Uma Nova Abordagem Robusta de Fusão Biométrica

Lee Luan Ling, Ricardo Nagel Rodrigues e Jennifer Chuin Lee

***Resumo* - Neste artigo analisamos a influencia no desempenho de um sistema biométrico bimodal devido a ataque trapaceiro. Como conseqüência, é proposto uma nova abordagem robusta de fusão biométrica para sistema multimodal levando em consideração a influência de ataques trapaceiros. O método proposto é uma extensão do esquema de fusão biométrica baseado na razão verossimilhança com o objetivo de aumentar o nível de segurança de sistemas biométricos multimodais contra ataques trapaceiros.**

***Palavras-Chave* – Biometria, Fusão Biométrico, Ataque Trapaceiro.**

***Abstract* - In this work we analyze the impacts on the performance of a bimodal biometric system due to spoof attacks. As result, a new robust approach for multimodal biometric fusion that takes into account the influence of spoof attacks. The proposed method is an extension of the fusion scheme based on the likelihood ration method in order to increment the security level of multimodal biometric systems against spoof attacks.**

***Keywords* – Biometrics, Biometric Fusion, Spoof Attack.**

I. INTRODUÇÂO

Com o objetivo de adquirir máximo aproveitamento das vantagens de uma abordagem biométrica multimodal, é essencial implementar um método eficaz para fusão de informações biométricas provenientes de fontes diferentes. Maioria dos métodos de fusão propostos recentemente demonstra que sistemas multimodais biométricos podem incrementar na forma significativa as taxas de reconhecimento quando comparados com sistemas biométricos unimodais [2-7]. Apesar destas tentativas, nenhuma destas abordagens tem explicitamente explorada a questão de segurança do sistema biométrico.

Quando se trata de trapacear um sistema biométrico multimodal, várias perguntas podem surgir, como por exemplo, "é necessário trapacear todas as modalidades biométricas envolvidas em fusão para enganar um sistema multimodal?", "Qual é o grau de comprometimento em questão de segurança, quando apenas os biométricos de baixo nível de segurança em um sistema multimodal forem trapaceados com sucesso?".

O método de razão verossimilhança (*likelihood ratio*) entre a distribuição de genuíno e a de impostor tem sido usado em sistemas biométricos multimodais e é considerado como o método de fusão ótimo em termo de mínima probabilidade de erro [8, 9]. Porém, a determinação destas distribuições não é uma tarefa trivial, principalmente para a categoria de impostor. Para simplificar, por exemplo, em [8] um modelo de mistura Gaussiana é usado para modelar ambos os tipos de distribuição. Mesmo assim, ainda há outros fatores que podem comprometer a confiabilidade das distribuições estimadas. Por exemplo, as abordagens de estimação sem levar em consideração da possibilidade de um dos modos biométricos sido trapaceado com sucesso já que apenas as amostras de impostores não trapaceiros normalmente são usadas no processo de treinamento.

Neste trabalho, é proposto um novo esquema de fusão biométrica multimodal levando em consideração da hipótese de ocorrência de trapaceira e simultaneamente a questão da segurança dos sistemas biométricos unimodais envolvidos na fusão. Este esquema pode ser visto como uma extensão da aplicação do método de razão verossimilhança.

O presente artigo é organizado da seguinte forma. O esquema de fusão proposto é ilustrado na seção 2. Na seção 3 relatamos os experimentos conduzidos para fim de análise da robustez do esquema proposto contra amostras de baixa qualidade e possíveis ataques trapaceiros. Os resultados destes experimentos são apresentados na seção 4. Finalmente na seção 5 concluímos.

Lee Luan Ling, Ricardo 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, email_do_nagel, jennifer.chuin.lee@gmail.com. Este trabalho foi parcialmente financiado pelo CNPq.

II. ESQUEMA DE FUSÃO

Neste trabalho consideramos apenas casos de verificação, ou seja, o usuário declara sua identidade e o sistema decidirá se o usuário é genuíno ou impostor. A figura 1 mostra a estrutura global do sistema bimodal ($M = 2$). As informações biométricas são combinadas no nível de índice de casamento (*matiching score*). Isso significa que cada sistema biométrico i ($i \in \{1, 2\}$) individualmente executa a comparação entre a amostra de treinamento e a nova amostra de teste calculando o índice de similaridade (s_i) entre duas amostras. Assumimos que para cada sistema biométrico *i*, existe um especialista que é capaz de fornecer uma nota numérica r_i ponderando a qualidade da amostra biométrica dada. A segurança de um sistema biométrico i é modelada pelo parâmetro c_i que representa o grau de dificuldade de trapacear este sistema. É importante ressaltar que a mensuração deste grau de dificuldade não é um trabalho trivial, mesmo sendo uma tarefa realizável [10]. Neste trabalho, manualmente atribuímos um valor ao parâmetro c_i baseado no conhecimento e nossa experiência. A descrição de uma avaliação qualitativa da segurança de alguns sistemas biométrico pode ser encontrada em [1].

