UNIVERSIDADE FEDERAL DE SANTA CATARINA
PROGRAMA DE PÓS-GRADUAÇÃO EM CIÊNCIA DA COMPUTAÇÃO

Sérgio Roberto de Lima e Silva Filho

AUTENTICAÇÃO CONTÍNUA PELA DINÂMICA DA DIGITAÇÃO USANDO MÁQUINAS DE COMITÊ

Dissertação submetida à Universidade Federal de Santa Catarina como parte dos requisitos para a obtenção do grau de Mestre em Ciência da Computação

Prof. Mauro Roisenberg, Dr.
Orientador

Florianópolis, Novembro de 2005

AUTENTICAÇÃO CONTÍNUA PELA DINÂMICA DA DIGITAÇÃO USANDO MÁQUINAS DE COMITÊ

Sérgio Roberto de Lima e Silva Filho

Esta Dissertação foi julgada adequada para a obtenção do título de Mestre em Ciência da Computação, área de Concentração Sistemas de Conhecimento e aprovada em sua forma final pelo Programa de Pós-Graduação em Ciência da Computação.

_____

Prof. Raul Sidnei Wazlawick, Dr. (Coordenador)

Banca Examinadora

_____

Prof. Mauro Roisenberg, Dr. (Orientador)

_____

Prof. Guilherme Bittencourt, Dr.

_____

Prof. Raul Sidnei Wazlawick, Dr.

_____

Prof. Ricardo Felipe Custódio, Dr.

_____

Prof. Jovelino Falqueto, Dr.

Ofereço este trabalho a meus pais
que são os responsáveis por
mais esta conquista em
minha vida.

Agradecimentos

Primeiramente agradeço a Deus por ter me dado saúde e força para vencer mais esta etapa em minha vida.

Agradeço também a Universidade Federal de Santa Catarina, em especial ao Departamento de Pós-Graduação em Ciência da Computação.

A Mauro Roisenberg pela excelente orientação, cooperação e incentivo. Não apenas durante a realização desta dissertação, mas em toda minha formação superior.

Aos membros da banca: Guilherme Bittencourt, Raul Sidnei Wazlawick, Ricardo Felipe Custódio e Jovelino Falqueto, pelas excelentes contribuições à dissertação.

Agradeço muito a meus pais Sérgio Roberto de Lima e Silva e Célia Maria Cinto de Lima e Silva por minha educação e principalmente pelas oportunidades oferecidas durante toda minha vida, principalmente acadêmica. Oportunidade esta que não tiveram em suas vidas, portanto divido com vocês o mérito de meu trabalho.

Agradeço a minha namorada Karina Fries, pelo amor, carinho, incentivo e compreensão.

A Marcelo Brocardo, pela compreensão em me liberar do serviço nos momentos de necessidade.

A todas as pessoas que contribuíram com este trabalho na coleta de informações do padrão de digitação e todos meus amigos.

Sumário

Lista de Figuras viii

Lista de Tabelas ix

Lista de Siglas x

Resumo xi

Abstract xii

Capítulo 1 - Introdução 1

Introdução 1

1.1 – Motivação 1

1.2 – Objetivos 5

1.2.1 – Objetivo Geral 5

1.2.2 – Objetivos Específicos 6

1.3 – Justificativa 6

1.4 – Organização da Dissertação 9

Capítulo 2 – Biometria e a Dinâmica da Digitação 10

Introdução 10

2.1 - Biometria 10

2.1.1 – Métodos Automáticos 11

2.1.2 – Identificação e Verificação 12

2.1.3 – Pessoa Viva 13

2.1.4 – Características Fisiológicas e Comportamentais 13

2.1.5 – Medidas de Desempenho 14

2.2 – Funcionamento dos Sistemas Biométricos 16

2.3 – Métodos de Identificação por Prova Biométrica 18

2.3.1 – Impressão Digital 18

2.3.2 – Padrões do Olho 19
2.3.3 – Escaneamento da Mão 19
2.3.4 – Outros Dispositivos Fisiológicos 19
2.3.5 – Dispositivos para Características Comportamentais 20
2.3.6 – Dinâmica da Digitação 20
2.4 – Trabalhos Relacionados 23
2.5 – Conclusão 28

Capítulo 3 - Reconhecimento de Padrões e Redes Neurais Artificiais 30

Introdução 30
3.1 – Reconhecimento de Padrões 30
3.2 – Redes Neurais 33
3.2.1 – Modelos de Neurônios 34
3.2.1.1 – Modelo de McCulloch-Pitts 35
3.2.1.2 – Modelo Geral de Neurônio 35
3.2.2 – A Rede Neural Artificial 36
3.2.3 – Máquinas de Comitê 37
3.2.5.1 – Média de Ensemble 39
3.2.5.2 – Reforço 40
3.3 – Conclusão 40

Capítulo 4 – Definindo a Aplicação 41

Introdução 41
4.1 – Metodologia do Sistema Biométrico Proposto 41
4.2 – Aspectos Importantes na Definição do Sistema Biométrico 46
4.2.1 – Usuários Analisados 46
4.2.2 – Informação Alvo e o Coletor de Dados 47
4.2.3 - Ambiente de Coleta 50
4.2.4 – Quantidade de Amostras 50
4.2.5 – Características Coletadas e Armazenamento 50

4.2.6 – Precisão do Tempo 51
4.2.7 – Redução da Dimensionalidade 52
4.2.8 – Conjuntos de Treinamento e de Testes do Usuário 52
4.2.9 – Classificação 53
4.3 – Ferramentas Implementadas 54
4.3.1– RNA 54
4.3.2 – Manipulador de Dados 57
4.4 – Infra-Estrutura e Ferramentas Utilizadas 60
4.5 – Conclusão 61

Capítulo 5 – Experimentos e Resultados 62

Introdução 62
5.1 – Experimento 1 - Análise dos Parâmetros Configuráveis da RNA 62
5.1.1 – Resultados do Experimento 1 63
5.2 – Experimento 2 – Utilização de RNA Única para Representar o Usuário 65
5.2.1 – Resultados do Experimento 2 66
5.3 – Experimento 3 – Utilização de Máquina de Comitê para Representar o Usuário 69
5.3.1 – Etapa 1 - Análise sobre a Frase Fixa 69
5.3.1.1 – Resultados do Experimento 3 etapa 1 70
5.3.2 – Etapa 2 - Análise sobre o Texto Fixo 75
5.3.2.1 – Resultados do Experimento 3 etapa 2 75
5.3.3 – Etapa 3 - Análise sobre o Texto Fixo e Texto Livre 80
5.3.3.1 – Resultados do Experimento 3 etapa 3 80
5.4 – Experimento 4 – Utilização de Limiares Individuais para cada Usuário 82
5.5 – Resultados dos experimentos 85
5.6 – Conclusão 86

Capítulo 6 - Conclusão 87
6.1 – Trabalhos Futuros 89

Referências Bibliográficas 91

Lista de Figuras

Fig. 2.1- Relação entre FAR e FRR (adaptado de [3]) *15*
Fig. 2.2 - Funcionamento básico dos sistemas biométricos (adaptado de [26]). *16*
Fig. 2.3 - Principais métodos de identificação biométricas (adaptado de [3]). *18*
Fig. 3.1 - Processo de reconhecimento de padrão (adaptado de [13]) *31*
Fig. 3.2 - O neurônio (extraído de [40]). *34*
Fig. 3.3 - Modelo de Waren McCulloch e Walter Pitts (adaptado de [5]). *35*
Fig. 3.4 - Neurônio artificial (extraído de [40]). *35*
Fig. 3.5 - Exemplo de RNA (adaptado de[5]). *36*
Fig. 3.6 - Máquina de comitê baseada em média de ensemble (adaptado de [18]) *39*
Fig. 4.1 - Estrutura composta por uma RNA para representação do usuário *42*
Fig. 4.2 - Estrutura baseada em máquinas de comitê para representação do usuário. *42*
Fig. 4.3 - Treinamento da estrutura baseada em máquinas de comitê. *43*
Fig. 4.4 - Procedimento de coleta e formação do modelo *43*
Fig. 4.5 - Procedimento de classificação do usuário *45*
Fig. 4.6 - Coletor de dados *48*
Fig. 4.7 - Freqüência das latências entre teclas de pressionamento *55*
Fig. 4.8 - Exemplo de propagação de valores de entrada a RNA composta por 257 neurônios na camada de entrada e 2 neurônios na camada intermediária. *56*
Fig. 4.9 - Manipulador de dados. *59*
Fig. 5.1 - Representando o problema do experimento 2 ..... *67*
Fig. 5.2 - O problema do experimento 2 separado por usuário. *68*

Lista de Tabelas

Tabela 2.1 - Resumo das principais pesquisas de autenticação estática (adaptado de [3]) *27*
Tabela 2.2 - Resumo das principais pesquisas de autenticação dinâmica (adaptado de [3]) *28*
Tabela 4.1 - Quantidade de usuários por grupo pesquisado *47*
Tabela 5.1 - Eficiência das RNA quanto ao número de neurônios de entrada *64*
Tabela 5.2 - FRR obtido na etapa 1 do experimento 3 ..... *71*
Tabela 5.3 - FAR de usuários do grupo 1 obtido na etapa 1 do experimento 3 ..... *72*
Tabela 5.4 - FAR de usuários do grupo 2 obtido na etapa 1 do experimento 3 ..... *73*
Tabela 5.5 - Taxas de proporção de erros da etapa 1, experimento 3 ..... *74*
Tabela 5.6 - FRR obtido na etapa 2 do experimento 3 ..... *76*
Tabela 5.7 - FAR de usuários do grupo 1 obtido na etapa 2 do experimento 3 ..... *77*
Tabela 5.8 - FAR de usuários do grupo 2 obtido na etapa 2 do experimento 3 ..... *78*
Tabela 5.9 - Taxas de proporção de erros da etapa 2, experimento 3 ..... *79*
Tabela 5.10 - Taxas de proporção de erros da etapa 3, experimento 3 ..... *81*
Tabela 5.11 - Resultados do experimento 4 para frase fixa *83*
Tabela 5.12 - Resultados do experimento 4 para texto fixo *84*
Tabela 5.13 - Resultados do experimento 4 para texto fixo e texto livre *85*
Tabela 5.14 – Resumo dos resultados obtidos neste trabalho *86*

Lista de Siglas

FAR	Taxa de falsa aceitação (*False Aceptance Rate*)
FRR	Taxa de falsa rejeição (*False Rejection Rate*)
RNA	Rede Neural Artificial
ANN	Artificial Neural Network
TPE	Taxa de proporção de erros

Resumo

O uso de sistemas automatizados simplifica a vida das pessoas, no entanto a dependência destes sistemas gera informações críticas armazenadas nos computadores tornando-os possíveis alvos de ataques. Para proteger o acesso a estas informações existem mecanismos de autenticação. Atualmente a maioria destes mecanismos autentica o usuário apenas na entrada do sistema, sendo que o usuário pode deixar o computador sem sair da sessão ou bloquear seu acesso, possibilitando a um intruso acessar os recursos disponíveis. Isto mostra a insuficiência dos mecanismos de autenticação realizados apenas na entrada do sistema.

O objetivo deste trabalho é apresentar uma metodologia de baixo custo e não intrusiva que possibilite a autenticação contínua do usuário enquanto este está utilizando o teclado de um computador. A autenticação é realizada através do reconhecimento do padrão de digitação do usuário, que é uma característica biométrica comportamental.

Neste trabalho foram abordadas duas metodologias para solução deste problema de reconhecimento de padrões, ambas utilizando Redes Neurais Artificiais (RNAs). Na primeira abordagem, uma única RNA é utilizada para representar o modelo de cada usuário e classificar dados apostos ao sistema biométrico, já na segunda abordagem é utilizado o conceito de máquinas de comitê, onde um conjunto de RNAs combinadas formam o modelo do usuário. Cada uma destas RNAs possui a capacidade de resolver uma tarefa simples, mas ao serem combinadas possibilitam a solução de uma tarefa complexa.

Experimentos realizados para testar as abordagens propostas mostram que a utilização da primeira abordagem não possibilitou a classificação dos usuários testados neste trabalho, no entanto na segunda abordagem, os resultados mostram que, utilizando como informação alvo um texto fixo e limiares diferentes para cada usuário, o sistema apresentou taxa de falsa aceitação (FAR) de 0,15% e taxa de falsa rejeição (FRR) de 0%.

Palavras-chave: autenticação, dinâmica da digitação, redes neurais artificiais, máquinas de comitê.

Abstract

The automation of systems have simplified the life of people, however the dependency on these systems generates critical information stored in computers becoming them targets of attacks. In order to protect the access to the information that is considered critical, the use of authentication mechanisms has been adopted. Nowadays, most of these mechanisms authenticate the user only in the entry of the system, being that the user can leave the computer without logging out or locking its access, this gives an intruder a chance to have access rights to the available resources. This shows the insufficiency of mechanisms of authentication only in the entry of the system.

The objective of this work is to present an inexpensive and not-intrusive methodology that makes possible the continuous authentication of the user while he is using the keyboard of a computer. The authentication is performed through the pattern recognition of the users' keystroke, which is a behavioral biometric characteristic.

This work presents two Artificial Neural Networks (ANNs) methodologies as alternative solution for this pattern recognition problem. In the first methodology just one ANN is used to represent the template of each user and to classify data presented to the biometric authentication system. The second methodology uses the concept of committee machines, where a set of ANNs builds the template of a given user. This ANNs show the capacity to solve a simple task but when being combined they make possible the solution of a complex task.

Based on experiments performed on the proposed methodologies, it's possible to conclude that by using the first methodology it is not possible to classify the users tested in this work. However in the second methodology the results show that using as target information a fixed text and different thresholds for each user the system presented false acceptance rate (FAR) of 0.15% and false rejection rate (FRR) of 0%.

Keywords: authentication, keystroke dynamics, artificial neural networks, committee machine.

Capítulo 1 - Introdução

Introdução

Neste capítulo é apresentada a motivação para a escolha do tema da dissertação: autenticação segura e contínua de usuários em um computador ou sistema. Apresentam-se ainda os objetivos (geral e específicos) a serem atingidos e a justificativa da utilização da dinâmica de digitação, como "ferramenta" complementar, na autenticação de usuários em sistemas computacionais. No final deste capítulo é apresentada a forma em que esta dissertação foi organizada.

1.1 – Motivação

Nos dias atuais houve um aumento no número de pessoas que utilizam os computadores para realizar suas tarefas diárias. Estas tarefas podem ser simples, como por exemplo, escrever textos como este, ou mais complexas como administrar toda uma empresa através do computador. Com os sistemas disponíveis atualmente, é possível manter todos os documentos da empresa na forma digital, realizar pagamentos através de sistemas bancários disponíveis na internet, trocar mensagens com parceiros corporativos, entre outras.

Este aumento significativo de sistemas automatizados simplifica em muito a vida das pessoas, mas ao mesmo tempo, estas se tornam extremamente dependentes dos computadores e da Internet, pois estes serviços aumentam a produtividade e diminuem os custos [17],[31],[33].

Com esta facilidade de se realizar cada vez mais tarefas a um menor custo, a quantidade de informações sigilosas, valiosas e críticas, tanto pessoais como corporativas armazenadas nos computadores, aumentou drasticamente nos últimos anos [2], [30], [37]. Com isto os computadores vêm se tornando alvos de ataques, pois o atacante pode se

apoderar de informações valiosas. Estes ataques podem ser realizados localmente ou através da Internet.

Estes crimes podem causar sérios danos, incluindo queda de comunicação, visualização de documentos classificados, destruição, falsificação e roubo de informações [2],[25].

Imagine um usuário que armazena a senha de sua conta bancária em um arquivo em seu computador. Se uma pessoa não autorizada conseguir o acesso a este computador, poderá verificar qual a senha bancária e através da própria Internet, com seus sistemas automatizados, poderia movimentar dinheiro para uma outra conta. Ainda, se o usuário da máquina realiza compras constantes com o cartão de crédito e mantém o número do cartão armazenado, o invasor teria um número de cartão de crédito para comprar o que quisesse via lojas virtuais.

Portanto um grande problema nos computadores e sistemas computacionais é a necessidade de um mecanismo de autenticação do usuário, que possibilite que apenas usuários válidos tenham acessos aos recursos computacionais críticos, sejam estes o próprio acesso ao computador, a um determinado sistema ou ainda a uma determinada informação. Para isto, devem existir mecanismos eficientes de autenticação para que pessoas não autorizadas não consigam se passar por pessoas válidas e acessar estes recursos restritos [11],[14],[23],[36]. Mas como um usuário pode ser autenticado?

Para responder esta pergunta pode-se definir e exemplificar os mecanismos de autenticação a partir de uma síntese das referências [3],[12],[27],[31] classificando 3 mecanismos de autenticação:

- Através de algo que somente o usuário sabe;
- Através de algo que somente o usuário possui;
- Através de algo que o indivíduo é.

Um exemplo para a primeira forma de autenticação é a utilização de uma senha ou número de identificação pessoal. Esta forma é a mais utilizada nos sistemas e computadores utilizados atualmente, pois é simples e tem baixo custo de implementação. No entanto, apresenta graves problemas: a perda, o extravio ou a observação da digitação da senha

possibilita que pessoas não autorizadas acessem os recursos desejados. Outra fragilidade do processo que pode ser citada é que geralmente as pessoas utilizam senhas "fáceis" de serem descobertas, como por exemplo, o nome, data de nascimento, palavras conhecidas etc.. Esta classe de senhas permite ataques do tipo "ataque do dicionário" onde um indivíduo, através de ferramentas específicas, pode descobrir a senha do usuário facilmente. Inúmeros outros problemas podem ser citados, como a dificuldade de gerenciar um grande número de senhas que muitas vezes levam as pessoas a anotá-las, correndo o risco de cair no exemplo de roubo de informação, citado anteriormente. Este tipo de autenticação é também conhecido como autenticação por prova de conhecimento.

Na segunda forma de autenticação, podem-se citar os cartões magnéticos, *smart-cards* e *tokens*. Estes dispositivos podem armazenar informações do usuário, como por exemplo, um certificado digital e sua respectiva chave privada. Neste tipo de autenticação, também conhecido como prova por posse, a segurança é muito maior, pois é necessário que o usuário possua um dispositivo que libere seu acesso ao recurso computacional.

Geralmente este tipo de autenticação é realizado em conjunto com o primeiro mecanismo. Desta forma um possível violador terá que conhecer a senha para liberação de acesso à chave privada contida em um *smart-card*, por exemplo, e ainda precisará ter posse do cartão contendo as informações. O extravio das informações contidas nestes cartões ou *tokens* pode ocorrer por perda, roubo ou "clonagem". Este último exemplo não é possível com o uso de certificação digital, pois a chave privada correspondente à chave pública de um determinado certificado digital, não pode ser "clonada" se estiver armazenada em algum dispositivo seguro como, por exemplo, *tokens* ou *smart-cards*.

A utilização de certificados digitais e sua respectiva chave privada, nestes dispositivos, tornam inviável computacionalmente descobrir qual a chave privativa correspondente ao certificado do usuário (chave pública), fazendo com que o ataque mais eficiente seja a descoberta da senha de liberação de uso da chave privada, porém estes dispositivos muitas vezes implementam formas de dificultar o ataque para se descobrir esta senha de liberação. Estes mecanismos incluem o apagamento do conteúdo do dispositivo, ou o bloqueio do mesmo se a senha for digitada de maneira incorreta algumas vezes, ou ainda exigindo a espera de um determinado tempo para que duas tentativas de senha possam ser realizadas, o que inviabiliza o ataque por força bruta. Portanto este mecanismo

de autenticação é muito mais seguro e vem ganhando muito espaço nos sistemas de autenticação de usuários. Como problemas deste mecanismo, podemos citar o custo elevado de alguns dispositivos de armazenamento de informações, além de problemas que serão abordados a seguir. Para se obter maiores informações sobre infra-estrutura de chaves públicas e certificados digitais, sugere-se a leitura de [19],[41],[43].

Por fim a terceira forma de autenticação, conhecida como prova por biometria, é baseada em uma característica fisiológica ou comportamental do indivíduo. Como exemplos de características fisiológicas têm-se a impressão digital, leitura da íris, padrão das linhas da mão, etc., já as características comportamentais podem ser a dinâmica da digitação, reconhecimento de voz, entre outros. Esta forma de autenticação é a mais segura já que não se pode roubar o que o indivíduo é. É claro que o usuário pode ser coagido a se identificar através de um mecanismo de biometria, no entanto esta discussão não faz parte do objetivo da dissertação. O principal problema da maioria dos procedimentos de autenticação por biometria é o elevado custo dos dispositivos de captação e análise dos dados necessários na autenticação. O capítulo 2 é específico sobre o assunto biometria, e contém informações mais detalhadas sobre este tema.

Definidos os mecanismos de autenticação, podemos concluir que existem mecanismos seguros e eficientes. No entanto, estes mecanismos geralmente são caros e apresentam um problema pouco abordado nos sistemas de autenticação usados hoje em dia e que é a motivação do desenvolvimento deste trabalho. O problema é que na maioria destes mecanismos de autenticação o usuário é autenticado apenas na entrada do sistema e, portanto, o usuário não necessita se autenticar durante todo o tempo em que está utilizando um determinado recurso computacional, mas apenas se autentica no acesso ao mesmo. Como citado em [42] um usuário pode deixar seu computador sem sair ou bloquear o mesmo, dando uma chance ao intruso de utilizar o sistema. Isto mostra a insuficiência dos mecanismos de autenticação, seja ele qual for, se for aplicado apenas na entrada do sistema. Voltando ao exemplo de roubo de informações citado anteriormente, mesmo que o acesso ao computador fosse realizado com certificados digitais (e sua respectiva chave privada) ou através da impressão digital (biometria), que são mecanismos muito seguros e eficientes, se o usuário autêntico que utilizou o mecanismo de autenticação confiável para acessar o recurso foi corretamente validado e saiu para tomar um café, esquecendo seu computador

ligado, outra pessoa pode facilmente ter acesso às suas informações críticas, possibilitando a ocorrência de danos já citados.

Muitos usuários não se preocupam suficientemente ou não conhecem os perigos existentes na utilização de recursos computacionais, portanto este trabalho visa desenvolver um método de autenticação seguro, barato e contínuo do usuário. Assim, desde o momento do acesso ao recurso até o momento em que o usuário não estiver mais utilizando o mesmo, este deverá ser autenticado. Desta forma se o usuário sair de seu computador para tomar um cafezinho ou para ir a uma reunião, não precisa se preocupar com as informações sigilosas armazenadas, pois o mesmo estará seguro de ataques de pessoas não autorizadas em todo momento. Se alguma pessoa sem autorização tentar acessar o sistema, esta não será autenticada e o sistema poderá realizar alguma ação para resolver este problema de identidade, como, por exemplo, bloquear o recurso até que uma nova autenticação bem sucedida seja realizada na solicitação do recurso, e durante sua utilização.

1.2 – Objetivos

1.2.1 – Objetivo Geral

O objetivo principal deste trabalho é implementar um método de autenticação seguro e contínuo do usuário através da característica biométrica de dinâmica da digitação com a utilização de Redes Neurais Artificiais (RNAs). O método deve ser utilizado em conjunto com métodos já existentes como os certificados digitais. Visa-se também comparar os resultados obtidos com os resultados de trabalhos já realizados na área de autenticação baseada na dinâmica da digitação.

1.2.2 – Objetivos Específicos

Como objetivos específicos podem-se listar:

- Implementação de uma aplicação para coletar amostras de digitação de usuários, analisar os dados coletados, executar a fase de treinamento e testes utilizando RNAs e que possa mostrar graficamente os tempos das amostras digitadas;
- Procurar obter resultados aceitáveis comparados aos trabalhos já realizados nesta área;
- Abster-se da necessidade de tratamento e verificações especiais dos erros de digitação cometidos pelo usuário, sendo que quando o mesmo comete tais erros o sistema deverá considerar a amostra;

1.3 – Justificativa

Através do conceito de autenticação, pode-se constatar que o ideal, mais seguro e confiável, seria aplicar as três formas possíveis de autenticação no mecanismo de acesso aos computadores ou sistemas. Como visto, a segunda forma de autenticação pode incluir a primeira, pois é possível habilitar o acesso à chave privada de um *smart-card*, que é algo que você tem, com uma senha, ou seja, algo que você sabe. Portanto a única forma de autenticação que faltaria é a autenticação por prova de biometria. Além disto, uma necessidade básica para cumprir os objetivos da dissertação é que a autenticação por prova de biometria seja contínua, ou seja, durante todo o processo de utilização do recurso o usuário deve ser autenticado.

A autenticação contínua é inviável através do primeiro mecanismo de autenticação, pois seria uma tarefa extremamente cansativa ter que ficar digitando a senha várias vezes no acesso a um recurso. Na utilização do segundo mecanismo, caso fosse necessário inserir o *smart-card* várias vezes durante o acesso ao recurso, muitos usuários deixariam o mesmo sempre conectado ao computador, podendo esquecê-lo conectado ao sair para tomar seu

café. Isto também possibilitaria o acesso a um intruso, por isso os métodos de autenticação por biometria são os melhores na autenticação contínua. Entretanto, a maioria destes métodos podem ser descartados, pois seria totalmente inviável o usuário ter que constantemente colocar o dedo polegar num leitor de impressão digital, ou ainda ficar falando num reconhecedor de voz. Por este motivo à autenticação pela dinâmica da digitação, que é apresentada em detalhes no capítulo 2, foi à escolhida para autenticar o usuário continuamente.

Para este trabalho será então utilizado o método de reconhecimento de padrão do usuário para autenticação mediante a dinâmica de sua digitação.

