilizar uma escala logarítmica no respetivo eixo. De notar ainda que, de acordo com a relação entre os valores da sensibilidade e de FNMR (e naturalmente assumindo que é utilizada a

mesma escala nos eixos), o cruzamento da curva ROC com a diagonal entre os pontos (0,1) e (1,0) fornece o valor de EER, tal como indicado na Figura 9.

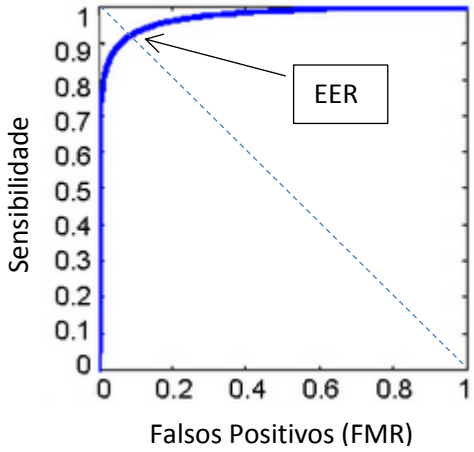


Figura 9 - Exemplo de uma curva ROC[10]

A diagonal entre os pontos (0,0) e (1,1) assume um significado especial. Qualquer ponto sobre essa diagonal evidencia um benefício igual ao custo, ou seja, o algoritmo de decisão que lhe estivesse associado gerava tantos falsos positivos quantos os verdadeiros positivos. Como estamos perante uma decisão binária, idêntico desempenho seria obtido por um simples sistema de decisão aleatório. Sendo assim, esta diagonal representa um limite inferior para qualquer algoritmo de decisão útil, já que abaixo desse limite seria preferível substituí-lo por um decisor aleatório, sem sequer ter em conta o valor de similaridade, que nem precisaria de ser calculado.

Um indicador adicional que pode ser usado é a área da zona inferior limitada pela curva ROC. De uma forma geral, quanto maior for essa área, melhor será o desempenho do sistema biométrico em questão. Contudo, a determinação da área não é uma tarefa simples, porque a curva ROC não é, normalmente, uma curva paramétrica, sendo obtida a partir de dados experimentais. No entanto, usando técnicas de interpolação, essa área pode ser estimada através do algoritmo proposto em (Fawcett 2006).

Avaliação individual

A análise feita anteriormente agrega resultados estatísticos de toda a população alvo, podendo dizer-se que consiste numa visão sistémica de alto nível assente no princípio otimista de que o sistema biométrica exibirá um comportamento semelhante com todos os indivíduos. Sem dúvida que esse tipo de análise (operacional) é essencial para reportar a avaliação do desempenho desse sistema. Contudo, essa análise deve ser complementada com uma outra individual, uma vez que é bem possível obter níveis de desempenho substancialmente diferentes com diversos indivíduos.

Do ponto de vista metodológico esta análise individual não difere muito da anterior, consistindo simplesmente em considerar os utilizadores de forma individual (em vez de agregados), quer no papel de genuíno quer no papel de atacante (contra todos os padrões

[10] Gráfico adaptado de http://spie.org/x17545.xml, consultada em 9 de Março, de 2013.

armazenados) e obter as respetivas funções de densidade de probabilidades, as taxas de erro e, possivelmente, as curvas DET ou ROC associadas. O objetivo último dessa análise é procurar classificar os indivíduos segundo as diferenças detectadas, assim como procurar casos singulares acentuadamente díspares, procurar compreender as razões que originam as diferenças e, dessa forma, procurar antecipar os problemas de aplicação a médio/longo prazo resultantes da implementação do sistema biométrico.

Tal como já foi referido anteriormente, é espectável que o processo de amostragem e quantização de uma biometria por um sensor introduza alguns erros, que podemos considerar de ordem aleatória. Estes erros são intrínsecos ao sensor e são inevitáveis (eventualmente serão resolvidos numa evolução futura da tecnologia usada no sensor), não sendo o foco de interesse nesta análise. O foco estará sim nas razões de ordem fisiológica, comportamental e de interação, relacionadas com o indivíduo. De uma forma resumida, cada um desses fatores pode interferir com o sistema biométrico da seguinte forma:

- Fatores fisiológicos – em primeiro lugar, um indivíduo pode evidenciar alguma deformação (eventualmente provocada por acidente) que distorça ou mesmo impeça a leitura biométrica; em segundo lugar, a idade pode ter influência no padrão biométrico; em terceiro lugar e eventualmente por um dos efeitos anteriores, a característica biométrica a ser medida pode ter sofrido ligeiras alterações, que não impedem a leitura, mas que provocam variações acentuadas de quantização.
- Fatores comportamentais – incluem todos os aspetos da forma como o indivíduo aborda o sensor e, de uma maneira geral, podem ter um efeito muito acentuado; são particularmente críticos nas biometrias comportamentais (por maioria de razão); evidenciam uma tendência de alteração lenta mas continuada, sobretudo com a idade; podem obrigar a condicionar, de alguma forma, o acesso ao sensor – e.g., limitando o movimento da cabeça no reconhecimento facial, ou colocando guias no leitor de assinatura.
- Fatores de interação – normalmente estão associados a casos particulares de indivíduos que não se adequam ao sensor (e.g., condições de luz não fornecem contraste suficiente para indivíduos de pele escura, ou um sensor de voz que distorce determinados timbres, ou ainda um leitor de impressões digitais que é sensível à pressão exercida).

Alguns destes fatores podem ser detetados precocemente, logo na fase de registo e, nesse caso, originam erros do tipo FTE se impedirem esse mesmo registo. Mas mesmo não impedindo o registo, pode-se detetar uma variabilidade anormal para um indivíduo, que deixa antecipar futuros problemas. Nesse caso poder-se-á associar ao registo um indicador de qualidade, que ajude a lidar melhor com esses erros na fase da decisão, eventualmente definindo uma valor de limiar τ Individualizado. Contudo, estas soluções devem ser ponderadas com muito cuidado, já que podem aumentar consideravelmente a complexidade do sistema, assim como comprometer a validade estatística da própria avaliação.

