Universidade de Brasília
Instituto de Ciências Exatas
Departamento de Ciência da Computação

Computação Ubíqua

Danilo Ávila Monte Christo Ferreira
Tales Mundim Andrade Porto

Monografia apresentada como requisito parcial
para conclusão do Bacharelado em Ciência da Computação

Orientador
Prof. Dr. Carla Denise Castanho

Brasília
2011

Universidade de Brasília — UnB
Instituto de Ciências Exatas
Departamento de Ciência da Computação
Bacharelado em Ciência da Computação

Coordenador: Prof. Lamar

Banca examinadora composta por:

Prof. Dr. Carla Denise Castanho (Orientador) — CIC/UnB
Prof. Dr. Professor I — CIC/UnB
Prof. Dr. Professor II — CIC/UnB

CIP — Catalogação Internacional na Publicação

Ferreira, Danilo Ávila Monte Christo.

Computação Ubíqua / Danilo Ávila Monte Christo Ferreira, Tales Mundim Andrade Porto. Brasília : UnB, 2011.
31 p. : il. ; 29,5 cm.

Monografia (Graduação) — Universidade de Brasília, Brasília, 2011.

1. palvrachave1, 2. palvrachave2, 3. palvrachave3

CDU 004.4

Endereço: Universidade de Brasília
Campus Universitário Darcy Ribeiro — Asa Norte
CEP 70910-900
Brasília–DF — Brasil

Universidade de Brasília
Instituto de Ciências Exatas
Departamento de Ciência da Computação

Computação Ubíqua

Danilo Ávila Monte Christo Ferreira
Tales Mundim Andrade Porto

Monografia apresentada como requisito parcial
para conclusão do Bacharelado em Ciência da Computação

Prof. Dr. Carla Denise Castanho (Orientador)
CIC/UnB

Prof. Dr. Professor I
CIC/UnB

Prof. Dr. Professor II
CIC/UnB

Prof. Lamar
Coordenador do Bacharelado em Ciência da Computação

Brasília, 2 de maio de 2011

Dedicatória

Dedico a....

Agradecimentos

Agradeço a....

Resumo

A ciência...

Palavras-chave: palvrachave1, palvrachave2, palvrachave3

Abstract

The science...

Keywords: keyword1, keyword2, keyword3

Sumário

Lista de Figuras

Lista de Tabelas

Capítulo 1

Introdução

A computação ubíqua a tempos vem sendo tema de diversas pesquisas ao redor do mundo. Mark Weiser diz que o computador do futuro deve ser algo invisível (11, 12), o que proporciona ao usuário um melhor foco na tarefa e não na ferramenta. A computação ubíqua tenta atribuir a invisibilidade aos computadores. Como aconteceu com o motor, o computador também vive um momento "down-size", diminuindo cada vez mais o seu tamanho e se acoplando aos objetos do dia-a-dia.

O SmartSpace é um ambiente onde a computação ubíqua acontece em sua totalidade (1). Esse ambiente provê ao usuário uma melhor forma de interagir com os computadores usando diversas tecnologias que estimulam a interatividade natural. Tais tecnologias são capazes de fornecer inteligência, ao SmartSpace, necessária para concretizar a visão da ubicomp (4).

Para conseguir uma boa interação entre as diversas peças que compõem o SmartSpace é necessário que se tenha a disposição informações de contexto, como quem está no ambiente, onde está, o que está fazendo e outras que ajudam o sistema a definir o melhor ajuste dos equipamentos. Com uma base rica de informações de contexto, contendo os perfis dos usuários, garantimos uma maior acurácia na tomada de decisões. Informações de contexto como essas são complicadas de se obter devido a alta dinamicidade do ambiente, no qual usuários entram e saem a todo momento e interagem com diversos equipamentos.

A identificação de usuário em um SmartSpace é feita por meio de sistema de reconhecimento automático. Há alguns anos, um grande número de pesquisas vem sendo desenvolvidas para criação sistemas deste tipo (3). Um dos motivos clássicos é que os métodos baseados em cartões de identificação e senhas não são altamente confiáveis. Estes podem ser perdidos, extraviados e até fraudados (10).

