Fusão biométrica com lógica nebulosa

Lee Luan Ling, Nagel Rodrigues e Jennifer Chuin Lee

***Resumo*—É proposto um novo método de fusão de dois sistemas biométricos unimodais. A fusão dos dados biométricos é feita no nível de comparação de padrões onde são avaliados índices de similaridade, índices de confiabilidade das amostras coletadas e índices de segurança dos sistemas unimodais. Estas informações da qualidade das amostras e dos sistemas biométricos são processadas através de um sistema de inferência nebuloso para fim de autenticação pessoal.**

***Palavras-Chave*—Biometria Multimodal, Fusão biométrica, Lógica nebulosa, Reconhecimento de Padrões.**

***Abstract*—A new approach for unimodal biometric systems is proposed. The fusion of biometrics is carried out on the comparison level where the pattern similarity index, the sample reliability index and the biometric system security indices are processed by a fuzzy inference system for personal authentication purposes.**

I. INTRODUÇÃO

A biometria multimodal tem como objetivo melhorar o processo automático de autenticação pessoal através da utilização de mais de um tipo de características biométricas [1]. Apesar deste esforço, como adequadamente combinar as informações dadas por diversas características biométricas ainda é um problema sem uma solução definitiva.

Segundo Jain *et al* [1], uma boa estratégia de fusão de informações biométricas é essencial para o sucesso de um sistema biométrico multimodal – alcançando uma alta taxa de reconhecimento. A fusão de informações biométricas pode ser realizada em cada um dos 4 estágios seqüenciais (4 níveis) de um processo de reconhecimento de padrões - nível de sensor, nível de extração de características, nível de comparação (*matching scores*) e nível de decisão.

Um número considerável de trabalhos de pesquisa tem sido publicado recentemente neste tema de fusão de sistemas biométricos [1-10]. A fusão de vários sistemas biométricos é freqüentemente vista como um problema de combinação de classificadores, também conhecido como *fusão de classificadores*, *mistura de sistemas especialistas*, etc. [11]. Embora uma aplicação direta da técnica de fusão de classificadores na implementação de um sistema biométrico multimodal possa resultar em melhor desempenho, a técnica é incapaz de fornecer soluções adequadas para questão de segurança e confiabilidade. Isso é devido ao fato que apenas os índices de similaridade são usados na fusão. Para consertar esta deficiência, os trabalhos recentes têm explorado a idéia de adicionar "informações auxiliares" no processo de fusão, tais como qualidade da amostra biométrica [6-8] e parâmetros específicos para cada usuário [12] na tentativa de construir sistemas biométricos mais adaptativos e confiáveis.

Em [6] os autores fizeram uma revisão sobre o tema de fusão de informação e propuseram uma abordagem biométrica multimodal baseado na informação de face e de voz. Várias estratégias de fusão foram testadas, incluindo soma ponderada, SVM (*Support Vector Machine*), classificação bayesiana, concatenação de vetor de característica. Os testes foram realizados em dois ambiente: com e sem presença de ruído. Foi observado que a maioria das abordagens não adaptativas (que usam apenas os índices de similaridade) e as adaptativas (que também utilizam "informações auxiliares" no processo de fusão) apresentaram praticamente os mesmos desempenhos em ambientes sem ruído. Porém as não adaptativas tiveram seu desempenho consideravelmente dete-riorado em ambientes ruidosos.

Fierrez-Aguilar et al. [13,14] testaram varias abordagens multimodais que levam em consideração as qualidades das amostras biométricas. Na combinação das biometrias (face com impressão digital e impressão digital com assinatura) as qualidades das amostras da impressão digital foram avaliadas por um especialista. Todos os testes comprovaram a relevância de incluir um índice de qualidade da amostra no processo de fusão, o que resultaria em melhor desempenho para o sistema biométrico mutlimodal.

O conceito nebuloso é um método apropriado para modelar incertezas do *matching* biométrico, que por sua vez está diretamente relacionado com a qualidade das amostras. Em [9] a qualidade da amostra biométrica foi engajada na fuzzificação do índice de similaridade realizada pelo processo de comparação (*matching*). Um algoritmo de agrupamento (*clustering*) estendido, baseado em *Fuzzy K-Means*, é proposto nesse trabalho para manipular as informações fuzzificadas. Cinco sistemas biométricos unimodais foram utilizados nos testes.

