FUNDAÇÃO DE ENSINO "EURÍPIDES SOARES DA ROCHA"
CENTRO UNIVERSITÁRIO EURÍPIDES DE MARÍLIA – UNIVEM
CURSO DE BACHARELADO EM SISTEMAS DE INFORMAÇÃO

Vítor Aurichio Espósito

Módulo Transacional de Biometria para Ambientes de Pagamento Off-line com Smart Card

MARÍLIA
2014

Vítor Aurichio Espósito

Módulo Transacional de Biometria para Ambientes de Pagamento Off-line com Smart Card

Trabalho de Curso apresentado ao Curso de Bacharelado em Sistemas de Informação da Fundação de Ensino "Eurípides Soares da Rocha", mantenedora do Centro Universitário Eurípides de Marília – UNIVEM, como requisito parcial para obtenção do grau de Bacharel em Sistemas de Informação.

Orientador
Profª: Dr. Fábio Dacêncio Pereira

MARÍLIA
2014

Espósito, Vitor

Módulo Transacional de Biometria para Ambientes de Pagamento Off-line com Smart Card / Vitor Espósito; orientador: Profª. Dr. Fábio Dacêncio Pereira. Marília, SP: ESPOSITO Vitor, 2014.

62 folhas

Monografia (Bacharelado em Sistemas de Informação): Centro Universitário Eurípides de Marília.

CENTRO UNIVERSITÁRIO EURÍPIDES DE MARÍLIA
BACHARELADO EM SISTEMAS DE INFORMAÇÃO

TRABALHO DE CONCLUSÃO DE CURSO – AVALIAÇÃO FINAL

Vítor Aurichio Esposito

Módulo Transacional de Biometria para Ambientes de Pagamento Off-line com Smart Card

Banca examinadora da monografia apresentada ao Curso de Bacharelado em Sistemas de Informação do UNIVEM/F.E.E.S.R., para obtenção do Título de Bacharel em Sistemas de Informação.

Nota: 7,0 (Sete)

Orientador: Fábio Dacêncio Pereira

1°. Examinador: Ildeberto de Gênova Bugatti

2°. Examinador: Rodolfo Barros Chiaramonte

Marília, 01 de dezembro de 2014.

Vitor Aurichio Espósito

Módulo Transacional de Biometria para Ambientes de Pagamento Off-line com Smart Card

Banca examinadora da monografia apresentada ao Centro Universitário Eurípides de Marília como parte dos requisitos necessários para a obtenção do grau de Bacharel em Sistemas de Informação.

Resultado: _____

ORIENTADOR: Dr. Fábio Dacêncio Pereira

1º EXAMINADOR: _____

2º EXAMINADOR: _____

Marília, ____de _____ de 2014.

A Deus, minha família e a todos os amigos que me ajudaram de alguma forma nesta caminhada difícil, mas não impossível e que me deram coragem e força o suficiente para chegar até aqui.

AGRADECIMENTOS

Aos meus colegas de sala, que com muito apavoro e medo enfrentaram estre trabalho de conclusão de curso com muita garra e determinações onde independentes do momento estavam sempre juntos um apoiando o outro.

A minha família que foi essencial nesta trajetória de muitas noites mal dormidas e muito trabalho e principalmente minha mãe que sempre esteve ao meu lado me apoiando e me dando forças para concluir este projeto.

Ao meu orientador Dr. Fabio Dacêncio Pereira que me motivou e me ajudou e muito nas reuniões onde cobrou e acompanhou todo o meu desenvolvimento sempre acreditando no meu potencial e na minha determinação.

Que os vossos esforços desafiem as impossibilidades, lembrai-vos de que as grandes coisas do homem foram conquistadas do que parecia impossível.
(Charles Chaplin)

RESUMO

Com o avanço tecnológico nas transações online, identifica-se uma dependência de serviço onde a conexão com a internet é vital ao decorrer de todo o processo. Porém o grande problema encontrado é quando esta conexão não é estabelecida com sucesso, por falta do serviço ou o mau funcionamento do mesmo. Desta forma, foi proposto um sistema para pagamentos off-line utilizando um smart card como ferramenta de pagamento, contudo como qualquer tipo de serviço de pagamento a segurança é fundamental, sendo que um dos requisitos que será destacado nesse projeto é a identificação do portador/usuário do smart card por meio da biometria. Neste contexto, a proposta desse projeto é, por meio de pesquisas, desenvolvimento e implementação elaborar um módulo Transacional de Biometria para Ambientes de Pagamento Off-line com Smart Card, além de adquirir um conhecimento sobre as técnicas de extração e análise biométrica não só especificamente o que será usado neste projeto.

Palavras-Chave: Biometria, Impressão Digital, Smart Card, meio de pagamento off-line

ABSTRACT

With the technological advance in online transactions, we identify a dependence on this service where the connection to the Internet is vital during the whole process. However, the great problem we find is when this connection is not established successfully, due to the lack of service or bad functioning of it. This way, it has been proposed a system for payments offline, using a smart card as payment tool, although, as in any kind of payment service, the security is a priority, being one of the requisites that will be highlighted in this project the identification of the smart card user through biometric ways. In this context, the proposal of this project is, through researches, developments and implementation, to elaborate a Transactional module of Biometric identification for Environments of offline Payment with Smart cards, besides acquiring a knowledge in extraction technologies and biometric analyses, beyond the ones that will be used in this project.

Keywords: Biometric, Fingerprint, Smart Card, Offline payment

LISTA DE ILUSTRAÇÕES

LISTA DE TABELAS

LISTA DE ABREVIATURAS E SIGLAS

APDU	*Application Protocol Data Units.*
CLA	*Class of instruction*
P1	Parâmetro um
P2	Parâmetro dois
INS	*Instruction code*
PIN	*Personal Identification Number*
PUK	*PIN unlock key*
RAM	*Random Access Memory*
EEPROM	*Eletric Erasable Programmable Read only Memory*
ROM	*Ready only memory*
JVM	Maquina Virtual Java
OCF	*OpenCard Framework*
CAP	*Converted Applet*
PADI	Processamento e Análise Digital de Imagens

SUMÁRIO

Introdução

Com o avanço tecnológico onde cada vez mais deixa-se as operações manuais em segundo plano, torna-se cada vez mais útil e importante a utilização de senhas e códigos de segurança, tornando assim, a segurança um ponto de extrema importância.

Porém, senhas ou códigos de segurança não são suficientes, pois não há garantia de que seja o proprietário ou um usuário com permissão que está se identificando e efetuando aquele acesso, ou também podem até serem extraídas com técnicas de engenharia social onde através da interação das pessoas ou o próprio convívio pode causar a extração de informações valiosas, consequentemente, podendo adivinhar a senha (COELHO, 2014). Procurando um novo meio para se conseguir uma maior segurança ou um meio para se identificar o usuário, pode-se adotar a biometria.

Biometria é a identificação através de traços biológicos e únicos que cada indivíduo possui, como por exemplo: retina, íris, forma da face, disposição das veias da mão e entre outros (LEONCIO, 2006). Para este trabalho foi escolhida a biometria com foco nas impressões digitais, mais especificamente as impressões do polegar, pois uma de suas vantagens é que as impressões digitais de uma pessoa permanecem inalteradas durante toda a sua vida e pode ser caracterizada por meio de formações únicas como: bifurcações, curvas, ou outras características que se denominam minúcias (MITINIK Kevin, 2014).

> "A extração das características da impressão digital é dividida em quatro partes: Pré-processamento, afinamento das linhas, extração de minúcias e pós-processamento. Depois de extraídas estas características, pode-se usar um algoritmo de identificação (*Matching*). Dentre essas etapas o pós-processamento é feito para diminuir os falsos negativos" (COELHO Igor de Carvalho, 2014).

Por meio dos estudos deste comportamento característico biológico, seja datiloscopia ou papiloscopia, pode-se chegar a uma validação conclusiva e plausível na identificação da pessoa. Além de ser um processo barato, simples, rápido e seguro, utilizado como uma das principais formas de identificação (THAI Raymond, 2014).

Processos de identificação das impressões digitais: Reconhecimento, verificação e identificação. Identificação e o reconhecimento trabalham com um exemplo contra um banco de dados (1:n) com o intuito de encontrar um par, enquanto a verificação trabalha a comparação de um exemplo com outro (1:1) para que o sistema conclua a identificação do usuário.

Existem muitas formas de se identificar duas digitais idênticas, observando o comportamento das linhas, distância entre elas, bifurcações, término de linhas, ou seja, está

fortemente acoplado ao tipo de algoritmo adotado. O foco deste projeto é identificar o algoritmo que mais se adere limitações de um *smart card*.

Motivação e Justificativa

Atualmente com as facilidades oferecidas por parte das empresas de cartão de crédito, é facilmente perceptiva a dependência que criamos neste tipo de serviço de pagamento. Contudo é necessária para a utilização deste serviço uma conexão web ou via telefone para atualizar e manter o serviço em funcionamento.

Analisando este cenário, foi iniciada uma pesquisa para que seja criada uma forma de pagamento para que o serviço não fique comprometido na falta de uma conexão a internet oferecida por terceiros, no caso um Módulo Transacional de Biometria para Ambientes de Pagamento Off-line.

Totalmente off-line, sem a necessidade de conexão, é uma boa solução para os problemas que o serviço disponibilizado atualmente pode apresentar garantindo que a transação seja concluída sem problema algum independente de qualquer tipo de fator externo.

Objetivos Gerais

Objetivo geral deste projeto é desenvolver um módulo transacional de biometria para pagamento off-line por *smart card* com foco na segurança. Este módulo irá conter um leitor biométrico, que irá capturar um modelo com características biométricas, precisando de um ou mais exemplos dependendo do hardware utilizado, e um software para tratar este exemplo identificando os pontos chaves pré-definidos pelo algoritmo, gerando assim um código matemático (assinatura) que será armazenado no *smart card* e posteriormente recuperado e reconhecido.

O leitor biométrico possui alguns recursos mínimos para a sua utilização como: Sistema operacional *Microsoft Windows* 2000/2003/XP/Vista/7, processador com uma arquitetura x86, um *scanner* biométrico e uma conexão entre o *host* e o *scanner*.

O leito de *smart card* utilizado para este projeto é o leitor Gemalto Gem PC Twin USB, e o *smart card* é o cartão *Java Card* Gemalto ICP D72 FXR1.

Os objetivos específicos estão divididos em:

- Por meio desta pesquisa, aprimorar conhecimentos sobre *smart card*;
- Conhecer não apenas a forma abordada neste projeto de identificação

biométrica, mas também construir um amplo conhecimento de todas as formas e validações de segurança;

- Pesquisar, escolher e implementar um algoritmo em c++ que fará a verificação da imagem gerada pelo leitor biométrico, tendo como objetivo desenvolver um projeto mais compacto possível e;
- Pesquisar e desenvolver a implantação de uma biblioteca c++ em uma aplicação java que controla o *applet* do *smart card*;

Organização do Trabalho

O projeto foi organizado em dois pilares: (i) tipos de biometria e especificamente a impressão digital e o *smart card*. Os primeiros capítulos I e II relatam uma base histórica e científica sobre a biometria para reforçar e justificar a escolha deste método para segurança.

Posteriormente são apresentadas as formas de tratamento de imagem, como pré-processamento, afinamento das linhas entre outros. Este processo foi ressaltado, pois, possui uma grande importância no processo de conversão da imagem para uma sequencia numérica de identificação.

No capítulo quatro descreve-se a biblioteca e que tipo de algoritmo foi utilizado para concluir o objetivo em extrair a biometria de um indivíduo, realizar os tratamentos necessários para a conversão e finalmente gravar em um *template* que será armazenado no *smart card*.

Para conclusão da monografia é proposto um modelo de integração com *smart card* e seu mecanismo de comunicação, segurança, armazenamento entre outros. Demonstrando assim todo o mecanismo que será utilizado e sua importância no resultado final esperado.

1 Conceitos e Aplicações de Sistemas Biométricos

Atualmente com o avanço tecnológico, pode-se identificar um crescente estudo em relação a identificação de um individuo através da biometria, demonstrando ser um dos métodos mais utilizados para esta finalidade. Podemos identificar muitos tipos de formas e métodos para se realizar este tipo de verificação, que será ressaltada e descrita neste capítulo além da base histórica relevante que este método possui.

A autenticação de pessoas é ultimamente um método muito utilizado para diversos tipos de finalidades, onde é possível identificar dois tipos: verificação e identificação (BOLLE apud COSTA Luciano R., OBELHEIRO Rafael R., FRAGA Joni S., 2006). Referente a verificação, a característica biométrica extraída é comparada juntamente com uma identidade alegada pelo usuário que está solicitando a verificação, portanto podemos definir que este tipo de autenticação é dita como 1:1, ou busca fechada em um banco de dados com perfis biométricos. Entretanto, na identificação o usuário fornece apenas sua característica biométrica para que seja comparada com o banco de dados lhe retornando o perfil mais compatível com a amostra coletada, dita como 1:N, ou busca aberta.

(Segundo CLARKE apud COSTA Luciano, 2006) Qualquer característica fisiológica ou comportamental humana pode ser usada como característica biométrica desde que ela satisfaça alguns requisitos básicos, que são elas:

- Universidalidade: Toda a população deve possuir a característica em questão;
- Unicidade: A característica precisa ser única, onde a possibilidade de dois indivíduos possuírem a mesma característica seja nula ou desprezível. Contudo é aceitável que uma compatibilidade possa ser encontrada em maior ou menor grau de unicidade, mas nunca idênticas;
- Permanência: É extremamente importante que as características sejam imutáveis, ou seja, não podem sofrer alterações ocasionadas por envelhecimento, mudanças de condições de saúde entre outros e;
- Coleta: A característica deve ser mensurada por meio de um dispositivo.
- Aceitação: A coleta deve ser tolerada pelo individuo em questão;

Nos dias de hoje, a grande maioria das formas utilizadas para verificação biométrica já estão de acordo com os requisitos básicos esperados, mas não é possível encontrar no momento nenhuma característica biométrica que atenda a todos os requisitos com perfeição. Ao decorrer dos tempos, pode-se identificar muitas tecnologias sendo pesquisadas e

desenvolvidas, portanto para isso foi feita uma classificação para estas tecnologias biométricas existentes, por conveniência, (Segundo COSTA Luciano, 2006) em dois grupos:

O primeiro grupo é classificado em: fisiológicas ou estáticas.

> "Essas características são traços fisiológicos, originários de carga genética do individuo, e essencialmente variam pouco (ou nada) ao longo do tempo. As principais características estáticas são a aparência facial, o padrão da íris, a geometria das mãos e as impressões digitais".

Este tipo de tecnologia biométrica pode ser utilizado em aplicações das mais variadas finalidades para o controle de acesso físico (liberar a entrada em uma sala de segurança, acesso a um cofre) ou de acesso lógico (*login* de uma aplicação) onde se cria um acesso com uma identificação eficaz e irrevogável. Segundo a qual todas as aplicações podem ser particionadas em sete categorias, pelo menos. (WAYMAN apud COSTA Luciano R., OBELHEIRO Rafael R., FRAGA Joni S., 2006).

