Perquirere, 12 (2): 127-141, dez. 2015

http://perquirere.unipam.edu.br

Aplicação de reconhecimento biométrico por meio de impressão digital no Centro Universitário de Patos de Minas

Application of biometrics recognition based on fingerprint on Centro Universitário de Patos de Minas

Anderson Luís de Sousa Ferreira
Graduando do curso de Sistemas de Informação (UNIPAM).
E-mail: andersonls@unipam.edu.br

José dos Reis Mota
Professor orientador (UNIPAM).
E-mail: josereis@unipam.edu.br

Resumo: Este trabalho apresenta um sistema biométrico baseado em impressão digital, a ser utilizado no Centro Universitário de Patos de Minas (UNIPAM), em situações que necessitem de segurança no reconhecimento de pessoas, como nos processos seletivos para ingresso na instituição e no registro de frequência dos alunos. A implantação do sistema permitiu o registro da impressão digital e a captura de fotos dos candidatos do curso de Medicina no vestibular do ano de 2014, sendo que os dados registrados foram verificados no momento da matrícula, garantindo segurança e credibilidade à instituição. Em relação à aplicação do registro de frequência, foram efetuados testes para verificar sua viabilidade. Espera-se utilizar o sistema em processos críticos da instituição que necessitem de autenticação, garantindo segurança e informações confiáveis para a tomada de decisão.
Palavras-chave: Segurança. Biometria. Impressão Digital.

Abstract: This article shows a biometric system based on fingerprint, that will be used at Centro Universitário de Patos de Minas (UNIPAM), in situations that require security in the recognition of people, as in selection processes for entry into the institution and the students attendance register . The system implementation allowed the fingerprint's registration and pictures taken of the medical school candidates in the entrance exam of 2014, and the data recorded were checked at the time of enrollment, ensuring security and credibility to the institution. Regarding the implementation of the attendance record, testes were carried out to verify its viability. It is expected to use the system for critical processes of the institution that require authentication, ensuring safety and reliable information for decision making.
Keywords: Security. Biometrics. Fingerprint.

---

1 INTRODUÇÃO

Com a utilização cada vez maior de tecnologias de informação e comunicação, surgem problemas relacionados à segurança, em particular, à questão da autenticação e

identificação do utilizador. Essa questão é, hoje, fundamental, já que o acesso indevido à informação ou a ausência de informações confiáveis pode provocar sérios prejuízos a uma organização.

Conforme Thian (2001), o problema de estabelecer uma associação entre um indivíduo e sua identidade pode ser dividido em duas categorias: autenticação e identificação. Autenticação refere-se ao problema de confirmar ou negar uma alegada identidade de um indivíduo, enquanto identificação é o estabelecimento de uma associação entre um indivíduo e identidade.

Os processos tradicionais de gerenciamento de identidade, por meio de senhas ou cartões de identificação, apresentam problemas, pois podem ser fraudados, perdidos ou esquecidos. Como forma de se garantir a segurança no gerenciamento de identidade e evitar os problemas dos métodos tradicionais, destaca-se o reconhecimento biométrico, feito com base nas características físicas ou comportamentais de uma pessoa.

Dentre os métodos utilizados para biometria, o reconhecimento por meio da impressão digital, atualmente, possui um nível de aceitação alto devido ao fato de não ser um método invasivo, possuir um bom nível de segurança, um custo baixo de equipamentos e poder ser utilizado em todos os tipos de aplicações para autenticação.

Assim, este trabalho descreve o desenvolvimento de um sistema para reconhecimento biométrico por meio de impressões digitais, utilizado no Centro Universitário de Patos de Minas, especialmente em processos seletivos para ingresso de alunos, nos quais é necessário proporcionar legitimidade ao processo, evitando fraudes e, consequentemente, garantindo a credibilidade da instituição.

Espera-se que, com o desenvolvimento do sistema de reconhecimento biométrico, além de solucionar os problemas mencionados anteriormente relacionados à segurança e identificação, que ele possa ser utilizado em outras situações, como no registro de frequência de alunos, visando à melhoria nos processos internos do Centro Universitário de Patos de Minas. Este trabalho contribui também nesse aspecto, propondo sua utilização no registro de frequência e em outros processos internos da instituição.

Então, o objetivo geral deste trabalho foi modelar e desenvolver um sistema para reconhecimento biométrico por meio de impressão digital para o Centro Universitário de Patos de Minas (UNIPAM) e utilizá-lo em processos internos da instituição em que é necessário verificar a autenticidade dos usuários, como em processos seletivos para ingresso de alunos e no registro de frequência dos discentes. Para a consecução desse objetivo, foram ainda percorridos outros, quais sejam: pesquisar sobre a utilização de recursos de biometria em instituições de ensino; pesquisar e avaliar diferentes kits de desenvolvimento de *software* (SDKs) para sistemas biométricos, selecionando um para desenvolvimento do sistema proposto; avaliar e selecionar equipamentos necessários para a implantação de um sistema biométrico, comparando custo e benefício dos mesmos para cada situação em que serão aplicados; modelar e desenvolver um sistema para a realização de reconhecimento biométrico que permita o registro das impressões digitais e a posterior verificação da autenticidade do usuário; desenvolver um sistema biométrico que facilite o reuso, de forma que outras aplicações possam utilizar suas funcionalidades quando necessário; testar o sistema em

um projeto piloto relacionado à frequência dos discentes da instituição, analisando procedimentos para tornar o processo mais eficiente, e outro relacionado ao processo seletivo para ingresso de alunos, simulando o registro das digitais dos candidatos de uma sala.