Assim sendo, os conjuntos $X = \{s_1, s_2, r_1, r_2\}$ e $\{c_1, c_2\}$ formam os dados de entrada para o esquema de fusão que processa a informação de entrada e gera em seguida um único valor escalar na saída, denotado por s_f. Um valor alto de s_f indica que o usuário é mais provável de ser genuíno (ou impostor). Uma operação de decisão limiar é então aplicada em seguida para classificar o valor de saída s_f entre genuíno e impostor.

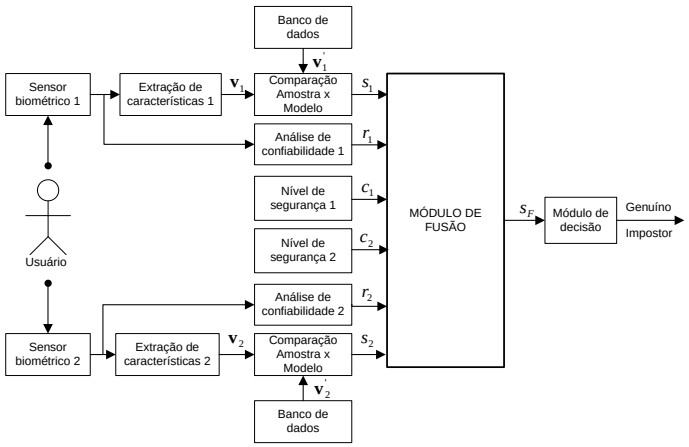

Figura 1. Uma visão global da arquitetura do sistema bimodal.

A. Razão Verossimilhança Estendida

Seja I uma variável aleatória binária que indica se um usuário é um impostor ($I=1$) ou genuíno ($I=0$). Nossa meta final é avaliar a razão verossimilhança entre a distribuição de genuíno $p(X/I=0)$ e a distribuição de impostor $p(X/I=1)$ como a seguir:

$$z=\frac{p(X/I=0)}{p(X/I=1)} \qquad (1)$$

Para diferentes tipos de sistemas biométricos, assumimos que s_i e r_i sejam independentes de s_j e r_j para *i* diferente de *j*. Logo a equação (1) pode ser reescrita como:

$$p(X/I)=p(s_1,r_1/I)p(s_2,r_2/I)=p(q_1)p(s_1/I,r_1)p(r_2)p(s_2/I,r_2) \quad (2)$$

Geralmente as distribuições condicionais encontradas na equação (1) são aprendidas usando um banco de dados de treinamento, onde *I* é conhecido como um conjunto de treinamento composto de dados de entrada (*X*). Porém, esta abordagem original de razão verossimilhança não está considerando o fato de que, na prática, um impostor poderia ter trapaceado um ou mais de um modo biométrico, logo a distribuição de impostor estimada poderia não ser realística. Para solucionar esta deficiência, o modelo bimodal proposto neste trabalho está baseado na suposição de que se um sistema biométrico for trapaceado com sucesso por um impostor, a nota (*score* s_i) de similaridade deve seguir uma distribuição de probabilidade genuína. Baseada nesta suposição introduzimos inicialmente algumas variáveis aleatórias ocultas que modelam a probabilidade de um ataque trapaceiro e a probabilidade de um ataque trapaceiro sucedido. Em seguida, estas variáveis são marginalizadas para fim de obtenção da distribuição real de impostor. O processo de marginalização sobre as variáveis escondidas pode ser interpretado como se fosse considerando todas as situações nas quais um sistema multimodal pode ser trapaceado.