Outros fatores que levam a escolha desta abordagem são[3],[10]:

- baixo custo de implementação deste método de prova por biometria, pois é necessário apenas um teclado e um software para coleta, treinamento e verificação do padrão do usuário. Diferentemente, noutros métodos são necessários caríssimos sistemas de captação da característica;
- não intrusivo, ou seja, o usuário não se sente constrangido ao digitar dados em um teclado. Muitas vezes ele pode nem saber que está sendo analisado para a autenticação, diferentemente de outros sistemas como, por exemplo, a leitura da íris. Neste método de autenticação a pessoa precisa colocar um olho num aparelho que irá fazer uma varredura da íris, podendo constranger a pessoa por ter que provar que é ela mesma, além de causar o constrangimento de expor seu olho a um feixe de luz que fará a leitura da íris;

Portanto a escolha do método de autenticação pela dinâmica da digitação é um dos mais apropriados, pois além deste ser um dos únicos que possibilitam a autenticação contínua, não acarreta em custos para a implementação e não é constrangedor para posterior autenticação. A única etapa onde este método pode se tornar um pouco desagradável é na coleta dos dados para treinar uma aplicação capaz de reconhecer os padrões do usuário posteriormente. Este empecilho como alguns outros serão discutidos ao longo da dissertação.

Em [30] é citado que os sistemas que utilizam classificadores neurais treinados por retro-propagação apresentam alta performance nos resultados, entretanto ressalta que a cada novo usuário adicionado no sistema, as RNAs tem que ser retreinadas. Explorando esta alta performance das RNAs treinadas por retro-propagação, nos sistemas de reconhecimento de padrões, este trabalho utiliza este tipo de classificador. Para solucionar o problema da necessidade de retreinamento destas RNAs na adição de novos, este trabalho também estuda a utilização destas RNAs dispostas em uma máquina de comitê.

Antes de apresentar a organização desta dissertação, duas observações importantes relativas ao trabalho devem ser descritas:

- O sistema de autenticação contínua estudado neste trabalho leva em consideração apenas as entradas relativas à digitação do usuário em seu teclado durante a utilização de seu computador. Atualmente existem outras formas de utilização de um computador como, por exemplo, através do mouse, no entanto as entradas referentes a este dispositivo não são tratadas nesta dissertação. Portanto sempre que citada a autenticação contínua do usuário relacionada a este trabalho, entenda-se que é a autenticação contínua apenas quando o usuário utiliza seu teclado como dispositivo de entrada de dados ao computador.
- A utilização da expressão "dinâmica da digitação" nesta dissertação se deve ao fato de que este é o termo adotado no Brasil para a análise sobre o padrão de digitação dos usuários. Entretanto neste trabalho são considerados apenas os aspectos estáticos ou instantâneos da digitação, isto é, são considerados os tempos de digitação de dígrafos[1] não levando em consideração as teclas digitadas anteriormente.

[1] Duas teclas digitadas uma após a outra [6].

1.4 – Organização da Dissertação

Esta dissertação foi dividida e organizada em seis capítulos para melhor desenvolver os conceitos abordados, idéias, aplicações implementadas e conclusões sobre o tema desenvolvido no decorrer deste trabalho. A seguir é feita uma breve descrição dos tópicos abordados em cada capítulo.

No Capitulo 2, "Biometria e a Dinâmica da Digitação", é abordado mais detalhadamente o tema de biometria, com breves descrições de cada método de autenticação, definição da diferença entre identificação e verificação, apresentação das medidas de desempenho dos sistemas biométricos e um enfoque mais detalhado sobre o método de dinâmica da digitação que é o abordado nesta dissertação. Por fim é feita uma descrição resumida de trabalhos relacionados à autenticação de usuários baseada no método da dinâmica da digitação e que fazem parte das referências bibliográficas deste trabalho.

O terceiro Capítulo, "Reconhecimento de padrões e as Redes Neurais Artificiais", traz a teoria de reconhecimento de padrões e as abordagens de classificação mais conhecidas além de apresentar as RNAs e as máquinas de comitê.

A organização da dissertação prossegue no Capítulo 4, "Definindo a aplicação", que aborda quais aplicações foram desenvolvidas para atingir os objetivos do trabalho, traz a especificação de cada uma das aplicações, o objetivo da aplicação, definição da mesma e o porquê da necessidade de determinada implementação. Define quais os parâmetros da digitação do usuário são coletados e analisados para posterior utilização na autenticação, formato de armazenamento dos parâmetros e definição da estrutura da RNA utilizada.

O Capítulo 5, "Experimentos e resultados", apresenta quais experimentos foram realizados, quais modificações da estrutura da RNA foram testadas e os resultados obtidos.

Finalmente o Capítulo 6, "Conclusões", apresenta quais objetivos do trabalho foram alcançados, discussões sobre resultados, implementações e características do mecanismo de autenticação, assim como as contribuições relevantes do trabalho. Finalizando são apresentadas propostas para trabalhos futuros sobre o tema abordado.

Capítulo 2 – Biometria e a Dinâmica da Digitação

Introdução

A palavra Biometria vem do grego Bios = Vida e Metron = medida, portanto biometria significa a medida da vida. Segundo o dicionário Aurélio [15], temos que biometria é o ramo da ciência que estuda a mensuração dos seres vivos. Nos sistemas computacionais, a palavra biometria está ligada à verificação da identidade de um indivíduo por meio de uma característica única deste, ou seja, que represente o que o indivíduo é. Esta característica pode variar da impressão digital até a maneira de digitar textos através de um teclado de computador. Os sistemas de autenticação por biometria têm se difundido muito nos últimos anos por serem os mais seguros, no entanto o alto custo desta tecnologia dificulta sua utilização em aplicações comuns. Este capítulo tem por objetivo apresentar o conceito de Biometria, diferenciando os conceitos de identificação e verificação, medidas de desempenho e os métodos de autenticação por prova biométrica. O método da dinâmica da digitação é abordado de maneira mais abrangente por ser o objeto de estudo desta dissertação. Por fim o capítulo apresenta trabalhos já realizados no ramo de autenticação de usuários através da dinâmica da digitação.

2.1 - Biometria

Segundo [28] apud [31] “tecnologias biométricas são definidas como métodos automáticos de verificação ou reconhecimento da identidade de uma pessoa viva baseada em características fisiológicas ou comportamentais”. Estas características fisiológicas ou comportamentais dos seres vivos são únicas para cada indivíduo e, portanto, possibilitam que os sistemas dotados de mecanismos biométricos de verificação de identidade consigam identificar através destas características quem é o indivíduo que está tentando utilizar-se do sistema [12],[31],[32]. Outra importância fundamental dos sistemas biométricos e que os tornam excelentes candidatos para verificação de identidade, é que ao contrário das senhas,

as características biométricas de um indivíduo não podem ser perdidas, roubadas, duplicadas ou copiadas pela observação, como na digitação de senhas [12],[31].

De acordo com as definições identificadas até o momento, podem-se destacar algumas palavras chaves que serão abordadas nos tópicos seguintes.

2.1.1 – Métodos Automáticos

Segundo a definição utilizada para tecnologias biométricas, estas são identificadas como métodos automáticos porque os dispositivos biométricos de controle de acesso implementam vários componentes que após serem configurados deverão ser capazes de identificar uma pessoa sem a necessidade de intervenção humana [3].

Os componentes a serem configurados podem ser divididos em três:

- um mecanismo para escanear e capturar uma imagem analógica ou digital das características da pessoa viva. Este componente é o responsável por extrair todas as informações pertinentes à característica única da pessoa que se deseja utilizar para posterior verificação de identidade;
- mecanismos de compressão, processamento e extração das características biométricas da imagem. Depois de capturados, os dados devem ser processados e armazenados num formato específico de cada dispositivo.
- mecanismo de verificação/identificação, que faz as comparações de novas capturas de uma imagem das características do indivíduo com o padrão já armazenado pelo sistema.

Portanto, após a coleta de uma determinada amostra de uma dada característica de um indivíduo e posterior processamento e armazenamento das informações pelo dispositivo biométrico, o mesmo deverá ser capaz de automaticamente identificar se novas características apresentadas ao dispositivo pertencem ou não ao indivíduo. Esta decisão deverá ser tomada pelo próprio "sistema biométrico que é essencialmente um sistema de reconhecimento de padrões que realiza a identificação pessoal pelo estabelecimento da autenticidade das características do usuário específico" [32].

2.1.2 – Identificação e Verificação

Os dispositivos biométricos podem ser classificados em dois grupos principais quanto à maneira que os dados de entrada capturados são comparados à base de dados existente no dispositivo. Estes grupos são: Identificação e verificação [3],[9],[21],[32].

- Identificação: uma identificação ocorre quando os dados de entrada do dispositivo biométrico serão utilizados para selecionar uma entre muitas "imagens" de características armazenadas na base de dados do mesmo. Este grupo de dispositivos realiza então uma comparação "um-para-muitos" e serve para responder perguntas do tipo "Você sabe quem eu sou?". Geralmente estes sistemas retornam uma lista de possíveis candidatos que podem ser os proprietários dos dados de entrada. O preço destes sistemas é muito alto. Um exemplo são os sistemas de identificação de indivíduos pela sua impressão digital que geralmente são utilizados por órgãos responsáveis pela segurança.

- Verificação: a verificação da identidade do usuário ocorre quando os dados de entrada são utilizados para realizar uma comparação "um-para-um". Desta forma o indivíduo deverá informar quem ele é e apresentar sua característica. O dispositivo então faz uma verificação para constatar se a característica coletada é realmente compatível com as características armazenadas na base de dados do dispositivo para o usuário que o indivíduo diz ser, e a partir desta verificação o dispositivo dá uma resposta se o indivíduo é autêntico ou não. Este grupo de dispositivos serve para responder perguntas do tipo "Você confirma que eu sou fulano?". Os preços dos dispositivos deste grupo são bem inferiores ao dos de identificação e a resposta deste tipo de dispositivo é muito mais rápida.

2.1.3 – Pessoa Viva

O significado desta palavra chave dos sistemas biométricos parece bastante óbvio, no entanto é muito importante definir que o termo pessoa viva em sistemas biométricos representa que estes devem identificar alguns fatores que indicam que a pessoa que está apresentando suas características ao dispositivo esteja viva. Num dispositivo de reconhecimento da impressão digital, por exemplo, um dos fatores que podem identificar que o indivíduo esteja vivo é o uso de sensores que medem a temperatura do dedo. Isto evitaria que um dedo artificial construído com uma "cópia" da impressão digital de determinada pessoa passasse pelo dispositivo biométrico. Não são todos os sistemas biométricos que implementam esta característica, no entanto estas características que provam que o indivíduo esteja vivo aumenta a segurança dos sistemas biométricos. Este termo também diferencia a indústria biométrica do campo da identificação forense [3],[10].

2.1.4 – Características Fisiológicas e Comportamentais

As características fisiológicas de um indivíduo também são conhecidas como características estáticas, pois são relativamente estáveis e praticamente não se alteram ao longo da vida, a menos que algum acidente ou trauma no indivíduo, como por exemplo, uma queimadura, cause a alteração da característica. Como exemplos de sistemas biométricos que utilizam características fisiológicas na autenticação de usuários, têm-se: impressão digital, reconhecimento da íris, reconhecimento da retina, da mão, da face, entre outros. Já as características comportamentais do indivíduo, também conhecidas como não estáticas, podem sofrer algumas alterações, dependendo do estado psicológico da pessoa. Por exemplo, a voz de um indivíduo pode sofrer alterações se o mesmo está num estado de medo, gripado ou correndo perigo. Exemplos de sistemas biométricos que utilizam as características comportamentais são: reconhecimento da voz, reconhecimento da assinatura manuscrita, dinâmica da digitação e outros [3],[6],[10].

Devido a esta certa variabilidade das características comportamentais, a maioria dos sistemas biométricos que são construídos para verificação deste grupo de características,

necessita de uma atualização constante de sua base de dados para capturar ao longo do tempo pequenas variações que podem ir ocorrendo com o passar do tempo. Por exemplo, um adolescente apresenta variações em seu tom de voz na puberdade. Se o sistema biométrico não for atualizado com novas amostras de voz do indivíduo, o dispositivo biométrico pode ter sua eficiência prejudicada. Portanto, sistemas biométricos baseados em características comportamentais apresentam uma maior complexidade no desenvolvimento, devido a estas variações com o passar do tempo, com o estado psicológico do indivíduo e também devido a traumas [3],[6],[10].

Os sistemas de verificação e identificação, construídos para capturar características fisiológicas, têm se mostrado muito mais eficientes e apresentam taxas baixíssimas de erros no processo de verificação pessoal. Entretanto apresentam preços muito altos, pois sempre há a necessidade de dispositivos de captura especiais e muitas vezes estes são intrusivos. Por outro lado os dispositivos comportamentais podem ser muito mais baratos, pois exigem menos dispositivos físicos, como por exemplo, sensores, para captar as informações de entrada. Em alguns casos como na análise da dinâmica da digitação, nenhum dispositivo especial é necessário, apenas o teclado [6],[10],[17].

2.1.5 – Medidas de Desempenho

Para se discutir qual o desempenho de um sistema biométrico existem duas medidas de eficácia. Elas são utilizadas para medir a força de identificação dos sistemas biométricos e são conhecidas como:

- Taxa de Falsa Rejeição (FRR - False Rejection Rate) – indica quantos usuários que eram legítimos foram considerados intrusos, ou ainda, não foram reconhecidos pelo sistema biométrico. Esta taxa também é conhecida como: erro tipo I ou False Alarm Rate; e
- Taxa de falsa aceitação (FAR - False acceptance Rate): a taxa de usuários que não eram autorizados a entrar no sistema e foram considerados como usuários legítimos pelo sistema biométrico. Esta taxa também é conhecida como: erro tipo II ou Impostor Pass Rate.

Quando a FAR é muito alta, indica que o sistema é muito suscetível a intrusões, indicando uma falha no sistema de segurança. Por outro lado, quando FRR é alta, indica a quantidade de frustração dos usuários do sistema. O problema é que a FRR e FAR são grosso modo inversamente proporcionais e, portanto a diminuição de uma determinada taxa acarreta no aumento da outra. Com isto os sistemas biométricos devem possuir limiares para controlar estas taxas de erro, de modo que uma relação de troca entre as duas taxas seja estabelecida, permitindo ao sistema aceitar e rejeitar usuários com uma porcentagem aceitável [32],[37],[38],[45].

A Figura 2.1 apresenta um exemplo da relação entre FRR e FAR:

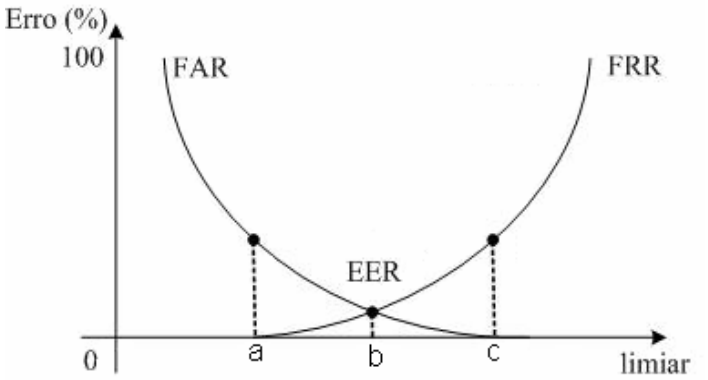


Fig. 2.1- Relação entre FAR e FRR (adaptado de [3])

Da Figura 2.1 pode-se ressaltar a existência de três pontos (**a**, **b** e **c**) importantes na relação entre as duas taxas [3]:

- O ponto **a** indica a mínima FRR
- O ponto **b** indica um limiar onde FRR e FAR são iguais. Na literatura este ponto é conhecido como taxa de erros iguais (EER - Equal Error Rate).
- Finalmente o ponto **c** indica a mínima FAR.

Cada sistema biométrico deve buscar o melhor limiar para o propósito de utilização do sistema em determinada aplicação, por exemplo, se o sistema for utilizado em aplicações que devem minimizar o acesso de indivíduos não autorizados, o sistema deverá funcionar próximo ou no ponto **c**, pois neste ponto a FAR é igual a 0.

2.2 – Funcionamento dos Sistemas Biométricos

Como já visto, os sistemas biométricos podem ser separados em dois grupos quanto à maneira da utilização dos dados de entrada na comparação com a base de dados existente no sistema. Em qualquer um destes grupos, o funcionamento básico dos sistemas biométricos é igual, ou seja, existe uma fase de coleta de dados, inscrição das características, armazenamento e posteriormente a verificação de novas características captadas pelos sistemas biométricos que resultaram num resultado de aceitação ou rejeição [1],[3],[26],[32].

A Figura 2.2. mostra o funcionamento básico dos sistemas biométricos:

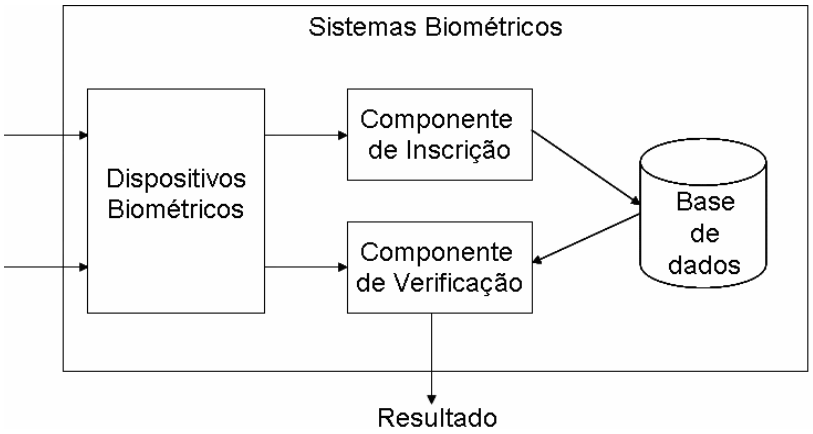


Fig. 2.2 - Funcionamento básico dos sistemas biométricos (adaptado de [26]).

Como pode ser visto na Figura 2.2, existem quatro componentes principais que formam um sistema biométrico. São eles:

- Dispositivos biométricos: compostos principalmente por sensores, estes dispositivos são encarregados de fazer uma leitura da característica a ser examinada pelo dispositivo e passar estes dados ao segundo componente; que pode ser um componente de "inscrição" (*enrollment*) ou um componente de verificação;
- Componente de "inscrição": este componente é responsável por processar os dados de entrada e criar uma amostra biométrica da característica coletada

através do processamento dos dados de entrada e extração de características desejadas. Depois de processada a informação, esta formará um modelo ("*template*") que será armazenado no componente "base de dados";

- Componente de verificação: no processo de verificação, os dados de entrada do sistema, ao invés de serem enviados para o componente de "inscrição", são enviados para o componente de verificação que é responsável por processar os dados de entrada e extrair suas características desejadas, a fim de criar um modelo. Este modelo será comparado com os já existentes na base de dados. A comparação seguirá a regra "um-para-um" ou "um-para-muitos" de acordo com a classificação do sistema biométrico.
- O quarto componente que pode ser identificado é a base de dados que armazenará todos os modelos disponíveis no sistema biométrico em questão. A forma de armazenamento pode ser um banco de dados que é o mais comum, mas o modelo também pode ser armazenado em um *token* ou *smart-card*.

O funcionamento do sistema biométrico é o seguinte: primeiramente cada usuário deverá ser registrado no sistema, para isto o usuário deverá apresentar suas características, sejam fisiológicas ou comportamentais, para os dispositivos biométricos. No momento do cadastro do usuário os dados captados pelos dispositivos biométricos são processados e apenas as características desejadas são extraídas pelo componente de inscrição que monta um modelo do usuário. Depois de montado, este modelo é armazenado na base de dados do sistema. Quando o usuário deseja ser verificado, este apresenta novamente suas características aos dispositivos biométricos, no entanto estes dados são propagados para o componente verificador, que monta um modelo destes novos dados coletados pelos dispositivos biométricos. Este novo modelo deve ser comparado com os existentes na base de dados. O sistema biométrico então realizará a procura, de acordo com a política de funcionamento do sistema, para identificar ou verificar o usuário, gerando como resposta uma lista de possíveis usuários ao que o padrão pertence, se for um processo de identificação, ou uma resposta de aceitação ou rejeição caso o sistema seja de verificação.

2.3 – Métodos de Identificação por Prova Biométrica

Existem no mercado diversos tipos de sistemas biométricos, como por exemplo, sistemas de: identificação de íris, impressão digital, reconhecimento de voz, reconhecimento da dinâmica da digitação, reconhecimento da face, identificação da retina, geometria da mão, reconhecimento da assinatura, entre outros.

A Figura 2.3 mostra os principais métodos de identificação divididos conforme a classe das características coletadas:

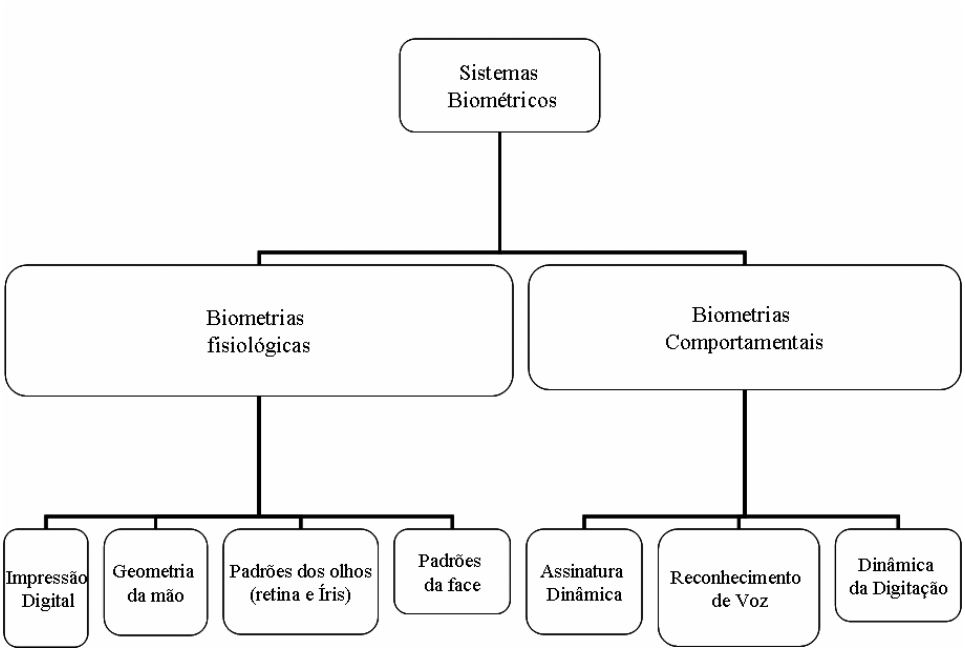


Fig. 2.3 - Principais métodos de identificação biométricas (adaptado de [3]).

A seguir uma breve descrição de alguns métodos é apresentada, sendo que um detalhamento mais aprofundado é realizado no método de dinâmica da digitação, que é o objeto de estudo deste trabalho [4],[10],[26],[32].

2.3.1 – Impressão Digital

A impressão digital certamente é atualmente um dos mais antigos e mais difundidos métodos de biometria. A identificação de uma pessoa pela sua impressão digital é realizada

através de testes complexos de características da mesma, como por exemplo, linhas, arcos, laços, entre outras. A pessoa precisa apresentar o dedo a ter a característica examinada a um dispositivo que fará uma varredura de sua imagem e captará as informações necessárias para montar o modelo da impressão.

2.3.2 – Padrões do Olho

Outros métodos de biometria são os que utilizam os padrões da retina e íris que são únicos para cada pessoa. Estas técnicas são mais recentes e são poucas as empresas que produzem dispositivos para os padrões dos olhos. Os padrões da retina são pouco utilizados porque existe a necessidade de se focalizar o olho contra um feixe de luz, já no reconhecimento da íris isto não é necessário, pois a mesma está na superfície do olho.

2.3.3 – Escaneamento da Mão

Semelhante à impressão digital, existe também o método de escaneamento da mão, onde um indivíduo coloca a mão em um leitor óptico que fará a varredura de sua mão e irá extrair características da geometria da mesma.

2.3.4 – Outros Dispositivos Fisiológicos

Além dos dispositivos citados acima, existem ainda dispositivos biométricos baseados em características fisiológicas para reconhecimento facial, de temperatura da face, entre outros [4],[10],[26],[32].

2.3.5 – Dispositivos para Características Comportamentais

Os dispositivos vistos até aqui são todos baseados em extração de características fisiológicas dos seres vivos. Neste tópico é feita uma breve descrição de alguns dispositivos biométricos baseados na extração de características comportamentais das pessoas.

Um dos métodos biométricos comportamentais é através da identificação baseada na assinatura da pessoa. Cada pessoa tem um estilo único de escrever, mas duas assinaturas de uma mesma pessoa nunca serão exatamente iguais, isto torna este sistema não eficaz para todas as aplicações, mas em muitos casos é um bom método de identificação biométrica, pois sua aceitação pelos usuários é muito grande. Outro exemplo de biometria por características comportamentais é a identificação de pessoas pela voz. A voz de uma pessoa também é considerada única entre cada pessoa, no entanto como qualquer outra característica comportamental, pode conter algumas pequenas alterações que dificultam a identificação.

Os métodos biométricos comportamentais têm algumas vantagens e desvantagens com relação aos métodos fisiológicos, sendo que a principal desvantagem é a imprecisão deste grupo de dispositivos por estes serem desenvolvidos para captar características que podem sofrer pequenas modificações, sejam estas relativas ao estado psicológico da pessoa, ou de acordo com a idade da mesma, como ocorre com a variação do tom de voz na puberdade. Como a principal vantagem deste grupo de dispositivos, pode-se destacar a grande aceitação dos usuários e baixo custo comparado com dispositivos fisiológicos.

No tópico a seguir é detalhado o método de identificação através da dinâmica da digitação. É um método comportamental que tem provocado muitas pesquisas na área por ser extremamente barato e pela sua fácil implantação nos sistemas, pois a única necessidade é a presença de um teclado.

2.3.6 – Dinâmica da Digitação

De acordo com [23] “os mesmos fatores neurofisiológicos que tornam a assinatura manuscrita única também são exibidos pelo padrão de digitação dos usuários. Quando uma

pessoa digita em um teclado, esta deixa uma assinatura digital na forma de latências[2] entre as teclas digitadas".

