PROPOSTA DE DUPLO SISTEMA BIOMÉTRICO PARA REDUÇÃO DE FRAUDES EM SISTEMAS DE AUTENTICAÇÃO DE IMPRESSÃO DIGITAL

Gilson Torres Dias
gilson@maempec.com.br
Oswaldo Ortiz Fernandes Junior
oswaldo@imes.edu.br
Universidade IMES – São Caetano do Sul - SP

Resumo

Os sistemas biométricos surgiram para permitir o desenvolvimento de sistemas de identificação de indivíduos com maior segurança e minimizar os problemas encontrados nos métodos tradicionais de identificação (senhas e cartões). Os mesmos identificam indivíduos com base em suas características físicas ou comportamentais. Dentre as características que podem ser analisadas, as impressões digitais tem se destacado no contexto de reconhecimento de indivíduos por ser um dos métodos mais simples de se implantar, necessitar de menores custos de investimento, apresentar resultados satisfatórios de segurança e ser uma das técnicas mais antigas no reconhecimento de indivíduos. Devido à sua facilidade de implantação e grande difusão, também é um dos mais fraudáveis. Propõe-se através desse trabalho, uma forma de reduzir ao mínimo a possibilidade de fraude através de uma verificação ao sistema de identificação digital.

1. Introdução

O reconhecimento por impressões digitais é um dos sistemas biométricos mais utilizados e apresenta como vantagem na sua utilização o baixo custo de implantação. Entretanto tal sistema de identificação é vulnerável a fraudes que também podem ser realizadas sem grandes esforços [1]. Porém, o reconhecimento por impressões digitais não deve ser descartado em função de suas fragilidades quanto à possibilidade de fraudes, ao contrário, ainda poderíamos pensar em soluções alternativas e complementares capazes de restringi-las. Outros tipos de sistemas biométricos, por exemplo, poderiam ser utilizados como agentes de verificação de uma identificação realizada por reconhecimento de impressões digitais.

Do ponto de vista da segurança, biometria significa a verificação da identidade de uma pessoa através de uma característica única inerente a essa pessoa. Essa característica pessoal pode ser tanto fisiológica (como uma impressão digital ou características faciais) ou comportamental (como a assinatura manuscrita ou uma amostra de voz).

2. Registro, Identificação e Validação

O mecanismo de autenticação por biometria pode ser dividido nos seguintes processos: registro, identificação e validação. Inicialmente na biometria, cada usuário deve ser registrado pelo administrador do sistema. O processo de registro consiste no armazenamento de uma característica biológica do individuo (física ou comportamental) para ser usada, posteriormente, na identificação do usuário.

A característica biológica é tipicamente adquirida por um dispositivo de hardware, o qual está no *front-end* do mecanismo de autenticação por biometria. O componente do *front-end* para estes sistemas é um dispositivo conhecido como sensor. Quando uma característica física é apresentada ao sensor, ele produz um sinal que é modulado em resposta as variações da quantidade física sendo medida. Se, por exemplo, o sensor for um microfone usado para capturar um padrão de voz, ele ira produzir um sinal cuja amplitude varia com o tempo em resposta a variação da freqüência em uma frase falada.

Pelo fato dos sinais produzidos pela maior parte dos sensores serem analógicos por natureza, é necessário converter estes sinais para digitais, para que possam ser processados por um computador. Ao invés de usar todos os dados do sensor, os sistemas biométricos freqüentemente processam estes dados para extrair apenas as informações relevantes ao processo de autenticação. Uma vez que a representação digital foi processada para o ponto desejado, ela é armazenada. A característica biológica armazenada na forma digital é chamada de *template* (modelo). Muitos dispositivos biométricos capturam amostras múltiplas durante o processo de

registro para contabilizar graus de variação na medida destas características. Uma vez que o usuário esta registrado, os dispositivos biométricos são usados na identificação do usuário. Quando o usuário necessita ser autenticado, sua característica física é capturada pelo sensor. A informação analógica do sensor é então convertida para sua representação digital. A seguir, esta representação digital é comparada com o modelo biométrico armazenado. A representação digital utilizada na identificação é chamada de *live scan* (amostra). A amostra, tipicamente, não confere exatamente com o modelo armazenado. Como geralmente há alguma variação na medida, estes sistemas não podem exigir uma comparação exata entre o modelo original armazenado e a amostra corrente. Ao invés disso, a amostra corrente é considerada válida se estiver dentro de um certo intervalo estatístico de valores. Um algoritmo de comparação é usado para determinar se um usuário quando identificado é o mesmo que foi registrado.

