Ex@tas Online

ISSN 2178-0471
vol. 1 n. 7 Mar. 2016
pág. 1-13

Automação para fiscalização de CNH utilizando dispositivos móveis e biometria

Automation for Inspection of CNH using mobile devices and biometrics

Jéssica Cerqueira Santos[1], Saulo Correa Peixoto[2], Alex Ferreira dos Santos[3], Robson Hebraico Cipriano Maniçoba[2]

[1]Faculdade de Tecnologia e Ciências (FTC), [2]Universidade Estadual do Sudoeste da Bahia (UESB), [3]Universidade Federal do Recôncavo da Bahia (UFRB)

Resumo

Atualmente devido o crescente número de pessoas habilitadas, observou-se a necessidade em se ter novos métodos de verificação de autenticidade, que venha auxiliar os agentes fiscalizadores do trânsito durante uma *blitz*. A partir deste cenário, o presente trabalho propõe uma solução com a utilização de dispositivos móveis e biometria, para garantir melhor eficiência e segurança durante as abordagens. Desenvolveu-se assim um aplicativo capaz de identificar o condutor através da leitura de sua digital e mostrar sua situação perante a lei com consultas de infrações e afins, nos bancos de dados oficiais pertinentes.

Palavras-chave: Biometria, Dispositivos Móveis, Condutor, Sistema de Informação.

Abstract

Currently due to the increasing number of skilled people, there was the need to have new methods of verification of authenticity, which may assist the supervising traffic police during a traffic stop. From this scenario, this paper proposes a solution to the use of biometrics and mobile devices, to ensure best efficiency and safety during approaches. Thus developed an application that can identify the driver by reading its digital, and show their status before the law with queries and related offenses, on the banks of relevant official.

Keywords: Biometrics, Mobile Devices, Conductor, Information System.

1. Introdução

Dados divulgados pelo Departamento Nacional de Trânsito (DENATRAN) mostram que a Bahia em 2003, possuía uma frota de 790.510 veículos entre automóveis e motocicletas. Em setembro de 2013, a marca chegou a aproximadamente 2.364.900, aumento de quase 300%. O município de Jequié possuía 12.750 veículos entre carros e motos em sua frota, e considerando o mesmo período, cresceu 288% chegando à marca de 36.738 veículos, com um aumento de aproximadamente 8,2% entre setembro de 2012 e 2013 [1].

O número de pessoas que possuem a Carteira Nacional de Habilitação (CNH) tornou-se significativo, principalmente no município de Jequié, onde os valores estão em torno 65.533 indivíduos habilitadas, segundo dados divulgados pelo DETRAN da Bahia [2].

Assim como qualquer outro documento, a CNH também pode ser fraudada. Atualmente, segundo a fonte Serasa Experian [3], foram indicadas 837 mil tentativas de golpes com documentos falsos entre janeiro e maio de 2013, sendo que em 2012 no período de janeiro a dezembro, 2.14 milhões foram indicadas. A cada 14,8 segundos um consumidor brasileiro é vítima da tentativa de fraude conhecida como roubo de identidade, através das quais dados pessoais são usados por criminosos para obter crédito com a intenção de não honrar os pagamentos ou fazer um negócio sob falsidade ideológica.

ISSN 2178-0471
vol. 1 n. 7 Mar. 2016
pág. 1-13

Nesse contexto, buscando reduzir esses indicadores negativos, é proposto como objetivo principal desse estudo construir um aplicativo para dispositivos móveis, que proporcione mobilidade e eficiência aos agentes fiscalizadores do trânsito, através do uso de técnicas biométricas.

A biometria (do grego bios = vida e metron = medida) é o estudo estatístico de fenômenos quantitativos pertinentes a objetos de estudo das ciências biológicas. Atualmente, a biometria é usada na identificação criminal, controle de acesso, etc. Os sistemas chamados biométricos podem basear o seu funcionamento em características de diversas partes do corpo humano, por exemplo, os olhos, a palma da mão, as digitais do dedo, a retina ou íris dos olhos, dentre outras [4]. A premissa em que se fundamentam é a de que cada indivíduo é único e possuí características físicas e de comportamento (a voz, a maneira de andar, etc.) distintas, traços aos quais são característicos de cada ser humano.

Por meio de softwares e algoritmos que tornaram o reconhecimento confiável e rápido, juntamente com as tecnologias de hardware, foi possível chegar ao desenvolvimento de aplicações biométricas. Os sistemas de reconhecimento biométrico podem fazer a autenticação segura de usuários, utilizando a leitura e o armazenamento de informações em bases de dados sólidas [4].

Assim, o presente estudo buscou analisar as falsificações realizadas em documentos e entender como a biometria pode ser utilizada neste contexto para a construção de uma solução que possa ser agregada ao serviço de identificação de um cidadão habilitado em uma ocorrência de *bliz*[1] de trânsito.

2. Modelo Teórico

2.1 Carteira Nacional de Habilitação (CNH)

A CNH atesta que o cidadão brasileiro está apto a conduzir veículos, e esta é obrigatória para conduzir o veículo. O modelo atual de CNH possui a fotografia da pessoa, o número da Carteira de Identidade (Registro Geral – RG) e do Cadastro de Pessoa Física (CPF). Assim, a CNH pode ser utilizada para identificação em todo território nacional, conforme atesta a Lei nº 9.503/97. Em seu Art. 159, dispõe que a CNH "conterá fotografia, identificação e CPF do condutor, terá fé pública equivalerá a documento de identidade em todo território nacional" [5].