Sendo assim, (Segundo OTAVIANO Christopher Henrique, 2007) sistemas biométricos podem ser utilizados em qualquer situação onde seja necessária a identificação ou a validação de uma determinada pessoa. Algumas situações onde a biometria é utilizada atualmente:

- Controle de Fronteira: Autenticando a identidades de viajantes que cruzam fronteiras internacionais, auxiliando na identificação de criminosos;
- Transações financeiras: Autenticando o usuário em transações financeiras ou permitindo acesso a terminais bancários;
- Identificação Pessoal: Auxilia na garantia de identificação de usuários de sistemas;
- Acesso Físico: Promove maior rigidez e segurança no controle de acesso a locais ou construções restritas e;
- Segurança Publica: Utilizada para cadastramento de pessoas a fim de garantir a segurança e identificar criminosos;

1.1 Breve histórico da biometria

Por muitas vezes, este tipo de tecnologia em questão era vista como uma tecnologia não muito utilizada ou fictícia. Contudo com o avanço tecnológico de empresas e pesquisadores nesta área, permitiu que a biometria se tornasse uma das formas de segurança

mais usadas e utilizadas atualmente.

Estudos comprovaram que havia diversas referencias sobre indivíduos que eram identificados pelas suas características físicas (altura, peso, cor dos olhos, cicatrizes, etc.). Eram sistemas usados no setor de agricultura, para identificação dos proprietários de grãos e provisões que eram armazenados em uma central.

Biometria (do grego *bios*: vida; *metron*: medida) é o uso de características biológicas em mecanismos de identificação. Designa um método automático de verificação ou reconhecimento baseado em medidas anatômicas, fisiológicas e características comportamentais de um indivíduo (CORRÊA Vanderlei Antônio, 2014).

A utilização das impressões digitais na identificação pessoal vem sendo observada desde a pré-história, quando povos primitivos marcavam com impressões digitais seus produtos de cerâmica. Os primeiro povos a usarem a impressão digital foram os chineses no século VII, em processos de divorcio, e posteriormente no século XIV, nos casos criminais.

Na Índia, durante o século IX, as impressões digitais foram usadas pelos analfabetos para a legislação de papeis (OTAVIANO Christopher Henrique, 2007). O sucesso neste modo de identificação foi tão satisfatório que logo toda a índia estava adotando este tipo de identificador.

Através de estudos e da evolução tecnológica, as técnicas utilizadas antigamente foram constantemente modificadas e melhoradas, novas ideias surgiram para deixar cada vez mais este tipo de identificação mais apurada e precisa.

1.2 Tipos de identificadores biométricos

Com o avanço da tecnologia, muitos serviços foram desenvolvidos para atender esta nova demanda de usuários que estavam disseminando e popularizando a internet. A transação de dados aumentou de forma significativa na mesma velocidade que a web crescia, trazendo com ela a necessidade de uma segurança que satisfaça o usuário.

Estes fatos impulsionaram o desenvolvimento e aprimoramento de métodos de identificação biométrico como forma de garantia de segurança (OTAVIANO Christopher Henrique, 2007). Aplicando-se em organizações, transações bancarias e até mesmo *smartphones*, este método evoluiu juntamente com os equipamentos de extração e coleta biométrica, utilizado hoje em numerosos projetos.

Biometria é a identificação através de traços biológicos e únicos que cada indivíduo possui, como por exemplo: retina, íris, forma da face, disposição das veias da mão e entre

outros (LEONCIO, 2006).

A biometria torna-se um componente essencial de soluções de identificação pessoal e eficaz porque esses traços biométricos não podem ser compartilhados, e eles representam o indivíduo. O reconhecimento de uma pessoa por seu corpo é uma ferramenta muito poderosa de gerenciamento de identidade com um potencial, tanto quanto positivo quanto negativo. Consequentemente, a biometria não é apenas um reconhecimento de padrões, se usado com cuidado, é uma tecnologia que permite tornar a nossa sociedade mais segura, reduzir a fraude e oferecer a conveniência do usuário (*user friendly* interface homem- máquina) (MALTONI Davide; MAIO Dario; JAIN Anil K.; PRABHAKAR Salil, 2009).

1.2.1 Geometria da Mão

A biometria da geometria da mão coleta uma imagem tridimensional e mede o seu tamanho e o comprimento dos dedos e das articulações. É um dos preferidos da indústria e tem sido utilizado por muitos anos predominantemente para aplicações de controle de acesso. Apesar da geometria da mão não alcançar os maiores níveis de precisão, seu uso é conveniente e a vantagem primordial é a grande quantidade de usuários que podem ser processados rapidamente (Consultores Biometricos, 2006).

(Segundo CUSTÓDIO Klecius Vinicius Assis, 2007) O processo de geometria da mão é o seguinte:

- Captura: o usuário coloca sua mão no leitor, alinha os dedos em guias especialmente posicionados. Uma câmera posicionada acima da mão ou abaixo dependendo do dispositivo, captura uma imagem. Medidas tridimensionais de pontos selecionados da mão são então tomadas;
- Extração: o equipamento biométrico extrai as medidas 3D em um identificador matemático único e então um *template* é criado e;
- Comparação: a geometria da mão é usada predominantemente para identificação um-para-um (1:1);

1.2.2 Íris

A íris é o anel colorido que circunda a pupila do olho. Cada íris possui uma estrutura única, caracterizando um padrão complexo. Pode ser uma combinação de características específicas como coroa, glândula, filamentos, sardas, sulcos radiais e estriamentos. É

conhecido que uma duplicação artificial da íris é virtualmente impossível devido às suas propriedades únicas. A íris é estreitamente ligada ao cérebro humano e dizem ser uma das primeiras partes a se desintegrar após a morte. É, portanto muito improvável que uma íris artificial possa ser recriada ou que uma íris morta possa ser usada para fraudar a passagem no sistema biométrico (Consultores Biometricos, 2006).

Foi relatada que a simplicidade de comparação garante o seu alto desempenho e é apropriado para fins de identificação de grande escala. Contudo reconhecer um individuo através da íris não é simples, levando em consideração os possíveis tipos de ruídos que podem estar presentes na imagem. Localizado atrás da córnea, que é um espelho altamente reflexivo, as imagens resultantes da extração podem ser, por conseguinte prejudicadas por reflexos de iluminação.

Este ruído é de difícil detecção uma vez que sua forma de localização é aleatória. Mesmo com essas dificuldades relatadas, ainda sim podemos considerar que por sua riqueza de informação e características, esta modalidade biométrica é considerada adequada e eficaz (DELACRETAZ Dijina Petrovska, 2009).

Um método muito utilizado em classificação de imagens de extração da iris é o filtro de Gabor. Isto devido as suas características, especialmente as representações de frequência e orientação, que são similares ao do sistema visual humano. Além disso, o filtro tem propriedades de localização espacial, orientação seletiva e seletividade espaço-frequencial, permitindo assim que a extração de características possa ser realizada.

É comum que os algoritmos de reconhecimentos de íris simulem mudanças que possam acontecer, como a expansão e contração da pupila em resposta a luz, por exemplo. Estas informações recolhidas nesta etapa do processo são utilizadas para compor o *IrisCode* (Código de identificação da Iris), que possui um registro de 512 bytes (OTAVIANO Christopher Henrique, 2007).

1.2.3 Retina

A retina é a camada de veias sanguíneas situada na parte de trás do olho. Assim como na íris, a retina forma um padrão único e começa a se desintegrar logo após a morte. As biometrias de retina são geralmente tidas como o método biométrico mais seguro. O acesso não autorizado em um sistema de retina é virtualmente impossível. Um procedimento preciso de cadastramento é necessário, o que envolve o alinhamento da vista para alcançar uma leitura otimizada (Consultores Biometricos, 2006).

A área em torno do disco óptico tem uma alta concentração de vasos sanguíneos e, além disso, o disco óptico está perto do ponto de rotação dos olhos, por conseguinte a parte mais estável da retina em termos de extração de imagens, denominado movimentos oculares.

O primeiro passo de codificação é a identificação de vasos sanguíneos dentro de cada imagem, onde serão separadas a partir de *distracters*, tais como a textura da coroide. A localização e percurso dos vasos sanguíneos da retina, em seguida, são quantitativamente descrito e sua estrutura é identificada e reduzida para uma modelo de codificação eficiente. Ao final define-se uma similaridade entre os padrões dos vasos sanguíneos codificados e o cálculo final desta similaridade deve levar em conta as diferenças entre as duas imagens de origem (RATHA Nalini K.; GOVINDARAJU Venu, 2008).

1.2.4 Voz

Verificação de voz consiste em verificar a identidade reivindicada de uma pessoa através do som de sua voz. A voz é um produto de um comportamento complexo que transmite diferentes traços específicos que são potenciais fontes de informação complementares. Consequentemente, os seres humanos usam vários níveis de estímulos perceptivos para o reconhecimento da voz, estas características podem ser classificadas em "alto nível" e atributos "de baixo nível" (DELACRETAZ Dijina Petrovska, 2009).

(Segundo RATHA Nalini K.; GOVINDARAJU Venu, 2008) Como exemplo, podemos considerar a estimativa da *Mel frequency cepstral coefficients* (MFCCs), que são os recursos mais utilizados no processo de reconhecimento. O processo pode ser dividido em três passos: Em primeiro lugar, as características básicas são calculadas da seguinte forma, o segmento de voz é dividido em segmentos sobrepostos. A resposta de frequência é calculada em cada uma delas e a saída é então processada com um banco de filtros centrado uniformemente em uma escala *Mel*. Os *cepstral coefficients* correspondem a transformada discreta de saída dos filtros.

No segundo passo, uma variedade de transformações é aplicada aos MFCCs para reduzir sua sensibilidade ou estender seu poder expressivo. Estas transformações incluem: cálculo de coeficientes de delta, *cepstral mean subtraction* (CMS), *coefficient stream filtering* (HERMANSKY apud RATHA Nalini K.; GOVINDARAJU Venu, 2008), e normalização com base em histograma (PELECANOS apud RATHA Nalini K.; GOVINDARAJU Venu, 2008). Finalmente, os MFCCs transformados são condicionados a palavras ou identidades obtidas a partir de um reconhecedor de voz automático (ASR) e modelado separadamente.

1.2.5 Face

Identificar um indivíduo através da análise da face é um processo complexo que normalmente requer artifícios inteligentes sofisticados e técnicas de aprendizagem computacional (*machine learning techniques*). Uma quantidade de fornecedores biométricos está envolvida na venda desses sistemas, usando tanto vídeos padrões como imagens termais para capturar imagens faciais (CUSTÓDIO Klecius Vinicius Assis, 2007).

O reconhecimento facial se destaca como a modalidade mais atraente, na medida em que é o modo natural de identificação entre os seres humanos. Ao mesmo tempo, no entanto, ele é uma das modalidades mais difíceis (ZHAO apud RATHA Nalini K.; GOVINDARAJU Venu, 2008). A investigação sobre reconhecimento de face foi desenvolvido para ser identificado mais visualmente por uma variedade de razões. (Segundo PAVLIDIS apud RATHA Nalini K.; GOVINDARAJU Venu, 2008) São eles: disponibilidade e baixo custo de câmeras para o reconhecimento e o fato inegável de que o reconhecimento do rosto é uma das principais atividades do sistema visual humano.

Porem o reconhecimento de rostos humanos, no entanto, tem se mostrado mais problemático do que o reconhecimento de rosto executada por seres humanos. O grande culpado é a variabilidade de luz, que é predominante no momento da visualização que pode ocasionar em diferentes resultados de comparação dificultando a analise da imagem. Problemas secundários estão associados com a dificuldade de detectar possíveis disfarces faciais.

1.2.6 Assinatura Manuscrita

A biometria de assinatura geralmente é denominada como uma Verificação Dinâmica de Assinatura (DSV) e observa a forma como assinamos nossos nomes. O DSV pode ser diferenciado do estudo estatístico de assinaturas em papel. Algumas características podem ser extraídas e medidas pelo DSV. Por exemplo, o ângulo no qual a caneta é segurada, o tempo que se leva para assinar, a velocidade e a aceleração da assinatura, a pressão exercida quando segura-se a caneta e o número de vezes que a caneta é levantada do papel - tudo isso pode ser extraído como características comportamentais únicas. O DSV não é baseado em uma imagem estática, portanto mesmo que uma assinatura seja copiada, um impostor precisará saber a dinâmica da assinatura. Isso torna a falsificação muito difícil (Consultores Biometricos, 2006).

A assinatura é o meio mais aceitável socialmente e juridicamente e é, portanto, uma modalidade confrontada com ataques de alto nível. Quando uma pessoa quer burlar um sistema, o mesmo forja a assinatura de outra pessoa, tentando reproduzir o mais próximo possível a assinatura do alvo. Este tipo de verificação biométrica é favorável à verificação da identidade desta assinatura, porque a fim de produzir uma falsificação, o impostor tem de reproduzir mais do que a imagem estática da assinatura, isto é, um pessoal e bem aplicado "gesto" de assinatura, mais complexo de se reproduzir do que a própria imagem da assinatura.

Contudo, não é uma característica muito estática, pois a assinatura de um individuo pode ser afetado por diferente motivos, tornando esta verificação um desafio enorme para a pesquisa e avaliação, mas por causa de sua ampla utilização, permanece um campo promissor e com grande potencial no ponto de vista de seu desenvolvimento (DELACRETAZ Dijina Petrovska, 2009).

1.2.7 Impressão Digital

Impressões digitais humanas foram descobertas em um grande número de artefatos arqueológicos e itens históricos e embora esses resultados forneçam evidências de que os povos antigos estavam cientes da individualidade das impressões digitais, tal consciência não parece ter qualquer século que a técnica de impressão digital foi iniciada (GAENSSLEN apud MALTONI Davide, 2009, p. 31).

A primeira descrição detalhada da formação de impressões digitais foi realizada por Mayer em 1788, em que uma série de características de impressões digitais foram identificadas e caracterizadas. A partir de 1809, Thomas Bewick começou a usar impressão digital como sua marca registrada, um dos marcos mais importante na história de impressões digitais. Purkinje , em 1823, propôs a primeira classificação de impressões digitais, onde classificou as impressões digitais em nove categorias (MOENSSENS apud MALTONI Davide, 2009).

A impressão digital de uma pessoa permanece inalterada durante toda a sua vida e pode ser caracterizada por meio de formações únicas como: bifurcações, curvas, ou outras características que se denominam minúcias (THAI, 2003).

> “A extração das características da impressão digital é dividida em quatro partes: Pré-processamento, afinamento das linhas, extração de minúcias e pós-processamento. Depois de extraídas estas características, pode-se usar um algoritmo de identificação (*Matching*).

> Dentre essas etapas o pós-processamento é feito para diminuir os falsos negativos” (COELHO, 2011).

No passo de combinação, as características extraídas da impressão digital de entrada são comparadas contra os dados armazenados (obtidos a partir de uma base de dados com base na identidade reivindicada). O resultado do processo obtido é um grau de semelhança (também chamado de pontuação correspondente) ou uma decisão de aceitação/rejeição.

