UNIVERSIDADE EDUARDO MONDLANE

FACULDADE DE ENGENHARIA

Departamento de Engenharia Eletrotécnica-DEEL

ENGENHARIA ELECTRÓNICA

Relatório do Trabalho de Licenciatura

Tema:

PROJECTO DE UM SISTEMA BIOMÉTRICO PARA RECÉM NASCIDOS EM MOÇAMBIQUE

Autor(**a**): Naira Lúcia Nhatsave

Supervisor: Eng José Consolo

Maputo, Novembro de 2022

UNIVERSIDADE EDUARDO MONDLANE

FACULDADE DE ENGENHARIA

Departamento de Engenharia Eletrotécnica-DEEL

ENGENHARIA ELECTRÓNICA

Relatório do Trabalho de Licenciatura

Tema:

PROJECTO DE UM SISTEMA BIOMÉTRICO PARA RECÉM NASCIDOS EM MOÇAMBIQUE

Autor(**a**): Naira Lúcia Nhatsave

Supervisor: Eng José Consolo

Maputo, Novembro de 2022

NAIRA LÚCIA NHATSAVE

PROJECTO DE UM SISTEMA BIOMÉTRICO PARA RECÉM NASCIDOS EM MOÇAMBIQUE

Monografia apresentada ao departamento de Engenharia Eletrotécnica da Faculdade de Engenharia da Universidade Eduardo Mondlane- como requisito parcial para obtenção de grau de Licenciatura em Engenharia Eletrónica.

Supervisor: José Consolo, Eng°

Coordenador: Julian Garzon, Eng°

Maputo, Novembro de 2022

UNIVERSIDADE EDUARDO MONDLANE

FACULDADE DE ENGENHARIA

DEPARTAMENTO DE ENGENHARIA ELECTROTÉCNICA

TERMO DE ATRIBUIÇÃO DE TEMA DE TRABALHO DE LICENCIATURA

REFERÊNCIA DO TEMA:	2022-01-EETLPL-03	Data:

1. TÍTULO DO TEMA

PROJECTO DE UM SISTEMA BIOMÉTRICO PARA RECÉM NASCIDOS EM MOÇAMBIQUE

2. DESCRIÇÃO SUMÁRIA DO TRABALHO A DESENVOLVER

Objectivo geral

- Projectar um sistema biométrico para o registo e identificação das parturientes e recém-nascidos na sala do parto.

Objectivos específicos

- Desenvolver um software para o registo e armazenamento de dados na entrada e saída das unidades hospitalares (maternidade);
- Comparar os diferentes tipos de Biometria a ser aplicados para a identificação neonatal nas unidades hospitalares (maternidades);
- Criar um protótipo para a colheita da Biometria do recém-nascido, Mãe ou responsável, acoplada a base de dados do software para o controle de pacientes nas unidades hospitalares (maternidades);

3. LOCAL DE REALIZAÇÃO

Faculdade de Engenharia da Universidade Eduardo Mondlane

4. SUPERVISOR e COORDENADOR

	Nome	Assinatura
Supervisor	Engº. Jose Consolo	
Coordenador	Engº. Julian Garzon	

5. DATAS-CHAVE

Entrega do Tema:		Conclusão	
		Após melhoria:	

Maputo, ____ de ____ de 2022

Chefe da Comissão Científica

_____

Visto do Chefe do Departamento

_____

Declaro que recebi o tema do Trabalho de Licenciatura na data acima indicada

Nome: _____ Ass: _____

UNIVERSIDADE EDUARDO MONDLANE

FACULDADE DE ENGENHARIA

DEPARTAMENTO DE ENGENHARIA ELECTROTECNICA

AVALIAÇÃO DOS SUPERVISORES

Autor: Naira Lúcia Nhatsave

Supervisor da Faculdade Nota

_____ _____

(Eng°. José Consolo)

Maputo, Novembro de 2022

UNIVERSIDADE EDUARDO MONDLANE

FACULDADE DE ENGENHARIA

DEPARTAMENTO DE ENGENHARIA ELECTROTÉCNICA

TERMO DE ENTREGA DO TRABALHO DE LICENCIATURA

Declaro que o estudante_____entregou no dia _____/____/2022 as _____copias do seu Trabalho Corrigido, com a referência: _____

Intitulado

_____

_____

Maputo, _____ de _____ de 2022

O chefe de Secretaria

_____

DECLARAÇÃO DE HONRA

Eu, Naira Lúcia Nhatsave, declaro por minha honra que o presente trabalho foi elaborado por mim e que constitui resultado da minha investigação pessoal, estando indicadas no texto e nas referências bibliográficas, as fontes utilizadas.

Declaro também que este trabalho nunca foi apresentado para efeitos de avaliação para qualquer outra entidade ou instituição, para além da(s) directamente envolvida(s) na sua elaboração, sendo esta a primeira vez que o submeto para obtenção de um grau académico numa instituição educacional.

_____

(Naira Lúcia Nhatsave)

DEDICATÓRIA

Eu dedico este trabalho a minha Mãe, Ercília Isaías Nhatsave que esteve comigo desde o primeiro dia da minha vida e que apesar de todas as dificuldades e barreiras que a vida possa ter colocado em seus caminhos, encheu-me de amor e empreendeu todos os esforços para me tornar na pessoa que eu sou hoje.

EPÍGRAFE

“*se as feridas do teu próximo não lhe causam dor,*

a tua doença é pior que a dele”

Tinho Aires

AGRADECIMENTOS

Em primeiro lugar quero agradecer a Deus pelo dom da vida e por ter-me protegido e guiado neste percurso cheio de adversidades, dizer que sem a sua bênção eu não estaria aqui.

Agradecer a minha Mãe por ter sido uma Mãe e um Pai em simultâneo, a minha Irmã Rindzela por ter sido a minha fonte de inspiração, aos meus avós, Deolinda Muhate e Isaías Nhatsave, aos meus tios e primos pelo amor e apoio incondicional.

Agradeço ao meu supervisor Eng. José Consolo pelo apoio na escolha do tema, orientação, paciência e por ter acreditado em mim como estudante.

Agradecer ao meu grupo de amigas, por estarem comigo em todos os tombos, choros, fracassos e também em todos os risos, brincadeiras, aventuras, conquistas e celebrações.

Agradecer ao Claúdio Bauque, Kevin Ruco, Abel Junga, que foram sem sombra de dúvidas as melhores pessoas que eu conheci na UEM, caminharam comigo desde o primeiro ano e assistiram todo o meu percurso académico e pessoal nesse período. Obrigada por terem estado comigo nessa batalha.

Agradeço por último a todos os Colegas, Docentes e Amigos que cruzaram meu caminho nesses últimos anos em que aprendi, cresci, vivi, chorei e celebrei. Cada um deles teve um papel fundamental e insubstituível na minha formação.

RESUMO

A forma encontrada para registar pessoas em quase todo o mundo sempre foi à impressão digital e fotos, que são registadas em fichas e permitem a identificação sem maiores problemas. Entretanto, o número de produtos e serviços que envolvem a identificação de indivíduos tem crescido fortemente nos últimos anos. Com isso, por utilizar características biológicas ou comportamentais no processo de identificação, a Biometria tem vindo a ganhar relevância, pois é mais simples e conveniente que a memorização de senhas e não exige que o usuário possua algum objeto para ser identificado. A implementação da Biometria nos hospitais, concretamente nas maternidades é uma inovação com objectivo de tranquilizar as parturientes e fortalecer a segurança do próprio recinto, dando assim confortabilidade aos pacientes e eliminando a má-fé do ser humano, bem como, evitar o tráfico de bebés que tem ocorrido dentro das unidades hospitalares. Caso sejam seguidos corretamente protocolos de aquisição de amostras, sejam utilizados tanto equipamentos apropriados quanto métodos de reconhecimento adaptados às características dos recém-nascidos, será possível colher as suas impressões digitais ainda na sala de parto. O sistema Neonatal 2022 faz o registo digitalizado dos dados da Mãe assim como regista e guarda a sua impressão em uma base de dados do software, e minutos após o parto, durante o registo dos dados do recém-nascido, é também colhida a impressão digital do bebé e acoplados ao registo da mãe, e as verificações são feitas a saída do hospital.

Palavras-chave: Biometria, Impressão digital, Roubo, troca, Hospital, Recém-nascido.

ABSTRACT

The way found to register people almost all over the world has always been fingerprint and photos, which are registered on cards and allow identification. However, the number of products and services that involve identification of individuals has grown strongly in recent years. Therefore, biometrics has gained relevance, as it is simpler and more convenient than the memorization of passwords and the user doesn't need to carry an ID for identification as its done using biological or behavioral characteristics. The usage of biometrics technilogies in hospitals, specially in maternity hospitals, is an innovation with the final goal of security reiforncement, providing comfort to patients and avoiding babies trafficking, that has occurred within hospital units. If sample acquisition protocols are correctly followed, both appropriate equipment and recognition methods adapted to the characteristics of newborns are used, it will be possible to collect their fingerprints while still in the delivery room. Neonatal 2022 is a digitalized system that register the mother's personal data as well as fingerprints in a software database, and minutes after labor delivery, during the registration of the newborn's data, the baby's fingerprint is also taken and attached to the mother's record, and upon leaving the hospital their identities are checked/confirmed.

Keywords: Biometrics, Fingerprint, theft, swap, Hospital, Newborn

Lista de Figuras

Lista de Tabelas

Lista de Siglas

AFIS *Automated Fingerprint Identification System* (Sistema Automatizado de Identificação de Impressões Digitais.)

DNA *Deoxyribonucleic acid* (Ácido desoxirribonucleico)

EER *Equal Error Rate* (Taxa igual de erro)

FAR *False acceptance rate* (Taxa de falsa aceitação)

FRR *False rejection rate* (Taxa de falsa Rejeição)

GND Ground (Terra)

LCD *Liquid Crystal Display* (Visor de cristal líquido)

LED *Light Emitting Diode* (Diodo emissor de luz)

ROC *Receiver Operating Characteristic* (Características operacionais do receptor)

OLED *Organic Light Emitting Diode* (Diodo emissor de luz orgânico)

PCB *Print Circuit Board* (Placa de Circuito Impresso)

PIN *Personal Identification Number* (Número de identificação pessoal)

TI *Information Technology* (Tecnologia de Informação)

VC *Voltage Common Collector* (Tensão de Coletor Comum)

Índice

CAPÍTULO 1: Introdução

1 INTRODUÇÃO

Cada ser humano tem um traço único físico e difícil de ser reproduzido. O registo biométrico para identificação e autenticação de dados é um método bastante usado ao nível mundial em várias áreas da vida. Tem se visto a sua aplicação em áreas indústrias com o objectivo de reforçar a segurança no recinto. Este método de identificação está cada vez mais comum, a tecnologia digital é utilizada actualmente em vários lugares, tais como aeroportos, escolas, no serviço de identificação civil e outros.

A segurança das informações contidas nos documentos de identidade assegura a sua validade, eliminando as fraudes e falsificações. Além da impressão digital, reconhecimento de íris, retina e facial, existem outros métodos tais como o reconhecimento pela voz, palma da mão, assinatura e digitação. (Ponte, 2008)

Segundo MANDL, 2003 (apud, Nogueira, 2011), o uso de um sistema biométrico é simples. O sistema consiste no envio de dados das características do usuário para um sistema de controlo e gerenciamento dessas informações, e vale desde a impressão digital até a composição da retina da pessoa. Depois disso, existe uma comparação entre as informações colectadas com as que estão num banco de dados e, caso exista semelhança a autenticação é efectuada com sucesso.

A tecnologia biométrica é de grande interesse em áreas onde é realmente importante verificar a real identidade de um indivíduo. Inicialmente estas técnicas eram empregadas em aplicações especializadas de alta segurança, entretanto nós estamos vendo agora a sua utilização e proposta de uso numa grande e crescente área de situações em utilizações públicas no nosso dia a dia. Neste trabalho pretende-se realizar um estudo sobre a possível implementação de um sistema biométrico nas maternidades em Moçambique, procura-se trazer uma abordagem sobre como é que as pessoas encaram esse problema que há muito assola as famílias, mas poucos casos são reportados. A par do pressuposto de preocupação para a questão social, o foco do estudo está em projectar um Sistema de registos biométricos numa maternidade.

1.1 Problema de Pesquisa

A pior notícia que um médico pode dar a uma mãe e a mesma dar a sua família é que seu filho foi trocado ou roubado, e não que ele tenha nascido sem vida. Se o tráfico de bebés afeta ao médico que comunica a notícia, é possível imaginar o que ela causa a família que se depara com o acontecido.

A grande semelhança física existente entre os recém-nascidos, aliada a incapacidade de comunicação e a grande circulação que eles em geral têm nos hospitais (da sala de parto para sala de limpeza, daí ao berçário, e depois ao quarto da mãe, etc.) são fatores que contribuem para a ocorrência da troca e do tráfico de bebês.

Existe um maior risco em grandes hospitais públicos, influenciada pelo grande número de partos, e por consequência de bebês circulando no hospital, aliado a carência de recursos, tanto humanos (poucas enfermeiras para o número de bebês) quanto materiais (pulseirinha de identificação em falta ou com baixa qualidade, etc.). Porém, as maternidades pequenas e as particulares não estão isentas de ser palco de uma troca de bebês. Assim, equivoca-se quem afirma que a obrigação de identificação de bebés é procedimento necessário apenas nos grandes hospitais. Nas pequenas maternidades também é possível ocorrer troca e o tráfico de bebês.

1.2 Pergunta de Pesquisa

O nascimento de um ser humano é visto como o maior e melhor Dia da Família e dos amigos que o recebem, porém, as vezes essa felicidade vem a se tornar um terror quando não ocorre como esperamos (problemas durante o parto, roubo, troca, assim como o abandono), daí houve a necessidade de pensar numa solução viável para evitar e quiçá acabar de uma vez por todas com esse problema que afecta a sociedade. Dito isso se levanta a seguinte pergunta de pesquisa: ***"COMO É QUE A BIOMETRIA PODE REDUZIR OU ELIMINAR CASOS DE OCORRÊNCIA DE TROCAS E TRÁFICO DE BEBÉS?"***

1.3 Relevância da pesquisa

A tecnologia tem vindo a cada dia a superar as espectativas do ser humano no nosso quotidiano e diminuindo assim o árduo trabalho em praticamente todas áreas da vida, as invenções e inovações tem substituído e o trabalho feito pelo homem.

Vê-se a necessidade de se fazer esse estudo, pois muitas vezes tráfico de bebés é um problema que afecta não só a sociedade moçambicana, assim como o mundo, por sua vez, a troca de bebês normalmente é descoberta apenas algum tempo depois. É um problema frequente, mas não muito falado. Com a realização deste projecto tem-se em vista a minimização do acto, far-se-á um estudo sobre a real necessidade de se pôr em prática a solução para esse problema, implementando o sistema de registo biométrico dos recém-nascidos acoplando os seus dados com os da mãe ou responsável minutos após do parto, a Biometria evita também outro problema muito comum das maternidades, o abandono dos bebês, com o cadastramento biométrico, o bebé abandonado terá rapidamente sua identidade reconhecida, assim como aquela da mãe e dos responsáveis. O sistema pode, aos poucos ser implementado por outros hospitais do país. A troca e o tráfico, podem ocorrer em diferentes locais e advir de causas diversas, razão pela qual se faz firmar o exacto conceito que a expressão assume neste trabalho. A necessidade da implementação do projecto deve-se ao facto de que os registos das parturientes actualmente nos hospitais públicos e centros de saúde, são feitos a manuscrito e arquivados em uma sala, abrindo a possibilidade desse método ser fraudado.