As primeiras carteiras de motoristas não possuíam foto e não serviam como documento válido para identificação pessoal. A sua validade dependia da apresentação em conjunto com o documento de identidade. Na Figura 1, é perceptível a diferença entre CNH antiga e a atual.

Figura 1: Carteiras de Motorista de 1984 (esquerda) e Atual (direita).

[1] Segundo Dicionário Michaelis: trata-se de uma Batida policial de improviso e que utiliza grande aparato. Conjunto oficial organizado para combater qualquer tipo de infração

ISSN 2178-0471
vol. 1 n. 7 Mar. 2016
pág. 1-13

2.2 Falsificações

Segundo Parodi [6] existem vários tipos de documentos falsificados, com diferentes níveis de qualidade e sofisticação. Em se tratando de documento de identificação, os casos mais comuns são:

- Documentos montados a partir de espelhos autênticos, roubados e sucessivamente preenchidos com os dados de identidades fictícias ou verdadeiras (roubo de identidade).
- Documentos montados a partir de espelhos falsos mais impressos com qualidade (*offset*). Normalmente as cores e detalhes do espelho diferem do original, assim como no preenchimento com caracteres e demais detalhes diferentes dos originais.
- Documentos verdadeiros, roubados e adulterados. O caso mais comum é o da substituição da foto, através de recorte da original, colagem da nova foto e sucessiva replastificação do documento.
- Documentos digitalizados, adulterados ou remontados e impressos. Apesar da alta definição de algumas impressoras, normalmente a qualidade de impressão é ruim, bem como a definição e os detalhes, e as cores dos caracteres usados são diferentes.

Pode-se afirmar que grandes partes das fraudes envolvem o uso de algum tipo de documento ou identidade falsa. Isso por que os golpistas os utilizam para alterarem suas próprias identificações. É um dos momentos em que os fraudadores são mais vulneráveis, quando uma verificação eficiente e sistemática geraria melhores resultados [6].

A lei brasileira considera alguns documentos válidos para identificação pessoal dentre eles temos:

- Cédula de Identidade (Registro Geral – RG);
- Passaporte;
- Carteiras Profissionais emitidas pelos conselhos (OAB, CRECI, CRC, CRM, dentre outros.), modelos com foto;
- Carteira de Trabalho;
- Carteiras Funcionais emitidas pelas repartições públicas;
- CNH modelos com foto.

Novas tecnologias (sobretudo as biométricas) estão sendo adotadas no mundo inteiro, tanto no setor público quanto no setor privado, para limitar e contornar o problema das fraudes ligadas a roubo de identidade. No Brasil, apesar destas tecnologias ainda terem uma presença muito esporádica no setor público e estar apenas engatinhando no setor privado, a tendência é que haja um progressivo aumento de sua presença e uso [6].

2.3 Biometria

A biometria é definida como ciência da aplicação de métodos de estatística quantitativa a fatos biológicos, mas pode ser definida também como o estudo das características físicas ou comportamentais dos humanos. Este termo tem sido também alvo de pesquisa como forma de identificação de pessoas, sendo usado nas mais diversas aplicações, tais como controle de acessos e segurança de dispositivos, entre outras. A biometria, na área do reconhecimento, recorre a partes exclusivas do corpo humano para a extração de características únicas a serem usadas no reconhecimento, como a impressão digital, reconhecimento da voz, geometria das mãos, padrão da íris e da retina entre outros [8].

Qualquer característica fisiológica ou comportamental humana pode ser usada como característica biométrica desde que ela atenda a alguns requisitos básicos [8]:

- **Universalidade:** significa que todas as pessoas devem possuir a característica;
- **Singularidade:** indica que esta característica não pode ser igual em pessoas diferentes;
- **Permanência:** significa que a característica não deve variar com o tempo;

ISSN 2178-0471
vol. 1 n. 7 Mar. 2016
pág. 1-13

- **Mensurabilidade:** indica que a característica pode ser medida quantitativamente;
- **Desempenho:** refere-se à precisão de identificação, aos recursos requeridos para conseguir uma precisão de identificação aceitável e ao trabalho ou fatores ambientes que afetam a precisão da identificação;
- **Aceitabilidade:** indica o quanto as pessoas estão dispostas a aceitar os sistemas biométricos;
- **Proteção:** refere-se à facilidade/dificuldade de enganar o sistema com técnicas fraudulentas.

As técnicas biométricas são tecnologias que estão evoluindo muito rapidamente, por causa do grande apelo comercial, proveniente principalmente das áreas forenses, como a identificação criminal e a segurança de prisão, como também em aplicações civis. Nesse setor podem ser usadas para prevenir acesso sem autorização aos Bancos 24 horas, telefones celulares, cartões inteligentes, computadores pessoais, Workstations, e redes de computadores, e também podem ser usadas em transações efetuadas por telefone e internet (comércio eletrônico) [9].

2.4 Reconhecimento pela Digital

A impressão digital é um método biométrico bastante comum e baseia-se na unicidade comprovada dos sulcos que a compõem. Esta unicidade leva que, dela possam ser extraídas características (minúcias). Estes sistemas baseiam-se primeiro, em um método de recolha da imagem da impressão digital e posteriormente em algoritmos de detecção de minúcias que levam à consequente recolha das características que permitam identificar/autenticar o sujeito. Apresenta uma elevada eficácia nas taxas de identificação e os sistemas são cada vez mais simples e fáceis de utilizar. Na Figura 2, pode ser observada a identificação de alguns pontos característicos das impressões digitais [10].

Figura 2: Pontos utilizados para reconhecimento a partir de impressão digital.