O método de identificação através da dinâmica da digitação está baseado na hipótese de que cada indivíduo, quando está digitando textos em um teclado, segue formas de digitação diferentes, ou seja, quando um indivíduo está digitando textos, o ritmo da digitação varia de pessoa para pessoa sendo que este é único. Conseqüentemente, se o ritmo de cada indivíduo é único, é possível identificá-lo através desta característica [14].

O termo "dinâmica da digitação" também é conhecido na literatura como ritmo de digitação ou padrão de digitação e como [31] observa, o que importa não é o que o indivíduo digita, mas sim como ele digita.

Portanto quando um indivíduo está digitando textos, toda informação digitada por ele é monitorada no intuito de extrair o seu ritmo de digitação e através deste ritmo identificá-lo posteriormente. No estudo da dinâmica da digitação de uma pessoa existem várias características que podem ser medidas enquanto o usuário digita textos no teclado [1],[21],[39].

Exemplos:

- Latência entre digitações consecutivas – a latência pode ser medida de várias maneiras, como, por exemplo, através da latência entre duas teclas pressionadas, latência entre duas teclas soltas, latência entre o pressionar de uma tecla e soltar de outra, entre outras;
- Duração do tempo em que a tecla é mantida pressionada;
- Velocidade total de digitação;
- Freqüência de erros e correções de erros de digitação;
- O hábito de utilizar teclas em determinadas posições do teclado, como, por exemplo, utilizar os números do "*keypad*" ou os números do próprio teclado.
- Correlação entre as teclas pressionadas, principalmente quando digita-se letras maiúsculas e acentuação;
- A pressão exercida sobre as teclas, entre outras.

[2] Indica o tempo decorrido entre dois eventos. Estes eventos podem ser tanto o pressionamento ou a soltura de teclas.

Como [3] e [32] mostram, a tecnologia de autenticação através da dinâmica da digitação pode ainda ser dividida, quanto ao momento da autenticação, em duas abordagens, sendo elas:

- Abordagem estática – onde a autenticação do usuário é realizada geralmente no acesso do usuário ao sistema
- Abordagem dinâmica – onde o usuário é autenticado continuamente pelo sistema, podendo desta forma constatar se houve troca de usuários do decorrer da execução do sistema.

A abordagem dinâmica é muito mais segura que a estática, no entanto um dos problemas desta abordagem é a exigência de um maior processamento por parte do dispositivo biométrico e a maior complexidade de programação do sistema. Nesta abordagem existem vários métodos de coleta dos dados para treinamento do dispositivo para formar o modelo do usuário, podendo ser destacadas a coleta através de:

- Texto estático – onde um texto padrão é apresentado para o usuário e ele deverá digitar o texto numa aplicação que analisa seu ritmo de digitação.
- Texto livre – nesta metodologia de coleta de dados o usuário pode digitar qualquer informação de maneira livre para que a aplicação analise seu padrão.

Por se tratar de um sistema biométrico comportamental, a eficiência da dinâmica da digitação está sujeita ao estado físico e comportamental do indivíduo que está sendo verificado, sendo esta a desvantagem de utilização do método. No entanto os sistemas biométricos que utilizam características fisiológicas requerem ferramentas específicas, como câmeras e leitores ópticos, aumentando desta forma o custo de utilização e implantação, já a dinâmica da digitação, é praticamente gratuita. Esta com certeza é a maior vantagem dos sistemas que utilizam a dinâmica da digitação, além destes serem não intrusivos e terem uma aceitabilidade muito grande por parte de seus usuários [6],[31],[32].

Nesta dissertação será utilizada como abordagem de autenticação a dinâmica, pois o objetivo da mesma é criar um sistema de autenticação contínuo que detecte em qualquer

momento a utilização do sistema por um usuário não autorizado. Como método de coleta de dados as duas metodologias serão empregadas. A intenção de utilizar as duas metodologias de coleta é verificar se existe alguma melhoria no processo de identificação com a utilização de texto livre. Já a característica analisada na digitação de cada pessoa será a latência entre sucessivos pressionamentos e soltura de teclas. Detalhes e discussões sobre a metodologia empregada serão discutidos no Capítulo 4.

2.4 – Trabalhos Relacionados

Neste tópico serão apresentados alguns dos trabalhos já realizados que abordam o tema da dinâmica da digitação, apresentando sucintamente as pesquisas mais referenciadas e tentando levantar alguns aspectos importantes destes trabalhos, como, por exemplo, a informação utilizada para montar os modelos dos usuários, a quantidade de amostras utilizadas na obtenção do modelo e na fase de testes do experimento, os classificadores utilizados, características amostradas, medidas de desempenho, entre outros. É importante lembrar antes desta descrição, que muitos trabalhos apresentam várias medidas de desempenho durante o experimento, assim como tipos de classificadores e características analisadas, além de que outros não apresentam todas estas informações, portanto o conteúdo deste tópico é apenas parcial e para obter informações mais completas é necessário consultar as referências.

No século 19, observações dos operadores de telégrafo mostraram que cada operador tinha seu próprio padrão de digitar as mensagens e os operadores conseguiam reconhecer outros operadores apenas pela forma que eles digitavam as mensagens [21]. Recentemente, muitos outros estudos foram realizados sobre o tema da dinâmica da digitação. Em 1980 Gaines et. al. [16] apud [23],[30] publicou um trabalho utilizando a dinâmica da digitação para autenticação num grupo de sete secretárias utilizando métodos estatísticos (t-tests) para classificação e verificação do acesso. Gaines utilizou três textos, sendo o primeiro um texto em inglês, o segundo um conjunto de palavras randômicas e o terceiro um conjunto de frases randômicas. Todos os textos tinham tamanhos variando de 300 a 400 palavras e cada um dos textos foi coletado duas vezes sendo que a segunda coleta foi realizada 4 meses depois da primeira. A latência entre dígrafos foi utilizada como

característica medida, mas apenas para os dígrafos que ocorreram mais que 10 vezes. O método de Gaines gerou uma FAR de 0% e FRR de 4%.

Experimentos similares a este, conforme [3] e [23], foram realizados por Umphress e Williams que utilizaram 17 programadores num processo de identificação contínuo. Os autores verificaram a latência entre digitações consecutivas em um texto de 1400 caracteres no processo de cadastramento e 300 caracteres na verificação, obtendo uma FAR de 6%. Em outro trabalho Leggett e Williams melhoraram o experimento anterior, realizando experimentos com 36 participantes com textos de 537 caracteres, sendo que houve uma primeira coleta e após um mês uma nova coleta. A primeira coleta serviu para montar um modelo e a segunda para testar o modelo proposto. Eles obtiveram uma FAR de 5 % e FRR de 5,5 %.

Em 1990 Joyce e Gupta [23] desenvolveram um trabalho tratando da abordagem estática de autenticação através dos dados de "*login*", senha, primeiro e último nome de 33 usuários. Foram coletados 8 vezes estas informações para treinamento e 5 para testar o modelo. A característica estudada foi o tempo entre teclas e o classificador utilizado foi o estatístico. Este modelo resultou em uma FAR de 0,25% e FRR de 16,67%.

O modelo adotado por [9] utiliza como informações de entrada a senha e frases das quais mede a latência entre teclas e utiliza o classificador de Bayes e o de distância mínima. Dois experimentos foram realizados, um com 9 voluntários num período de 9 semanas e o segundo com 10 voluntários, num período de 5 semanas e 26 voluntários no período de 8 semanas. Para testar o sistema, o autor utiliza 10 usuários válidos e 22 impostores. O trabalho resultou em uma FAR de 0,5% e FRR de 3,1%.

Outro trabalho muito citado é [11] que utiliza como informação alvo o nome do usuário medindo o tempo entre as teclas digitadas e também a duração de tempo que uma mesma tecla permanece pressionada. Este trabalho utiliza-se de técnicas de redes neurais artificiais (RNA) e distância euclideana como métodos de classificação e os dados de entrada que contêm erros são rejeitados. São utilizados dois grupos de usuários no trabalho, o primeiro com 25 usuários e o segundo com 21, sendo que o conjunto de treinamento do primeiro grupo é formado em média por 29,3 exemplos válidos do usuário e 45,3 exemplos inválidos sendo o melhor resultado uma FAR de 12% e FRR de 0%. No segundo grupo, os

exemplos válidos são em média 47,7 e os inválidos 22,8. O melhor resultado é uma FAR de 21,2% e FRR de 0%.

Obaidat e Macchiarolo [34] realizaram seus trabalhos analisando 6 usuários, sendo que estes digitaram frases com 30 caracteres, mas apenas os 15 primeiros foram analisados. Neste trabalho foram coletadas 40 amostras por usuário e as amostras contendo erros de digitação foram rejeitadas. As 40 amostras coletadas foram separadas de diversas maneiras para formar o conjunto de treinamento e o conjunto de testes, os autores usaram três abordagens de RNA como classificador: rede direta com algoritmo de retro-propagação, rede soma dos produtos e rede soma dos produtos híbrida. A característica analisada foi a latência entre teclas e o método classificou corretamente o usuário em 97,8% dos casos. Os mesmos autores no trabalho [35] apresentam mais detalhadamente os resultados, demonstrando que a rede direta com algoritmo de retro-propagação obteve as melhores porcetagens de acerto, sendo que este paradigma classificou corretamente os usuários em 97,5% dos casos, seguida da rede de soma dos produtos hibrida com 96,2% e rede soma dos produtos com 93,7%, entretando os autores não diferenciam os erros entre FAR e FRR. Em [36] Obaidat e Saudon utilizam a rede direta com algoritmo de retro-propagação, "*counterpropagation*" e ART-2 para o mesmo problema e novamente a rede direta com algoritmo de retro-propagação apresenta o melhor resultado com 97,5% de acerto, a rede "*counterpropagation*" apresentou taxa de 95,83% de acerto e por último a ART-2 com 89,17%. Grandes melhorias nos resultados dos trabalhos realizados pelos autores citados acima foram alcançadas em [33] e [37]. Nestes trabalhos a latência entre teclas e a duração de tempo que uma tecla fica pressionada foram analisadas sobre o "*login*" dos usuários que foi a informação coletada. Os autores alteraram o sistema de manipulação de interrupções do computador por um específico e com precisão do relógio de 0,1 milisegundos. Foram analisados 15 usuários, sendo que cada um deles digitou o seu "login" 15 vezes e também digitou 15 vezes o "*login*" de cada um dos outros usuários. Muitos classificadores tanto estatísticos como neurais foram utilizados nestes experimentos, e os autores chegaram a obter o incrível resultado de 100% de classificação dos usuários com alguns métodos de classificação baseados em redes neurais. Outro fator importante citado pelos trabalhos é que o tempo de duração de pressionamento de uma tecla resulta em melhores resultados

que a medida da latência entre teclas diferentes, mas os melhores resultados são obtidos quando os autores utilizam as duas medidas em conjunto.

Muitos outros trabalhos foram desenvolvidos utilizando a dinâmica da digitação como método de autenticação de usuários. A maioria deles utiliza a abordagem estática de autenticação. Estes trabalhos podem ser vistos em [1-3],[9],[11],[12],[17],[23-25],[29],[31],[33-39],[45]. Outros trabalhos também foram desenvolvidos seguindo a abordagem dinâmica [6],[30],[42]. Por fim, alguns estudos analisam as duas formas de autenticação [14],[21],[32],[44]. Algumas pesquisas interessantes são: [44] que utiliza informações do mouse como característica biométrica; [1] e [6] que utilizam correlação entre teclas como característica medida; [29] que propõe um sistema de senhas seguras com a utilização de dinâmica da digitação e ainda expõe a possibilidade de construir um modelo para cifrar arquivos baseado nas informações da dinâmica da digitação do indivíduo; [27] que mostra a existência de uma variabilidade significante na maneira que cada digitador produz cada dígrafo; e [7] que implementa uma aplicação comercial de autenticação através da dinâmica da digitação.

Quanto às técnicas de classificação empregadas podemos encontrar principalmente os métodos estatísticos, as redes neurais, a lógica difusa, entre outras.

Muitos dos trabalhos utilizam a latência entre teclas como característica medida, entretanto, como já citado, novas técnicas passaram a ser abordadas nos trabalhos, como por exemplo, duração de pressionamento de uma tecla, correlação entre teclas, característica da digitação (código das teclas digitadas – pode se utilizado para verificar se o usuário utiliza os número do "*keypad*" ou do próprio teclado por exemplo) e controle de erros. Quanto ao controle de erros a maioria dos artigos citados simplesmente ignora os exemplos que contêm erros de digitação.

Para facilitar a visualização de alguns trabalhos, a Tabela 2.1 adaptada de [3], apresenta as pesquisas que abordam a autenticação estática. Esta tabela também informa o classificador, FAR e FRR obtidos, entre outros.

É importante salientar que muitos trabalhos exibem mais do que um experimento, podendo conter muitos resultados, metodologias de classificação ou ainda não apresentar todos os dados desejados, por isso a Tabela 2.1 pode conter alguns campos incompletos ou ainda apresentar resultados absolutos, sem especificar a FAR e FRR isoladamente.

Ref.	Número de amostras	Característica medida	Classificador	FAR	FRR	Número de pessoas pesquisadas
[44]	15 a 30, sendo 10 para treinar	Latência e duração da digitação	Estatístico	7%	7%	11
[2]	25	Latência da digitação	RNA	4,2%	1,4%	5
[25]	3 para treinar	Latência e duração da digitação	RNA	6,56% e 0%	2,22% e 1,11%	90 válidos e 61 inválidos
[33]	15 para cada usuário durante 8 semanas	Latência e duração da digitação	Vários métodos estatísticos e neurais	0%	0%	15
[24]	-	Latência da digitação	RNA	3%	22%	-
[12]	15	Latência e duração da digitação	RNA	de 0% a 15%	0% 22%	10
[9]	30	Latência da digitação	Estatístico	0,5%	3,1%	de 9 a 26
[34]	40	Latência da digitação	RNA	97,8% de sucesso		6
[35]	40	Latência da digitação	RNA	97,5 % de sucesso		6
[37]	15 para cada usuário durante 8 semanas	Latência e duração da digitação	Vários métodos Estatísticos e neurais	0%	0%	15
[11]	Varia de acordo com o experimento	Latência e duração da digitação	Estatístico e RNA	0%	12%	Varia
[38]	30 para treinar e 20 para testar	Latência da digitação	RNA	9,9%	30%	14
[1]	1000 teclas para treinar e 100 para testar	Correlação entre teclas	Estatístico e RNA	0%	0%	30
[39]	15 para treinar e 5 para testar	Latência da digitação	Estatístico	4,2%	14%	11
[29]	188	Latência e duração da digitação	Estatístico	77,1 % de sucesso		13
[23]	8 para treinar e 5 para testar	Latência da digitação	Estatístico	0,25%	16,36%	33
[45]	150 a 400 para treinar e 5 para testar	-	Estatístico	0%	3,69%	21 válidos 15 inválidos
[36]	40	Latência da digitação	RNA	97,5 % de sucesso		6
[31]	-	Latência da digitação	Estatístico	92,14 % de sucesso		63
[32]	15	duração da digitação e código da tecla	Estatístico	0%	23,4%	20
[3]	10	Latência e duração da digitação, códigos da tecla	Estatístico e lógica nebulosa	1,91%	1,55%	50

Tabela 2.1 - Resumo das principais pesquisas de autenticação estática (adaptado de [3])

Da mesma maneira, a Tabela 2.2, também adaptada de [3], apresenta as pesquisas que utilizam a autenticação dinâmica como método de autenticar os usuários. A Tabela 2.2 apresenta as mesmas características da Tabela 2.1.

Ref.	Número de amostras	Característica medida	Classificador	FAR	FRR	Número de pessoas pesquisadas
[44]	2 a 3 texto de 10 linhas, sendo 1 para treinar	Latência e duração da digitação	Estatístico	0% e 15%	0% e 15%	6
[42]	-	Latência e duração da digitação	Estatístico	-	-	-
[30]	-	Latência e duração da digitação	Estatístico	90,7 % de sucesso	31	
[6]	5 para usuários válidos, sendo 4 para treinar e 1 para inválidos	Correlação entre trígrafos	Estatístico	0,01%	4%	44 válidos 110 inválidos
[32]	1 página	duração da digitação	Estatístico	-	-	20

Tabela 2.2 - Resumo das principais pesquisas de autenticação dinâmica (adaptado de [3])

2.5 – Conclusão

Neste capítulo podemos verificar que os sistemas biométricos baseados na dinâmica da digitação de usuários vêm sendo largamente pesquisados e os trabalhos indicam cada vez mais alternativas e formas de utilização desta técnica para autenticação de pessoas. Os resultados são cada vez mais satisfatórios e novas técnicas são testadas visando sempre um aumento na confiabilidade do sistema.

Conclui-se deste capítulo que alguns aspectos importantes na definição de um sistema biométrico precisam ser especificados. Alguns destes aspectos são:

- Informação Alvo – são os dados que serão coletados
- Quantidade de amostras – indica quantas amostras para treinar e testar o sistemas devem ser coletadas
- Características medidas – informa quais são as características que o sistema biométrico mede para formar um modelo e posterior verificação

- Precisão do tempo – qual deve ser a precisão do tempo desejada, este aspecto não é importante a todos os sistemas biométricos, no entanto, na área de dinâmica da digitação é essencial
- Classificador de padrões – define qual deve ser o classificador que o sistema biométrico utiliza para tomar suas decisões

Estes aspectos são discutidos no capítulo 4 onde a metodologia utilizada neste trabalho é apresentada.

Capítulo 3 - Reconhecimento de Padrões e Redes Neurais Artificiais

Introdução

Por se tratar de assuntos muito conhecidos, abordados e utilizados em diversas pesquisas, o reconhecimento de padrões e as redes neurais artificiais são abordados de maneira bastante resumida neste capítulo. No decorrer do texto são apresentadas as referências que foram utilizadas e que devem ser consultadas para um aprofundamento teórico, caso seja desejado.

3.1 – Reconhecimento de Padrões

Nos dias atuais muitos sistemas automáticos de reconhecimento de padrão estão sendo desenvolvidos para serem utilizados nas mais diversas áreas, isto porque os computadores possibilitam o processamento de grandes quantidades de dados facilitando o uso e elaboração de métodos de classificação e análise [22].

Muitas são as definições para reconhecimento de padrões. De acordo com [22] "reconhecimento de padrões é o estudo de como máquinas podem observar o ambiente, aprender a distinguir padrões de interesse deste meio e produzir decisões seguras e razoáveis sobre as categorias de padrões". Em [5] tem-se que "reconhecimento de padrões é o processo de identificar objetos, através da extração de suas características a partir de dados sobre o objeto".

Por fim, [13] apresenta que "o reconhecimento de padrões pode ser pensado como uma classificação automática pelo computador de um estímulo externo em uma de inúmeras classes". A Figura 3.1 representa um processo básico de reconhecimento de padrão.

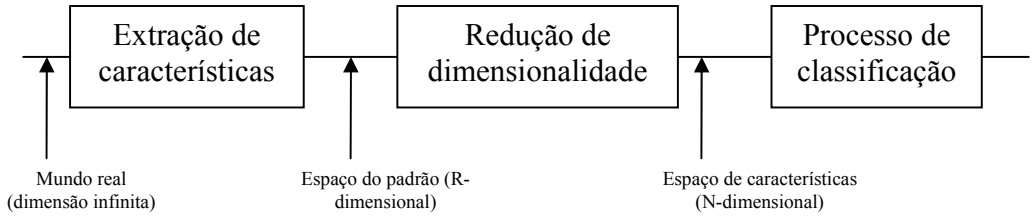


Fig. 3.1 - Processo de reconhecimento de padrão (adaptado de [13])

Em geral, estes sistemas envolvem alguns aspectos importantes que podem ser listados como [3],[13],[22],[31]:

- Extração de características: através de dispositivos de captura, como por exemplo: sensores, câmeras, leitores ópticos, entre outros. O sistema mapeia um objeto do mundo real (dimensão infinita) para o mundo do padrão analisado (R-dimensional). Este mapeamento ocorre através da captura de um conjunto adequado de características que podem ser adquiridas pelos dispositivos de captura.
- Redução da dimensionalidade: o espaço de características do padrão capturado (R-dimensional) pode ser excessivo, por isso há a necessidade de reduzir as características analisadas, pois características extras aumentam a complexidade computacional do problema e não trazem benefícios reais. Depois desta redução, temos o espaço de características desejado (N-dimensional). Um exemplo de redução de dimensionalidade: quando se analisa a impressão digital de um indivíduo nem todas as informações coletadas são necessárias, mas apenas informação como linhas, arcos, laços.
- Representação dos dados: as características coletadas do mundo real devem ser representadas de forma compreensível para o mundo computacional. Esta representação pode ser através de valores numéricos, vetores de características, etc. Por exemplo, quando se deseja reconhecer uma letra do alfabeto, pode-se utilizar como forma de representação dos dados os valores da área da letra, perímetro, ângulo entre linhas, etc.

- Classificação: após coletar e representar os dados de um determinado padrão a ser reconhecido é necessário decidir a qual classe de padrão estes dados pertencem. O aspecto da classificação é analisado a seguir.

O reconhecimento ou classificação de um determinado padrão pode ser realizado de duas maneiras diferentes [3],[22]:

- Classificação supervisionada: onde o padrão de entrada é identificado como membro de uma das classes pré-definidas pelo projetista do sistema; e
- Classificação não supervisionada: onde o reconhecimento do padrão é baseado em um aprendizado feito sobre a similaridade dos padrões.

Ainda referente ao aspecto de classificação de padrões, podemos citar algumas das principais abordagens de classificação utilizadas pelos sistemas de reconhecimento de padrão. São elas [3],[22]:

- "Casamento" de modelos: uma das primeiras e mais simples abordagens de reconhecimento de padrão. O "casamento" é uma operação genérica para avaliar a similaridade entre duas entidades do mesmo tipo, como por exemplo: pontos, curvas ou formas. A medida de similaridade pode ser uma correlação ou uma função de distâncias, e esta medida pode ser otimizada pela disponibilidade de um conjunto de treinamento. Esta abordagem exige bastante processamento.
- Estatístico: nesta abordagem os padrões são representados por vetores de características. Dado um conjunto de treinamento dos padrões de cada classe, o objetivo desta abordagem é estabelecer fronteiras de decisões no espaço de características de forma a separar os diferentes padrões em diferentes classes, utilizando para isto distribuições probabilísticas dos padrões pertencentes a cada classe.
- Sintático: os padrões são vistos numa perspectiva hierárquica, onde um padrão é decomposto em sub-padrões simples que por sua vez vão ser

novamente decompostos até o sub-padrão mais simples que é denominado de primitiva. Os padrões são representados em termos de inter-relações entre estas primitivas.

- Redes Neurais: as redes neurais podem ser vistas como um grande número de processadores simples interconectados, formando um sistema computacional paralelo. Esta abordagem tenta usar alguns princípios organizacionais como aprendizado, generalização, adaptação, tolerância a falhas e representação distribuída numa rede de pesos onde os nodos são neurônios artificiais. As principais características desta abordagem são: habilidade em aprender relações não lineares complexas de entrada e saída, uso de procedimentos de treinamento seqüencial e adaptação. As redes neurais mais utilizadas nos sistemas de reconhecimento de padrão são as redes diretas e o aumento da utilização desta abordagem nos sistemas de padrão se deve à sua baixa dependência no conhecimento do domínio específico e à existência de algoritmos de aprendizado eficientes.
- Nebulosa: abordagem utilizada quando há ambigüidade nos dados do padrão. A lógica nebulosa é uma generalização da lógica tradicional e trata os padrões através de graus de pertinência sobre diversos valores (multivalorada) diferentemente da definição tradicional em que qualquer premissa sempre é verdadeira ou falsa (bi-valorada).

3.2 – Redes Neurais

O cérebro humano é composto por bilhões de neurônios, que são células componentes do sistema nervoso e que atuam sobre todas as funções e movimentos do nosso organismo. O neurônio tem um corpo celular chamado soma e diversas ramificações. As ramificações conhecidas como dendritos conduzem sinais das extremidades para o corpo celular, e a ramificação, geralmente única, conhecida como axônio, transmite as informações do corpo celular para as suas extremidades. As extremidades do axônio de um neurônio se conectam aos dendritos de outros neurônios através de sinapses e em muitos

casos um axônio pode estar conectado com outros axônios ou com o corpo celular de outro neurônio. O conjunto de todos os neurônios conectados forma uma grande rede denominada Rede Neural que possibilita uma enorme capacidade de processamento e armazenamento de informação [5],[40].

A comunicação entre os neurônios desta rede neural é realizada por impulsos. O neurônio transmissor pode controlar esta freqüência de impulsos aumentando ou diminuindo a polaridade na membrana pós sináptica. Com isto o neurônio pode excitar ou inibir um outro neurônio. Esta capacidade de modificar os valores das conexões entre os neurônios permite à rede neural uma mudança de comportamento e esta mudança representa um aprendizado da Rede. O estudo das redes neurais também é conhecido como conexionismo, pois o comportamento da rede neural está diretamente ligado aos valores de suas conexões sinápticas [5],[40].

Os principais constituintes da célula neural podem ser vistos na Figura 3.2:

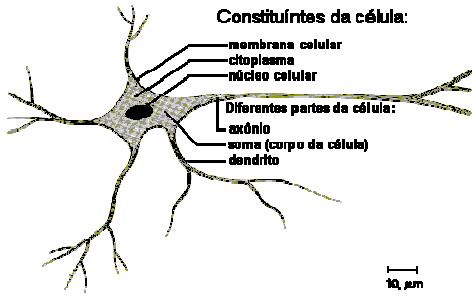


Fig. 3.2 - O neurônio (extraído de [40]).