1.3.1 Delimitação do Tema

Temporal

O período do projecto, da aquisição dos componentes e da recolha de dados foi de seis meses e duas semanas, a escrita e entrega do relatório ocorreu em simultâneo com o processo da espera da chegada dos componentes.

Espacial

A montagem do protótipo ocorreu na Faculdade de Engenharia, Localizada na Cidade de Maputo, no laboratório de controle do Departamento de Electrotécnia, e na sala do

núcleo dos estudantes. A recolha de dados foi feita na maternidade do Hospital Central de Maputo. A escolha do local de estudo deve-se ao facto de ser a maior unidade hospitalar no país, e com o maior número de partos diários, assim sendo, foi possível ter informação fidedigna de profissionais com muitos anos de experiência sobre alguns casos ocorridos no recinto. O Hospital Central também serve frequentemente como centro de investigação e de ensino. Devido a sensibilidade do tema roubo e troca de recém-nascidos, não foi possível ter acesso aos dados estatísticos desta ocorrência, pois a maioria dos casos não é reportada.

Figura 1**.** Localização geográfica do Hospital Central de Maputo(Fonte: Google Maps, acessado em 2022)

Figura 2 Localização geografia da Faculdade de Engenharia(Fonte: Google Maps, acessado em 2022)

2 OBJECTIVOS

2.1 Objectivo Geral

Projectar um sistema biométrico para o registo e identificação das parturientes e recém-nascidos na sala do parto.

2.2 Objectivos específicos

- Desenvolver um software para o registo e armazenamento de dados na entrada e saída das unidades hospitalares (maternidade);
- Comparar os diferentes tipos de Biometria a ser aplicados para a identificação neonatal nas unidades hospitalares (maternidades);
- Criar um protótipo para a colheita da Biometria do recém-nascido, Mãe ou responsável, acoplada a base de dados do software para o controle de pacientes nas unidades hospitalares (maternidades);

2.3 METODOLOGIA

O processo de investigação do presente projecto consistiu na busca de informações obtidas em produções científicas e dados da internet. Fez-se um estudo numa unidade hospitalar visando colher informação por parte dos funcionários. O estudo será baseado nos seguintes métodos:

- Pesquisa Exploratoria;
- Revisão Bibliografica;
- Pesquisa Aplicada.

2.4 Estrutura Do Trabalho

Este trabalho é apresentado em 4 capítulos cuja descrição é apresentada a seguir:

CAPÍTULO I - Este capítulo consiste na apresentação do trabalho em linhas gerais, inclui também os objetivos que se pretendem alcançar com a implementação do projecto e a metodologia usada.

CAPÍTULO II - O segundo capítulo visa fazer a apresentação da revisão bibliográfica em volta do tema do trabalho e descrever os tipos de Biometria existentes e os actuais métodos usados no campo de pesquisa e visa apresentar o desenvolvimento do projecto e fazendo a descrição dos dispositivos e componentes a serem usados para a concepção do sistema.

CAPÍTULO III - Neste capítulo são levantados todos os requisitos funcionais e especificações técnicas do projecto, simulações e o orçamento do projecto.

CAPÍTULO IV - Nesta última fase são dadas as conclusões e recomendações para o desenvolvimento de futuros trabalhos relacionado ao tema, estão também incluídos os anexos que contêm os programas usados para o desenvolvimento do projecto.

CAPÍTULO 2: Contextualização teórica

3 FUNDAMENTAÇÃO TEÓRICA

A elaboração do estudo de caso que será responsável pela aplicação dos conceitos obtidos, necessita primeiramente de uma pesquisa teórica com a finalidade de adquirir toda a fundamentação básica que o tema requer. Neste capítulo será feita uma descrição dos assuntos de forma a fornecer toda a base de conhecimento exigida pela área estuda.

3.1 Biometria

A Biometria é ramo da ciência que estuda as medidas físicas dos seres vivos, daí o termo identificação biométrica para indicar as tecnologias que permitem a identificação de pessoas através dos traços físicos característicos e únicos de cada ser humano: os traços faciais, a íris, e a impressão digital, fixando sua identificação perto da margem zero de erro. (Ponte, 2008).

3.2 Reconhecimento de Padrões

O Reconhecimento de Padrões (RP) é a ciência que tem por objetivo a classificação de objetos em categorias ou classes. Desde os primórdios da computação, a tarefa de implementar algoritmos emulando essa capacidade humana, tem se apresentado como uma das mais intrigante e desafiadora (JAIN, Anil; DUIN, Robert; MAO, Jianchang., 2000) As técnicas de reconhecimento de padrões apresentam um vasto leque de aplicações nas áreas científicas e tecnológicas, principalmente na área de informática. O interesse na área de reconhecimento de padrões tem aumentado recentemente devido as novas aplicações que são não só um desafio, mas também computacionalmente mais exigentes. Estas aplicações incluem data mining ou mineração de dados que identifica um padrão ou uma relação entre milhões de modelos: A classificação de documentos, muito útil para procurar documentos de texto; Previsões financeiras; Organização e recuperação de bancos de dados multimídia e Biometria, que é a identificação pessoal baseada em vários atributos físicos ou comportamentais. A tabela 1 mostra algumas aplicações do reconhecimento de padrões.

Domínio do problema	**Aplicação**	**Padrão de Entrada**	**Classes de padrão**
Bioinformática	Analise de sequência	DNA/Sequencia de proteínas	Tipos conhecidos de genes/padrões
Mineração de dados	Busca por padrões significantes	Pontos em um espaço multidimensional	Compactar e bem separar grupos
Classificação de documentos	Busca na internet	Documento texto	Categorias semânticas (negócios, desporto e etc.,)
Análise de documentos de imagem	Máquinas de leitura para cego	Documento de imagem	Palavras e caracteres alfanuméricos
Automação industrial	Inspeção de circuito imprenso em placas	Intensidade ou alcance de imagem	Produto defeituoso ou não defeituoso
Recuperação de base de dados multimídia	Busca na internet	Vídeo clipe	Géneros de vídeos
Reconhecimento biométrico	Identificação pessoal	Face, iris, impressão digital	Usuários autorizados para controlo de acesso
Sensoriamento remoto	Prognostico da produção da colheita	Imagem multiespectral	Desenvolvimento de padrões de colheita
Reconhecimento de voz	Inquérito por telemóvel sem assistência	Voz em forma de onda	Palavras faladas

Tabela 1: Aplicações do reconhecimento de padrões (JAIN; DUIN; MAO, 2000)

3.3 História

Segundo Dantas, 2008, O primeiro método de identificação biométrica aceite oficialmente foi desenvolvido por Alphonse Bertillon no final do século XVIII. Também chamada de antropometria, o sistema se baseava numa combinação de medidas físicas tiradas de acordo com elaborados procedimentos. As métricas junto com a cor de cabelo, de olhos e fotos de frente e de costas eram arquivadas. Bertillon criou 243 categorias.

A técnica foi adoptada pela polícia de Paris em 1882 e rapidamente copiada por toda a França e Europa. Em 1887 os Estados Unidos aderiram ao sistema. O fracasso do método de Bertillon deveu-se a dificuldade no armazenamento e na consulta dos dados e ao complicado método para coletar as medidas.

Mas havia outra falha no sistema de Bertillon. Ao contrário do que se pensava, as categorias criadas não eram únicas. Aconteceram muitos erros que causaram o descrédito do sistema. Um dos mais conhecidos foi a prisão de um homem que alegou nunca ter passado pela prisão. No entanto, ao verificar as informações, verificou-se que havia outro homem com as mesmas características do primeiro que estava detido noutro presídio.

O método de Bertillon foi substituído pelo sistema de impressões digitais, criado pelo oficial britânico William Herschel. Em missão na Índia, Herschel estava descontente com os comerciantes locais, que não cumpriam contratos. O oficial passou a pedir que colocassem além das assinaturas, a impressão das digitais nos documentos. A ideia, segundo o próprio, era "assustar os comerciantes, de modo que não pudessem repudiar sua assinatura".

Outros pesquisadores também começaram a estudar as impressões digitais na mesma época. Em 1870, o cirurgião Henry Faulds começou a vislumbrar nas digitais um caminho para comprovar identidades. Mas a classificação final ficou por conta do oficial Edward Richard Henry, que criou e adoptou o sistema em 1897, na cidade indiana de Bengal. O sistema funcionou tão bem que foi adotado em toda Índia.

Pouco tempo depois, um comitê da Scotland Yard testou e aprovou o sistema, implantado na Inglaterra em 1901. O sistema antropométrico de Bertillon estava ultrapassado, apesar de algumas agências o terem usado até à década de 30. (Dantas, 2008).

3.4 Características Biométricas

Qualquer característica física ou comportamental do ser humano pode ser usada na identificação biométrica, desde que apresente as seguintes propriedades: Universalidade, que significa que a característica deve ser comum a todas as pessoas. Unicidade, que garante que a característica seja única para cada indivíduo. Permanência, pois a característica não pode sofrer grandes alterações com o passar do tempo. Coleta, que indica que a característica pode ser medida quantitativamente. Além disso, a característica deve ter a aceitação pública e ser de fácil aquisição (MAZI, Renan Corio., 2009).

A Biometria pode utilizar aspectos comportamentais ou características físicas do usuário. Dados como os da impressão digital, face, íris e formato da mão são classificadas como características físicas ou estáticas. Já o reconhecimento de voz e as análises de assinatura encontram-se no grupo de características comportamentais ou dinâmicas (GARCIA, Rodrigo de Luis, et al., 2003). A figura 3 ilustra as características biométricas mais comuns usadas. O uso de características biométricas para identificação é viável porque se apresentam de formas diferentes em cada pessoa, nem mesmo entre irmãos gêmeos, que apesar de serem muito parecidas, elas não são idênticas.

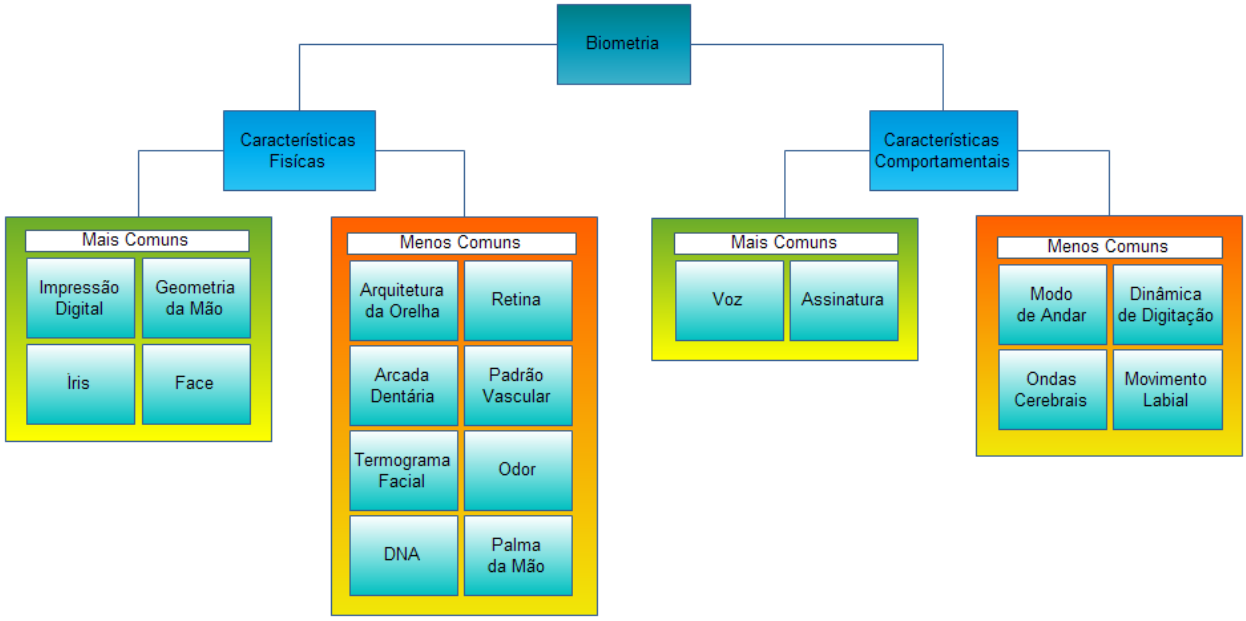

Figura 3: Características biométricas mais comuns e outras (COSTA, 2006)

A tabela 2 mostra um comparativo entre as principais características biométricas.

Biometria	Universalidade	Unicidade	Permanência	Coleta	Aceitação
Digital	Media	Alta	Alta	Media	Media
Face	Alta	Baixa	Media	Alta	Alta
Iris	Alta	Alta	Alta	Media	Baixa
Mão	Media	Media	Media	Alta	Media
Assinatura	Baixa	Baixa	Baixa	Alta	Alta
Voz	Media	Baixa	Baixa	Media	Alta

Tabela 2: Comparativo entre características biométricas **(COSTA, Luciano., 2007)**

3.5 Vantagens dos Sistemas Biométricos

Os sistemas convencionais de identificação levam em consideração mecanismos que utilizam dois elementos: o que se sabe e o que se possui. O elemento conhecimento é o mais utilizado para fornecer uma identidade aos sistemas computacionais, como

senhas, chaves de criptografia ou PIN, as soluções baseadas na entidade propriedade caracterizam-se por um objeto físico que o usuário possui como cartões inteligentes (*smartcard*), cartões magnéticos ou *token*. A figura 5 ilustra a evolução dos dispositivos utilizados em sistemas de identificação.