Observando a distribuição da densidade de probabilidades para cada indivíduo é possível realizar uma classificação que se tem revelado útil para compreender melhor o seu efeito. As classes definidas constituem aquilo a que se tem chamado *biometric menagerie* (Yager and

Dunstone 2010) e tem por base a forma e localização da função de distribuição da densidade de probabilidades individuais, quando comparadas com o caso geral (obtido por agregação e descrito na secção anterior) e, numa segunda abordagem, com a função da densidade de probabilidades enquanto impostor. Para o primeiro caso e assumindo como referência as funções de densidade de probabilidades da Figura 6, os indivíduos pode ser classificados como:

- *Sheep* – classe que inclui a grande maioria, com a função de densidade de probabilidades idêntica ao do caso geral (aliás, é este grupo que define o caso geral);
- *Goats* – são os indivíduos que irão evidenciar problemas de verificação porque a distribuição genuína aparece concentrada em valores de similaridade mais baixos. Assim, para o mesmo valor de limiar, geram mais falsos negativos;
- *Lambs* – são os indivíduos cuja distribuição genuína apresenta uma maior sobreposição com a dos impostores. Assim, são mais sensíveis à impersonificação e, portanto, potenciais responsáveis pela geração de um maior número de falsos positivos; e
- *Wolves* – são os indivíduos que obtém valores de similaridade elevados quando considerados impostores; face à maioria dos indivíduos, a sua distribuição de impostor aproxima-se mais da dos genuínos e, por isso, têm tendência a impersonalizar todos os outros, aumentando número de falsos positivos.

Do ponto de vista da distribuição de valores de similaridade não existe diferença entre os *Lambs* e os *Wolves*. Na verdade, a única diferença consiste na perspetiva da análise, pois no primeiro caso a perspetiva é a de quem se autentica e no segundo é a de quem ataca.

Focando agora a análise na posição relativa das distribuições de probabilidades (genuíno e impostores) individuais, é possível obter a seguinte classificação complementar (continuando a ter como referência a distribuição geral apresentada na Figura 6 e assumindo um valor de limiar constante):

- *Doves* – obtém valores de similaridade bem diferenciados como genuínos e como impostores, consistindo no grupo melhor adaptado ao sistema biométrico em questão;
- *Worms* – ao contrário dos anteriores, obtém valores relativamente baixos de similaridade como genuínos e relativamente elevados como impostores, consistindo no grupo menos adaptado ao sistema biométrico em questão;
- *Chameleons* – obtém valores de similaridade muito elevados, quando confrontados com eles próprios ou com todos os outros, tendo assim a capacidade de impersonalizar qualquer indivíduo (responsáveis pelo aumento de falsos positivos); e
- *Phantoms* – contrariamente aos anteriores, obtém normalmente valores de similaridade baixos, quer eles próprios, quer com os outros (responsáveis pelo aumento dos falsos negativos).

A Figura 10 mostra as distribuições típicas individuais destes últimos quatro grupos, assim como da classe *Sheep* definida como comportamento de referência, na classificação anterior. É ainda útil visualizar graficamente a forma como se relacionam as distribuições individuais de genuíno e impostor, para toda a população. Esse tipo de gráfico é normalmente designado por *Zoo Plot* e um exemplo é mostrado na Figura 11. Neste gráfico, como facilmente se pode

deduzir, quanto mais os pontos representados (indivíduos) estiverem concentrados no topo superior direito melhor será o desempenho do sistema biométrico em análise – gráfico do lado esquerdo da figura.

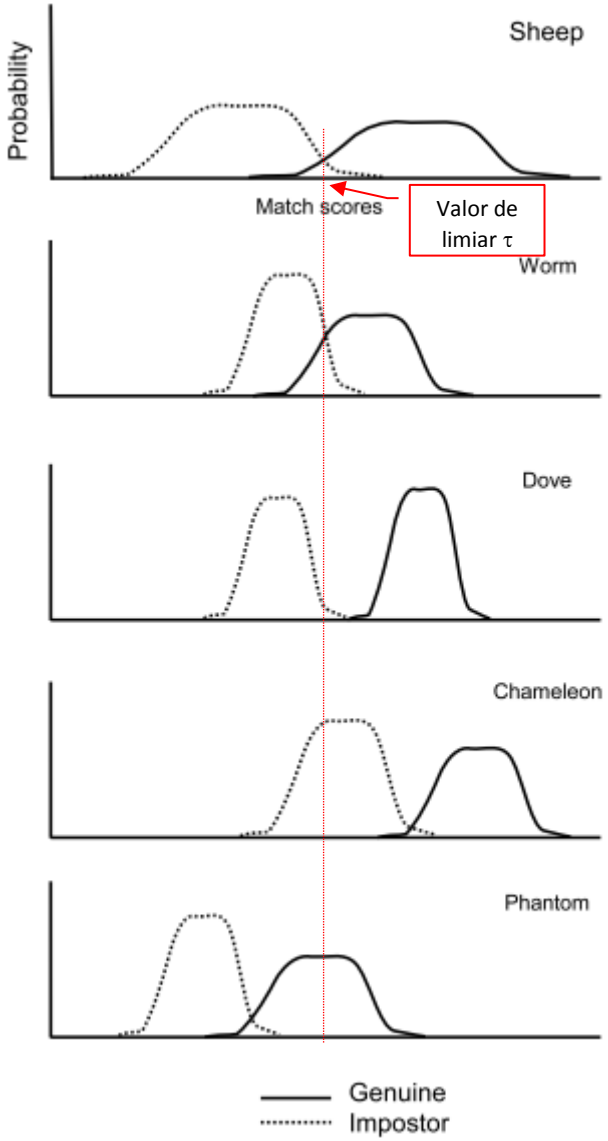


Figura 10 - Comparação entre classes de indivíduos – adaptado de (Dunstone and Yager 2010)