As minúcias ou pontos característicos são acidentes que se encontram nas cristas papilares como, por exemplo, linhas que determinam abruptamente ou se bifurcam, e tem por finalidade estabelecer a unicidade das impressões digitais. O American National Standards Institute (ANSI) propôs quatro maiores grupos de minúcias: cristas finais, bifurcações, cruzamentos e pontos indeterminados. Porém, as minúcias consideradas mais importantes são as cristas finais e bifurcações, pois ocorrem frequentemente nas imagens de impressões digitais [14].

A crista final é definida com um ponto onde a crista termina abruptamente. A crista bifurcada é definida como um ponto onde a crista diverge dentro de cristas brancas, ou seja, vales (linhas brancas).

ISSN 2178-0471
vol. 1 n. 7 Mar. 2016
pág. 1-13

Lagos ou ilhas são definidos como duas bifurcações conectadas. Cristas independentes ou curtas são definidas como cristas finais muito pequenas ou simplesmente como cristas quebradas. Esporas são formadas pela combinação de bifurcações conectadas na vizinhança, ou seja, duas bifurcações com um caminho conectado [14]. A Figura 3 ilustra os aspectos de impressões digitais.

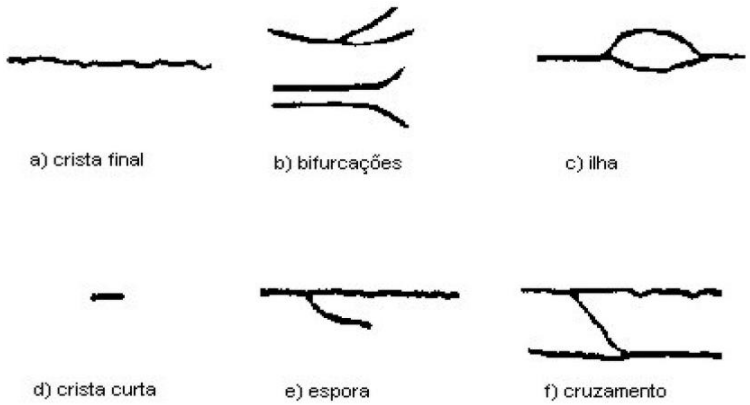

Figura 3: Aspectos de impressões digitais.

Segundo Costa [11], para a verificação das impressões digitais se faz necessário:

- Que haja coincidência em no mínimo doze pontos característicos;
- Que não exista nenhuma discordância entre estes pontos, ou seja, eles devem ser idênticos e ter a mesma localização.

De acordo com Lourenço [12], a impressão digital pode ser estampada em papel, pressionando o dedo previamente preparado com tinta, para posteriormente ser digitalizada por meio de um scanner. Um exemplo deste tipo de imagens são as impressões digitais latentes encontradas em cenas de crimes, que podem ser recuperadas por meio de um procedimento especial. A impressão digital também pode ser obtida “ao vivo”, por meio de dispositivos eletrônicos especiais. O princípio básico de todos é a detecção das rugosidades dos dedos que estão em contato com o dispositivo.

3. Metodologia

O software proposto foi modelado a partir do uso da notação *Unified Modeling Language* (UML), que segundo Guedes [13] UML é uma linguagem visual para modelar sistemas computacionais por meio de paradigma de Orientação a Objetos. Por ser apenas uma linguagem e, portanto, é somente uma parte de um método para o desenvolvimento de um software, ela é independente do processo, apesar de ser perfeitamente utilizada em um processo orientado a caso de usos, centrado na arquitetura, interativo e incremental. As Figuras 4 e 5 ilustra o diagrama gerado a partir da modelagem.

O diagrama da Figura 4 consiste em um diagrama de caso de uso que tem por objetivo descrever as funcionalidades do sistema proposto. Já a Figura 5, mostra o funcionamento do banco de dados relacional fictício, desenvolvido para o funcionamento do aplicativo. O banco de dados é dito fictício, pois não foi possível obter acesso à estrutura do Banco de Dados Oficial (INFOSEG) e do sistema do Departamento Estadual de Trânsito (DETRAN). Entretanto, sendo aplicado em um contexto real em nada irá interferir nas funcionalidades do aplicativo.

ISSN 2178-0471
vol. 1 n. 7 Mar. 2016
pág. 1-13

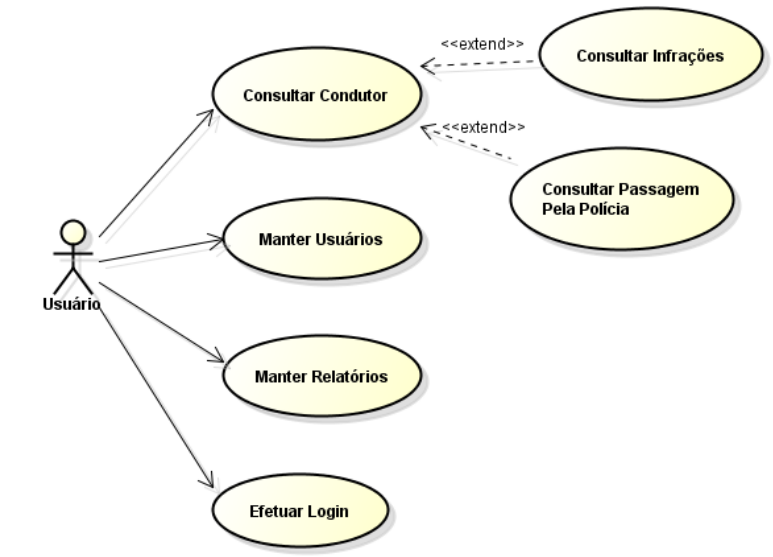

Figura 4: Diagrama de Caso de Uso do aplicativo.