3.2.1 – Modelos de Neurônios

As redes neurais artificiais (RNA) são inspiradas nos neurônios que compõem o sistema nervoso, entretanto, hoje em dia sua estrutura é muito diferente das redes neurais naturais. O primeiro modelo de neurônio que será visto a seguir, é um modelo simples, mas que tem a intenção de imitar a realidade biológica. Atualmente os pesquisadores estão mais motivados pela construção de computadores com alto grau de paralelismo e modelar o sistema nervoso com uma precisão suficiente, de modo que um comportamento emergente possa ser observado servindo de apoio às hipóteses usadas na modelagem [5].

3.2.1.1 – Modelo de McCulloch-Pitts

McCulloch interpretou o funcionamento do neurônio como sendo um circuito binário onde as entradas são binárias e combinadas por uma soma ponderada produzem a entrada efetiva do neurônio conforme Figura 3.3 [5]:

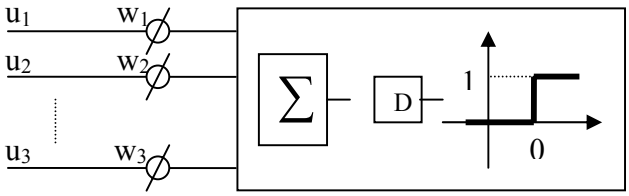


Fig. 3.3 - Modelo de Waren McCulloch e Walter Pitts (adaptado de [5]).

McCulloch e seu aluno, Walter A. Pitts, usando argumentos lógicos, provaram a equivalência de suas redes com a máquina de Turing [5].

3.2.1.2 – Modelo Geral de Neurônio

O modelo geral de neurônio que pode ser visualizado na Figura 3.4 é uma generalização do modelo de McCulloch-Pitts. Neste modelo uma combinação das entradas WiUi com uma função Φ produz o estado de ativação do neurônio e a saída do mesmo é determinada pela função η, sendo que pode ser determinada ainda uma polarização θ que determina que valores abaixo desta polarização devem acarretar numa saída nula [5].

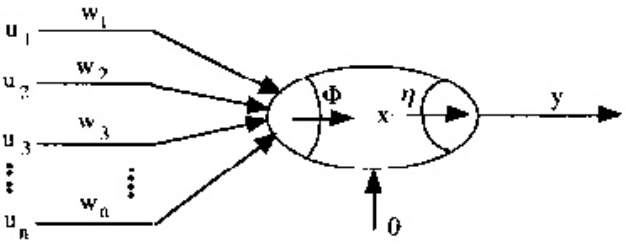


Fig. 3.4 - Neurônio artificial (extraído de [40]).

3.2.2 – A Rede Neural Artificial

As redes neurais artificiais (RNA) são compostas por vários neurônios artificiais que são conectados uns aos outros por conexões sinápticas. Nas RNAs multi-camadas, os neurônios podem ser classificados em: neurônios de entrada, neurônios intermediários ou "*hidden*" e neurônios de saída. Os neurônios de entrada recebem excitações do mundo exterior, eles correspondem aos neurônios dos órgãos dos sentidos. Os neurônios de saída produzem respostas que são usadas para alterar o mundo exterior sendo correspondentes aos neurônios biológicos que excitam os músculos [5],[40].

De acordo com [5] os neurônios internos são importantes para a rede por vários aspectos, como:

- Importância Biológica: podem apresentar uma independência aos estímulos externos e sua excitação pode provocar uma evolução durante um tempo relativamente longo.
- Importância Matemática: sem a presença deles é impossível resolver problemas não linearmente separáveis.

A Figura 3.5 representa uma RNA contendo 3 neurônios de entrada, 2 intermediários e 2 de saída, sendo que todos os neurônios de entrada são ligados a todos os neurônios intermediários através de conexões sinápticas (pesos) e os neurônios intermediários se ligam a todos os neurônios de saída.

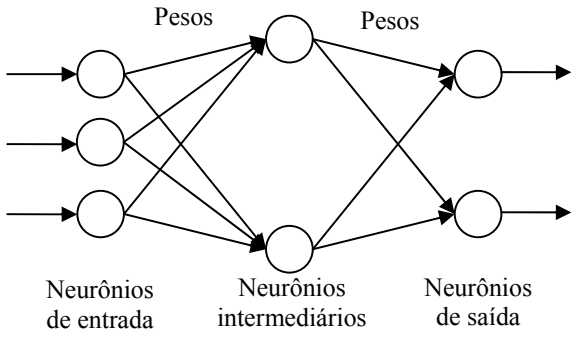


Fig. 3.5 - Exemplo de RNA (adaptado de[5]).

Para que uma RNA possa ser caracterizada, diversos fatores devem ser especificados e não apenas a sua topologia como visto na Figura 3.5. Estes fatores são:

- os neurônios,
- a resposta de cada neurônio,
- o estado global de ativação da rede,
- a conectividade da rede,
- como se propaga a atividade da rede,
- como se estabelece a conectividade,
- o ambiente externo da rede,
- como o conhecimento é representado na rede.

Um melhor detalhamento de cada um dos fatores acima citados pode ser encontrado em [5]. Uma descrição mais formal e aprofundada da utilização das RNAs em problemas de reconhecimento de padrão pode ser encontrada em [8],[18].

3.2.3 – Máquinas de Comitê

Quando uma tarefa é complexa, geralmente o melhor a fazer é subdividi-la em pequenas tarefas simples e combinar as soluções destas tarefas para resolver o todo. Segundo HAYKIN [18] este é o princípio de "dividir e conquistar" muito utilizado na engenharia.

HAYKIN [18] afirma que: "na aprendizagem supervisionada, a simplicidade computacional é alcançada distribuindo-se a tarefa de aprendizagem entre um número de especialistas, que, por sua vez, divide o espaço de entrada em um conjunto de subespaços". Esta combinação de especialistas constitui uma máquina de comitê.

Segundo BISHOP [8], "é uma prática comum nas aplicações de redes neurais treinar muitos candidatos a rede e então selecionar o melhor, baseando-se no desempenho de um conjunto de validação independente, por exemplo, e utilizar somente esta rede descartando as demais. Há duas desvantagens nesta aproximação. Primeiro, todo o esforço envolvido no

treinamento das redes restantes é desperdiçado. Segundo, o desempenho da generalização no conjunto de validação possui um componente aleatório devido a ruídos nos dados, e portanto a rede que obteve os melhores resultados sobre o conjunto de validação pode não ser a que apresentará melhor performance sobre um novo conjunto de testes."

Portanto, uma máquina de comitê supostamente produz resultados melhores do que quando utilizado qualquer especialista individualmente, pois ela utiliza o conhecimento de vários especialistas para chegar a uma decisão. As máquinas de comitê podem ser classificadas em duas categorias [18],[20]:

- Estruturas estáticas: onde o mecanismo de combinação entre os especialistas independe dos dados de entrada. Esta categoria pode ainda ser subdividida em: média de ensemble, onde a saída global é o resultado de uma combinação linear das saídas de cada especialista; e reforço, onde um algoritmo fraco de aprendizagem torna-se um algoritmo que alcança precisão alta.
- Estruturas dinâmicas: ao contrário das estruturas estáticas, envolvem os dados de entrada no mecanismo de combinação das saídas de cada especialista para gerar a saída global. Esta categoria também pode ser subdividida em 2 métodos, sendo eles a mistura de especialistas, onde as respostas dos especialistas são combinadas não linearmente por uma única rede de passagem; e a mistura hierárquica de especialistas, onde várias redes de passagem são dispostas hierarquicamente para combinar não linearmente as saídas de cada especialista. As estruturas dinâmicas também podem ser vistas como redes modulares.

Nesta dissertação apenas as estruturas estáticas serão utilizadas, sendo que apenas os métodos desta estrutura serão detalhados. Para verificar o funcionamento das estruturas dinâmicas é aconselhada a consulta a [8],[18].

3.2.5.1 – Média de Ensemble

No método de média de *ensemble* um número de especialistas é treinado diferentemente, compartilhando os mesmos dados de entrada e as saídas produzidas por cada um destes especialistas deverão ser combinadas de alguma forma para produzir uma saída global [18].

A Figura 3.6 exemplifica uma máquina de comitê baseada na média de ensemble:

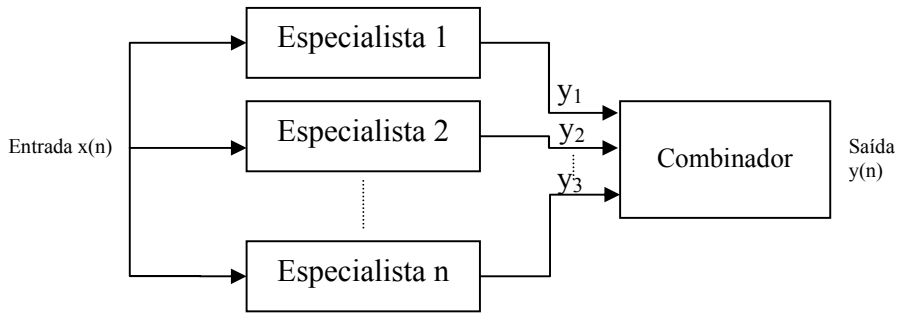


Fig. 3.6 - Máquina de comitê baseada em média de ensemble (adaptado de [18])

Alguns pontos podem ser observados quando utilizamos a média de ensemble [18],[20]:

- Se apenas uma rede neural fosse utilizada o número de parâmetros ajustáveis seria grande, além de que, o tempo para treinar esta rede seria maior que treinar várias redes mais simples em paralelo;
- Quando o número de parâmetros é grande, se comparado com o tamanho do conjunto de treinamento, aumenta a possibilidade de ajuste em excesso;
- Como nas máquinas de comitê existem vários especialistas sendo treinados e o processo de treinamento é antecedido por uma etapa de ajuste aleatório dos pesos, cada rede deverá iniciar seus pesos com valores diferentes. Desta forma cada rede deve convergir para um mínimo local diferente e com isso espera-se que o desempenho global seja melhorado;

3.2.5.2 – Reforço

No método de reforço ou "*boosting*", o objetivo é melhorar o desempenho de qualquer algoritmo de aprendizagem. Neste método os especialistas são treinados com conjuntos de dados com distribuições diferentes. O reforço pode ser implementado de 3 modos diferentes [18],[20]:

- Reforço por filtragem – assume que os dados de treinamento são muito grandes, e estes podem ser descartados ou mantidos durante o treinamento. Este modo de reforço filtra os exemplos de treinamentos por diferentes versões de um algoritmo fraco. É o modo por reforço que exige menos memória;
- Reforço por subamostragem – a amostra de treinamentos é fixa e os exemplos são amostrados mais do que uma vez de acordo com distribuições probabilísticas. O erro é calculado sobre os exemplos;
- Reforço por ponderação – a amostra de treinamentos é fixa e o algoritmo pode receber exemplos ponderados. O erro é calculado sobre os exemplos ponderados.

3.3 – Conclusão

Neste capítulo aspectos importantes dos sistemas de reconhecimento de padrões foram apresentados, sendo que este levantamento facilita a percepção das ferramentas que é necessário implementar para se construir um sistema de reconhecimento de padrões da dinâmica da digitação de indivíduos. Também foram apresentadas as RNA e exibida a teoria das máquinas de comitê que segue o princípio "dividir e conquistar" para resolver problemas complexos, dividindo-os em pequenos problemas mais simples. Como o reconhecimento do padrão de digitação das pessoas é uma tarefa complexa, a utilização das redes de comitê pode ajudar na solução do problema.

Capítulo 4 – Definindo a Aplicação

Introdução

Neste capítulo serão abordados e definidos: a metodologia do sistema biométrico proposto; os aspectos mais importantes na definição do sistema biométrico; as aplicações implementadas para coleta, manipulação e classificação dos dados, relacionando cada aplicação com os aspectos cobertos por elas; a RNA implementada e a infra-estrutura disponível e ferramentas utilizadas.

4.1 – Metodologia do Sistema Biométrico Proposto

A metodologia proposta para autenticação do usuário através da dinâmica de sua digitação pode ser dividida em duas etapas: etapa de coleta dos dados e formação do modelo do usuário; e etapa de coleta de dados e classificação dos mesmos para autenticar ou invalidar o usuário de acordo com um modelo.

Tanto na etapa de geração de modelo de um usuário como na etapa de classificação do usuário, a estrutura da RNA utilizada é muito importante, pois é ela que define como será gerado o modelo do usuário, assim como a própria estrutura da RNA que será utilizada na classificação do usuário. Como estrutura de RNA, este trabalho propõe duas abordagens:

- Estrutura composta por apenas uma RNA que representará cada um dos usuários: nesta abordagem, cada usuário terá uma RNA treinada e os pesos desta RNA constituirão seu modelo, na etapa de autenticação do usuário. Os dados a serem analisados são apresentados à sua RNA treinada que decidirá se o usuário é válido ou não. Para o treinamento, o conjunto de treinamento do usuário é apresentado à RNA como exemplos válidos e o conjunto de treinamento de todos os outros usuários do grupo 1 são apresentados como exemplos inválidos. A Figura 4.1 exemplifica esta estrutura de RNA.

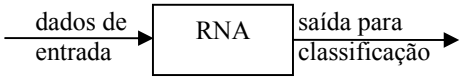


Fig. 4.1 - Estrutura composta por uma RNA para representação do usuário

- Estrutura baseada em máquinas de comitê para representação do usuário: nesta abordagem, cada usuário será representado por um conjunto de 13 RNAs idênticas sendo que o modelo do usuário é uma combinação destas 13 RNAs. Na etapa de autenticação do usuário os dados a serem analisados são apresentados a todas as redes e uma combinação das saídas de todas as RNAs decidirá se o usuário é válido ou é um intruso. A Figura 4.2 exemplifica esta estrutura de RNA.

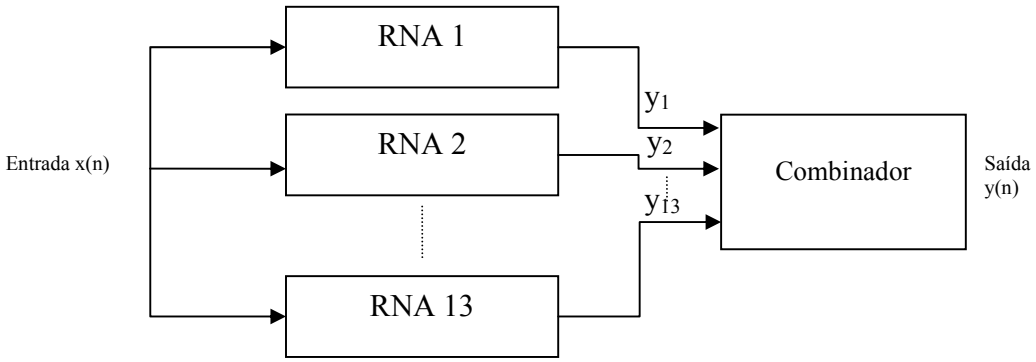


Fig. 4.2 - Estrutura baseada em máquinas de comitê para representação do usuário.

Para o treinamento desta máquina de comitê, o conjunto de treinamento do usuário válido é apresentado para todas as RNA como dados válidos e para cada uma das RNAs o conjunto de dados inválidos será o conjunto de treinamento de cada um dos 13 usuários do grupo 1 restantes. A Figura 4.3 demonstra a estrutura da máquina de comitê no treinamento da máquina do usuário 1. Para simplificação, a sigla CT indica conjunto de treinamento.

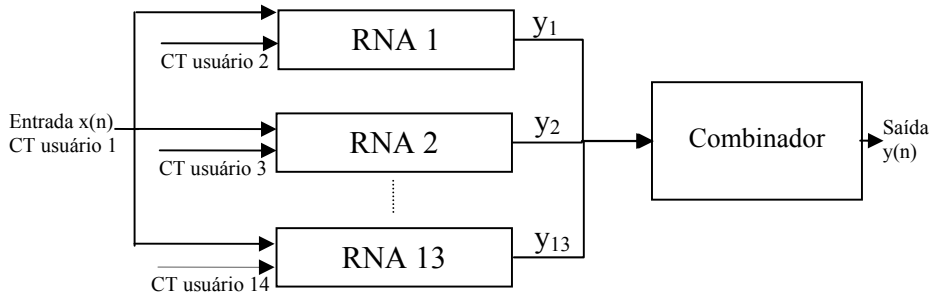


Fig. 4.3 - Treinamento da estrutura baseada em máquinas de comitê.

Na etapa de treinamento a figura do combinador é meramente ilustrativa, pois cada RNA é treinada separadamente com os dados do conjunto de treinamento apresentados a ela. Após treinadas todas as RNAs é possível montar a máquina de comitê de cada usuário. Na verificação da identidade de um usuário, o combinador tem papel fundamental e seu funcionamento será descrito adiante. A figura 4.2 representa a máquina de comitê já treinada de um dado usuário.

Definidas as estruturas de RNAs que podem ser utilizadas, pode-se então especificar o funcionamento do sistema biométrico. Como visto no inicio deste tópico, o sistema biométrico foi dividido em duas etapas. A Figura 4.4 representa o funcionamento da etapa de coleta dos dados e formação do modelo.

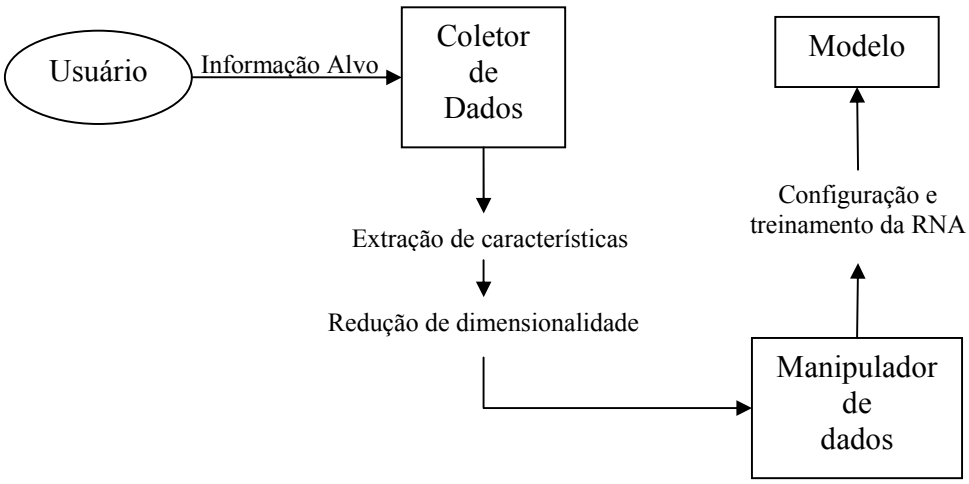


Fig. 4.4 - Procedimento de coleta e formação do modelo

O funcionamento do procedimento descrito na Figura 4.4 é o seguinte:

1. Todos os usuários (tópico 4.2.1) realizam o processo de coleta das informações alvo (tópico 4.2.2) através do sistema coletor de dados (tópico 4.2.2) até atingir a quantidade de amostras desejadas (tópico 4.2.4);
2. O sistema coletor de dados realizará a extração de características da digitação do usuário (tópico 4.2.5);
3. Um procedimento de redução da dimensionalidade (tópico 4.2.7) é realizado;
4. As amostras coletadas são separadas em conjunto de treinamento e conjunto de testes para cada usuário (tópico 4.2.8), sendo que apenas os conjuntos de treinamento são importados pelo sistema manipulador de dados (tópico 4.3.2).
5. O conjunto de treinamento da RNA é composto pelo conjunto de treinamento do usuário válido e do conjunto de treinamento de usuários inválidos conforme a estrutura de RNA utilizada. Desta forma depois de configurada e treinada a estrutura da RNA gera um modelo do usuário válido. Este modelo é composto pelo conjunto de pesos da estrutura da RNA.

Depois de realizada a etapa de coleta de dados e formação do modelo dos usuários, o sistema está pronto para identificar se determinadas amostras apresentadas pertencem a um determinado modelo de usuário ou não. A Figura 4.5 representa o funcionamento da etapa de coleta dos dados e classificação do usuário.

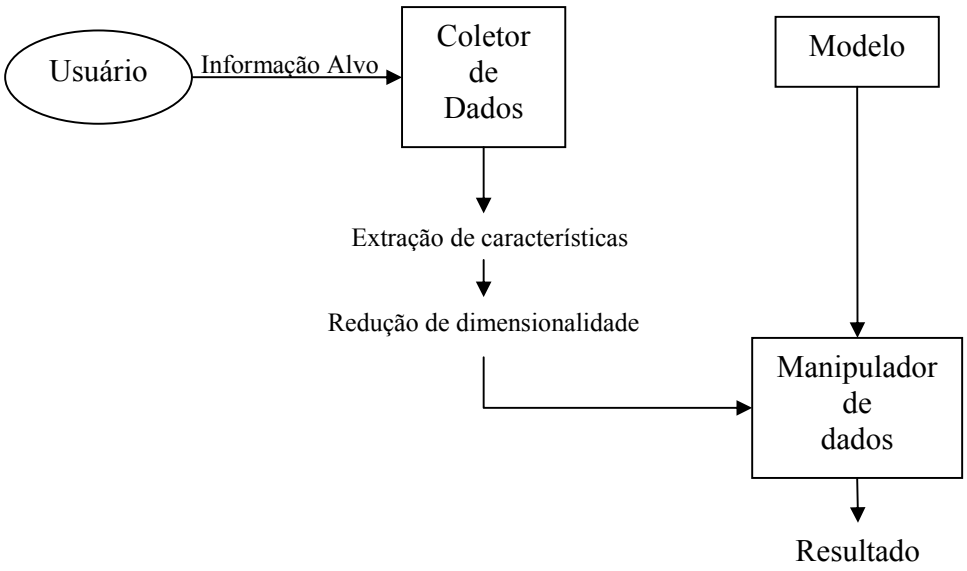


Fig. 4.5 - Procedimento de classificação do usuário

As únicas diferenças desta etapa para a etapa de geração do modelo é que ao invés de utilizar como entrada no manipulador de dados os conjuntos de treinamento dos usuários, nesta etapa serão apresentados os conjuntos de testes, tanto dos usuários do grupo 1 como dos usuários do grupo 2, e além disto é selecionada a estrutura de RNA do usuário que diz estar entrando com os dados. Estes dados são propagados pela estrutura de RNA já treinada gerando um resultado de classificação do usuário.

Para determinar se uma amostra apresentada é válida ou não, foram definidos alguns limiares. Na estrutura composta por uma única RNA, definiu-se um limiar configurável da porcentagem de dígrafos classificados como válidos pela RNA do usuário; portanto se este limiar for configurado em 50%, por exemplo, as amostras de testes somente serão consideradas válidas se 50% ou mais dos dígrafos desta forem classificados como válidos pela RNA do usuário, caso contrário, a amostra será considerada como de um intruso. A variação deste limiar aumenta ou diminui a segurança do sistema de classificação.

Para a estrutura de RNA composta por uma máquina de comitê, foram definidos 2 limiares configuráveis: o primeiro é relacionado à porcentagem de dígrafos classificados corretamente pela máquina de comitê; o segundo limiar é relacionado ao número de RNAs que devem classificar o dado como válido. Este segundo limiar é utilizado pelo combinador da máquina de comitê. Desta forma a resposta de uma máquina de comitê apenas apontará

os dados de entrada apresentados como válidos, se a quantidade de RNAs que apresentam saída válida for maior ou igual ao valor configurado para este limiar.

Por exemplo, configurando o limiar de porcentagem de dígrafos classificados corretamente em 50% e o limiar de número de RNAs que classificam o dígrafo corretamente em 8, somente as amostras que obtiverem a classificação correta de 50% ou mais de seus dígrafos pela máquina de comitê, são considerados válidos. A resposta da máquina de comitê para um dígrafo de entrada, será valida apenas se 8 ou mais RNAs considerarem o dado de entrada válido (cálculo realizado pelo combinador), caso contrário este dado de entrada é considerado inválido. Novamente o relaxamento ou rigidez na configuração destes limiares implica a menor ou maior segurança do sistema biométrico.

4.2 – Aspectos Importantes na Definição do Sistema Biométrico

Como visto no capítulo 2, alguns aspectos precisam ser especificados na construção de um sistema biométrico. Esta seção apresentará a definição de cada um destes aspectos e a ferramenta implementada para coletar os dados dos usuários que serão analisados. Na seção 4.3 serão apresentadas as ferramentas implementadas para a manipulação destes dados.

4.2.1 – Usuários Analisados

Neste trabalho foram analisados 20 usuários sendo que estes não precisavam apresentar nenhuma característica especial, como por exemplo, terem curso de datilografia, mas deveriam apenas conhecer e saber utilizar um microcomputador e seu teclado.

Estes usuários foram divididos em 2 grupos. O grupo 1 é composto por 14 usuários que tiveram seus dados coletados divididos em dois conjuntos: conjunto de treinamento e conjunto de testes. Já o grupo 2, constituído por 6 usuários, tiveram seus dados utilizados apenas no teste do sistema biométrico, sendo que estes usuários agiram apenas como "intrusos" e são essenciais para verificar a eficácia do sistema biométrico quanto à falsa aceitação de usuários.

Grupo	Número de Usuários
Grupo 1	14
Grupo 2	6

Tabela 4.1 - Quantidade de usuários por grupo pesquisado

Os dados de testes dos usuários do grupo 1 foram utilizados para verificar a eficácia do sistema quanto a falsa rejeição de usuários válidos e também quanto a falsa aceitação de intrusos.

4.2.2 – Informação Alvo e o Coletor de Dados

Como informação alvo, ou seja, as informações que foram coletadas para análise da metodologia proposta, foram utilizadas: uma frase contendo 32 caracteres, um texto fixo com 347 caracteres e um texto livre cujo tamanho varia de acordo com a vontade do usuário analisado.

Para facilitar a memorização do texto fixo, foi escolhida para este propósito uma música. Esta medida visa minimizar a interrupção da digitação pelo usuário para ler o conteúdo do texto; isto é desejável, já que estas interrupções geram coletas de medidas de tempo que geralmente não correspondem ao tempo padrão de digitação do usuário.