O UNIPAM disponibiliza aos professores e alunos diversos sistemas que suportam todos os processos inerentes às atividades de ensino e às demais atividades da instituição. Para acesso a essas ferramentas, é necessário que os usuários utilizem técnicas para sua identificação que se baseiam, atualmente, em usuário e senha. Além disso, a instituição realiza diversos eventos, como o processo seletivo para ingresso de alunos, em que é necessária a confirmação da identidade do candidato, que era feita apenas com base em documentos de identificação. Tanto a primeira forma de autenticação, baseada na utilização de códigos memorizados, quanto a segunda, baseada no porte de documentos pessoais, podem ser fraudados, roubados, repassados a outras pessoas ou simplesmente esquecidos.

Nesse contexto, a adoção de uma nova forma de identificação baseada no reconhecimento biométrico, que foi a proposta deste trabalho, possibilitou ao UNIPAM solucionar vários problemas relacionados à segurança e identificação. Dentro desse cenário destacam-se os seguintes pontos:

- evitar fraudes nos processos seletivos (vestibulares), garantindo a segurança no processo e a credibilidade da instituição;
- realizar a frequência dos discentes, otimizando o tempo do professor, que poderá dedicar-se melhor à prática de ensino, e ainda garantindo que a frequência seja realizada corretamente, possibilitando assegurar a presença ou a ausência do aluno e, dessa forma, permitir que a instituição, por meio do Núcleo Docente Estruturante (NDE) dos cursos, tenha acesso às informações e intervenha ao notar a ausência consecutiva de alunos, diminuindo a evasão.

Além dos pontos destacados, o sistema de reconhecimento biométrico poderá auxiliar a instituição em outros processos em que seja necessário garantir a presença e a autenticidade de pessoas, por exemplo:

- registro de participação em eventos e minicursos realizados pela instituição;
- registro de ponto para professores, feito, atualmente, por meio de registro em folhas de ponto.
- acesso aos laboratórios e à biblioteca da instituição, verificando se a pessoa realmente pertence à comunidade acadêmica do UNIPAM ou ao corpo técnico-administrativo e impedindo acesso indevido.

Assim, além de proporcionar segurança a alguns processos fundamentais, o sistema de identificação biométrica desenvolvido pode auxiliar no levantamento de um conjunto de informações confiáveis que auxiliarão os processos de tomada de decisão na instituição, o que justifica o seu desenvolvimento.

2 REVISÃO DE LITERATURA

Nesta seção, são apresentados conceitos referentes ao reconhecimento biométrico que foram importantes para o desenvolvimento desse trabalho.

4.1 RECONHECIMENTO BIOMÉTRICO

Um dos maiores problemas enfrentados atualmente em termos de segurança em computação é a autenticação de usuários, que implica em garantir que a pessoa que está tentando acessar um sistema é quem ela realmente diz ser.

A autenticação de um usuário pode ser feita a partir de informações que o usuário conhece como senhas ou a partir de dispositivos que o usuário possua como cartões magnéticos, códigos de barras ou chaves. Em todos os casos citados, os dispositivos de autenticação podem ser perdidos ou roubados.

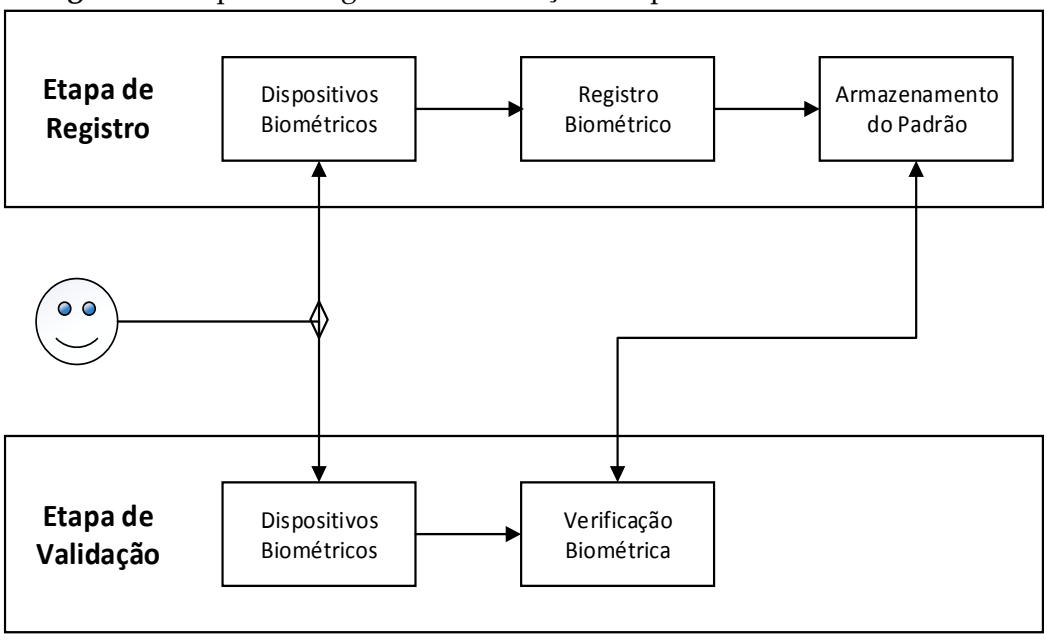
A biometria propõe-se a solucionar esse problema, pois, ao contrário das outras técnicas, ela se baseia em informações obtidas nas características físicas ou comportamentais de uma pessoa, dificultando o processo de fraude. Assim, técnicas de autenticação baseadas em características biométricas, como impressões digitais, exames de retina e da palma das mãos, vêm sendo cada vez mais utilizadas para garantir a autenticidade dos usuários.

Segundo Fernandes e Plinio (2006), biometria é o conjunto de métodos automatizados para reconhecer uma pessoa com base em características comportamentais ou fisiológicas. São exemplos de características comportamentais: escrita manual, assinatura, gestos. São exemplos de características físicas: face, impressões digitais, geometria da mão, íris.