Começamos pela definição de T_i como sendo uma variável aleatória que indica se há uma tentativa de trapacear o sistema biométrico unimodal *i*:

$$T_i=\begin{cases}1, & \text{se há tentativa de trapacear sistema biométrico } i,\\ 0, & \text{não há tentativa de trapacear sistema biométrico } i.\end{cases} \qquad (3)$$

A distribuição conjunta condicional $p(T_1,T_2|I=1)$ indica "quanto freqüente" impostores tentam trapacear os sistemas biométricos envolvidos. Esta distribuição depende da aplicação visto que algumas aplicações poderiam sofrer tentativas trapaceadas por falsificadores com maior freqüência do que outras. Por outro lado, obviamente não faz sentido em dizer que um usuário autêntico tentará trapacear o sistema. Assim sendo, atribuímos $p(T_1=0,T_2=0|I=0)=1$. Para usuários impostores definimos:

$$p(T_1,T_2|I=1)=\begin{cases}1-\alpha, & \text{se } T_1=0,\\ \dfrac{\alpha}{2^2-1}, & \text{caso contrário.}\end{cases} \qquad (4)$$

onde α é um parâmetro que indica a probabilidade de ocorrência de ataques trapaceiros. Note que para a fusão de *M=2* sistemas biométricos unimodais, há $2^M-1=3$ diferentes esquemas de ataques trapaceiros. Neste trabalho, atribuímos as probabilidades equiprováveis para estas $2^M-1=3$ possíveis combinações.

Definimos outra variável aleatória F_i indicando se um dado ataque trapaceiro tem sido sucedido ou não. A distribuição de probabilidade para esta variável está condicionada pela existência (ou não) de tentativa trapaceira. Obviamente se não houve tentativa de ataque trapaceiro $(T_i=0)$, a probabilidade de um ataque trapaceiro sucedido $(F_i=1)$ seria zero, ou seja, $p(F_i=1|T_i=0)=0$. Logo, como conseqüência, tem-se $p(F_i=0|T_i=0)=1$. Além disso, é importante ressaltar que a probabilidade de um ataque trapaceiro a ser sucedido está diretamente relacionada com o nível de segurança de um sistema biométrico. Assim sendo, definimos a probabilidade de sucesso de um ataque trapaceiro como $p(F_i=1|T_i=1)=1-c_i$. Isso implica que a probabilidade de fracasso de um ataque trapaceiro seja $p(F_i=0|T_i=1)=c_i$.

A figura 2 mostra o modelo proposto para um sistema bimodal, relacionando os parâmetros e variáveis envolvidos. Sob as suposições feitas, podemos marginalizar as variáveis escondidas introduzidas no modelo para estimar $p(X|I)$ como a seguir:

$$\begin{aligned}p(X/I)&=\sum_{T_1}\sum_{T_2}\sum_{F_1}\sum_{F_2}p(X,T_1,T_2,F_1,F_2/I)\\&=\sum_{T_1}\sum_{T_2}\sum_{F_1}\sum_{F_2}p(T_1,T_2/I)\prod_{i=1}^{2}\left[p(F_i/T_i)p(s_i,r_i/F_i,I)\right]\end{aligned} \qquad (5)$$

Para avaliar a probabilidade $p(X/I)$ dada pela equação (5) ainda precisamos conhecer a distribuição $p(s_i,r_i|F_i,I)$, para $i\in\{1,2\}$. Em situações quando o sistema biométrico *i* não for trapaceado (ou seja, $F_i=0$), esta distribuição pode ser aprendida diretamente dos dados de treinamento. É importante observar que não há necessidade conhecer $p(s_i,r_i|F_i=1,I=0)$ visto que assumimos anteriormente que

um usuário genuíno nunca tentará trapacear o sistema. Adotando a suposição de que s_i possua a distribuição genuína quando o sistema biométrico for trapaceado com sucesso, temos $p(s_i, r_i \mid F_i = 1, I = 1) = p(s_i, r_i \mid F_i = 0, I = 0)$. Agora, dada a entrada de teste *X*, podemos usar a equação (5) para avaliar a razão verossimilhança dada pela equação (1).

Usamos a distribuição de gama para modelar a distribuição de genuíno e de impostor quando $F_i = 0$. A adoção da distribuição Gama foi motivada pela evidência empírica de índices de similaridade apresentando distribuições de "*long tails*" [8]. Note que, porém, esta distribuição depende do comparador sendo usado na fusão e poderia ser facilmente alterada para aplicações que utilizam diferentes tipos de comparador. Seja $Gama(x;\theta;\beta)$ denotando a distribuição de gama, onde θ e β são o parâmetro de formato e o de escala inversa, respectivamente. Logo temos:

$$p(s_i, r_i \mid F_i = 0, I = 1) = Gama(X_i; \theta_i^{imp}, \beta_i^{imp})$$
$$p(s_i, r_i \mid F_i = 0, I = 0) = Gama(X_i; \theta_i^{gen}, \beta_i^{gen})$$

onde os parâmetros $\theta_i^{imp}, \beta_i^{imp}, \theta_i^{gen}$ e β_i^{gen} são estimados baseados em dados de treinamento via máxima verossimilhança.

