Sistema de Controle de Acesso com Biometria da Digital

Gabriel Pitágoras Silva e Brenner
gabrielbrenner@aedb.br
AEDB

Walter Bizarria
jwpbiz@gmail.com
UNITAU

Resumo:A necessidade de identificar o indivíduo corretamente para prover segurança em Sistemas de Controles de Acessos fez com que o uso das características físicas ou comportamentais individuais (biometria) se popularizasse e passasse a ser utilizado nas mais diversas soluções sistêmicas. A digital, por ter uma individualidade alta e ser uma característica física de fácil leitura e rápido processamento, passou a ser amplamente utilizada com esse objetivo. Qualquer Sistema de Controle de Acesso tem como principal preocupação a verificação se o indivíduo é quem ele diz ser e, com a evolução dos mecanismos de leitura e dos algoritmos de processamento do dado biométrico, tornou-se possível fazer isso de forma rápida, o que viabilizou a utilização de biometria para as mais diversas soluções sistêmicas. Propor um mecanismo de armazenamento das credenciais biométricas, recuperação e identificação dos indivíduos através a comparação dos dados armazenados com os lido no momento do acesso é o primeiro passo do desenvolvimento de um Sistema integrado que faça uso de credenciais biométricas. Com a utilização de sensores biométricos e bibliotecas de terceiro é possível criar uma solução que seja expansível e integrável em um sistema completo, isolando completamente a parte de armazenamento e identificação biométrica das outras responsabilidades necessárias a um Sistema de Controle de Acesso.

Palavras Chave: Acesso - Biometria - Digital - NITGEN - Autenticação

1. INTRODUÇÃO

Em sistemas de informação, os mecanismos de controle de acesso, geralmente estão vinculados com verificação de autenticidade através de usuários e senhas, podendo também ser utilizados equipamentos eletrônicos que armazenem algoritmos específicos de criptografia contendo a identificação do usuário, que junto com uma senha garantirá a verificação da autenticidade.

No entanto, cada vez mais, características físicas são utilizadas como garantia de que o usuário identificado é realmente quem diz ser, tornando com isso a identificação do usuário mais segura.

O presente artigo abordará Sistemas de Controle de Acesso e suas influências no controle de segurança patrimonial e de informações, com ênfase nas responsabilidades e características necessárias que um sistema desse nível precisa possuir.

Abordará também a utilização da biometria da digital para identificação dos usuários, trazendo uma proposta para armazenamento e recuperação das identificações biométricas em banco de dados e utilização, com o FingKey Hamster da NITGEN, através da SDK (*Software Development Kit*) [NITGEN SDK] fornecida pelo fabricante em um programa escrito na linguagem C# utilizando a .NET Framework 3.5.

2. OBJETIVOS

O presente artigo visa identificar o que é e quais são as características de Sistemas de Controle de Acesso com foco em acesso físico utilizando credenciais biométricas, em especial a biometria da digital. Visa também propor uma estrutura de armazenamento e recuperação das credenciais biométricas utilizando C#, resolvendo com isso um dos principais problemas de um Sistema de Controle de Acesso que é identificar se o usuário efetivamente é quem ele diz ser.

3. SISTEMA DE CONTROLE DE ACESSO FÍSICO

> *"É um Sistema que permite ou não a entrada de um indivíduo ou objeto em determinados locais, em determinados horários, mediante sua identificação."* [SOUZA, 2010. p. 17]

Os Sistemas de Controle de Acesso podem ser lógicos (controle de acesso às informações, dentro de um sistema de informação) ou físicos (controle de acesso a áreas restritas, com delimitação de perímetros de segurança e áreas controladas).

Em indústrias, bancos e locais com altos valores agregados ou risco a saúde ou à vida é comum que existam restrições de acesso, não somente externo, mas também para o pessoal interno (da própria empresa).

Para fazer esse controle é necessário estabelecer perímetros de controle, com acesso isolado, partindo de partes mais externas para as mais internas, focando tanto a entrada dos indivíduos quanto a saída. Os perímetros, normalmente são delimitados e controlados por barreiras físicas e tecnologias de detecção. [SOUZA 2010, p. 17].

Sistemas de Controle de Acesso Físico tem como objetivo permitir que somente usuários autorizados tenham acesso aos seus respectivos ambientes, impedindo os não autorizados e visam automatizar o processo de verificação de acesso ou auxiliar nas tarefas relativas à proteção patrimonial. Para serem usados para autenticação, precisam de uma base de dados contendo informações de identificação e, para o nível de permissão, informações do que o usuário pode fazer. [PINHEIRO 2008, p. 23].