Existem técnicas de correspondência de impressão digital que comparam diretamente as imagens em escala de cinza utilizando métodos à base de correlação, de modo que o modelo de impressão digital coincida com a imagem em escala de cinza comparada. No entanto, a maior parte dos sistemas de reconhecimento de impressão digital é feita por características extraídas por algoritmos a partir da imagem em escala de cinza (DELACRETAZ Dijina Petrovska, 2009).

Por meio dos estudos deste comportamento característico biológico, qual seja datiloscopia ou papiloscopia, pode-se chegar a uma validação conclusiva e plausível na identificação da pessoa. Além de ser um processo barato, simples, rápido e seguro, utilizado como uma das principais formas de identificação (THAI, 2003).

Processos de identificação das impressões digitais: Reconhecimento, verificação e identificação. Identificação e o reconhecimento trabalham com um exemplo contra um banco de dados (1:n) com o intuito de encontrar um par, sendo denominado busca aberta, enquanto a verificação trabalha a comparação de um exemplo com outro (1:1) para que o sistema possa reconhecer e identificar o usuário, conhecido como busca fechada.

1.3 Considerações finais do capitulo

Após a realização desse estudo sobre o conceito de característica biométrica e suas variadas formas e tipos de extração, comparação, grau de segurança, vantagens e desvantagens apresentados neste projeto podemos identificar que para se encontrar um método que mais se encaixe no ambiente proposto muitas variáveis precisam ser levadas em conta, como a situação em que o identificador ira ser aplicado, lugar, necessidade, entre outras.

Concluindo assim que nenhuma característica está no seu estado de perfeição, porém em constante pesquisa e evolução para se conseguir com mais exatidão possível e eficaz a identidade do individuo. Muitos autores recomendam ainda que uma solução plausível para se alcançar a identificação precisa de um individuo seria combinar mais de uma característica.

2 Referencial teórico para reconhecimento de impressão digital

A identificação através da impressão digital é uma das formas mais utilizadas e mais conhecidas atualmente, pois se caracteriza por ser um método barato e fácil de implementação comparado aos outros métodos, sendo o foco deste projeto. Será descrito todo o processo que uma imagem coletada por um *scanner* deve se submeter até ser convertida em uma sequencia numérica para identificação.

As impressões digitais estão totalmente formadas em cerca de sete meses de desenvolvimento do feto. Estas características não mudam ao longo da vida de um indivíduo, exceto devido a acidentes, como contusões e ou cortes nas pontas dos dedos (Babler apud MALTONI Davide, 2009). É por estas e outras razões que as impressões digitais se tornam um atraente identificador biométrico onde aparência física e impressões digitais são, em geral, uma parte do fenótipo de um indivíduo onde sua formação é semelhante ao crescimento de vasos sanguíneos. Há tantas variações durante sua formação que é praticamente impossível que duas impressões digitais sejam exatamente iguais mesmo não seguindo nenhum padrão, tornando assim totalmente aleatórias. (MALTONI, 2009)

A aquisição de impressões digitais ao longo do tempo foi se modificando e se aperfeiçoando juntamente com a evolução tecnológica, sua forma de extração inicialmente era o processo de espalhar tinta na superfície do dedo e pressionado a um cartão de papel que posteriormente seria utilizado para a identificação. Contudo hoje já podemos encontrar modos mais tecnológicos, rápidos e precisos para este tipo de verificação biométrica, como sensores que detectam e reproduzem uma imagem biométrica que utilizando-se de algoritmos pré-programados fazem a identificação e armazenamento da imagem.

(Segundo GOMES, 2001) De acordo com a figura 1, podemos conferir este processo utilizando o termo Processamento e Análise Digital de Imagens (PADI) para demonstrar sua sequência que engloba as técnicas de PDI e ADI.

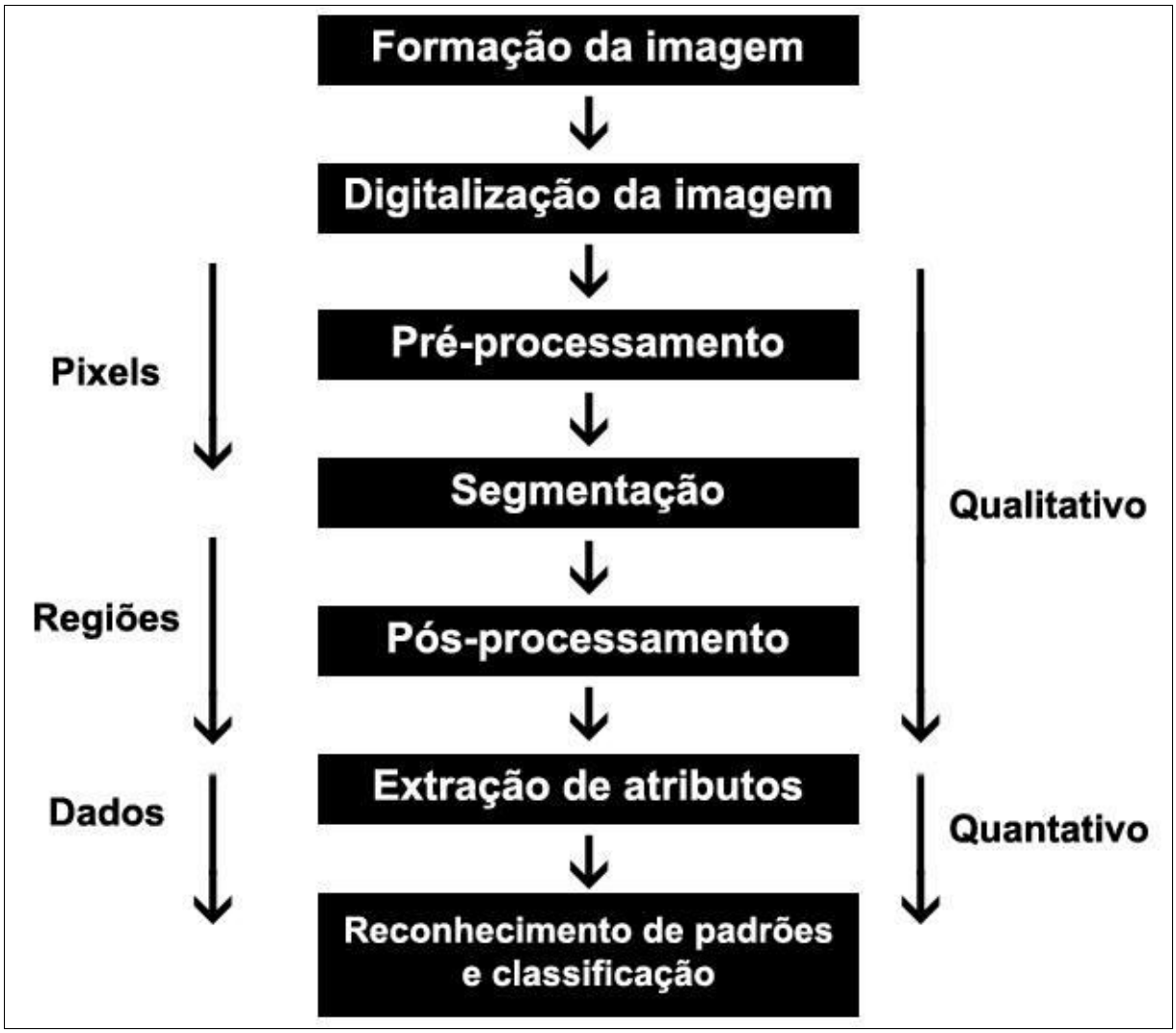

Figura 1 Sequência padrão de PADI (GOMES, 2001)

2.1 Identificação e reconhecimento de impressão digital

O reconhecimento e a identificação da impressão digital, se feito manualmente por um especialista humano ou automaticamente por uma máquina, é predominantemente baseada em recursos utilizando interpretação física e comparações. Através de uma amostra de traços físicos que o indivíduo possui é possível comparar ou até mesmo criar pontos chaves de identificação que varia do tipo de algoritmo utilizado.

(Segundo DORIZZI, 2009) Podem-se encontrar três tipos de sensores com base na tecnologia eletrônica para a extração e identificação biométrica:

- *Solid-State* ou sensores de silicone – Trata-se de uma matriz de pixels, sendo que cada pixel é um sensor. Sua forma de utilização se define em posicionar o dedo verificador sobre a superfície e sua identificação pode ser realizada de

algumas formas como: capitação térmica, elétrica entre outros. Sua grande vantagem, em consequência da tecnologia utilizada é que seu tamanho físico é considerável;

- Óptica – Para a identificação o procedimento inicial é o posicionamento do dedo verificador em um vidro onde será iluminada com uma luz difusa, a luz é refletida e focada para um sensor CCD ou CMOS, tornando uma das melhores formas de extração por suportar uma ampla área de detecção com uma boa qualidade de imagem e;
- Ultra-som – São enviados sinais acústicos e consequentemente capturando os sinais refletidos na superfície da impressão digital. Tem como vantagem a capacidade de atravessar qualquer impureza presente na pele conseguindo concluir a identificação, porem como este tipo de tecnologia fica quase que inviável pelo tamanho dos scanners e pela demora necessária que o mesmo leva até a identificação;

(Segundo COELHO, 2011) A extração biométrica é uma das formas mais plausíveis no ponto de vista da identificação de um individuo que se divide em quatro partes: Pré-processamento, afinamento das linhas, extração das minúcias e pós-processamento. Depois de todo o processo é aplicado algoritmo(s) de identificação (*Matching*).

2.1.2 Pré-processamento

O pré-processamento consiste em melhorar a imagem extraída a fim de aplicar os filtros e comparações necessárias eliminando assim quaisquer problemas na visualização das minúcias ou imperfeição que possa ocasionar na falha do processo. Uns dos filtros que podem ser utilizados para este processo denomina-se filtro de Gabor, baseado em frequência onde possibilita o realce das linhas afinando-as em apenas um pixel de espessura.

Este filtro necessita de duas informações sobre a imagem avaliada: a direção e a frequência das linhas, posteriormente extraindo as minúcias levando em conta como identificação as bifurcações e as terminações de linhas (COELHO, 2011).

(Segundo GOMES, 2001) Os procedimentos realizados por esta etapa são operações matemáticas que operam diretamente sobre os *pixels* das imagens podendo ser divididas em quatro tipos:

- Operações pontuais: Esta função pode ser caracterizada por linear que modifica o brilho e o contraste da imagem, não alterando muito a forma de

seu histograma ou não-lineares que alteram mais acentuadamente a forma do histograma da imagem, modificando alguma região do histograma ou visando dar a ele uma forma determinada;

- Operações entre imagens: Envolvem duas ou mais imagens onde um operador varre *pixel* a *pixel* relacionando os *pixels* correspondentes;
- Operações locais: Conhecido também como operações de vizinhança ou filtros espaciais são operações que definem um determinado *pixel* de saída baseado não somente no *pixel* analisado e sim aos outros *pixels* vizinhos presentes e;

Operações geométricas: São operações onde a relação entre os *pixels* é alterada. Consiste em uma transformação espacial que é muito útil no tratamento de imagens com problema de baixa resolução;

2.1.3 Segmentação

Este processo de analise de imagem tem como principal objetivo a extração do fundo para que os traços principais que serão analisados fiquem realçados e sem nenhum ruído ou algo que atrapalhe sua analise, é a partir deste resultado que o algoritmo pode identificar os pontos chaves na identificação de uma biometria principalmente no caso da extração de impressões digitais.

Tudo se inicia com a captura de uma imagem, a qual normalmente corresponde à iluminação que é refletida na superfície dos objetos, realizada através e um sistema de aquisição. Após a captura por um processo de digitalização, uma imagem precisa ser representada de forma apropriada para tratamento computacional. Imagens podem ser representadas em duas ou mais dimensões e o primeiro passo efetivo de processamento é comumente conhecido como pré-processamento, o qual envolve passos como a filtragem de ruídos introduzidos pelos sensores e a correção de distorções geométricas causadas pelo sensor (QUEIROZ, 2001).

2.1.4 Limiarização

Limiarização nada mais é que definir um valor padrão que será utilizado como parâmetro na hora de identificar se o *pixel* que no caso será analisado individualmente pertence ao *background* ou a região de interesse. O sucesso desta verificação depende do quão

bem definido esta às massas de *pixels* no histograma da imagem segmentada.

Fundamentada na análise da similaridade de níveis de cinza, de modo a extrair objetos de interesse mediante a definição de um limiar T que separa os agrupamentos de níveis de cinza da imagem. Uma das dificuldades do processo reside na determinação do valor mais adequado de limiarização, do ponto de separação dos *pixels* da imagem considerada.

Através da análise do histograma da imagem, é possível estabelecer um valor para T na região do vale situado entre picos que caracterizam regiões de interesse na imagem. Há diversas variantes onde a mais simples delas é a técnica de particionamento do histograma da imagem por um limiar único T. A segmentação define-se em analisar a imagem, *pixel* a *pixel*, e rotulando cada um como sendo do objeto ou do fundo, em função da relação entre o valor do *pixel* e o valor do limiar (QUEIROZ, 2001).

Muitas vezes é necessária a identificação de mais de um objeto em uma imagem, sendo suficiente a utilização deste método para alcançar o objetivo esperado. A limiarização multi-modal onde é definido *n* fases determinando o inicio e o fim de uma faixa tonal onde será identificado o fundo da imagem e ressaltado os objetos para identificação. (GOMES, 2001)

2.1.5 Binarização

Neste processo de binarização, o objetivo é reduzir uma imagem a apenas dois valores reconhecidos apenas pelos identificadores zero ou um. Através de um limiar (*threshold* ou valor de corte) é determinado um valor base de forma que todos os valores inferiores sejam levados a base ou identificados como *background* e os superiores sejam levados ao valor de topo que será a parte de interesse da imagem. É possível também obter uma imagem com apenas dois níveis, partindo de uma imagem em escala cinza (OTAVIANO Christopher Henrique,2007).

Existem varias técnicas que aplicam esta técnica de alterar uma imagem com 256 níveis de cinza em uma imagem binária, reduzindo os dados a serem tratados facilitando a extração e analise do manuscrito. (Segundo SARAMELA, 2011) Uma das formas utilizada é a Global de OTSU, que apresenta um dos melhores resultados, pois não causa perda de informação.

Este método caracteriza-se por sua natureza não paramétrica e não supervisionada de seleção de limiar e possui algumas vantagens como: O processo como um todo é simples de se realizar, são utilizadas apenas os momentos cumulativos zero e de primeira ordem do

histograma de níveis de cinza e viabiliza a análise de outros aspectos importantes, tais como estimativa dos níveis médios das classes e, separabilidade das classes (MONTEIRO, 2013).

Pode-se também identificar outras técnicas utilizadas como: limiarização iterativa ou método iterativo de Lam-Leung, algoritmo de Chehikian, Fisher Lat, Fuzzy Yager, Renyi, entre outras técnicas (ALVES,2004).

2.1.6 Afinamento

Afinamento nada mais é que um algoritmo que retira os pixels redundantes sem afetar o formato ou a conectividade dos objetos deixando os traços da imagem com apenas um pixel de largura, trazendo uma melhor eficiência na comparação das características. (Segundo OTAVIANO, 2007) A fórmula de *Holt* com a *staircase removal* se constitui em uma poderosa ferramenta para afinamento, superando os resultados do algoritmo de Zhang Suen, sendo mais rápido e simples de implementar.