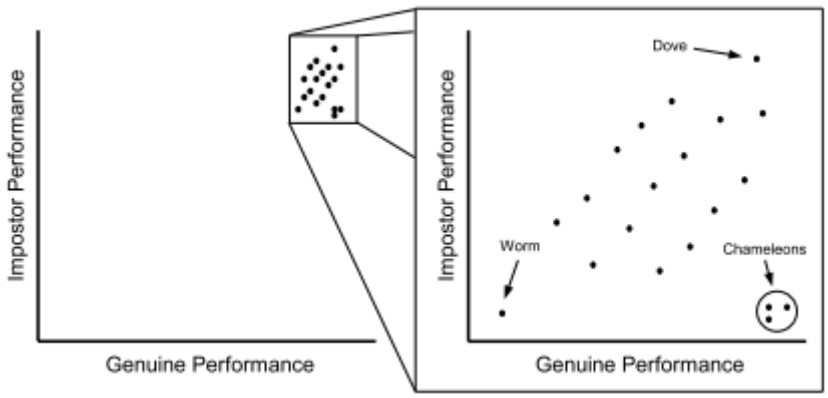


Figura 11 - Exemplo de um *Zoo Plot* (Dunstone and Yager 2010)

A Figura 11 mostra ainda que o *Zoo Plot* pode ser usado para avaliar em maior detalhe como é que os indivíduos de posicionam ao nível do grupo, identificando quantos ou mesmo quem integra cada classe – gráfico do lado direito da figura.

Aplicação prática do modelo de avaliação

Apesar da sua relativa simplicidade, o modelo acima descrito evidencia algumas limitações importantes. A mais significativa reside na dificuldade em determinar as funções de densidade de probabilidades. O Teste de Hipóteses recorre tipicamente a distribuições conhecidas *a priori* e claramente esse não é o caso das biometrias, onde essa distribuição é determinada através de uma amostra suficientemente grande (supostamente) de utilizadores legítimos e impostores. Para além da dimensão da amostra, mais alguns cuidados são necessários, nomeadamente:

- A amostra deve ser representativa
- Devem ser recolhidas amostras que produzam toda a gama (ou próximo disso) de valores de similaridade
- Deve recolher-se o máximo possível de amostras genuínas e impostoras
- Nunca assumir alguma forma paramétrica de distribuição, como seja a normal (essa assunção muita raramente é justificada e pode conduzir a erros relevantes).

A importância da avaliação das biometrias e dos respetivos procedimentos de teste é de tal forma elevada que, para além das normas já anteriormente referidas, motivou mesmo a publicação de um relatório técnico com boas práticas, pelo NPL (*National Physical Laboratory*), no Reino Unido e que contém um conjunto importante de recomendações (Mansfield and Wayman 2002).

Para ilustrar as dificuldades acima referidas e também para exemplificar o processo de avaliação, é apresentado em seguida um exemplo baseado em dados reais obtidos a partir de uma experiência realizada com dez utilizadores num sistema biométrico comportamental de *keystroke dynamics*. Por questões de simplicidade, para esta exemplificação apenas se consideram 2 utilizadores como registados (*enrolment*). Cada utilizador não registado fez entre 20 a 30 capturas, enquanto os registados fizeram mais do que 30 capturas, sendo que algumas foram descartadas por não evidenciarem um conjunto de características coerentes. O resumo dos valores obtidos encontra-se no Anexo A – dados para exemplo de avaliação de biometria. Os valores de similaridade estão apresentados numa escala de 0 a 100, em intervalos de 5, como se pode verificar na respectiva tabela.

Depois de calculados os valores de similaridade para os utilizadores legítimos e impostores, é possível construir um histograma, que representa de forma discreta, a frequência de ocorrências de valores de similaridade (ver o Anexo B – Histograma e variáveis estatísticas associadas). É igualmente possível estimar a função de densidade de probabilidades, dividindo as ocorrências de cada valor de similaridade pelo total de valores obtidos (segunda linha da tabela no Anexo A – dados para exemplo de avaliação de biometria). As funções assim obtidas não são paramétricas, dificultando muito a utilização de um modelo formal. A Figura 12 mostra num gráfico de barras os valores obtidos, assim como uma possível aproximação para

as funções de densidade de probabilidades, obtidas através do cálculo das médias móveis, com um período igual a 2^{11}.

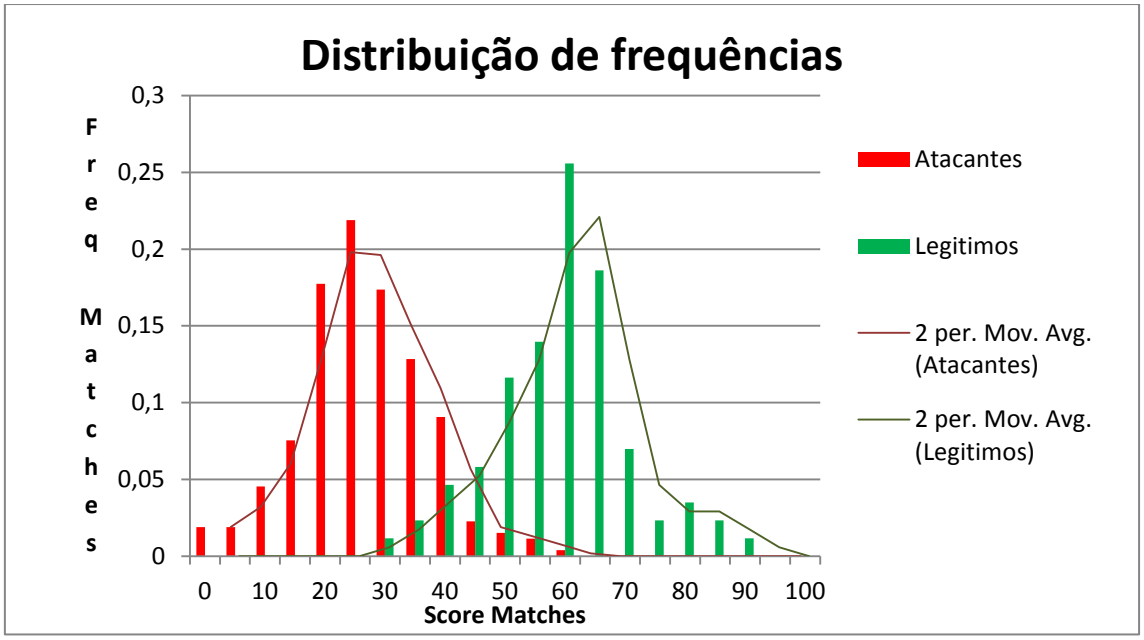


Figura 12 - Distribuição de frequências e função de densidade de probabilidades para o exemplo apresentado