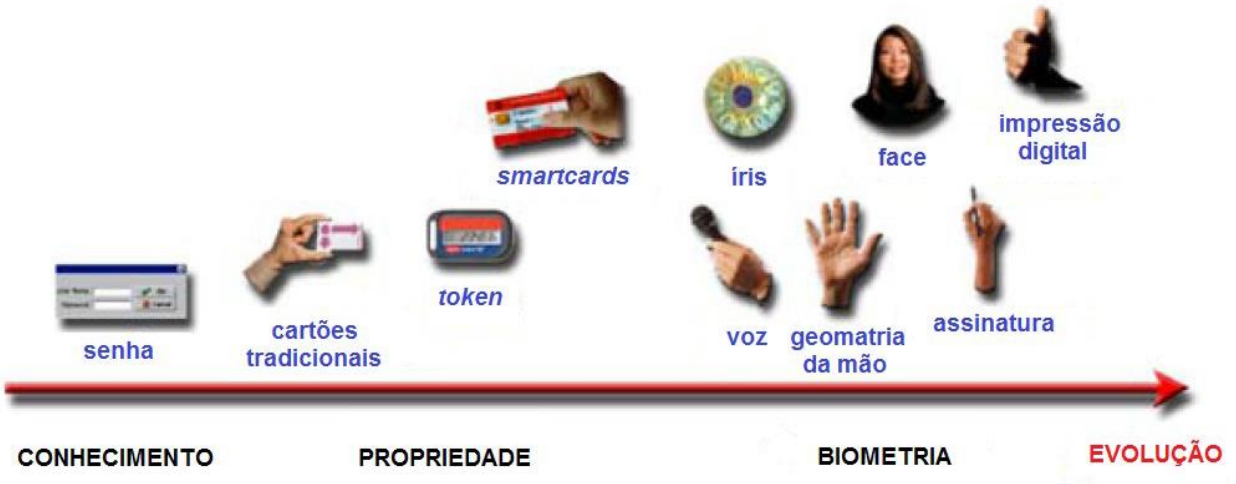

Figura 4: Evolução dos dispositivos utilizados na identificação (fonte:COSTA, 2001)

Normalmente alguns sistemas usam a combinação de algo conhecido com a posse de objetos para identificação, o problema é que os objetos podem ser perdidos, roubados ou esquecidos e os códigos e senhas podem ser descobertos ou compartilhados. Uma vez que isso aconteça, qualquer pessoa não autorizada poderia se passar pelo legitimo usuário (JAIN; BOLLE; PANKANTI, 2002). As três principais vantagens que o uso da Biometria em lugar dos sistemas convencionais proporciona são:

- **Identificação mais confiável**: Com a Biometria, é mais provável que a pessoa que tenta obter acesso a determinado bem ou serviço é quem diz ser, uma vez que o risco de ter a chave biométrica perdida é bastante reduzido. É praticamente impossível que um impostor encontre um dedo ou olho perdido para se submeter ao reconhecimento biométrico;

- **Eliminação de compartilhamento de senha**: A característica biométrica está associada a uma única pessoa e não pode ser separada desta pessoa, o que elimina o compartilhamento de senhas por parte dos usuários;

- **Identificação mais conveniente**: A forma em que as soluções biométricas são implementadas podem tornar a identificação mais conveniente do que os sistemas convencionais. Apresentar a impressão digital para efetuar uma identificação é mais prático e leva menos tempo do que digitar o nome de usuário e a senha.

O uso de sistemas biométrico, além de proporcionar comodidade às pessoas pelo fato de não precisarem lembrar diversas senhas ou carregarem diversos cartões, também traz melhorias na segurança.

3.6 Taxas de Erro na Biometria

O desempenho de um sistema biométrico pode ser obtido por meio da taxa de reconhecimento, levando-se em conta duas medidas. (PEREIRA, Leonardo de Pádua Costa., 2003).

- **Taxa de falsa aceitação** (FAR - False Acceptance Rate) - A FAR é a probabilidade que tem um sistema biométrico de identificar incorretamente um indivíduo ou falhar na rejeição de um impostor, ou seja, representa a percentagem de usuários não autorizados que são incorretamente identificados como usuários válidos.

- **Taxa de falsa rejeição** (FRR - False Rejection Rate) – A FRR é a probabilidade que tem um sistema biométrico de falhar na identificação de um usuário legítimo e representa a 62 percentagem de usuários cadastrados que são incorretamente rejeitados pelo sistema.

A taxa de erro igual (EER Equal Error Rate) é o ponto em que a taxa de falsa aceitação é igual à taxa de falsa rejeição. Dessa forma, um sistema que apresente tanto a FRR como a FAR de 1%, também terá um EER de 1%. Este é um parâmetro muito importante na avaliação de algoritmos de reconhecimento, de forma que quanto menor a EER, melhor o algoritmo.

A figura 6 mostra um gráfico onde é possível observar a relação existente entre as taxas FAR, FRR e EER.

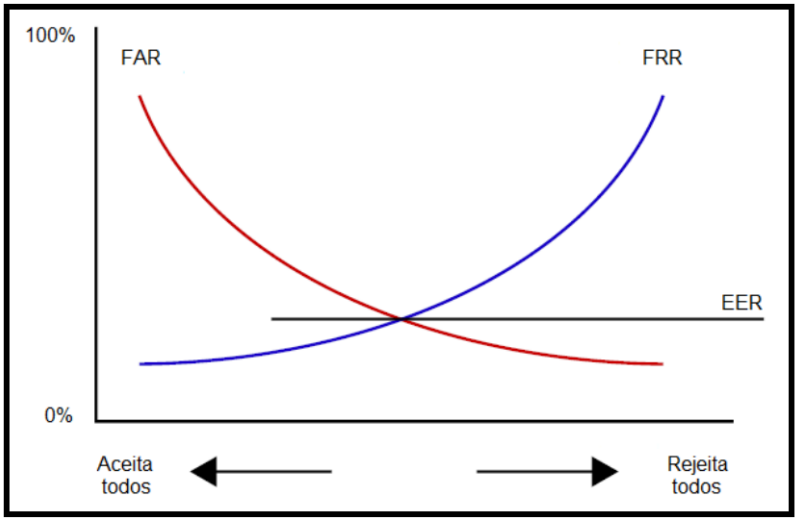

Figura 5: Relação entre FAR, FRR e ERR (fonte:PEREIRA, 2003)

A Tabela 1, mostra os números da Biometria, assim como as taxas de falsa rejeição, aceitação e o tempo que leva para a leitura dos dados.

Tabela 3: Números da Biometria (Fonte: www.Biometria.com.br)

Tipo de Sistema	Falsa rejeição (%)	Falsa aceitação (%)	Tempo (seg.)
Impressão digital	9,40	0,00	7
Retina	1,50	1,50	7
Palma da mão	0,00	0,00025	3
Reconhecimento facial	0,10	0,10	3
Voz	8,20	0,40	3

3.7 Metodos actualmente usados

A troca e roubo de bebés está geralmente ligada a má-fé do ser humano, á não verificação da identidade do bebé, aliada a escassez de recursos, tanto humanos como materiais. O registo das parturientes é feito em um livro de registo a manuscrito e guardados em pastas de arquivos em uma sala, o método de registo digitalizado será guardado em uma base de dados, e a probabilidade do desaparecimento de qualquer registo de dados é chegada a zero visto que os dados serão guardados em uma "nuvem". A esse respeito, os fatores que mais contribuem para a incidência das trocas e roubo de bebés nos hospitais são:

a) Pulseirinha plástica com fecho que não é resistente;
b) Similaridade nos nomes das parturientes (quando o mesmo esta identificado na pulseirinha);
c) Pulseirinha feita com esparadrapo: descolam-se com facilidade;
d) Nascimento de vários bebés em simultâneos e escassez de recursos humanos na assistência;
e) Não verificação das pulseirinhas "mãe-bebé" na saída do hospital após a alta;
f) Ausência total de identificação do neonato;
g) Diferenças físicas entre a mãe e o bebé.

3.8 Comparação entre os tipos de Biometria para Recém-Nascidos

Existem diversos tipos de Biometria, desde os que se baseiam na geometria das mãos à analise de assinatura, os sistemas biométricos se baseiam em características intrínsecas do ser humano, podem ser empregues como métodos de autenticação rápida e com alto nível de precisão. Tem, como uma de suas principais vantagens, o facto de ser intransferível, não poder ser perdido e nem roubado.

- **Impressão digital**

A Impressão digital é formada durante a gestação, sendo constituída por sulcos presentes nas pontas dos dedos. A forma como estes sulcos estão dispostos formam as características da impressão digital, as minúcias, que são únicas em cada indivíduo. Estas características são extraídas através de um software de processamento de imagem e transformadas em um modelo biométrico que é utilizado para o reconhecimento. A impressão digital é o método mais utilizado, pois além de ser mais barato também é muito seguro (HOUSE, 2010). O método da impressão digital é o mais viável para o reconhecimento dos recém-nascidos por essa fazer a leitura das digitais do ser humano, essas que são únicas e inerentes de cada ser humano e não podem ser fraudadas dado que todo ser humano tem impressão digital diferente um ao outro. A figura 7 mostra o dispositivo de reconhecimento por impressão digital.

Figura 6: Reconhecimento por impressão digital (Fonte: HOUSE, 2010)

- **Leitura de íris**

A estrutura da Íris é complexa e única em cada pessoa, o que a torna uma característica para identificação biométrica. Uma imagem digital da íris tirada sob

uma iluminação infravermelha é processada por algoritmos que extraem a amostra biométrica necessária para o processo de reconhecimento (GREGORY; SIMNO, 2008). Além disso, não há certeza de que as características obtidas serão mantidas com o passar do tempo. A figura 8 mostra o reconhecimento pela íris.

Figura 7: Reconhecimento por íris (Fonte: DETROIT, 2022)

- **Reconhecimento facial**

O sistema biométrico de identificação pela imagem facial baseia-se na característica única de cada face humana. De maneira geral, um sistema biométrico de identificação pela imagem facial funciona da seguinte maneira (três etapas): Um sensor, ou câmara digital, regista a imagem facial. Embora o reconhecimento facial seja uma tarefa rotineira para os humanos, para uma máquina é extremamente complexa a tarefa de comparar duas imagens digitais de face. O problema é que a máquina não tem a capacidade que os humanos têm 69 de observar as alterações típicas da aparência facial como expressões, presença de barba, maquiagem ou mudanças no corte de cabelo (GREGORY; SIMNO, 2008). Devido a semelhança que os recém-nascidos tem, o reconhecimento facial não se adequa ao nosso objectivo de estudo. figura 9 mostra o reconhecimento através da face.

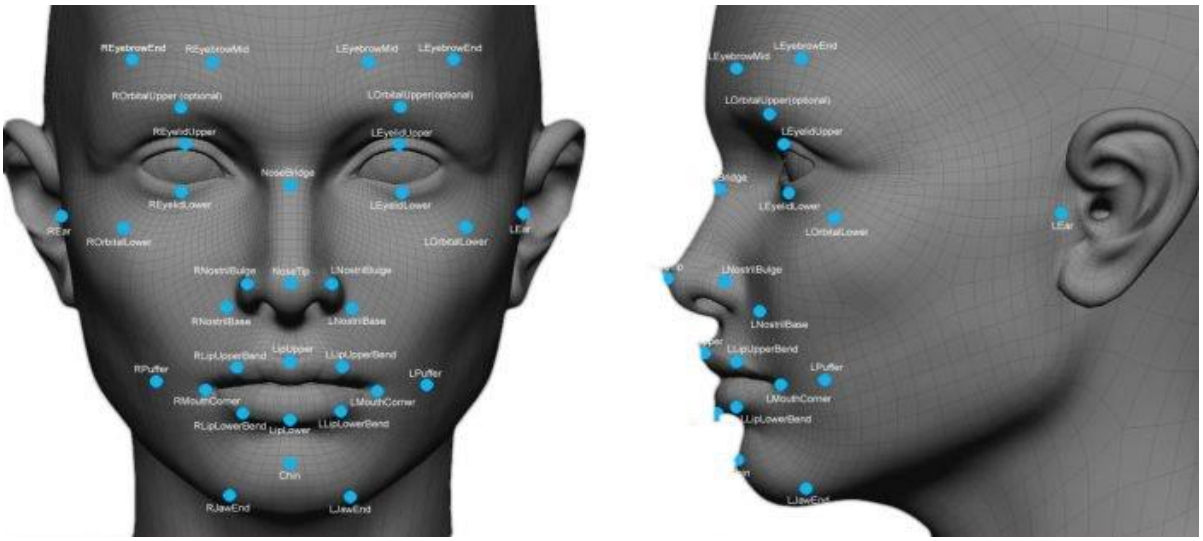

Figura 8: Reconhecimento facial **(**Fonte: Biometrics Ideal Test, http://biometrics.idealtest.org)

- **DNA**

Para o DNA, há dois aspectos que precisam ser mencionados. Além do fato de ser uma tecnologia invasiva, existe a necessidade de tirar o sangue para capturar as informações, método este que pode ser fraudado e que não apresenta resultados dos objectivos.

Figura 9: DNA (fonte: http://biometrics.idealtest.org)

- **Geometria da Mão**

A geometria da mão é outro método que também pode ser usado no processo de reconhecimento. Consiste na medição da mão, tamanho do dedo, largura e área. Estas características são distintas o suficiente para permitir a autenticação de um indivíduo, no entanto, não são suficientes para uma pesquisa de identificação (JUNIOR; ORLANS; HIGGINS, 2002). No momento da utilização o usuário posiciona sua mão no leitor, sempre na mesma posição, e uma câmara posicionada acimacaptura a imagem. Para que não ocorra a rotação da mão durante a utilização, os dispositivos leitores contêm pinos que indicam onde cada dedo deve ficar posicionado, melhorando a qualidade da imagem (PEREIRA, 2003). A figura 11 mostra o reconhecimento através da geometria das mãos.

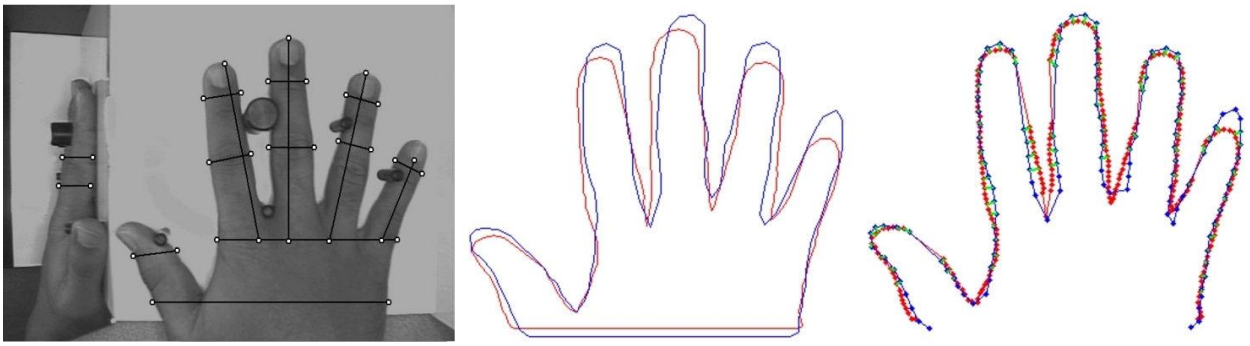

Figura 10: identificação geométrica da mão (Fonte: JAIN; ROSS; PANKANTI, 1999)

- **Assinatura**

A assinatura pode ser usada em um sistema de identificação biométrica de dois métodos: um examina a assinatura já escrita, como se fosse uma imagem, e compara com o modelo armazenado; o outro não se baseia apenas na comparação de assinaturas, mas consiste em analisar características tais como velocidade, direção e pressão exercida durante o processo de realizar a assinatura. Os dispositivos utilizados

para análise dinâmica são canetas óticas e superfícies sensíveis (COSTA; OBELHEIRO; FRAGA, 2006). A figura 12 mostra o reconhecimento por assinatura.

Figura 11: Reconhecimento de assinatura **(ZONE, Pro Security., 2022)**

- **Voz**

O reconhecimento de voz analisa o som produzido pelas cordas vocais e é um dos sistemas menos invasivos. O reconhecimento leva em consideração características como a frequência e o tamanho das ondas sonoras que estão relacionadas ao formato da boca e cavidades nasais. Durante o processo de captura o usuário utiliza um microfone para pronunciar algo específico ou uma frase qualquer, repetida vezes, para a extração de um modelo biométrico (PEREIRA, 2003). A figura 13 mostra como é o reconhecimento de voz.