2.1.7 Filtros

Filtros são constantemente utilizados em imagens para realçar bordas, valorizar o contraste, suavizar a imagem entre varias outras finalidades. Para a extração biométrica pode ser utilizado dois filtros em questão: filtro de média e filtro direcional (OTAVIANO, 2007).

A grande dificuldade da aplicação de filtros são os fatores externos como iluminação ou até mesmo a separação e identificação de cores similares, fazendo-se necessário somente utilizar imagens em escala cinza para garantir que este problema não ocorra.

2.1.8 Extrações de minúcias

Uma das técnicas mais utilizadas para a extração de minúcias é conhecida como *Crossing Number* (CN). Essa técnica determina as propriedades de um *pixel* simplesmente contando o número de transições preto e branco existentes na vizinhança do *pixel* que está sendo processado (OTAVIANO, 2007).

Após a imagem estar disponível para a verificação através dos pontos de *pixel*, é identificado bifurcações que são reconhecidos por três pontos de *pixel*s e terminações de crista identificados quando é apresentado apenas um *pixel*. Na prática, algumas das minúcias são detectadas após passar por um processo onde a mesma será filtrada para remover qualquer

ruído que possa prejudicar a imagem consequentemente a identificação.

Como exemplo, podemos citar os tipos de minúcias que apresentam algum tipo de imperfeição: Minúcias que não têm um cume adjacente em ambos os lados (principalmente as terminações de linhas). Minúcias que terminam em direções opostas (a diferença entre duas direções chega a aproximadamente 180 ◦), entre outras características. (JAIN, 2011)

2.1.9 Pós-processamento

Este processo é realizado ao fim de todas as etapas que uma imagem deve ser submetida para tratamento como: pré-processamento, limiarização, filtros entre outros. Seu objetivo é corrigir imagens binarias aplicando procedimentos como: separação de objetos que se tocam ou agrupamento de objetos mais complexos, implementados através de operações lógicas e operações morfológicas.

2.2 Considerações finais do capítulo

É facilmente perceptivo a importância que a extração biométrica possui em relação a identificação de um individuo, possuindo uma tecnologia em constante evolução e acessível onde priorizado como elemento chave a segurança, consequentemente escolhida e utilizada para este projeto.

É necessário alguns processos até se chegar a um *template* ou a uma amostra valida para identificação de uma impressão digital, pois o mesmo não deve possuir nenhum ruído e seu objetivo é tornar a imagem o mais simples possível para a conversão em binário.

3 Trabalhos Correlatos

No cenário atual identificamos a biometria como um dos métodos mais utilizados na questão da segurança para a identificação de um indivíduo. Existem muitos recursos para se definir a identificação de uma pessoa como impressão digital, face, palma da mão, íris entre outros.

Segundo ARAUJO (2010), podemos identificar como uma solução de segurança um controle de identificação utilizando a biometria e um *smart card*. O sistema irá permitir o cadastro de usuários, capturando sua impressão digital e os dados cadastrais, posteriormente o usuário é vinculado a um cartão inteligente. O acesso será liberado apenas quando o individuo for identificado como proprietário do cartão.

> "O diferencial do projeto está na unificação de tecnologias de segurança já contempladas. A posse de um cartão inteligente **e a impressão digital constitui** um controle de acesso baseado em dois fatores: autenticação baseada no que se possui e autenticação baseada nas características individuais**."**

É possível identificar um indivíduo através da combinação de dois ou mais métodos para se alcançar o objetivo esperado, sendo descritos a seguir:

- Autenticação baseada no que se conhece: Este nível de segurança é o mais baixo, pois se baseia no conhecimento de senhas, chaves criptográficas ou nomes para acesso ao sistema;
- Autenticação baseada no que se possui: Se caracteriza por algo que o usuário possua para ter acesso ao sistema como: *smart cards*, *tokens* entre outros dispositivos dotados de memória ou não que servem como chave de acesso. Este processo possui mais recursos de segurança do que o exemplo anterior citado e;
- Autenticação baseada nas características individuais: Trata-se de alguma característica única que o individuo possua, baseado em sua medida fisiológica, característica comportamental ou até mesmo sua biometria. Exemplo: Mão, íris, impressão digital, assinatura. É o nível mais recomendado e mais seguro do que os outros métodos anteriores;

Portanto através destes recursos biométricos, o mesmo tem como objetivo utilizar um leitor biométrico para a captura da impressão digital, um leitor e gravador de *smart card* para efetuar o armazenamento dos dados extraídos. Sua integração ocorrerá através de um *software* responsável pela captura biométrica e armazenamento da cadeia de caracteres em um banco de dados.

Posteriormente será atribuído mais alguns dados a esse resultado e criptografado e somente ao final deste processo o mesmo será alocado em algum *container* disponível do *smart card*.

O possível problema a ser enfrentado por este projeto será a garantia de que a conexão ao banco de dados ou os dados armazenados fiquem corretos ao armazenar no *smart card* onde há a preocupação de que garantir um espelhamento dos registros para que as informações dos dois lados fiquem identificas.

Segundo TONHÁ (2011) A utilização de um *smart card* com a tecnologia biométrica soluciona também um problema ocorrente em lojas virtuais em relação a fraude ou clonagem de cartões, que utilizando-se de dados para verificação armazenados garante uma validação por meio desta como garantia de que o portador do cartão é realmente o proprietário e que sua utilização esta autorizada.

Nos dias de hoje pode-se utilizar como medida para evitar fraudes ou possíveis prejuízos aos comércios eletrônicos três medidas básicas de segurança:

- Identificação minuciosa dos clientes: Verificar documentos com fotos para se constatar a identificação do mesmo, verificando os dados na receita federal, sistema de proteção ao credito (SPC, Serasa e etc.) para garantir que o comprador é de boa índole;
- Verificação dos itens de segurança do cartão: É informado e verificado as todas a informação necessária para autenticação do cartão como seu código de segurança, data de validade entre outros e;
- Utilização da tecnologia *smart card*: A utilização de um cartão com esta tecnologia possibilita que o usuário valide sua senha através do código PIN dentro de um ambiente seguro;

Seguindo um mesmo padrão apresentado no projeto anterior, o autor descreve que será utilizado um cartão *smart card*, um leitor e um leitor biométrico onde o processo será: Extração da biometria do usuário, armazenamento dos dados com algumas novas informações além do código de identificação gerado que para o projeto é necessário e seu armazenamento a um banco de dados.

Vale ressaltar que o mesmo pode enfrentar alguns problemas ao depender de um fator externo que é a conexão com a internet, pois o ambiente onde o mesmo será implementado necessita deste tipo de serviço. Sua única diferença é o foco com o qual o projeto esta proposto a solucionar.

Para BONATO (2011), os métodos biométricos por impressão digital são ideias para

a utilização em sistemas de identificação, além das técnicas de reconhecimento das impressões, focando no reconhecimento por cristas e minúcias, onde ambas as técnicas utilizam-se de operações de pré-processamento, ressaltando ainda mais o porque a biometria é de extrema importância para este projeto.

Segundo o autor podemos descrever três tipos de abordagens relacionadas a identificação de uma impressão digital:

- Baseada em correlação: Duas imagens com a mesma escala de cores são comparadas *pixels* a *pixels* para identificar se as duas imagens pertencem ao mesmo individuo;
- Baseado em minúcias: Consiste em identificar na imagem extraída a quantidade de pontos característicos presentes no *template* para garantir assim através desta soma se a impressão digital comparada é a mesma que a analisada e;
- Baseada em cristas: Localiza e identifica todas as cristas presentes na imagem para utilizar a quantidade encontrada como resultado da comparação;

Além dos tipos de abordagem, o projeto ainda especifica como deve ser filtrada e tratada a imagem para que se consiga uma comparação de qualidade para que seu resultado seja preciso. O foco em questão é demonstrar o quão importante é o pré-processamento de imagem antes que um algoritmo de identificação biométrica seja utilizado.

O objetivo do projeto é demonstrar através de pesquisas a importância que a biometria tem atualmente e a evolução tecnologia que a acompanha onde define-se técnicas e métodos para esta área da impressão digital.

Como exposto por MINORA, ALEIXO e DIOLINO (2007) é possível desenvolver aplicações para um *smart card* ou *Java card* utilizando subconjuntos da plataforma Java. Contudo programar para este tipo de tecnologia não é simples, pois a comunicação entre o *host* e o cartão é feita por sequencias de *bytes* utilizando uma camada de comunicação conhecida como APDUs (*Application Protocol Data Unit*).

Os *applets* Java são classes Java convencionais que possuem a regra de negocio que será aplicada e as funções necessárias que estendem da classe javacard.framework.Applet. As classes e os *applets* são empacotados em um único arquivo chamado CAP (*Converted Applet*), onde é inserido e instalado no cartão.

As aplicações *host* são aplicações externas que controlam o *applet* podendo ser programado em qualquer linguagem desejada. Para a linguagem Java é possível utilizar-se o *OpenCard Framework* (OCF), que é um conjunto de bibliotecas desenvolvida para facilitar a

comunicação entre diferentes *hardwares* e *softwares* podendo ser utilizada em qualquer maquina ou dispositivo que apresente uma maquina virtual Java (JVM) compatível.

O projeto ainda ressalta como é efetuada a comunicação entre os dispositivos através de uma camada de transporte se preocupando com a segurança onde a plataforma utilizada (*OpenPlataform*) deve estar em concordância com o componente *Card Manager*. Este componente é uma aplicação responsável pela administração da central que realiza múltiplas responsabilidades.

A partir disto foi possível desenvolver neste projeto uma ferramenta denominada *Smart Interface* que é um software livre com o objetivo de aperfeiçoar o *smart shell* alterando o modo com que esta ferramenta demonstrava seus dados transformando-o em uma ferramenta gráfica.

Este projeto tem a sua importância, pois traz um projeto e uma ferramenta para desenvolvedores de *smart card* identificarem e realizarem algum tipo de comunicação de forma facilitada e agilizando diversas operações através desta interface gráfica elaborada e desenvolvida.

4 Projeto e implementação de módulo transacional de biometria

Para êxito dos objetivos desse projeto é importante a identificação de um algoritmo que se encaixe nos requisitos mínimos esperados para realizar todos os procedimentos pré-definidos por este projeto. Será descrito de que forma a aplicação que controlará o leitor possa gerar um *template* da assinatura biométrica para ser armazenado em um *smart card.*

Inicialmente, cumpre esclarecer que o presente projeto foi realizado através de um algoritmo fornecido pela empresa de desenvolvimento Zhongkong Automation System Inc. Ltda especializada em investimentos de risco, finanças, títulos, imóveis e produção de produtos de base tecnológica biométrica e fornecedora do produto ZKFinger utilizado e estudado para este projeto. Possui código totalmente aberto para desenvolvedores de software que podem utilizar-se da sua eficácia para identificação biométrica tanto para 1:1 (um para um) quanto para 1:N (um para muitos).

Em 1999 a empresa realizou um investimento em uma de suas filias no setor de desenvolvimento e pesquisa de produtos tecnológicos biométricos visando seu desenvolvimento, e dedica-se na promoção e divulgação dos produtos biométricos desde então. Localizado na China, porém com seus produtos comercializados pelo mundo todo, a empresa atingiu um reconhecimento quase que imediato com mais de 2500 produtos utilizados por todas as instituições governamentais da China.

O algoritmo utilizado conta com um desempenho rápido e eficaz com uma série de vantagens especificadas pela empresa como: Rapidamente integrados a qualquer tipo de sistema em questão, com suporte a qualquer dispositivo ou scanner de impressão digital. Trata todo ruído ou qualquer coisa que danifique ou impeça a identificação ou armazenamento de qualidade, utilizando-se de contraste e realce nas linhas extraídas para alcançar este objetivo, além de ser projetado para utilizar de pouca memória visando a utilização em sistemas embarcados.

4.1 Arquitetura utilizada pelo ZKFinger

Utilizando deste software é possível o usuário construir aplicações em diversas linguagens que suportam o controle ActiveX como: VC++, C++, Delphi, VB, Visual FoxPro, PB, entre outros. Podemos identificar seu funcionamento na figura 2 onde basicamente segue a seguinte ordem em níveis de execução: Aplicação (códigos, interface, funções), logo em seguida o controle ActiveX que possui todas as funções pré-definidas e funciona como um

controle entre a aplicação e o driver do dispositivo instalado, em seguida o driver do dispositivo que irá repassar para a aplicação o *template* adquirido e por fim o scanner biométrico ou a imagem a ser analisada.

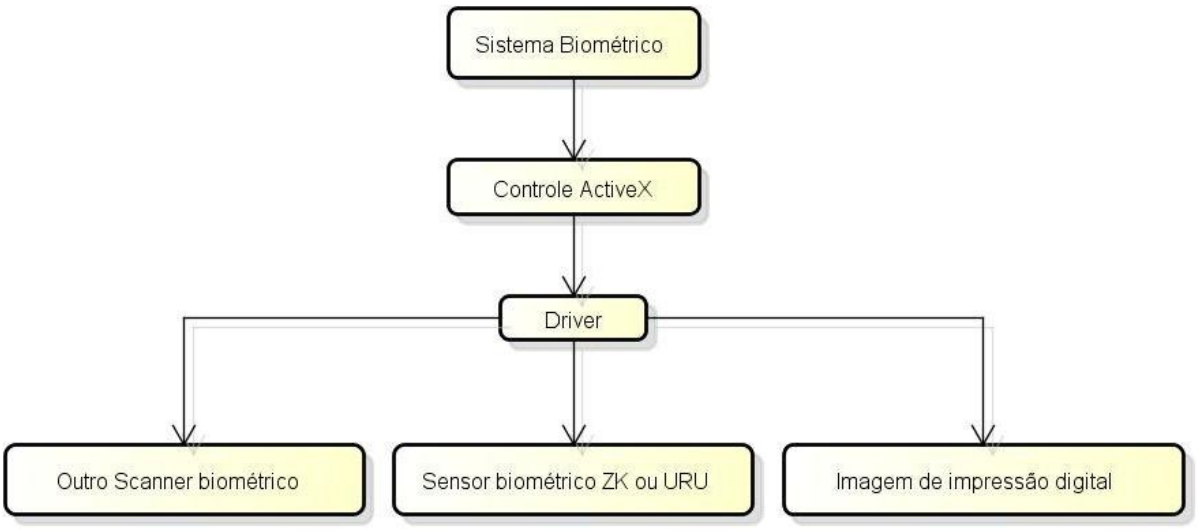

Figura 2 Modelo explicativo sobre o funcionamento do algoritmo (ZKFinger SDK 5.0 Manual, nossa tradução)

4.2 Controle Activex

Este controle se dedica em dois tipos de verificação: 1:1 (um para um) e 1:N (um para muitos), todas as funções utilizadas são as mesmas para os dois tipos onde sua única diferenciação é na relação de comparação. No final do processo obtemos um vetor de bytes que será posteriormente armazenado a um arquivo com extensão pré-definida (.tlp) podendo ser fácilmente recuperado e analisado.

