Biometria através de Impressão Digital

Biometrics through Digital Printing

Márcia Santos da Silva [1]
Venicio Siqueira Filho [2]

Artigo Original

Original Paper

Palavras-chave:

Sistemas biométricos

Biometria digital

Controle de acesso por biometria digital

Resumo

Este artigo tem como objetivo atender as necessidades do Unifoa, um centro universitário que por vez tem dificuldades com a agilidade do tráfego de pessoas e segurança nas portarias, e como solução desses problemas o sistema SCB atende respectivamente tais requisitos, além de oferecer maior controle de volume de acessos na instituição, fazendo uso da ferramenta para gerar relatórios essenciais. Como metodologia, adotamos os princípios da orientação a objetos seguindo os padrões da UML buscando desenvolver uma documentação clara que apresenta métricas, padrões e estimativas utilizando diagramas e tabelas. Com o auxilio da UML, o SCB foi desenvolvido na linguagem Java, sendo utilizado Oracle que é um SGBD de grande porte que utiliza a linguagem PL/SQL como interface e atenderá a demanda necessária. Com essas informações e ferramentas disponíveis, buscamos como objetivo solucionar o problema apresentado pelo nosso cliente bem como atender a todas suas expectativas e proporcionando plena satisfação, uma vez seguindo um padrão pode-se desenvolver um produto de qualidade com todas as características necessárias melhorando o gerenciamento de acesso e segurança para torná-los um fator diferencial entre as demais instituições de ensino.

Recebido em 03/2011

Aprovado em 04/2011

Abstract

The aim of this article is to deal with the necessities of Unifoa, a university that has some difficulties to control a faster traffic flow and to assure security in that situation. As a solution to these problems the SCB system attends, respectively, such requirements and it offers greater control of the institution access using tools to generate essential reports. The methodology we adopted was based on object orientation principles, following UML rules in order to develop a clear documentation that shows metrics, standards and estimates using diagrams and tables. With the help of UML, the SCB was developed in Java, and uses Oracle, a large DBMS that implements PL / SQL language interface, which will answer the issues. With these available information and tools we intend to solve the problems presented by our client as well as their expectations and give them full satisfaction. Once following this pattern a product of quality can be developed with all the needed characteristics improving the access and security management to make them a distinguishing factor among other educational institutions.

Key words:

Biometric systems

Digital biometrics

Access control through digital biometrics

[1] Graduação em Sistemas de Informação – UniFOA

[2] Professor Msc. do Curso Sistemas de Informação – UniFOA

1. Introdução

Com o objetivo de promover a agilidade e facilidade no acesso às dependências da faculdade, verificou-se a necessidade de um sistema que melhore o desempenho deste controle no UniFOA. Mediante pesquisas realizadas com os próprios alunos, observamos que estes esquecem, perdem ou quebram suas carteirinhas escolares com facilidade e com isso é gerada uma fila nas entradas da faculdade.
Outro problema identificado é a baixa durabilidade do cartão de acesso que danifica-se com o tempo de uso, descascando e perdendo sua identificação (código de barras).

Nossa utilização da biometria também será na entrada do sistema para cadastramento das digitais dos alunos, funcionários, professores e demais pessoas que frequentam a faculdade.

A proposta do sistema é diminuir custos com impressões de cartão de acesso estudantis e preocupações a empresa quanto à segurança da informação contida no sistema atual por meio da identificação digital do estudante de forma a obter as seguintes vantagens:

- Evitar perdas, roubos e manutenções futuras de cartão de acesso;
- Agilizar o tráfego de pessoas na entrada e saída da universidade;
- Aumentar a segurança da informação que o sistema possui,

Isso será realidade com a utilização de uma catraca biométrica, onde os alunos cadastrarão suas impressões digitais e, ao entrar na faculdade, será necessário apenas colocar o dedo na catraca a fim de ser identificado através de nosso software, liberando ou não a entrada do aluno.

O sistema que os funcionários usarão para cadastrar as digitais de usuários terá uma identificação por login, senha e digital. Somente os funcionários terão acesso a esse sistema e isso será verificado através da biometria. Teremos dois níveis de acesso para os funcionários que cadastrarão usuários no sistema. O de administrador e o de usuário comum. Administrador poderá cadastrar outros funcionários para acessar o sistema; usuário comum apenas poderá cadastrar digitais de alunos e funcionários para acesso a universidade.