Um ambiente ubíquo capaz de reconhecer seus usuários, pode prover uma personalização automática do ambiente de acordo com as prefrências de cada usuário e até mesmo prover um ambiente mais seguro com controle de acesso físico e prevenção de fraudes (3). Atualmente, os métodos de reconhecimento mais utilizados são baseados no uso de cartões magnéticos e senhas, que requerem sua utilização durante uma transação, mas que não verificam sua idoneidade (5).

Hoje em dia, várias técnicas de reconhecimento por meio de faces, íris, voz, entre outras, vêm sendo estudadas e utilizadas em sistemas de reconhecimento automático (10). O reconhecimento facial pode ser considerada como uma das principais funções do ser humano pois permite identificar uma grande quantidade de faces e aspectos psicológi-

cos demonstrados pela fisionomia. Pode ser considerada, também, como um problema clássico da visão artificial pela complexidade existente na detecção e reconhecimento de características e padrões (3).

O reconhecimento facial vem se desenvolvendo junto a "quarta geração"de computadores através de sua aplicação na nova geração de interfaces que consiste na detecção e reconhecimento de pessoas (3).

É proposta então uma solução para o problema de localização e identificação de perfis de usuários em um SmartSpace utilizando como base o middleware UbiquitOS (6) integrado com o Kinect.

1.1 Organização do trabalho

Explicar a estrutura da monografia.

Capítulo 2

Reconhecimento Facial

Algo explicando o que terá nesse capítulo.

2.1 Biometria

As abordagens de identificação pessoal que utilizam "alguma coisa que você sabe", como Número de Indetificação Pessoal (PIN - "Personal Identification Number"), ou "alguma coisa que você tenha", como um cartão de identificação, não são confiáveis o suficiente para satisfazer os requisitos de segurança de um sistema de transações eletrônicas porque não têm a capacidade de diferenciar um usuário legítimo de um impostor que adiquiriu de forma ilegal o privilégio de acesso (8). Esta fragilidade pode ser evitada se utilzarmos o nosso corpo como chave do sistema. Alguns traços fisícos ou comportamentais são muito mais complicados de serem forjados que uma cadeia de caracteres (7).

Biometria é uma tecnologia utilizada para identificação de um indivíduo baseado em suas características físicas ou comportamentais, baseia-se em "alguma coisa que você é ou faz" para realizar a identificação e, por isso, tem a capacidade de diferenciar entre um indivíduo legítimo de um impostor (8). As características físicas estão relacionadas a composição do corpo humano e seu formato e as comportamentais estão relacionadas ao comportamento das pessoas (7). A figura 2.1contém alguns exemplos desses dois tipos diferentes de características biométricas.

Teoricamente, qualquer característica física/comportamental pode ser utilizada para identificação caso siga alguns dos seguintes requisitos (2):

1. **universidade**: qualquer pessoa pode ser avaliada sobre essa característica;
2. **singularidade**: dada duas pessoas distinas, elas não podem ter a mesma característica;
3. **permanência**: a característica não pode mudar de acordo com o tempo;
4. **exigibilidade**: significa que a característica pode ser mensurada quantitativamente;

Porém, na prática também são considerados outros requisitos (2):

1. **desempenho**: o processo de identificação deve apresentar um resultado aceitável;