II. MÉTODOS PROPOSTOS

A Fig.1 mostra o diagrama geral do sistema biométrico multimodal proposto operando no modo de verificação de identidade. Primeiramente, o usuário fornece uma amostra biométrica para cada sistema unimodal *i*, onde neste caso *i* = 1,2. Cada amostra é utilizada para extrair um vetor de características v_i, que é comparado com o vetor modelo v_i' armazenado no banco de dados. Desta forma, um índice de similaridade s_i é gerado. O desenvolvimento do módulo de análise da confiabilidade não será o foco deste trabalho, pois

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

a forma como ele é implementado depende do tipo de sistema biométrico unimodal que está sendo utilizado na fusão. No entanto, é importante mencionar que os principais aspectos que podem influenciar a confiabilidade de uma amostra e que podem ser usados no cálculo de r_i são:

Qualidade da amostra - existem muitos métodos para fazer a análise da qualidade de uma amostra biométrica. Amostras de baixa qualidade podem dificultar ou impedir a extração de características confiáveis e, conseqüentemente, gerar um erro no reconhecimento de um usuário. Desta forma, quanto pior a qualidade da amostra capturada, menor deve ser o valor do parâmetro r_i .

Idade do vetor modelo usado na comparação - algumas características biométricas sofrem alterações com o passar do tempo. Desta forma, o parâmetro r_i deve decair de acordo com a diferença de tempo entre a data em que o cadastro do usuário foi feito e a data em que a amostra testada foi capturada. A taxa de decaimento depende da característica biométrica que está sendo usada.

Parâmetros específicos do usuário - uma característica biométrica que é muito distintiva para um usuário, pode não ser tão boa para outros usuários. Muitos artigos já exploram este fato. Portanto, o parâmetro de confiabilidade r_i pode ser calculado de forma que reflita a diferenciabilidade de cada usuário em relação à característica biométrica.

O parâmetro $c_i \in R$ está relacionado com o nível de segurança do respectivo sistema unimodal *i*. O valor deste parâmetro é definido pelo operador do sistema e representa o grau de dificuldade com que um sistema biométrico é fraudado. Este parâmetro será usado para evitar que sistemas biométricos de baixa segurança se tornem um "elo fraco" quando integrados com sistemas biométricos de alta segurança. Por exemplo, um sistema de reconhecimento da face pode ser facilmente enganado através da apresentação de uma fotografia da face do usuário autêntico na frente da câmera. Isto pode fazer com que um sistema multimodal que utiliza a face e a íris, por exemplo, se torne vulnerável, mesmo com a utilização da íris, que é difícil de ser fraudada. Através da utilização do parâmetro c_i , a segurança de cada sistema biométrico será levada em conta durante a etapa de fusão.

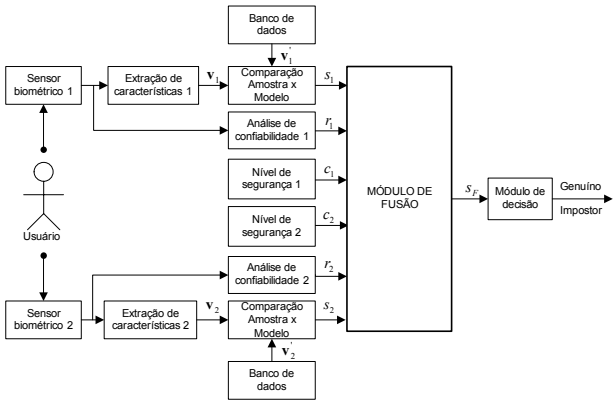

Fig.1: Método de fusão biométrica proposto.

Estes seis parâmetros ($s_1, s_2, r_1, r_2, c_1, c_2$) serão então usados pelo módulo de fusão, que foi implementado através de um sistema de inferência nebuloso, para gerar um único índice de similaridade s_F . Finalmente, o valor de s_F será usado pelo módulo de decisão para tomar a decisão final entre *genuíno* ou *impostor*.

III. módulo de fusão

Conforme ilustrado na Fig.1, o módulo de fusão recebe seis parâmetros de entrada ($s_1, s_2, r_1, r_2, c_1, c_2$), que serão processados através de um sistema de inferência nebuloso, produzindo assim, um único índice de similaridade final s_F que será usado para classificação final do usuário.

A Fig.2 mostra as três etapas do módulo de fusão. Primeiramente, cada um dos seis parâmetros de entrada $p \in \{s_1, s_2, r_1, r_2, c_1, c_2\}$ será representado por uma variável lingüística. Para cada variável lingüística, um conjunto nebuloso apropriado descreverá o valor lingüístico *alto*. Desta forma, cada parâmetro de entrada será mapeado em um valor de pertinência ($p \rightarrow p^{alto}$), que representará no intervalo [0,1] quão alto é o valor deste parâmetro. O valor lingüístico *baixo* será definido como o complemento do valor lingüístico alto e seu valor de pertinência será $p^{baixo} = 1 - p^{alto}$.

O índice de similaridade final s_F também será modelado através de uma variável lingüística, mas terá três valores lingüísticos: *baixo*, *médio* e *alto*.