4.2.1 Propriedades

O algoritmo selecionado para a funcionalidade biométrica possui diversas propriedades para o auxilio da verificação, validação e registro da biometria adquirida como podemos visualizar na tabela 1. Logo em seguida na tabela 2 pode-se visualizar as funções utilizadas pela API para os dois cenários para identificação biométrica (1:1 ou 1:N).

Método/Atributo	Descrição
Ativação (Active)	Retorno do tipo Boolean, sua função é informar a aplicação se o leitor biométrico está conectado, ativado e instalado corretamente.
Validação da ferramenta (EngineValid)	Indica se o sistema esta funcionando corretamente ou não. Se a função initEngine for utilizada esta verificação será retornada.
Extração e cadastro biométrico (EnrollIndex)	Indica a quantidade de registros de impressão digital é necessário para o cadastro ser concluído com sucesso.
Quantidade de extrações (EnrollCount)	Defini a quantidade de vezes necessária para se extrair as características biométricas do usuário antes de concluir o cadastro.
Versão do software (FPEngineVersion)	Indica qual a versão que está sendo utilizada, podendo ser a versão nove (ZKFinger 9.0) ou a versão dez (ZKFinger 10.0).
Altura da imagem (ImageHeight)	Indica a altura de uma imagem de impressão digital pré-definida pelo usuário.
Comprimento da imagem (ImagemWidth)	Indica o comprimento de uma imagem de impressão digital pré-definida pelo usuário.
Verifica o registro (IsRegister)	Função que retorna se a impressão digital foi cadastrada e esta armazenada ou não.
Qualidade do template (OneToOneThreshold)	Defini a qualidade do limiar que o leitor irá considerar, podendo estar no intervalo de um a cem (1-100). O valor padrão definido é dez (10) e a verificação de 1:1 não possui esta função.
Defini o nome do arquivo que será armazenado (RegTplFileName)	Defini o nome do arquivo que será salvo quando o evento OnEnrollToFile é utilizado.
Número de Scanners conectados (SensorCount)	Demonstra a quantidade de Scanner que estão conectados simultaneamente no mesmo PC.
Identificação do leitor (SensorIndex)	Defini uma ordem de numeração para cada Scanner conectado simultaneamente, iniciando da posição zero (0) até a quantidade de dispositivos (N), se o numero identificador for menor que zero, o scanner conectado no momento não está

	funcionando corretamente.
Serial (SensorSN)	Demonstra o número serial identificador do leito biométrico.
Tamanho do vetor de bytes (TemplateLen)	Indica o tamanho do vetor de bytes no *template* criado. Para o identificador 1:N o mesmo possui um tamanho de 1152 bytes, e para o identificador 1:1 possui 310 bytes.
Qualidade do template (Threshold)	Defini a qualidade do limiar que o leitor irá considerar, podendo estar no intervalo de um a cem (1-100). O valor padrão definido é dez (10).
Defini o nome do arquivo que será armazenado (VerTplFileName)	Defini o nome do arquivo a ser salvo quando o evento OnCaptureToFile é inicializado.
Ultima qualidade extraída (LastQuality)	Retorna a qualidade da ultima extração realizada pelo sistema, sendo usada somente depois que a função OnFeatureInfo é utilizada. Se o valor retornado for menos que o valor presente no evento LowestQuality, a função OnFeatureInfo retorna um alerta de número insuficiente.
Defini a menor qualidade de impressão digital (LowestQuality)	É definido o menor valor considerável que será comparado ao valor da função LastQuality. Valor padrão é sessenta (60).

Tabela 1 Funções da API C++

Método/Atributo	Descrição
Registro do template (Sub BeginEnroll)	Inicia o registro de um novo template e o evento OnEnroll é acionado quando o registro é concluído.
Registro cancelado (Sub CancelEnroll)	Cancela o cadastro da impressão biométrica iniciada pela função BeginEnroll.
Obter o template (GetTemplate)	Retorna o ultimo template extraído.
Obter a imagem biométrica (GetFingerImage)	Retorna a imagem (formato BMP) da ultima extração realizada.
Identificação do sistema (InitEngine)	Inicializa o sistema de verificação de impressão digital. As funções SensorCount, SensonrSN, EngineValid, ImageHeight e Image Width não terão retorno se esta função não for inicializada.
Comparação de impressões digitais (VerFinger)	Verifica se dois template são correspondentes ou não. O retorno desta função é verdadeiro se as impressões forem correspondentes ou falso.
Defini um tamanho para a imagem adquirida (PrintImageAt)	Exibi a imagem no local especificado pelos parâmetros (x,y) com tamanho pré-definido pelos parâmetros de altura e comprimento.
Defini um formato para a imagem adquirida (PrintImageEllipseAt)	Exibi a imagem no local especificado pelos parâmetros (x,y) com tamanho pré-definido pelos parâmetros de altura e comprimento. A imagem será demonstrada em forma de Ellipse.
Armazena e salva o bitmap da imagem (SaveBitmap)	Salva a imagem da ultima impressão digital extraída no formato bitmap.
Salva a imagem no formato JPG (SavaJPG)	Salva a imagem da ultima impressão digital extraída no formato JPG.
Armazena e salva o template (SaveTemplate)	Salva o template obtido.
Codifica o template (EncodeTemplate)	Codifica a string gerada e armazenada no template.
Descodifica o template (DecodeTemplate)	Descodifica o template retornando uma string com as informações.

Inicia a captura (BeginCapture)	Inicia a captura da imagem biométrica utilizando o Scanner atual. O método CancelCapture é utilizada para anular a operação.
Finaliza a ferramenta (EndEngine)	Finaliza a inicialização do sistema feita pelo método InitEngine, podendo ser reinicializado.
Retorna um template em string (GetTemplateAsString)	Retorna o ultimo template verificado ou registrado obtido através das funções OnCapture, OnEnroll, OnCaptureToFile ou OnEntollToFile retornando formatado em string.

Tabela 2 Funções da API C++

4.2.2 Métodos de interface sobre uma imagem externa

Pode se identificar também como exemplo na tabela 3 os métodos de interface sobre uma imagem externa onde será possível realizar a identificação de um usuário final através da coleta de informação (utilizando o *scanner*) ou utilizando-se de uma imagem já coletada.

Método/Atributo	Descrição
Comparação de uma imagem externa (AddBitmap)	Cadastra ou verifica um usuário com um bitmap especificado pelo BitmapHandle.
Comparação de uma imagem externa (AddImageFile)	Cadastra ou verifica um usuário através de uma imagem (suporta os formatos BMP e JPG).

Tabela 3 Funções da API C++

4.2.3 Eventos

A seguir na tabela 4 pode-se identificar quais os eventos presentes na API como cadastro, identificação entre outros em relação a coleta de uma determinada biometria.

Método/Atributo	Descrição
Capturando impressão digital (OnCapture)	Quando este método for verdadeiro, significa que este template foi obtido, identificado e o seu resultado foi armazenado em um vetor com sucesso.
Capturando impressão digital de um arquivo (OnCaptureToFile)	Adquiri o template de verificação de impressão digital salvo em um arquivo que se encontra no caminho especificado pelo parâmetro deste método. Se retornado verdadeiro, o mesmo foi obtido com sucesso.
Registrando uma impressão digital (OnEnroll)	Este evento é acionado ao final do processo de registro de uma nova impressão digital, se retornar verdadeiro o mesmo indica que o processo foi concluído com sucesso.
Registrando uma impressão digital em um arquivo (OnEnrollToFile)	Este evento é acionado ao final do processo de registro de uma nova impressão digital em um arquivo especificado pelo pela propriedade RegTplFileName, se retornar verdadeiro o mesmo indica que o processo foi concluído com sucesso.
Adquiri a qualidade da impressão digital (OnFeatureInfo)	Representa um valor da qualidade da impressão adquirida: Zero (0), o mesmo foi adquirido com sucesso, um (1), o mesmo foi insuficiente, dois (2), outras razões resultarão na falha da captura da impressão.
Extração do template através de uma imagem (OnImageReceived)	Esse evento é chamado quando é recebido uma imagem ou adicionado pelos eventos AddImageFile ou AddBitmap. Se o template for extraído com sucesso, o mesmo retorna verdadeiro.
OnFingerTouching	Este evento é acionado quando o sensor biométrico é pressionado.
OnFingerLeaving	Este evento é acionado quando o dedo é retira do sensor biométrico.

Tabela 4 Eventos da API C++

4.3 Diagrama de atividade do projeto

A seguir na figura 3 será especificado e demonstrado o diagrama de atividade representando o fluxo e o modelo de métodos sobre o funcionamento do sistema biométrico desenvolvido para este projeto em questão.

Inicialmente o leitor é ativado através da função *InitEngine* para iniciar o software previamente instalado na maquina, após feito isso inicia a chamada das funções *EngineVersion* para identificar a versão escolhida pelo usuário e logo em seguida as funções

para ativar a extração biométrica.

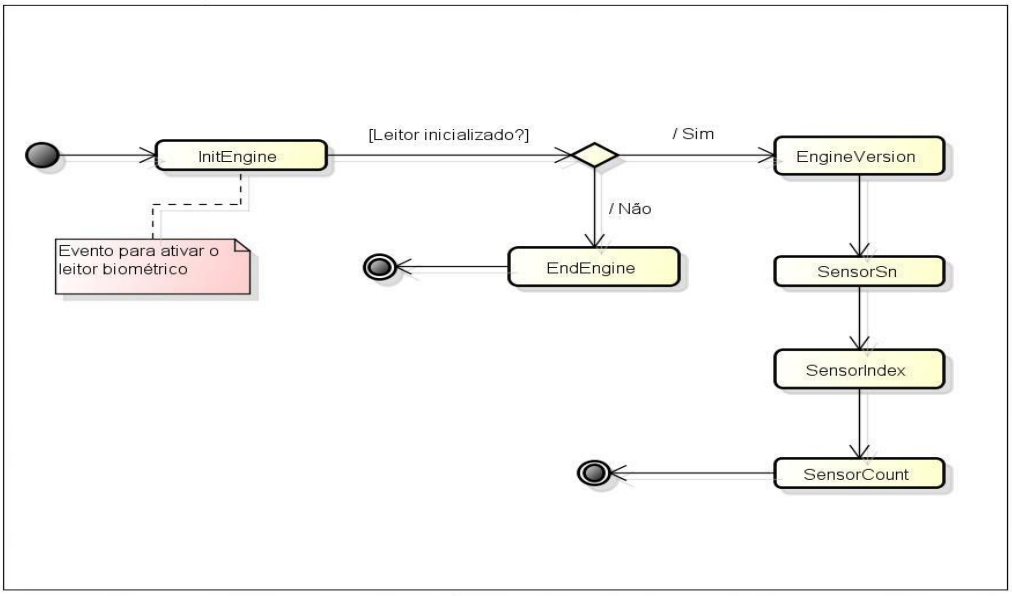

Figura 3 Diagrama de classe da inicialização do leitor
Fonte 1 – Próprio autor

Após a inicialização do *scanner*, a figura 4 demonstra como é feita o cadastro biométrico onde é definido quantas coletas serão feitas por parte do algoritmo e após feito isso será gerado um *template* com as características biométricas do usuário.

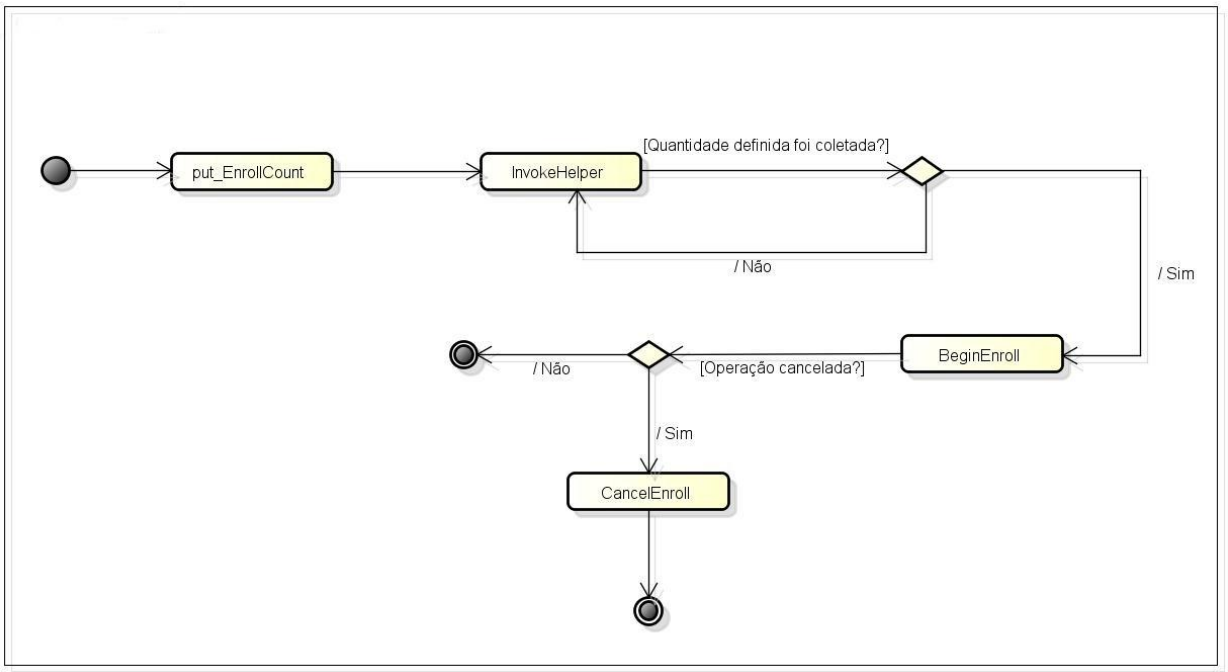

Figura 4 Diagrama de atividade do processo de cadastro biométrico
Fonte 2 – Próprio autor

4.4 Sistema biométrico

A figura 5 esta demonstrando a interface inicial do sistema biométrico, onde as opções são selecionar a versão e ativar o sensor. Esta interface conta também com algumas opções para administrar um identificador por radiofrequência (RFID), um método de identificação automática através de sinais de radio.

Para este projeto será utilizado somente a parte biométrica disponível por esta *interface* desenvolvida, as opções além de registrar uma impressão biométrica em um *template* é também salvar a imagem no dispotivo nos formatos *Joint Photographic Experts Group* (JPG) ou no formato BMP.