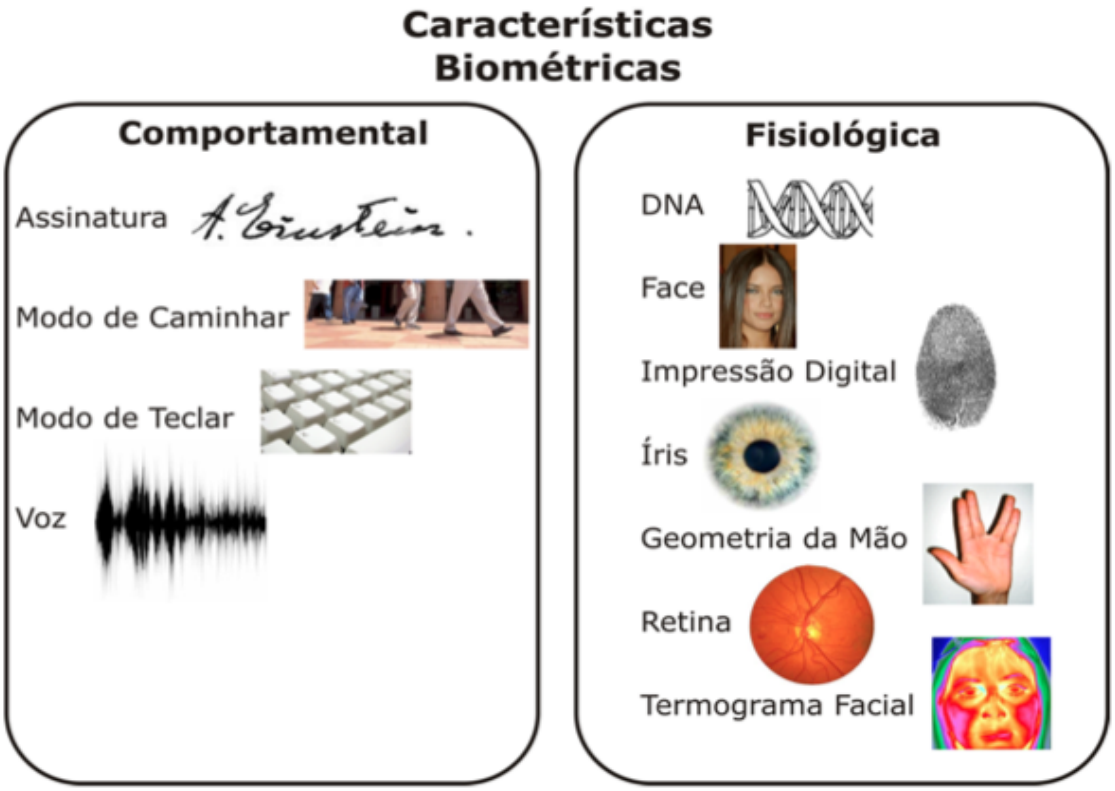

Figura 2.1: Exemplos de algumas características biométricas (7).

2. **aceitação**: indica em que ponto as pessoas estão dispostas a aceitar o sistema biométrico;
3. **evasão**: refere a facilidade de ser adulterado;

São várias as vatangens que os sistemas biométricos têm em relação aos sistemas convencionais. Listamos as vatagens vistas como principais (7):

- características biométricas não podem ser perdidas ou esquecidas;
- características biométricas são difíceis de serem copiadas, compartilhadas e distribuídas;
- os sistemas biométricos necessitam que a pessoa esteja presente no local da autenticação;

Na prática um sistema biométrico deve ser capaz de (8):

1. atiginr uma acurácia aceitável e com uma velocidade razoável;
2. não ser prejudiciável pelos indivíduos e ser aceito pela população alvo;
3. ser suficientemente robusto para vários métodos fraudulentos;

Novas técnicas de reconhecimento por meio de faces, íris, retina e voz, entre outras, têm sido abordadas para aplicações em sistemas de reconhecimento automático (3, 10). O reconhecimento facial é apenas uma das nove características biométricas utilizadas atualmente (2). Nas tabelas 2.1 e 2.2 são mostradadas as noves características e seus respectivos comportamentos baseados nos requisitos mencionados acima.

Tabela 2.1: Requisitos teóricos para algoritmos de reconhecimento facial (2).

Biometria	**Universidade**	**Singularidade**	**Permanência**	**Exigibilidade**
Face	Alta	Baixa	Média	Alta
Digital	Média	Alta	Alta	Média
Geometria da Mão	Média	Média	Média	Alta
"Hand Vein"	Média	Média	Média	Média
Iris	Alta	Alta	Alta	Média
"Retina Scan"	Alta	Alta	Média	Baixa
Assinatura	Baixa	Baixa	Baixa	Alta
Voz	Média	Baixa	Baixa	Média
Termograma	Alta	Alta	Baixa	Alta

Tabela 2.2: Requisitos práticos para algoritmos de reconhecimento facial (2).