Os valores de FNMR e FMR são determinados através da contagem dos Falsos Negativos e dos Falsos Positivos (fixando naturalmente o valor de limiar τ, neste caso em 42), dividindo-os pelo número total de tentativas legítimas e de ataques – terceira linha da tabela. Todos os restantes parâmetros de avaliação da precisão podem então ser deduzidos, tal como consta no Anexo B – Histograma e variáveis estatísticas associadas.

Quanto ao valor EER ele merece uma atenção mais detalhada, uma vez que na prática, atendendo à forma como se obtêm os valores de FNMR e FMR, não se consegue construir uma curva DET como a sugerida na Figura 7. De facto, para averiguar a variação daquelas variáveis, o que é vulgar fazer é atribuir diversos valores a τ e registar os valores obtidos para FNMR e FMR. Com esse exercício é possível obter um gráfico como o da Figura 13, que mostra a respectiva variação em função de τ. Através desse gráfico não é normalmente fácil identificar diretamente o ponto de cruzamento que identifica o EER.

[11] Esta aproximação é obtida diretamente com ferramentas do Excel, que foi usado neste exemplo.

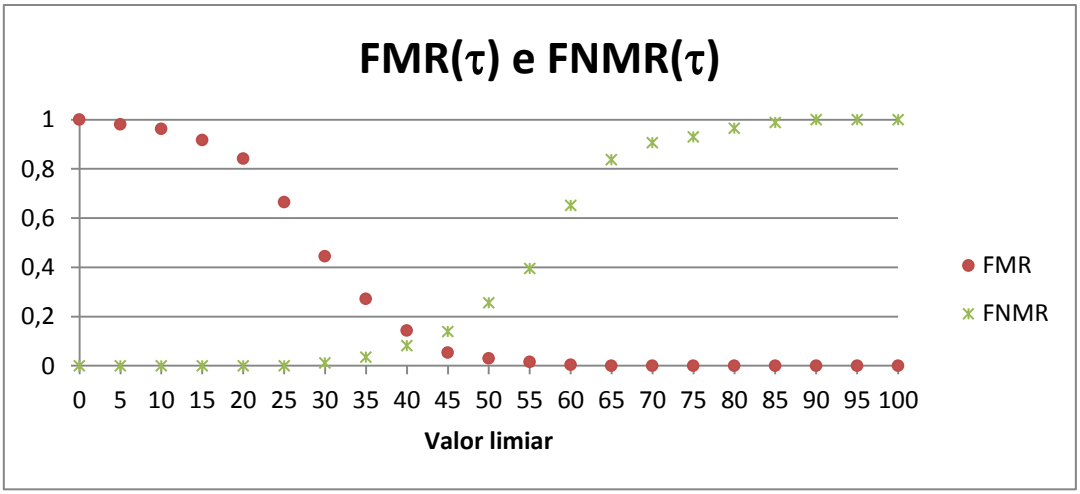


Figura 13 - Gráfico de FMR e FNMR em função do valor limiar (τ) para o exemplo apresentado

Na prática, a forma usual de obter o EER é através da média calculada a partir dos dois valores mais próximos de FMR e FNMR. Como existem sempre dois pares de valores que limitam, à esquerda e à direita, o ponto de cruzamento, procura-se o par que evidencia a menor diferença. Do ponto de vista do algoritmo, o processo consiste em determinar:

$$\tau_1 = \max_{\tau}\{\tau | FNMR(\tau) \leq FMR(\tau)\},$$

$$\tau_2 = \min_{\tau}\{\tau | FNMR(\tau) \geq FMR(\tau)\},$$

$$[EER_{low}, EER_{high}] = \begin{cases} [FNMR(\tau_1), FMR(\tau_1)] & if\ FNMR(\tau_1) + FMR(\tau_1) \leq \\ & FMR(\tau_2) + FNMR(\tau_2) \\ [FNMR(\tau_2), FMR(\tau_2)] & otherwise \end{cases}$$

$$e\ EER = \frac{EER_{low} + EER_{high}}{2}$$

No exemplo em análise a aplicação deste algoritmo identifica facilmente os valores mais próximos de FNMR e FMR a considerar (0,08 e 0,14 respetivamente), quando τ=40, o que se pode comprovar facilmente consultando a terceira linha da tabela do Anexo A – dados para exemplo de avaliação de biometria. Assim, EER fica com valor aproximado de 0,11.

De seguida pode-se gerar a curva ROC que, como foi descrito, relaciona a sensibilidade (ou taxa de verdadeiros positivos, dada simplesmente por $1 - FNMR$) com os falsos positivos. A Figura 14 mostra a curva obtida, a qual é apresentada com duas possíveis escalas, uma linear e outra logarítmica, no gráfico b), por forma a realçar a zona de variação mais crítica, correspondendo aos valores baixos de FMR. Mais uma vez, a aproximação à curva é realizada através do cálculo das médias móveis, com um período igual a 2.