Conforme exposto em Liu et al. (2001), existem, hoje, muitas características utilizadas isoladamente ou em conjunto para autenticar e/ou identificar um sujeito. Cada um dos métodos pode ser avaliado por meio de vários parâmetros: grau de fiabilidade, nível de conforto, nível de aceitação e custo de implementação.

Tipicamente, o processo de uso de tecnologias biométricas passa por duas etapas bem definidas, o registro e a validação, conforme mostrado na Figura 1.

Figura 1 - Etapas de Registro e Verificação dos processos biométricos



Fonte: autoria própria

- Etapa de Registro: consiste na captura e armazenamento do *template* de uma impressão digital por meio de algum dispositivo biométrico. O *template* armazenado possibilita futuras consultas na base de dados.
- Etapa de Validação: a partir de registros arquivados, o usuário do sistema realiza a validação de sua impressão digital, quando é comparada sua impressão digital com a impressão digital armazenada na etapa de registro. Se consideradas compatíveis, a identidade é válida e o usuário terá acesso à aplicação ou ao recurso desejado.

O reconhecimento biométrico baseia-se nas características e comportamentos de uma pessoa e pode ser feito de diversas formas. Conforme Prahbakar, Pankanti e Jain (2003), a autenticidade de um sistema biométrico dependerá da precisão do mesmo. Considerando que se forem realizados ataques de força bruta, em que há uma precisão baixa (em torno de 0.001 por cento de precisão), seriam necessárias 100.000 tentativas para que algum ataque pudesse ser bem sucedido. Ou seja, a garantia de autenticidade em sistemas biométricos é considerada alta.

Conforme Canedo (2014), existem duas tecnologias de reconhecimento biométrico: uma denominada verificação ou (1:1) – um contra um – e outra chamada de identificação ou (1:N) – um contra N. Os sistemas biométricos de verificação apenas comparam dois *templates* e determinam se eles são, de fato, da mesma pessoa. Normalmente, um dos *templates* está gravado em banco de dados enquanto o outro é adquirido ao vivo. Os sistemas biométricos de identificação comparam um *template* com todo o banco de dados e retorna a identidade da pessoa, se ela foi encontrada no banco de dados. A identificação tem a vantagem de identificar a pessoa, independente de quem a pessoa diz ser. Por outro lado, a verificação é muito mais simples e requer muito menos poder computacional. Fazer identificação em bases de dados grandes exige muitos recursos computacionais, podendo comprometer o desempenho do sistema.

Existem várias formas de se realizar o reconhecimento biométrico, como aquela baseada nas características faciais. Segundo Jain, Ross e Nandakumar (2011), a face é a porção frontal da cabeça humana estendendo-se a partir da testa ao queixo e inclui a boca, nariz, bochechas e olhos. O processo de reconhecimento automatizado de rostos possui uma série de desafios. Imagens da face de uma pessoa podem ter variações de acordo com a idade, a pose, a iluminação e as expressões. Além disso, pode haver semelhanças entre a face de pessoas diferentes, especialmente se elas estão geneticamente relacionadas (por exemplo, gêmeos idênticos, pai e filho). Essas semelhanças agravam a dificuldade de reconhecer as pessoas com base em seus rostos.

Ainda de acordo com Jain, Ross e Nandakumar (2011), no caso da autenticação biométrica por impressões digitais, o dispositivo de captura capta e analisa padrões na pele da ponta dos dedos, gerando um padrão biométrico baseado em uma das principais abordagens utilizadas: casamento de minúcias (método policial), casamento de padrões retilíneos, padrões moiré ou uso de ultrassom.

A impressão digital é considerada uma marca única e imutável, mesmo lesões e hematomas podem alterá-la apenas temporariamente, devido a capacidades regenerativas da epiderme. O desenho digital de uma criança, por exemplo, sofre apenas uma alteração de tamanho em função de seu crescimento, de forma semelhante

a uma ampliação fotográfica.

Essas características favorecem a utilização de impressões digitais para a autenticação em aplicações. Além disso, graças aos avanços em mecanismos de autenticação biométrica, seus dispositivos se tornaram pequenos e de baixo custo e podem gerar rapidamente imagens biométricas para análise e comparação.

O sistema a ser desenvolvido terá como base, portanto, o reconhecimento biométrico por meio de impressões digitais, devido aos motivos descritos anteriormente e confirmados por Fernandes e Plinio (2006), que acrescentam que algumas das vantagens do uso da autenticação biométrica por impressões digitais, quando comparada com outras formas de autenticação biométrica, são baixo custo do hardware, boa confiabilidade, tamanho reduzido dos dispositivos de captura e fácil integração dos dispositivos com a aplicação.

4.2 SCRUM

Conforme Schwaber e Sutherland (2013), Scrum é um processo de desenvolvimento de *software* ágil que permite a mudança de requisitos durante todo o ciclo de desenvolvimento e baseia-se em uma constante colaboração entre os desenvolvedores de software e os clientes. O desenvolvimento do *software* ocorre com a separação do produto final esperado em partes, em que cada parte é desenvolvida e entregue separadamente. Dessa forma, é possível responder e adaptar o *software* com as avaliações dos clientes em cada entrega.

No Scrum, os projetos são desenvolvidos a partir de uma série de iterações chamadas *sprints*. O tempo para cada *sprint* é definido pela equipe de desenvolvimento, que se reúne com o cliente ou proprietário do produto antes de cada *sprint*, para decidir o que será feito durante a *sprint* em questão, selecionando as tarefas que a equipe completará ao fim dessa iteração. Existem reuniões de acompanhamento diárias. Nessas reuniões, que são preferencialmente de curta duração (aproximadamente quinze minutos), são discutidos pontos como o que foi feito desde a última reunião e o que precisa ser feito até a próxima. As dificuldades encontradas e os fatores de impedimento são identificados e resolvidos.