Após todos os parâmetros de entrada e saída terem sido devidamente representados por variáveis lingüísticas, eles serão processados por um conjunto de 12 regras nebulosas. Estas regras foram inspiradas na forma como o cérebro humano, utilizando os mesmos dados de entrada, atuaria para fazer o reconhecimento de uma pessoa. A principal lógica das regras é que amostras com baixa confiabilidade têm um peso menor na decisão final e que sistemas com baixa segurança só podem influenciar na autenticação de uma pessoa caso um sistema de alta segurança também indique que o usuário é autêntico.

Finalmente, um processo de defuzzificação combina os resultados individuais produzidos por cada uma das 12 regras nebulosas, gerando assim, um índice de similaridade final s_F que será usado pelo módulo de decisão. Quanto maior for o valor de s_F , maior é a certeza de que o usuário é genuíno.

A seguir serão descritas detalhadamente as etapas da construção do sistema de inferência nebuloso utilizado no módulo de fusão proposto: Fuzzificação; Criação das regras nebulosas e defuzzificação.

IV VARIÁVEIS NEBULOSAS E FUZZIFICAÇÃO.

Pertinência do Índice de Similaridade ($s_i \rightarrow s_i^{alto}$)

Os índices de similaridade s_1 e s_2 serão mapeados nos valores de pertinência s_1^{alto} e s_2^{alto}, respectivamente. As funções de pertinência que farão o mapeamento $s_i \rightarrow s_i^{alto}$,

i=1,2, devem ser escolhidas cuidadosamente a fim de manter o significado da expressão *alta similaridade*. Várias funções para normalização do índice de similaridade dos sistemas biométricos vem sido propostas na literatura [8,15,16] e podem ser usadas como funções de pertinência, tais como função sigmoidal, Min-Max e Tangente hiperbólica.

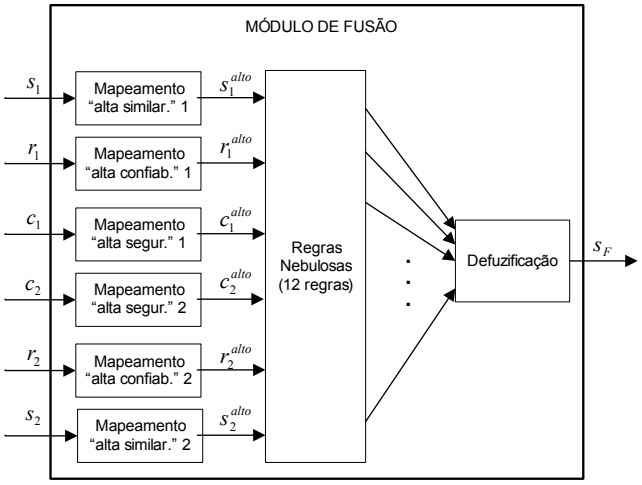

Fig. 2: Módulo de fusão biométrica proposto.

Na verdade qualquer função monotonicamente crescente com contra-domínio entre zero e um pode ser usada aqui como função de pertinência, desde que represente de forma conveniente a expressão *alta similaridade*. Desta forma, uma nova função de normalização, que visa representar a expressão lingüística da melhor forma, será proposta neste trabalho:

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

onde $s_{i,zeroFRR}$ e $s_{i,zeroFAR}$ são os pontos com menores FAR e FRR, para taxa zero de falsa rejeição e de falsa aceitação, respectivamente. A Fig. 3 ilustra a função dada pela eq (1) em relação ao gráfico de FAR e FRR. Observe que a transição ocorre onde existe a sobreposição entre a FAR e FRR, mapeando desta forma a incerteza existente neste intervalo. Conforme definição, temos $s_i^{baixo} = 1 - s_i^{alto}$.

Pertinência do Índice de Confiabilidade ($r_i \to r_i^{alto}$)

Conforme descrito anteriormente, o parâmetro r_i pode ser interpretado como a certeza de que o valor s_i seja uma medida correta. Neste caso, o mapeamento $r_i \to r_i^{alto}$, *i=1,2,* feito por qualquer função de pertinência monotonicamente crescente com contra-domínio entre zero e um. A escolha da função de pertinência apropriada depende da forma como o módulo que faz o cálculo de r_i é implementado, que é diferente para cada tipo de sistema biométrico. No entanto, a função de pertinência deve ser definida de forma que mantenha o significado da expressão *alta confiabilidade*, sendo que a escolha mais simples e genérica para este caso é a função Min-Max:

$$r_i^{alto} = \frac{r_i - \min(R_i)}{\max(R_i) - \min(R_i)} \quad (2)$$

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. Conforme definição, temos $r_i^{baixo} = 1 - r_i^{alto}$.