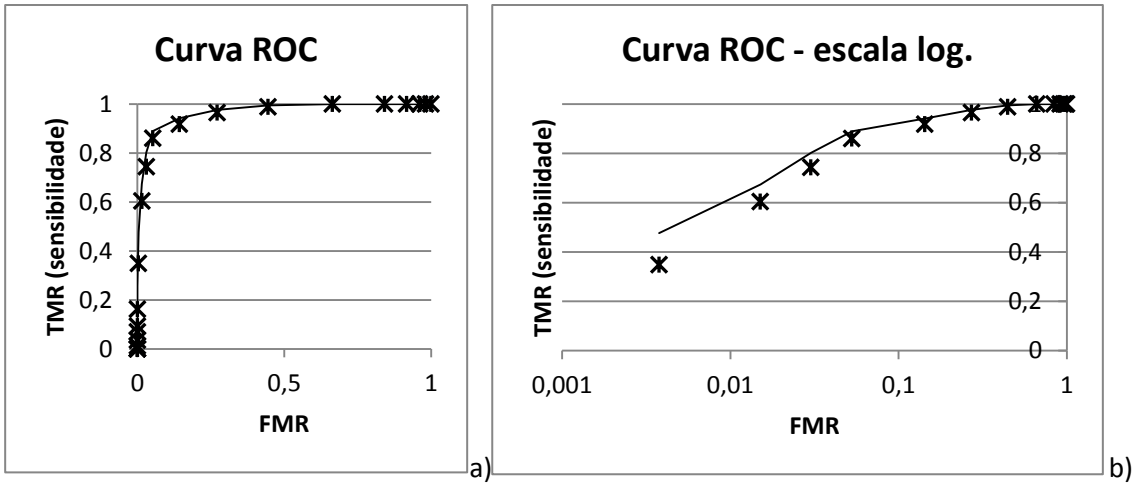


Figura 14 - Curva ROC para o exemplo apresentado

Finalmente, na Figura 15 são apresentadas as distribuições de frequência obtidas para os dois utilizadores individualizados na tabela do Anexo A – dados para exemplo de avaliação de biometria. Neste caso em particular, porque apenas existem dois utilizadores legítimos, não será muito relevante classificar os utilizadores face ao desempenho global dos legítimos (primeira dimensão no *biometric menagerie*). No entanto, observando as distribuições de cada um deles e assumindo que as suas distribuições enquanto atacantes estariam próximas da distribuição do grupo, seriamos levados a classificar o utilizador 2 como um *Dove*, enquanto o utilizador 1 se aproxima muito mais de um *Worm*. Com base nesta observação e muito embora os resultados globais até sejam interessantes, facilmente se concluiria que o sistema biométrico em causa apresenta limitações consideráveis, carecendo de um estudo mais aprofundado.

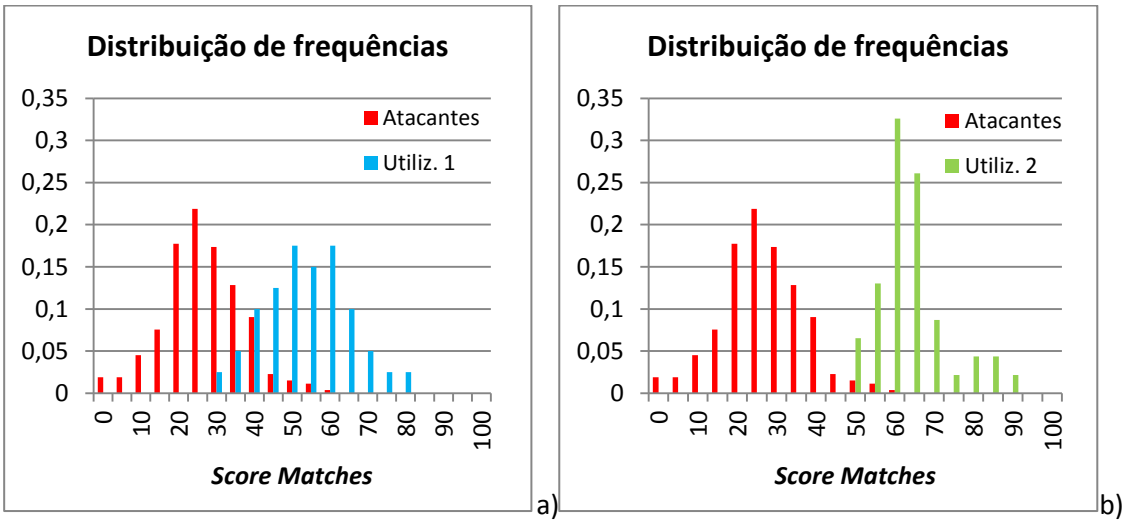


Figura 15 - Distribuição de frequências para os dois utilizadores considerados no exemplo apresentado

4.6.Segurança e Privacidade

Não obstante o importante papel que a tecnologia biométrica assume na mitigação de vários riscos de segurança da informação, ao nível do controlo de acesso, convém também refletir sobre o seu impacto negativo – no limite, qualquer medida de segurança impõe algum tipo de

limitação que se traduz em alguma perda de flexibilidade, sendo sempre aconselhável avaliar a relação custo/benefício.

A integridade dos sistemas biométricos assenta no pressuposto que o indivíduo relativamente ao qual se faz uma captura de uma biometria é efetivamente o seu detentor – frequentemente assumido como um axioma. A quebra dessa relação é exatamente uma das principais ameaças e, a promover esta ameaça, está o facto de uma biometria não ser um segredo. Na realidade, durante o nosso dia-a-dia deixamos as nossas marcas biométricas um pouco por todo o lado, fisicamente ou em algum tipo de registo (e.g., fotografia ou vídeo), o que deixa a um potencial atacante um potencial espaço de exploração. Assim, será aconselhável admitir que, algum dia, um padrão biométrico pode ser forjado.

As propriedades fundamentais das biometrias, descritas na secção 4.1, também evidenciam algumas fragilidades. Uma delas é criada pela unicidade, que traduz o facto de se assumir que não há dois indivíduos com o mesmo padrão biométrico, dentro do universo de utilizadores considerado. Esta propriedade é particularmente relevante na identificação, mas mesmo no caso da autenticação tem uma consequência potencialmente danosa: uma biometria, por definição não é revogável. Isto significa que, ao contrário de uma palavra-chave que podemos alterar quando achamos que foi comprometida, uma biometria, por si só e mesmo que tenhamos a certeza que foi comprometida, não poderá ser alterada. Juntando esta à ameaça anterior é necessário encontrar uma medida que responda ao risco de um ou mais utilizadores se virem privados da possibilidade de usar um seu padrão biométrico (Newman 2009).