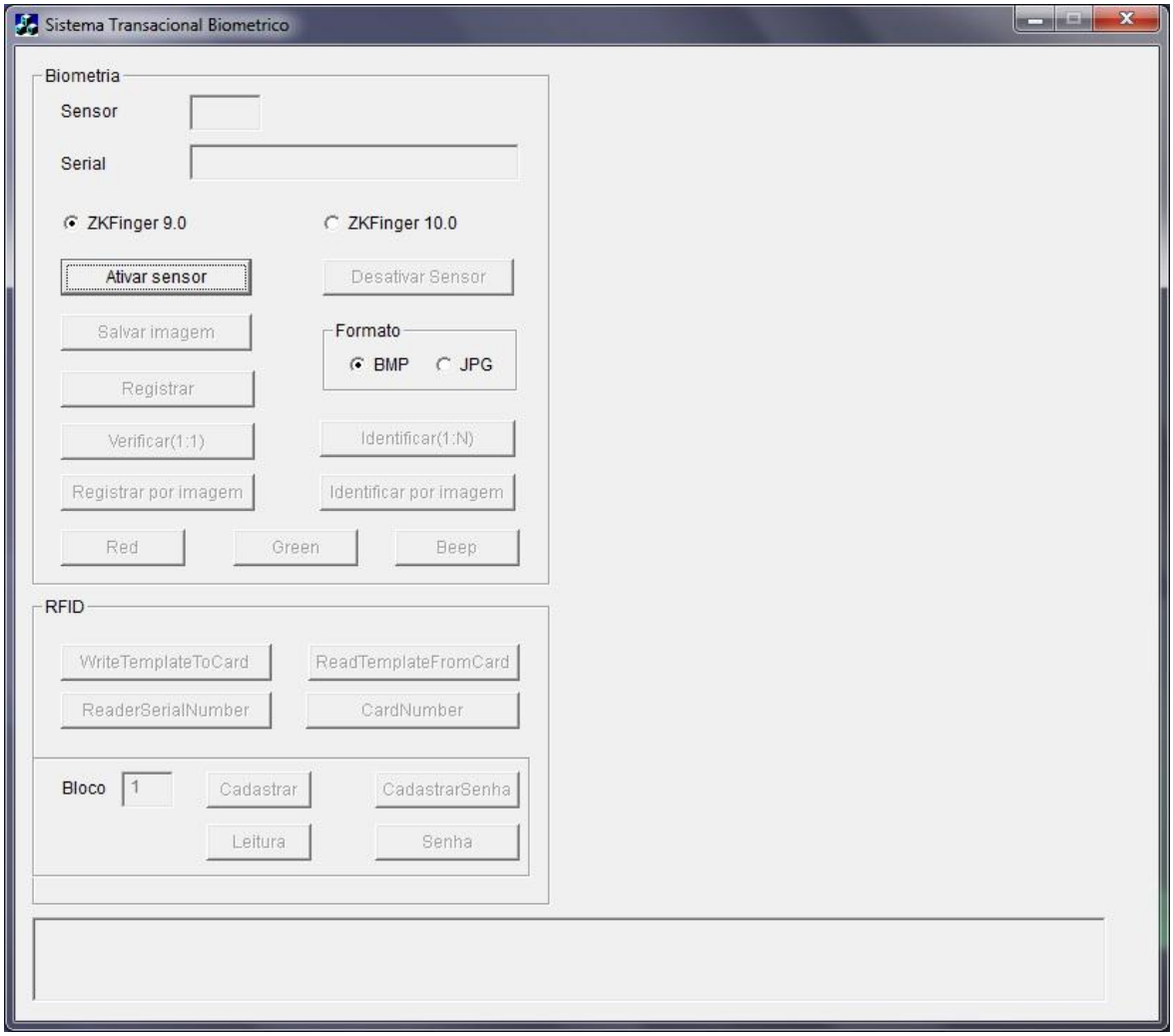

Figura 5 Tela principal do sistema biometrico (ZKFinger SDK 5.0)

Nesta etapa representada pela figura 6, 7 e 8 esta sendo demonstrado como é realizado o cadastro biométrico, e assim que a quantidade necessária de amostra for coletada o mesmo apresenta uma mensagem de sucesso e cria logo em seguida um *template* com as características biométricas.

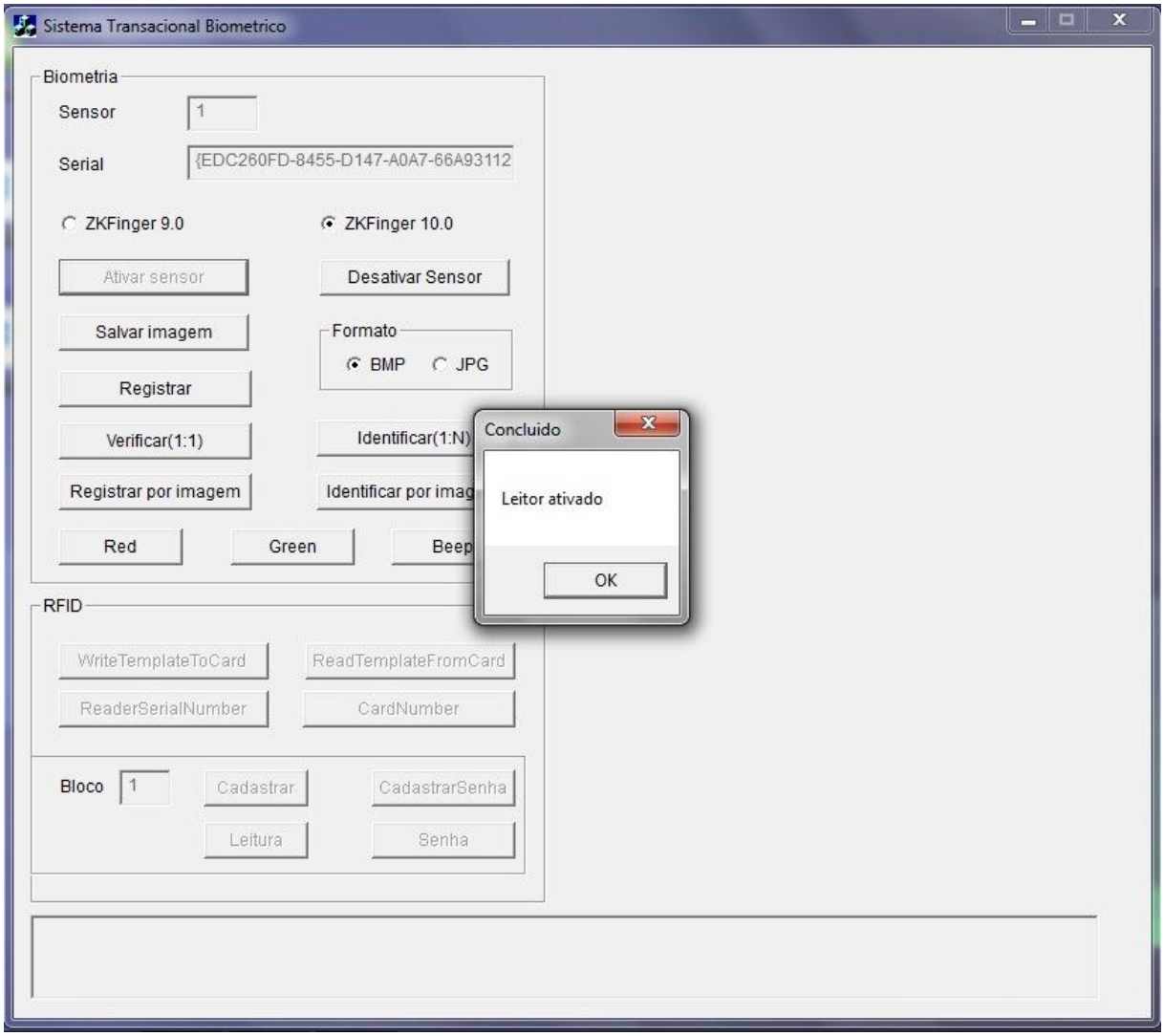

Figura 6 Tela principal do sistema biométrico (ZKFinger SDK 5.0)

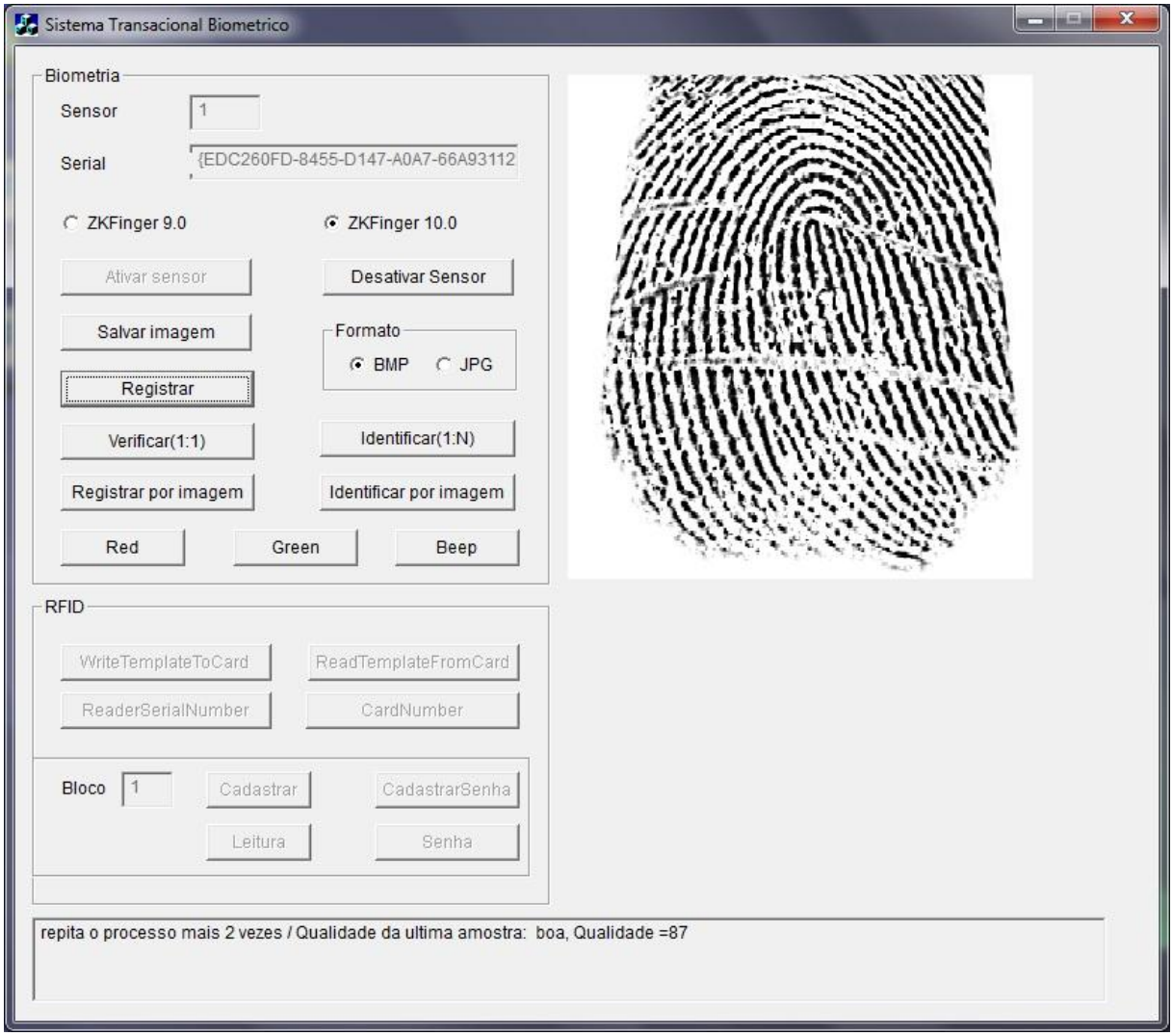

Figura 7 Tela principal do sistema biométrico (ZKFinger SDK 5.0)

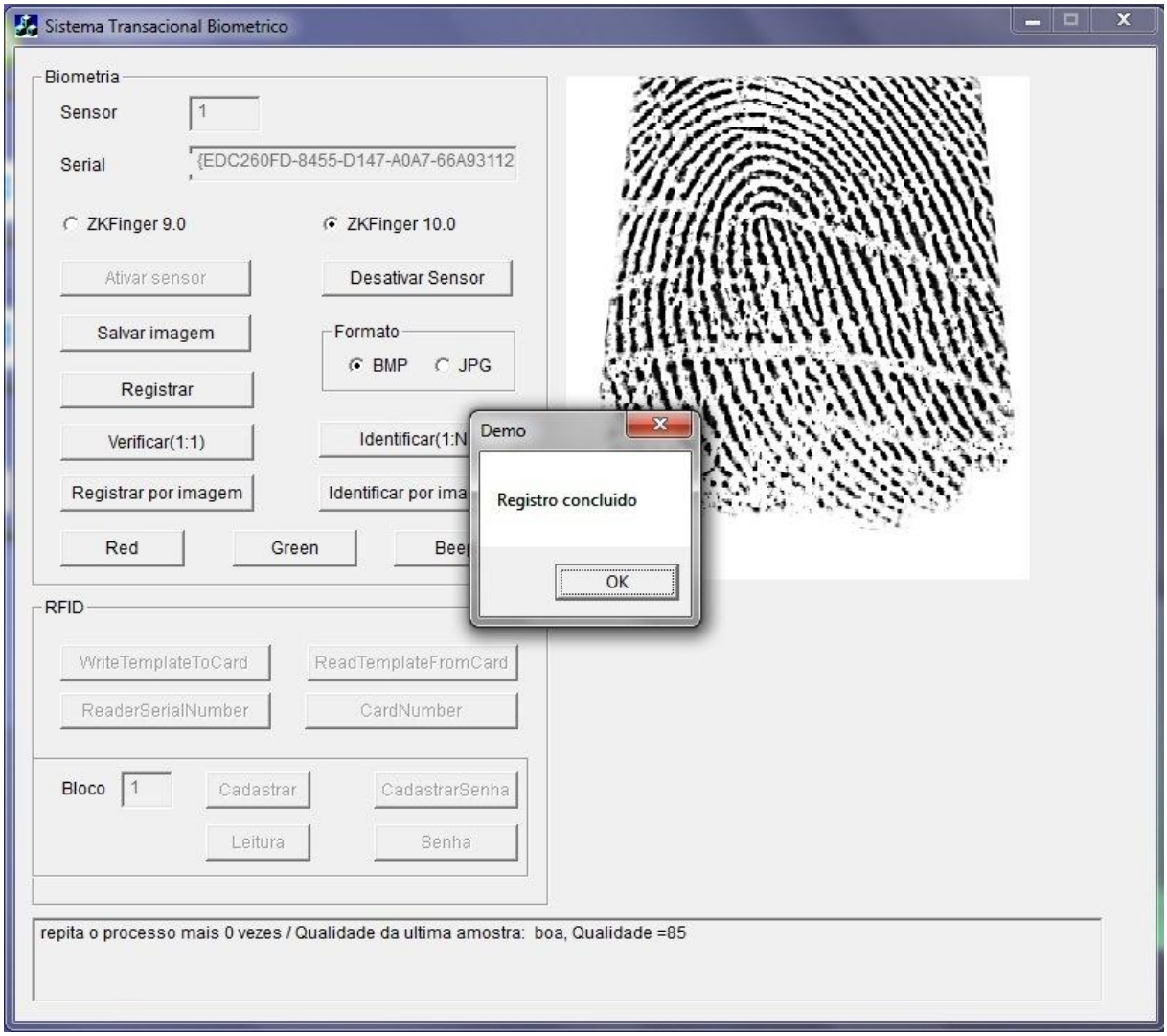

Figura 8 Tela principal do sistema biométrico (ZKFinger SDK 5.0)

5 Integração com SmartCard

Smart card ou cartão inteligente é uma tecnologia muito utilizada principalmente por entidades financeiras, pois possui a capacidade de armazenamento de informação, recuperação e identificação. Além de possuir total independência da uma base de dados podendo assim garantir uma transação off-line. (ARAUJO Marco, 2010)

Nessa seção demonstra-se como é o funcionamento de um *SmartCard*, apresentando quais as formas de comunicação existente entre a aplicação e o *applet* instalado no Javacard. Vale ressaltar que a preocupação inicial é garantir que os dados trafeguem de forma segura, onde a obtenção do mesmo não seja o suficiente para se identificar quais os valores reais contidos no momento da transferência.