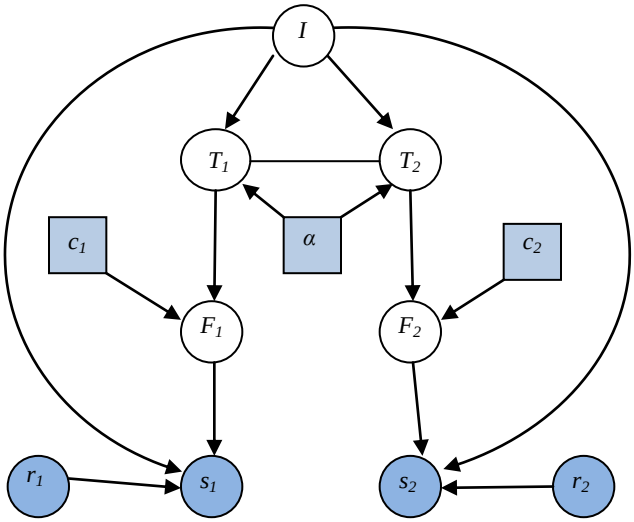

Figura 2: Modelo gráfico ilustrando a relação entre as variáveis e parâmetros. Círculos assombrados: variáveis aleatórias observadas; círculos brancos: variáveis aleatórias escondidas; quadrados assombradas: parâmetros fixos. Nosso objetivo é inferir se um usuário é impostor ($I = 1$) ou autentico ($I = 0$) baseado nas variáveis aleatórias observadas.

II. INVESTIGAÇÃO EXPERIMENTAL

O desempenho do esquema de fusão proposto foi avaliado a partir de concatenação de dois sistemas biométricos unimodais: um sistema de reconhecimento de face usando a técnica de *eigenfaces* [14] e um sistema de impressões digitais disponível publicamente desenvolvido por NIST [15]. A qualidade das amostras de impressões digitais é calculada usando o programa NFIQ [16], também desenvolvido por NIST. A qualidade das imagens de face é manualmente rotulada baseada nas seguintes informações observadas: rotação da face, nível de iluminação e expressão facial. Para aplicações práticas, a qualidade da imagem de rosto poderia ser automaticamente calculada usando os métodos descritos em [17] ou [18]. Usamos as notações subscritas *face* e *fing* para referenciar o sistema de face e o de impressões digitais, respectivamente. Por exemplo, s_{fing} denota o nível de similaridade para a dada amostra de impressões digitais. Atribuímos os parâmetros de segurança como $c_{face} = 0{,}3$ e $c_{fing} = 0{,}7$. Para o método de razão verossimilhança (*likelihood ratio* – LRR) estendida, atribuímos com $\alpha = 0{,}01$, ou seja, a probabilidade (taxa) de um ataque trapaceiro é de 1%.

O banco de dados multimodal foi gerado pela combinação aleatória entre os usuários registrados em FVC2004-DBI [19] e os de face FERET-b Series [20], gerando chamado "usuário multimodal virtual" [21]. As amostras biométricas para cada usuário virtual são aleatoriamente e unicamente combinadas para gerar as amostras multimodais usadas. A base de dados FVC2004-DBI contém 1000 impressões digitais distintas originadas de 100 usuários diferentes (10 impressões digitais por usuário), enquanto a base de dados FERET-b Series é composta de 2200 imagens de faces coletadas de 200 usuários (11 imagens por usuário).

O mesmo procedimento experimental foi repetido 10 vezes sendo que em cada rodada um novo conjunto de dados multimodais foi aleatoriamente formado e usado. Selecionamos aleatoriamente 40 usuários do conjunto de dados multimodais para treinamento dos modelos de fusão e usamos os dados dos 60 usuários restantes em testes dos modelos. Os resultados apresentados aqui são obtidos como a média aritmética dos resultados dos 10 testes rodados. Três diferentes tipos de experimentos foram executados usando estes dados bimodalisde teste:

Experimento I: O objetivo desta investigação experimental é testar os métodos de fusão sob condições normais de operação, onde não há presença de amostras de baixa qualidade. Em outras palavras, apenas aquelas amostras com $q_{face} \geq 0{,}6$ e $q_{fing} \geq 0{,}6$ são usadas nos testes.

Experimento II: Nesta parte da investigação experimental, todas as amostras são empregadas, independentemente de suas qualidades. Comparando os resultados obtidos deste experimento com os obtido no Experimento I, podemos avaliar o grau de robustez do método de fusão investigados principalmente quando estes estão sob ambiente ruidoso.