Para coletar estas informações alvo, fez-se necessária a implementação de uma ferramenta de coleta de dados, chamada de coletor de dados. Nesta ferramenta, cada usuário analisado pode digitar os textos componentes de cada informação alvo. Cada texto digitado corresponde a uma amostra da informação alvo selecionada. A Figura 4.6 demonstra a interface do programa coletor de dados.

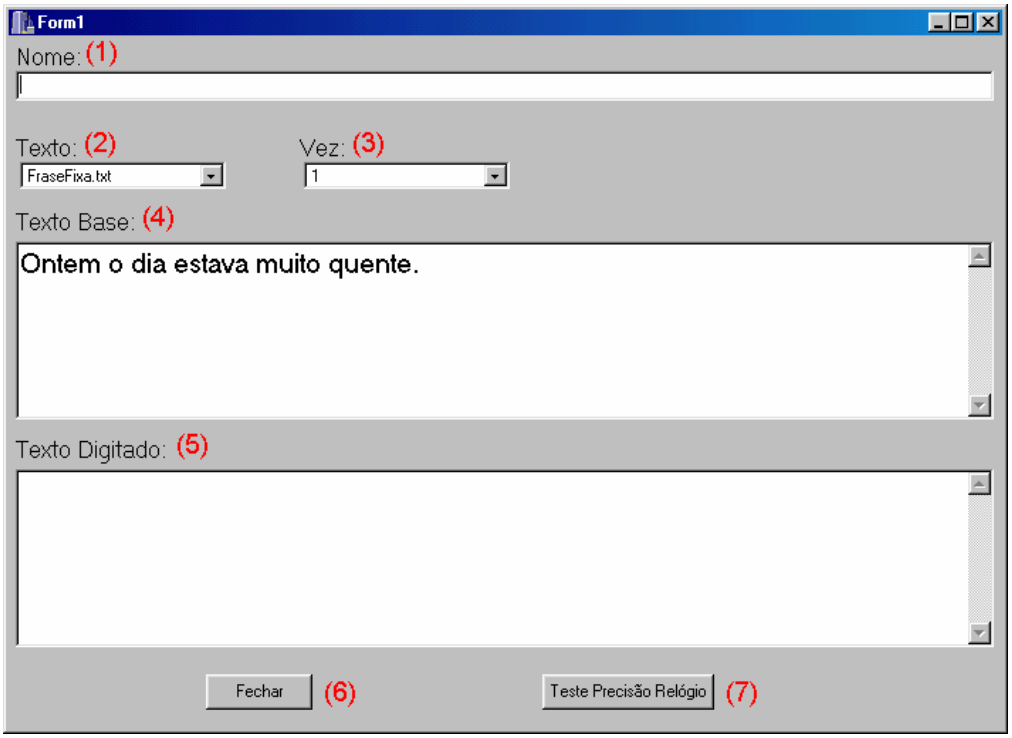


Fig. 4.6 - Coletor de dados

A Figura 4.6 identifica alguns pontos importantes da ferramenta. Estes pontos, que foram marcados por números entre parênteses na figura são:

1. Nome: cada usuário analisado deve digitar seu nome neste campo. O nome do usuário será utilizado para identificar a amostra da informação alvo coletada, desta forma é possível determinar a quem a amostra pertence;
2. Texto: o usuário deve selecionar neste campo qual a informação alvo que ele deseja digitar. Depois de selecionada esta opção a caixa de texto "*Texto Base",* identificada por (4) na figura, será atualizada com o conteúdo da informação alvo selecionada. O nome da informação alvo selecionada também é utilizado na identificação da amostra coletada;
3. Vez: este campo é utilizado para selecionar qual é o número da vez que o usuário está digitando a informação alvo num determinado dia. O valor deste campo também é utilizado para identificar a amostra coletada. O tópico 4.2.4 definirá qual a quantidade de amostras solicitadas neste trabalho;

4. Texto Base: será atualizado conforme a seleção do campo "*Texto*", identificado por (2) na figura. Neste campo será colocada a informação que o usuário deverá digitar. Se o conteúdo desta informação excede os limites mostrados na tela, uma atualização constante na posição mostrada é efetuada de modo que o texto corre sozinho à medida que o usuário digita a informação no campo "*Texto Digitado*" (5), desta forma o usuário não necessita interromper a digitação para baixar a barra de rolagem do "*Texto Base*";
5. Texto Digitado: é o campo onde o usuário deverá copiar as informações contidas no campo "*Texto Base*" (4). Conforme o usuário digita dados neste campo, as características de sua digitação são coletadas. O tópico 4.2.5 definirá quais são as características coletadas neste trabalho e qual a forma de armazenamento destas informações;
6. Fechar: botão para fechar o programa, somente deve ser acionado após coletar todas as amostras definidas pelo tópico 4.2.4 de todas as informações alvo;
7. Teste precisão relógio: este botão é essencial para o funcionamento do programa. Quando pressionado ele executa uma rotina de verificação da precisão do relógio do computador em questão. Se o tempo verificado for maior que 1 milisegundo, que é o limite de precisão imposto no trabalho, o computador não poderá ser utilizado no processo de coleta de dados. Esta operação sempre deverá ser realizada antes de qualquer coleta. O tópico 4.2.6 define a rotina de verificação da precisão adotada.

O programa coletor de dados apresentado na Figura 4.6 está diretamente relacionado aos aspectos definidos pelos tópicos 4.2.1 à 4.2.6 e é através deste programa que se fez possível coletar todas as informações necessárias pelas outras ferramentas implementadas que serão abordadas no tópico 4.3.

4.2.3 - Ambiente de Coleta

Cada usuário realizou o processo de coleta, através do programa coletor de dados, na própria máquina que está habituado a utilizar, sendo que algumas restrições foram impostas na utilização desta. São elas:

- Utilização do sistema operacional Windows: pois a aplicação de coleta utilizada foi desenvolvida para esta plataforma;
- Apresentar precisão de 1 milisegundo.

4.2.4 – Quantidade de Amostras

Em cada processo de coleta o usuário teve que digitar todas as informações alvo 5 vezes num mesmo dia. Este processo foi realizado uma única vez pelos usuários do grupo 2 e foi repetido 6 vezes pelos usuários do grupo 1, sendo que cada coleta foi realizada obrigatoriamente em dias distintos.

Como resultado destas coletas tem-se que cada usuário do grupo 1 forneceu 30 amostras de cada informação alvo, já os usuários do grupo 2 forneceram 5 amostras de cada informação alvo.

4.2.5 – Características Coletadas e Armazenamento

Para cada tecla pressionada ou liberada durante o processo de coleta da informação alvo foram armazenados o seu código virtual e o tempo em que a mesma foi digitada. O armazenamento destas informações foi realizado através da gravação de dois arquivos: um contento os dados das teclas pressionadas e o outro contento os dados das teclas liberadas. Cada arquivo é identificado pela data da coleta, nome do usuário, informação alvo coletada, número da vez que a amostra está sendo coletada e identificação de arquivo de pressionamento ou liberação de teclas. Por exemplo, o arquivo identificado pelo nome 04-02-2005_Usuario1_FraseFixa_1_KeyDown.txt, corresponde a coleta das características

no dia 4 de fevereiro de 2005 pelo usuário 1, sendo a informação coletada a frase fixa na sua primeira amostra e referente aos tempos de pressionamentos das teclas.

Com estas informações é possível calcular qualquer medida de latência entre teclas, seja a latência entre o pressionamento de duas teclas consecutivas, o pressionamento e liberação da mesma tecla ou qualquer outra medida envolvendo a latência entre uma ou mais teclas. Desta forma o sistema biométrico poderia utilizar qualquer uma das características de latência entre teclas.

Outro fator importante a salientar é que como qualquer tecla pressionada ou liberada gera uma ação de gravação do evento ocorrido, o sistema de captura não precisa se preocupar com o fato de que o texto digitado não pode conter erros. Pelo contrário, caso o erro ocorra, o padrão de correção do erro também poderá ser medido pela análise do tempo em que o usuário leva para apagar um ou mais caracteres.

Portanto, para cada processo de coleta através da ferramenta coletora de dados, um usuário produzirá 30 arquivos com informações de suas características, sendo que para cada informação alvo existirá 5 arquivos com os tempos referentes ao pressionamento das teclas e 5 para os tempos de liberação das teclas.

Como os usuários do grupo 2 realizam o processo de coleta uma única vez, existem 30 arquivos de características coletadas para cada usuário deste grupo. Já para os usuários do grupo 1, que devem realizar o processo de coleta em 6 dias distintos, existem 180 arquivos de características coletadas.

4.2.6 – Precisão do Tempo

Para coletar o tempo no momento do pressionamento ou liberação de uma tecla foi utilizada a função do Windows "*timeGetTime*" que recupera a quantidade de tempo em que o sistema está ligado. Este valor do tempo de funcionamento do sistema está expresso em milisegundos. Nas versões mais antigas do Windows, como por exemplo, Windows 95 e 98, esta função apresenta precisão de 1 milisegundo, entretanto nas versões mais recentes como o Windows 2000 ou o XP, esta precisão vai ser dependente da máquina.

Para resolver este problema de precisão de algumas das versões foi criada uma função que analisa se a precisão do computador é de 1 milisegundo. Caso esta função

verifique que o computador não apresenta a precisão desejada este não poderá ser utilizado no experimento do trabalho em questão.

4.2.7 – Redução da Dimensionalidade

As características das teclas coletadas possibilitam uma grande variedade de cálculos de latência como citado no tópico 4.2.5. Cada um destes cálculos compõe uma característica diferente da dinâmica da digitação de um determinado indivíduo. Para não trabalhar com todas estas características, uma redução da dimensionalidade do espaço de características foi proposto de modo a utilizar apenas o tempo da latência entre o pressionamento de duas teclas consecutivas. Esta redução se faz necessária devido ao pouco tempo disponível para realizar as pesquisas e principalmente pela redução de complexidade e custo computacional do sistema, já que estes aumentam proporcionalmente a cada nova característica adotada.

Outro fator determinante na escolha de apenas uma característica é o fato de se analisar os resultados do sistema biométrico proposto, sendo que em caso de bons resultados, outras características podem ser incorporadas ao sistema em trabalhos futuros. Deste modo os arquivos coletados com informações de liberação das teclas não serão utilizados neste trabalho.

4.2.8 – Conjuntos de Treinamento e de Testes do Usuário

Como descrito no tópico 4.2.1, as amostras coletadas pelos usuários do grupo 1 foram divididas em conjunto de treinamento e conjunto de testes, sendo que estes conjuntos foram definidos da seguinte maneira:

- Conjunto de treinamento: composto pelas coletas ímpares de cada dia, ou seja, como cada usuário coletou 5 vezes cada informação alvo em cada dia, as amostras de número 1, 3 e 5 de cada dia para a informação em questão formam o conjunto de treinamento do usuário para esta informação alvo.

- Conjunto de testes: as amostras pares compõem o conjunto de testes de cada usuário para a informação alvo.

Portanto cada usuário do grupo 1 terá um conjunto de treinamento formado por 18 amostras e um conjunto de testes formado por 12 amostras para a frase fixa, o texto fixo e o texto livre. Já os usuários do grupo 2 terão apenas o conjunto de testes de cada informação, sendo que este conjunto será formado por todas as coletas da informação, ou seja, cada conjunto de teste possui 5 amostras de coleta.

É difícil definir o tamanho exato de cada conjunto de treinamento, pois ele varia de acordo com a informação alvo que ele representa e também de acordo com o usuário. Esta variação no tamanho do conjunto de treinamento para cada usuário se deve principalmente a dois fatores: alguns usuários podem ter cometido mais erros de digitação do que outros e alguns usuários digitaram todas as acentuações do texto corretamente e outros não.

Como referência, pode-se citar que o tamanho mínimo para o conjunto de treinamento (formado por 18 amostras) da frase fixa é composto por 558 exemplos de latências entre dígrafos e 6246 exemplos para o texto fixo. Quanto ao tamanho do conjunto de treinamento do texto livre, nada se pode afirmar, pois o tamanho é livre.

Com relação ao tamanho das amostras de testes, pode-se definir como 31 o tamanho mínimo de uma amostra da frase fixa e 347 para amostras de texto fixo; novamente nada pode ser dito a respeito do tamanho das amostras de texto livre.

Estes conjuntos de treinamentos de cada usuário do grupo 1 serão utilizados para montar o modelo ("*template"*) do usuário de acordo com a metodologia empregada. As amostras de testes serão utilizadas para fazer a verificação da eficácia do sistema proposto e os experimentos e resultados obtidos serão apresentados no Capítulo 5.

4.2.9 – Classificação

O processo de classificação do sistema biométrico proposto é realizado através de RNAs, sendo que as características da RNA implementada neste trabalho podem ser

verificadas no tópico 4.3.1. Quanto à metodologia de classificação, o tópico 4.1 mostra o funcionamento do sistema biométrico proposto.

4.3 – Ferramentas Implementadas

Para viabilizar a construção do sistema biométrico proposto foram necessárias as implementações de duas ferramentas auxiliares: coletor de dados e manipulador de dados. O coletor de dados já foi apresentado no tópico 4.2.2, portanto neste tópico serão apresentadas as RNAs implementadas e o programa manipulador de dados, que utiliza estas RNAs para montar o modelo dos usuários e também na verificação da validade dos dados apresentados por um determinado usuário.

4.3.1– RNA

Para o propósito de classificação dos padrões analisados foi implementada uma arquitetura de RNA direta com algoritmo de aprendizado supervisionado (retro-propagação) utilizando a tangente hiperbólica como função de saída. A rede implementa bias da camada de entrada para a camada intermediária e da camada intermediária para a camada de saída. Na RNA é possível configurar os seguintes parâmetros:

- Número de neurônios de entrada: pode ser escolhido entre os valores 3, 257, 258 e 513 (explicados a seguir);
- Número de neurônios na camada intermediária: pode variar de 1 a 257;
- Coeficiente de aprendizado; e
- Número de iterações: usado como critério de parada no algoritmo de treinamento

A rede sempre utiliza apenas um neurônio na camada de saída e quando o valor de saída deste for maior ou igual a zero, os dados de entrada apresentados para a rede são considerados válidos, caso contrário os mesmos são considerados dados de intrusos.

Os valores da latência entre teclas são normalizados entre -1 e 1 levando em consideração que o valor para o tempo mínimo é de 0 ms e o tempo máximo é de 600 milisegundos. Este valor máximo adotado para a latência foi obtido através da análise das freqüências dos tempos de latência entre pressionamento de teclas de todos os usuários.

O gráfico apresentado na Figura 4.7 mostra a distribuição de freqüência das latências entre teclas obtidas nas coletas de dados dos usuários.

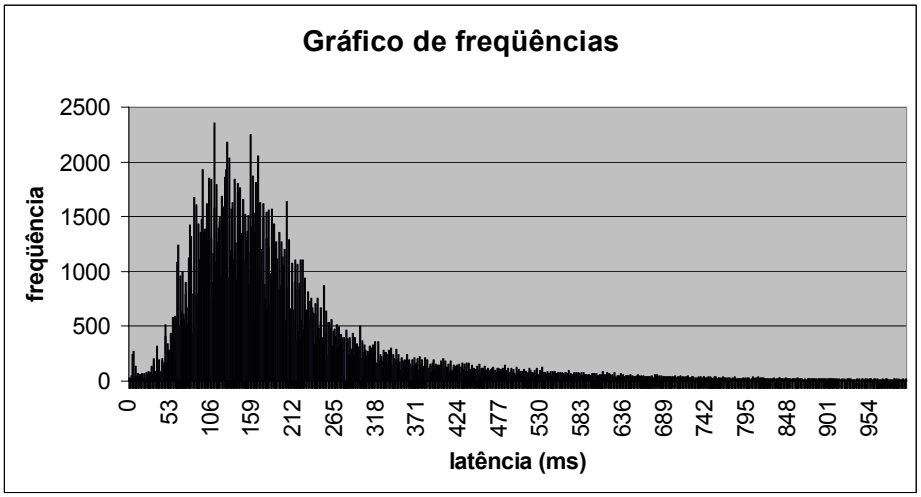


Fig. 4.7 - Freqüência das latências entre teclas de pressionamento

Dos valores contidos no gráfico expresso na Figura 4.7 tem-se que o tempo médio de latência entre duas teclas seguidas para todos os usuários é de 248,58 milisegundos e a porcentagem de amostras com tempo inferior à média é de 75%. Observando a porcentagem de amostras contempladas até um valor máximo, obteve-se que aproximadamente 95% das latências estavam entre 0 e 600 milisegundos. Portanto decidiu-se que tempos de latência entre teclas acima de 600 milisegundos são correspondentes a interrupções do usuário na digitação. Todas as configurações de RNA possíveis utilizarão, portanto este valor de normalização para o tempo de latência entre as teclas pressionadas.

Quanto ao número de neurônios na camada de entrada, quando a rede trabalha com apenas 3 neurônios, o primeiro neurônio deverá ser ativado com o valor do código virtual normalizado da primeira tecla do dígrafo pressionada, o segundo neurônio deverá ser ativado com o valor do código normalizado da segunda tecla pressionada e o terceiro neurônio com o valor da latência (normalizado) entre os pressionamentos consecutivos. Os

valores dos códigos virtuais das teclas variam entre os valores 0 e 255 e estes valores são normalizados entre -1 e 1. Esta configuração da RNA aprende latências de teclas, considerando a ordem em que a tecla foi digitada.

Se a opção do número de neurônios na camada de entrada escolhida for de 257, dos primeiros 256 neurônios (nomeados de neurônio 0 à neurônio 255), apenas os neurônios referentes aos códigos virtuais das teclas pressionadas deverão estar ativos com o valor 1. Os demais neurônios devem estar desativados, contendo o valor 0. O valor do último neurônio (nomeado de neurônio de latência) deverá conter o tempo normalizado da latência medida entre as teclas. Esta RNA aprende as latências independente da ordem em que as teclas foram pressionadas. Para ilustrar um exemplo de propagação de um valor de entrada na RNA a Figura 4.8 pode ser consultada.

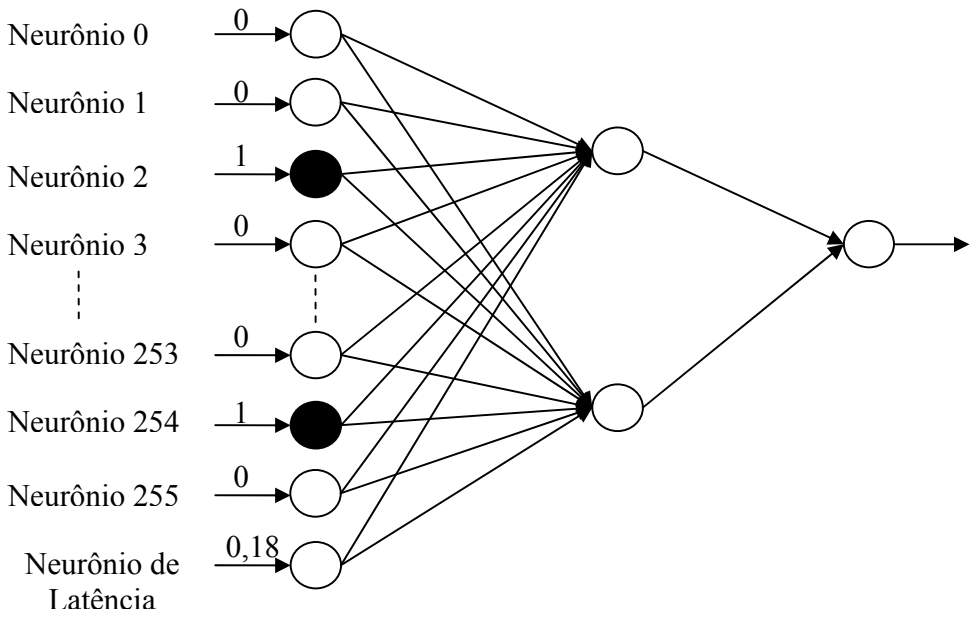


Fig. 4.8 - Exemplo de propagação de valores de entrada a RNA composta por 257 neurônios na camada de entrada e 2 neurônios na camada intermediária.

A Figura 4.8 representa os valores de entrada para a RNA considerando um exemplo de dígrafo propagado pela RNA composto pelos códigos virtuais 2 e 254 (onde 2 é o código virtual da 1ª tecla pressionada e 254 é o código virtual da 2ª tecla pressionada) e latência normalizada entre os pressionamentos consecutivos de 0,18 (353 ms).

Na configuração de 258 neurônios de entrada a única alteração ocorre com a adição de mais um neurônio (nomeado neurônio de ordem) que indicará a ordem dos códigos virtuais, ou seja, a ordem com que as teclas do dígrafo foram digitadas é considerada. Se o código da primeira tecla pressionada é menor que o da segunda, então o neurônio estará ativado (valor 1) senão estará desativado com valor 0.

Finalmente na configuração com 513 neurônios de entrada o seguinte padrão é seguido: dentre os primeiros 256 neurônios (nomeados de neurônio 0 da primeira tecla à neurônio 255 da primeira tecla), apenas o de número referente ao código virtual da primeira tecla pressionada estará ativado, os outros 255 estarão desativados; dos próximos 256 neurônios (nomeados de neurônio 0 da segunda tecla à neurônio 255 da segunda tecla), apenas o de número referente ao código virtual da segunda tecla pressionada estará ativado, por fim o último neurônio (nomeado de neurônio de latência) estará ativado com o valor normalizado do tempo de latência entre as teclas. Esta RNA também leva em consideração a ordem em que as teclas foram digitadas.

No treinamento da RNA, sempre serão considerados apenas os exemplos do conjunto de treinamento que apresentam medida de latência entre as teclas menor ou igual a 600 milisegundos, sendo que tempos medidos acima deste limite são ignorados pelo algoritmo de treinamento por serem considerados interrupções na digitação normal do usuário. Esta medida também evita que a RNA receba exemplos distorcidos que podem prejudicar o aprendizado da RNA. Esta medida é aceitável já que o valor de 600 milisegundos está bastante acima da média de latência calculada com todos os usuários.

No próximo capítulo, “Experimentos e Resultados”, serão apresentados os motivos de ser ter implementado estes tipos diversos de RNA quanto ao número de neurônios na camada de entrada.

4.3.2 – Manipulador de Dados

A última ferramenta implementada, chamada de manipulador de dados, possui um mecanismo de análise gráfica dos dados válidos e inválidos dos usuários testados e integra a RNA implementada. Esta ferramenta é a principal do sistema e ela compõe os mecanismos de “inscrição” e “verificação” descritos no capítulo 2, tópico 2.2.

Num primeiro momento, esta ferramenta pode ser utilizada para manipular os dados coletados de um determinado usuário com o objetivo de treinar uma ou mais RNAs. Na etapa de treinamento são apresentados ao sistema o conjunto de treinamento do usuário válido e conjuntos de treinamento de usuários inválidos. O próximo tópico especifica mais detalhadamente quais são os conjuntos de treinamentos envolvidos. Após a apresentação destes dados, o sistema permite comparar as medidas dos dados válidos para o usuário e os dados inválidos, possibilitando analisar se estes dados podem ser visivelmente separados entre o padrão do usuário válido e o dos usuários inválidos.

Após esta análise os dados podem ser apresentados a uma ou mais RNAs, descritas no tópico 4.3.1, para que esta(s) possa(m) ser treinada(s). O conjunto de pesos desta(s) RNA(s) treinada(s) para o usuário em questão formará o modelo do usuário que representa a sua "inscrição" no sistema.

Para o mecanismo de verificação, a ferramenta possibilita que um modelo de usuário seja carregado e após este procedimento é possível apresentar dados de digitação, pertencentes ao conjunto de testes, para que estes sejam analisados e verificados se pertencem ao modelo do usuário carregado, ou seja, pertencem ao usuário válido, ou são dados de um intruso. Esta verificação é realizada através da classificação dos dados analisados pela(s) RNA(s) treinada(s).