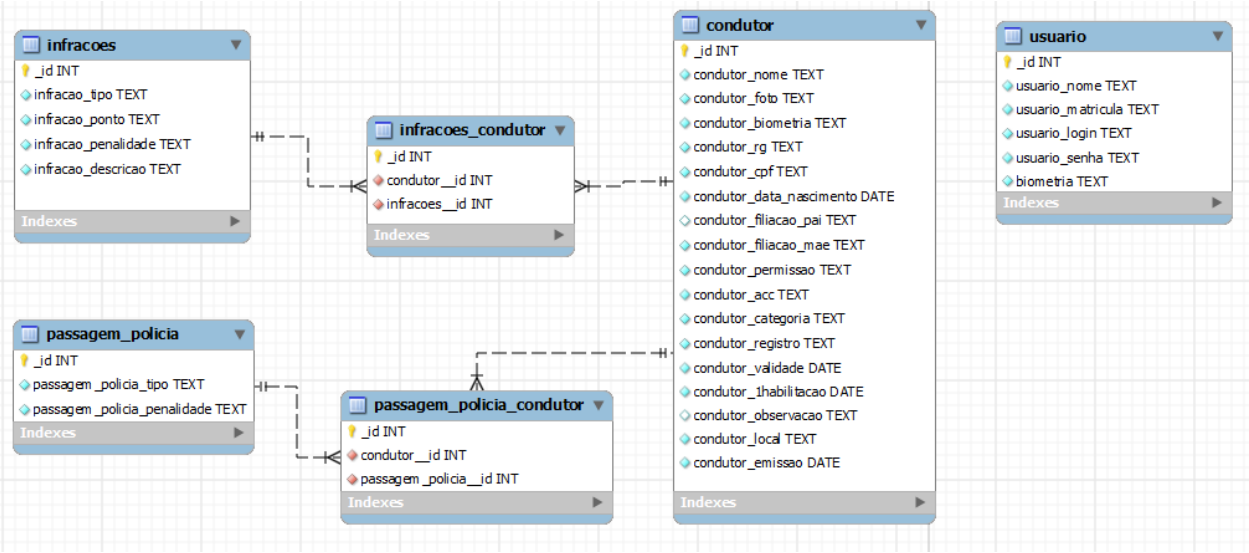

Figura 5: Modelagem do Banco de Dados

A primeira parte do desenvolvimento do aplicativo consistiu em fazer o levantamento dos requisitos etapa pela qual foi realizado o alinhamento do projeto, a realidade em que será aplicado. Em seguida a escolha do hardware que se adequasse as especificações mínimas exigidas para a utilização do leitor biométrico, neste caso o leitor Nitgen Hamster DX - FingerTech.

Optou-se por utilizar um ambiente de desenvolvimento livre para a programação, portanto foi utilizado o Ambiente Integrado de Desenvolvimento (IDE) Eclipse, que é um *framework* gratuito, com código aberto para desenvolvimento de programas. O aplicativo irá funcionar no Sistema Operacional (SO) Android a partir da sua versão 3.2 (*Honeycomp*), fazendo uso da plataforma de programação JAVA, que possui uma linguagem simples e de fácil utilização [14].

Com a aquisição do leitor biométrico da empresa FingerTech, foi disponibilizado documentação, bibliotecas e um pequeno aplicativo de código aberto para o entendimento de como se realiza a captura e a comparação das digitais. Na Figura 6 e 7 temos uma parte deste código que mostra como é feita a captura da digital e como ela é comparada com outras digitais para a identificação de pessoas.

ISSN 2178-0471
vol. 1 n. 7 Mar. 2016
pág. 1-13

Na linha 153 (Figura 6), é realizada a captura da digital e os valores pertinentes a essa captura são enviados para a variável inputFIR, que posteriormente poderá ser convertida tanto para valores binários quanto para texto, para que assim seja armazenada no banco de dados.

```
147         NBioBSPJNI.FIR_HANDLE hCapturedFIR, hAuditFIR;
148         NBioBSPJNI.CAPTURED_DATA capturedData;
149         hCapturedFIR = bsp.new FIR_HANDLE();
150         hAuditFIR = bsp.new FIR_HANDLE();
151         capturedData = bsp.new CAPTURED_DATA();
152
153         bsp.Capture(NBioBSPJNI.FIR_PURPOSE.ENROLL, hCapturedFIR, 10000, hAuditFIR, capturedData, this);
154
155         if (bsp.IsErrorOccured())  {
156             msg = "NBioBSP Capture Error: " + bsp.GetErrorCode();
157         }
158         else  {
159             NBioBSPJNI.INPUT_FIR inputFIR;
160             inputFIR = bsp.new INPUT_FIR();
161
162             {
163                 NBioBSPJNI.Export.DATA exportData;
164                 inputFIR.SetFIRHandle(hCapturedFIR);
165                 exportData = exportEngine.new DATA();
166
167                 exportEngine.ExportFIR(inputFIR, exportData, NBioBSPJNI.EXPORT_MINCONV_TYPE.ISO);
168
169                 if (bsp.IsErrorOccured())  {
170                     msg = "NBioBSP ExportFIR Error: " + bsp.GetErrorCode();
171                     Toast.makeText(this, msg, Toast.LENGTH_SHORT).show();
172                     return ;
173                 }
174
175                 if (byIso1 != null)
176                     byIso1 = null;
177
178                 byIso1 = new byte[exportData.FingerData[0].Template[0].Data.length];
179                 byIso1 = exportData.FingerData[0].Template[0].Data;
```

Figura 6: Código de captura da digital.