Experimento III: Esta parte da investigação experimental tem como objetivo responder a seguinte pergunta: "O que acontece com um sistema multimodal quando um sistema unimodal biométrico foi trapaceado com sucesso?" Para responder esta pergunta, o presente experimento simula um cenário onde o sistema de face tem sido trapaceado com sucesso. Assim sendo, as comparações com impostores no sistema multimodal foram feitas utilizando-se uma amostra impostora de impressão digital junto com uma amostra genuína de face de qualidades regulares, $q_{face} \geq 0{,}6$ e $q_{fing} \geq 0{,}6$. Note que para alcançar o objetivo deste experimento, estamos assumindo que não há como distinguir entre uma face genuína com aquela que trapaceou o sistema de face com sucesso.

Além de investigar os esquemas de fusão propostos na seção 2, também realizamos as simulações sobre outros esquemas de fusão descritos abaixo:

Razão Verossimilhança (LLR) [8]: A fusão LLR é caracterizada pela equação (1) apresentada anteriormente. Aqui, usamos a abordagem tradicional para estimar a distribuição genuína e a de impostora. Em outras palavras, não será considerada aqui a possibilidade de ter um ataque trapaceiro. Assim sendo, a atual cenário é equivalente ao esquema de fusão de razão verossimilhança estendido descrito na seção 2.2 com a probabilidade de um ataque trapaceiro igual a zero (ou seja, $\alpha = 0$).

Soma Ponderada: Alguns artigos [6,7] concluíram que os bons desempenhos para o método de fusão do tipo "regra de soma", mesmo quando o método é comparado com outras abordagens mais sofisticadas como redes neurais [7] e árvores de decisão [6]. O esquema de fusão de soma ponderada calcula a combinação linear entre níveis de similaridade como a seguir:

$$z = w_1 s_1 + w_2 s_2 \qquad (12)$$

onde w_i é o peso atribuído ao sistema biométrico *i*. Outra forma para expressar a equação (12) é:

$$\frac{z}{w_{face}} = z' = k s_{fing} + s_{face} \qquad (13)$$

onde $k = \frac{w_{fing}}{w_{face}}$. O valor ótimo do parâmetro *k* utilizado neste trabalho foi estimado experimentalmente através de testes exaustivos sobre os dados de treinamento.

Lógica Nebulosa: um método de fusão baseada numa abordagem de lógica nebulosa que permite a descrição explicita dos heurísticos usando expressões lingüísticas foi proposto em [13]. O sistema lógico nebuloso envolve 3 passos principais: (i) definição de variáveis nebulosas e suas funções de pertinências (*processo de fuzzificação*); (ii) construção de regras nebulosas que relacionam as variáveis nebulosas; (iii) estabelecimento de um método apropriado de defuzzificação[11]. A implementação do sistema de lógica nebulosa está baseada no método Takagi-Sugeno-Kang de primeira ordem [12].

IV. Resultados de Investigações Experimentais

Os resultados das investigações experimentais são analisados através do uso da Curva de Operação de Receptor (*Receiving Operating Curve* – ROC) [1]. Uma curva ROC é obtida pela variação do valor de decisão limiar, expressado em termos da taxa de aceitação genuína (*Genuine Acceptance Rate* – GAR) e da taxa de falsa aceitação (*False Acceptance Rate* – FAR) para cada limiar de decisão dado implicitamente. A GAR é a probabilidade de um usuário genuíno sendo corretamente aceito com genuíno e a FAR é a probabilidade de um impostor sendo erradamente aceito como genuíno. Note que freqüentemente a taxa de falsa rejeição (*False Rejection Rate* – FRR) substitui a GAR, onde FRR é a probabilidade de um genuíno sendo erradamente rejeitado e $GAR = 1 - FAR$.

Na prática um sistema biométrico normalmente opera com um único limiar de decisão para todas as situações praticas. Raramente possuímos algum conhecimento a priori sobre ataques trapaceiros contra sistemas de face, o que dificulta na seleção de um valor limiar especifico ótimo. Além disso, quando traçarmos as curvas ROC distintas para seus respectivos experimentos, os valores limiares são mantidos implícitos, o que causa a perda de referência quando os desempenhos de um mesmo sistema biométrico, porém sob diferentes experimentos são comparados. A solução adotada neste trabalho para minimizar esta deficiência usa a curva ROC do Experimento I como um performance de referência de comparação, ou seja, fixamos os limiares de decisão de referência de comparação que resultam em taxa FAR de 1%, 0,1% e 0,01% (denotada por trs_1, e $trs_{0,1}$ e $trs_{0,01}$, respectivamente). Logo, podemos avaliar as taxas FAR e FRR para outros experimentos usando sempre os mesmos limiares escolhidos. A tabela 1 lista as taxas de erro para estes limiares escolhidos. Analisando o conteúdo desta tabela, temos os seguintes comentários importantes:

- No Experimento I, os métodos de fusão de soma ponderada e de razão verossimilhança lideram os melhores desempenhos.
- No Experimento II, o método de fusão de razão verossimilhança lidera o melhor resultado. Os métodos que consideram níveis de qualidade de amostra apresentam um aumento menor na taxa FRR quando são comparados com os executados no Experimento I. Este resultado sugere o uso do parâmetro de qualidade de amostra no esquema de fusão para incrementar a robustez do sistema multimodal contra amostras ruidosas. Note que alguns métodos de fusão podem provocar um pequeno aumento na taxa FAR também.
- No Experimento III, ambas as abordagens de fusão, a de soma ponderada e a de razão verossimilhança, apresentaram um aumento drástico da taxa FAR em comparação com a FAR de referencia (Experimento I). Por exemplo, quando a fusão LLR operando com o limiar $trs_{0,1}$, um impostor que tem sucedido em trapacear o sistema biométrico de face possui a 42,99% de chance de ser aceito usando sua própria impressão digital, enquanto para a fusão de lógica nebulosa, sua chance se reduz a 4,71% e para a fusão probabilística, 4,33% (apresentados pelos números realçados na coluna $trs_{0,1}$).

Ainda ampliarmos nossa análise comparativa entre os Experimentos I e III conforme relatada a seguir. Para cada valor de FAR no Experimento I (denotado por FAR_1), fixamos o limiar e avaliamos a FAR correspondente no Experimento III (denotado por FAR_3). Os resultados desta análise são mostrados na figura 3. Pode-se notar que a fusão LLR, qual oferece o melhor desempenho nos Experimentos I e II, foi a mais afetada pelo ataque trapaceiro sobre o sistema de face. Na realidade o método de soma ponderada também foi afetado significativamente. A fusão de lógica nebulosa apresentou os melhores resultados. Para baixos valores de FAR_1, seu desempenho é semelhante ao da fusão probabilística (LLR estendida). Este resultado demonstra que a introdução do parâmetro de segurança pode realmente aumentar o grau de segurança do esquema de fusão.

Tabela I: Comparação de taxas de erro para valores limiares de decisão de referencia fixos.

			Experim. I		Experim. II		Experim. III	
Reference	System	Thrs.	FAR(%)	FRR(%)	FAR(%)	FRR(%)	FAR(%)	FRR(%)
trs_1	Fing	17.34	1.01	17.70	1.08	19.43	1.27	18.83
	Face	0,55	1,00	28,01	0,54	68,73	72,38	27,62
	ProbF	2,68	1,00	6,96	1,57	11,95	52,26	6,52
	Fuzzy	0,21	1,00	8,52	1,25	14,02	24,40	8,02
	LLR	1,85	1,00	4,88	1,14	12,59	69,36	4,77
	WSum	0,71	1,00	5,36	0,61	20,29	68,02	5,01
$trs_{0.1}$	Fing	24,07	0,10	25,16	0,12	27,63	0,06	26,41
	Face	0,70	0,10	54,49	0,05	82,53	45,83	54,17
	ProbF	31,42	0,10	18,04	0,22	22,31	**4,33**	18,83
	Fuzzy	0,30	0,10	15,21	0,16	21,46	**4,71**	15,36
	LLR	6,30	0,10	11,63	0,11	21,54	**42,09**	11,69
	WSum	0,88	0,10	11,60	0,06	28,85	**38,51**	11,85
$trs_{0.01}$	Fing	30,94	0,01	33,23	0,02	34,63	0,03	34,09
	Face	0,78	0,01	71,22	0,00	90,20	28,51	71,49
	ProbF	185,94	0,01	29,59	0,00	63,12	0,80	31,70
	Fuzzy	0,39	0,01	22,33	0,02	28,91	0,80	22,24
	LLR	10,57	0,01	18,48	0,03	29,12	26,30	18,27
	WSum	1,01	0,01	18,87	0,01	36,13	12,25	19,49

A. Validação

Nesta seção, realizamos a validação dos resultados mostrados na seção anterior usando um conjunto de dados diferente: *The NIST Biometric Scores Set – Release 1* [22], que é um banco de dados multimodais contendo valores numéricos de nível de similaridade para um sistema biométrico de face e o de impressão digital. Foram escolhidos o conjunto de imagens de impressão digital do polegar e o conjunto "C" de reconhecimento de face. Como este banco de dados que não apresenta os níveis de qualidade das amostras, assumimos que as amostras possuem o mesmo grau de qualidade.