O ciclo de vida da *Scrum* é baseado em três fases principais, divididas em subfases:

- Pré-planejamento (*pre-game phase*): os requisitos são descritos em um documento chamado *backlog*. Posteriormente, eles são priorizados e são feitas estimativas de esforço para o desenvolvimento de cada requisito. O planejamento inclui também, entre outras atividades, a definição da equipe de desenvolvimento, as ferramentas a serem usadas, os possíveis riscos do projeto e as necessidades de treinamento. Finalmente, é proposta uma arquitetura de desenvolvimento. Eventuais alterações nos requisitos descritos no *backlog* são identificadas, assim como seus possíveis riscos.
- Desenvolvimento (*game phase*): as muitas variáveis técnicas e do ambiente identificadas previamente são observadas e controladas durante o desenvolvimento. Ao invés de considerar essas variáveis apenas no início do projeto, como no caso das metodologias tradicionais, no Scrum o controle é feito

continuamente, o que aumenta a flexibilidade para acompanhar as mudanças. A cada ciclo, ou *sprint*, novas funcionalidades são adicionadas. Cada um desses ciclos é planejado para durar de uma semana a um mês.

- Pós-planejamento (*post-game phase*): após a fase de desenvolvimento são feitas reuniões para analisar o progresso do projeto e demonstrar o *software* atual para os clientes. Nessa fase, são feitas as etapas de integração, testes finais e documentação.

No caso do sistema proposto tendo em vista um acompanhamento mais próximo do projeto, o processo de pesquisa e desenvolvimento será baseado nos conceitos do Scrum, ou seja, serão levantados os requisitos do projeto e ciclos iterativos para a conclusão de cada etapa planejada anteriormente.

3 METODOLOGIA

A metodologia de pesquisa deste trabalho foi aplicada e experimental, já que utilizou conhecimento científico e prático, referentes à segurança e à biometria, para o desenvolvimento de um novo produto, mais especificamente um produto de *software*, utilizando o processo de desenvolvimento SCRUM. Além disso, o objetivo final do trabalho contemplou também a implantação do sistema no Centro Universitário de Patos de Minas em processos seletivos para ingresso de alunos e testes referentes ao registro de frequência.

Inicialmente, foi feito um estudo bibliográfico sobre reconhecimento biométrico, os diferentes tipos de sistemas biométricos e em que situações utilizá-los. Logo em seguida, também foi feita uma análise de *kits* de desenvolvimento de *software* (SDKs) para desenvolvimento de sistemas biométricos existentes no mercado, gratuitos e/ou pagos, levando-se em consideração os recursos que cada um possui e os custos envolvidos em sua aquisição. Como uma SDK gratuita acompanha os equipamentos para captura das impressões digitais, optou-se por sua utilização. Os recursos disponíveis na SDK estão descritos em seu NITGEN (2011).

Foram comparados, ainda, diferentes tipos de equipamentos para realização da captura e verificação de impressões digitais, levantando-se os recursos e custos de diferentes modelos, para selecionar o modelo mais adequado e com melhor custo/benefício para as situações em que serão utilizados na instituição.

Optou-se pelo modelo Hamster III DX, por apresentar o melhor custo/benefício, já que, apesar de ser um dispositivo simples, que não captura digital rolada, por exemplo, garante um alto grau de segurança, dificultando fraudes, pois consegue diferenciar entre tecido vivo e tecido morto. Dessa forma, o equipamento impede tentativas de fraudes como as cópias de silicone ou o uso de moldes de dedos.

Como se pretendia utilizar o sistema inicialmente nos processos seletivos para ingresso de alunos, em novembro de 2014, foi feito um levantamento, com base no último vestibular, de quantas salas foram alocadas, considerando que em cada sala será necessário um equipamento para captura das impressões digitais. No último processo seletivo, foram confirmadas 2.644 inscrições apenas para o curso de Medicina,

totalizando 53 salas. Para todos os cursos, foram 6.842 inscrições, totalizando 136 salas[1].

Em relação à frequência pretendia-se fazer um levantamento sobre o custo para o registro, considerando também um equipamento por sala e o número de salas ocupadas e considerando, ainda, que os equipamentos adquiridos para o processo seletivo podem também ser utilizados para o registro de frequência. No entanto, há outros fatores limitantes para a implantação do registro de frequência, como descrito nos resultados e na conclusão do trabalho.

Foram analisadas, ainda, outras situações e formas de se empregar o sistema de identificação biométrica no UNIPAM, para posterior desenvolvimento e implantação de processos, como em registro de participação de eventos e no acesso aos laboratórios de informática e a outras dependências da instituição.

A modelagem do sistema e a definição do projeto foram feitas levando-se em consideração a utilização do sistema por outras aplicações que necessitam de reconhecimento biométrico. Para facilitar essa reutilização, as funcionalidades presentes no sistema foram disponibilizadas por meio de serviços web.

Durante todo o processo de desenvolvimento, foi feito um desenvolvimento iterativo, baseado no Scrum, definindo-se o *backlog* do produto e os itens implementados em cada *sprint*. Ao final de cada *sprint* as funcionalidades desenvolvidas eram testadas e acopladas ao *software*.

Após o desenvolvimento do sistema, foram feitos os testes iniciais, a partir de um projeto piloto para cada situação. Para o processo seletivo, foi simulada a captura das impressões digitais de candidatos de uma sala, ocasião em que será cronometrado o tempo gasto para esse procedimento. Para o processo de frequência, o tempo para captura das impressões digitais não é fator preponderante, já que pode ser feito a qualquer momento; o fator mais relevante nessa situação é o tempo gasto para verificação das digitais armazenadas a fim de efetuar o registro das faltas. Da mesma forma que o tempo gasto será cronometrado para o processo seletivo, isso foi feito também para o processo de frequência.