A preocupação com a identificação do indivíduo está diretamente ligada ao valor da informação ou do bem que poderá ser furtado/desviado, caso um acesso indevido seja realizado. De acordo com Pinheiro [PINHEIRO 2008, p. 16] o roubo de identidade afeta milhões de pessoas e vem sendo o tipo de fraude mais praticado em ambientes de rede e, por esse motivo, a autenticação é um item fundamental para a segurança.

Um Sistema de Controle de Acesso que tenha como característica a verificação da autenticidade do indivíduo e o nível de permissão de acesso que ele possui precisa verificar se ele é realmente quem diz ser e se ele tem permissão para fazer o que deseja fazer.

Segundo Silva [SILVA 2008, p. 7] a autenticação provê a garantia da identidade de um usuário, ou seja, é responsável por verificar se um requerente é quem ele diz ser, por meio de suas credencias, sendo que suas credencias são as evidências que um requerente apresenta para estabelecer sua identidade como um usuário válido e Pinheiro [PINHEIRO 2008, p. 16] complementa que a identificação é a função em que o usuário declara sua identidade ao sistema e a autenticação é a função responsável pela validação dessa declaração e que somente após a validação é que o sistema poderá conceder ou negar acesso.

Segundo Silva [SILVA 2008, p. 7], também defendido por Pinheiro [Pinheiro 2008 p. 17-21] mecanismos de autenticação se baseiam em três paradigmas: algo-que-você-sabe (senha de acesso, por exemplo), algo-que-você-tem (chaves, cartões de acesso e chaves criptográficas, por exemplo) ou algo-que-você-é (voz, impressão digital, retina, palma da mão e qualquer outra característica biométrica).

Os problemas identificados por Silva [SILVA 2008, p. 8] para a utilização de identificação por algo-que-você-sabe, estão identificados abaixo:

- As senhas são facilmente visualizadas, tanto diretamente quanto em seu meio de transporte, caso ele não seja criptografado;
- Um intruso pode penetrar em um computador do sistema e ler o arquivo de senhas;
- Alguém pode adivinhar uma senha mal escolhida;
- Um intruso pode quebrar uma senha, tentando exaustivamente, todas possíveis combinações ou palavras de um vocabulário.

Já, para algo-que-você-tem, que consiste basicamente em posses de chaves, cartões, carteiras e demais tokens de acesso, quando usado em conjunto com senhas podem prover um nível de segurança maior, no entanto, os tokens podem ser roubados ou copiados, não sendo também totalmente seguros.

Já algo-que-você-é, que consiste na biometria, provê a segurança da identidade de um requerente baseado em uma característica que ele possua e que seja mensurável, como comportamento ou sua morfologia.

Qualquer uma dessas técnicas sozinha, não provê garantia suficiente da identidade de um requerente, sendo necessário desenvolver um sistema de autenticação que possa utilizar mais de um tipo de evidência para provar sua identidade, como por exemplo, mesclar tokens com senhas ou tokens com características biométricas.

Uma das responsabilidades de um Sistema de Controle de Acesso é verificar o nível de Autorização que um usuário identificado possui no Sistema, nesse caso, um dos serviços de segurança que trata sobre isso é os Serviço de Autorização. Transpondo o que Silva [SILVA 2008, p. 9] defende sobre Sistemas de Segurança para Controle de Acesso Físico, onde é ressaltado que o objetivo da autorização é proteger contra o acesso não autorizado a uma informação ou recurso computacional, podemos dizer que isso também se aplica a uma área física restrita. E também, onde é ressaltado que um Sistema de Segurança requer uma fase inicial de autenticação para depois identificar o nível de acesso que o usuário possui e quais informações podem acessar também se aplica ao acesso físico, já que será necessário identificar a identidade do usuário e se o mesmo possuirá ou não acesso aquela área restrita.

Trazendo essas informações para Sistemas de Controle de Acesso Físico, que estão ligados, geralmente, a proteção patrimonial ou segurança individual/coletiva, os equipamentos utilizados variarão de acordo com o risco de danos ao patrimônio e riscos de danos a saúde ou a vida das pessoas, sendo que, quanto maior o prejuízo agregado ao acesso indevido, maior

será a quantidade de equipamentos e técnicas de verificação agregados para garantir que somente acesse quem deva acessar e que, quem esteja acessando, realmente seja quem diz ser.