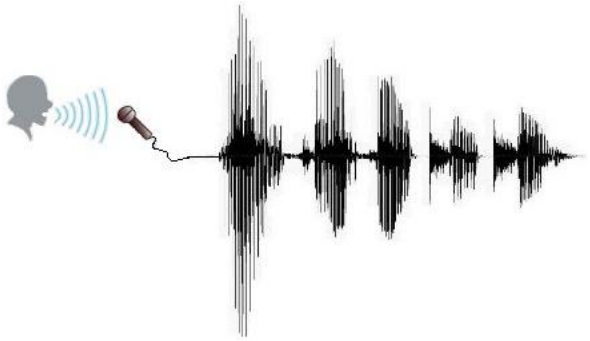

Figura 12: Reconhecimento de voz(Fonte: PEREIRA, 2003)

Dentre as características biométricas existentes algumas são mais utilizadas devido ao melhor custo/beneficio e também pela facilidade de utilização devido a vários aplicativos no mercado. A tabela 4 mostra em percentagem a utilização das principais características biométricas.

Tabela 4: Utilização das principais características biométricas (COSTA, 2007)

Tecnologia	Utilização
Digital	52%
Face	16%
Iris	12%
Voz	10%
Mão	6%
Assinatura	3%

4 DESENVOLVIMENTO DO TRABALHO

Neste capítulo será apresentada a elaboração do estudo de caso para a aplicação dos conceitos obtidos durante a revisão bibliográfica. É apresentada também a modelagem do problema, bem como os métodos utilizados para obter a solução.

4.1 Descrição do projecto

Neste projecto foi desenvolvido um sistema biométrico que utiliza dois procedimentos de reconhecimento. O primeiro é quando a paciente se apresenta como parturiente e é feito o registo dos seus dados na entrada a sala do parto. O segundo, é quando a identificação da paciente ocorre a partir do dado biométrico dela, acoplando ao dado biométrico do neonato, então, guarda-se as informações e faz-se uma busca no banco de dados, comparando as informações até que seja encontrado ou não um registo idêntico ao que é procurado.

4.2 Identificação por Impressão Digital

De acordo com Vaesken 2006, Juan Vucetich foi o primeiro a sugerir a identificação sistemática de recém-nascido através de suas impressões digitais coletadas no momento do parto, em 1915. Galton, 1899, entretanto, relata que foi consultado quanto a possibilidade de se coletar a impressão digital de bebés, para poder reconhecê-los caso fossem sequestrados e recuperados passado algum tempo.

Como a primeira utilização das impressões digitais para a identificação está relacionada à área penal, algumas pessoas se sentem desconfortáveis em fornecer suas impressões em aplicações civis. Entretanto, por oferecer um elevado grau de confiança, os sistemas biométricos de identificação baseados em impressões digitais estão se tornando cada vez mais populares (PRABHAKAR, Salil., 2001).

4.3 Formação e Constituição

O conjunto de cristas e vales que constituem a impressão digital forma desenhos característicos. Estes desenhos são desenvolvidos durante os primeiros sete meses de gestação do feto, como consequência genética e também pelas condições do ambiente

uterino, e a configuração dos seus traços não sofre alterações durante a vida toda (PRABHAKAR, 2001).

A posição no interior do útero e o fluxo de líquidos em torno do feto mudam durante a gestação fazendo com que as células dos dedos cresçam em um microambiente diferente. Os dedos de cada indivíduo e os próprios dedos de uma mesma pessoa apresentam detalhes que são determinados pelas mudanças dos diferentes microambientes onde estão inseridos.

Devido ao grande número de mudanças que ocorre durante o processo de gestação, é praticamente impossível que duas impressões digitais sejam iguais, embora, pelo fato dos genes também contribuem para sua formação, alguns dos traços que definem a impressão digital podem apresentar grandes semelhanças, principalmente entre gêmeos idênticos (PRABHAKAR, 2001). Porém mesmo com a semelhança das impressões, elas não são iguais. A figura 14 mostra as impressões digitais de gêmeos idênticos.

Figura 13: Impressões digitais de gêmeos idênticos (Fonte: PRABHAKAR, 2001)

4.4 Identificação de recém-nascidos

Segundo a Natosafe, Empresa brasileira criada com o propósito de contribuir para um mundo mais seguro. Pioneira no segmento "*INFANT ID*", ou solução de identificação infantil, a companhia se dedica ao desenvolvimento de tecnologias de identificação biométrica para crianças de 0 a 5 anos. A Plataforma *INFANT.ID* é a primeira no mundo capaz de colectar impressões digitais com alta qualidade desde as primeiras horas de vida de um bebé(https://natosafe.com.br).

A identificação dos recém-nascidos é uma das principais atribuições da equipa medica na hora do parto, e tem por objectivo objectivo evitar a troca de bebés, bem como possibilitar uma futura confirmação da identidade da criança e de seus pais. Além disso a coleta de material que possibilite a identificação da criança pode servir de instrumento para evitar o trafico ou adoções ilegais, e também para a emissão de documentos de identidade para recém-nascidos. A figura 15 ilustra o momento em que a impressão do recém-nascido é colhida usando um leitor biométrico para recém-nascidos.

Figura 14: Funcionamento Scanner Biométrico da Nilmaone (Fonte: natosafe.com.br/infantid/)

4.5 Implementação do sistema de identificação biométrica na maternidade

Um dos métodos não biométricos mais utilizados é a colocação de pulseiras com códigos de identificação, logo após o nascimento. Entretanto, tal método pode ser defraudado alterando-se ou removendo-se a pulseira, além disso, o método não serve para uma futura identificação da criança. Outro método bastante popular, inequívoco e frequentemente empregado é a identificação utilizando o DNA. Entretanto, o método ainda demanda laboratórios sofisticados e não pode ser utilizado em tempo real. Além

disso, não é capaz de diferenciar gêmeos univitelinos[1], e é potencialmente invasivo. (LEMES, et. al., 2012).

Um sistema de identificação biométrico é composto por um dispositivo de registo biométrico (reconhecimento facial, geometria das mãos, leitura da Iris, leitura da retina e padrões de assinatura) acoplado a uma plataforma de dados que são recebidos a tempo real.

O reconhecimento facial com taxas altas de eficiência ainda é uma tarefa difícil até mesmo quando aplicado a adultos. Isto ocorre porque tais sistemas são suscetíveis às variações de iluminação, pose e expressão. Além disso, a face de recém-nascidos também sofre drásticas mudanças nos primeiros dias e meses de vida, tornando difícil o reconhecimento de dado indivíduo no futuro utilizando esta mesma característica.

Embora o reconhecimento por íris obtenha taxas expressivas de reconhecimento em adultos, não é viável sua utilização em bebês, uma vez que dificilmente abrem seus olhos. Além disso, deve-se evitar qualquer contato do olho do recém-nascido com tais dispositivos. Outro facto relevante é que o padrão da íris somente se estabiliza depois do segundo ano de vida da criança. Entretanto, quando se considera a captura de imagens de impressões digitais, impressões palmares e plantares, estudos reportam que é uma tarefa desafiadora coletar tais imagens de recém-nascidos. Este problema reside basicamente no facto de que os sensores não apresentam resolução adequada às especificidades das impressões digitais em recém-nascidos. Assim como a leitura da retina, os padrões de assinatura são métodos não viáveis para o registo dos recém-nascidos.

No projecto em causa, por tratar-se de recém-nascidos achou-se viável usar as cristas papilares presentes nos dedos da mão (impressão digital). Isto se deve principalmente ao facto de que são não invasivas, possuem alta disponibilidade, possuem grande aceitação por parte do usuário. Além disso, são sem dúvida as características mais utilizadas e estudadas. A figura 16 ilustra o vínculo biométrico entre mãe e filho.

[1] Gemêos Univitelinos (monozigóticos) são os que nascem com caracteristicas identicas e que são geralmente do mesmo sexo.

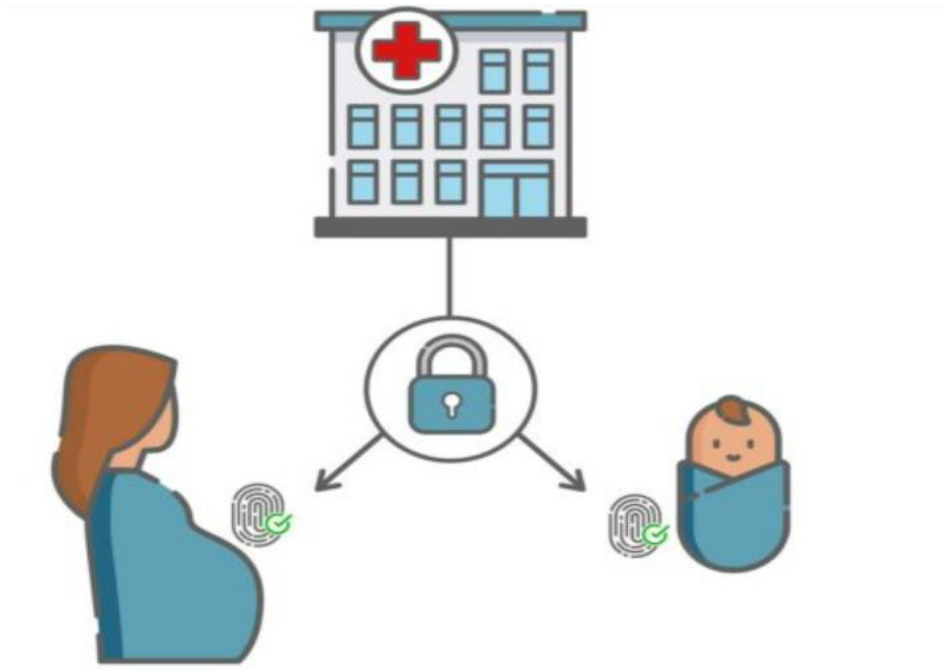

Figura 15: Vínculo Biométrico entre mãe e filho (Fonte: https://natosafe.com.br)

4.6 Modelo Autenticação Biométrica

Um ponto importante da Biometria é a diferença entre autenticação e identificação. Na autenticação, uma pessoa precisa informar ao sistema sua identidade juntamente como o dado biométrico. O sistema apenas diz se a pessoa é quem diz ser ou não. Esse processo é conhecido como comparação 1:1, pois a pessoa informa ao sistema qual perfil deve ser comparado com a amostra fornecida no momento do reconhecimento. A figura 17 ilustra o processo de autenticação.

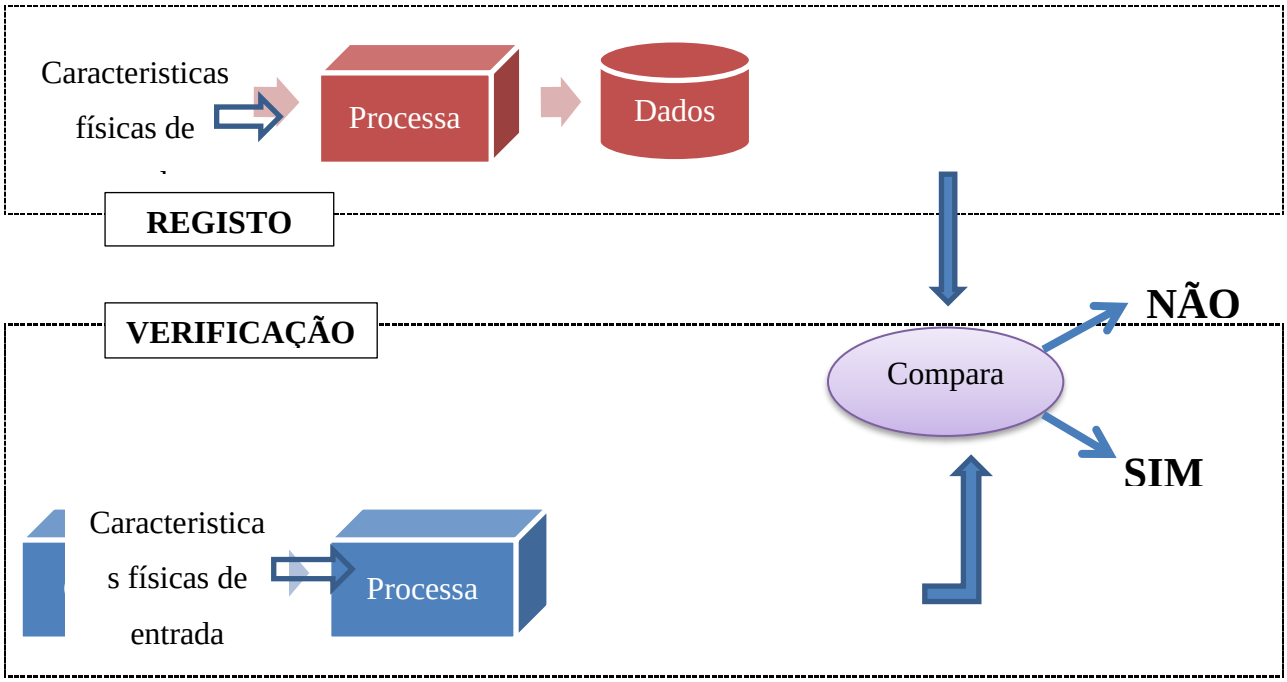

Figura 16: Diagrama de blocos **(Dantas, 2008)**

Segundo DANTAS (2008), O mecanismo de autenticação por Biometria tem dois modos: Registro e Verificação. Para o uso inicial da Biometria, cada usuário deve ser registado pelo administrador do sistema. Este verifica se cada indivíduo registado é um usuário autorizado. O processo de registo consiste no armazenamento de uma característica biológica do indivíduo (física ou comportamental) para ser usada, posteriormente, na verificação da identidade do usuário. Uma vez que o usuário está registado, os dispositivos biométricos são usados na verificação da identidade do usuário. Quando o usuário necessitar ser autenticado, sua característica física é capturada pelo sensor. A informação analógica do sensor é então convertida para sua representação digital. A seguir, esta representação digital é comparada com o modelo biométrico armazenado. A representação digital usada na verificação é chamada de amostra (live scan).

Na identificação apenas com a leitura biométrica o sistema é capaz de dizer quem é a pessoa. É um processo conhecido como comparação 1:N, uma vez que o sistema pega a amostra biométrica e compara com todos os perfis armazenados no banco

de dados, informando, caso exista um perfil com a semelhança exigida, quem é a pessoa. A figura 18 mostra o processo de identificação.

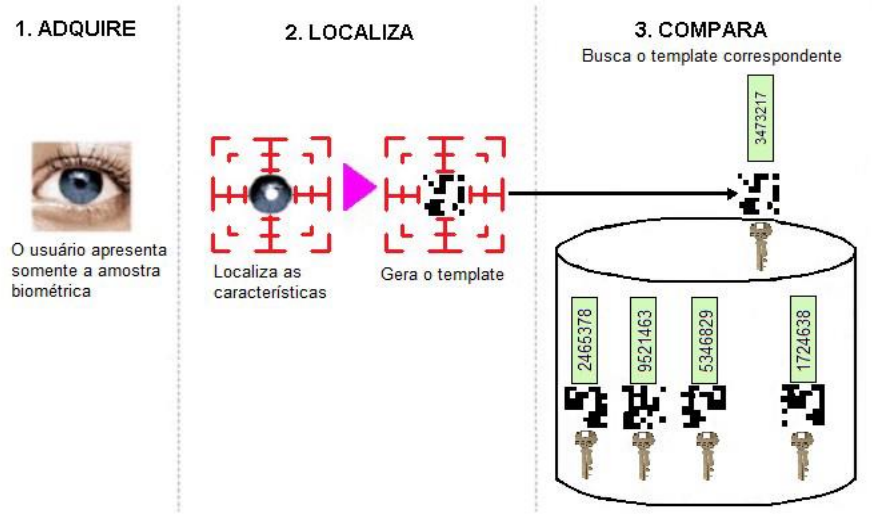

Figura 17: Sistema biométrico de identificação (Fonte: PEREIRA, 2003)

Apenas uma comparação é realizada na autenticação, o que facilita muito sua implementação, mas exige algum componente extra de identificação, como um código pessoal. A identificação é muito utilizada pela polícia que pode identificar um criminoso, mesmo que não exista uma lista de suspeitos, apenas pela obtenção das impressões digitais por ele deixadas na cena do crime.