Na linha 725 (Figura 7), temos o código responsável pela comparação de digitais, a variável inputFIR1, que possui os dados das digitais armazenadas no banco de dados, a variável inputFIR2 que contém os dados da digital que será usada para ser comparada com as outras do banco de dados, e a bResult que retornará se as digitais comparadas são true (digital da mesma pessoa), e false (as digitais não são compatíveis).

```
715             // Verify Match
716             NBioBSPJNI.INPUT_FIR inputFIR1, inputFIR2;
717             Boolean bResult = new Boolean(false);
718
719             inputFIR1 = bsp.new INPUT_FIR();
720             inputFIR2 = bsp.new INPUT_FIR();
721
722             inputFIR1.SetFIRHandle(hPorcessedFIR1);
723             inputFIR2.SetFIRHandle(hPorcessedFIR2);
724
725             bsp.VerifyMatch(inputFIR1, inputFIR2, bResult, null);
726
727             if (bsp.IsErrorOccured())  {
728                 msg = "NBioBSP VerifyMatch Error: " + bsp.GetErrorCode();
729             }
730             else  {
731                 if (bResult)
732                     msg = "VerifyMatch Successed";
733                 else
734                     msg = "VerifyMatch Failed";
735             }
736
737             hLoadAudit1.dispose();
738             hLoadAudit2.dispose();
739             hPorcessedFIR1.dispose();
740             hPorcessedFIR2.dispose();
741
742             Toast.makeText(this, msg, Toast.LENGTH_SHORT).show();
743         }
744         else
745             Toast.makeText(this, "Can not find captured data", Toast.LENGTH_SHORT).show();
746
747         tvInfo.setText(msg);
```

Figura 7: Código de comparação de digitais.

Foi utilizando o Sistema Gerenciador de Banco de Dados (SGDB) SQLite interno do Android, que fornece um ambiente de banco de dados relacional muito funcional e flexível, que consome o

ISSN 2178-0471
vol. 1 n. 7 Mar. 2016
pág. 1-13

mínimo de recursos. Este SGDB foi aplicado somente para a criação de um protótipo funcional, para a formulação de testes. O seu funcionamento em uma base de dados real, exige a utilização de um servidor externo de dados.

4. O aplicativo

Foi desenvolvido um aplicativo para dispositivos móveis, com o objetivo de auxiliar as autoridades fiscalizadoras do transito, fazendo uso de técnicas biométricas para a identificação do condutor. A solução visa permitir os agentes fiscalizadores ter acesso a CNH, infrações e passagens pela polícia do cidadão que está sendo identificado. A seguir será descrito os passos utilizados para obtenção dos dados do condutor.

Passo 1: inicialmente o usuário do sistema efetua a sua identificação através da leitura da sua digital cadastrada no banco de dados.

Passo 2: usuário irá selecionar a opção condutora que ativará o leitor biométrico para o recebimento das digitais, e posteriormente a identificação do cidadão habilitado.

Passo 3: após o condutor ter sua digital comparada ao banco de dados, trará como resultados seus dados mostrados em tela para o agente que estiver realizando a fiscalização.

Passo 4: por fim, o usuário poderá escolher identificar outro condutor, retornar ao menu inicial ou sair do aplicativo.

O aplicativo possui um nome fictício UNO - Identificação Biométrica Móvel, significando um ou único, que faz referência à biometria que em sua metodologia utiliza características únicas do ser humano para sua identificação.

A tela inicial é ilustrada na Figura 8. O aplicativo UNO é composto por três módulos:

- Gerenciamento de usuários: onde é possível realizar cadastros, alterações, listagens e consultas dos usuários do sistema;
- Gerenciamento de relatórios: que será possível gerar arquivos para impressão contendo a lista de pessoas que foram identificadas, o nome do agente responsável pela blitz, local e data em que ela foi realizada;
- Identificação do condutor: modulo de maior importância para o usuário.

No módulo de identificação do condutor ilustrado na Figura 9, é mostrado como é feita a captura dos dados e como as informações do condutor são mostradas em tela para o agente fiscalizador, essa é a parte de maior importância do aplicativo, pois é com ela que atingimos o objetivo da realização do sistema.

Com a consulta realizada, caso precise visualizar as infrações e passagens pela polícia do condutor identificado, é só apertar o botão de infrações ou passagem polícia e será realizada outra consulta assim como demonstra as Figura 10.

ISSN 2178-0471
vol. 1 n. 7 Mar. 2016
pág. 1-13

Figura 8: Tela Inicial do sistema UNO.