4. BIOMETRIA

Biometria é uma palavra de origem grega, bios (vida) e metros (contagem ou medida) e é a ciência que estuda, estatisticamente, as características físicas, fisiológicas ou comportamentais dos seres vivos e atualmente é utilizada como forma de identificar indivíduos através dessas informações [LOURENÇO 2009, p. 13].

Os sistemas de informação, através de algoritmos estatísticos são capazes de, com algumas características biométricas, fazer o reconhecimento do indivíduo, com um grau de certeza aceitável, na maioria das vezes.

Pinheiro defende [PINHEIRO 2008, p. 37-39] o uso a biometria para resolver o problema de identificação, ou seja, para verificar a identidade através de características únicas usando-a, em Sistemas de Controle de Acesso, para a autenticação dos usuários, através de métodos automatizados que permitem autenticar, identificar ou verificar automaticamente a identidade de um indivíduo.

Segundo Lourenço [LOURENÇO 2009, p. 14] as características fisiológicas estão relacionadas com o organismo da pessoa, por exemplo, respiração, batimentos cardíacos por minuto e são variáveis de acordo com a situação do indivíduo. As comportamentais, ou dinâmicas, estão relacionadas ao comportamento, ou seja, a forma como o indivíduo interage com o ambiente e são extremamente voláteis e variáveis de acordo com a situação e tempo, como por exemplo, a assinatura, forma de digitação, jeito de andar, etc. Já as características físicas, são traços no corpo do indivíduo, relacionado com sua herança genética e variam pouco ou muito pouco no tempo, como a digital, ires e retina.

Segundo Lourenço [LOURENÇO 2009, p. 14], para serem utilizadas na identificação do individuo a característica biométrica deve satisfazer os seguintes requisitos:

- **Universalidade**: Todos os indivíduos devem possuir a característica que será utilizada;
- **Singularidade**: A característica tem que variar de um indivíduo para o outro, permitindo com isso identificá-lo;
- **Permanência**: A característica não deve variar no tempo ou variar de forma irrisória ou em tempo mensurável de forma que, de tempos em tempos, seja possível coletar a característica novamente;

- **Desempenho**: Precisão e agilidade com que a característica é processada para a identificação do indivíduo a ponto de atingir uma medição aceitável;
- **Aceitabilidade**: O dispositivo de leitura biométrica deve ser aceito pelos indivíduos;
- **Proteção**: O dispositivo de leitura biométrica e o Sistema de Informação responsável pelo armazenamento das credenciais devem possuir uma imunidade aceitável contra violações do sigilo da credencial e da criação de cópias biométricas aceitáveis.

5. BIOMETRIA DA DIGITAL

Segundo Boechat [Boechat 2008, p. 27] a impressão digital fornece uma universalidade média, ou seja, é bem disseminada entre os indivíduos, unicidade alta, ou seja, dificilmente existem duas iguais, permanência alta, ou seja, varia pouco no tempo, desempenho alto, ou seja, possuem algoritmos rápidos e eficiências para sua identificação, aceitação média, ou seja, a população a aceita, de modo geral e proteção média, ou seja, de certa dificuldade para cópia e fraudar um sistema que possua esse tipo de autenticação.

Com esses dados, chega-se a conclusão que a impressão digital não é um mecanismo totalmente seguro, no entanto, como a necessidade de proteção variará de acordo com a região a ser acessada e, em conjunto com outros mecanismos, como tokens e senhas para tornar a identificação dos usuários mais segura e como o universo de usuários que acessam uma área controlada em um ambiente determinado é limitado, foi definido que a digital era suficientemente segura para ser utilizada em um Sistema de Controle de Acesso.

As digitais possuem pequenos pontos chamados minúcias, que podem ser pontos de finalização de linha, pontos de junção de linha, quantidade de vales e sulcos, bifurcações, no entanto, essas características podem ser alteradas devido a fatores externos, como cortes, queimaduras ou por atrito, devido a atividades profissionais [Boechat 2008, p. 20].