O sistema foi implantado com antecedência para a realização das provas do processo seletivo para ingresso em 2015, sendo instalado em computadores de 70 salas de aula que receberam os candidatos de Medicina. Posteriormente, foi instalado em outras dependências da instituição.

4 RESULTADOS

Para facilitar o reuso e garantir a segurança no acesso ao banco de dados, as funcionalidades foram desenvolvidas utilizando-se serviços web. Até o momento, foram implementados os seguintes serviços web, que podem ser utilizados por qualquer aplicação que necessite de reconhecimento biométrico:

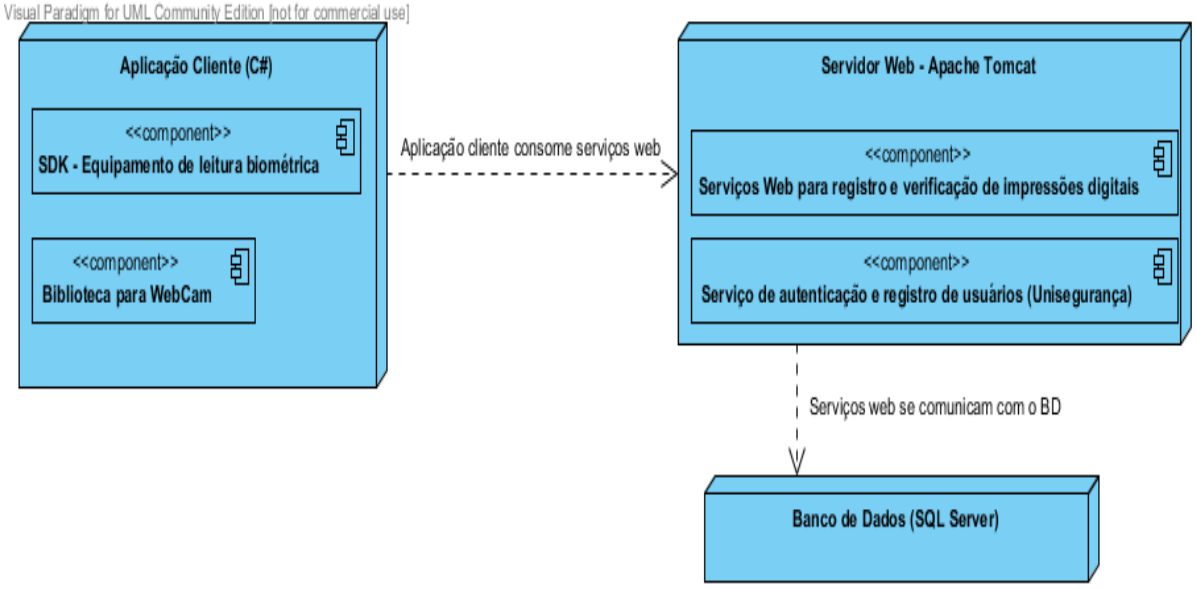
- BuscarCandidatoPorInscricao: para buscar o candidato para o qual será registrada a digital.

[1] Como descrito nos resultados deste trabalho, o número de candidatos para o curso de Medicina foi maior no vestibular de 2014 para ingresso em 2015, mas não houve problemas no registro das impressões digitais.

- BuscarCandidatosPorNome: para buscar uma lista de candidatos pelo nome.
- RegistrarDigital: serviço genérico utilizado na primeira etapa da biometria, ou seja, para o registro dos *templates*.
- VerificarDigital: serviço genérico utilizado para a verificação biométrica (1:1).
- IdentificarPessoa: serviço genérico utilizado para a identificação biométrica (1:N).

Na Figura 2, é detalhada a arquitetura da aplicação com foco nos componentes utilizados. Percebe-se, na Figura 4, que a aplicação cliente utiliza os serviços web e não se comunica diretamente com o banco de dados. Para garantir a segurança, toda a comunicação será feita por meio dos serviços, ou seja, não é necessário liberar acesso direto ao servidor de banco de dados. A aplicação utiliza, ainda, um serviço de autenticação para vincular os usuários que utilizarão o sistema (Unisegurança). Existe, ainda, a opção de acesso com ou sem *proxy*, já que os usuários do Centro Universitário de Patos de Minas utilizarão usuário e senha de *proxy* para acesso à internet.

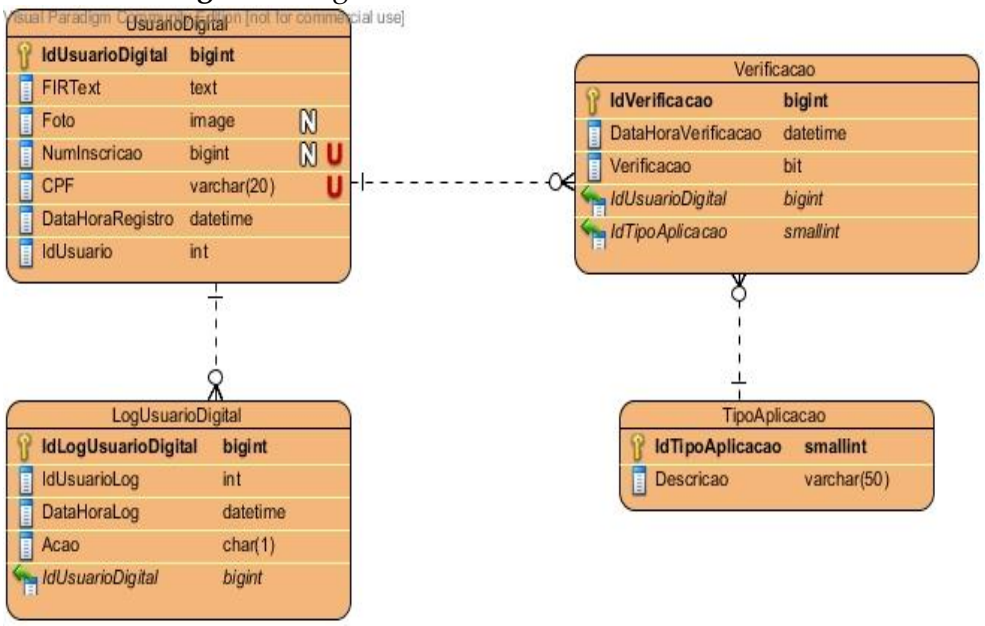
Figura 2 Arquitetura do Sistema Biométrico



Fonte: autoria própria

O Digrama de Entidade e Relacionamento detalha como é a estrutura de armazenamento das informações inerentes aos processos biométricos, como mostra a Figura 3.