Portanto, o sistema procura compor uma única ação de leitura biométrica as funcionalidades de gravação de dados e permissão, criando assim uma maior facilidade e rapidez tanto para o trânsito de pessoas na entrada da faculdade quanto para segurança.

Para esse Projeto, serão realizadas várias etapas de desenvolvimento, a primeira delas é a Análise de Requisitos, que tem como objetivo conhecer o sistema atual: detectar os problemas existentes e as necessidades não contempladas visando definir alternativas para a construção de um novo sistema. Esta etapa contém os seguintes produtos principais: descrição dos processos e procedimentos, tabelas de Casos de Usos, Diagramas de Casos de Usos, novas necessidades e alternativas de implementação.

Em seguida, dando continuidade aos trabalhos, vem a etapa de Análise (Modelo Conceitual do Sistema) que define um conjunto de características que o sistema deve possuir para atingir seu propósito. Podemos destacar: o Diagrama de Classe Conceitual, Diagrama de Objetos relevantes, Diagrama de Estado dos Objetos e Diagramas de Atividades.

A seguir vem a Etapa do Projeto que abrange a modelagem física do sistema, englobando os Diagramas de Interação (Diagrama de Sequência ou Diagrama de Colaboração) e o Diagrama de Classe do Projeto.

A última etapa é a Implementação que consiste na elaboração dos Diagramas de Componentes e de Implantação. Nesta etapa temos ainda os seguintes produtos: requisitos de segurança e confiabilidade do sistema, layout das telas e relatórios, plano de implementação do novo sistema e o plano de contingência.

Contudo, com o desenvolvimento do sistema proposto, procuramos agregar valor ao negócio da empresa agilizando as consultas, dar mais segurança e eficiência, para atender as demandas de trabalhos existentes.

2. Conceituações e Contextualizações da Biometria

A comunicação em qualquer lugar e a qualquer hora é uma realidade dos sistemas de informação na atualidade. De acordo com Pinheiro (2008), para aqueles que administram

sistemas computacionais, proteger adequadamente a informação é uma necessidade. O ambiente de redes de computadores tem sido palco de inúmeros incidentes de segurança, provocados por falhas na infraestrutura computacional como tentativas de invasão. Um dos maiores problemas enfrentados em termos de segurança da informação é a autenticação dos usuários que utilizam os recursos dos sistemas computacionais. Precisamos garantir que o usuário é realmente quem ele diz que é. Essa preocupação é também vista quando se trata de acesso a uma dependência, como por exemplo, a empresas ou universidades. Certificarmo-nos que os usuários que transitam no ambiente realmente eram para estar lá se transforma em um desafio quando temos tantos recursos disponíveis para facilitar o acesso indevido.

2.1 Segurança da Informação

Por que precisamos proteger a informação? Segundo Pinheiro (2008, p. 7):

As tecnologias baseadas em sistemas computacionais têm crescido em uso e incorporado mudanças surpreendentes na sociedade atual, principalmente nas atividades cotidianas dos indivíduos, que se deparam cada vez mais com situações e procedimentos onde são obrigados a provar sua identidade para que assim se confirme que são realmente quem dizem ser. Com a exigência cada vez maior de novas funcionalidades nos sistemas de informação, surgem, com crescente evidência, novos problemas de segurança e, em particular, a questão da autenticação dos usuários desses sistemas. Por essas razões, tem aumentado o interesse no desenvolvimento de métodos para a autenticação da identidade pessoal que levem em consideração uma estrutura dotada de mecanismos de segurança da informação mais eficiente.

2.2 Ameaças e Ataques

Vivemos diariamente sofrendo ataques e ameaças em nossos sistemas que podem ser intencionais ou acidentais. Acidental seria aquela que não foi planejada. Pode ser, por exemplo, uma falha no hardware (um defeito no disco rígido) ou uma falha de software (um bug[1] no sistema operacional, por exemplo). Já uma ameaça intencional, como o próprio nome já diz, está relacionada a intencionalidade premeditada. Algumas das principais ameaças aos sistemas envolvem a destruição de informações ou recursos, modificações, deturpação, roubo, remoção ou perda da informação, revelação de informações confidenciais ou não, chegando até a interrupção de serviços de rede.

Já um ataque varia desde a pura curiosidade, passando pelo interesse de adquirir mais conhecimento, até o extremo envolvendo ganhos financeiros, extorsão, chantagem de algum tipo, espionagem industrial com a venda de informações confidenciais e, o que está muito na moda, ferir a imagem de um governo ou uma determinada empresa ou serviço.

