Estudo e Implementação de um Sistema Biométrico Multimodal com Lógica Nebulosa

Jennifer Chuin Lee, Andréa Akiko Fugimoto Ynui e Lee Luan Ling

***Resumo* - Este artigo apresenta a implementação de um sistema biométrico multimodal que é a fusão de biometrias para a verificação de identidade, utilizando Lógica Nebulosa. Deste modo, a fusão processa os dados e parâmetros de sistemas unimodais, produzindo resultados satisfatórios de reconhecimento.**

***Palavras-Chave* – Sistema Multimodal, Lógica Nebulosa, Biometria.**

***Abstract* - This paper presents an implementation of a multimodal biometric system, which combines biometrics for identity verification, using Fuzzy Logic. Therefore, it processes unimodal systems data e parameters, which produces significant recognition results.**

***Keywords* – Multimodal System, Fuzzy Logic, Biometrics.**

I. INTRODUÇÂO

A tecnologia de biométrica é baseada no reconhecimento de características físicas do individuo, e garante mais segurança de identificação pessoal do que a autenticação por meio de objetos como cartões e chaves, ou senhas. No entanto, a biometria não apresenta resultados que são 100% efetivos para a identificação do individuo, podendo haver muitos fatores que comprometam no reconhecimento biométrico, como por exemplo, imperfeições na imagem ou mudanças fisiológicas. Portanto para que sejam minimizados os erros que interferem na decisão da identificação do individuo (genuíno ou impostor), a melhor solução é a utilização de sistemas multimodais. Neste artigo, o sistema multimodal apresenta a arquitetura de sistemas unimodais de forma paralela, em que cada sistema biométrico atua independentemente e seus dados são combinados utilizando a Lógica Nebulosa, com o método [1], para que essas informações sejam tratadas, gerando uma única saída de decisão.

Este trabalho é baseado na dissertação de mestrado concluída pelo Ricardo Nagel Rodrigues (Tese de Mestrado base) [2].

II. MÉTODOS E RESULTADOS

Para que fosse feita uma análise primária de um sistema multimodal envolvendo três biometrias, foram propostas regras nebulosas para o módulo de fusão.

A. Regras Nebulosas

Primeiramente, é oferecida uma amostra biometria de cada sistema unimodal *i*.

Lee Luan Ling, Andréa Akiko Fugimoto Ynui e Jennifer Chuin Lee, Faculdade de Engenharia Elétrica e de Computação, Universidade Estadual de Campinas, Campinas, Brasil, E-mails: lee@decom.fee.unicamp.br, jennifer.chuin.lee@gmail.com. Este trabalho foi parcialmente financiado pelo CNPq.

Estas amostras são utilizadas para extrair características v_i, e assim, serão comparadas com modelos que foram previamente armazenados no banco de dados, gerando índices de similaridade s_i.

Paralelamente, analisamos cada amostra biométrica o módulo de análise de confiabilidade, que gera o parâmetro r_i, indicando o quão confiável é o índice de similaridade s_i. O parâmetro c_i é um valor fixo que relaciona com o nível de segurança de cada sistema unimodal *i*. Todos os parâmetros serão usados pelo módulo de fusão, implementado através de um sistema de inferência nebulosa, parar gerar um único índice de similaridade s_F. Este índice é usado pelo modulo de decisão para decidir se o usuário é genuíno ou impostor.

Para evitar que amostras não-confiáveis influenciem negativamente na identificação de um individuo, é utilizado o índice de confiabilidade r_i. As amostras biométricas podem apresentar baixa qualidade, ou porque a qualidade do sensor é ruim, ou quando a biometria não é tão distinta para um individuo quanto para outro. Para fazer o mapeamento deste parâmetro, foi utilizada a função Min-Max.

$$r_i^{alto} = \frac{r_i - \min(R_i)}{\max(R_i) - \min(R_i)}$$

onde R_i representa o domínio da variável r_i; min (R_i) e max (R_i) representam o valor mínimo e máximo deste domínio, respectivamente. Por definição, tem-se $r_i^{baixo} = 1 - r_i^{alto}$.

O índice de segurança, c_i, revela quão fácil (ou difícil) é fraudar o sistema. Este parâmetro é restringido ao intervalo [0,1], onde 0 representa o menor nível de segurança e 1, o maior. Portanto o mapeamento pode ser feito através da equação $c_i^{alto} = c_i$. Como no caso anterior, $c_i^{baixo} = 1 - c_i^{alto}$.

Para o índice de similaridade s_i, a função utilizada é a mesma proposta na Tese de Mestrado base [2]:

$$s_i^{alto} = \min\left[1, \max\left(0, \frac{s_i - s_{i,ZeroFRR}}{s_{i,ZeroFAR} - s_{i,ZeroFRR}}\right)\right]$$

onde $s_{i,ZeroFRR}$ e $s_{i,ZeroFAR}$ são os pontos onde as taxas de falsa rejeição e aceitação, respectivamente, são zero. Novamente, $s_i^{baixo} = 1 - s_i^{alto}$.

No processo de obter uma única saída, os resultados obtidos após a aplicação de cada uma das regras gera uma variável de saída s_F (escalar) que possui três valores lingüísticos: *baixo*, *médio* e *alto*. Esta variável é gerada através da média ponderada das regras nebulosas. Como o método utilizado é do tipo [1], os valores lingüísticos serão constantes, de modo que:

$$s_F^{alto} = 1, \quad s_F^{médio} = 0.5 \quad e \quad s_F^{baixo} = 0$$

Quanto maior o valor, maior a certeza de que o indivíduo deve ser autenticado.