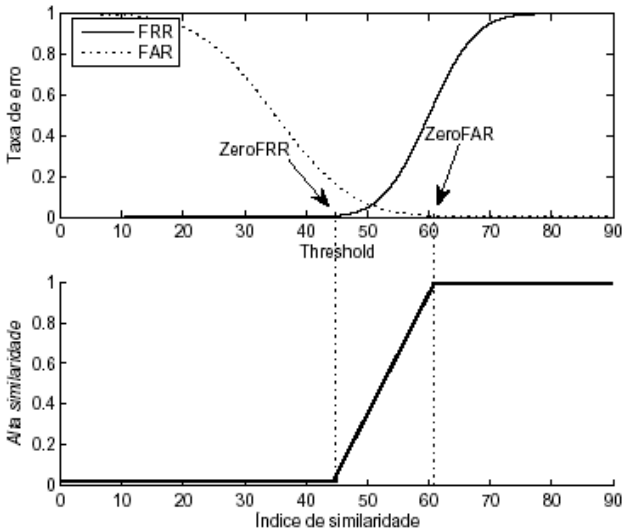

Fig. 3: Função de pertinência da expressão lingüística *alta similaridade*.

Pertinência do Nível de Segurança ($c_i \to c_i^{alto}$)

Como definido anteriormente, o nível de segurança de cada sistema unimodal é especificado diretamente pelo administrador do sistema. Restringindo-se este valor no intervalo [0,1], onde zero significa o menor nível de segurança e um o maior, o mapeamento da expressão *alta segurança* ($c_i \to c_i^{alto}$, *i=1,2*) pode ser feita diretamente através da equação $c_i^{alto} = c_i$. Analogamente, temos $c_i^{baixo} = 1 - c_i^{alto}$

Funções de Pertinência da Saída

A variável de saída s_F também será representada através de uma variável lingüística e terá três possíveis valores lingüísticos: *baixo*, *médio* e *alto*. Como o sistema de inferência que está sendo usado é do tipo Takagi-Sugeno-Kang [18] de primeira ordem, estes valores lingüísticos terão valores constantes, definidos da seguinte forma: $s_F^{baixo} = 0$, $s_F^{médio} = 0{,}5$ e $s_F^{alto} = 1$, respectivamente. Quanto maior seu valor numérico, maior é a certeza de que o usuário deve ser autenticado.

IV DEFINIÇÃO DAS REGRAS

As regras nebulosas implementadas para o sistema proposto:

1. Se s_1 é alto e s_2 é alto, então s_F é alto.
2. Se s_1 é baixo e s_2 é baixo, então s_F é baixo.
3. Se c_1 é alto e r_1 é baixo e r_2 é baixo e s_1 é alto e s_2 é baixo, então s_F é médio.

4. Se c_1 é alto e r_1 é baixo e r_2 é alto e s_1 é alto e s_2 é baixo, então s_F é baixo.
5. Se c_1 é alto e r_1 é alto e r_2 é baixo e s_1 é alto e s_2 é baixo, então s_F é alto.
6. Se c_1 é alto e r_1 é alto e r_2 é alto e s_1 é alto e s_2 é baixo, então s_F é médio.
7. Se c_1 é baixo e s_1 é alto e s_2 é baixo, então s_F é baixo.
8. Se c_2 é alto e r_1 é baixo e r_2 é baixo e s_1 é baixo e s_2 é alto, então s_F é médio.
9. Se c_2 é alto e r_1 é alto e r_2 é baixo e s_1 é baixo e s_2 é alto, então s_F é baixo.
10. Se c_2 é alto e r_1 é baixo e r_2 é alto e s_1 é baixo e s_2 é alto, então s_F é alto.
11. Se c_2 é alto e r_1 é alto e r_2 é alto e s_1 é baixo e s_2 é alto, então s_F é médio.
12. Se c_2 é baixo e s_1 é baixo e s_2 é alto, então s_F é baixo.

O conector "*e*" utilizado nas regras nebulosas é implementado através da multiplicação do valor de pertinência de cada proposição nebulosa. Estas regras foram definidas de forma empírica baseando-se nas seguintes premissas:

- Uma amostra biométrica com baixo índice de confiabilidade (baixo r_i) fornece pouca informação sobre a identidade do usuário. Desta forma, há uma tendência de que amostras com baixa confiabilidade interfiram negativamente na autenticação e levem a uma falsa rejeição. Portanto, amostras com baixa confiabilidade devem possuir um peso menor na decisão final.
- A informação fornecida por um sistema biométrico com baixa segurança só pode ser usada para fazer a autenticação de uma pessoa caso outro sistema biométrico mais seguro também indique que a pessoa é autêntica. Desta forma, caso um fraudador falsifique somente o sistema unimodal menos seguro, ele ainda não conseguirá enganar o sistema multimodal.