Segundo Davide [DAVIDE 2009, p.99] Os setes tipos mais comuns de minúcias são:

Figura 1: Terminação de Crista (ridge ending)

Figura 2: Bifurcação (bifurcation)

Figura 3: Lago (lake)

Figura 4: Crista independente (independent ridge)

Figura 5: Ponto ou ilha (point or island)

Figura 6: Esporão (spur)

Figura 7: Cruzamento (crossover)

6. SISTEMA DE IDENTIFICAÇÃO BIOMÉTRICA ATRAVÉS DA IMPRESSÃO DIGITAL

Um Sistema de Controle de Acesso pode fazer uso da Biometria da Digital para identificar os indivíduos e, para isso, precisará armazenar dados de identificação para a autenticação.

O objetivo de um Sistema Biométrico é fornecer mecanismos para que seja possível, através das características do indivíduo, identificá-lo com um grau de certeza aceitável e, se utilizado de forma apropriada pode diminuir, consideravelmente, os problemas relacionados com a segurança. Um sistema biométrico consiste em um conjunto de hardware e software para o reconhecimento de padrões, que opera através da aquisição automática das informações biométricas, extraindo um modelo a partir dessas informações e esse modelo será armazenado e utilizado para as comparações, ou seja, em uma primeira fase, amostras da característica biométrica são recolhidas, transformadas em um modelo e armazenadas e, em uma segunda etapa, uma amostra da característica biométrica é recolhida e comparada com as previamente armazenadas para ser possível chegar na identidade do indivíduo. O processo de registro de perfil, também é conhecido como *enrollment*, e o processo de comparação, como *matching*. Os processos de validação por biometria possuem uma pontuação que define o grau de semelhança necessária entre o modelo armazenado e o modelo lido. Apesar de relativamente estáveis as características biométricas sofrem com a ação do tempo, da interação com o ambiente e com os equipamentos que fazem a coleta da amostra, então, mesmo para o mesmo indivíduo, não teremos amostras 100% iguais na maioria das vezes. [PINHEIRO, 2008, 43-46].

Segundo Lourenço [LOURENÇO 2009, p. 16] Um sistema que faça uso da biometria terá duas etapas distintas para que funcione, ou seja, uma etapa onde as características biométricas do grupo utilizador do sistema serão coletadas, conhecida como fase de registro e outra etapa onde essas características serão utilizadas para a identificação do usuário, conhecida como fase de autenticação.

O protótipo trabalhado no artigo possui as duas fases, a de captura e de autenticação, possuindo duas formas de autenticar, uma sem a utilização de um indexador e outra que precisa da identidade do usuário antes de autenticá-lo biometricamente, fornecendo um mecanismo de autenticação dupla. Em um ambiente real de controle de acesso, a autenticação dupla seria feita, primeiramente, por um token (crachá rf-id, cartão inteligente, chave criptográfica, etc), que serviria para buscar, através de índices, a identificação biométrica armazenada do usuário, fornecendo um mecanismo mais ágil e seguro de comparação.

O detalhamento do funcionamento do armazenamento e recuperação dos perfis biométricos está detalhado na **Figura 8**.