A Figura 4.9 demonstra a interface gráfica da ferramenta implementada e algumas funções importantes. Estas funções, que foram marcadas por números entre parênteses na figura são:

1. Arquivo do conjunto de treinamento na etapa de inscrição ou arquivo do conjunto de teste na etapa de verificação a ser adicionado no sistema;
2. Caixa de seleção para informar se os dados do arquivo informado em (1) são válidos ou inválidos;
3. Adiciona o conteúdo do arquivo (1) na lista (5) definindo se os mesmos são válidos ou não de acordo com a seleção escolhida em (2);
4. Botões para mostrar a lista de dados já inseridos;

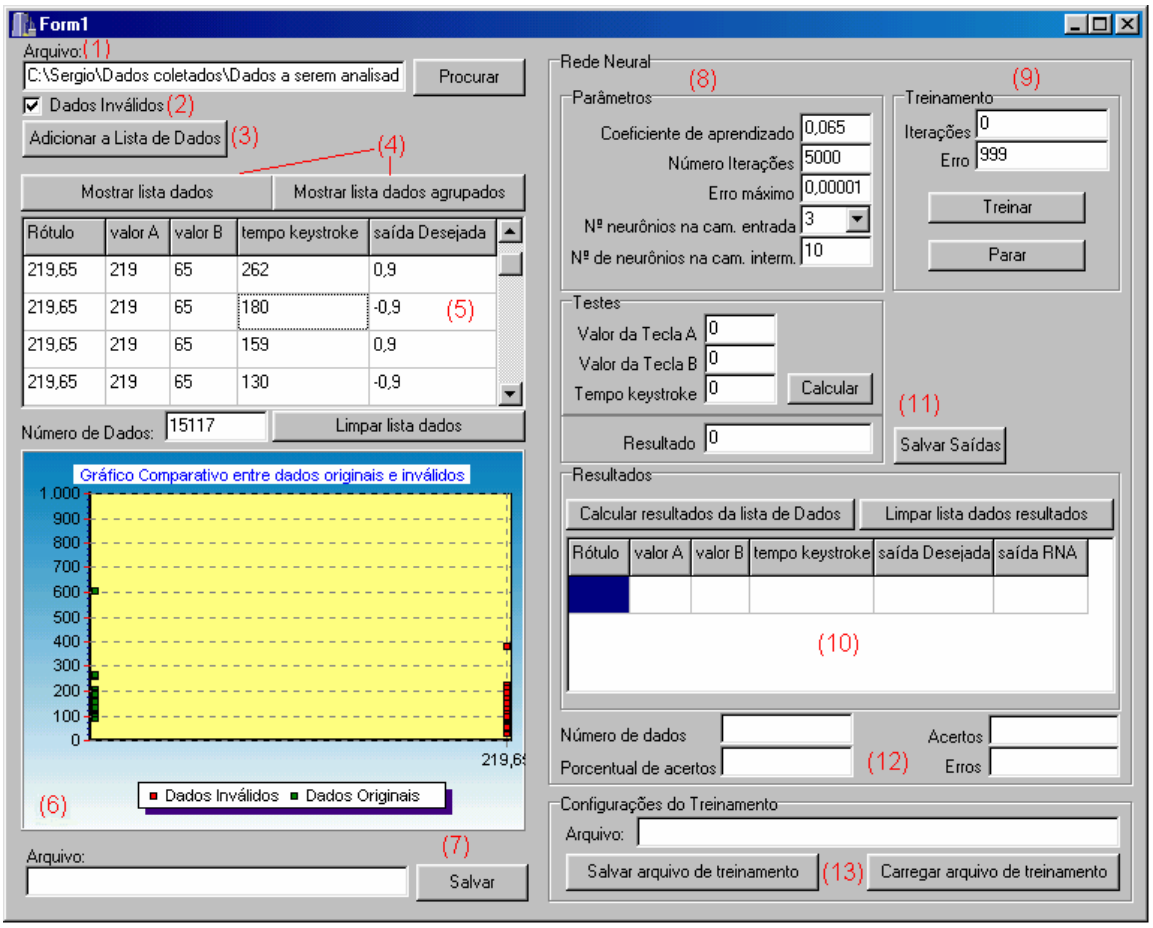


Fig. 4.9 - Manipulador de dados

5. Lista de todos os dados inseridos no sistema; através desta lista pode-se verificar o tempo da latência entre duas teclas consecutivas, os códigos das teclas e ainda qual é a saída desejada no processo de treinamento da RNA. Quando uma das células é clicada, o gráfico (6) é atualizado com todos os dados referente aos tempos dos dígrafos válidos e inválidos para o respectivo conjunto de teclas selecionado;
6. Gráfico comparativo entre os dados válidos do usuário e os dados de usuários inválidos. Este gráfico é atualizado conforme a célula da lista (5) selecionada;
7. Opção para salvar os dados que estão inseridos na lista (5);
8. Parâmetros configuráveis da RNA, estes parâmetros serão utilizados no treinamento da RNA e também para definir a estrutura da RNA;

9. Informações do treinamento: é possível clicar no botão treinar para iniciar um treinamento, parar o treinamento e ainda acompanhar qual o número de iterações de treinamento já realizadas e qual o erro total dos dados de saída;
10. Lista de resultados da operação de apresentação dos dados da lista (5) para a RNA treinada.
11. Botão para salvar os resultados apresentados na lista (10). Estes resultados serão analisados de acordo com limiares para verificar se os dados são válidos ou não;
12. Estatísticas sobre a quantidade de acertos e erros da RNA quanto aos exemplos apresentados à RNA;
13. Opções de salvar ou carregar os pesos de uma determinada RNA. Esta função é importante para gravar um modelo de usuário e para recuperar modelos para realizar o processo de verificação.

O próximo tópico apresenta a metodologia do sistema biométrico proposto e especifica mais detalhadamente a interoperabilidade entre cada ferramenta. A ferramenta manipulador de dados, visualizada na Figura 4.9, foi utilizada em todos os experimentos descritos no Capítulo 5.

4.4 – Infra-Estrutura e Ferramentas Utilizadas

Este trabalho foi desenvolvido no Laboratório de Conexionismo e Ciências Cognitivas (L3C) da Universidade Federal se Santa Catarina (UFSC) e para a realização dos experimentos, implementação das aplicações e treinamento das RNA foram disponibilizados 2 microcomputadores Pentium 4 (1600 MHz e 1800 MHz) com 256 MB de memória RAM e 1 microcomputador Pentium 3 (600 MHz) com 128 MB de memória RAM. Como ferramentas auxiliares foram utilizadas o Borland C++ Builder 5.0 para implementar as aplicações além do Microsoft Excel para representar as tabelas de resultados.

4.5 – Conclusão

Neste capítulo foi especificado qual o tratamento dado a cada aspecto componente dos sistemas biométricos e quais as implementações realizadas para prover as ferramentas necessárias para analisar o sistema biométrico proposto no tópico 4.1. Ainda neste tópico foram apresentadas duas estruturas de RNA que podem ser utilizadas como estruturas de geração do modelo dos usuários e posterior classificação dos mesmos. Com isto, experimentos sobre o sistema biométrico proposto já podem ser realizados de modo a testar a eficácia do mesmo na classificação correta dos usuários do sistema e encontrar as melhores configurações de limiares para o sistema biométrico. Este é o tema do próximo capítulo: “Experimentos e Resultados”.

Capítulo 5 – Experimentos e Resultados

Introdução

Para avaliação do sistema biométrico proposto foram realizados alguns experimentos que são abordados neste capítulo. O primeiro experimento foi realizado com o objetivo de verificar qual a melhor configuração dos parâmetros da RNA. Os experimentos seguintes foram realizados para testar as estruturas do classificador propostas no Capítulo 4. Para cada experimento há uma seção de análise dos resultados obtidos.

5.1 – Experimento 1 - Análise dos Parâmetros Configuráveis da RNA

Como visto no Capítulo 4, as coletas de dados dos usuários geram uma grande quantidade de exemplos de treinamento que deverão ser apresentados para a RNA com o propósito de treinamento da mesma. Devido a esta grande quantidade de exemplos e o tempo limitado para realização da pesquisa abordada neste trabalho, torna-se inviável realizar testes sobre os conjuntos de treinamento completos para várias configurações possíveis da RNA, portanto este experimento tem o objetivo de realizar alguns testes preliminares, utilizando poucos exemplos de treinamento, para verificar o comportamento da RNA, dadas algumas configurações propostas e encontrar uma configuração aceitável, sendo que esta será utilizada pelos demais experimentos abordados neste capítulo.

No Capítulo 4 a RNA foi definida apresentando como parâmetros de configuração: o número de neurônios na camada de entrada, número de neurônios na camada intermediária, o coeficiente de aprendizado e o número de iterações de treinamento.

Quanto ao número de neurônios na camada de entrada, 4 possibilidades de configuração (3, 257, 258 e 513) são definidas, enquanto que os demais parâmetros apresentam um intervalo de variação muito maior.

Para este experimento foram utilizados apenas os conjuntos de treinamento referentes à coleta da frase fixa de apenas 2 usuários, sendo que o conjunto de treinamento

de um dos usuários foi apresentado à RNA como sendo o conjunto de dados válidos e o conjunto de treinamento do outro usuário foi apresentado como dados inválidos. O conjunto de treinamento da RNA para estes dois usuários apresentou tamanho de 1227 exemplos. Com este conjunto de treinamento de tamanho reduzido foi possível realizar os testes de configuração para treinar a RNA num tempo aceitável. Neste experimento, apenas os dados do conjunto de treinamento foram utilizados.

As 4 possibilidades de número de neurônios da camada de entrada foram combinadas com os seguintes valores dos demais parâmetros configuráveis:

- Número de neurônios na camada intermediária: 5, 10 e 15;
- Coeficiente de aprendizado: 0,01; 0,065 e 0,09;
- Número de iterações: 1000, 3000 e 5000.

5.1.1 – Resultados do Experimento 1

A análise dos resultados de treinamento mostrou que a eficiência deste não sofreu grandes alterações usando as variações propostas do coeficiente de aprendizado, número de neurônios na camada intermediária e número de iterações testadas, sendo que as RNAs numa determinada configuração apresentavam melhores resultados com um determinado valor destes parâmetros e em outra o melhor resultado era obtido com valores diferentes.

Uma observação importante neste experimento foi a ocorrência de uma grande variação entre as configurações da RNA com relação ao número de neurônios na camada de entrada. A Tabela 5.1 mostra a pior, a melhor e a média das porcentagens de acerto da RNA avaliando a saída obtida e a saída desejada sobre o conjunto de treinamento, para as diferentes configurações da RNA, quanto ao número de neurônios de entrada, levando em consideração todas as combinações dos demais parâmetros utilizados.

Nº. de neurônios de entrada	Pior % de acerto	Melhor % de acerto	Média (%)
3	54,6	58,6	56,27
257	64,6	76,1	72,42
258	74,4	79,6	77,45
513	75,3	80,1	78,25

Tabela 5.1 - Eficiência das RNA quanto ao número de neurônios de entrada

Conclui-se da Tabela 5.1 que os melhores resultados obtidos, provém das RNAs configuradas com 513 neurônios na camada de entrada, sendo que sua eficiência média é 21,98 pontos percentuais melhor do que a utilização de apenas 3 neurônios nesta camada.

A baixa eficiência na utilização de apenas 3 neurônios na camada de entrada se deve ao fato de que os valores de entrada, ou seja, o código virtual das teclas, deve ser normalizado entre -1 e 1 para que o treinamento da RNA seja realizado. No momento da normalização as teclas com códigos virtuais próximos apresentam valores muito semelhantes e quando dois dígrafos diferentes que possuem uma tecla em comum e outra com códigos virtuais próximos, como por exemplo, os dígrafos “ab” e “ac”, representarão uma pequena variação nos valores de entrada da RNA e esta pode não distinguir que estes se tratam de dígrafos diferentes. O mesmo pode ocorrer com dois dígrafos que apresentam códigos virtuais próximos para as duas letras que o compõem. Como a RNA por natureza não é muito precisa e trabalha com a aproximação, sua classificação será comprometida na ocorrência destes casos.

Na utilização da RNA com 257 neurônios na camada de entrada o problema exposto no parágrafo anterior não ocorre, entretanto nesta configuração um outro problema foi descoberto. Quando dois dígrafos diferentes que apresentam as mesmas letras, como por exemplo, os dígrafos “ab” e “ba”, os valores de entrada para a RNA serão os mesmos, pois apenas os neurônios referentes aos códigos virtuais das letras “a” e “b” estarão ativos. Desta forma a RNA não consegue distinguir os dígrafos que apresentam esta característica e a eficiência da RNA fica comprometida.

As topologias utilizando 258 e 513 neurônios na camada de entrada resolvem este problema, mas como a RNA com 513 neurônios apresentou os melhores resultados este valor será utilizado nos demais experimentos. Apesar da pequena diferença entre os resultados da utilização de 258 e 513 neurônios na camada de entrada, a escolha pela RNA

com 513 neurônios deve-se principalmente ao fato de que como este é um sistema de segurança da informação, é desejado obter os melhores resultados, mesmo que para isto um pouco mais de recurso computacional seja necessário.

Quanto aos demais parâmetros de configuração, como não houve grande diferença entre os valores analisados, foram adotados nos demais experimentos: 10 neurônios na camada intermediária, 5000 iterações e coeficiente de aprendizado de 0,065.

5.2 – Experimento 2 – Utilização de RNA Única para Representar o Usuário

Neste experimento foi utilizada a estrutura composta por uma única RNA, apresentada no Capítulo 4, para representar cada usuário. Após o processo de treinamento de uma dada RNA os pesos desta representam o modelo do usuário que a RNA modela. Para treinar a RNA de um determinado usuário, o conjunto de treinamento do usuário é apresentado como sendo os dados válidos e o conjunto de treinamento de todos os demais usuários são apresentados como dados inválidos.

Portanto neste experimento, 14 RNAs devem ser treinadas, uma para cada usuário, sendo que todas as RNAs apresentam conjunto de treinamento de mesmo tamanho (9045 exemplos) e formado pelos dados de todos os usuários, sendo que apenas os dados referentes ao usuário que a RNA representa são apresentados como valores válidos.

Como determinado no tópico anterior, a RNA foi configurada com os seguintes parâmetros:

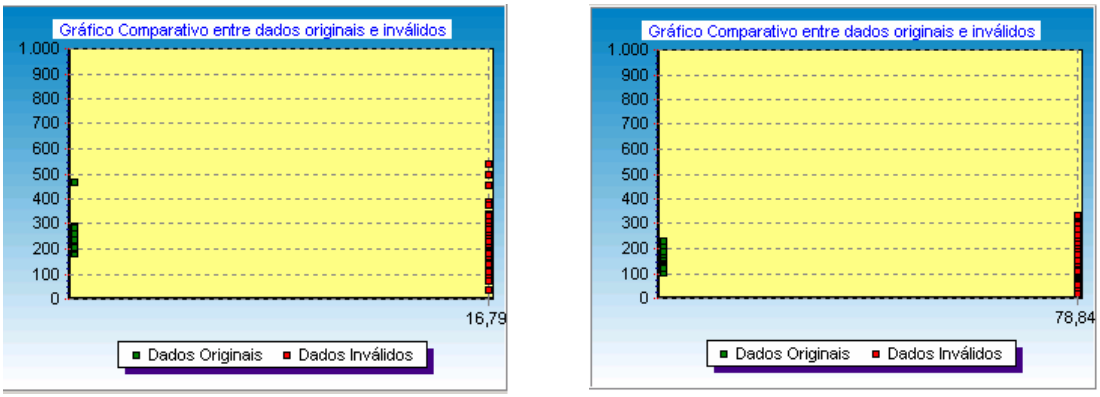
- 513 neurônios na camada de entrada;
- 10 neurônios na camada intermediária;
- coeficiente de aprendizado de 0,065; e
- 5000 iterações.

5.2.1 – Resultados do Experimento 2

Após o processo de treinamento constatou-se que a porcentagem de acertos da RNA sobre o conjunto de treinamento foi de 91,5% no entanto, quando as amostras de teste do usuário válido foram apresentadas para a RNA apenas 11,5% das latências foram classificadas corretamente, ou seja, como pertencentes a um usuário válido. Apresentando as latências das amostras de teste dos demais usuários do grupo 1, em média 3,1% das latências foram classificadas como sendo amostras de um usuário válido enquanto na análise das amostras dos usuários do grupo 2 a média de classificação de latências consideradas válidas foi de 4,3%. Para os treinamentos das RNAs restantes, ou seja, das RNAs de todos os demais usuários do grupo 1, os resultados foram muito semelhantes e as mesmas características foram obtidas.

Analisando cada uma das RNA treinadas, percebe-se que para cada usuário, a RNA que o representa consegue aprender a classificar corretamente apenas poucos dígrafos do usuário, portanto a "assinatura" do usuário para este sistema seria este pequeno conjunto de dígrafos que a RNA conseguiu aprender. O problema é que quando o usuário digitar textos que não contenham tais dígrafos de sua "assinatura", o sistema deverá classificar o usuário como sendo um usuário inválido. Outro problema que pode ser relatado neste experimento é que um possível intruso teria menos trabalho para acessar um sistema com tais características, pois bastaria que este intruso aprendesse o padrão de digitação de pouquíssimos dígrafos de um usuário válido.

Para entender melhor a causa de uma taxa reduzida de classificação correta pela RNA de cada usuário, foi realizada uma análise sobre os dados do conjunto de treinamento da RNA, através do programa "manipulador de dados", que possibilita comparar o tempo das latências dos dígrafos dos usuários válidos e inválidos foi realizada. Esta análise possibilitou verificar que, para praticamente todos os dígrafos presentes no conjunto de treinamento das RNA, os valores das latências pertencentes a usuários inválidos destes dígrafos cobre um intervalo que abrange o intervalo das latências pertencentes ao usuário válido. A Figura 5.1 representa graficamente o problema.

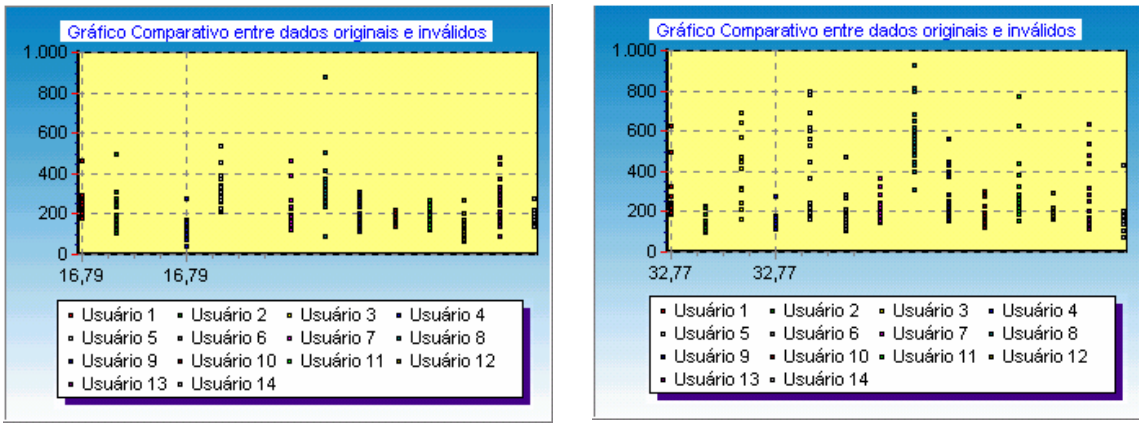


(a) comparação do dígrafo 16-79 *(b) comparação do dígrafo 78-84*

Fig. 5.1 - Representando o problema do experimento 2

Como pode ser visto na Figura 5.1, para praticamente todos os exemplos válidos apresentados para a RNA existem exemplos inválidos com valores iguais ou próximos a estes e, além disto, a quantidade de exemplos inválidos é maior do que os exemplos válidos. Isto impossibilita a RNA de aprender a classificar os dados apresentados a ela como válidos ou inválidos, pois na fase de treinamento alguns valores de latência entre teclas foram apresentados à RNA como sendo válidos e inválidos causando uma confusão na RNA.

Se esta análise for realizada sobre o conjunto de treinamento, mas separando os dados de treinamento por usuário a que o dado pertence, verifica-se que para praticamente todos os dígrafos analisados, existem 2 ou mais usuários que possuem latência semelhante entre teclas do dígrafo, por isso praticamente todos os valores das latências pertencentes a usuários inválidos neste experimento cobrem um intervalo que abrange o intervalo das latências pertencentes ao usuário válido. Para exemplificar a análise dos dados agrupados por usuários pode-se mostrar a Figura 5.2.



(a) comparação do dígrafo 16-79 *(b) comparação do dígrafo 32-77*

Fig. 5.2 - O problema do experimento 2 separado por usuário

A análise da Figura 5.2(a) permite verificar que para o dígrafo 16-79, os dados referentes às latências deste dígrafo para o usuário 10 é abrangido pelo intervalo de latências dos usuários 2, 7, 9, 11, e 13. Ainda nesta figura é possível verificar semelhanças entre as latências para outros usuários. A Figura 5.2(b) mostra ainda que alguns usuários apresentam latências muito diferentes para o dígrafo 32-77 e isto também ocorre para muitos outros dígrafos. Esta não uniformidade das latências faz com que quando os dados de todos os usuários, menos o que será considerado válido para treinamento da RNA, são agrupados para formar o conjunto de dados inválidos da RNA representem um grande intervalo de latências e que muitas vezes abrangem o intervalo de latências dos exemplos válidos.

Portanto deste experimento podemos concluir que a classificação de usuários através dos dados da latência de um dígrafo é uma tarefa bastante complexa, pois não há uma separação nítida entre os dados válidos e inválidos no conjunto de treinamento. Este experimento mostra que tal tarefa de classificação não é possível de ser realizada utilizando a estrutura composta por apenas uma RNA.

5.3 – Experimento 3 – Utilização de Máquina de Comitê para Representar o Usuário

Como os resultados do experimento 2 foram extremamente ruins, recorreu-se ao conceito de máquinas de comitê para tentar solucionar o problema, pois como verificado no experimento 2 a tarefa de reconhecer os padrões de um usuário através de sua dinâmica da digitação é bastante complexa e não pode ser realizada por apenas um especialista (RNA).

Recorrendo aos resultados do experimento 1 pode-se constatar que a classificação dos padrões de digitação entre 2 únicos usuários foi bastante eficiente. Estimulado por estes resultados foi proposta uma máquina de comitê, conforme descrição do Capítulo 4, para resolver o problema do reconhecimento dos padrões de digitação dos usuários através da análise dos dados dos usuários combinados 2 a 2. Para melhor visualização da metodologia empregada, as Figuras 4.2 (página 42) e 4.3 (página 43) podem ser consultadas.

A análise dos dados expressa pela Figura 5.2 mostra que para praticamente todos os dígrafos existem 2 ou mais usuários que apresentam tempos semelhantes. Isto poderia prejudicar a classificação dos usuários, entretanto com a utilização dos limiares propostos para a metodologia de máquinas de comitê, ou seja, limiar de porcentagem de dígrafos classificados corretamente pela RNA e limiar do número de RNAs que classificam o dado como válido, espera-se que a máquina de comitê consiga classificar corretamente os dados de cada usuário.

Este experimento pode ser subdivido em 3 etapas: análise dos usuários através dos conjuntos de treinamento dos dados da frase fixa, do texto fixo e do texto fixo junto com o texto livre.

Cada uma destas etapas é detalhada nos tópicos seguintes.

5.3.1 – Etapa 1 - Análise sobre a Frase Fixa

Nesta etapa, para cada usuário foram treinadas 13 RNAs. O conjunto de treinamento de cada RNA é composto pelo conjunto de treinamento do usuário válido e o conjunto de treinamento de um outro usuário do grupo 1. Portanto a máquina de comitê que representa

o usuário, por exemplo usuário 1, será composta de uma RNA cujos dados do conjunto de treinamento é composto pelo conjunto de treinamento do usuário 1 como dados válidos e o conjunto de treinamento do usuário 2 como dados inválidos, uma RNA com dados do conjunto de treinamento do usuário 1 como dados válidos e conjunto de treinamento do usuário 3 como dados inválidos e assim sucessivamente até a 13ª RNA, que será composta pelos dados do usuário 1 e usuário 14. A Figura 4.3 ilustra este treinamento.

A saída de todas as RNAs são combinadas de modo que os resultados serão avaliados como válidos ou não, de acordo com os limiares propostos para a estrutura de máquinas de comitê.

5.3.1.1 – Resultados do Experimento 3 etapa 1

O conjunto de treinamento de cada RNA tem tamanho variável (da ordem de 1000 exemplos), pois as amostras de cada usuário podem conter tamanhos distintos. Esta diferença no tamanho dos conjuntos de treinamento deve-se principalmente à ocorrência de erros e a possibilidade de que alguns usuários digitaram a acentuação corretamente e outros não.

Após o processo de treinamento, cada uma das amostras de teste de cada usuário válido foi apresentada à sua máquina de comitê treinada. Os resultados das máquinas de comitê foram importados para o Excel para que uma análise sobre as diversas combinações de limiares pudesse ser testada. Esta verificação foi realizada para avaliar a taxa de falsa rejeição (FRR) do sistema. A Tabela 5.2 nos mostra a FRR obtida variando-se os dois limiares propostos: limiar de porcentagem de dígrafos classificados corretamente pela RNA (representado pela letra "*a*" na tabela) e limiar do número de RNAs que classificam o dado como válido (representado pela letra "*b*" na tabela). Neste experimento, 170 amostras de teste válidas foram analisadas.

a \ b	1	2	3	4	5	6	7	8	9	10	11	12	13
0.05	0	0	0	0	0	0	0	0	0	0	0	0	0,065
0.1	0	0	0	0	0	0	0	0	0	0	0	0	0,276
0.15	0	0	0	0	0	0	0	0	0	0	0	0,018	0,412
0.2	0	0	0	0	0	0	0	0	0	0	0	0,071	0,671
0.25	0	0	0	0	0	0	0	0	0	0	0,012	0,212	0,782
0.3	0	0	0	0	0	0	0	0	0	0	0,029	0,382	0,876
0.35	0	0	0	0	0	0	0	0	0	0,006	0,106	0,565	0,924
0.4	0	0	0	0	0	0	0	0	0	0,024	0,212	0,706	0,953
0.45	0	0	0	0	0	0	0	0	0,006	0,053	0,382	0,824	0,976
0.5	0	0	0	0	0	0	0	0	0,018	0,112	0,506	0,865	0,994
0.55	0	0	0	0	0	0	0	0	0,029	0,247	0,671	0,912	1
0.6	0	0	0	0	0	0	0	0,012	0,129	0,418	0,782	0,947	1
0.65	0	0	0	0	0	0	0	0,041	0,229	0,571	0,847	0,971	1
0.7	0	0	0	0	0	0	0,006	0,129	0,365	0,729	0,929	0,988	1
0.75	0	0	0	0	0	0	0,071	0,265	0,518	0,829	0,953	1	1
0.8	0	0	0	0	0,006	0,059	0,235	0,447	0,741	0,929	0,988	1	1
0.85	0	0	0,006	0,018	0,076	0,212	0,459	0,682	0,876	0,994	1	1	1
0.9	0	0,012	0,024	0,071	0,206	0,376	0,629	0,818	0,953	1	1	1	1
0.95	0,006	0,059	0,129	0,312	0,529	0,729	0,894	0,965	0,988	1	1	1	1

Tabela 5.2 - FRR obtido na etapa 1 do experimento 3

Pode-se verificar através da Tabela 5.2 que a FRR aumenta conforme os valores dos limiares aumentam e muitas das combinações de limiares fornecem a perfeita classificação do usuário. Quanto maior a rigidez imposta pelos limiares, maior será a quantidade de amostras válidas rejeitadas pelo sistema, sendo que a utilização de valores altos para os 2 limiares faz com que o sistema rejeite todas as amostras de usuários válidos.