As regras nebulosas são mutuamente exclusivas e estão ilustradas na tabela 1 para uma melhor visualização. Observe que a saída é sempre alta quando s_1 e s_2 são ambos alto, independentemente das outras variáveis. Quando s_1 e s_2 são baixos, a saída é baixa. No entanto, quando um dos índices de similaridade é alto e o outro é baixo, o valor de s_F dependerá também do parâmetro de segurança e de confiabilidade.

Defuzzificação - No sistema proposto neste trabalho, a defuzzificação é realizada através da média ponderada das regras nebulosas conforme a equação a seguir:

$$s_F = \frac{\sum_{j=1}^{12} m_j z_j}{\sum_{j=1}^{12} m_j} \quad (3)$$

onde m_j é o valor de ativação da regra j e z_j seu respectivo valor de saída. O valor m_j resultante de cada uma das regras é apresentado a seguir:

$m_1 = s_1^{alto} s_2^{alto}$, $m_2 = s_1^{baixo} s_2^{baixo}$, $m_3 = c_1^{alto} r_1^{baixo} r_2^{baixo} s_1^{alto} s_2^{baixo}$,
$m_4 = c_1^{alto} r_1^{baixo} r_2^{alto} s_1^{alto} s_2^{baixo}$, $m_5 = c_1^{alto} r_1^{alto} r_2^{baixo} s_1^{alto} s_2^{baixo}$,
$m_6 = c_1^{alto} r_1^{alto} r_2^{alto} s_1^{alto} s_2^{baixo}$, $m_7 = c_1^{baixo} s_1^{alto} s_2^{baixo}$,
$m_8 = c_2^{alto} r_1^{baixo} r_2^{baixo} s_1^{baixo} s_2^{baixo}$, $m_9 = c_2^{alto} r_1^{alto} r_2^{baixo} s_1^{baixo} s_2^{alto}$,
$m_{10} = c_2^{alto} r_1^{baixo} r_2^{alto} s_1^{baixo} s_2^{alto}$, $m_{11} = c_2^{alto} r_1^{alto} r_2^{alto} s_1^{baixo} s_2^{alto}$ e
$m_{12} = c_2^{baixo} s_1^{baixo} s_2^{alto}$.

Após o processo de defuzzificação o valor de saída s_F estará no intervalo [0,1] e quanto maior seu valor, maior é a certeza de que o usuário é genuíno.

Tabela 1: Regras do sistema de inferência nebuloso

<table>
<tr><td colspan="3" rowspan="3"></td><td colspan="4">s_2 (A)</td><td colspan="4">s_2 (B)</td></tr>
<tr><td colspan="2">c_2 (A)</td><td colspan="2">c_2 (B)</td><td colspan="2">c_2 (A)</td><td colspan="2">c_2 (B)</td></tr>
<tr><td>r_2 (B)</td><td>r_2 (A)</td><td>r_2 (B)</td><td>r_2 (A)</td><td>r_2 (B)</td><td>r_2 (A)</td><td>r_2 (B)</td><td>r_2 (A)</td></tr>
<tr><td rowspan="6">s_1 (A)</td><td rowspan="3">c_1 (A)</td><td>r_1 (B)</td><td colspan="4" rowspan="6">S_F (A)</td><td>S_F (M)</td><td>S_F (B)</td><td>S_F (M)</td><td>S_F (B)</td></tr>
<tr><td>r_1 (A)</td><td>S_F (A)</td><td>S_F (M)</td><td>S_F (A)</td><td>S_F (M)</td></tr>
<tr><td rowspan="2">c_1 (B)</td><td>r_1 (B)</td><td colspan="4" rowspan="2">S_F (B)</td></tr>
<tr><td>r_1 (A)</td></tr>
<tr><td rowspan="6">s_1 (B)</td><td rowspan="3">c_1 (A)</td><td>r_1 (B)</td><td>S_F (M)</td><td>S_F (A)</td><td rowspan="6">S_F (B)</td><td colspan="4" rowspan="6">S_F (B)</td></tr>
<tr><td>r_1 (A)</td><td>S_F (B)</td><td>S_F (M)</td></tr>
<tr><td rowspan="2">c_1 (B)</td><td>r_1 (B)</td><td>S_F (M)</td><td>S_F (A)</td></tr>
<tr><td>r_1 (A)</td><td>S_F (B)</td><td>S_F (M)</td></tr>
</table>

VI. TESTES DOS MÉTODOS DE FUSÃO

Para testar o método de fusão proposto, faremos a combinação de dois sistemas biométricos: um sistema de impressão digital (que será chamado de sistema B1) implementado pelo NIST [20] e um sistema de face utilizando a técnica de *eigenfaces* [19] (sistema B2). Além do método proposto, outros dois métodos de fusão serão usados para fins de comparação: soma ponderada e soma normalizada. Esta comparação permite observar se a introdução dos novos parâmetros de entrada no módulo de fusão é capaz de melhorar o desempenho do sistema multimodal. Os experimentos foram realizados utilizado impressões digitais da FVC2004 e imagens da face do banco de dados FERET.