2.3 Segurança de Acesso

O roubo de identidade afeta milhões de pessoas em todo o mundo e tem sido um dos tipos de fraude mais praticados nos ambientes das redes de comunicação, especialmente a internet. Quando se juntam as vulnerabilidades do mundo real às vulnerabilidades do mundo virtual e às fraquezas do ser humano, é grande a possibilidade de vazamento de informações, tendo como um dos resultados possíveis o roubo da identidade. Por esse motivo, a autenticação é um item fundamental para a segurança do ambiente de uma rede de computadores ao validar a identificação dos usuários que desejam usar os recursos disponíveis.

A identificação é a função em que o usuário declara sua identidade para o sistema, enquanto que a autenticação é a função responsável pela validação dessa declaração de identidade do usuário. Somente após a identificação e autenticação do usuário é que o sistema concederá (ou não) a autorização para o acesso aos recursos da rede ou ao estabelecimento. Segundo Pinheiro (2008), muitos profissionais especializados em segurança da informação consideram que as medidas de autenticação simples, baseadas em identificador e senha precisam ser reforçadas através de uma au-

[1] bug – é um erro no funcionamento comum de um software, também chamado de falha na lógica programação, e pode causar discrepâncias no objetivo, ou impossibilidade de realização, de uma ação na utilização de um programa de computador. WIKIPEDIA. Defeito de software. 2010. Disponível em: <http://pt.wikipedia.org/wiki/Defeito_de_software>. Acesso em: 08 fev. 2010.

tenticação de fator múltiplo, ou seja, associar o que o individuo conhece, com algo que ele possua ou com suas características individuais. Esse tipo de autenticação é conhecido como "autenticação de dois fatores", pois são usados dois métodos e, "autenticação em três fatores", quando três métodos são utilizados.

2.4 Autenticação

Baseada no que se Conhece

Trata-se da autenticação baseada em algo que o usuário do sistema conheça. Nessa categoria encontramos os nomes de acesso (login), as senhas (password) e as chaves criptográficas.

Outro tipo muito utilizado é a "identificação positiva", que requer do usuário informações pessoais (que serão informações previamente cadastradas em um banco de dados), além do nome e da senha pessoal.

Por Senhas

Define-se senha como "um dado secreto, usualmente composto por uma sequência de caracteres, que é usado como informação para autenticar um usuário ou pessoa". Esse dado normalmente é utilizado em conjunto com uma identificação pessoal (login do usuário) durante o processo de autenticação, quando da entrada deste sistema computacional.

A senha é uma forma de assinatura eletrônica e deve garantir que determinado indivíduo é ele mesmo, permitindo seu acesso aos vários serviços disponibilizados em um sistema de informação. Portanto, ela é pessoal, intransferível e deve ser mantida em sigilo absoluto.

Baseada no que se Possui

O segundo método de autenticação é baseado em um dispositivo de posse do usuário (token[2]), o qual pode ser dotado de algum tipo de processamento (smart token – dispositivos inteligentes).

Os memories tokens (dispositivos de memória) são sempre usados em conjunto com as senhas. Um exemplo de sua aplicação está nos cartões bancários. Esses cartões contêm informações para a autenticação e são usados em conjunto com a senha no momento que o usuário utiliza o sistema do banco.

Já os smart tokens apresentam-se na forma de dispositivos eletrônicos e possibilitam o processamento de algumas informações. Eles podem ser divididos em três categorias básicas, a saber:

- Quanto à característica física – podem ser divididos em Smart Cards[3] e outros dispositivos semelhantes a chaves, chaveiros, bastões e outros objetos portáteis;

- Quanto à interface – podem funcionar como interfaces eletrônicas que requerem um dispositivo de leitura (como os Smart Cards) ou manuais, que utilizam um dispositivo de entrada de dados dotado de teclas ou visores para a interação entre o usuário e a máquina;

- Quanto ao protocolo - os protocolos usados para autenticação podem ser divididos em três categorias:

    - Senhas estáticas – o usuário do sistema se autentica no token e o token autentica o usuário no sistema;

    - Senhas dinâmicas – as senhas são alteradas automaticamente nos sistemas com interface eletrônica, mas devem ser lidas e digitadas pelos usuários que utilizam interface estática;

    - Desafio-resposta – protocolo baseado em criptografia, no qual o sistema envia um desafio ao usuário, que deve responder ao sistema, o qual avalia a resposta.