A figura 3 mostra a comparação entre FAR do Experimento I e a do Experimento III para os conjuntos de dados descritos acima sob o cenário onde a biometria de face foi trapaceada com sucesso. A figura 4 mostra o mesmo tipo de gráfico porém, num cenário onde a biometria de impressão digital foi trapaceada. As informações dadas pelas ambas as figuras validam a observação obtida anteriormente, ou seja, o proposto método de fusão (LLR estendido) e Lógica Nebulosa são mais robustos contra ataque trapaceiro quando comparados com o método LLR convencional e o de soma ponderada.

V. CONCLUSÃO

Neste trabalho efetuamos uma análise sobre impactos gerados pelo ataque trapaceiro em sistemas biométricos bimodais. As investigações experimentais demonstraram que quando os esquemas tradicionais (ou seja, razão verossimilhança e soma ponderada) forem usados, um falsificador pode aumentar drasticamente a chance de rachar um sistema multimodal trapaceando apenas um dos biométricos. Para reduzir esta deficiência, propusemos um novo esquema de fusão biométrica que leva em consideração do nível de segurança de cada sistema biométrico unimodal envolvido. Os resultados dos experimentos realizados revelam a existência de um compromisso entre a precisão de reconhecimento biométrico e a robustez contra ataque trapaceiro.

Os experimentos ainda apontam que o esquema de fusão via lógica nebulosa oferece o melhor desempenho global em relação ao esquema de fusão probabilística. Para trabalho futuro, iremos implementar um procedimento de treinamento que é capaz de automaticamente otimizar funções de pertinência na fusão por lógica nebulosa e efetuar testes dos ambos esquemas de fusão com um range maior de parâmetros.

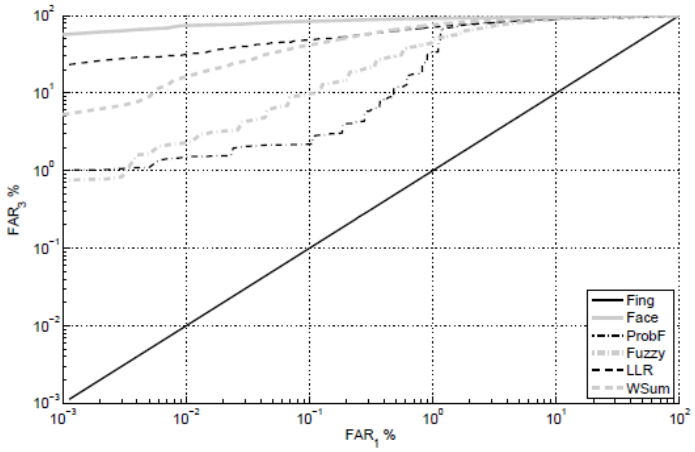

Figura 3: Comparação entre FAR do Experimento I (FAR_1) e FAR do Experimento III (FAR_3) em cenários onde os traços de faces foram trapaceados.

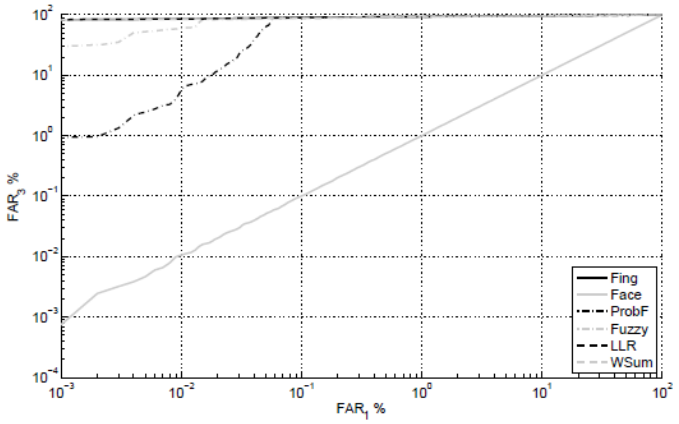

Figura 4: Comparação entre FAR do Experimento I (FAR_1) e FAR do Experimento III (FAR_3) em cenários onde os dados de impressão digital foram trapaceados.