Além da identificação, um processo complementar é o de validação. Neste caso, após a identificação do indivíduo, o conjunto de características associado ao mesmo pode ser novamente verificado por um algoritmo complementar ou outra metodologia pertinente, capaz de confirmar a identidade.

O algoritmo de comparação produz um resultado de quão perto a representação digital esta do modelo armazenado. Se o resultado for um valor aceitável, uma resposta afirmativa é dada. A aceitação difere para cada dispositivo biométrico. Para alguns, o administrador do sistema pode configurar o nível do valor de aceitação. Se este nível for muito baixo, o dispositivo biométrico falha por ser um mecanismo de autenticação válido. Se este nível for muito alto, os usuários podem ter problemas na autenticação.
Impressão digital: requer um dispositivo capaz de capturar, com um bom grau de precisão, os traços que definem a impressão dos dedos, além de um programa que trate a imagem capturada e faça o reconhecimento da digital.

2.2 Impressões Digitais

As impressões digitais, marcas presentes nas pontas dos dedos dos seres humanos, podem ser utilizadas para identificação de pessoas, já que dois seres humanos nunca possuem as mesmas digitais, nem mesmo irmãos gêmeos, e estes sinais em geral permanecem inalterados durante a vida de um indivíduo, exceto por ocorrência de lesões ou degeneração.

Esse fato possibilitou a utilização das impressões digitais para a identificação de pessoas.

Uma aplicação clássica é a identificação de criminosos pela polícia, através das digitais deixadas em locais de crime. Podemos também utilizar as digitais em sistemas de segurança, para liberar ou negar acesso a uma área restrita (um centro de alta segurança ou um edifício, por exemplo), ou para efetuar uma operação de *login* num sistema computacional.

Quando as impressões digitais começaram a ser utilizadas para identificação de pessoas, o reconhecimento era feito apenas manualmente, o que tornava o processo muito custoso, pois era necessário um especialista nesse tipo de aplicação para realizar o reconhecimento e as impressões digitais são estruturas com muitos detalhes, o que exigia muito tempo para verificar as particularidades existentes.

Devido a essas dificuldades, iniciaram-se diversos estudos de técnicas para acelerar este reconhecimento com auxílio computacional, e fazê-lo de forma automática, sem a necessidade de um especialista na área. Isto serviu como motivação para a criação de diversos sistemas para identificação automática de pessoas.

2.2. Minúcias

O ponto principal de análise das impressões digitais, são as minúcias, que são na verdade, pontos característicos das impressões que garantem a unicidade e individualidade da impressão digital.

As minúcias são aspectos que se encontram nas cristas papilares, como por exemplo, linhas que terminam abruptamente ou se bifurcam, e são consideradas na autenticação e definem a unicidade das impressões digitais.

As minúcias ou pontos característicos, são resumidamente classificadas dentro de duas categorias: aspectos básicos e compostos.

Os aspectos básicos são: cristas finas e cristas bifurcadas. Os aspectos compostos são: ilhas, cristas curtas, espora, cruzamento.

Os aspectos compostos são compostos a partir dos aspectos básicos, e a partir dos básicos encontram-se todos os outros.

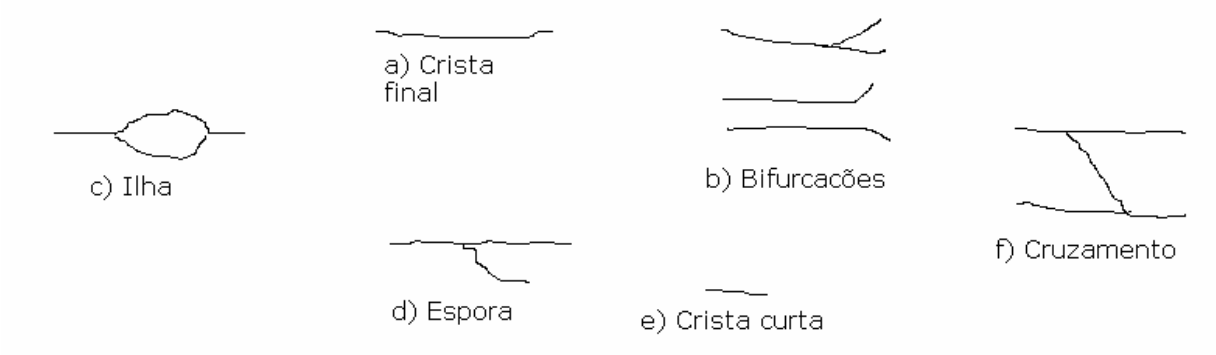

Figura 1 – Aspectos das minúcias

Fonte: COSTA 2000

3. Falsa Aceitação e Falsa Rejeição

Na escolha de um sistema de autenticação biométrico, o desempenho deve ser levado em conta. Este pode ser categorizado por duas medidas: a taxa de falsa aceitação (FAR – *False Acceptance Rate*) e a taxa de falsa rejeição (FRR - *False Rejection Rate*). A FAR, também chamada de erros do tipo 2, representa a percentagem de usuários não-autorizados que são incorretamente identificados como usuários válidos.