Existem dois modos possíveis para identificação: positivas e negativas. A identificação positiva procura determinar se uma pessoa realmente está cadastrada em uma base de dados específica, sendo aplicada quando o objetivo é verificar uma identidade única entre várias outras. Contrariamente, a identificação negativa determina se o cadastro de uma pessoa não está presente em um banco de dados, podendo ser utilizada para verificar se a referida identidade não consta em uma lista de procurados (DESSIMOZ; RICHIARDI, 2006).

4.7 Descrição dos Componentes

a) Microcontrolador Esp82866

O módulo ESP8266 na figura abaixo é um transceptor sem fio autônomo de baixo custo que pode ser usado para desenvolvimentos de IoT (internet das coisas) de ponto final. Para se comunicar com o módulo ESP8266, o microcontrolador precisa usar um conjunto de comandos AT. O módulo ESP8266 funciona apenas com 3,3 V, qualquer coisa acima de 3,7 V danificaria definitivamente o módulo, exigindo, por isto, grande cuidado no momento do uso e utilizando, por exemplo, um circuito divisor de tensão. A escolha do microcontrolador Esp82866 para o desenvolvimento do projecto deve-se ao facto de ele ser ambíguo, e por possuir várias bibliotecas.

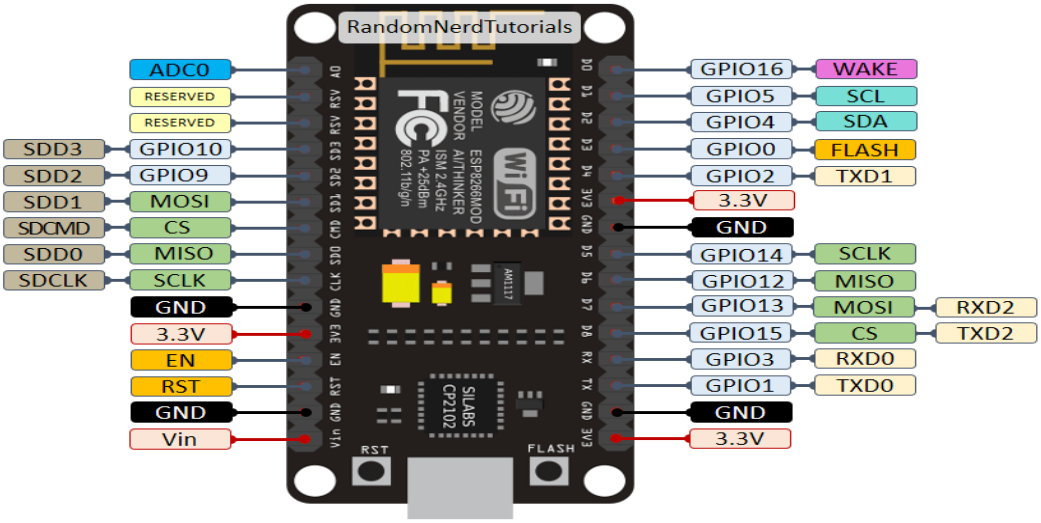

Figura 18: Esp82866(Fonte: https://blog.eletrogate.com/iot-com-modulo-wifi-esp8266-basico/ acessado 16/012/2021)

b) OLED 128x64

É uma tecnologia relativamente nova com potencial para substituir os atuais televisores LCD e LED, monitores e telas de telefones celulares. É um display com uma resolução de 128x64. OLED é uma tecnologia auto-emissora de luz composta por um filme

orgânico fino e multicamadas colocado entre um ânodo e um cátodo. No projecto o OLED fornecerá a informação da autenticação das Biometrias.

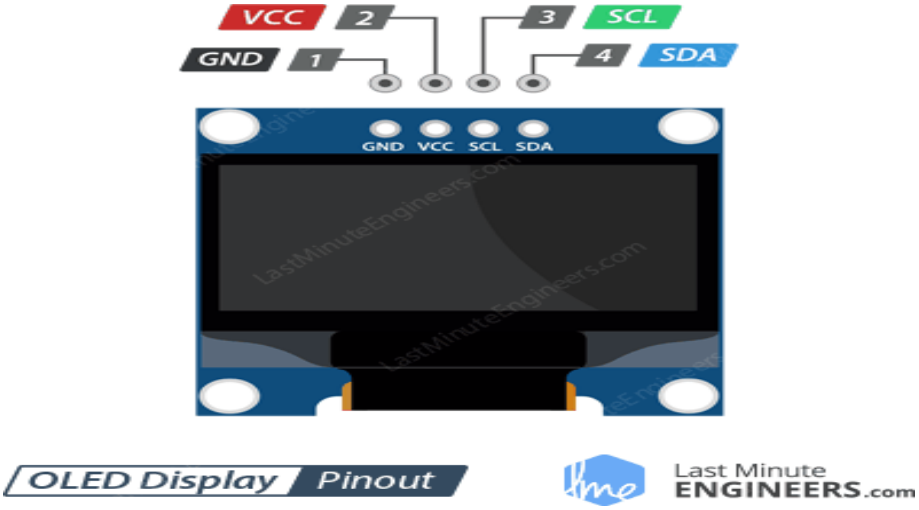

Figura 19: Display OLED (Fonte: https://lastminuteengineers.com/oled-display-arduino-tutorial/)

c) FingerPrint Display GT511C3

GT511C3 é um módulo similar de scanner de impressão digital introduzido pela ADH-Tech. É um pequeno módulo integrado a um Sensor Óptico que se comunica com os microcontroladores usando TTL Serial. Por esta razão, o módulo possui um protocolo receptor/transmissor assíncrono universal. Podemos ver a autenticação biométrica em quase todos os lugares ao nosso redor, sendo a digitalização de impressões digitais a mais frequente. O sensor irá comparar a impressão digital de teste com todos os modelos armazenados. Assim que a impressão digital digitalizada for distinguida, ela retornará o número de identificação. Quanto menor o número de modelos inscritos, mais rápido será o reconhecimento. A figura 21 ilustra o sensor de impressão digital.

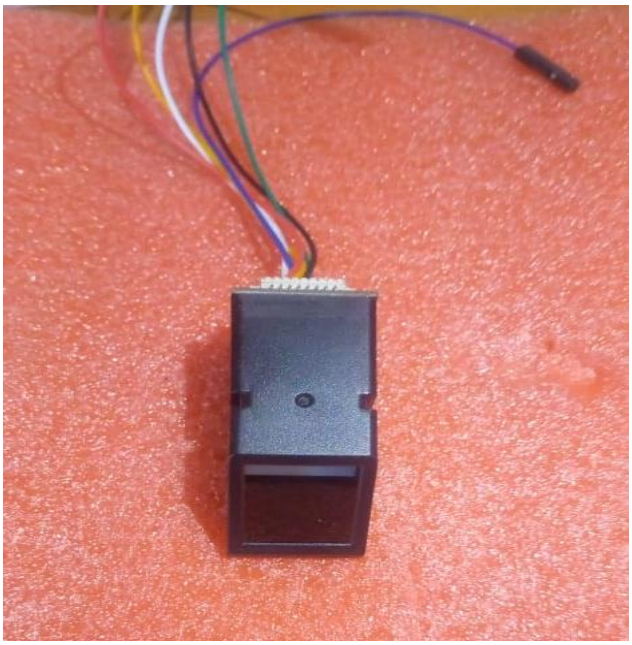

Figura 20: Fingerprint Display GT511C3 (Fonte: o autor)

d) Alimentação

Sendo o nosso dispositivo portátil, ele levará consigo fonte de alimentação, uma pilha carregada de 9 volts, que será controlada a partir de um botão liga e desliga conectado na placa do circuito impresso.

Figura 21: Pilha de 9v**(**Fonte: Google, acessado em junho de 2022)

CAPÍTULO 4: Protótipo do Projecto

5 DESENHO DO CIRCUITO

O módulo WiFi ESP82866 NodeMCU é uma das placas mais interessantes da família ESP8266, já que pode ser facilmente ligada à um computador e programada com a linguagem Lua e também utilizando a IDE do Arduíno, para o nosso trabalho foi usado a linguagem do IDE do Arduíno. A constituição do circuito do protótipo junto com as suas partes constituintes é demonstrada na figura(23), este dispositivo baseia-se em um circuito que faz a leitura dos dados biométricos pelo leitor de impressão digital ligado ao microcontrolador Esp82866 e envia a uma base de dados acoplada a base de dados da plataforma de registo, para que toda vez que quisermos buscar os dados do paciente seja digitando o nome ou inserindo a impressão digital, tenhamos os resultados desejados, o desenho foi feito na plataforma virtual Easyeda.

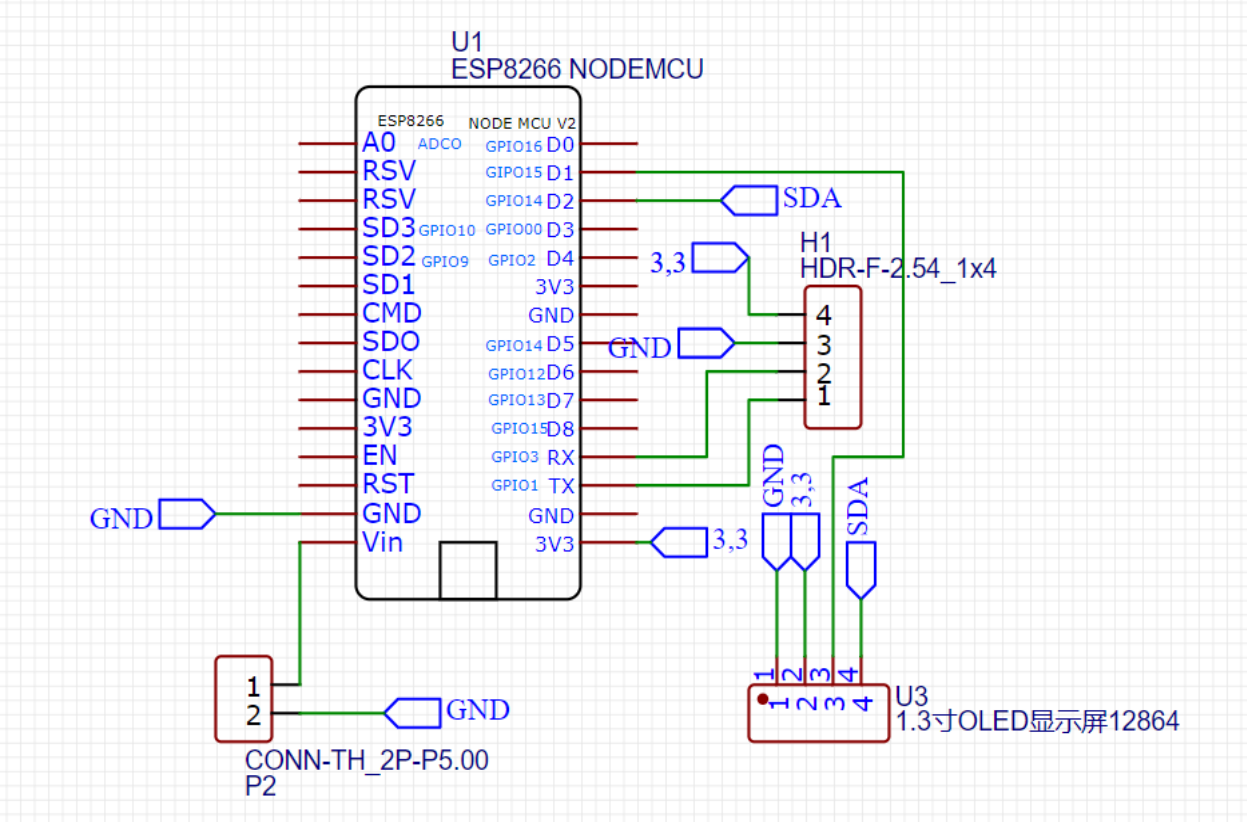

Figura 22: Desenho do circuito no Easyeda (fonte: o autor)

5.1 Plataforma Neonatal 2022

A plataforma Neonatal é um campo de registo digitalizado com o objetivo fazer o registo e de acoplar os dados do bebé à impressão digital que será colhida com o dispositivo, esse que será um dispositivo portátil dedicado com recursos que reduzissem o impacto dos modos de falha relacionados a bebês para obter imagens de impressões digitais reproduzíveis e de alto contraste acoplado a uma plataforma digital de registo. Dada a necessidade de iterar e testar rapidamente em circunstâncias reais, usamos um design de hardware modular e facilmente reconfigurável. Ao desenvolver qualquer sistema óptico, existem alguns elementos-chave de design que precisam ser otimizados para uma aplicação específica. A solução desenvolvida pela inclui um scanner biométrico e um sistema de registo seguro no acompanhamento e evolução dos traços biométricos de cada uma das crianças (e seus respectivos pais) que integram os bancos de dados.

Para o desenvolvimento do sistema da plataforma foi utilizada a linguagem programação JavaScript com Ambiente de execução Node.js, tendo em vista que ela é adequada para garantir a expansão dessas tecnologias. A tecnologia baseada em Biometria possui vários recursos associados, como banco de dados e aplicativos, o que facilita muito os desenvolvedores nos projetos.

5.2 Fluxogramas

A figura 24 e 25 ilustra os fluxogramas do sistema do registo dos pacientes.