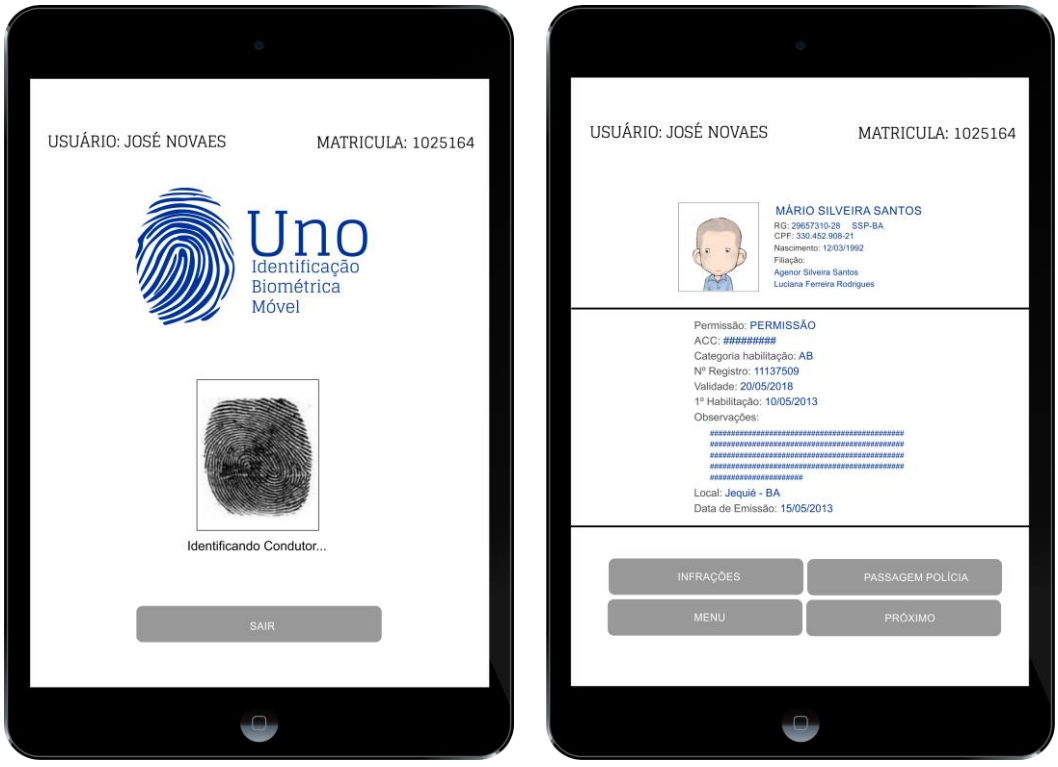

Figura 9: Tela de captura da digital (esquerda) e Tela de retorno de consulta (direita).

ISSN 2178-0471
vol. 1 n. 7 Mar. 2016
pág. 1-13

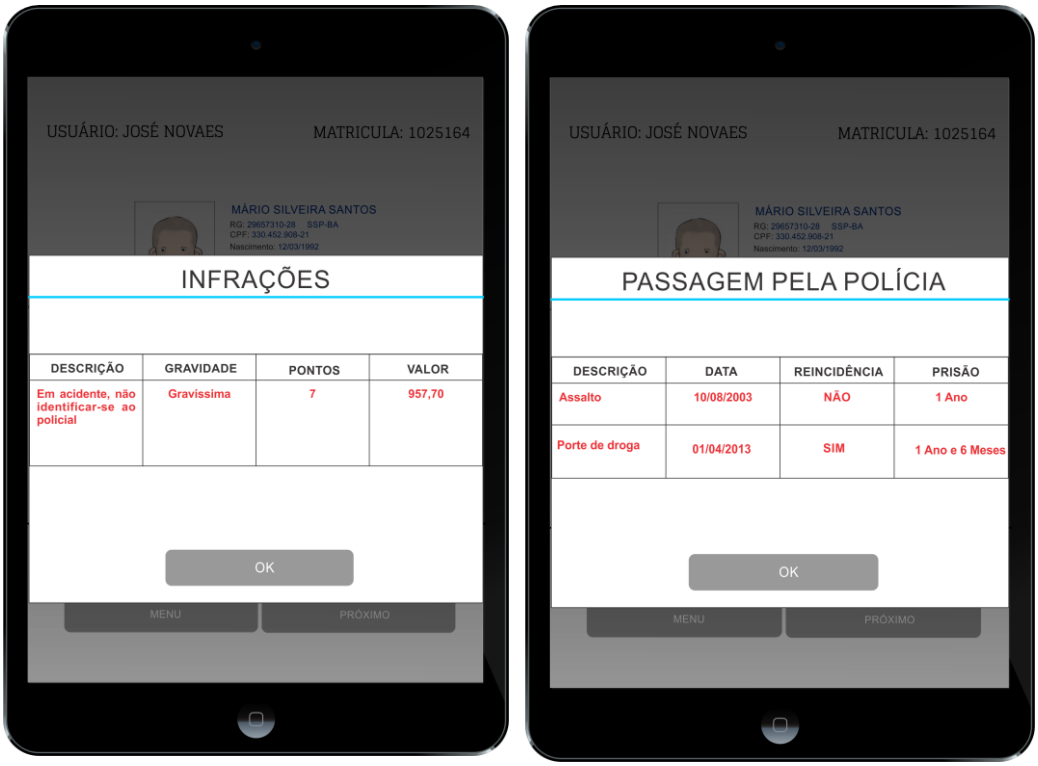

Figura 10 - Tela de consulta de infrações (esquerda) e Tela de consulta de passagens pela polícia (direita).

5. Tipo de estudo

Trata-se de uma pesquisa de natureza aplicada e explicativa, sob a forma de levantamento de dados utilizando questionários, entrevistas e observações informais diretas, como técnica de coleta de dados.

A natureza aplicada dessa pesquisa se comprova quando se tem por objetivo gerar conhecimento sobre a biometria e como ela juntamente com dispositivos móveis podem estar auxiliando a Polícia Militar para a aplicação em um cenário real.

A abordagem quantitativa se comprova mediante a busca por transformar opiniões e informações em variáveis mensuráveis para proporcionar solidez ao objetivo traçado [15].

6. Campo de estudo

O estudo foi realizado no município de Jequié - Bahia, com o 19º Batalhão da Polícia Militar, constituído por 300 policiais, sujeitos escolhidos por serem os responsáveis por realizar as *blitz* de trânsito no citado município. Também foi escolhida uma pequena amostra dos cidadãos habilitados de Jequié, que em sua totalidade são 65.533 (dados fornecidos pelo DETRAN do estado da Bahia), sendo que dos dados levantados, a coleta de dados foi realizada, com 30 policiais e 30 cidadãos habilitados.