A seguir é descrito o principal algoritmo criptográfico utilizando na criação de sessões seguras de comunicação entre o módulo transacional biométrico com o applet instalado no smart card, o algoritmo RSA.

5.1 Criptografia RSA

Entende-se que a criptografia nasceu com a ideia de transmitir mensagens secretas onde a ideia era simples e objetiva, “embaralhar” as informações garantindo assim o entendimento apenas do emissor e do receptor esperado. Mas o problema é que ambos necessitam do conhecimento da chave criptográfica para decifrar a mensagem transmitida e esta chave não poderia ser transmitida de forma segura (OLIVEIRA, 2012).

Para a solução deste problema foi elaborada e desenvolvida uma criptografia de chave simétrica, com duas chaves que se utilizam de uma chave pública compartilhada abertamente para qualquer emissor que tenha como objetivo enviar dados e informações, e uma chave privada que apenas o receptor possui e é altamente secreta que em hipótese nenhuma deve ser compartilhada.

Segundo OLIVEIRA Fernando (2012) O RSA foi construído sobre uma das áreas mais clássicas da matemática, a Teoria dos números, e se baseia na dificuldade em fatorar um número em seus componentes primos. As chaves públicas e privadas são geradas com base na multiplicação de dois números primos. Seu resultado será a chave pública, composta por um número grande o suficiente a dificultar sua fatoração deixando assim difícil a tentativa de identificação dos números primos.

5.2 Smart Card

Segundo MAGALHAES Paulo (2003) um *smart card* possui três tipos de memórias: *Random Access Memory* (RAM) volátil, *eletric erasable programmable read only memory* (EEPROM), que pode ser alterada após sua fabricação e *ready only memory* (ROM) que possuem dados somente para leitura. Mesmo com o grande avanço de tecnologia e sua evolução nos últimos anos, o *smart card* ainda possui uma capacidade de processamento muito limitada.

Sua limitação pode ser contornada através de um host que terá o papel de dividir este processamento e garantir também o controle dos arquivos e dados armazenados. Seu processamento mesmo sendo limitado pode ainda garantir a execução de algoritmos dentro de um ambiente bastante seguro.

Contudo uma destas limitações é a separação física entre o subsistema biométrico e o subsistema de suporte ao *smart card* que precisam estar interligados para realizar todo o processo necessário de verificação. Esta arquitetura possui algumas vulnerabilidades, pois a comunicação entre estes dois dispositivos podem ser violadas, sendo necessário a encriptação dos dados.

As principais aplicações *smart card* são cartões pré-pagos, sistema GMS (*Global Sisitem for Mobile Communication*), cartões de crédito ou débito, tarifa de transporte coletivo ou para acesso a algum ambiente. É portanto um produto com uma capacidade computacional ideal e adequada para a utilização em qualquer ambiente que necessite de um *hardware* e *software* com praticidade, flexibilidade e segurança (VIANA, 2007).

É necessário também que se mantenha uma padronização para esta crescente tecnológica feita pela indústria ISO (*Internacional Organization Standardization*) e suas sete partes: Características físicas, dimensões e localização de contatos, sinais eletrônicos e protocolos de transmissão, entre outros (MEIRELES apud MINORA Leonardo, ALEIXO Fellipe, DIOLINO Gleison, 2007).

5.3 *Applet* LSITEC

Para o controle dos dados ou arquivos armazenados em um dos 8 *containers* do cartão é necessário um *applet* já instalado em um cartão teste que executa através de comandos APDUs todas as funções como: autenticação, armazenamento, verificação, exclusão de dados ou documento entre outros. O cartão também deve suportar a autorização

de uso do serviço através do PIN e suportar o armazenamento de até 8 documentos com no máximo 4KB cada.

Os procedimentos de inicialização e utilização do *applet* seguem as seguintes características: os valores iniciais do PIN (*Personal Identification Number*) e do PUK (*PIN Unlock Key*) são inicializados com os valores 00000000 e 12345678 com a finalidade de servir como uma senha de autorização e o resgate do PIN no caso de perda ou bloqueio respectivamente com no máximo cinco tentativas para garantir que o usuário que desconhece a senha consiga fazer quantas tentativas forem necessárias para violar as informações presentes no cartão. É de extrema importância que estes valores sejam alterados posteriormente.

Para o envio desta senha para o cartão é necessário que o mesmo passe por uma criptografia simétrica AES-128 e posteriormente enviado dentro de um bloco de dados no formato PKCS#1 RSA – OAEP para o *applet*, porém este é apenas uma das etapas que a aplicação e o *applet* devem se submeter.

5.4 Comunicação APDU e protocolo de segurança

O protocolo APDU utilizado é especificado pela ISO 7816-4 e possui o papel de realizar a comunicação e o trafego de dados entre a aplicação e o *Smart Card*. Para o lado da aplicação ele possui o objetivo de transmitir informação ou o comando a ser realizado por parte do *applet* e se encarrega também de servir como um retorno de informação.

Sua estrutura para comunicação esta subdividida em:

- CLA (*class of instruction*);
- INS (*instruction code*);
- P1 (parâmetro 1) e;
- P2 (parâmetro 2);

Após a definição do *header* podemos descrever também quais os parâmetros opcionais como: Lc (especifica o tamanho do arquivo), *data field* (determina qual o arquivo que será enviado) e Le (quantidade de bytes do arquivo a ser transferido pelo comando APDU).

É possível identificar também a estrutura de retorno em: *data field*, onde seu tamanho pode ser identificado pelo parâmetro Le e os parâmetros SW1 e SW2 que retornam uma sequencia numérica para que o aplicativo identifique se o comando foi realizado corretamente.

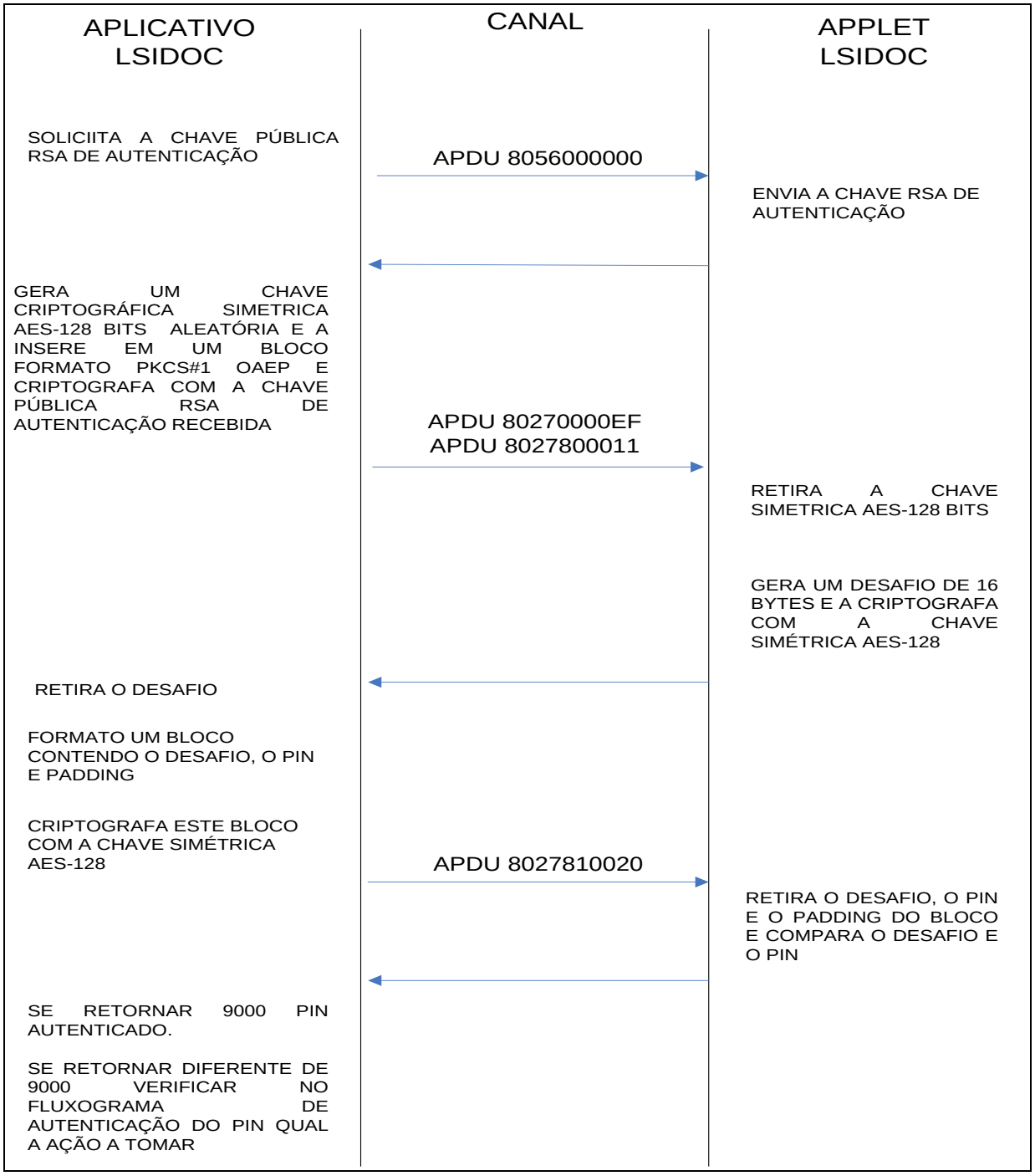

Figura 9 Especificação técnica do Applet LSIDOC (CARRAZZA, 2013)

Inicialmente é necessário que o aplicativo solicite para o *applet* a sua respectiva chave publica para assim utiliza-la para envio de informação como demonstrado na figura 9. O *applet* retorna a chave, e o aplicativo utilizando da chave publica envia sua chave

criptográfica simétrica AES-128 bits. Ao final deste processo o *applet* retorna para a aplicação um desafio para que o mesmo envie o PIN de identificação para validar e autorizar o recebimento de comandos APDUs.

5.4.1 Definição de valores e Escolhendo números primos

(Segundo OLIVEIRA Fernando, 2012) É necessário que toda e qualquer letra seja representada por um numero, pois a criptografia de RSA codifica números apenas. Como exemplo a figura 10:

1	2	3	4	5	6	7	8	9	10	11
A	B	C	D	E	F	G	H	I	J	L

Figura 10 Entendendo a criptografia RSA (OLIVEIRA, 2012)

Posteriormente é necessária a escolha de dois números primos para um aproveito máximo na segurança onde o recomendado é que se utilize uma chave de 2048 bits. Neste exemplo será demonstrado como definir um conjunto finito de valores para a identificação do caminho inverso realizado para cifrar a mensagem.

Define-se então os valores primos dezessete (17) e quarenta e um (41) aplicando a multiplicação entre eles, obtendo o resultado final de seiscentos e noventa e sete (697) que representa, portanto um conjunto finito como podemos observar na figura 11.

$$n = 17 * 41 = 697$$

Figura 11 Entendendo a criptografia RSA (OLIVEIRA, 2012)

5.4.2 Função Totiente

(Segundo OLIVEIRA Fernando, 2012) O objetivo neste momento é calcular e identificar a quantidade de co-primos de um numero que são menores que ele mesmo. No caso do exemplo citado na figura 12, deve-se encontrar o co-primo do numero seiscentos e

noventa e sete (697) através da função a seguir:

$$\phi(n) = (p - 1) * (q - 1)$$

$$\phi(697) = (17 - 1) * (41 - 1)$$

$$\phi(697) = 640$$

Figura 12 Entendendo a criptografia RSA (OLIVEIRA, 2012)

5.4.3 Calculando a chave publica e cifrando a mensagem

(Segundo OLIVEIRA Fernando, 2012) É necessário definir um número co-primo maior que um e menor que o valor encontrado na função totiente (640). Será definido o valor treze (13) como demonstrado na figura 13.

$$\text{Chave pública} = (n , e)$$

$$\text{Chave pública} = (697 , 13)$$

Figura 13 Entendendo a criptografia RSA (OLIVEIRA, 2012)

Definindo o valor, aplicamos a aritmética modular aplicando a seguinte formula demonstrado na figura 14:

$$c = m \ ^\wedge \ e \mod n$$

Figura 14 Entendendo a criptografia RSA (OLIVEIRA, 2012)

Pegamos uma palavra como exemplo para aplicar a formula gerando um resultado

demonstrado na figura 15:

T	19 ^ 13 mod 697	15
U	20 ^ 13 mod 697	692
R	17 ^ 13 mod 697	391
I	09 ^ 13 mod 697	501
N	13 ^ 13 mod 697	421
G	07 ^ 13 mod 697	176

Figura 15 Entendendo a criptografia RSA (OLIVEIRA, 2012)

Resultado obtido ao final do processo: 15, 692, 391, 501, 421, 176.

5.4.4 Calculando a chave privada

(Segundo OLIVEIRA Fernando, 2012) Para a identificação da chave priva é preciso encontrar o inverso multiplicativo do número treze (13) definido anteriormente. Logo é preciso aplicar algumas operações demonstrados na tabela 5:

Operação	Resultado	Resto
13 : 640	0	13
640 : 13	49	3
13 : 3	4	1

Tabela 5 Entendendo a criptografia RSA (OLIVEIRA, 2012)

Ao concluir os cálculos iniciais até encontra o resto um, é necessário aplicar outras operações demonstradas na tabela 6:

13 = (1 * 13) – (0 * 640)
3 = (1 * 640) - (49 * 13)
3 = (1 * 640) - 49 * ((1 * 13) - (0 * 640))
3 = (1 * 640) - (49 * 13) - (0 * 640)
3 = (1 * 640) - (49 * 13)

1 = (1 * 13) - (4 * 3)
1 = (1 * 13) - 4 * ((1 * 640) - (49 * 13))
1 = (1 * 13) - (4 * 640) + (196 * 13)
1 = (197 * 13) - (4 * 640)

Tabela 6 Entendendo a criptografia RSA (OLIVEIRA, 2012)

Concluindo que o inverso do numero treze (13) será o numero cento e noventa e sete (197) tento como resultado a figura 16.