Em resposta a estas ameaças tem-se assistido a um importante esforço tecnológico ao nível dos sensores para mitigar o risco de utilização fraudulenta, nomeadamente refinando os processos de verificação das propriedades físicas subjacentes às características capturadas (e.g., garantir que um dedo tem circulação sanguínea através de um sensor de infra vermelhos). Mas mesmo esta medida de mitigação tem um potencial risco associado, ao reforçar a não refutação e que se pode traduzir na (pouco provável, mas possível) errada imputação de responsabilidades pelo uso de uma biometria.

Um outro risco que não pode ser menosprezado, sobretudo considerando a utilização de biometrias em larga escala, é o da bio exclusão. Como resultado de acidentes ou mesmo por questões de deformação, é sempre possível encontrar indivíduos que não exibam determinadas características biométricas.

Avaliando o risco destas ameaças em geral e tendo em conta que o valor dos recursos dependentes do controlo de acesso é normalmente muito elevado, a solução que tem vindo a ser investigada e adotada baseia-se no uso de várias biometrias em simultâneo – sistemas multimodais. Contudo, um obstáculo importante é o custo e a complexidade das implementações.

Do ponto de vista da infraestrutura, um sistema biométrico não é mais que um sistema de computação complexo (tal como foi anteriormente descrito) e enquanto tal está naturalmente sujeito a um conjunto de ataques bem conhecidos. A Figura 16 apresenta um diagrama de um sistema biométrico com todos os pontos passíveis de ataques devidamente assinalados (Adler 2008).

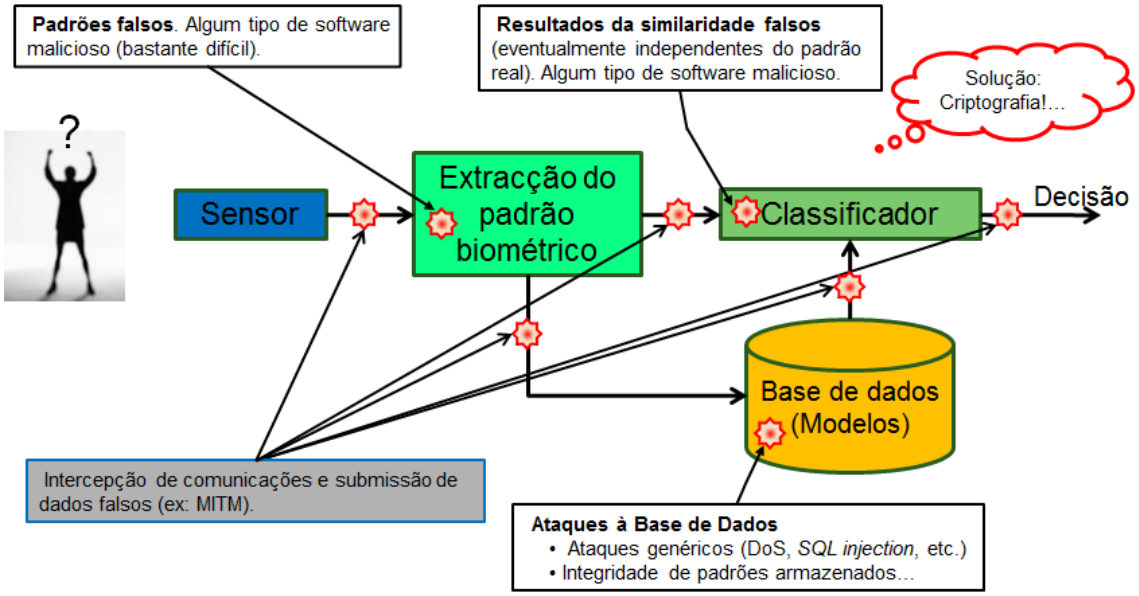


Figura 16 - Possíveis ataques à infraestrutura de um sistema biométrico

Relativamente às medidas de controlo que incidem sobre a infraestrutura, têm demonstrado bastante utilidades as técnicas de criptografia, não só na cifra de dados em trânsito, mas também na autenticação dos diversos componentes interligados e, sobretudo, na garantia de confidencialidade e integridade dos padrões armazenados na base de dados (Tuyls and Goseling 2004) e (Jain, Ross et al. 2005).

No que respeita à privacidade dos dados biométricos, é habitualmente assumido que esses dados, por serem padrões definidos por um conjunto limitado de características, muito dificilmente podem ser usados, sem mais informação, para identificar os seus proprietários. No entanto, alguns investigadores têm demonstrado que, sobretudo na biometria facial mas também com outras, explorando a informação dos padrões e os resultados de similaridade, é efetivamente possível associar uma identidade a um padrão biométrico (Adler 2008). Assumindo que tal risco existe, um sistema biométrico colocará naturalmente questões importantes de privacidade. Este constitui mais um aspeto da segurança da informação onde a criptografia pode ser utilizada com sucesso, à semelhança do que ocorre com outras bases de dados de informação privada. A questão central é assumir definitivamente que os dados biométricos são dados privados.

5. Conclusões

Nesta aula são apresentados os fundamentos das tecnologias biométricas, enquanto ferramenta de autenticação dos utilizadores e no âmbito da implementação do controlo de acessos. Para além dos conceitos essenciais e das questões de normalização, a aula incide sobretudo nos problemas de avaliação dos sistemas biométricos. Esta ênfase é justificada pela criticidade da função desses sistemas, assim como o efeito de escalabilidade que lhes está associado, já que no limite todos os utilizadores de dispositivos informáticos podem ser afetados por decisões boas ou más tomadas sobre essas tecnologias.