Figura 3 Diagrama de Entidade e Relacionamento



Fonte: autoria própria

A Tabela UsuarioDigital armazena as informações biométricas do candidato, o campo NumInscricao vincula o aluno à sua inscrição do vestibular. Armazenam-se, ainda, a data e a hora de registro da digital e qual o usuário realizou a coleta. Vale destacar as seguintes características dessa tabela:

- FIRText: para armazenar os *templates* da impressão digital. O sistema registra os dados das digitais nesse campo.
- Foto: foi armazenada uma foto para cada um dos candidatos do vestibular, como mais uma medida de segurança para garantir a identificação da pessoa de quem foi armazenada a digital no momento da matrícula.
- CPF: o sistema terá como base o registro do CPF. Por meio dessa informação, será possível vincular a pessoa tanto no processo seletivo quando no registro de frequência ou a outros processos e sistemas que possam necessitar de reconhecimento biométrico.

Na tabela LogUsuarioDigital, fica armazenado todo o registro de alterações referentes às coletas de impressões de digital, ou seja, se algum usuário realizar uma alteração indevida em uma digital, ficará armazenada nessa tabela para verificação posterior. Foi implementada uma barreira no momento da matrícula para que apenas candidatos que não fossem do curso de Medicina pudessem ser registrados, para evitar uma possível atualização de dados e a consequente perda das informações biométricas dos candidatos de Medicina.

Na tabela de Verificacao, ficará salvo todo o tipo de reconhecimento realizado[2], registrando a data de identificação, o usuário que foi identificado e o tipo de aplicação, informando se é um registro de verificação de frequência ou vestibular. À medida que

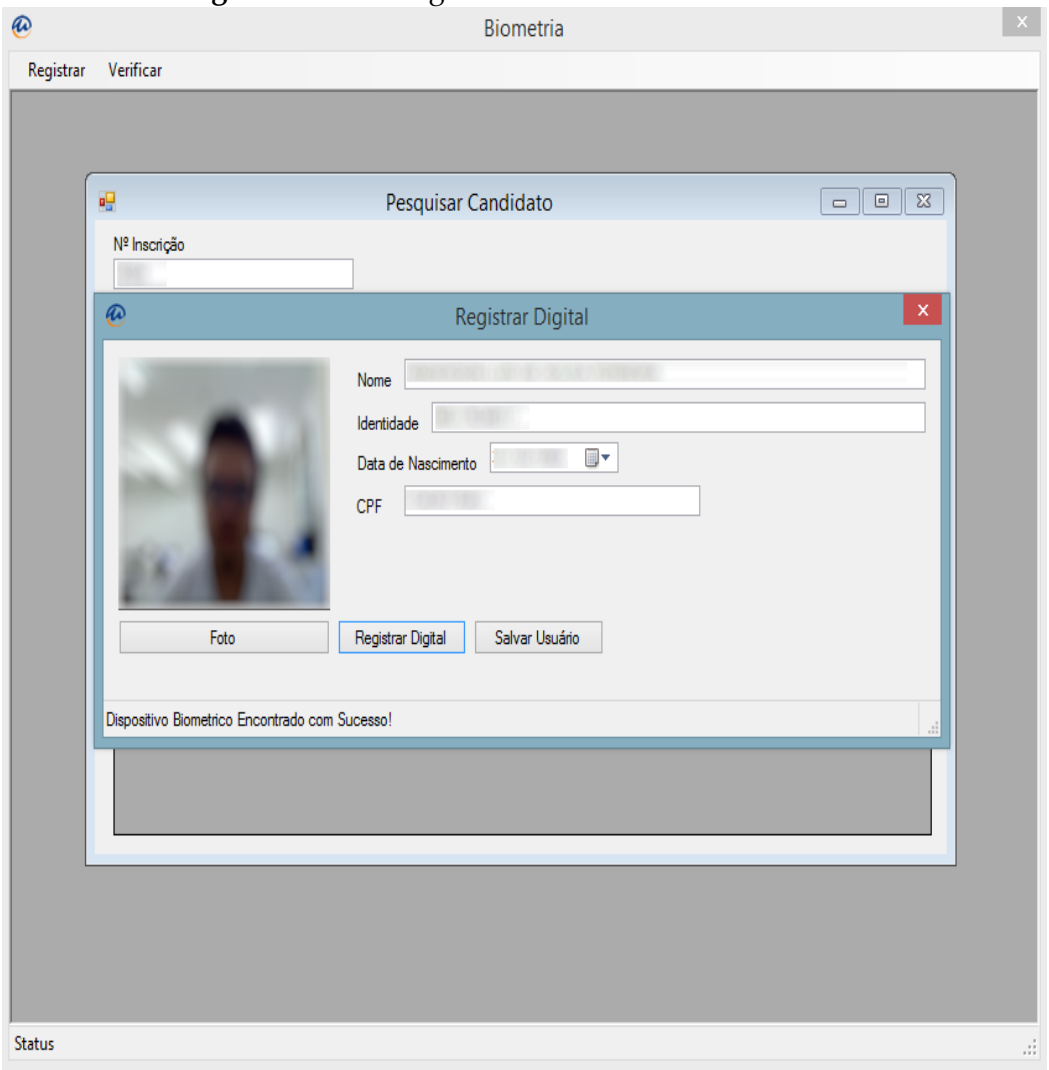
[2] 1:1 que corresponde ao processo de verificação, ou 1:N, que corresponde ao processo de identificação, como exposto no referencial teórico deste trabalho.

novas aplicações que utilizem biometria forem sendo desenvolvidas, outros tipos de aplicação serão inseridos.