A FRR, também chamada de erros do tipo 1, representa a percentagem de usuários autorizados que são incorretamente rejeitados (7).

O nível de precisão configurado no algoritmo de comparação tem efeito direto nessas taxas. O modo como estas são determinadas é fundamental para a operação de qualquer sistema biométrico e assim deve ser considerado um fator primário na avaliação de sistemas biométricos. Deve-se ter cuidado com os números de FRR e FAR dos fabricantes, porque estes são extrapolados por pequenos conjuntos de usuários e a condição de extrapolação é, algumas vezes, errada (6). Os dispositivos biométricos físicos tendem a ter uma melhor taxa de falsa aceitação por causa da estabilidade da característica medida e porque as características comportamentais são mais fáceis de serem duplicadas por outros usuários. A configuração do valor limite para tolerância a estes erros é critica no desempenho do sistema. A falsa rejeição causa frustração e a falsa aceitação causa fraude. Muitos sistemas podem ser configurados para fornecer detecção sensível (baixa FAR e alta FRR) ou detecção fraca (baixa FRR e alta FAR). A medida crítica é conhecida como taxa de cruzamento (*crossover rate*). Ela é o ponto onde o FAR e o FRR cruzam-se. Muitos sistemas biométricos comerciais tem taxas de cruzamento abaixo de 0,2%, e alguns abaixo de 0,1%. A taxa aumenta com a freqüência do uso, com os usuários acostumando-se com o sistema e o sistema tornando-se mais afinado com o nível de variação esperado.

As taxas FAR e FRR podem ser obtidas através de protocolos de uma tentativa ou três tentativas.

No protocolo uma tentativa os usuários tem apenas uma chance de passar no teste biométrico. Os dados são coletados em apenas uma oportunidade e então são analisados. A partir disso vem a rejeição ou aceitação. No três tentativas, o usuário tem ate três chances antes que seja definitivamente rejeitado. Se as medidas consecutivas são estatisticamente independentes, isto melhora a FRR sem, no entanto, deteriorar a FAR. Entretanto, dependendo do tipo de aplicação, este protocolo de três tentativas pode não ser aceitável por uma questão de tempo ou ate mesmo por conveniência (8).

4. Processo de tentativa de fraude

A escolha da gelatina em pó para a construção das películas baseou-se na leitura de um trabalho do pesquisador japonês Tsutomu Matsumoto e colegas [Impact of Artificial "Gummy" Fingers on Fingerprint Systems, 2002] demonstraram que a película de gelatina apresenta algumas características muito próximas às da pele humana viva. Enquanto a gelatina apresenta umidade de 23% e resistência elétrica de 20Mohms/cm, a pele viva apresenta 16% de umidade e 16Mohms/cm de resistência.

5. Proposta de Solução

Uma proposta capaz de tornar o reconhecimento de impressões digitais uma técnica mais segura é a utilização de um segundo sistema biométrico que teria a função de validar o indivíduo após a sua autenticação por impressões digitais. A grande vantagem aqui observada é de que no processo de validação o custo de tempo de busca no banco de dados de informações é baixo, permitindo assim a utilização de técnicas complementares ainda que estas envolvam custos computacionais maiores em seus algoritmos de reconhecimento.
A identificação do indivíduo seria realizada pelo sistema de reconhecimento por impressões digitais. A partir da identificação o segundo sistema biométrico realizaria a etapa de validação, restringindo assim drasticamente as possíveis tentativas de fraude. Os sistemas, na fase de captura, trabalham de forma paralela, e após a identificação, busca a segunda característica biométrica no registro identificado com o objetivo de validar o indivíduo.
No momento que este artigo estava sendo escrito, dois duplos sistemas biométricos estavam sendo implementados com o objetivo de validar o sistema de identificação digital, e posteriormente serem comparados entre si.

REFERÊNCIAS BIBLIOGRÁFICAS

[1] Fernandes Jr, Oswaldo O. et al, É possível Fraudar Scanners de Impressões Digitais? – 5º. Congresso Internacional de Sistemas de Instrumentação, Automação e Contrôle – Isashow 2005 – São Paulo – SP.