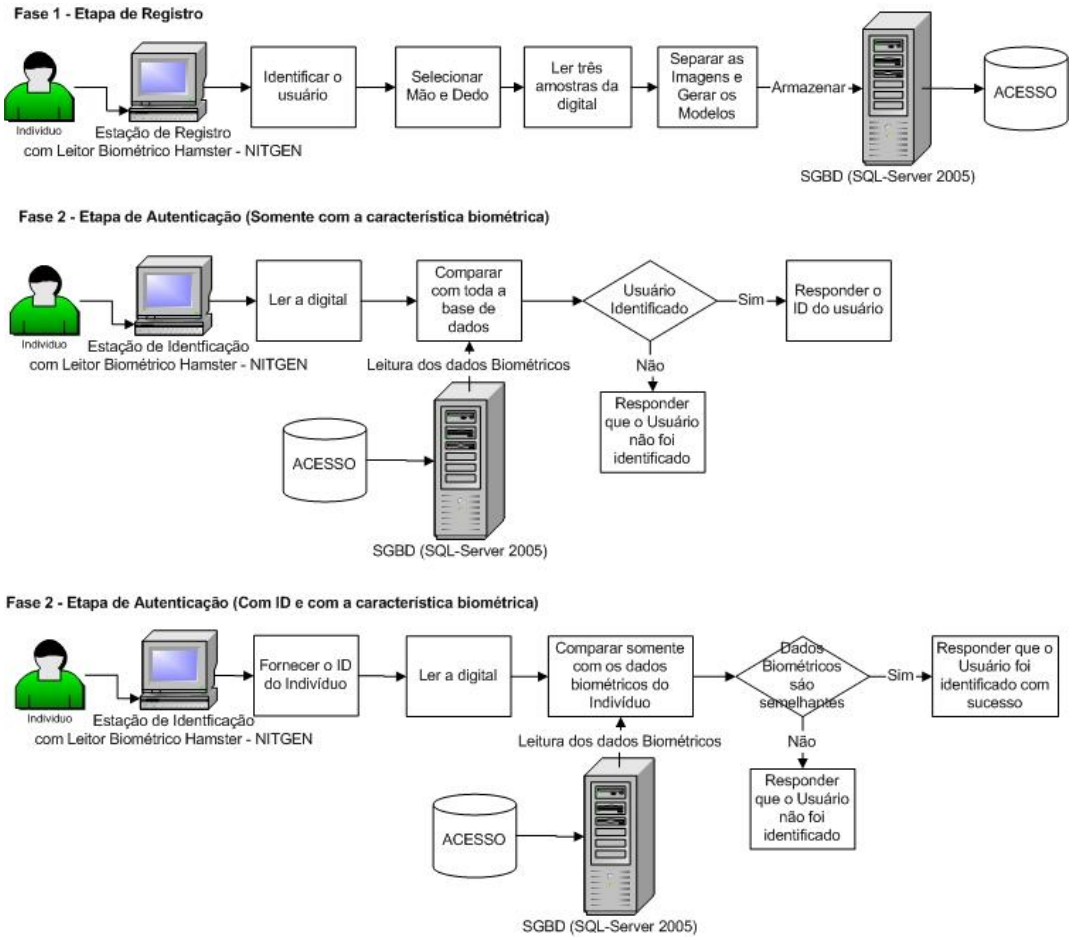

Figura 8: Detalhes de funcionamento do protótipo.

Para os testes do protótipo foram utilizados um notebook, com seu hardware e software detalhados na **Tabela 1**, o leitor HAMSTER HFDU04 da NITGEN e, para desenvolvimento do protótipo, Visual Studio 2008, utilizando a .NET Framework 3.5 com C# como linguagem de programação utilizando LINQ to SQL para acessar os dados e a SDK do FINGKEY Hamster da NITGEN [NITGEN SDK], fornecida pelo fabricante, para controlar o FINGKEY.

Tabela 1: Configuração da estação de testes

Notebook Sony Vaio modelo PCG-5K1L	
Hardware	Processador: Core 2 Duo 1,83Ghz Memória: 4gb Ram DDR2 HD sansung 7200 rpm de 250gbyte Monitor 14.1 polegadas
Programas Instalados	Windows Vista Home Premium Microsoft Visual Studio Professional 2008 .NET Framework 3.5 SDK do FINGKEY Hamster da NITGEN SQL-Server Express 2005

O protótipo de testes, desenvolvido em C# com a .NET Framework 3.5, separa a camada de dados da camada de aplicação, sendo que somente a camada de dados se comunicará com o SGBD SQL-Server 2005 e encontra-se ilustrado na **Figura 9**.

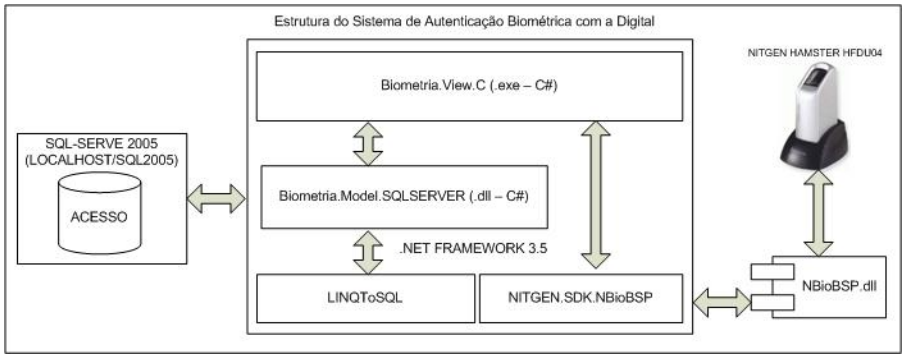

Figura 9: Estrutura do Protótipo de aquisição e autenticação com biometria da digital.