Na etapa de verificação e identificação, o sistema armazenará os dados referentes à pessoa identificada e à data e hora da verificação/identificação. Assim, esses dados podem ser utilizados por qualquer aplicação que necessite, como, por exemplo, o registro acadêmico poderá se basear no horário de verificação para registrar a falta ou a presença de um aluno em uma determinada aula.

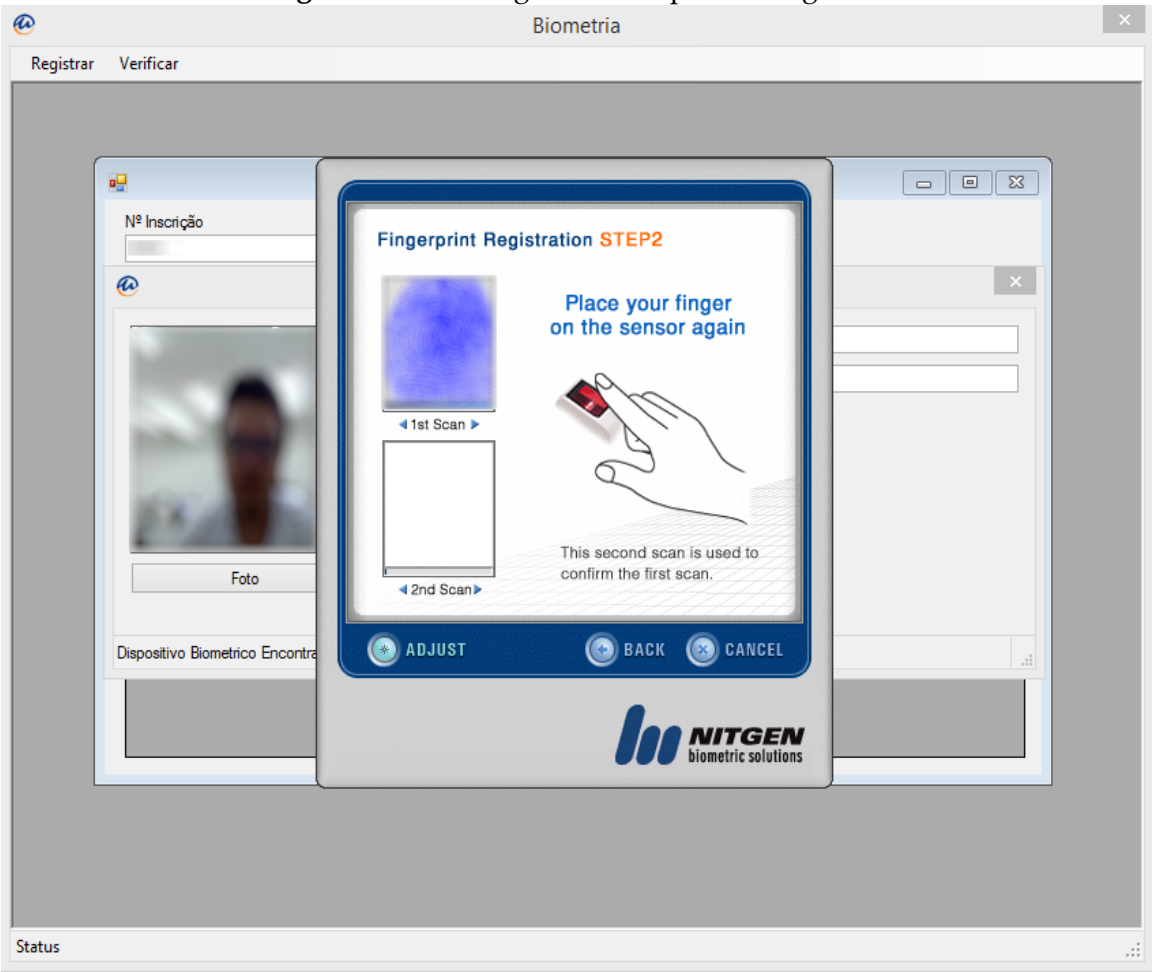
A aplicação cliente desenvolvida, representada na Figura 2, que utiliza os serviços web, é uma aplicação desktop que, além de permitir o registro da digital, permite a captura de uma foto utilizando-se uma *webcam*, conforme mostram as Figuras 4 e 5.

Figura 4 Tela de registro de candidato do vestibular.



Fonte: autoria própria

Figura 5 Tela de registro da impressão digital.



Fonte: autoria própria

Foram registradas as impressões digitais e as fotos de todos os candidatos do vestibular do curso de medicina (aproximadamente 3000 pessoas, distribuídas em 70 salas, sendo que o registro levou em torno de 1 minuto por candidato). Para viabilizar o processo, foram adquiridos equipamentos de coleta de impressão digital Nitgen Hamster III e *webcams* modelo Logitech HD Pro C920, que foram instalados nos computadores das salas de aula.

Para os candidatos aprovados no vestibular para o curso de medicina, a verificação foi feita no momento da matrícula. Para isso, foi utilizado o método 1:1 (um contra um), ou seja, o usuário digitava parte do nome ou o CPF, ou ainda o número de inscrição do vestibular e, ao localizar o candidato, era realizada a verificação biométrica.