Método da soma ponderada (F1): É representado através da seguinte expressão:

$$s_F = k s_1 + s_2$$

onde k é uma constante que representa o peso do sistema biométrico B1 em relação ao peso do sistema biométrico B2.

O parâmetro k será empiricamente definido para cada aplicação através da busca extensiva por um valor ótimo.

Método da soma normalizada (F2): Cada índice de similaridade $s_i, i = 1,2$, será normalizado de acordo com a regra Min-Max definida pela seguinte equação:

$$\overline{s_i} = \frac{s_i - \min(S_i)}{\max(S_i) - \min(S_i)}$$

onde S_i denota o domínio da variável s_i. O índice de similaridade final é dado por

$$s_F = s_1 + s_2 \ .$$

Método fuzzy (F3). Supondo que r_i e c_i representem o índice de confiabilidade e de segurança, respectivamente. Logo,

$$s_F = M\left(s_1^{alto}, s_2^{alto}, r_1^{alto}, r_2^{alto}, c_1^{alto}, c_2^{alto}\right)$$

onde a função $M(\cdot)$ é dada pela eq. (3) e

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

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

$$c_i^{alto} = c_i$$

onde $\min(R_i)$ e $\max(R_i)$ representam o valor mínimo e máximo do domínio da variável r_i, respectivamente.

Os índices de confiabilidade (r_1 e r_2) das amostras serão definidos pelo seu respectivo IQA (Índice de Qualidade da Amostra) [17]. Os parâmetros de segurança (c_1 e c_2) serão fixados através de uma análise qualitativa da segurança do respectivo sistema biométrico. A segurança da impressão digital será definida como $c_{fing} = 0,7$, no entanto existem muitas variáveis dependentes da aplicação que podem influenciar na atribuição deste valor. Por exemplo, uma segurança maior pode ser atribuída a um sistema de impressões digitais caso ele utilize um sensor capaz de detectar se o dedo empregado na leitura realmente pertence a uma pessoa viva. A segurança da face será definida como $c_{face} = 0,3$. A tabela 5.1 resume os parâmetros utilizados nos métodos de fusão.

Três diferentes experimentos foram conduzidos:

• **Experimento I** - Este experimento visa simular um ambiente normal de operação. Para isto, os dados de testes serão filtrados de forma que somente amostras de qualidade regular, onde $r_1^{alto} \geq 0,7$ e $r_2^{alto} \geq 0,7$ serão utilizadas nos testes. Geralmente, este é o único tipo de experimento realizado para avaliação dos sistemas multimodais, no entanto, é insuficiente para avaliar todos os quesitos de um sistema biométrico.

• **Experimento II** - Este experimento visa testar o que acontece quando amostras de baixa qualidade são introduzidas. Todas as amostras do conjunto de testes serão usadas, independentes da sua qualidade.

Tab. 5.1: Parâmetros dos métodos de fusão biométrica.

Método de fusão	Parâmetros, Imp.Dig.(B1)+Face(B2)
Soma ponderada	$k = 0,02$
Soma Normalizada	$\max(S_1) = 230$, $\min(S_1) = 0$, $\max(S_2) = 0,95$, $\min(S_2) = -0,8$
Fuzzy	$s_{1,ZeroFRR} = 2,5$, $s_{1,ZeroFAR} = 50$, $s_{2,ZeroFRR} = -0,15$, $s_{2,ZeroFAR} = 0,9$, $\max(R_1) = 8$, $\min(R_1) = 0$, $\max(R_2) = 1$, $\min(R_2) = 0$, $c_1 = 0,7$, $c_2 = 0,3$

• **Experimento III** – Este experimento simula a situação quando o sistema de faces foi fraudado. Para isto, as comparações de impostores do sistema multimodal foram feitas utilizando-se uma amostra impostora da impressão digital (como de costume) junto com uma amostra genuína da face com qualidade regular ($r_1^{alto} \geq 0,7$ e $r_2^{alto} \geq 0,7$).

Os resultados de testes obtidos são ilustrados através da curva ROC (GAR=1-FRR, FAR) [1]. A figura 4 mostra a curva ROC dos sistemas biométricos para o Experimento 1. Pode-se perceber que todos os métodos de fusão obtiveram resultados melhores quando comparados com os sistemas unimodais. A soma ponderada obteve o melhor desempenho neste experimento.