Após a formulação do problema da avaliação dos sistemas biométricos, é apresentado um enquadramento formal necessário para suportar uma avaliação adequada. No entanto há muitas limitações à aplicação desse modelo formal, tendo que se recorrer a algumas simplificações. Esse processo é demonstrado através de um exemplo de aplicação. Finalmente são apresentadas e discutidas algumas questões relacionadas com a própria segurança dos sistemas informáticos, assim como o seu impacto na privacidade.

6. Referências

Adler, A. (2008). Biometric System Security. Handbook of Biometrics. A. K. Jain, P. Flynn and A. A. Ross, Springer US**:** 381-402.

Bewick, V., L. Cheek, et al. (2004). "Statistics review 13: receiver operating characteristic curves." Crit Care **8**(6): 508-512.

Cimato, S., M. Gamassi, et al. (2006). Personal identification and verification using multimodal biometric data. IEEE International Conference on Computational Intelligence for Homeland Security and Personal Safety, Alexandria, VA.

Delac, K. and M. Grgic (2004). A survey of biometric recognition methods. 46th International Symposium Electronics in Marine, ELMAR-2004.

Deravi, F. (2008). Biometrics Standards. Advances in Biometrics: Eensors, Algorithms and Systems. N. K. Ratha and V. Govindaraju, Springer London**:** 473-489.

Dunstone, T. and N. Yager (2010). Biometric System and Data Analysis: design, evaluation and data mining, Springer.

Fawcett, T. (2006). "An introduction to ROC analysis." Pattern Recognition Letters **27**(8): 861-874.

Flynn, P. (2008). Biometrics databases. Handbook of Biometrics. A. K. Jain, P. Flynn and A. A. Ross, Springer US**:** 529-548.

Gamassi, M., M. Lazzaroni, et al. (2005). "Quality assessment of biometric systems: a comprehensive perspective based on accuracy and performance measurement." Instrumentation and Measurement, IEEE Transactions on **54**(4): 1489-1496.

Ho, C. C. and C. Eswaran (2011). Consodilation of fingerprint databases: A Malaysian case study. Hybrid Intelligent Systems (HIS), 2011 11th International Conference on, IEEE.

Hong, J.-H., E.-K. Yun, et al. (2005). "A Review of Performance Evaluation for Biometrics Systems." International Journal of Image and Graphics **05**(03): 501-536.

Islam, M. R., H. M. Baniamin, et al. (2012). "Institutional Mechanism of National Identification Card: Bangladesh Experience." Public Policy and Administration Research **2**(2): 1-13.

Jain, A. K. and A. Ross (2002). Learning user-specific parameters in a multibiometric system. Image Processing. 2002. Proceedings. 2002 International Conference on, IEEE.

Jain, A. K., A. Ross, et al. (2004). "An introduction to biometric recognition." Circuits and Systems for Video Technology, IEEE Transactions on **14**(1): 4-20.

Jain, A. K., A. Ross, et al. (2005). Biometric template security: Challenges and solutions. Proceedings of European Signal Processing Conference (EUSIPCO).

Jakobsson, M., R. I. Chow, et al. (2012). "Authentication-Are We Doing Well Enough?[Guest Editors' Introduction]." Security & Privacy, IEEE **10**(1): 19-21.

Jarosz, H. and J. C. Fondeur (2005). Large-scale identification system design, Springer London.

Jones, L. A., A. I. Antón, et al. (2007). Towards understanding user perceptions of authentication technologies. Proceedings of the 2007 ACM Workshop on Privacy in Electronic Society, Alexandria, Virginia, USA, ACM, New York, NY.

Krishna, S., V. Balasubramanian, et al. (2010). Person-Specific Characteristic Feature Selection for Face Recognition. Biometrics: Theory, Methods, and Applications. N. V. Boulgouris, K. N. Plataniotis and E. Micheli-Tzanakou. **9:** 113-142.

Magalhães, S. T., R. Kenneth, et al. (2008). Using Technology to Overcome the Password's Contradiction. Handbook of Research on Social and Organizational Liabilities in Information Security. M. Gupta and R. Sharman, Information Science Reference.

Magalhães, S. T. and H. D. Santos (2003). Biometria e Autenticação. 4ª Conferência da Associação Portuguesa de Sistemas de Informação (APSI) CAPSI03, Porto, Portugal, APSI.

Maltoni, D., D. Maio, et al. (2009). Handbook of fingerprint recognition, Springer.

Mansfield, A. J. and J. L. Wayman (2002). Best practices in testing and reporting performance of biometric devices. NPL Report CMSC. **14**.

Martin, A. (2012). National Identity Infrastructures: Lessons from the United Kingdom. ICT Critical Infrastructures and Society. M. Hercheui, D. Whitehouse, W. McIver, Jr. and J. Phahlamohlaka, Springer Berlin Heidelberg. **386:** 44-55.

Matthews, T. (2012). "Passwords are not enough." Computer Fraud & Security **2012**(5): 18-20.

Neumann, P. G. (1994). "Risks of passwords." Communications of the ACM **37**(4): 126.

Newman, R. (2009). Security and Access Control Using Biometric Technologies, Course Technology Ptr.

Ratha, N. K. and V. Govindaraju, Eds. (2008). Advances in biometrics: sensors, algorithms and systems, Springer.

Reddy, A. K. (2011). "A Case Study on Iindian EVMS Using Biometrics." International Journal of Engineering Science & Advanced Technology (IJESAT) **1**(1): 40-42.

Revett, K., S. T. Magalhães, et al. (2005). Developing a Keystroke Dynamics Based Agent Using Rough Sets. International workshop on Rough Sets and Soft Computing in Intelligent Agent and web Technologies, in conjunction with the 2005 IEEE/WIC/ACM International Conference on Web Intelligence and Intelligent Agent Technology, Compiègne, France, IEEE Computer Society Press.

Richardson, R. (2011). 2010/2011 Computer Crime and Security Survey, Computer Security Institute. **XV**.

Ryan, R. (2009). "The importance of biometric standards." Biometric Technology Today **2009**(7): 7-10.