[2] Token - é um dispositivo (hardware), com conexão via USB, que permite armazenar e transportar de forma segura seu certificado digital. Dessa forma, o usuário poderá fazer assinaturas digitais de qualquer computador com uma porta USB, não ficando limitado a assinar digitalmente somente através de seu computador. ELIEL SILVERIO. O que é TOKEN?. 2010. Disponível em: <http://www.systemar.com.br/digital_sign.php>. Acesso em: 08 fev. 2010.

[3] Smart Cards - é um cartão contendo um chip responsável pela geração e o armazenamento de certificados digitais, informações que dizem quem você é. GABRIEL TORRES. Smart Card. 2002. Disponível em: <http://www.clubedohardware.com.br/artigos/665>. Acesso em: 08 fev. 2010

Baseada nas Características Individuais

A proteção de informações importantes requer um método de autenticação no qual a possibilidade de acesso indevido ao sistema seja mínima, de forma que a autenticação garanta a identificação do usuário de modo inequívoco e eficaz. Esse método é baseado em alguma característica física ou comportamental própria do usuário do sistema, conhecida como "característica biométrica".

Os sistemas de autenticação, utilizados na segurança computacional, têm procurado aperfeiçoar o uso do identificador biométrico e da senha pessoal como formas de validar um usuário que utilize os recursos do sistema computacional.

2.5 Tipos de Controle de Acesso

Físico

É comum em um controle de acesso físico estabelecer-se restrições de acesso a locais e equipamentos de valor dentro das corporações, não somente evitando-se acesso de pessoal externo, mas, muitas vezes, limitando-se também o acesso do pessoal da própria empresa de acordo com seu nível hierárquico ou funcionalidade desenvolvida. Assim, o objetivo do controle de acesso físico é permitir que apenas os usuários autorizados obtenham esse acesso.

O controle de acesso físico às instalações é um aspecto particularmente importante da segurança física. Os acessos de visitantes, clientes e outras pessoas- não diretamente envolvidas com a operação do sistema- deve ser o menor possível.

Em geral, a segurança física é obtida através de dispositivos como fechaduras, catracas e portas dotadas de dispositivos eletrônicos que bloqueiam o acesso ao ambiente dos equipamentos ou sistemas que se deseja proteger.

Lógico

Considerando que o controle de acesso físico não é suficiente para garantir a segurança das informações de um sistema computacional, serão necessários controles de acesso lógico, representados por medidas de segurança baseadas em hardware e software com a finalidade de impedir acessos não autorizados ao sistema.

Os controles de acesso lógico envolvem o fornecimento da identificação do usuário e de uma senha que serve de autenticação, provando ao sistema que o individuo realmente é quem diz ser. O identificador deve ser único, ou seja, cada usuário deve ter sua identidade própria. O principal objetivo do controle acesso lógico é que apenas usuários autorizados tenham acesso aos recursos da rede realmente necessários à execução de suas tarefas. Isso significa a existência de dispositivos que impeçam os usuários de executar transações incompatíveis com suas funções ou além de suas responsabilidades.

2.6 Conceituando a Biometria

Mas afinal, o que é a biometria? A biometria pode ser formalmente definida como a ciência da aplicação de métodos de estatística quantitativa a fatos biológicos, ou seja, é o ramo da ciência que se ocupa da medida dos seres vivos (do grego bio = vida e métron = medida). Resumindo, a biometria reconhece um indivíduo pelas suas características humanas mensuráveis (físicas ou comportamentais) para autenticar a identidade de um indivíduo. A biometria pode ser usada para incrementar a segurança em redes de computadores, proteger as transações financeiras, controlar o acesso as instalações de alta segurança, prevenir fraudes, entre outras aplicações.

2.7 Sistema Biométrico Básico

Como mencionado, em um sistema biométrico, uma característica individual precisa ser registrada e a sua gravação é chamada de registro (enrollment). Esse registro está baseado na criação de um modelo (template), que é a representação digital de uma característica física.

O modelo é normalmente um externo conjunto de caracteres alfanuméricos baseados em algum tipo de algoritmo biométrico, que descreve as características físicas de um indivíduo.

Um algoritmo é uma sequencia limitada de instruções ou passos que um sistema computacional utiliza pra resolver um problema específico. Na biometria são utilizados diferentes tipos de algoritmos, para processamento de imagens, geração de templates, para comparação, entre outros, com o objetivo de aten-

der aos diferentes tipos de sistemas. Assim, o algoritmo biométrico pode ser visto como o tradutor da característica física em uma representação digital na forma de um modelo.