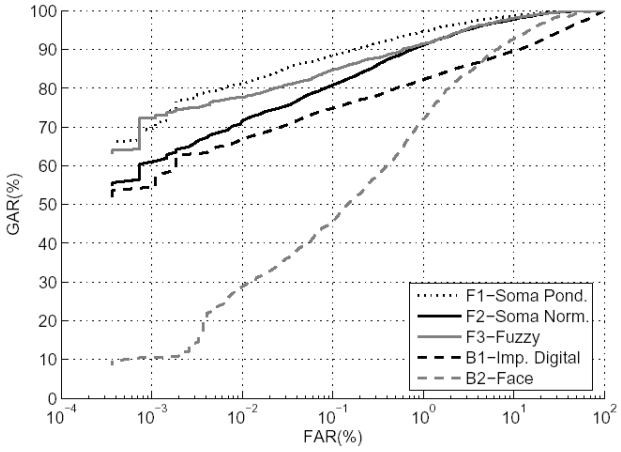

Fig. 4: Curva ROC do Experimento I.

A figura 5 mostra a curva ROC dos sistemas biométricos para o Experimento II. Devido à introdução de amostras com baixa qualidade, ambos sistemas unimodais tiveram acentuada queda no desempenho, o que, conseqüentemente, também foi observado nos sistemas multimodais. No entanto, o sistema nebuloso foi o menos afetado, o que evidencia sua capacidade de adaptação em ambientes ruidosos. Observa-se também que o resultado da soma normalizada caiu muito, ficando inclusive pior que o sistema de impressão digital.

A figura 6 mostra a curva ROC dos sistemas biométricos para o Experimento 3. Neste experimento, todos os métodos de fusão foram influenciados negativamente pela face (que foi fraudada), mas como o parâmetro de segurança da face foi definido como baixo ($c_{face} = 0,3$), a fusão através do método nebuloso foi a menos afetada, tendo um comportamento

muito parecido com o da impressão digital, cujo parâmetro de segurança é maior ($c_{fing} = 0{,}7$).

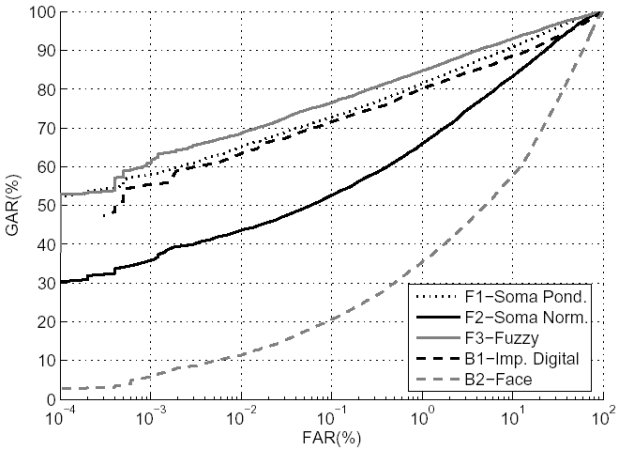

Fig. 5: Curva ROC do Experimento II

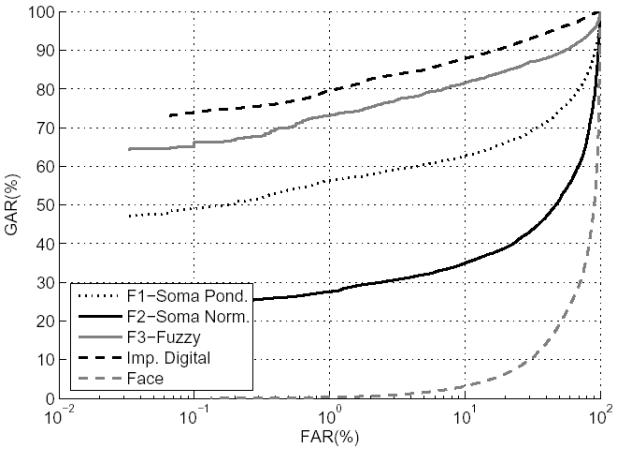

Fig. 6: Curva ROC do Experimento III

VI. RESULTADOS E CONCLUSÕES

Neste trabalho, apresentamos uma nova estratégia de fusão biométrica. Uma das principais inovações foi a introdução de dois novos parâmetros no módulo de fusão: índice de confiabilidade da amostra e nível de segurança do sistema unimodal. Outra inovação da nossa proposta está no modo como o módulo de fusão foi implementado, que se baseou em um sistema de inferência nebuloso. O método de fusão proposto foi comparado com a fusão através da soma ponderada e soma normalizada, sendo que os testes foram feitos na integração da face com impressão digital. Os procedimentos de testes adotados simularam o funcionamento do sistema multimodal tanto em condições normais de operação como em condições adversas. A partir dos dados dos testes da integração da face com a impressão digital, as seguintes conclusões gerais podem ser feitas:

• Quando as amostras têm níveis regulares de qualidade, a soma ponderada apresenta melhores resultados que a fusão nebulosa.