Biometria	**Desempenho**	**Aceitação**	**Evasão**
Face	Baixa	Alta	Baixa
Digital	Alta	Média	Alta
Geometria da Mão	Média	Média	Média
"Hand Vein"	Média	Média	Alta
Iris	Média	Média	Alta
"Retina Scan"	Alta	Baixa	Alta
Assinatura	Baixa	Alta	Baixa
Voz	Baixa	Alta	Baixa
Termograma	Média	Alta	Alta

Os sistemas biométricos podem ser classificados em sistemas de verificação ou identificação. Sistemas de verificação são aqueles que autenticam a identidade dos usuários comparando-os com os próprios templates. Eles conduzem uma comparação "um para um" e determinam se o usuário é quem realmente diz ser. O maior desáfio para esse tipo de sistema é a acurácia. Geralmente, não é muito difícil satisfazer o requisito de tempo de resposta pois somente uma comparação "um para um" é feita (8).

Sistemas de identificação reconhecem um indivíduo pesquisando em todo o banco de dados procurando por uma correspondência. Eles conduzem uma comparação "um para muitos" para estabelecer a identidade do indivíduo. Ao contrátio dos sistemas de verificação, nesse tipo de sistema tanto a acurácia quanto o tempo são os grandes desafios, por causa da necessidade de explorar todo o banco de dados. Geralmente, é muito mais difícil desenvolver um sistemas de identificação que um de verificação (8).

Um sistema biométrico responde a dois eventos: um usuário é ou não quem afirma ser. Como resposta a esses eventos, o sistema pode classificar o usuário como um cliente ou um impostor. Nessa tomada de decisão pode ocorrer dois tipos de erros: uma falsa aceitação, ao aceitar um impostor, (*False Acceptance* - FA) ou uma falsa rejeição (*False Rejection* - FR), ao rejeitar um cliente. Baseado nesses erros, duas taxas são utilizadas para avaliar sistemas biométricos: taxa de falsa aceitação (*False Acceptance Rate* - FAR) e taxa de falsa rejeição (*False Rejection Rate* - FRR) (7).

A FAR é a probabilidade de um sistema biométrico aceitar um impostor como cliente. Ela é calculada pela equação (2.1) em que Nfa é o número de falsas aceitações e Ni é o número de impostores que tentaram acessar o sistema. A variação da taxa é representada pelo intervalo fechado $[0, 1]$, onde o valor 1 significa que todos os impostores foram falsamente aceitos e o valor 0 significa que todos impostores foram identificados como tao. Logo quando menor o FAR mais seguro o sistema é (7).

$$FAR = \frac{Nfa}{Ni}(7) \tag{2.1}$$

A FRR é a probabilidade de um sistema biométrico rejeitar um cliente e classifica-lo como impostor. Ela é calculada pela equação (2.2) em que Nfr é o número de falsas rejeições e Nc é o número de clientes que tentaram acessar o sistema. A variação da taxa é representada pelo intervalo fechado $[0, 1]$, onde o valor 1 significa que todos os clientes foram falsamente rejeitados e o valor 0 significa que todo os cliente foram aceitos corretamente. Em sistemas cuja performance tem maior grau de prioridade que a segurança, deve-se reduzir a FRR para minimizar a ocorrência de falsas rejeições (7).

$$FRR = \frac{Nfr}{Nc}(7) \tag{2.2}$$

A partir dessas taxas de erro, pode-se obter outras medidas como a *Equal Error Rate* (ERR). Esta corresponde a taxa de erro na qual a tanto a FAR quanto a FRR possuem o mesmo valor. Como diferentes sistemas têm comportamentos diferentes, a ERR normalmente é utilizada para uma comparação mais rigorosa entre o sistemas. Quanto menor for a ERR, mas presciso é considerado o sistema (7).

2.2 Reconhecimento Facial

O reconhecimento facial é uma das atividades mais comuns realizadas diariamente por seres vivos dotados de certa inteligência. Esta atividade corriqueira vem despertando o interesse de pesquisadores que trabalham com Visão Computacional e Inteligência Artificial. O objetivo desses pesquisadores é de construir sistemas artificiais capazes de realizar o reconhecimento de faces humanas e a partir desta capacidade construir os mais diferentes tipos de aplicações: sistemas de vigilância, controles de acesso, definções automáticas de perfis, entre outros (9).

Um dos motivos que icentivou os diversos estudos sobre reconhecimento facial são as vantagens que o mesmo possui em relação a impressão digital e a íris. No reconhecimento por impressão digital, a desvantagem consiste no fato que nem todas as pessoas possuem uma impressão digital com "qualidade" suficiente para ser reconhecida por um sistema. Já o reconhecimento por íris apresenta uma alta confiabilidade e larga variação, sendo

estável pela vida toda. Porém, a desvantagem está relacionada ao modo de captura da íris que necessita de uma alinhamento entre a câmera e os olhos da pessoa (3).