O protótipo possui as seguintes divisões:

- **Biometria.View.C**: Camada de aplicação, responsável pelo interfaceamento com o usuário final.
- **Biometria.Model.SQLSERVER**: Camada de dados, responsável pela comunicação com o banco de dados, isolando os detalhes de comunicação com os dados, fornecendo os objetos e métodos necessários para armazenamento e recuperação dos registros através de objetos;
- **LinqToSQL**: Mapeamento Objeto Relacional (MOR), responsável pela manipulação e persistência dos objetos no SGBD;
- **Localhost/SQLServer2005**: Instância do SQL-Server onde o banco de dados responsável pelo armazenamento dos modelos biométricos encontra-se;
- **NITGEN.SDK.NBioBSP**: Namespace de acesso as funcionalidades do FingKey Hamster da NITGEN através de .NET. É instalado junto com a SDK;

- **NBioBSP.dll**: componente responsável pela comunicação em si com o FingKey Hamster, fornecendo o interfaceamento entre o hardware e a biblioteca NITGEN.SDK.NBioBSP e pelo algoritmo de criação do modelo biométrico;
- **NITGEN HAMSTER HFDU04**: Hardware responsável pela aquisição do dado biométrico, responsável por fazer a leitura e digitalização da imagem da digital;

Para possibilitar o armazenamento das credenciais biométricas do grupo de indivíduos desejado, é necessário que exista o armazenamento em um banco de dados para futura utilização e sua estrutura está definida na **Figura 10**.

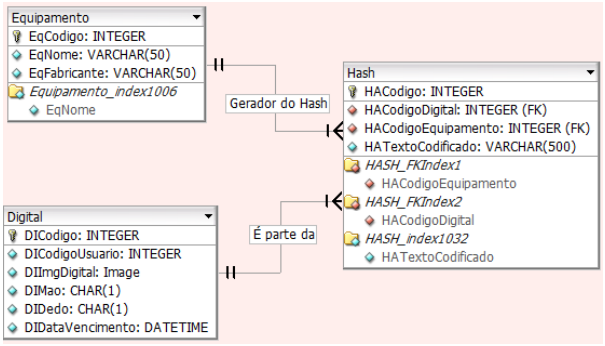

Figura 10: Estrutura do Banco de Dados de Armazenamento das Credenciais Biométricas

Como o modelo biométrico variará de acordo com a biblioteca e equipamento utilizado (algoritmo) e como o sistema está sendo planejado com o objetivo de ser extensível, uma tabela de equipamentos foi necessária para identificar qual equipamento gerou o modelo.

O modelo gerado é armazenado na tabela Hash, em forma de texto, de acordo com o equipamento.

Serão armazenadas três digitais para cada dedo que tiver seus dados biométricos recolhidos. O Sistema apresentado opta por armazenar a imagem da digital, para ser possível, se necessário, gerar novos modelos para outros equipamentos ou bibliotecas, caso sejam acrescidas novas funcionalidades ao sistema. As digitais são armazenadas com a identificação do usuário, da mão, do dedo e com uma data de vencimento, para obrigar, de tempos em tempos, os usuários recadastrarem seus dados biométricos.

As classes de dados responsáveis pela comunicação com o banco de dados, presentes no projeto **Biometria.Model.SQLSERVER** estão definidas na **Figura 11**.

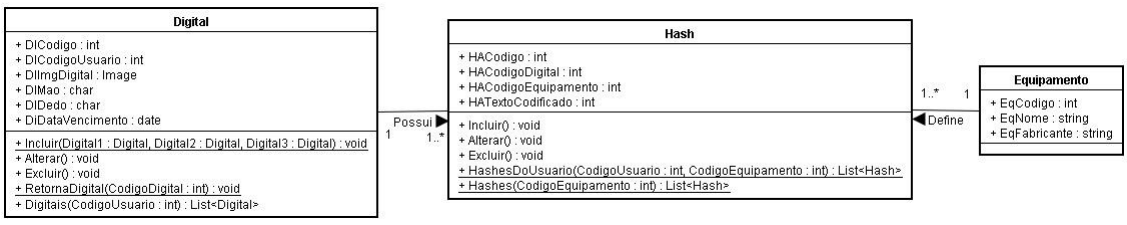

Figura 11: Estrutura das Classes de Dados

A camada responsável pela interface com o usuário final, também é responsável pela comunicação com o FINGKEY da Hamster e, para isso, uma classe de comunicação foi criada com a responsabilidade de isolar os códigos responsáveis pela utilização da SDK para aquisição e comparação dos modelos biométricos. A classe, ilustrada na **Figura 12**, encontra-se detalhada na **Tabela 2**.