O algoritmo também permite comparar o modelo registrado em um Banco de Dados Biométrico com o modelo de um indivíduo que deseja se autenticar no sistema, chamado de "modelo vivo". Quando os modelos são comparados, o sistema calcula a semelhança entre eles. Se a comparação for positiva, a pessoa será autenticada, caso contrário, seu registro será negado.

2.8 Componentes do Sistema Biométrico

Segundo Pinheiro (2008), a arquitetura de um sistema biométrico básico pode ser dividida em quatro componentes principais:

- **Subsistema Interface de usuário** (Sensor) – conjunto de elementos que contém os dispositivos ou sensor que capta a amostra biométrica do indivíduo e a converte em um formato adequado para ser utilizada. O desempenho de todo o sistema é afetado pela qualidade da amostra fornecida e pelo desempenho do próprio sensor ou dispositivo de coleta;

- **Subsistema Estação de Controle** (Cérebro) – é responsável pelas funções de controle dos dispositivos, inclui o hardware associado que pode estar dentro da própria máquina ou pode ser um computador conectado ao equipamento ao qual se encontram todos os recursos de programação, processamento e armazenamento da informação. É responsável por receber a amostra biométrica fornecida pelo subsistema de interface de usuário e convertê-la em uma forma adequada para o processamento pelo módulo de comparação;

- **Subsistema Comparador** (Comunicações e Processamento) – esta etapa faz a comparação da amostra biométrica apresentada com o template da base de dados. Ele verifica se as amostras são similares para tomar a decisão que identifica que a amostra apresentada pertence ou não ao proprietário do template selecionado da base de dados. Para tomar essa decisão um limiar deve ser estabelecido para poder delimitar até que valor de similaridade é considerado como uma amostra autêntica ou uma amostra falsa.

- **Subsistema de Armazenamento** (Banco de Dados) – este módulo mantém os templates dos usuários cadastrados no sistema biomético. Ele disponibiliza a adição, subtração ou atualização dos templates registrados, podendo conter para um único usuário apenas um template ou vários, dependendo para quais finalidades o sistema foi desenvolvido. Cada template é armazenado com um identificador do usuário que permita determinar a que individuo, ele pertence.

Elementos Biométricos

Dentre os tipos de elementos biométricos podemos identificar sistemas baseados na identificação física (reconhecimento facial, impressão digital, geometria da mão, identificação pela íris e retina, DNA, odores, entre outros) ou comportamental do indivíduo (reconhecimento da voz, dinâmica datilográfica, assim como a própria assinatura).

Os critérios normalmente usados para a escolha de um sistema biométrico em particular consideram, nomeadamente, o conforto na utilização, a precisão, a relação entre a qualidade e o preço e o nível de segurança. Dependendo do nível de segurança desejado para o sistema computacional, recomenda-se o uso simultâneo de pelo menos dois tipos de tecnologias de autenticação. Outra recomendação, segundo Pinheiro (2008), é que os sistemas que armazenam dados biométricos devem ser protegidos com o uso de alguma técnica de criptografia.

Deve-se evitar a utilização descontrolada desta como de qualquer outra tecnologia de reconhecimento de ambiente de trabalho. É importante manter uma posição prudente e equilibrada que incentive os fabricantes de sistemas biométricos a adotar soluções técnicas que, protegendo a privacidade, minimizem os riscos de utilização indevida.

Tabela 1 - Modelos de identificação biométrica

Tipo de Acesso	Descrição
Reconhecimento Facial	A tecnologia de reconhecimento facial considera as medidas do rosto que nunca se alteram, mesmo que o indivíduo seja submetido a cirurgias plásticas. Essas medidas básicas são: distância entre os olhos, distância dentre a boca, nariz e olhos e distância entre olhos, queixo, boca e linha dos cabelos.
	Vantagens
	A identificação pode ser feita sem qualquer contato físico.
	Desvantagens
	É um processo extremamente complexo que deve levar em consideração as mudanças que o rosto sofre no decorrer do tempo.
Geometria da mão	Descrição
	Para a leitura da geometria da mão, o scanner possui guias que se assemelham a pinos que se encaixam entre os dedos. Essas guias facilitam o reconhecimento do desenho da mão. O sistema calcula e registra as proporções entre os dedos e articulações, que são decisivas para identificar a pessoa.
	Vantagens
	É um sistema que apresenta baixo custo de implementação.
	Desvantagens
	Apresenta problemas com a presença de anéis nos dedos e o indivíduo precisa encaixar corretamente a mão no equipamento de leitura.