Para avaliar a taxa de falsa aceitação (FAR) foram criadas duas tabelas, uma que é a análise de autenticação em relação às amostras de testes dos 13 usuários do grupo 1, que têm seus conjuntos de treinamento envolvidos no treinamento de cada RNA da máquina de comitê e uma segunda tabela que contém a análise das amostras de testes coletadas junto aos usuários do grupo 2.

A Tabela 5.3 mostra a FAR referente às 2210 amostras de teste inválidas dos usuários do grupo 1 testadas.

a \ b	1	2	3	4	5	6	7	8	9	10	11	12	13
0.05	1	1	1	1	1	1	1	1	0,995	0,98	0,923	0,714	0,3
0.1	1	1	1	1	1	1	1	0,991	0,976	0,907	0,719	0,348	0,063
0.15	1	1	1	1	1	0,999	0,997	0,981	0,943	0,814	0,538	0,178	0,024
0.2	1	1	1	1	0,999	0,994	0,983	0,944	0,862	0,636	0,3	0,055	0,006
0.25	1	1	1	1	0,997	0,982	0,962	0,903	0,762	0,481	0,17	0,03	0,001
0.3	1	1	1	0,999	0,988	0,959	0,921	0,812	0,587	0,28	0,073	0,01	0
0.35	1	1	1	0,991	0,968	0,924	0,846	0,68	0,4	0,14	0,031	0,002	0
0.4	1	1	1	0,979	0,942	0,877	0,762	0,547	0,266	0,072	0,014	0,001	0
0.45	1	1	0,992	0,955	0,898	0,793	0,621	0,37	0,139	0,031	0,006	0	0
0.5	1	1	0,986	0,93	0,856	0,71	0,519	0,263	0,089	0,019	0,005	0	0
0.55	1	0,998	0,961	0,885	0,76	0,562	0,348	0,143	0,04	0,008	0,001	0	0
0.6	1	0,99	0,929	0,814	0,65	0,433	0,21	0,064	0,019	0,003	0	0	0
0.65	1	0,976	0,89	0,738	0,534	0,315	0,117	0,038	0,012	0,001	0	0	0
0.7	0,995	0,953	0,818	0,621	0,393	0,177	0,057	0,016	0,004	0	0	0	0
0.75	0,984	0,918	0,739	0,507	0,283	0,108	0,029	0,007	0	0	0	0	0
0.8	0,959	0,843	0,591	0,325	0,118	0,034	0,005	0,001	0	0	0	0	0
0.85	0,92	0,699	0,375	0,155	0,039	0,005	0	0	0	0	0	0	0
0.9	0,875	0,538	0,206	0,06	0,009	0	0	0	0	0	0	0	0
0.95	0,654	0,195	0,037	0,007	0	0	0	0	0	0	0	0	0

Tabela 5.3 - FAR de usuários do grupo 1 obtido na etapa 1 do experimento 3

É possível constatar da Tabela 5.3 um comportamento inverso ao obtido na análise da Tabela 5.2. Quando a taxa analisada é a FAR, quanto mais altos os valores dos limiares, mais difícil é um usuário inválido se passar como um usuário autêntico, sendo que em muitas combinações destes limiares todas as amostras são corretamente rejeitadas, entretanto um relaxamento dos valores dos limiares possibilita que usuários intrusos sejam aceitos pelo sistema. Como pode ser visto na Tabela 5.3 para muitas combinações de limiares todas as amostras de usuários intrusos foram aceitas como sendo de um usuário válido.

A Tabela 5.4 mostra a FAR referente as 490 amostras de teste inválidas dos usuários do grupo 2 testadas.

a \ b	1	2	3	4	5	6	7	8	9	10	11	12	13
0.05	1	1	1	1	1	1	1	1	1	0,992	0,969	0,814	0,398
0.1	1	1	1	1	1	1	1	0,998	0,988	0,943	0,8	0,476	0,104
0.15	1	1	1	1	1	1	0,998	0,984	0,957	0,865	0,633	0,286	0,022
0.2	1	1	1	1	1	0,998	0,988	0,971	0,9	0,7	0,433	0,11	0
0.25	1	1	1	1	1	0,988	0,982	0,931	0,822	0,569	0,265	0,063	0
0.3	1	1	1	1	0,998	0,978	0,933	0,853	0,684	0,384	0,122	0,002	0
0.35	1	1	1	1	0,986	0,939	0,863	0,737	0,498	0,212	0,053	0	0
0.4	1	1	1	0,994	0,973	0,896	0,81	0,639	0,355	0,131	0,02	0	0
0.45	1	1	0,998	0,984	0,922	0,839	0,71	0,48	0,214	0,055	0	0	0
0.5	1	1	0,998	0,963	0,884	0,792	0,612	0,376	0,153	0,022	0	0	0
0.55	1	1	0,99	0,908	0,82	0,673	0,459	0,202	0,065	0,002	0	0	0
0.6	1	0,998	0,951	0,849	0,71	0,496	0,29	0,09	0,027	0	0	0	0
0.65	1	0,99	0,9	0,778	0,604	0,376	0,159	0,039	0,006	0	0	0	0
0.7	1	0,955	0,827	0,669	0,461	0,243	0,071	0,01	0	0	0	0	0
0.75	0,998	0,914	0,769	0,567	0,314	0,137	0,039	0,006	0	0	0	0	0
0.8	0,978	0,849	0,618	0,347	0,155	0,045	0,008	0	0	0	0	0	0
0.85	0,927	0,714	0,382	0,155	0,043	0,004	0	0	0	0	0	0	0
0.9	0,88	0,543	0,212	0,063	0,012	0	0	0	0	0	0	0	0
0.95	0,647	0,22	0,027	0,008	0	0	0	0	0	0	0	0	0

Tabela 5.4 - FAR de usuários do grupo 2 obtido na etapa 1 do experimento 3

A análise da Tabela 5.4 é a mesma verificada na Tabela 5.3.

Como visto a FAR é inversamente proporcional a FRR e cresce de acordo com a diminuição dos limiares, portanto, para se obter uma boa eficácia do classificador, faz-se necessário escolher valores de limiares que possam possibilitar um resultado aceitável para as duas taxas de eficácia do sistema. Isto ocorre porque se o sistema utilizar valores altos para ambos os limiares, todos os intrusos serão rejeitados, no entanto os usuários válidos também serão. Se o sistema utilizar valores baixos para os limiares, nenhum usuário válido será rejeitado pelo sistema, mas usuários intrusos também serão aceitos pelo mesmo.

Como na maioria dos sistemas a FAR é mais crítica, pois a menor taxa de falsa aceitação é desejada para que intrusos não ganhem direito de acesso, foi criada uma tabela (Tabela 5.5) de taxa de proporção de erros (TPE). Esta taxa de proporção de erros é calculada pela média das 3 medidas de eficácia (2 FAR e 1 FRR) para cada par de limiare. Deste modo, tem-se que a FAR terá um peso maior na obtenção da tabela de taxas de proporção de erros enquanto a FRR terá peso 1. Os valores da FRR e FAR utilizados para o cálculo da TPE são os expressos nas Tabelas 5.2, 5.3 e 5.4. A fórmula (I) representa o cálculo da TPE.

$$(I)\quad TPE = \frac{FAR_{\text{Usuários grupo 1}} + FAR_{\text{Usuários grupo 2}} + FRR_{\text{Usuários grupo 1}}}{3}$$

O cálculo desta taxa de proporção de erros será utilizado para encontrar quais os melhores valores de configuração dos limiares para o sistema, ou seja, para quais valores de limiares o sistema fornece os melhores resultados.

a \ b	1	2	3	4	5	6	7	8	9	10	11	12	13
0.05	0,667	0,667	0,667	0,667	0,667	0,667	0,667	0,667	0,665	0,657	0,631	0,509	0,254
0.1	0,667	0,667	0,667	0,667	0,667	0,667	0,667	0,663	0,654	0,617	0,506	0,275	0,148
0.15	0,667	0,667	0,667	0,667	0,667	0,666	0,665	0,655	0,633	0,56	0,39	0,16	0,153
0.2	0,667	0,667	0,667	0,667	0,666	0,664	0,657	0,638	0,587	0,445	0,244	0,079	0,225
0.25	0,667	0,667	0,667	0,667	0,666	0,657	0,648	0,611	0,528	0,35	0,149	0,102	0,261
0.3	0,667	0,667	0,667	0,666	0,662	0,646	0,618	0,555	0,424	0,221	0,075	0,132	0,292
0.35	0,667	0,667	0,667	0,664	0,651	0,621	0,57	0,472	0,299	0,119	0,063	0,189	0,308
0.4	0,667	0,667	0,667	0,658	0,639	0,591	0,524	0,395	0,207	0,076	0,082	0,236	0,318
0.45	0,667	0,667	0,663	0,646	0,607	0,544	0,444	0,283	0,12	0,046	0,13	0,275	0,325
0.5	0,667	0,667	0,661	0,631	0,58	0,501	0,377	0,213	0,087	0,051	0,17	0,288	0,331
0.55	0,667	0,666	0,65	0,598	0,527	0,412	0,269	0,115	0,045	0,086	0,224	0,304	0,333
0.6	0,667	0,663	0,627	0,554	0,453	0,31	0,166	0,055	0,058	0,14	0,261	0,316	0,333
0.65	0,667	0,655	0,597	0,505	0,379	0,23	0,092	**0,039**	0,082	0,191	0,282	0,324	0,333
0.7	0,665	0,636	0,548	0,43	0,285	0,14	0,045	0,052	0,123	0,243	0,31	0,329	0,333
0.75	0,661	0,611	0,503	0,358	0,199	0,082	0,046	0,093	0,173	0,276	0,318	0,333	0,333
0.8	0,646	0,564	0,403	0,224	0,093	0,046	0,083	0,149	0,247	0,31	0,329	0,333	0,333
0.85	0,615	0,471	0,254	0,109	0,053	0,073	0,153	0,227	0,292	0,331	0,333	0,333	0,333
0.9	0,585	0,364	0,147	0,065	0,076	0,125	0,21	0,273	0,318	0,333	0,333	0,333	0,333
0.95	0,436	0,158	0,064	0,109	0,176	0,243	0,298	0,322	0,329	0,333	0,333	0,333	0,333

Tabela 5.5 - Taxas de proporção de erros da etapa 1, experimento 3

Da tabela de taxas de proporção de erros (Tabela 5.5) tem-se que, se os limiares utilizados na verificação da autenticidade dos dados testados forem configurados para aceitar um usuário como válido quando 8 entre as 13 RNA classificarem o mesmo como válido e com classificação correta de 65% das latências dos dígrafos componentes da informação alvo, a taxa de proporção de erros terá o seu menor valor, ou seja, 3,9%. Referente a estes limiares o sistema apresenta uma FRR de 4,11% (7 erros de 170 amostras) e uma FAR de 3,77% (102 erros de 2700 amostras, sendo 83 erros referentes a amostras dos usuários do grupo 1 e 19 erros referentes a amostras de usuários do grupo 2).

Pode-se ainda verificar da tabela de taxas de proporção de erros (Tabela 5.5) que os melhores resultados de classificação ocorrem quando há uma utilização de valores intermediários para os limiares ou ainda a utilização de um limiar com valor alto e outro com valor baixo, portanto o sistema biométrico terá sua maior eficácia quando há certa "troca" entre os limiares para rejeitar impostores e aceitar todos os usuários válidos. Esta "troca" se faz necessária pela característica inversamente proporcional entre as duas medidas de eficácia, a FRR e a FAR.

5.3.2 – Etapa 2 - Análise sobre o Texto Fixo

Esta etapa segue as mesmas características da etapa 1, sendo que a única diferença é que os conjuntos de treinamento e testes analisados nesta etapa do experimento 3 são os referentes às informações coletadas do texto fixo.

5.3.2.1 – Resultados do Experimento 3 etapa 2

O conjunto de treinamento de cada RNA nesta etapa do experimento 3 também apresenta tamanho variável pelo mesmo motivo citado na etapa 1, no entanto, nesta etapa os conjuntos de treinamentos são muito maiores dos que os analisados na etapa 1, sendo que o número de exemplos é da ordem de 14000.

Depois de treinadas as RNAs, os mesmos procedimentos da etapa 1 foram adotados, sendo que a Tabela 5.6 mostra os valores da taxa de falsa rejeição (FRR) obtidos nesta etapa do experimento 3 referente a 170 amostras válidas testadas.

a \ b	1	2	3	4	5	6	7	8	9	10	11	12	13
0.05	0	0	0	0	0	0	0	0	0	0	0	0	0,229
0.1	0	0	0	0	0	0	0	0	0	0	0	0,041	0,747
0.15	0	0	0	0	0	0	0	0	0	0	0	0,229	0,924
0.2	0	0	0	0	0	0	0	0	0	0	0	0,435	0,971
0.25	0	0	0	0	0	0	0	0	0	0	0,059	0,694	1
0.3	0	0	0	0	0	0	0	0	0	0	0,2	0,894	1
0.35	0	0	0	0	0	0	0	0	0	0	0,412	0,935	1
0.4	0	0	0	0	0	0	0	0	0	0,018	0,676	0,982	1
0.45	0	0	0	0	0	0	0	0	0	0,124	0,871	1	1
0.5	0	0	0	0	0	0	0	0	0	0,353	0,965	1	1
0.55	0	0	0	0	0	0	0	0	0,006	0,635	0,988	1	1
0.6	0	0	0	0	0	0	0	0	0,165	0,876	1	1	1
0.65	0	0	0	0	0	0	0	0,024	0,418	0,976	1	1	1
0.7	0	0	0	0	0	0	0,006	0,088	0,729	1	1	1	1
0.75	0	0	0	0	0	0,006	0,053	0,382	0,924	1	1	1	1
0.8	0	0	0	0	0	0,041	0,176	0,794	1	1	1	1	1
0.85	0	0	0	0	0,029	0,159	0,629	0,976	1	1	1	1	1
0.9	0	0	0,024	0,053	0,2	0,594	0,976	1	1	1	1	1	1
0.95	0	0,006	0,135	0,353	0,788	0,994	1	1	1	1	1	1	1

Tabela 5.6 - FRR obtido na etapa 2 do experimento 3

Os resultados mostrados na Tabela 5.6 seguem as mesmas características obtidas na etapa 1 deste experimento, o que se percebe é que neste experimento houve um pequeno estreitamento da faixa de resultados intermediários, isto é, resultados onde as amostras não são sempre consideradas como válidas e nem como inválidas.

A Tabela 5.7 mostra a FAR referente às amostras de teste dos usuários do grupo 1, foram testadas 2210 amostras inválidas.

a \ b	1	2	3	4	5	6	7	8	9	10	11	12	13
0.05	1	1	1	1	1	1	1	1	0,996	0,985	0,923	0,476	0,022
0.1	1	1	1	1	1	1	0,998	0,99	0,972	0,92	0,648	0,076	0
0.15	1	1	1	1	1	0,996	0,987	0,967	0,923	0,785	0,237	0,02	0
0.2	1	1	1	1	0,996	0,984	0,964	0,928	0,853	0,572	0,075	0	0
0.25	1	1	1	0,999	0,988	0,966	0,935	0,888	0,724	0,289	0,035	0	0
0.3	1	1	1	0,992	0,972	0,94	0,895	0,813	0,565	0,119	0,01	0	0
0.35	1	1	1	0,984	0,952	0,908	0,852	0,691	0,37	0,051	0	0	0
0.4	1	1	0,998	0,965	0,925	0,876	0,772	0,547	0,2	0,021	0	0	0
0.45	1	1	0,988	0,947	0,892	0,822	0,663	0,391	0,096	0,007	0	0	0
0.5	1	1	0,976	0,915	0,862	0,746	0,532	0,249	0,039	0,002	0	0	0
0.55	1	1	0,953	0,886	0,803	0,625	0,405	0,135	0,017	0	0	0	0
0.6	1	0,995	0,926	0,848	0,724	0,51	0,292	0,054	0,005	0	0	0	0
0.65	1	0,983	0,9	0,784	0,6	0,408	0,16	0,022	0,002	0	0	0	0
0.7	1	0,96	0,855	0,697	0,484	0,292	0,071	0,005	0	0	0	0	0
0.75	0,998	0,93	0,791	0,575	0,385	0,175	0,013	0,001	0	0	0	0	0
0.8	0,981	0,9	0,67	0,438	0,244	0,07	0,003	0	0	0	0	0	0
0.85	0,962	0,795	0,517	0,28	0,129	0,009	0	0	0	0	0	0	0
0.9	0,925	0,605	0,348	0,152	0,026	0	0	0	0	0	0	0	0
0.95	0,755	0,349	0,163	0,037	0	0	0	0	0	0	0	0	0

Tabela 5.7 - FAR de usuários do grupo 1 obtido na etapa 2 do experimento 3

Novamente pode-se constatar que os resultados nesta etapa do experimento, visualizados na Tabela 5.7, são muito parecidos com os resultados da etapa anterior demonstrados na Tabela 5.3. Uma pequena melhora na quantidade de limiares que rejeitam todas as amostras inválidas pode ser observada nesta etapa.

A tabela de FAR dos usuários do grupo 2 (Tabela 5.8) referente a 420 amostras inválidas testadas pode ser vista a seguir.

a \ b	1	2	3	4	5	6	7	8	9	10	11	12	13
0.05	1	1	1	1	1	1	1	1	1	0,983	0,967	0,602	0,045
0.1	1	1	1	1	1	1	1	1	0,969	0,952	0,724	0,093	0
0.15	1	1	1	1	1	1	0,995	0,971	0,948	0,843	0,326	0,043	0
0.2	1	1	1	1	1	0,99	0,974	0,948	0,881	0,631	0,105	0,01	0
0.25	1	1	1	1	0,998	0,976	0,95	0,912	0,774	0,371	0,064	0	0
0.3	1	1	1	1	0,983	0,96	0,926	0,84	0,6	0,16	0,024	0	0
0.35	1	1	1	0,998	0,964	0,945	0,871	0,731	0,448	0,093	0	0	0
0.4	1	1	1	0,974	0,955	0,9	0,802	0,576	0,267	0,038	0	0	0
0.45	1	1	0,995	0,96	0,936	0,826	0,698	0,462	0,155	0,012	0	0	0
0.5	1	1	0,983	0,948	0,883	0,76	0,569	0,345	0,071	0,005	0	0	0
0.55	1	1	0,969	0,926	0,812	0,657	0,445	0,224	0,017	0	0	0	0
0.6	1	1	0,95	0,864	0,738	0,548	0,367	0,1	0,007	0	0	0	0
0.65	1	0,988	0,921	0,802	0,667	0,45	0,233	0,017	0,005	0	0	0	0
0.7	1	0,979	0,883	0,721	0,507	0,338	0,11	0,01	0	0	0	0	0
0.75	1	0,938	0,807	0,626	0,412	0,21	0,043	0	0	0	0	0	0
0.8	0,993	0,905	0,679	0,44	0,279	0,131	0	0	0	0	0	0	0
0.85	0,976	0,84	0,512	0,312	0,167	0,038	0	0	0	0	0	0	0
0.9	0,91	0,617	0,364	0,181	0,095	0	0	0	0	0	0	0	0
0.95	0,757	0,371	0,193	0,081	0	0	0	0	0	0	0	0	0

Tabela 5.8 - FAR de usuários do grupo 2 obtido na etapa 2 do experimento 3

As três tabelas (Tabelas 5.6, 5.7 e 5.8) que demonstram os resultados desta etapa do experimento também comprovam a propriedade inversa das taxas de eficácia do sistema.

Para verificar quais os limiares que permitem a melhor eficácia do sistema, novamente foi calculada a tabela de taxas de proporção de erros para este experimento.

a \ b	1	2	3	4	5	6	7	8	9	10	11	12	13
0.05	0,667	0,667	0,667	0,667	0,667	0,667	0,667	0,667	0,665	0,656	0,63	0,36	0,099
0.1	0,667	0,667	0,667	0,667	0,667	0,667	0,666	0,663	0,647	0,624	0,457	0,07	0,249
0.15	0,667	0,667	0,667	0,667	0,667	0,665	0,661	0,646	0,624	0,543	0,188	0,097	0,308
0.2	0,667	0,667	0,667	0,667	0,665	0,658	0,646	0,625	0,578	0,401	0,06	0,149	0,324
0.25	0,667	0,667	0,667	0,666	0,662	0,647	0,628	0,6	0,499	0,22	0,053	0,232	0,333
0.3	0,667	0,667	0,667	0,664	0,652	0,633	0,607	0,551	0,388	0,093	0,078	0,298	0,333
0.35	0,667	0,667	0,667	0,66	0,639	0,618	0,575	0,474	0,273	0,048	0,138	0,312	0,333
0.4	0,667	0,667	0,666	0,646	0,627	0,592	0,525	0,374	0,156	0,026	0,225	0,327	0,333
0.45	0,667	0,667	0,661	0,635	0,609	0,549	0,454	0,284	0,084	0,047	0,29	0,333	0,333
0.5	0,667	0,667	0,653	0,621	0,582	0,502	0,367	0,198	0,037	0,12	0,322	0,333	0,333
0.55	0,667	0,667	0,641	0,604	0,538	0,427	0,283	0,12	**0,013**	0,212	0,329	0,333	0,333
0.6	0,667	0,665	0,625	0,571	0,488	0,353	0,22	0,051	0,059	0,292	0,333	0,333	0,333
0.65	0,667	0,657	0,607	0,529	0,422	0,286	0,131	**0,021**	0,141	0,325	0,333	0,333	0,333
0.7	0,667	0,646	0,58	0,473	0,33	0,21	0,062	0,034	0,243	0,333	0,333	0,333	0,333
0.75	0,666	0,623	0,533	0,4	0,266	0,13	0,036	0,128	0,308	0,333	0,333	0,333	0,333
0.8	0,658	0,602	0,449	0,293	0,174	0,081	0,06	0,265	0,333	0,333	0,333	0,333	0,333
0.85	0,646	0,545	0,343	0,197	0,108	0,069	0,21	0,325	0,333	0,333	0,333	0,333	0,333
0.9	0,611	0,407	0,245	0,129	0,107	0,198	0,325	0,333	0,333	0,333	0,333	0,333	0,333
0.95	0,504	0,242	0,164	0,157	0,263	0,331	0,333	0,333	0,333	0,333	0,333	0,333	0,333

Tabela 5.9 - Taxas de proporção de erros da etapa 2, experimento 3

Observando a tabela de taxas de proporção de erros (Tabela 5.9) desta etapa do experimento, pode-se analisar dois resultados importantes. O primeiro é referente a utilização de um limiar de 9 entre as 13 RNAs para classificar um usuário como válido se 55% ou mais das latências dos dígrafos componentes da informação alvo forem classificados como correto. Para a utilização destes valores de limiares tem-se uma taxa de proporção de erros de 1,3%. Calculando as taxas de eficácia para estes limiares tem-se uma FRR de 0,58% (1 erro em 170 amostras) e uma FAR de 1,67% (44 erros de 2630 amostras, sendo 37 erros referentes a amostras dos usuários do grupo 1 e 7 erros referentes a amostras de usuários do grupo 2).

A segunda observação importante é referente aos limiares analisados na etapa 1 (8 de 10 RNA e 65% das latências), nesta segunda etapa do treinamento, a taxa de proporção de erros caiu de 3,9% para 2,1%, sendo que para esta etapa do experimento, estes limiares resultaram em uma FRR de 2,35 % (4 erros em 170 amostras) e uma FAR de 2,09% (55 erros de 2630 amostras, sendo 48 erros referentes a amostras dos usuários do grupo 1 e 7 erros referentes a amostras de usuários do grupo 2).

Esta melhora na classificação dos dados se deve principalmente à maior quantidade dos dados analisados que possibilita uma maior ocorrência dos dígrafos e conseqüentemente o conjunto de treinamento é mais consistente.

5.3.3 – Etapa 3 - Análise sobre o Texto Fixo e Texto Livre

Esta etapa segue as mesmas características das etapas anteriores, no entanto aqui serão utilizados como conjunto de treinamento das RNA os dados referentes às coletas do texto fixo e do texto livre. Para verificação da eficácia desta etapa, serão analisados os conjuntos de testes do texto fixo. O objetivo desta etapa do experimento 3 é verificar se digitando textos de maneira independente, ou seja, livre da necessidade de copiar uma informação pré-determinada, o padrão do usuário continua constante.

5.3.3.1 – Resultados do Experimento 3 etapa 3

O conjunto de treinamento de cada RNA apresenta tamanho variável pelos mesmos motivos citados nas etapas anteriores e o número de exemplos é da ordem de 19000.