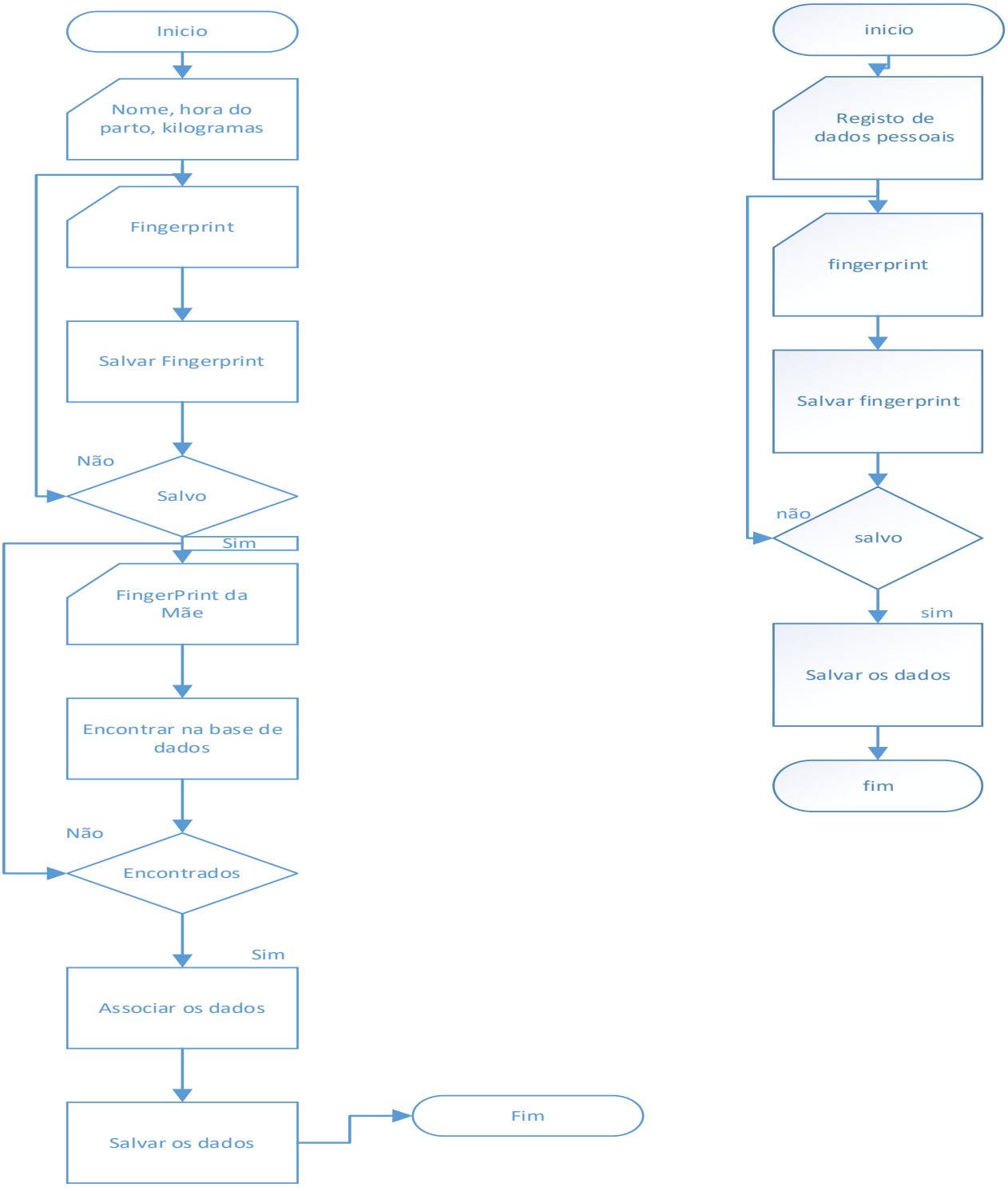

Figura 23: Registo dos dados do bebé (a esquerda), e da mãe (a direita)**. (**Fonte: o autor, desenho feito no Microsoft visio)

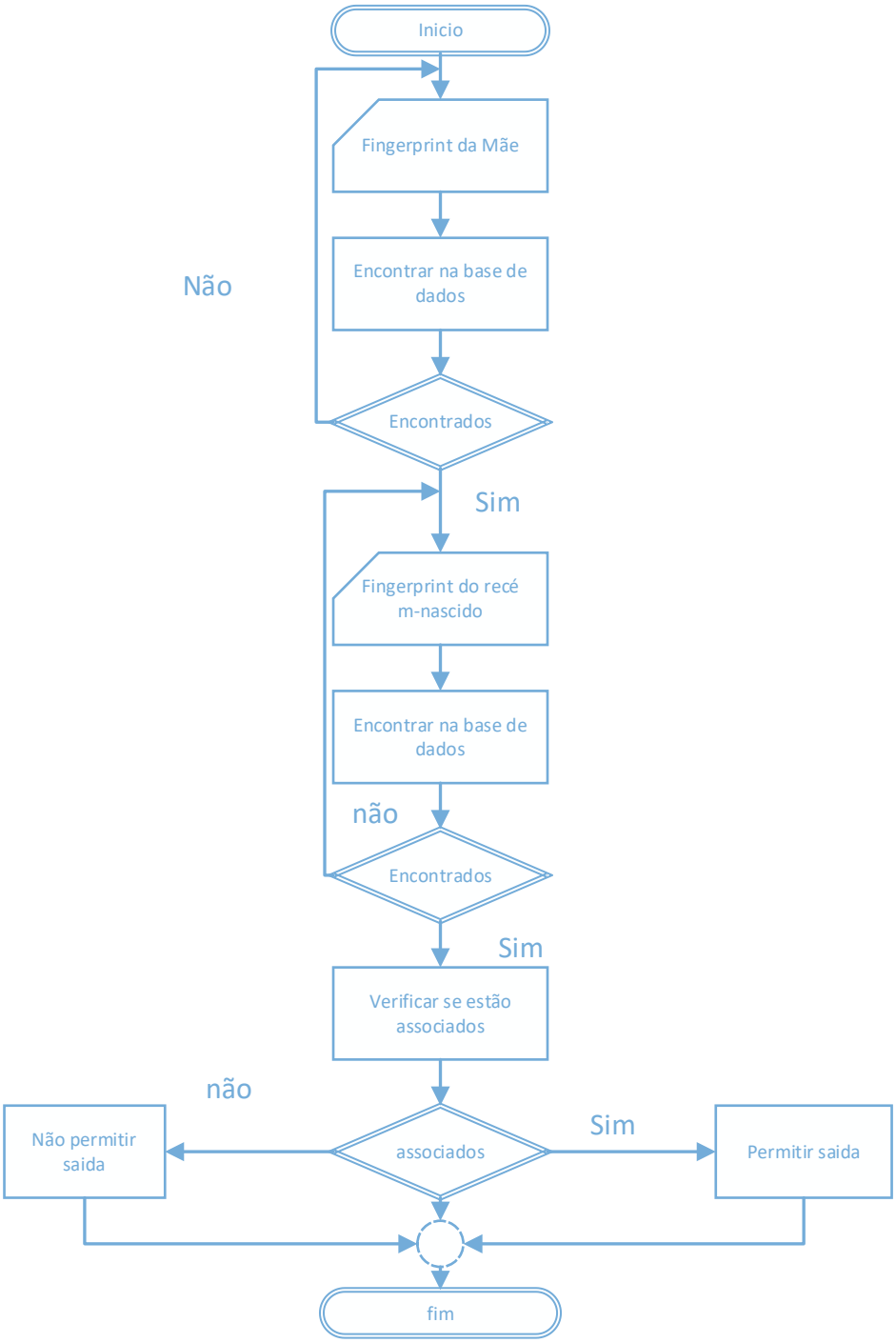

Figura 24 verificação dos dados da mãe e do bebé**(**Fonte: o autor (desenho feito no microsoftvisio)

O fluxograma mostra como serão feitos os registos do bebé e da mãe e que procedimento serão seguidos para o registo completo, utilizando a plataforma digital R-Neonatal. Ele permite registar os dados da mãe na sua chegada a unidade hospitalar, acoplando-os às do filho minutos após o parto guardando-as numa base de dados, as mãozinhas do bebé serão registadas por um leitor que automaticamente vincula as imagens à identidade da mãe ou responsável.

O registo é feito na seguinte forma:

1. Ao acessar a plataforma, depara-se com a página de entrada do sistema de Registo Neonatal com configuração simples.
2. A página inicial apresenta um menu vertical na lateral esquerda e duas abas à direita que ilustra o número de filhos e mães cadastrados no sistema, permitindo também novos cadastros no mesmo.
3. No campo aberto (perfil da mãe), encontram-se listados todos os dados pessoais de cada mãe, assim como a sua impressão digital colhida através do dispositivo na sua chegada à maternidade.
4. Após o parto, o mesmo processo acontece com o bebé, vinculando os seus dados aos da mãe. Esses dados podem ser encontrados pesquisando de forma independente cada um deles, o que possibilita o reconhecimento e confirma a maternidade da criança.

5.3 Layout da Plataforma Neonatal

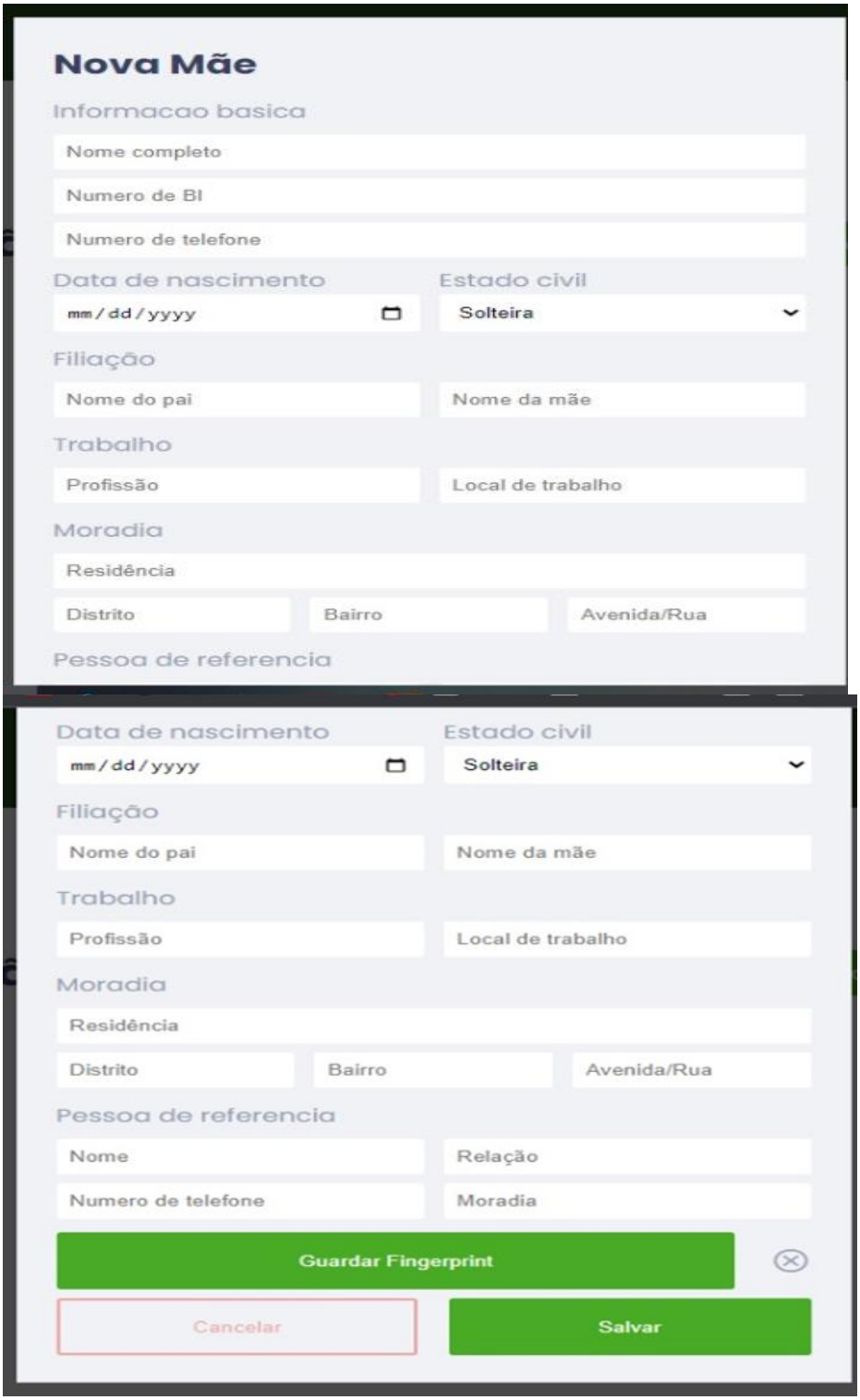

Figura 25: Layout do campo de registo da Mãe(Fonte: o autor)

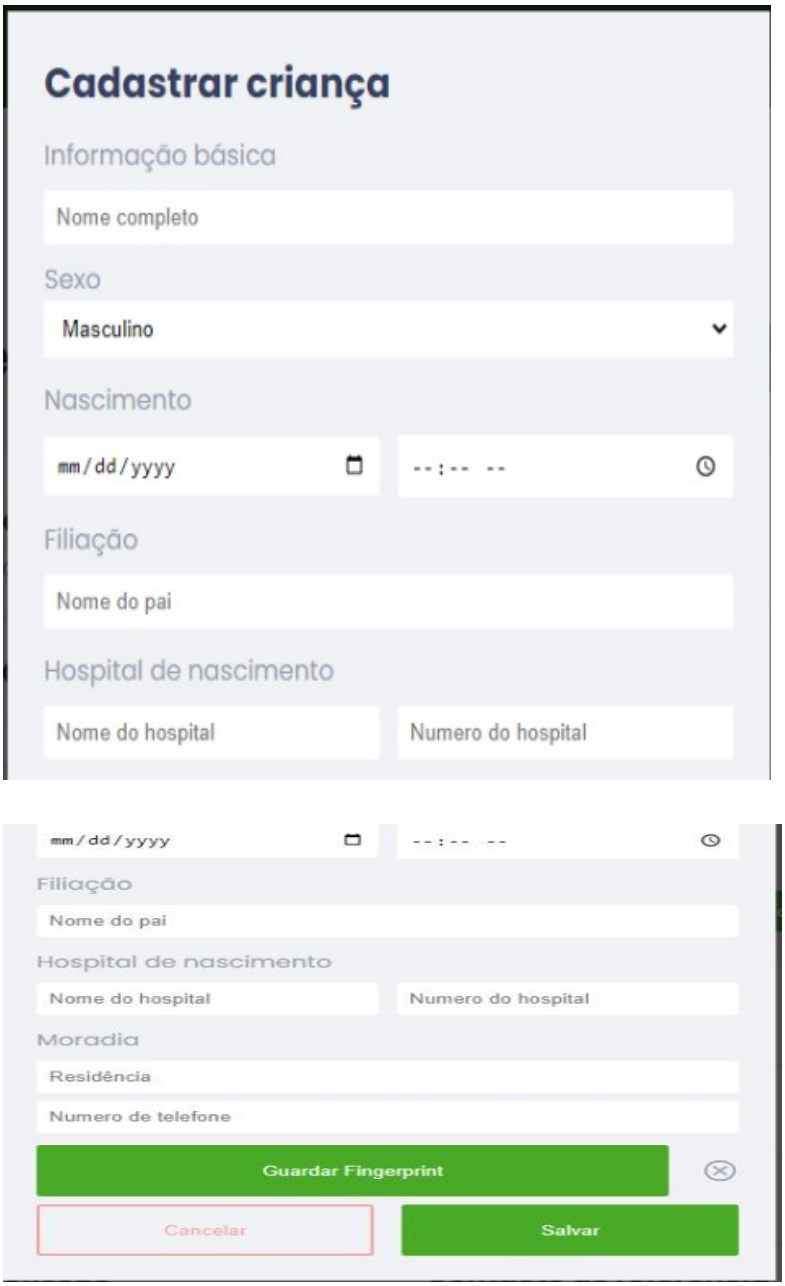

Figura 26: Layout do campo de registo do filho (Fonte: o autor)

5.4 CUSTOS DO MATERIAL

O custo total do projecto foi de 16 405,00mt calculado na base no valor da aquisição, importação e o desalfandegamento dos componentes.