As regras nebulosas descrevem relações entre variáveis lingüísticas através de do tipo: SE < >, ENTÃO< >. As regras nebulosas terão a seguinte sintaxe [1]:

Se *variável lingüística* é *valor lingüístico*, **então** *saída = k*

onde k é uma constante.

A principal lógica utilizada para a formação das regras é que amostras com baixo índice de confiabilidade (baixa qualidade) devem ter um peso menor na decisão final e sistemas com baixo nível de segurança só podem influenciar na autenticação de uma pessoa caso um sistema de alta segurança também indique que o usuário é autêntico.

B. Casos de Regras Nebulosas

Para o estudo deste sistema biométrico composto pela fusão de três biometrias, foi feita uma análise considerando-se que as biometrias utilizadas podem assumir dois níveis de segurança: alto ou baixo. As biometrias mais utilizadas são classificadas, segundo o parâmetro segurança, de acordo com a Tabela 1. Assumiu-se a existência de quatro casos a serem analisados, ou seja, quatro conjuntos de regras nebulosas, definidos de acordo com as possíveis combinações do parâmetro segurança de cada biometria.

TABELA 1:

c_i alto	**c_i baixo**
Íris	Dinâmica de Digitação
Impressão Digital	Face
DNA	Assinatura
Impressão da palma da mão	Voz

- Caso 1: c_1 baixo, c_2 baixo e c_3 baixo,
- Caso 2: c_1 alto, c_2 alto e c_3 alto,
- Caso 3: c_1 alto, c_2 alto e c_3 baixo,
- Caso 4: c_1 baixo, c_2 baixo e c_3 alto.

De modo geral, para os quatro casos citados acima, definiram-se as regras considerando duas variáveis que levam em conta certas características como segurança, idade do vetor modelo e qualidade de uma amostra capturada por sensores.

Os 4 casos possíveis de combinações são descritos a seguir.

Caso 1: Considerando que as três biometrias do sistema apresentam nível baixo de segurança, foram implementadas as 19 regras nebulosas, mutuamente exclusivas. Quando duas biometrias são consideradas não confiáveis, a decisão final é influenciada pela terceira biometria. No entanto, ainda deve-se considerar que, neste caso, nenhuma biometria é segura. Quando as três biometrias não são confiáveis, a saída s_F é baixa, de modo que não podemos confiar num resultado que acusa um genuíno. Neste caso, leva-se em conta a pior situação, em que o usuário é um impostor.

Caso 2: Considerando que as três biometrias do sistema apresentam nível alto de segurança, foram implementadas as 25 regras nebulosas, mutuamente exclusivas. Como as três biometrias apresentam o mesmo grau de confiabilidade, a decisão de s_F ficou a critério de s_i e r_i. Este é um sistema recomendável para aplicações onde se requer alto grau de segurança. Se for mantido um alto grau de confiabilidade o sistema operará de forma esperada, ou seja, se o usuário for genuíno, o sistema biométrico acusará usuário genuíno, caso contrário, o acusará impostor.

Caso 3: Considerando que duas das três biometrias do sistema apresentam nível alto de segurança, foram implementadas 13 regras nebulosas, mutuamente exclusivas. Neste caso, considerou-se c_1 alto, c_2 alto e c_3 baixo, sem perda de generalidade. Implementando as regras nebulosas com estas características, o peso da biometria 3 na decisão final de s_F passa a ser considerado somente quando as biometrias 1 e 2 se contradizem (quando uma acusa usuário genuíno e a outra, impostor) ou não são capazes de decidir uma saída adequada para s_F.

Caso 4: Considerando que duas das três biometrias do sistema apresentam nível baixo de segurança, foram implementadas 19 regras nebulosas, mutuamente exclusivas. Novamente, sem nenhuma perda de generalidade, considerou-se c_1 alto, c_2 baixo e c_3 baixo. O julgamento final deste sistema biométrico foi altamente influenciado pela biometria 1, que apresenta maior nível de segurança. Como as outras duas biometrias apresentavam nível de segurança baixo, para que o sistema ficasse menos sensível a fraudes, as regras foram implementadas de modo que estas duas biometrias tivessem pouca influência sobre o resultado final de s_F.

III. ESTUDO EXPERIMENTAL E CONCLUSÕES

Foram propostas novas regras para o Trabalho de Tese base [2] e comparadas com as já implementadas anteriormente. O resultado mostra que com a menor chance do sistema de aceitar um impostor, a taxa de falsa rejeição aumentara, fazendo com que os genuínos sejam considerados impostores. A inclusão de uma biometria a mais no módulo de fusão aumenta significamente a quantidade de regras nebulosas que devem ser implementadas, de modo que para maior simplicidade da análise, dividiu-se o sistema em quatro casos, segundo o critério de segurança. No caso da fusão de três biometrias, o nível de segurança foi crucial no desempenho do sistema. Sistemas com três biometrias com baixa segurança não devem ser utilizados em aplicações em que, de forma alguma, um impostor deve ser aceito. Para que este sistema tenha um funcionamento razoável, é necessário que se mantenha o índice de confiabilidade sempre alto, implicando em uma manutenção freqüente das amostras de comparação. O melhor caso ocorre quando as três biometrias são seguras, onde a decisão final é feita partindo do princípio que a biometria com menor índice de confiabilidade pouco influencia no resultado final do sistema.

REFERÊNCIAS

[1] A. Ross and A.K. Jain, “Information fusion in biometrics”, Pattern Recognition Letters, vol. 24, 2003.

[2] M. Sugeno, K.T. Kang, “Structure identification of fuzzy model”, Fuzzy Sets and Systems 28 (1991) 191-212.

[3] R. N. Rodrigues, “Fusão Biométrica com Lógica Nebulosa”, Tese de Mestrado, FEEC-UNICAMP, 2006.