Por se tratar da mesma análise já realizada nas etapas 1 e 2, nesta etapa será apresentada apenas a tabela de taxas de proporção de erros, como pode ser vista na Tabela 5.10.

a \ b	1	2	3	4	5	6	7	8	9	10	11	12	13
0.05	0,667	0,667	0,667	0,667	0,667	0,667	0,667	0,667	0,665	0,649	0,595	0,269	0,236
0.1	0,667	0,667	0,667	0,667	0,667	0,667	0,666	0,662	0,65	0,602	0,316	0,159	0,264
0.15	0,667	0,667	0,667	0,667	0,667	0,667	0,66	0,652	0,619	0,433	0,211	0,195	0,285
0.2	0,667	0,667	0,667	0,667	0,667	0,661	0,652	0,634	0,541	0,26	0,151	0,228	0,29
0.25	0,667	0,667	0,667	0,667	0,663	0,654	0,641	0,589	0,414	0,169	0,15	0,269	0,32
0.3	0,667	0,667	0,667	0,667	0,657	0,643	0,614	0,538	0,289	0,127	0,166	0,282	0,333
0.35	0,667	0,667	0,667	0,661	0,65	0,624	0,584	0,427	0,171	0,131	0,227	0,286	0,333
0.4	0,667	0,667	0,667	0,655	0,638	0,601	0,522	0,329	0,113	0,135	0,249	0,304	0,333
0.45	0,667	0,667	0,664	0,647	0,621	0,567	0,444	0,223	0,089	0,164	0,266	0,324	0,333
0.5	0,667	0,667	0,655	0,635	0,599	0,522	0,356	0,118	0,119	0,226	0,284	0,329	0,333
0.55	0,667	0,667	0,647	0,618	0,561	0,452	0,244	0,079	0,131	0,262	0,294	0,333	0,333
0.6	0,667	0,667	0,635	0,591	0,515	0,366	0,157	0,065	0,166	0,267	0,322	0,333	0,333
0.65	0,667	0,661	0,614	0,541	0,451	0,262	0,084	**0,1**	0,223	0,291	0,331	0,333	0,333
0.7	0,667	0,646	0,582	0,509	0,357	0,161	0,049	0,147	0,258	0,314	0,333	0,333	0,333
0.75	0,667	0,629	0,546	0,455	0,252	0,089	0,073	0,205	0,294	0,331	0,333	0,333	0,333
0.8	0,666	0,596	0,507	0,351	0,144	**0,033**	0,155	0,265	0,318	0,333	0,333	0,333	0,333
0.85	0,651	0,561	0,44	0,232	0,07	0,089	0,226	0,316	0,331	0,333	0,333	0,333	0,333
0.9	0,61	0,492	0,316	0,123	0,078	0,226	0,312	0,329	0,333	0,333	0,333	0,333	0,333
0.95	0,541	0,352	0,15	0,124	0,267	0,324	0,333	0,333	0,333	0,333	0,333	0,333	0,333

Tabela 5.10 - Taxas de proporção de erros da etapa 3, experimento 3

Da Tabela 5.10, pode-se verificar que os melhores resultados são obtidos quando 6 ou mais RNAs classificam o usuário como válido em 80% das latências entre os dígrafos apresentados. Para estes limiares o sistema apresenta uma FRR de 1,76% (3 erros em 170 amostras) e uma FAR de 3,23% (85 erros de 2630 amostras, sendo 63 erros referentes à amostras dos usuários do grupo 1 e 22 erros referentes a amostras de usuários do grupo 2).

Outra verificação importante é que a taxa de proporção de erros para o limiar de 8 ou mais RNA classificar ao menos 65% das latências corretamente subiu nesta etapa do experimento para 10 %. Uma explicação que pode ser dada a este fato é que muitas vezes as pessoas, quando estavam digitando a informação livre, ficavam indecisas sobre o que escrever. Esta indecisão fez com que a quantidade de interrupções na digitação livre fosse muito maior do que na digitação de um texto estipulado previamente.

5.4 – Experimento 4 – Utilização de Limiares Individuais para cada Usuário

O quarto e último experimento realizado neste trabalho utiliza os resultados do experimento 3, mas ao invés de utilizar um limiar fixo para todos os usuários, neste experimento é proposta a utilização de limiares diferentes para cada usuário. Este experimento, como o anterior, foi realizado sobre as informações alvo da frase fixa, texto fixo e texto fixo junto com texto livre.

A apresentação dos resultados através de tabelas como as mostradas no experimento 3 resultaria numa grande quantidade de tabelas, dificultando a visualização dos resultados obtidos, portanto os resultados deste experimento são mostrados através de uma tabela que indica qual a FRR e FAR obtidas para cada usuário, considerando os melhores limiares de classificação do mesmo.

O número de amostras de testes válidas e inválidas são os mesmo utilizados no experimento 3.

A análise da Tabela 5.11, que mostra os resultados obtidos quando o classificador é utilizado para classificar amostras de testes da informação alvo da frase fixa, permite verificar que 6 usuários foram perfeitamente classificados através da utilização de limiares diferentes para cada usuário. Apenas 1 único usuário que era válido foi classificado incorretamente pelo sistema 2 vezes em 12 tentativas o que fez com que a FRR deste usuário fosse alta. Em relação a FAR, apenas os 6 usuários que foram perfeitamente classificados não puderam ser confundidos por outros usuários. Dos demais houve falsa aceitação pelo sistema, entretanto nenhum usuário apresentou FAR muito elevada. Como resultados totais, obteve-se um FRR de 1,18% (2 erros em 170 amostras) e uma FAR de 1,04% (28 erros de 2700 amostras, sendo 20 erros referentes a amostras dos usuários do grupo 1 e 8 erros referentes a amostras de usuários do grupo 2). Os resultados obtidos neste experimento demonstram uma melhora considerável se comparado ao experimento com limiar único para todos os usuários onde uma FRR de 4,11% e uma FAR de 3,77% foram obtidas.

Usuário	FRR	FAR
usuário 1	0 %	0 %
usuário 2	0 %	1,55 %
usuário 3	0 %	0 %
usuário 4	0 %	0 %
usuário 5	0 %	0 %
usuário 6	0 %	2,07 %
usuário 7	16,66 %	0,52 %
usuário 8	0 %	2,07 %
usuário 9	0 %	0 %
usuário 10	0 %	1,55 %
usuário 11	0 %	1,04 %
usuário 12	0 %	0 %
usuário 13	0 %	2,07 %
usuário 14	0 %	3,63 %
Total	1,18 %	1,04 %

Tabela 5.11 - Resultados do experimento 4 para frase fixa

Quando a informação alvo utilizada pelo classificador é o texto fixo, há uma melhora muito mais significativa no sistema.

Nesta etapa do experimento 4 pode-se verificar na Tabela 5.12, que mostra os resultados deste experimento, que 13 usuários foram perfeitamente classificados e para apenas 1 único usuário (usuário 14) o sistema possibilitou que outros usuários pudessem se passar por ele em 4 vezes de 188 tentativas de intrusão, o que significa uma FAR de 2,13%. Os resultados totais obtidos neste experimento mostram um excelente desempenho, sendo que o experimento apresentou FRR de 0% (0 erros em 170 amostras) e FAR de 0,15% (4 erros de 2630 amostras, sendo 3 erros referentes a amostras dos usuários do grupo 1 e 1 erro referente a amostras de usuários do grupo 2). Comparando estes resultados com os obtidos no experimento com limiar fixo para todo o sistema, tem-se novamente uma

melhora na classificação considerando que o experimento com limiar único apresentou uma FRR de 0,58% e uma FAR de 1,67%.

Usuário	FRR	FAR
usuário 1	0 %	0 %
usuário 2	0 %	0 %
usuário 3	0 %	0 %
usuário 4	0 %	0 %
usuário 5	0 %	0 %
usuário 6	0 %	0 %
usuário 7	0 %	0 %
usuário 8	0 %	0 %
usuário 9	0 %	0 %
usuário 10	0 %	0 %
usuário 11	0 %	0 %
usuário 12	0 %	0 %
usuário 13	0 %	0 %
usuário 14	0 %	2,13 %
Total	0 %	0,15 %

Tabela 5.12 - Resultados do experimento 4 para texto fixo

Por fim tem-se a Tabela 5.13 com os resultados do experimento que utiliza as informações do texto fixo e do texto livre.

Para a última etapa do experimento 4, a Tabela 5.13 mostra que os resultados apresentam a perfeita classificação de 12 usuários enquanto que para o usuário 8 e 14 algumas amostras de usuários inválidos foram classificadas como válidas sendo que o número de amostras classificadas incorretamente do usuário 8 foram 4 (e de usuários do grupo 1 e 1 de usuários do grupo 2) e para o usuário 14 foram 3 amostras indevidamente classificadas como válidas (todas de usuários do grupo 1).

Usuário	FRR	FAR
usuário 1	0 %	0 %
usuário 2	0 %	0 %
usuário 3	0 %	0 %
usuário 4	0 %	0 %
usuário 5	0 %	0 %
usuário 6	0 %	0 %
usuário 7	0 %	0 %
usuário 8	0 %	2,13 %
usuário 9	0 %	0 %
usuário 10	0 %	0 %
usuário 11	0 %	0 %
usuário 12	0 %	0 %
usuário 13	0 %	0 %
usuário 14	0 %	1,6 %
Total	0 %	0,27 %

Tabela 5.13 - Resultados do experimento 4 para texto fixo e texto livre

Novamente houve uma melhora nos resultados com a utilização de limiares distintos para cada usuário. Desta vez o sistema apresentou uma FRR de 0% (0 erros em 170 amostras) e uma FAR de 0,27% (7 erros de 2630 amostras, sendo 6 erros referentes a amostras dos usuários do grupo 1 e 1 erro referente a amostras de usuários do grupo 2) contra uma FRR de 1,76% (3 erro em 170 amostras) e uma FAR de 3,23% no sistema com limiar fixo.

5.5 – Resultados dos experimentos

Para facilitar a comparação entre os resultados obtidos em cada um dos experimentos realizados neste trabalho e também auxiliar na comparação destes resultados com o de outras pesquisas sobre o mesmo tema, a Tabela 5.14 foi construída. Esta tabela traz um resumo de todos os resultados obtidos neste trabalho.

Experimento	Informação Alvo	FAR	FRR
2	Todas	-	-
3	Frase Fixa	3,77 %	4,11 %
3	Texto Fixo	1,67 %	0,58 %
3	Texto Fixo e Texto Livre	3,23 %	1,76 %
4	Frase Fixa	1,04 %	1,18 %
4	Texto Fixo	0,15 %	0 %
4	Texto Fixo e Texto Livre	0,27 %	0 %

Tabela 5.14 – Resumo dos resultados obtidos neste trabalho

É importante salientar que o experimento 1 foi realizado apenas com o intuito de verificar qual a melhor configuração de RNA, para a partir desta configuração, realizar os demais experimentos. Por este motivo o experimento 1 não está presente na Tabela 5.14. No experimento 2, a FAR e FRR não estão especificadas pois não foi possível reconhecer o padrão dos usuários utilizando a estrutura de RNA proposta em tal experimento.

5.6 – Conclusão

Neste capítulo foram apresentados os experimentos realizados para verificar a eficácia do sistema biométrico proposto. Duas estruturas de RNA foram testadas sendo que a estrutura que utiliza apenas uma RNA como classificador do sistema biométrico não possibilitou a classificação correta dos usuários devido à ocorrência de dados ambíguos no conjunto de treinamento. Na estrutura que utiliza uma adaptação do conceito de máquinas de comitê o sistema biométrico conseguiu diferenciar os usuários entre usuários autênticos ou intrusos com boa precisão. O sistema biométrico utilizando a estrutura de máquinas de comitê foi testado sob dois pontos de vistas com relação aos limiares utilizados. No primeiro, um par de limiares para toda a aplicação foi definido; num segundo ponto de vista, pares de limiares diferentes para cada usuário foram testados, sendo que a metodologia utilizando limiares distintos para cada usuário apresentou os melhores resultados.

Capítulo 6 - Conclusão

Conclui-se deste trabalho que é possível implementar um método de autenticação seguro, barato e contínuo através da característica comportamental da dinâmica da digitação do usuário, utilizando como classificador as RNAs.

Para realizar os experimentos necessários na verificação da eficácia do sistema proposto, foram implementadas algumas ferramentas que possibilitam a coleta de dados dos usuários, o treinamento das RNAs através de exemplos coletados e a posterior análise e classificação dos dados de teste. A metodologia proposta para solução do problema utiliza duas estruturas diferentes de RNAs. Na primeira estrutura onde apenas uma RNA é utilizada como classificador do usuário, constatou-se que o sistema não apresenta resultados satisfatórios, entretanto utilizando as RNAs dispostas em uma adaptação de máquina de comitê os resultados obtidos permitem classificar o usuário como autêntico ou intruso com uma precisão competitiva com os demais trabalhos realizados na área, como discutido a seguir.

Os experimentos de classificação utilizando a máquina de comitê mostram que utilizando um par de limiares fixo para todos os usuários o sistema apresentou uma FRR = 4,11% e FAR = 3,77% quando as RNAs foram treinadas e testadas através da informação alvo da frase fixa. Quando a informação alvo utilizada foi o texto fixo os resultados foram FRR = 0,58% e FAR = 1,67% e finalmente usando como conjunto de treinamento das RNAs informações do texto fixo e do texto livre os resultados obtidos foram FRR = 1,76% e FAR = 3,23%.

Quando os pares de limiares não são fixos e cada usuário é analisado por um par de limiares específico, o sistema apresenta FRR = 1,18% e FAR = 1,04% para análise da frase fixa, FRR = 0% e FAR = 0,15% para análise do texto fixo e FRR = 0% e FAR = 0,27% quando analisando o texto fixo e o texto livre.

Destes resultados pode-se concluir que o sistema deve utilizar limiares diferentes para cada usuário, pois desta forma pode-se obter uma melhor eficácia do sistema.

Comparar estes resultados com os trabalhos relacionados é uma tarefa bastante complexa, pois os conjuntos de dados assim como todos os usuários pesquisados são

diferentes, portanto uma breve comparação será realizada através da apresentação das taxas de eficácia obtidas pelos trabalhos. Recorrendo a Tabela 2.2, que apresenta o resumo de resultados de 5 trabalhos que realizam a autenticação contínua do usuário, pode-se constatar que as pesquisas [32] e [42] não informam as taxas de eficácia obtidas. No trabalho [30], a única medida de eficácia apresentada é que o sistema classificou corretamente 90,7% dos dados. As pesquisas realizadas por [6] apresentam uma FAR de 0,01% e FRR de 4% enquanto que em [44] os resultados com textos pequenos (2 linhas) apresentam FAR=FRR=15% e com textos maiores (6 linhas) a FAR=FRR=0%.

A análise das taxas de eficácia destes trabalhos correlatos permite concluir que os resultados obtidos neste experimento são muito bons comparados aos demais trabalhos realizados na área. No entanto, classificar este trabalho como mais ou menos eficiente que os demais seria um erro, pois [44] apresenta taxas de eficácias menores que os demais quando textos longos são utilizados, mas esta pesquisa utiliza apenas 6 usuários para testar sua eficácia, [6] apresenta uma FRR = 4% que poderia ser considerada elevada considerando os resultados obtidos nesta dissertação e em [44], que utiliza 44 usuários válidos e 110 usuários inválidos em seu teste. Devido a estas grandes diferenças entre as metodologias empregadas não é possível dizer qual é o melhor resultado e qual o pior.

Outra consideração importante a ser ressaltada é que as RNAs implementadas são redes diretas com algoritmo de aprendizagem por retro-propagação, que é uma topologia muito simples de RNA. Aliado a este fator, a única manipulação sobre os dados de entrada realizada, foi a eliminação de exemplos do conjunto de treinamento da RNA que apresentassem latência entre teclas maior que 600 milisegundos. Quando teclas de correção de erros de digitação foram pressionadas, as latências destas teclas também foram coletadas sendo que a utilização do recurso de correção é tratada da mesma forma que na digitação correta dos dados, portanto nenhum tratamento especial foi adotado. Assume-se que da mesma forma que o usuário possui um padrão de digitação, este padrão também deve estar presente no momento de digitar as teclas de correção.

Muitos trabalhos nesta área de pesquisa mostram como principal fator negativo da utilização de RNAs a necessidade de re-treinamento das redes quando um novo usuário é adicionado ao sistema. Neste ponto está uma das principais contribuições deste trabalho, pois com a utilização da máquina de comitê adaptada, este trabalho de re-treinamento não é

necessário. Quando um novo usuário é adicionado no sistema de autenticação proposto basta treinar as RNAs que constituirão a máquina de comitê do usuário em questão e uma nova RNA para cada máquina de comitê dos usuários existentes. Após treinar todas as RNAs basta modificar a configuração do combinador da máquina de comitê para que este leve em consideração mais uma RNA. Se o número de usuários a serem inseridos no sistema de autenticação for muito grande, ao invés de aumentar indefinidamente o tamanho das máquinas de comitê, pode-se particionar os usuários em diferentes grupos e treinar uma máquina de comitê para cada grupo. Desta forma o trabalho de treinamento não seria excessivo. Como visto neste trabalho, uma máquina de comitê treinada com informações dos padrões de 14 usuários, apresenta FAR e FRR eficientes. Portanto modularizar as máquinas de comitê para que estas tenham em torno de 14 usuários é suficiente para que o sistema tenha uma boa eficácia.

6.1 – Trabalhos Futuros

Como trabalhos futuros a este pode-se relacionar:

- Implementação de um sistema de autenticação através do padrão de utilização do mouse: o sistema proposto autentica continuamente o usuário quando este está digitando textos, no entanto atualmente muitos sistemas possibilitam a realização de grande parte das tarefas através do mouse. Alguns trabalhos sobre este tema já foram realizados, entretanto os resultados apresentados não são satisfatórios;
- Aumentar o número de usuários analisados, tanto do grupo 1 como do grupo 2. Para este trabalho foram analisados 20 usuários e uma pesquisa com uma maior quantidade de usuários poderia demonstrar se a eficácia do sistema permanece estável na utilização em larga escala;
- Aumentar o número de amostras de teste e características analisadas;
- Implementar um módulo de autenticação que possa ser agregado aos sistemas operacionais existentes;

- Testar o sistema biométrico utilizando outros tipos de RNAs;

Referências Bibliográficas

[1] ALEXANDRE, T. J. Biometrics on smartcards: An approach to keyboard behavioral signature. *In Second Smart Card Researsh & Advanced Applications Conference, 1996.*

[2] ANAGUN, A. S. & CIN, I. A Neural Network based Computer Access Security System for Multiple Users. *Computers & Industrial Engineering*, Vol. 35, Nº. 1-2, pp. 351-354, 1998.

[3] ARAÚJO, L. C.F. Uma Metodologia para Autenticação Pessoal baseada em Dinâmica da Digitação. Mestrado, Universidade Estadual de Campinas, 2004

[4] ASHBOURN, J. The Biometric White Paper, 1999. Disponível em: http://www.avanti.1to1.org. Acesso em: 24 jul. 2005.

[5] BARRETO, J. M. Inteligência Artificial no limiar do Século XXI: Abordagem Híbrida - simbólica, conexionista e evolutiva. Segunda Edição, Florianópolis, Duplic Prest. Serviços, 2000, 324 p.

[6] BERGADANO, F.; GUNETTI, D. & PICARDI C. User authentication through Keystroke Dynamics. *ACM Transactions on Information and System Security (TISSEC)*, Vol. 5, Nº. 4, pp. 367-397, 2002.

[7] BioPassword® for Enterprise Networks 5.0. Disponível em: http://www.biopassword.com/bp2/products/bp50/overview.asp. Acesso em: 24 jul. 2005.

[8] BISHOP, C. M. Neural Networks for Pattern Recognition. Nova York, Editora Oxford, 1995, 482p.

[9] BLEHA, S.; SLIVINSKY, C. & HUSSIEN, B. Computer-Access Security Systems Using Keystroke Dynamics. *IEEE Transactions on Pattern Analysis and Machine Intelligence*, Vol. 12, Nº.12, pp. 1217-1222, 1990.

[10] BOWMAN, E. Everything You Need to Know About Biometrics. Identix Corporation, jan. 2000. Disponível em: http://www.ibia.org/EverythingAboutBiometrics.PDF. Acesso em: 15 maio 2005.

[11] BROWN, M. & ROGERS, S. J. User identification via keystroke characteristics of typed names using neural networks. *International Journal of Man-Machine Studies*, Vol. 39, Nº. 6, pp. 999-1014, 1993.

[12] CAPUANO, N.; MASELLA, M.; MIRANDA, S. & SALERNO, S. User authentication with neural networks. *Proceedings of the 5th International*

Conference on Engineering Applications of Neural Networks EANN 99, Warsaw, Poland, 1999.

[13] CHRISTODOULAKIS, S. An Interactive Pattern Recognition. *Proceedings of the eleventh SIGCSE technical symposium on Computer science education*, Kansas City, Missouri, United States, pp. 184, 1980.

[14] COLTELL, O.; BADÍA, J.M. & Torres, G. Biometric Identification System Based in Keyboard Filtering. *Proceedings of XXXIII Annual IEEE International Carnahan Conference on Security Technology, IEEE Pub.*, pp. 203-209, 1999.

[15] FERREIRA, A. B. H. Novo Dicionário Aurélio da Língua Portuguesa. São Paulo, Nova Fronteira, 1986.

[16] GAINES, R.; LISOWSKI, W.; PRESS, S. & SHAPIRO, N. Authentication by keystroke timing: Some preliminary results. Rand Report R-256-NSF. Rand Corporation, Santa Mônica, CA, 1980.

[17] GUVEN, A. & SOGUKPINAR, I. Understanding users keystroke patterns for computer access security. *Coputers & Security*, Vol. 22, Nº. 8, pp. 695-706, 2003.

[18] HAYKIN, S. Redes Neurais – Princípios e Práticas. Segunda Edição, Porto Alegre, Editora Bookman, 2001, 900 p.

[19] HOUSLEY, R. & POLK T. Planning for PKI – Best Practices Guide for Deploying Public Key Infrastructure. New York, John Wiley & Sons, Inc., 2000, 327 p.

[20] HYRAYAMA, V. Classificador de Qualidade de Álcool Combustível e Poder Calorífico de Gá GLP. Mestrado, Universidade de São Paulo, 2004.

[21] ILONEN, J. Keystroke Dynamics. Disponível em: http://www.it.lut.fi/kurssit/03-04/010970000/seminars/Ilonen.pdf. Acesso em: 24 jul. 2005.

[22] JAIN, A. K.; DUIN, R. P. W. & MAO, J. Statistical pattern recoginition: A review. *IEEE Transactions on Pattern Analysis and Machine Intelligence*, Vol. 22, Nº.1, pp. 4-37, 2000.

[23] JOYCE, R. & GUPTA G. Identity Authentication Based on Keystroke Latencies. *Communications of the ACM*, Vol. 33, Nº. 2, pp. 168 - 176, 1990.

[24] LAMMERS, A. & LANGENFELD, S. Identity Authentication Based on Keystroke Latencies Using Neural Networks. *Journal of Computing Sciences in Colleges*, Vol. 6, Nº. 5, pp. 48-51, 1991.

[25] LIN, D.T. Computer-Access Authentication with Neural Network Based Keystroke Identity Verification. *Proceedings in International Conference on Neural Networks*, Vol. 1, pp. 174-178, 1997.

[26] LIU, S. & SILVERMAN, M. A Practical Guide to Biometric Security Technology. *IT Professional*, Vol. 3, Nº. 1, pp. 27-32, 2001.

[27] MAHAR, D.; NAPIER, R.; WAGNER, M.; LAVERTY, W.; HENDERSON, R.D. & HIRON, M. Optimizing digraph-latency based biometric typist verification systems: inter and intra typist differences in digraph latency distributions. *International Journal of Human-Computer Studies*, Vol. 43, Nº. 4, pp. 579-592, 1995.

[28] MILLER, B. Vital sings of identity. *IEEE Spectrum*, pp 22-30, 1994.

[29] MONROSE, F.; REITER, M. K. & WETZEL, S. Password Hardening Based on Keystroke Dynamics. *Proceedings of the 6th ACM conference on Computer and communications security*, 1999.

[30] MONROSE, F. & RUBIN, A. D. Authentication via Keystroke Dynamics. *Proceedings of the 4th ACM conference on Computer and communications security*, pp. 48-56, 1997.

[31] MONROSE, F. & RUBIN, A. D. Keystroke Dynamics as a Biometric for Authentication. *Future Generation Computer Systems*, Vol. 16, Nº. 4, pp. 351-359, 2000.

[32] MROCZKOWSKI, P. Identity Verification using Keyboard Statistics. Mestrado, Linköping Institute of Technology, 2004.

[33] OBAIDAT, M. S. A verification Methodology for Computer Systems Users. *Proceedings of the 1995 ACM symposium on Applied computing*, Nashville, Tennessee, United States, pp. 258-262, 1995.

[34] OBAIDAT, M. S. & MACCHAIROLO, D.T. An On-Line Neural Network System for Computer Access Security. *IEEE Transactions on Industrial Electronics*, Vol. 40, Nº. 2, pp. 235-242, 1993.

[35] OBAIDAT, M. S. & MACCHAIROLO, D.T. A Multilayer Neural Network System for Computer Access Security. *IEEE Transactions on System, Man and Cybernetics*, Vol 24, Nº. 5, pp. 806-813, 1994.

[36] OBAIDAT, M. S. & SADOUN, B. A Simulation Evaluation Study of Neural Network Techniques to Computer User Identification. *Information Sciences: an International Journal*, Vol. 102, Nº. 1-4, pp. 239-258, 1997.

[37] OBAIDAT, M. S. & SADOUN, B. Verification of Computer Users Using Keystroke Dynamics. *IEEE Transactions on System, Man and Cybernetics*, Vol. 27, Nº. 2, pp. 261-269, 1997.

[38] ORD, T. & FURNELL, S. M. User authentication for keypad-based devices using keystroke analysis. *Proceedings of the Second International Network Conference*, pp. 263-272, 2000.

[39] PEACOCK, A. Learning User Keystroke Latency Patterns (Preliminary Report). Disponível em: http://pel.cs.byu.edu/~alen/personal/CourseWork/cs572/KeystrokePaper/. Acesso em: 24 jul. 2005.

[40] Redes Neurais. Disponível em: http://www.din.uem.br/ia/intelige/neurais2/. Acesso em: 24 jul. 2005.

[41] SCHNEIER, B. Applied Cryptography – Protocols, Algorithms, and Source Copde in C. Second Edition, New York, John Wiley & Sons, Inc., 1996, 757 p.

[42] SONG, D.; VENABLE, P. & PERRIG A. User Recognition by Keystroke Latency Pattern Analysis. Disponível em: http://www.ece.cmu.edu/~adrian/projects/keystroke/mid.pdf. Acesso em: 24 jul. 2005.

[43] STALLINGS, W. Cryptography and Network Security. Principles and Practice. Second Edition, New York, Prentice Hall, 1998, 569 p.

[44] SYLVAIN, H.; JEAN-YVES, R. & HUBERT, C. Users Authentication by a study of human computer interactions. Disponível em: http://www.univ-tours.fr/ed/edsst/comm2004/hocquet.pdf. Acesso em: 24 jul. 2005.

[45] YU, E. & CHO S. Keystroke dynamics identity verification – its problems and practical solutions. *Coputers & Security*, Vol. 23, Nº. 5, pp. 428-440, 2004.