Tabela 5: Custo do material utilizado (fonte: o autor)

Material	Preço (MZN)	Quantidade	Total(MZN)
Placa de circuito imprenso	165	5	825
Modulo de impressão digital	1040	2	2080
Microcontrolador Esp8286	1200	2	2400
Display OLED	875	1	875
Pilhas	70	2	140
Conector de pilha	20	1	20
Botão	90	1	90
Caixa	300	1	300
Spray	200	1	200
Transporte (placas e componentes)			5475
Impostos aduaneiros			4000
Total			16 405,00

Os valores foram calculados com base no câmbio do dia 30/03/2022, que era: USD 1 = 63.83 MT

5.5 Resultados Esperados

O sistema de registo de impressão digital em maternidades, na sua essência, é um sistema sofisticado de segurança. Entretanto, com o seu uso e principalmente nos hospitais, espera-se a diminuição do trafico de bebé que vem acontecendo nos hospitais. Com o sistema espera-se o registo digitalizando dos pacientes naquele recinto. Um sistema de registo de impressão digital permite-nos obter maior confiança e confortabilidade as parturientes e principalmente, sentimento de segurança. Espera-se que a posterior a preocupação dos pacientes que dão entrada para os trabalhos de parto não seja mais a de saber se o seu filho será roubado ou trocado, e sim uma certeza de que independentemente do seu estado de saúde ela pode ficar tranquila que sairá com o seu filho para casa.

5.6 Resultados Obtidos

Com bom agrado foi possível obter um sistema de impressão digital que corresponde ao desejado, sendo portando, possível registar os dados do bebé acoplados aos dados da mãe, tornando assim o sistema seguro. O sistema reconhece e distingue as diferentes impressões e possui a capacidade de guardar os dados em uma base de dados não volátil consoante o desejo do utilizador. A seguir foi feita uma simulação do funcionamento do sistema. A figura 28 ilustra os dados pessoais da mãe sendo inseridos na plataforma de registo.

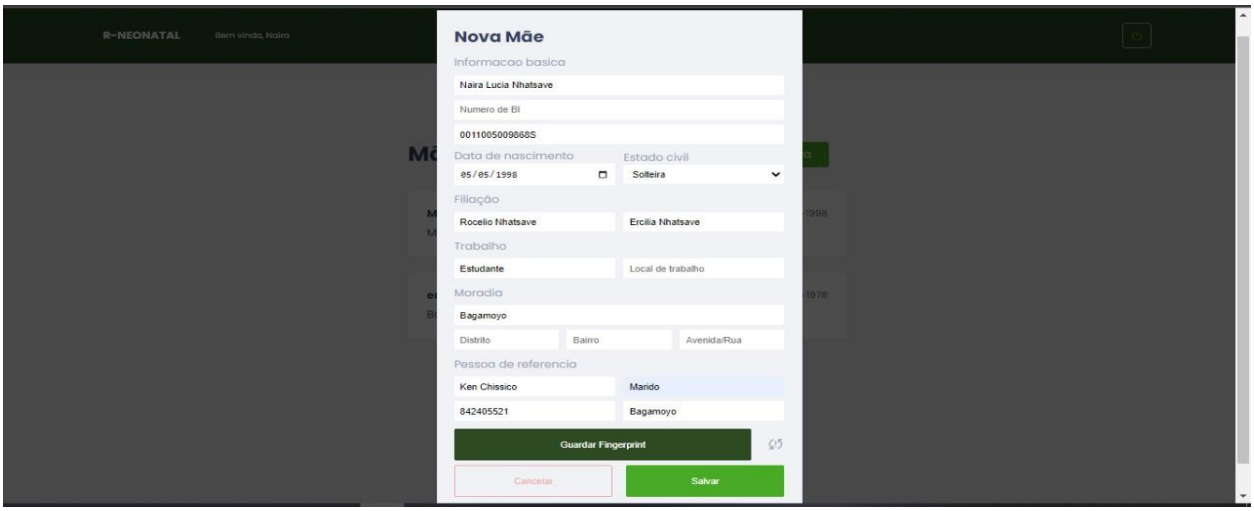

Figura 27: simulação da inserção de dados pessoais da mãe (fonte: o autor)

A figura 29, ilustra o momento em que a mãe insere a sua impressão digital.

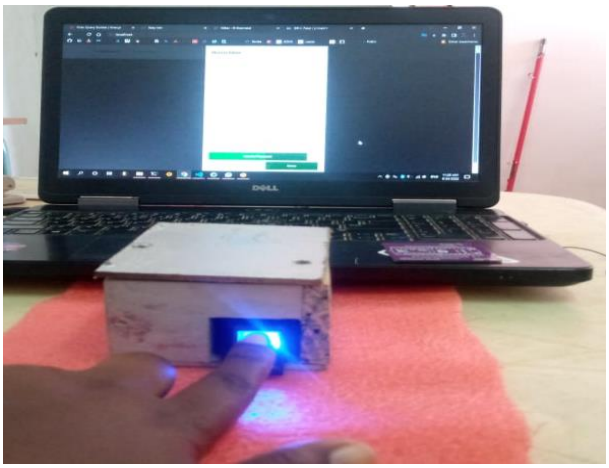

Figura 28: simulação da impressão digital da mãe (fonte: o autor)

A figura 30 ilustra o registo da impressão digital coletada e o momento em que os dados da mãe são salvos.

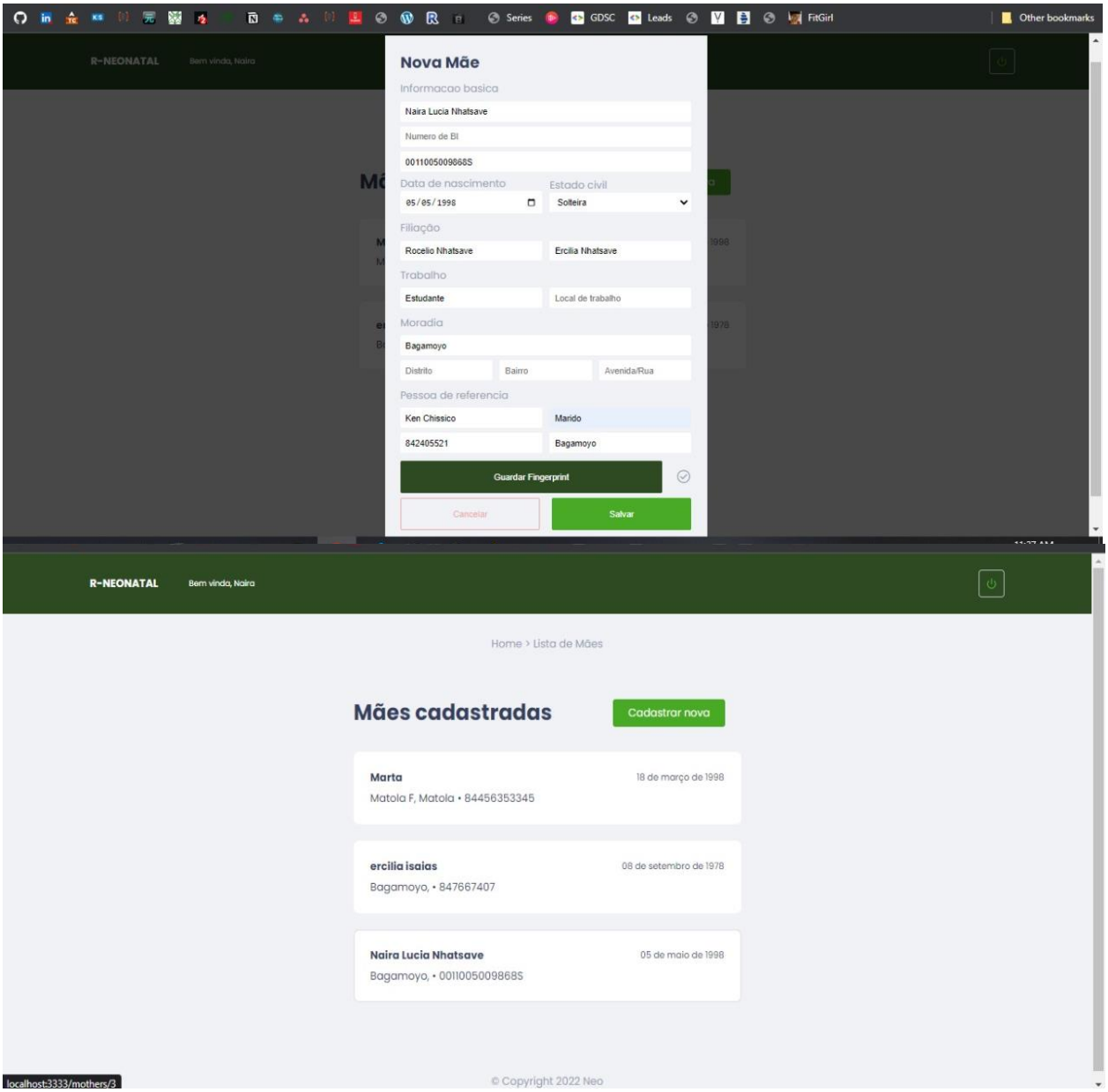

Figura 29: registo da impressão digital na plataforma. (fonte: o autor)

A figura 31 ilustra o momento em que são registados os dados do bebe e a sua impressão digital.

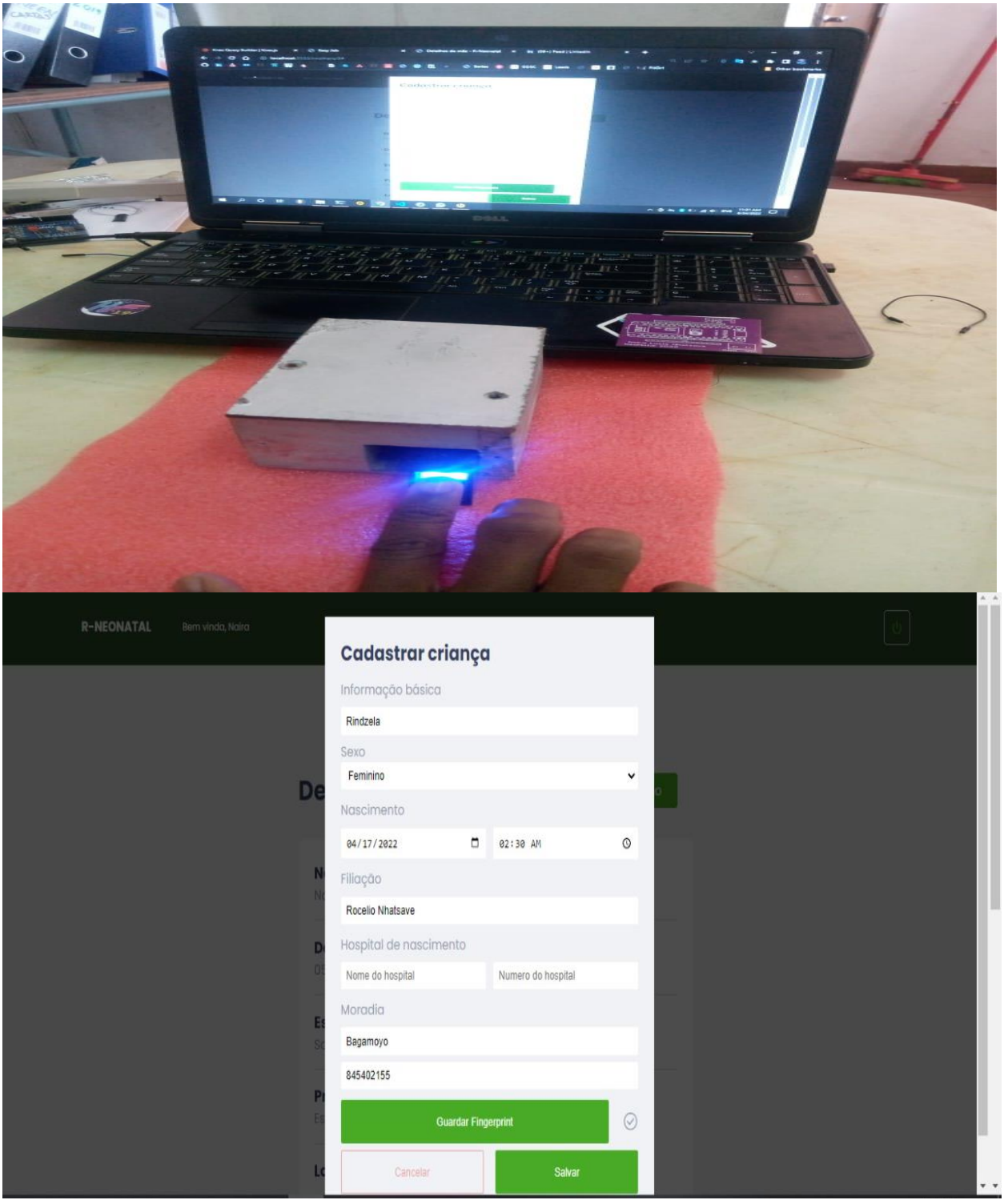

Figura 30: registo dos dados do bebe. (fonte: o autor)

A figura 32 ilustra os dados da mãe acoplados com as do bebe e guardados na plataforma.