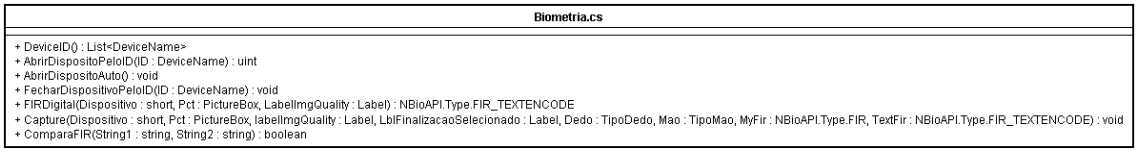

Figura 12: Classe responsável pela comunicação com o FINGKEY Hamster através da SDK

Tabela 2: Detalhamento da classe de Biometria

Biometria.cs	
Método	**Descrição**
DeviceID	Retorna a lista de hardware da NITGEN ligada no computador.
AbrirDispositivoPeloID	Abre o dispositivo de aquisição do dado biométrico pelo seu ID interno.
AbrirDispositivoAuto	Abre o dispositivo automaticamente. Método que deve ser utilizado somente quando houver um único dispositivo conectado a máquina.
FecharDispositivoPeloID	Fecha a comunicação com o hardware de aquisição do dado biométrico.
FIRDigital	Adquire um modelo biométrico da digital, sem se importar a qual dedo pertence.
Capture	Adquire um modelo biométrico da digital, com informações do dedo e da mão a qual pertence.
ComparaFIR	Compara dois modelos biométricos e retorna se eles pertencem ao mesmo indivíduo ou não.

A **Figura 13** ilustra a tela utilizada para a identificação do usuário, escolha do equipamento, mão e dedo que serão amostrados.

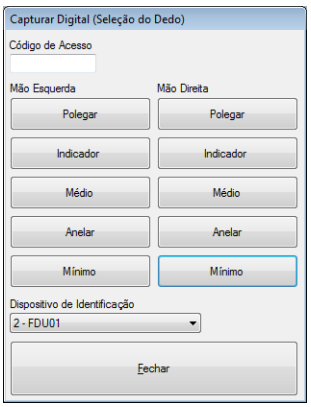

Figura 13: Tela de identificação da impressão digital que será coletada

Ao clicar em um dos botões que identifica um dos dedos, a janela de coleta das amostras da digital será acionada e possibilitará que as credenciais biométricas do dedo selecionado sejam coletadas e a tela, responsável por essa coleta, está ilustrada na **Figura 14**.

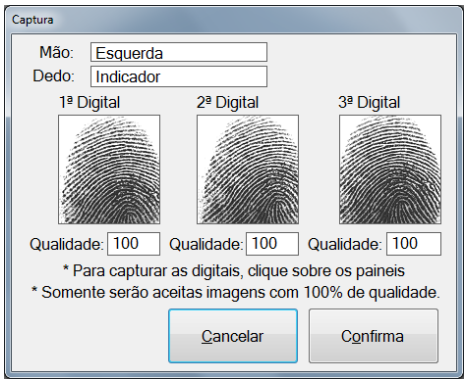

Figura 14: Tela de Captura da Identificação Biométrica

Ao clicar no botão salvar o sistema salva as imagens e os perfis biométricos criados para cada uma das amostras. O número de três amostras foi determinado para facilitar a identificação, já que, cada uma delas, por mais semelhante que sejam, são diferentes devido à posição e angulação do dedo no leitor.

A etapa de identificação do usuário, para Sistemas mais simples onde o a informação não tenha grande valor ou onde a área a ser acessada não necessite de um controle físico rigoroso, somente o método de autenticação biométrica pode ser utilizado. Essa solução tornou-se comum em academias de ginástica, que possuem uma catraca que somente é liberada após o usuário identificar-se e no registro de pontos de empregados. No entanto, quando o grupo de usuários for muito grande ou quando as informações ou área a ser acessada poderão, potencialmente, causar um grande prejuízo quando acessado por um indivíduo não autorizado, um mecanismo de autenticação mesclado será necessário.