A amostra escolhida caracterizou-se por ser probabilística sendo dividida em duas partes, a primeira constituída de policiais militares de Jequié – Bahia, sem exceção de patentes, pois todos podem participar de uma *blitz* de trânsito, e a segunda parte formada pelos cidadãos residentes na cidade escolhida, e que possuíam a CNH.

ISSN 2178-0471
vol. 1 n. 7 Mar. 2016
pág. 1-13

7. Resultados

Os resultados desta pesquisa foram obtidos através da análise dos questionários, das entrevistas e das observações diretas. Através dos questionários que foram aplicados foi possível responder as seguintes questões:

- O sistema proporcionaria confiança para ser utilizando em uma *blitz* de trânsito?
- O sistema será eficiente para um policial militar utilizar?
- O quanto seria o aumento de eficiência?
- O sistema poderá diminuir a quantidade de falsificações com CNH?
- O quanto poderia diminuir as falsificações?

Com a entrevista, após o esclarecimento sobre a pesquisa e todos os seus prontos primordiais fazendo uso de perguntas subjetivas, foi possível captar como ocorre todo o processo em uma *blitz* de trânsito. O uso da observação direta favoreceu a obtenção de mais informações, que foram somadas às adquiridas durante as entrevistas.

De acordo com a Figura 11, pode-se verificar que 90% dos policiais entrevistados sentem confiança para utilizar o aplicativo em uma *blitz*. Contudo, na Figura 12, 100% dos condutores sentiriam confiança em serem identificados através da biometria. Estes resultados mostram a confiabilidade em estar utilizando este tipo de tecnologia aplicado em um contexto real, tanto da população portadora da CNH, quanto dos profissionais que realizam a sua fiscalização.

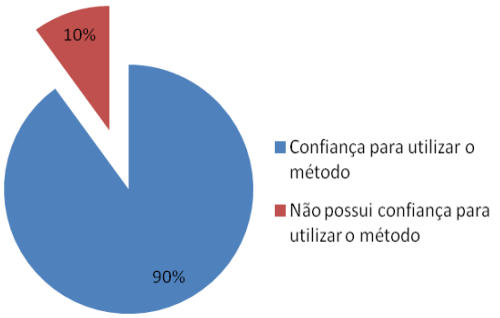

Figura 11: Confiabilidade do projeto para a polícia militar.

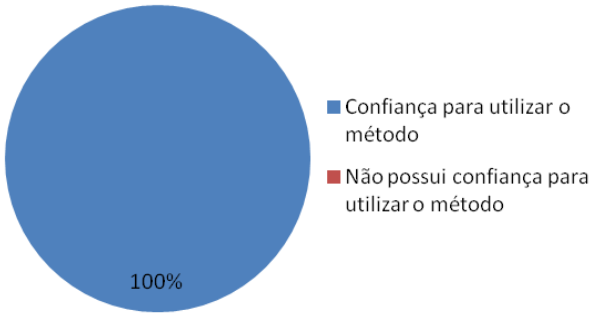

Figura 12: Confiabilidade do projeto para os condutores.

Nas Figuras 13 e 14, é mostrada que 97% dos entrevistados da polícia militar concordaram que o projeto sendo implantado poderia ser eficiente e 58% afirmam que essa eficiência aumentaria em 80%. Como os resultados apontam os profissionais destinados a utilizar o projeto proposto, acreditam que a eficiência durante as suas atividades de fiscalização iriam aumentar.

Figura 13: Eficiência do projeto para a polícia militar.

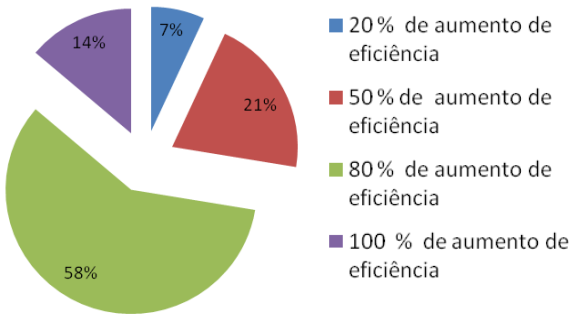

Figura 14: Aumento de eficiência em porcentagem

ISSN 2178-0471
vol. 1 n. 7 Mar. 2016
pág. 1-13

Por fim, para a diminuição de fraudes tanto a polícia quanto os condutores tiveram resultados aproximados. Na Figura 15 pode-se observar que as entrevistas com a polícia mostram que 93% concordam que o projeto iria proporcionar a diminuição das fraudes, e na Figura 16 os condutores em sua maioria de 97% também concordam. Nas Figuras 17 e 18 temos a porcentagem de diminuição dessas fraudes, 57% dos policiais entrevistados acham que 80% das fraudes com a CNH iriam diminuir e os condutores também em sua maioria de 66% confiam em 80% desta diminuição. Estes resultados demonstram que o aplicativo sendo utilizado em uma situação real, poderia haver a inibição de fraudadores e permitiria melhor ação durante estas fiscalizações, e proporcionaria mais segurança para a população que possui tal documento.

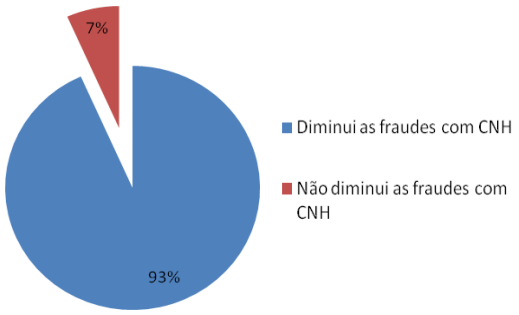

Figura 15: Diminuição de fraudes, de acordo com a polícia militar.