Basicamnente existem duas particularidades que fazem da face uma característica biométrica bastante atrativa (7):

1. A aquisição da face é feita de forma fácil e não-intrusiva;
2. Possui uma baixa privacidade de informação: como a face é exposta constantemente, caso uma base de faces seja roubada, essas informações não representam algum risco e não possibilitam um uso impróprio;

Umas das maiores dificuldades dos sistemas de reconhecimento é tratar a complexidade dos padrões visuais. Mesmo sabendo que todas as faces possuem padrões reconhecidos, como boca, olhos e nariz, elas também possuem variações únicas que devem ser utilizadas para determinar as características relevantes. Outra dificuldade encontrada em relação a essas características é que elas possuem uma larga variação estatística para serem consideradas únicas para cada indivíduo. O ideal seria que a variância inter-classe seja grande e a intra-classe pequena, pois assim imagens de diferentes faces geram os códigos mais diferentes possíveis, enquanto imagens de uma mesma face geram os códigos mais similares possíveis. Portanto, estabelecer uma representação que capture as características ideias é um difícil problema (3).

Entre os mais diferentes problemas encontrados nas tarefas envolvendo o reconhecimento facial, destacamos os mais comuns (3):

- iluminação;
- ângulos e poses;
- expressões;
- comésticos e acessórios;
- extração da face do contexto ou do fundo;

No anos 70, os estudos do reconhecimento facial eram baseados sobre atributos faciais mensuráveis como olhos, nariz, sobrancelhas, bocas, entre outros. Porém, os recursos computacionais eram escassos e os algoritmos de extração de características eram ineficiêntes. Então, as pesquisas na área ressurgiram nos anos 90, inovando os métodos existentes (3, 8).

Referências

[1] G. Abowd, C. Atkeson, and I. Essa. Ubiquitous smart spaces. *A white paper submitted to DARPA (in response to RFI)*, 1998. 1

[2] M. Arantes, A. N. Ide, and J. H. Saito. A system for fingerprint minutiae classification and recognition. In *Proceedings of the 9th International Conference on Neural Information Processing(ICONIP'O2)*, volume 5, pages 2474 – 2478. vii, 3, 5

[3] Â. R. Bianchini. Arquitetura de redes neurais para o reconhecimento facial baseado no neocognitron. Master's thesis, São Carlos, http://www.bdtd.ufscar.br/htdocs/tedeSimplificado//tde_busca/arquivo.php?codArquivo=164, 2001. 1, 2, 5, 7

[4] F. N. Buzeto. Um conjunto de soluções para a construção de aplicativos de computação ubíqua. Master's thesis, Universidade de Brasília, 2010. 1

[5] J. Daugman. Face and gesture recognition: Overview. *IEEE TRANSACTIONS ON PATTERN ANALYSIS AND MACHINE INTELLIGENCE*, 19(7), 1997. 1

[6] A. R. Gomes. Ubiquitos – uma proposta de arquitetura de middleware para a adaptabilidade de serviços em sistemas de computação ubíqua. Master's thesis, Universidade de Brasília; Departamento de Ciência da Computação, http://monografias.cic.unb.br/dspace/handle/123456789/110, 2007. 2

[7] S. A. D. Junior. Reconhecimento facial 3d utilizando o simulated annealing com as medidas surface interpenetration measure e m-estimator sample consensus. Master's thesis, Universidade Federal do Paraná, 2007. vi, 3, 4, 6, 7

[8] Hong L. and Jain A. Integrating faces and fingerprints for personal identification. *IEEE Transactions on Pattern and Machine Intelligence*, 20(12):1295–1307, dezembro 1998. 3, 4, 5, 7

[9] D. R. Oliveira. Reconhecimento de faces usando redes neurais e biometria. Master's thesis, INPE, 2006. 6

[10] S. Pankanti, R. M. Bolle, and A. Jain. Biometrics: The future of identification, 2000. 1, 5

[11] M. Weiser. The computer for the 21st century. *Scientific American*, 1991. 1

[12] M. Weiser. The world is not a desktop. *ACM Interactions*, 1993. 1