O objetivo das telas desenvolvidas foi permitir tanto a identificação a partir da digital bruta, sem nenhuma identificação de usuário, que é muito mais lenta, já que o perfil biométrico criado pela autenticação precisará ser comparado com toda a base armazenada ou, com um pré-filtro, através do código do usuário, identificação essa que viria de algum outro token (normalmente um cartão) que o identificaria como único, no banco de dados e traria somente os perfis biométricos armazenados para ele, tornando a identificação muito mais ágil, já que os dados serão localizados no banco de dados através de índices, não sendo necessário fazer a leitura de todas as informações.

A **Figura 15** ilustra a tela que faz a comparação com toda a base de perfis biométricos e retorna o código do usuário, de acordo com a digital fornecida ou uma mensagem de erro, se não encontrar a credencial.

Figura 15: Autenticação com verificação de toda a base.

A **Figura 16** ilustra a tela que faz o rastreamento com a utilização da identificação do usuário. Essa identificação, em um sistema completo, viria de um segundo método de autenticação que precederia a identificação biométrica.

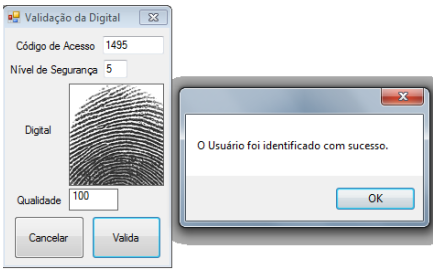

Figura 16: Identificação Biométrica com o auxílio da ID do Usuário.

7. RESULTADOS ENCONTRADOS

Através desse protótipo foi possível cadastrar os dedos e as identificações biométricas e os testes foram feitos com 100 pessoas, totalizando 1000 identidades biométricas, com 10 testes para cada digital, com menos de 1% de falsa rejeição e 100% de rejeição verdadeira, caracterizando com isso uma solução viável de ser adaptada para um sistema real de controle de acesso.

8. CONCLUSÃO

O Artigo teve o direcionamento e a preocupação de demonstrar uma forma eficiente de armazenar e recuperar as credenciais biométricas utilizando os leitores biométricos NITGEN – HAMSTER e, por analogia, essa mesma solução, com as devidas adaptações, pode ser utilizada para outros leitores de outros fabricantes, ou até mesmo com um algoritmo próprio para geração do perfil biométrico.

Criar um mecanismo de armazenamento e recuperação das credenciais biométricas é uma das grandes necessidades de um Sistema de Controle de Acesso que faça uso da biometria e a utilização de leitores e bibliotecas de terceiros facilitam essa atividade, permitindo que a complexidade do algoritmo de geração e validação das credenciais biométricas fique por conta do fabricante do componente.

É importante frisar que, para garantir a segurança na autenticação de um Sistema de Controle de Acesso, devem-se utilizar mais de um mecanismo além da biometria, como senhas e tokens e que esse tipo de sistema possui outras responsabilidades, além da autenticação como controlar as rotas e perímetros e quais níveis de acesso cada indivíduo possui.

9. REFERENCIAS

[PINHEIRO 2008] Pinheiro, José Maurício. Biometria nos Sistemas Computacionais. 1ª Edição. Ciência Moderna, 2008. ISBN: 978-85-7393-738-1

[SILVA 2008] Silva, Luis Gustavo Cordeiro, et al. Certificação Digital - Conceitos e Aplicações. Editora Ciência Moderna, 2008. ISBN: 978-85-7393-655-1.

[LOURENÇO 2009] Lourenço, Gonçalo Filipe da Fonseca (Novembro 2009). Dissertação de Mestrado - Reforço da Segurança das Biométricas utilizando Codificação de Fonte Distribuída. Instituto Superior Técnico da Universidade de Lisboa. Lisboa, Portugal.

[Boechat 2008] Boechat, G. (Fevereiro 2008). Dissertação de Mestrado - Proposta de um modelo de arquitetura biométrica para identificação pessoal com estudo da dinâmica da digitação, Universidade Federal de Pernambuco. Recife, Brasil.

[DAVIDE 2009] Maltoni, Davide, et al. (2009). Handbook of Fingerprint Recognition. Second Edition. Editora Springer. ISBN 978-1-84882-253-5

[NITGEN SDK] SDK do FINGKEY Hamster da NITGEN. http://www.nitgen.com.br/download/eNBSP_SDK_v4.zip, acessada em 06/05/2011.

[SOUZA 2010] Souza, Marcelo Barboza. Controle de Acesso: Conceitos, Tecnologias e Benefícios. 2010. Editora Sicurezza.