Santos, H. M. D. (2013). Engenharia da Segurança de Sistemas de Informação: Relatório da Unidade Curricular, Prova de Agregação no ramo de conhecimento de Tecnologias e Sistemas de Informação, Universidade do Minho.

Tuyls, P. and J. Goseling (2004). Capacity and Examples of Template-Protecting Biometric Authentication Systems. Biometric Authentication. D. Maltoni and A. Jain, Springer Berlin Heidelberg. **3087:** 158-170.

Vijayan, J. (2012). "Weak Passwords Still Subvert IT Security." Computerworld **46**(8): 8-8.

Wayman, J. L. (2001). "Fundamentals of biometric authentication technologies." International Journal of Image and Graphics **1**(01): 93-113.

Wayman, J. L., A. K. Jain, et al. (2005). Biometric systems: Technology, design and performance evaluation, Springer Verlag.

Yager, N. and T. Dunstone (2010). "The Biometric Menagerie." Pattern Analysis and Machine Intelligence, IEEE Transactions on **32**(2): 220-230.

Yampolskiy, R. V. and V. Govindaraju (2010). Taxonomy of behavioural biometrics. Behavioral Biometrics for Human Identification: Intelligent Applications. L. Wang and X. Geng, IGI Global**:** 1-43.

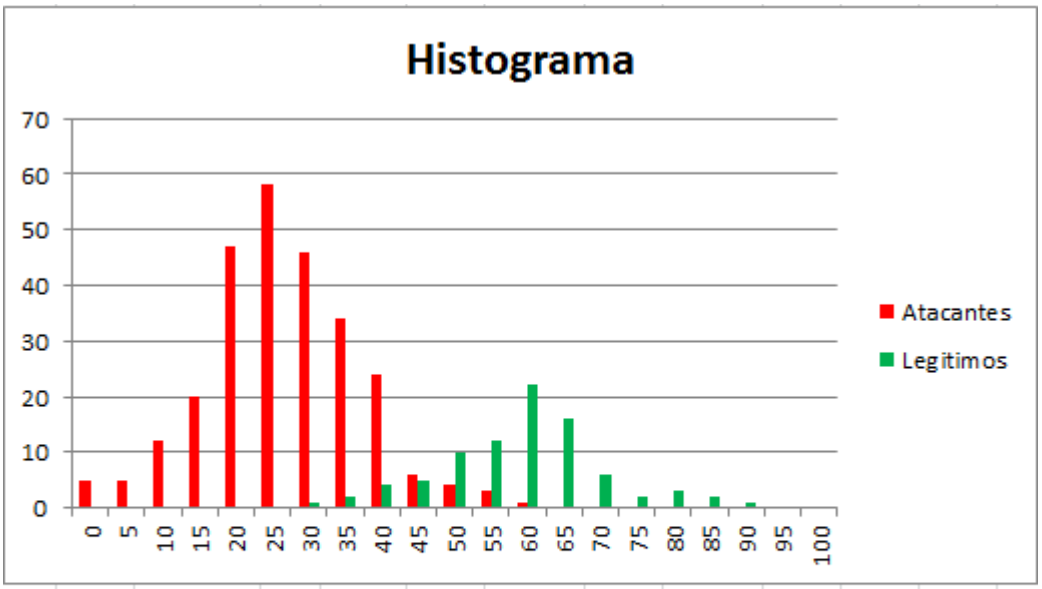
Ye, J. and S. Ji (2010). Discriminant analysis for dimensionality reduction: An overview of recent developments. Biometrics: Theory, Methods & Applications. N. V. Boulgouris, K. N. Plataniotis and E. Micheli-Tzanakou, Wiley**:** 1-20.

Zhao, W., R. Chellappa, et al. (2003). "Face recognition: A literature survey." ACM Comput. Surv. **35**(4): 399-458.

Anexo A – dados para exemplo de avaliação de biometria

Scores	0	5	10	15	20	25	30	35	40	45	50	55	60	65	70	75	80	85	90	95	100	
Atacantes	5	5	12	20	47	58	46	34	24	6	4	3	1	0	0	0	0	0	0	0	0	265
Legitimos	0	0	0	0	0	0	1	2	4	5	10	12	22	16	6	2	3	2	1	0	0	86
Atacantes	0,02	0,02	0,05	0,08	0,18	0,22	0,17	0,13	0,09	0,02	0,02	0,01	0	0	0	0	0	0	0	0	0	1
Legitimos	0	0	0	0	0	0	0,01	0,02	0,05	0,06	0,12	0,14	0,26	0,19	0,07	0,02	0,03	0,02	0,01	0	0	1
FMR	1	0,98	0,96	0,92	0,84	0,66	0,45	0,27	0,14	0,05	0,03	0,02	0	0	0	0	0	0	0	0	0	
FNMR	0	0	0	0	0	0	0,01	0,03	0,08	0,14	0,26	0,4	0,65	0,84	0,91	0,93	0,97	0,99	1	1	1	
TMR	1	1	1	1	1	1	0,99	0,97	0,92	0,86	0,74	0,6	0,35	0,16	0,09	0,07	0,03	0,01	0	0	0	
Utiliz. 1	0	0	0	0	0	0	1	2	4	5	7	6	7	4	2	1	1	0	0	0	0	40
Utiliz. 1	0	0	0	0	0	0	0,03	0,05	0,1	0,13	0,18	0,15	0,18	0,1	0,05	0,03	0,03	0	0	0	0	1
Utiliz. 2	0	0	0	0	0	0	0	0	0	0	3	6	15	12	4	1	2	2	1	0	0	46
Utiliz. 2	0	0	0	0	0	0	0	0	0	0	0,07	0,13	0,33	0,26	0,09	0,02	0,04	0,04	0,02	0	0	1

Anexo B – Histograma e variáveis estatísticas associadas



		Limiar (τ)	42									
				FM=	14	FMR=	0,05		EER=	0,11		
				FNM=	7	FNMR=	0,08					
				Mo=	93	TM=	79	TMR=	0,92	ACC=	0,94	
				NMo=	258	TNM=	251	TNMR=	0,95			