Tipo de Acesso	Descrição
Identificação pela Íris	O processo de reconhecimento através da íris humana pode ser dividido em três etapas distintas. A primeira etapa corresponde à aquisição da imagem da íris; a segunda etapa envolve a aplicação do algoritmo de extração e reconhecimento das características biométricas; a terceira refere-se ao processo de extração das características para gerar o IrisCode.
	Vantagens
	É mais preciso por ser a íris praticamente imutável com o passar do tempo e pouco suscetível a alterações físicas como sujeira e machucados que deixam cicatrizes.
	Desvantagens
	A íris não é um alvo fácil. É pequena (aproximadamente um centímetro), móvel, está localizada atrás de uma superfície refletora úmida e curvada, parcialmente oculta por pálpebras que piscam frequentemente e que pode ser obscurecida por óculos, lentes e reflexos e é deformada com a dilatação da pupila.
Reconhecimento pela Retina	Descrição
	Este sistema permite a identificação do indivíduo pelo tipo e característica dos vasos da retina. Os dados levantados durante o exame "in loco" são convertidos em sinal analógico que, por sua vez, são transformados em sinal digital. O perfil da retina é armazenado no banco de dados do sistema biométrico para fins de comparação e verificação.
	Vantagens
	O padrão de veias da retina é a característica com maior garantia de singularidade que um indivíduo pode apresentar.
	Desvantagens
	O sistema apresenta leitura difícil e incômoda na medida em que a captura dessa imagem exige que a pessoa olhe fixamente para um ponto de luz de infravermelho até que a câmera focalize os padrões e os capture. Além disso, oferece alto risco de implementação.

Reconhecimento por Voz	Descrição
	O funcionamento do sistema baseia-se na captura e no processamento digital do áudio falado, através de um algoritmo especializado que segmenta este áudio em pequenos pedaços conhecidos como fonemas, devendo ser utilizado um tipo de algoritmo para cada linguagem, mesmo que haja aparentemente pequenas diferenças.
	Vantagens
	É o fato de a fala ser inerente ao ser humano e sua comunicação com o mundo exterior ser também natural e simples. Permitir o uso mais inteligente das árvores de atendimento automatizadas, eliminando as limitações características dessas soluções que utilizam acesso por discagem telefônica.
	Desvantagens
	Alguns sistemas solicitam que o usuário fale, em voz alta e repetidas vezes, uma sequência aleatória de números ou uma frase qualquer, o que pode representar uma demora no processo de cadastramento do padrão vocal. O sistema também é afetado por ruídos ambientais e o estado físico ou emocional do indivíduo, gripe ou estresse, por exemplo, comprometem a precisão do reconhecimento.

2.9 Modelo escolhido – Impressão Digital

De todas as características biométricas, a impressão digital é a mais estudada, sendo empregada na área de segurança desde o século XIX como elemento de identificação de indivíduos. As impressões digitais são únicas para cada indivíduo e consideradas, segundo Pinheiro (2008), o tipo biométrico mais seguro para determinar a identidade depois do teste de DNA.

É o tipo mais popular de sistema biométrico, baseando-se na identificação através das irregularidades das impressões digitais, retiradas de um ou mais dedos, as chamadas "minúcias". A captura da imagem da impressão digital ocorre por meios ópticos, sendo que essa imagem é processada digitalmente pelo sistema, que identifica as características datiloscópicas, comparando com os registros de banco de dados, determinando ou não o acesso.

O banco de dados é gerado obtendo-se as impressões digitais dos usuários da rede. A finalidade é obter a impressão digital de todos os dedos, formando um arquivo decadactilar. Caso ocorra algum dano na impressão digital de um dos dedos, os outros poderão ser utilizados para o reconhecimento.

Figura 1 – Exemplos de minúcias encontradas na impressão digital

Fonte: PINHEIRO, José Mauricio. Biometria nos Sistemas Computacionais. Você é a senha. Rio de Janeiro: Editora Ciência Moderna, 2008.

Trata-se de um método biométrico conhecido também como Finger Scan, relativamente barato e rápido, que oferece uma confiabilidade relativamente boa, apresentando um baixo custo de implementação. Entretanto, apresenta algumas desvantagens: se o dedo estiver com as minúcias desgastadas, sujo ou muito seco poderão ocorrer erros no processo de comparação dos dados e deformidades nos dedos (calos, cortes) também podem impedir a correta identificação do indivíduo.