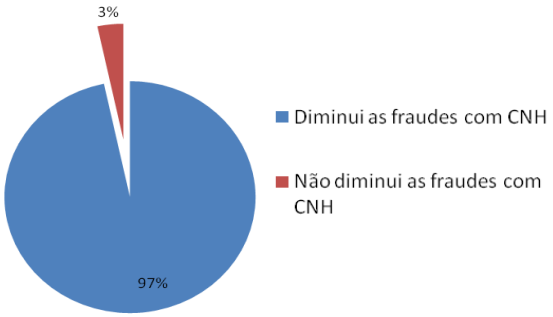

Figura 16: Diminuição de fraudes, de acordo com os condutores.

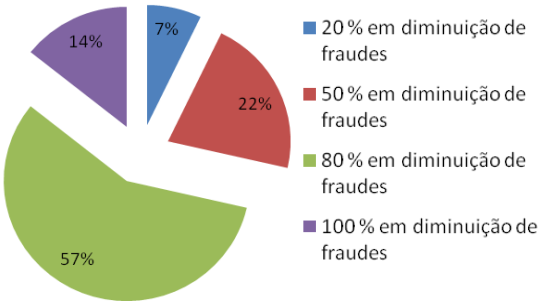

Figura 17: Diminuição de fraudes em porcentagem, de acordo com a polícia militar.

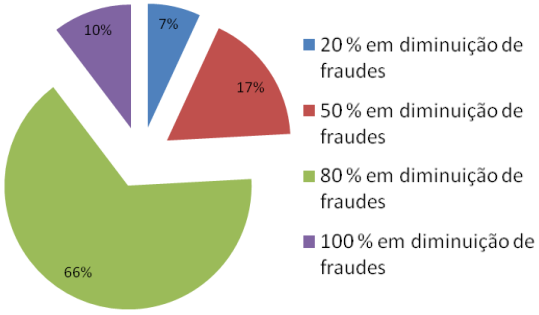

Figura 18: Diminuição de fraudes em porcentagem, de acordo com os condutores.

8. Considerações Finais

Neste artigo foi desenvolvido um aplicativo para dispositivos móveis, com o objetivo de auxiliar as autoridades fiscalizadoras do transito, fazendo uso de técnicas biométricas para a identificação do condutor. Até o dado momento, já é possível compreender a necessidade desta tecnologia para a fiscalização do trânsito, e a confiabilidade que este projeto proporciona tanto para os policiais quanto para os condutores entrevistados. Os policiais que participaram da entrevista apresentaram outras aplicações para o projeto, em utilizar-se de dispositivos móveis e biometria em: Abordagens de rotina, Área jurídica da polícia civil, Policiamento ostensivo, Segurança nos presídios, Entrada e saída da OPM e Identificação em praças desportivas. Desta forma o projeto poderia contribuir em outras áreas para a segurança pública.

Referências

[1] DENATRAN, Frota Nacional, Disponível em: <http://www.denatran.gov.br/frota2013.htm>, Acesso em 29 de Agosto de 2015.

[2] DETRAN Bahia, Habilitado por período, Disponível em: <http://www.detran.ba.gov.br/web/guest/estatisticas> Acesso em 29 de Agosto de 2015.

[3] SERASA EXPERIEN, Tentativas de fraude contra o consumidor somam 1,4 milhão entre janeiro e agosto de 2013, aponta indicador da Serasa Experian, Disponível em:< http://www.serasaconsumidor.com.br/tentativas-de-fraude-contra-o-consumidor-somam-14-milh%C3%A3o-entre-janeiro-e-agosto-de-2013-aponta-indicador-da-serasa-experian-5/ >Acesso em 29 de Agosto de 2015.

[4] A. L. Santos, "Gerenciamento de Identidades: Segurança da Informação", 1ª Edição, Rio de Janeiro, Brasport, 2007.

[5] L. B. Mendes, "Documentoscopia", Atualizador: Wanira Oliveira de Albuquerque. Organizador: Domingos Tocchetto. 3ª Edição, Campinas, SP, Millennium Editora, 2010.

[6] L. Parodi, "Manual das Fraudes". 2ª Edição, Rio de Janeiro, Brasport, 2008.

[7] J. M. Pinheiro, "Biometria nos Sistemas Computacionais", 1ª Edição, Ciencia Moderna, 2008.

[8] R. Clarke, Human Identification in Information Systems: Management Challenges and Public Policy Issues, Information Technology & People, Vol. 7 Iss: 4, pp.6-37.

[9] P. Q. Silva, Reconhecimento Facial Baseado em Eigenfaces e em PCA - Principal *Component Analysis* com Múltiplos *Thresholds*. Dissertação de mestrado, Universidade de Brasília. 2000.

[10] F. A. F. Marques, Viabilidade de Implementação de um Sistema Biométrico de Autenticação, Dissertação de mestrado, Universidade de Aveiro, 2008.

[11] S. M. F. Costa, Classificação e Verificação de Impressões Digitais, Dissertação de mestrado, Universidade de São Paulo, 2001.

[12] G. F. F. Lourenço, Reforço da Segurança das Biométricas utilizando Codificação de Fonte Distribuída. Dissertação de mestrado, Universidade Técnica de Lisboa, 2009.

[13] G. T. A Guedes, "UML: uma abordagem prática", 2ª Edição, São Paulo, Novatec, 2006.

[14] D. G. Costa, Java em Rede: Recursos Avançados de Programação, 1ª Edição, Brasport, 2008.

[15] S. C. Vergara, Projetos e relatórios de pesquisa em administração, 15ª Edição, São Paulo, Atlas 2014.