No momento da matrícula, foram coletadas a impressão digital e a foto dos candidatos aprovados nos demais cursos e armazenadas para sua futura utilização em outros processos que necessitem de autenticação.

Para agilizar o processo de matrícula, foi implementada uma funcionalidade para realizá-la a partir da aplicação desenvolvida. Dessa forma, após a identificação, o sistema já permite preencher todas as informações do registro acadêmico, presentes no

sistema do vestibular, incluindo dados pessoais, enturmação do aluno em primeira ou segunda opção de curso e, ainda, o registro da parte financeira. Além disso, foi desenvolvida uma função para facilitar o processo de digitalização dos documentos dos alunos, de forma que, após a matrícula do aluno e a digitalização dos documentos, o usuário pode solicitar que os arquivos digitalizados sejam renomeados seguindo uma ordem pré-estabelecida de documentos, inserindo-se no nome de cada arquivo o número de CPF do aluno, para que esses documentos possam ser pesquisados posteriormente. Para o envio para o sistema de gestão de documentos, os arquivos são compactados e copiados para um local determinado.

Foi desenvolvida, ainda, uma aplicação web para realizar a frequência biométrica, de forma que ela pudesse ser integrada ao Portal Acadêmico já utilizado na instituição.

Para o registro de frequência, inicialmente, o professor deverá se autenticar no sistema. Pode-se utilizar, nesse momento, qualquer um dois métodos de reconhecimento. Após a identificação do professor, por meio da consulta ao horário de aula, serão selecionados os alunos de uma turma específica. Como nesse caso a quantidade de alunos é pequena, será utilizada a identificação 1:N, permitindo-se ganho de tempo, pois, se fosse necessário verificar manualmente cada aluno, o processo não seria viável. Segue a Figura 6, que mostra a tela da aplicação de registro de frequência.

Figura 6 Tela da frequência biométrica

Fonte: autoria própria

Essa aplicação ainda não foi implantada em definitivo, mas foram realizados testes com duas turmas, com aproximadamente 50 alunos em cada. O tempo para identificação foi em torno de 5 minutos por turma.

5 CONCLUSÃO

O sistema desenvolvido permite o registro e a verificação/identificação de impressões digitais, além da captura de fotos. Houve algumas dificuldades na utilização de bibliotecas de terceiros para utilizar o equipamento biométrico e a *webcam*, mas agora essas bibliotecas já estão integradas ao sistema e em funcionamento.

O sistema foi utilizado no processo seletivo do UNIPAM, em novembro de 2014, para registro de digitais dos candidatos ao curso de Medicina, garantindo credibilidade à instituição e segurança para os candidatos.

Os funcionários que utilizaram o sistema estão cadastrados no sistema interno da instituição que controla o registro de usuários, bem como foi realizado treinamento para utilização do sistema.

Para o registro de frequência biométrica, os testes foram realizados com sucesso conforme descrito nos resultados. No entanto, sua utilização, atualmente, é inviável, sendo que é necessária uma máquina dedicada a somente essa tarefa em cada sala, de forma que o aluno se identifique no momento em que chegue à sala de aula e possa ver que sua frequência foi realizada. Como as salas de aula possuem uma máquina e os professores a utilizam para meios didáticos, não será possível interromper a aula para realizar a identificação do aluno.

Como projeto futuro, para viabilizar o registro de frequência, poder-se-ia desenvolver uma aplicação que funcionasse em um dispositivo de *hardware* mais simples, que viabilizasse os custos para dedicá-lo exclusivamente para essa função, evitando o uso do computador na sala de aula.

Ainda como projeto futuro, deve-se atualizar a aplicação cliente *desktop* para coleta de digitais de forma automática, evitando problemas referentes à manutenção de versões ou até mesmo reimplementá-la em uma aplicação web, disponibilizando-a no portal, amenizando as limitações de manutenção e gerenciamento de versão.

Como o sistema proposto foi utilizado com sucesso na autenticação dos candidatos ao processo seletivo da instituição, pode-se, ainda, adaptá-lo em outros processos, como no acesso às suas dependências e no registro de participação de eventos, a fim de dar maior segurança e garantir informações confiáveis referentes ao reconhecimento de pessoas, além de agilizar processos em que esse reconhecimento seja necessário.

REFERÊNCIAS

CANEDO, José Alberto. *Verificação (1:1) versus Identificação (1:N)*: fundamentos de biometria. 2011. Disponível em: <http://www.forumbiometria.com/fundamentos-de-biometria/191-verificacao-11-versus-identificacao-1n.html>. Acesso em: 10 mar. 2014.

FERNANDES, V.; PLINIO, M. Biometria, reconhecimento de impressão digital com Delphi. *Revista Clube Delphi*, v.76, 2006. Disponível em <http://www.devmedia.com.br/artigo-clube-delphi-76-biometria/11345> Acesso em 5 mar. 2014.

JAIN, Anil K.; ROSS, Arun A.; NANDAKUMAR, Karthik. *Introduction to biometrics*. New York: Springer, 2011.

LIU, Simon; SILVERMAN, Mark. *A practical guide to biometric security technology*. 2001. Disponível em: Acesso em: 16 mar. 2015.

PRAHBAKAR, Salil; PANKANTI, Sharath; JAIN, Anil K.. Biometric Recognition: Security and Privacy Concerns. *Ieee Security & Privacy*, Aaa, v. 1, p.33-42, abr. 2003. Bimestral.

SCHWABER, Ken; SUTHERLAND, Jeff. *Guia do Scrum:* um guia definitivo para o Scrum: As regras do jogo. São Paulo: Desc, 2013.

THIAN, N. *Biometric Authentication System*. Dissertação de mestrado. 2001. USM, Penang, Malásia. Disponível em: http://hydria.u-strasbg.fr/~norman/BAS/publications.htm.