Para esses tipos de problemas nosso sistema cadastrará se o usuário utilizará as digitais ou não. Se o usuário possuir um dos problemas acima, ele utilizará o cartão de acesso para entrada na universidade. O mesmo será adquirido como feito atualmente sendo gerado pelo sistema atual. Para os funcionários que utilizam o sistema de cadastramento de digitais e também tem problemas com a digital, será validado apenas login e senha.

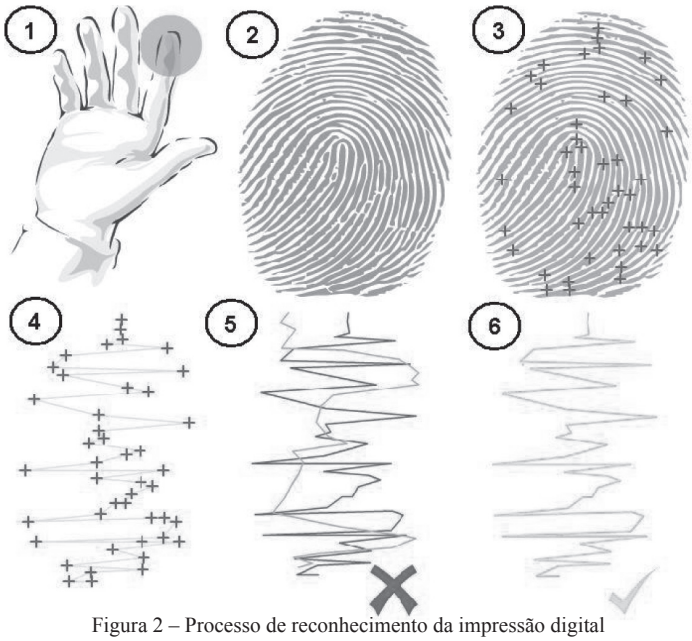

Figura 2 – Processo de reconhecimento da impressão digital

Seleção da fonte da amostra (1); captura da impressão digital (2); mapeamento das minúcias (3); geração do modelo a partir do algoritmo (4); comparação no banco de dados (5); identificação positiva (6).

Fonte: PINHEIRO, José Mauricio. Biometria nos Sistemas Computacionais. Você é a senha. Rio de Janeiro: Editora Ciência Moderna, 2008.

O reconhecimento por impressões digitais requer o uso de um scanner capaz de capturar, com um bom grau de precisão as minúcias (os traços que definem a impressão dos dedos), além de um software que trate a imagem capturada e faça o reconhecimento da digital. Os scanners para captura da impressão digital possuem tamanhos relativamente reduzidos. Atualmente, estão disponíveis sensores de impressões digitais portáteis, que podem ser anexados ao teclado, monitor ou gabinete do computador. Outros mais modernos já possuem o mecanismo acoplado a dispositivos como mouse e teclado sem fio. Os sensores biométricos utilizados para colher a impressão digital são classificados em dois tipos básicos e a diferença entre um sistema e outro está na forma de discriminar as minúcias:

- Sistema Real Time – a leitora de impressões digitais captura a amostra, processa e faz a comparação com os modelos de um banco de dados local, dando uma resposta em seguida. O controle de acesso é a sua aplicação mais popular;

- Sistema de Impressão Latente – a leitora captura a amostra biométrica e a envia para um banco de dados geral. O objetivo é determinar a quem pertence uma ou mais impressões a partir da comparação com todas as amostras disponíveis nesse banco de dados.

O modelo foi escolhido, pois de todos os pesquisados é o que apresenta menor custo de implementação e maior velocidade no reconhecimento.

3. Análise de Requisitos

3.1 Descrições do Sistema Atual e Problemas

Catraca Eletrônica: Acesso a Universidade

No período de desenvolvimento deste projeto a universidade possuía 5.862 alunos matriculados, 514 funcionários e 472 professores. Devido ao grande número de pessoas transitando na universidade, ela disponibilizou algumas catracas na entrada, onde alunos e professores passam seus crachás e são identificados podendo assim ter acesso a faculdade. Notam-se algumas falhas nesse processo, como por exemplo, o roubo e/ou empréstimo do crachá, sem possibilidade de averiguação pelos fiscais. Além disso, observamos outro problema no método atual que seria a perda e a quebra do crachá. Esquecimento e desgaste do mesmo também são fontes constantes de reclamações, trazendo transtornos por ter que providenciar outra e enfrentar filas nas entradas.