• No entanto, quando existem amostras de baixa qualidade, o sistema nebuloso não é tão influenciado e acaba apresentando as menores taxas de erro.

• Mesmo que um falsificador consiga fraudar o sistema de face com sucesso, as chances de ele ser aceito por um sistema multimodal que usa a fusão nebulosa ainda é baixa, o que não acontece quando a fusão é feita através da soma ponderada ou soma normalizada.

REFERENCIAS

[1] Arun Ross, Anil K. Jain, "Information Fusion in Biometrics", Pattern Recognition Letters, vol. 24, 2003.

[2] Yuhong Wang, Tieniu Tan, Anil K. Jain, "Combining Face and Iris Biometrics for Identity Veri¯cation", AVBPA, LNCS 2699, pp. 805-813, 2003.

[3] Lin Hong, Anil Jain, "Integrating Faces and Fingerprints for Personal Identification", IEEE Trans. On Pattern Analysis and Machine Intelligence, Vol. 20, No. 12, December 1998.

[4] Piotr Gutkowski, "Algorithm for retrieval and verification of personal identity using bimodal biometrics", Information Fusion 5, 65-71, 2004.

[5] Kalyan Veeramachaneni, Lisa A. Osadciw, Pramod K. Varshney, "An Adaptive Multimodal Biometric Management Algorithm". IEEE Trans. On Systems, Man and Cybernetics, Part C, Vol. 35, NO. 3, Aug. 2005.

[6] Conrad Sanderson, Kulpid K. Paliwal, "Identity verification using speech and face information", Digital Signal Processing, 14, 449-480, 2004.

[7] Julian Fierrez-Aguilar, Javier Ortega-Garcia, Joaquin Gonzalez-Rodriguez, Josef Bigun, "Discriminative Multimodal biometric authentication based on quality measures". Pattern Recognition, article in press, accepted Nov, 2004.

[8] Josef Bigun, J. Fierrez-Aguilar, J. Ortega-Garcia, J. Gonzalez-Rodriguez, "Multimodal biometric authentication using quality signals in mobile communications" Proc. 12th International Conference on Image Analysis and Processing ICIAP'03, 2003.

[9] Vassilios Chatzis, Adrian G. Bors, Ioannis Pitas, "Multimodal Decision-Level Fusion for Person Authentication", IEEE Trans. Systems, Man and Cybernetics, vol. 29, NO. 6, Nov. 1999.

[10] Yunhong Wang, Tieniu Tan, Anil K. Jain, "Combining Face and Iris Biometrics for Identity Verification", AVBPA 2003, LNCS 2688, pp. 805-813, 2003.

[11] Ludmila I. Kuncheva, James C. Bezdek, Robert P.W. Duin, "Decision templates for multiple classifier fusion: an experimental comparison". Pattern Recognition, 34, 299-314, 2001.

[12] Kar-Ann Toh , Xudong Jiang and Wei-Yun Yau, "Exploiting Global and Local Decisions for Multimodal Biometrics Verification", IEEE Transactions on Signal Processing, vol. 52, no. 10, pp. 3059-3072, Oct. 2004.

[13] Julian Fierrez-Aguilar, Javier Ortega-Garcia, Joaquin Gonzalez-Rodriguez, Josef Bigun, "Discriminative Multimodal biometric authentication based on quality measures". Pattern Recognition, article in press, accepted Nov, 2004.

[14] Josef Bigun, J. Fierrez-Aguilar, J. Ortega-Garcia, J. Gonzalez-Rodriguez, "Multimodal biometric authentication using quality signals in mobile communications" Proc. 12th International Conference on Image Analysis and Processing ICIAP'03, 2003.

[15] Robert Snelick, Umut Uludag, Alan Mink, Michael Indovina, and Anil Jain. Large-scale evaluation of multimodal biometric authentication using state-of-the-art systems. *IEEE Transactions on Pattern Analysis and Machine Intelligence*, 27(3):450–455, March 2005.

[16] Anil Jain, Karthik Nandakumar, and Arun Ross. Score normalization in multimodal biometric systems. *To appear in Pattern Recognition*, 2005.

[17] Elham Tabassi, Charles L. Wilson, and Craig I. Watson. Fingerprint image quality. Technical Report NISTIR 7151, National Institute of Standards and Technology (NIST), Aug. 2004.

[18] M. Sugeno and K. T. Kang. Structure identification of fuzzy model. *Fuzzy Sets and Systems*, 28:191–212, 1991.

[19] Matthew A. Turk and Alex P. Pentland. Face recognition using eigenfaces. In Proceedings of Computer Vision and Pattern Recognition, pages 586–591, 1991.

[20] NFIS, 2006. Nist fingerprint software. Página na internet, National Institute of Standards and Technology (NIST), Março 2006. http://fingerprint.nist.gov/NFIS/.