15	15 ^ 197 mod 697	19
692	692 ^ 197 mod 697	20
391	391 ^ 197 mod 697	17
501	501 ^ 197 mod 697	09
421	421 ^ 197 mod 697	13
176	176 ^ 197 mod 697	07

Figura 16 Entendendo a criptografia RSA (OLIVEIRA, 2012)

Resultado: TURING

5.5 Arquitetura de integração proposta

O *applet* possui uma área geral que contém a versão do *applet* que está sendo utilizado, os valores PIN e PUK que são necessários para validar cada comando APDU enviado, um par de chaves RSA (chave pública e privada) que vão garantir a segurança e a criptografia necessária para o trafego de dados e finalmente os oito *containers* onde a aplicação terá a responsabilidade e a finalidade de controlar, armazenar e conferir as informações contidas como demonstrado na imagem. (CARRAZA Mario, 2013)

A parte biométrica possui um leitor que realizara a coleta da imagem, o SDK faz a comunicação entre dispositivo e leitor garantindo assim que a imagem seja identificada onde o algoritmo será responsável pela captura e tratamento da imagem através de filtros e redução

de ruídos antes de ser enviado ao aplicativo que será responsável por controlar o *applet*.

A proposta é garantir que uma extração biométrica de uma determinada impressão digital seja identificado e armazenado em um *smart card*. A figura 17 será demonstrado tecnicamente como será o funcionamento desta integração detalhando as funções utilizadas neste processo.

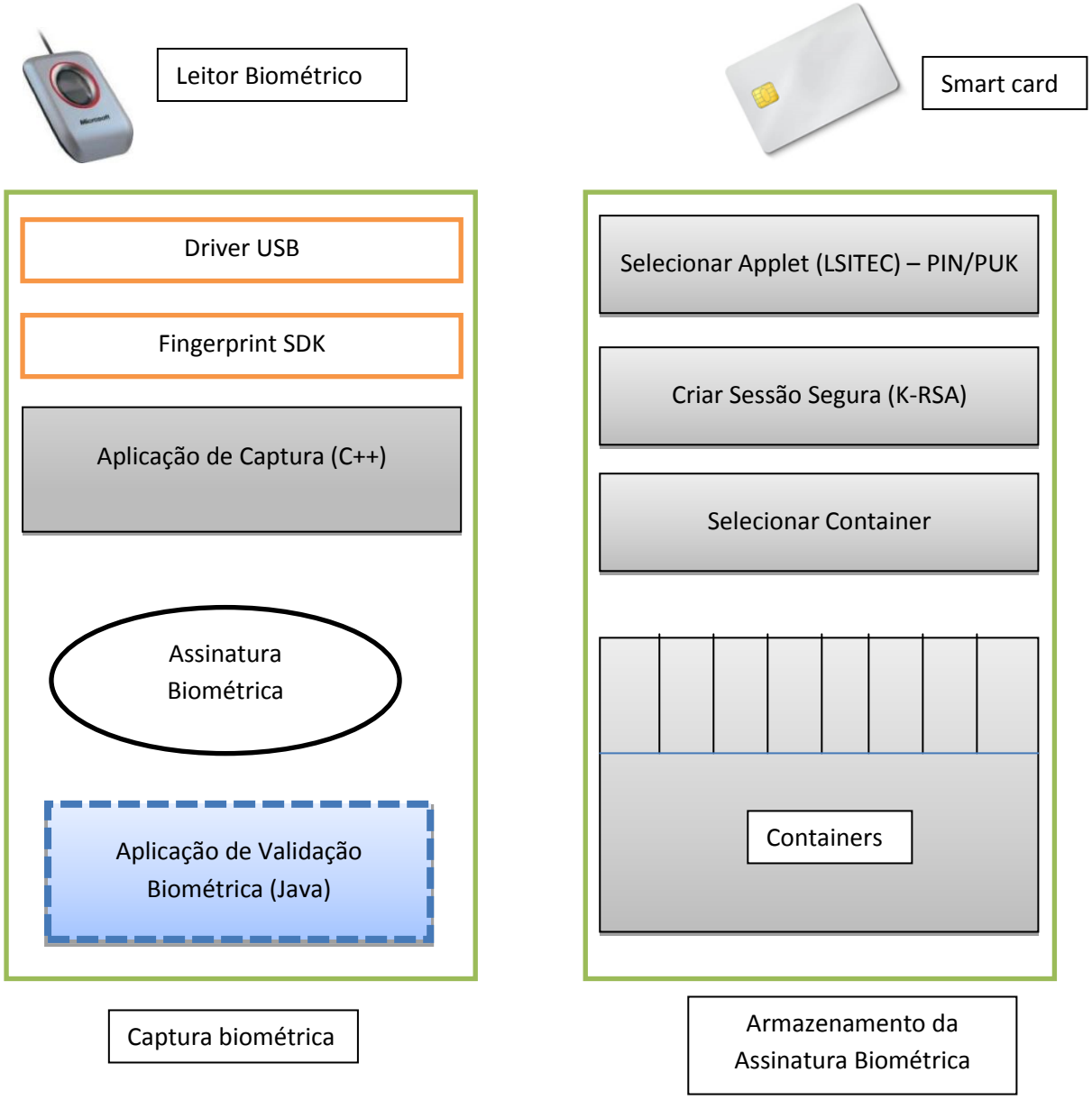

Figura 17 Especificação técnica do Applet LSIDOC integrado com a biometria
Fonte: 3 próprio autor

Inicialmente o processo começa invocando o método do leitor biométrico e coleta a quantidade necessária de exemplos pré-definidos pelo usuário, logo em seguida registra o *template* e inicia a comunicação com o *smart card* requisitando as chaves necessárias para o

envio do PIN. Ao final do processo o arquivo será armazenado no *smart card.*

A parte de validação posteriormente será com a extração dos dados contidos no *smart card* após todo o processo de validação de chaves, assim iniciando uma comparação direta com os dados coletados pelo *scanner*.

Após essas conclusões, a figura 18 irá demonstrar o diagrama de atividade do processo de extração biométrica com a integração com o *smart card* para que seja entendido como será o funcionamento das tecnologias.

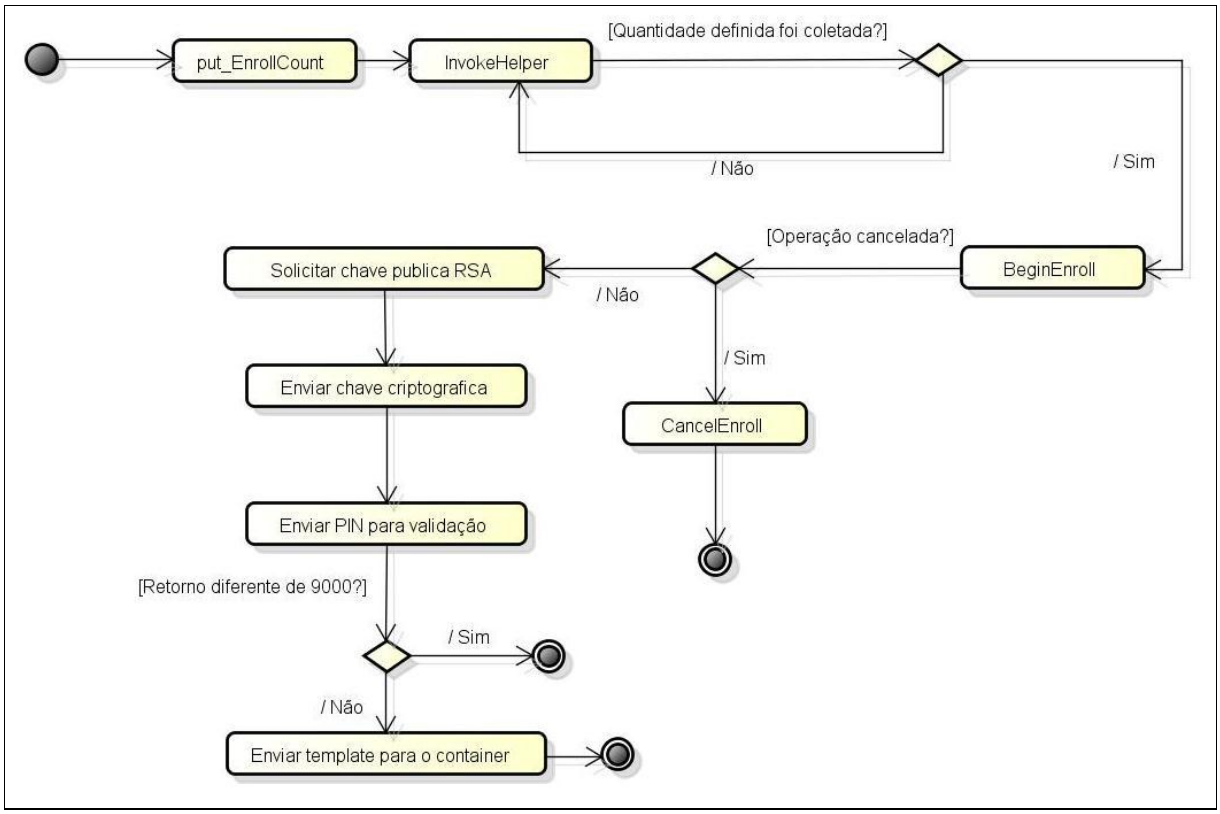

Figura 18 Diagrama de atividade do processo de extração biométrica e envio do template ao smart card

Fonte 4 – Próprio autor

CONCLUSÃO

Através da importância da biometria e seu avanço tecnológico percebe-se que o mesmo é uma poderosa ferramenta de identificação e extremamente necessária para este projeto, pois ela atende as necessidades mínimas do *smart card* gerando arquivos *templates* compactos o bastante para serem inseridos no cartão.

Foi possível através de pesquisas e estudos identificar um algoritmo que consiga compactar uma impressão digital a um *template* com um tamanho de quatro *kbytes* (4Kb). Esta redução é realizada através de filtros que tratam a imagem retirando *pixels* desnecessários garantindo a compactação e a identificação do mesmo.

Utilizando-se de criptografia e chaves simétricas é possível concluir o processo de envio de arquivo para o *smart card* de forma segura atingindo assim o objetivo que foi estipulado.

O objetivo alcançado por este projeto foi garantir que um *host* consiga armazenar um *template* em um *smart card* tornando assim uma opção valida e comprovada de que será possível a implementação sem qualquer problema por parte da integração entre o sistema biométrico e a aplicação que controla o *applet*.

Como trabalhos futuros propõem-se evoluir a sistema de captura e armazenamento de assinaturas biométricas garantindo que seja possível cadastrar mais de uma impressão digital por usuário e não só apenas do polegar. Por fim, evoluir a arquitetura do projeto, garantindo que uma aplicação seja executada e processada totalmente em um *smart card* não necessitando de um *host* para controlá-lo.

REFERÊNCIAS

ALVES (2014, 04 de junho). Segmentação de Imagens de Documentos Históricos, Disponível em: http://www.posgraduacao.poli.br/sistemapesquisa/pibic_files/artigos2004/victorouttes.pdf

ARAUJO, Paulo Gabriel Ribacionka góes. Sistema de controle de acesso via *smart card* com autenticação biométrica da impressão digital. Centro universitário de Brasilia (UniCEUB), 2010

BIOMETRICOS, Consultores. Como a Biometria Funciona. Disponível em: <http://www.consultoresbiometricos.com.br/>. Acesso em: 01 de Março de 2014

BONATO, Cassiana da Silva; FINZI Roberto Mendes Neto. Etapas de pré-processamento de imagens nas técnicas de reconhecimento biométricas por digitais. Universidade Federal de Goiás (UFG), 2011

CAMPISI, Patrizio. Security and Privacy in Biometrics. Londres: Springer-Verlag London Ltd, 2013.

COELHO, Igor de Carvalho. Identificação Biométrica Utilizando Impressões Digitais, Disponível em: <http://visual.k.u-tokyo.ac.jp/~igor/licenciatura.pdf>. Acesso em: 01 de Março de 2014.

ComputerId (2014, 04 de junho) IDKit SDK Disponível em: http://www.computerid.com.br/produtos/produtos_view.php?c=3&s=2&p=22

DELACRÉTAZ, Dijana Petrovska; CHOLLET, Gérard; DORIZZI, Bernadette. Guide to Biometric Reference Systems and Performance Evaluation. Londres: Springer-Verlag London Ltd, 2009.

GOMES, Otávio da Fonseca Martins. Processamento e Análise de imagens Aplicados á Caracterização Automática de Materiais. Departamento de Ciência de Materiais e Metalurgia Pontifícia Universidade Católica do Rio de Janeiro, 2001.

LEMES, Rubisley de Paula. Identificação biométrica de recém-nascidos. Journal of Health Informatics,2012

LEONCIO, Henrique Cezar Martins. O Uso de Certificados Digitais ICP Brasil, Padrão A3, Como tecnologia de Acesso a Conta-Cottente em Canal de Auto-Atendimento Internet, Disponível em: <http://repositorio.uniceub.br/bitstream/123456789/3307/2/20295181.pdf>. Acesso em: 01 de Março de 2014.

MAGALHÃES, Paulo Sergio. Biometria e autenticação. Portugal: 4º conferência da associação portuguesa de sistemas de informação, 2003.

MALTONI, Davide; MAIO, Dario; JAIN, Anil K.; PRABHAKAR, Salil. HandBook of Fingerprint Recognition. 2.ed. Londres: Springer-Verlag London Ltd, 2009.

MINORA, Leonardo Ataíde; ALEIXO, Fellipe Araújo; DIOLINO, Gleison Tavares. SMART INTERFACE: Ferramenta de Auxílio ao desenvolvimento de aplicações Java Card. 2007.

MITINIK, Kevin. A Arte de Enganar. Publisher Pearson Education, 2003 apud COELHO, Igor de Carvalho. Identificação Biométrica Utilizando Impressões Digitais, Disponível em: <http://visual.k.u-tokyo.ac.jp/~igor/licenciatura.pdf>. Acesso em: 01 de Março de 2014.

MONTEIRO, Leonardo Hiss. Binarização por Otsu e outra técnicas na detecção de placas. Universidade Federal Fluminense

OLIVEIRA, Fernando. Entendendo (de verdade) a criptografia RSA, Disponível em: <http://blog.lambda3.com.br/2012/12/entendendo-de-verdade-a-criptografia-rsa/>. Acessado em: 10 de outubro de 2014

OTAVIANO, Christopher Henrique. Biometria: Seus métodos e aplicações. Universidade do Mato Grosso do Sul, 2007

RATHA, Nalini K.; GOVINDARAJU, Venu. Advances in Biometrics: Sensors,Algorithms and System. Londres: Springer-Verlag London Ltd, 2008.

SARAMELA (2014, 04 de junho), Patrícia Mateus. Estudo e Implementação do Algotitimo Otsu para Limiarização de Cartas Forenses, Disponível em: http://www.cesumar.br/prppge/pesquisa/epcc2011/anais/patricia_mateus_saramela.pdf

THAI, Raymond. Fingerprint image enhancement and minutiae extraction, Disponível em: <https://www.sowenig.de/upload/public/uni/RaymondThai.pdf>. Acesso em: 01 de Março de 2014.

TONHÁ, Vinícius Rodrigues. Sistema de compras eletrônicas utilizando tecnologia *smart card* e biometria digital. Centro universitário de Brasília (UniCEUB), 2011.

VIANA, Cristina. Uma biblioteca java de apoio á comunicação com um cartão inteligente compatível com a GlobalPlatform. 2007.