REFERÊNCIAS

[1] A. K. Jain, A. Ross, and S. Prabhakar, "An introducation to biometric recognition," *IEEE Transactions on Circuit and Systems for Video Technology*. vol. 14, no. 1. January 2004.

[2] C. Sanderson and K. K. Paliwal, "Identity verification using speech and face information," *Digital Signal Processing*, vol. 14, pp. 449-480, 2003.

[3] J. Bigun, J. Fierrez-Aguilar, J. Ortega-Garcia, J. Gonzalez-Rodriguez, "Multimodal biometric authentication using quality signals in mobile communications" *Proceedings of the 12th International Conference on Image Analysis and Processing (ICIAP03)*, August 2003.

[4] J. Fierrez-Aguilar, J. Ortega-Garcia, J. Gonzalez-Rodriguez, and J. Bigun, "Discriminative Multimodal biometric authentication based on quality measures," *Pattern Reocogntion*, vol. 38, no. 5, pp. 777-779, May 2005.

[5] K.-A. Toh , X. Jiang and W.-Y. Yau, "Exploiting Global and Local Decisions for Multimodal Biometrics Verification," *IEEE Transactions on Signal Processing*, vol. 52, no. 10, pp. 3059-3072, October 2004.

[6] A. Ross, A. K. Jain, "Information Fusion in Biometrics," *Pattern Recognition Letters*, vol. 24, 2003.

[7] Y. Wang, T. Tan, and A. K. Jain, "Combining Face and Iris Biometrics for Identity Verification," *Lecture Notes in Computer Science*, vol. 2688, pp. 805-813, 2003.

[8] K. Nandakumar, Y. Chen, S. C. Dass, and A. K. Jain, "Likelihood ration-based biometric socre fusion," *IEEE Transactions on Pattern Analysis and Machine Intelligence*, vol. 30, no. 2, pp. 342-348, February 2008.

[9] S. Tulyakov and V. Govindaraju, "Classifier combination types for biometric applicaions," Computer Vision and Pattern Recognition Workshop (CVPRW), 2006.

[10] C. Soutar, "Biometric system security," 2004. Http://www.bioscrypt.com/assets/security_soutar.pdf.

[11] W. Pedry and F. A. C. Gomide, *An Introduction to Fuzzy Sets: Analysis and Design (Complex Adaptive Systems).* MIT Press, 1998.

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

[13] Lee L. Ling, Ricardo N. Rodriques and Jennifer C. Lee, "Fusão Biométric com Lógica Nebulosa", Anais do XXVI Simpósio Brasileiro de Telecomunicações, Setembro, 2008.

[14] M. A. Turk and A. P. Pentland, "Face recognition using eigenfaces," In *Proceedings of Computer Vision and Pattern Recognition*, pp. 586–591, 1991.

[15] "NIST fingerprint software," National Institute of Standards and Technology (NIST), Intenet Page, March 2006. Http://fingerprint.nist.gov/NFIS/.

[16] E. Tabassi, C. L. Wilson, and C. I. Watson. "Fingerprint image quality," National Institute of Standards and Technology (NIST), Technical Report NISTIR 7151, Aug. 2004.

[17] Y. Yao, B. Abidi, and M. Abidi, *Quality Assessment and Restoration of Face Images in Long Rang/High Zoom Video*. Springer, 2007, ch.4, pp. 43-60.

[18] Q. Xiong and C. Jaynes, "Mugshot database acquisition in video surveillance networks using incremental auto-clustering quality measures," in *AVSS '03: Proceedings of the IEEE Conference on Advanced Video and Signal Based Surveillance.* Washington, DC, USA: IEEE Computer Society, 2003, p.191.

[19] "FVC2004: Third international fingerprint verification competition," University of Bologna, Internet page, 2006. Http://bias.csr.unibo.it/fvc2004/.

[20] NIST, "The facial recognition technology (FERET) database," National Institute of Standards and Technology (NIST), Tech. Rep. NISTIR 7151, August. Http://www.itl.nist.gov/iad/humanid/feret/feret_Master.html.

[21] R. Snelick, U. Uludag, A. Mink, M. Indovina, and A. Jain, "Large-scale evaluation of multimodal biometric authentication using state-of-the-arte systems," *IEEE Transactions on Pattern Analysis and Machine Intelligence*, vol. 27, no. 3, pp. 450-455, March 2005.

[22] NIST, "Biometric scores set," National Institute of Standards and Technology (NIST), Tech. Rep. BSSR1, October 2004. Http://www.itl.nist.gov/iad/894.03/biometricscores/.