Sistema de Segurança Biométrico

O que podemos observar é que, assim como em outros sistemas, este possui apenas login e senha como identificação para acesso. No contexto de segurança e confiabilidade de dados, nota-se que este método é comum em muitas empresas. Senhas muitas das vezes são fáceis de serem burladas Apesar das senhas não aparecerem na tela, crackers[4] e "espertos" podem descobri-las facilmente. Sabemos que senhas fáceis de serem lembradas é um problema, pois podem ser óbvias para alguém que os conheça ou que tenha algum contato. E senhas mais difíceis as pessoas as esquecem com facilidade. Por isso, a preocupação com a segurança dos dados se torna maior.

3.2 Concorrência

Catraca Eletrônica: Acesso a Universidade

Podemos observar em pesquisas feitas na internet, jornais e revistas, que empresas estão cada vez mais interessadas em avanços tecnológicos que possam oferecer além de outros, agilidade em seus processos. Com a catraca biométrica, a universidade se destaca das demais com essa nova tecnologia, mostrando que se importa com os frequentadores e com a melhoria da mesma.

Sistema de Segurança Biométrico

Segurança: Nota-se também, por meio de notícias em jornais, que as empresas buscam dificultar a burla dos sistemas que possuem. Com esse sistema, a faculdade demonstra que se preocupa com a confiabilidade dos dados que fornecem aos funcionários e alunos. Além do alto nível de proteção contra fraudes e falsificações, a liberação de acesso ao sistema para cadastramento dos dados acontece somente quando autorizado.

3.3 Novo Sistema

O nosso sistema implantará uma nova estrutura de segurança e acesso na faculdade. As novas catracas serão biométricas, tendo o acesso identificado através de digitais. Essas catracas ficarão nas entradas e saídas, as mesmas serão interligadas através de um componente ao nosso sistema. Ela enviará a digital para o sistema que buscará no banco de dados o cadastro correspondente liberando ou não o acesso. O sistema de segurança através da biometria fará restrição de login, senha e digital para possibilitar manutenção do mesmo. O sistema fará a identificação necessária e liberará acesso ou não ao usuário.

4. Referências

- PINHEIRO, José Mauricio. **Biometria nos Sistemas Computacionais:** Você é a senha. Rio de Janeiro: Editora Ciência Moderna, 2008.
- TIBÉRIO, Juliano Ricardo. **Biometria, quando somente seu corpo autoriza.** Disponível em: <http://www.devmedia.com.br/articles/viewcomp.asp?comp=4486>. Acesso em: 13 ago. 2009.
- BEZERRA, Eduardo. **Princípios de análise e projeto de sistemas com UML**. Rio de Janeiro: Elsevier, 2002.
- GUEDES. Gilleanes T. A. **UML: Uma abordagem prática.** 3ºEd. São Paulo: Novatec Editora, 2008.
- MEDEIROS, Ernani. **Desenvolvendo Software com UML.** São Paulo: Pearson Makron Books, 2004.
- BOOCH, Grady. UML, **Guia do usuário.** 12º Reimp. Rio de Janeiro: Elsevier, 2000.

Endereço para Correspondência:
Venicio Siqueira Filho
venicio.vsf@uol.com.br
Centro Universitário de Volta Redonda
Campus Três Poços
Av. Paulo Erlei Alves Abrantes, nº 1325,
Três Poços - Volta Redonda / RJ
CEP: 27240-560

[4] crackers - é o termo usado para designar quem pratica a quebra (ou *cracking*) de um sistema de segurança, de forma ilegal ou sem ética. WIKIPEDIA. Cracker. 2010. Disponível em: < http://pt.wikipedia.org/wiki/Cracker>. Acesso em: 08 fev. 2010.

Informações bibliográficas:
Conforme a NBR 6023:2002 da Associação Brasileira de Normas Técnicas (ABNT), este texto científico publicado em periódico eletrônico deve ser citado da seguinte forma: SILVA, Márcia Santos da; FILHO, Venicio Siqueira. Biometria através de Impressão Digital. **Cadernos UniFOA**. Volta Redonda, Ano VI, n. 15, abril 2011.
Disponível em: <http://www.unifoa.edu.br/cadernos/edicao/15/19.pdf>