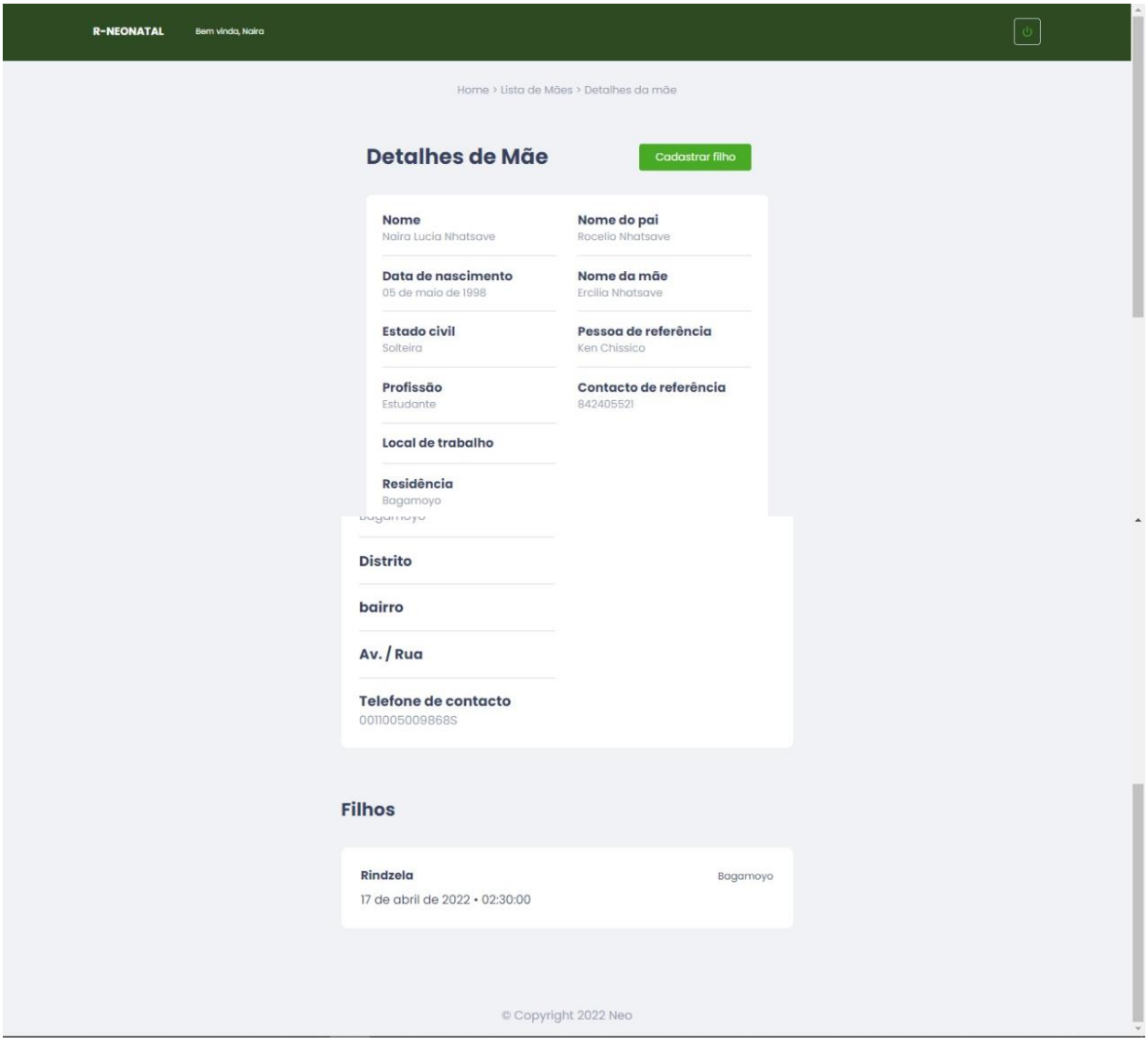

Figura 31: Acoplamento dos dados da mãe e do bebe. (fonte: o autor)

CAPÍTULO5: Conclusões e Recomendações

6 CONCLUSÕES

Este projecto apresenta resultados preliminares sobre a utilização da plataforma de cadastro, registo biométrico e identificação automática de recém-nascidos. Portanto, pode-se concluir que:

- A Plataforma Neonatal 2022 permite o registo, processamento e armazenamento digital dos dados das gestantes à entrada das unidades hospitalares e posterior registo e acoplamento dos dados dos recém-nascidos, garantindo controlo e segurança no processo de identificação outrora realizado de forma arcaica (preenchimento manual de ficha física, livro de arquivo e registo de nome da mãe/responsável nas pulseiras dos recém-nascidos);
- A Biometria apresenta-se como a solução mais viável e segura no que concerne a identificação a tempo real e com garantia vitalícia. Dentre os vários tipos de Biometria, foi escolhido o digital pois os dados podem ser colhidos com maior eficiência e permanecerão vinculados aos dados da mãe e posteriormente ser usados para a identificação civil;
- Com o desenvolvimento do protótipo para colheita da Biometria dos recém-nascidos ainda na sala de parto, as mãozinhas do bebê serão registadas por um leitor, que automaticamente vincula as imagens e dados colhidos à identidade da mãe já existente na plataforma, garantindo que nenhum bebê possa ser retirado da maternidade sem passar pelo reconhecimento biométrico.

6.1 RECOMENDAÇÕES

Para implementação do sistema neonatal com máxima eficiência em unidades Hospitalares de grande porte, recomenda-se:

- O uso de uma fonte de alimentação muito mais duradora de modo a garantir maior tempo de utilização do dispositivo;
- A realização da formação sobre como usar a plataforma direcionada às parteiras, os médicos, enfermeiros assim como as serventes;
- A aplicação da inteligência artificial para o uso da Biometria ligada a uma base de dados do Ministério de Saúde e ao Sistema de Registo civil para o reconhecimento e acesso a localização do bebé, no caso do trafico ou suspeita de troca em qualquer parte do Pais.

A toda comunidade científica, na realização de projectos futuros, recomenda-se:

O desenvolvimento de um leitor de impressão digital muito mais sensível para captar os traços biométricos (até de um recém-nascido prematuro), que podem ser usados no futuro para emissão de documentos, e capaz colher o maior número de impressões digitais (dado que o leitor usado no projecto colhe até 200 impressões).

6.2 BIBLIOGRAFIA E LINKOGRAFIA

AZEVEDO, N. (2005). Identificação neonatal. Belém – PA. XVIII Congresso Nacional de Criminalística. Oral presentation

BIOMETRICS IDEAL TEST, http://biometrics.idealtest.org

COSTA, Luciano. (2007). Um Modelo de Autenticação Biométrica para Web Banking. Dissertação (Mestrado) Universidade Federal de Santa Catarina,.

COSTA, Luciano; OBELHEIRO, Rafael; FRAGA, Joni. (2006). Introdução à Biometria. Universidade Federal de Santa Catarina: Apostila do Departamento de Automacao de Sistema .

COSTA, Silvia Maria Farani. (2001). Classificação e Verificação de Impressões Digitais. 123p. Dissertação (Mestrado) Universidade de São Paulo, São Paulo, 2001.

DANTAS, G. F. (2008). IDENTIFICAÇÃO BIOMÉTRICA: Sistemas Biométricos de Identificação Pela Imagem Facial . Histórico Biometria.

DETROIT,Unets.http://unstructuredlibertynetworks.files.wordpress.com/2009/11/irisscan.jpg Disponível em: Acesso em junho de 2022.

Lemes1, R. d., Bellon, O. R., Silva, L., & Cat, M. N. (s.d.). Identificacao biometrica de recem-nascidos.

COSTA, Luciano. (2007). *Um Modelo de Autenticação Biométrica para Web Banking.* Dissertação (Mestrado) Universidade Federal de Santa Catarina,.

COSTA, Luciano; OBELHEIRO, Rafael; FRAGA, Joni. (2006). *Introdução à Biometria.* Universidade Federal de Santa Catarina: Apostila do Departamento de.

COSTA, Silvia Maria Farani. (2001). *Classificação e Verificação de Impressões Digitais.* 123p. Dissertação (Mestrado) Universidade de São Paulo, São Paulo, 2001.

Dantas, G. F. (2008). IDENTIFICAÇÃO BIOMÉTRICA: SISTEMAS BIOMÉTRICOS DE IDENTIFICAÇÃO PELA IMAGEM FACIAL . *HISTÓRICO BIOMETRIA*.

DESSIMOZ, Damien; RICHIARDI, Jonas. (2006). *Multimodal Biometrics for Identity.* UNIL Université de Lausanne, Lausanne, Suíça, 2006.

DETROIT, Unets. (s.d.). <http://unstructuredlibertynetworks.files.wordpress.com/2009/11/irisscan.jpg>.

GARCIA, Rodrigo de Luis, et al. (2003). *Biometric Identification Systems.* Signal Processing, Elsevier, 2003.

GREGORY, Peter; SIMNO, Michael. (2008). *Biometrics for Dummies.* Wiley.

HOUSE, Anna Builds a. (s.d.). <http://annabuildsahouse.files.wordpress.com/2009/11/fingerprint-lock-2.jpg>.

JAIN, Anil; DUIN, Robert; MAO, Jianchang. (2000). *Statistical Pattern Recognition: A.* IEEE Transactions on Pattern Analysis and machine.

MAZI, Renan Corio. (2009). *Identificação Biométrica Através da Impressão Digital.* São José dos Campos: Instituto Tecnológico de.

Nicholas M. Orlans John D. Woodward Jr., Peter T. Higgins. (2022). *Biometrics.* McGraw Hill Professional, 2002.

Nogueira, F. R. (2011). *Captura de sinal biometrico utilizando arduino.* Assis: Fundacao educacional do municipio de Assis.

PEREIRA, Leonardo de Pádua Costa. (2003). *Mapeamento de Imagens Binárias: Um.* 57p. Monografia UNAMA: Universidade.

Ponte, G. (2008). Tecnologia digital para identificação de pessoas.

PRABHAKAR, Salil. (2001). *Fingerprint Classification and Matching Using a Filterbank.* Dissertação (Doutorado) Michigan State University, East Lansing,.

ZONE, Pro Security. (maio de 2022). Obtido de <http://www.prosecurityzone.com/Customisation/News/Images/3759-SignHear-7.jpg>.

21 https://www.ncbi.nlm.nih.gov/pmc/articles/PMC6667827

22 https://www.natosafe.com.br - acessado a 31 de janeiro de 2021

23 https://www.devmedia.com.br - acessado a 31 de janeiro de 2021

24 https://www.w3schools.com- acessado 17 de janeiro de 2022

Anexos

6.2.1.1 Anexo 1. Depoimento sobre casos em Moçambique

https://www.dw.com/pt-002/bebés-desaparecidos-e-violência-contra-mães-mobilizam-associações-em-moçambique/a-59486483 (caso da Lela em que não lhe fora mostrado o corpo do bebé) - acessado a 17 de marco de 2022

https://m.facebook.com/tvmiramar.mz/videos/fala-moçambique/1815465288633195/?refsrc=deprecated&locale2=ne_NP&_rdr (caso do bebé roubado e depois resgatado) - acessado a 17 de marco de 2022

https://verdade.co.mz/pessoal-de-saude-nao-e-culpada-do-roubo-de-bebes/ (opinião de Ivo Garrido no que diz respeito a um caso de desaparecimento de um bebé na unidade Hospitalar José Macamo)- acessado no dia 17 de marco de 2022

https://www.youtube.com/watch?v=RJhfRmVQ0kw (caso de roubo de bebé) - acessado no dia 17 de marco de 2022

https://www.usinainfo.com.br/blog/leitor-biometrico-arduino-sistema-de-cadastramento-e-leitura-de-digitais/ leitor de impressão com arduin

6.2.1.2 **Anexo 2. Código da plataforma**

```
import express, { NextFunction, Request, Response } from 'express';
import { resolve } from 'path';
import 'express-async-errors';

import './database';
import routes from './routes';

const app = express();
app.use('/views', express.static(resolve(__dirname, 'app', 'views')));
app.set('view engine', 'ejs');
app.set('views', resolve(__dirname, 'app', 'views'));

app.use(express.json());
app.use(routes);

app.listen(process.env.PORT || 3333, () =>
    console.log('Server running on 3333')
);


import { Router } from 'express';
import { childrenRoutes } from './children.routes';
import { mothersRoutes } from './mothers.routes';
import { pageRoutes } from './pages.routes';
import { searchRoutes } from './search.routes';
import { sessionRoutes } from './sessions.routes';
import { usersRoutes } from './users.routes';

const routes = Router();

routes.use('/sessions', sessionRoutes);
routes.use('/users', usersRoutes);
routes.use('/mothers', mothersRoutes);
routes.use('/children', childrenRoutes);
routes.use('/search', searchRoutes);
routes.use(pageRoutes);

export default routes;
import { Router } from 'express';
import childrenController from '../app/controllers/ChildrenController';
import authMiddleware from '../middlewares/auth';
const routes = Router();
```

```
routes.get('/', async (request, response) => {
    await childrenController().list(request, response);
});

routes.get('/:id', async (request, response) => {
    await childrenController().showById(request, response);
});

routes.use(authMiddleware);
routes.post('/', async (request, response) => {
    await childrenController().create(request, response);
});

export { routes as childrenRoutes };

import { Router } from 'express';
import motherController from '../app/controllers/MotherController';
import                        motherChildrenController                        from
'../app/controllers/MotherChildrenController';
import authMiddleware from '../middlewares/auth';

const routes = Router();

routes.get('/', async (request, response) => {
    await motherController().list(request, response);
});

routes.get('/:id', async (request, response) => {
    await motherController().showById(request, response);
});

routes.use(authMiddleware);
routes.post('/', async (request, response) => {
    await motherController().create(request, response);
});

routes.get('/:id/children', async (request, response) => {
    await motherChildrenController().list(request, response);
});

export { routes as mothersRoutes };
```

C

```
import { Request, Response } from 'express';
import { ChildrenRepository } from '../repositories/ChildrenRepository';
import { MothersRepository } from '../repositories/MothersRepository';
import { UsersRepository } from '../repositories/UsersRepository';

class ChildrenController {
    usersRepository: UsersRepository;
    mothersRepository: MothersRepository;
    childrenRepository: ChildrenRepository;
    constructor() {
        this.usersRepository = new UsersRepository();
        this.mothersRepository = new MothersRepository();
        this.childrenRepository = new ChildrenRepository();
    }
    async create(request: Request, response: Response): Promise<Response> {
        const {
            name,
            hospitalName,
            hospitalNumber,
            sex,
            fatherName,
            home,
            phone,
            motherId,
            birthday,
            birthtime
        } = request.body;

        const register = await this.usersRepository.findById(request.userId);
        const mother = await this.mothersRepository.findById(motherId);

        await this.childrenRepository.create({
            name,
            hospitalName,
            hospitalNumber,
            sex,
            fatherName,
            home,
            phone,
            mother,
            register,
            birthday,
            birthtime
        });
```

```
        return response.status(201).send();
    }

    async list(request: Request, response: Response): Promise<void> {
        const children = await this.childrenRepository.findAll();
        return response.render('pages/children', {
            title: 'Filhos',
            children
        });
    }

    async showById(request: Request, response: Response): Promise<void> {
        const { id } = request.params;

        const child = await this.childrenRepository.findById(Number(id));
        return response.render('pages/child-details', {
            title: 'Detalhes do filho',
            child
        });
    }
}

export default () => {
    const childrenController = new ChildrenController();

    return childrenController;
};

import { Request, Response } from 'express';
import { ChildrenRepository } from '../repositories/ChildrenRepository';
import { MothersRepository } from '../repositories/MothersRepository';

class MotherChildrenController {
    private mothersRepository: MothersRepository;
    private childrenRepository: ChildrenRepository;
    constructor() {
        this.mothersRepository = new MothersRepository();
        this.childrenRepository = new ChildrenRepository();
    }

    async list(request: Request, response: Response): Promise<Response> {
        const { id } = request.params;
        const children = await this.mothersRepository.findChildren(Number(id));
        return response.json(children);
    }
```

E

```
    async count(request: Request, response: Response) {
        const countChildren = await this.childrenRepository.count();
        const countMothers = await this.mothersRepository.count();
        return response.render('pages/home', {
            title: 'Home',
            countChildren,
            countMothers
        });
    }
}

export default () => {
    const motherChildrenController = new MotherChildrenController();
    return motherChildrenController;
};

import { Request, Response } from 'express';
import { AppError } from '../errors/AppError';
import { MothersRepository } from '../repositories/MothersRepository';

class MotherController {
    private mothersRepository: MothersRepository;

    constructor() {
        this.mothersRepository = new MothersRepository();
    }

    async create(request: Request, response: Response): Promise<Response> {
        const {
            bi,
            name,
            father,
            mother,
            birthday,
            maritalStatus,
            work,
            workplace,
            home,
            district,
            neighborhood,
            avenue,
            phone,
            referencePlace,
            referencePerson,
            referenceRelation,
```

```
        referencePhone
    } = request.body;
    const register = request.userId;

    const parsedBirthday = new Date(Date.parse(birthday));
    const today = new Date();

    const age = today.getFullYear() - parsedBirthday.getFullYear();
    if (age < 14) {
        throw new AppError('Invalid birthday');
    }

    const motherExists = await this.mothersRepository.findByBi(bi);
    if (motherExists) {
        throw new AppError('Mother already exists!');
    }

    await this.mothersRepository.create({
        register,
        bi,
        name,
        father,
        mother,
        birthday: parsedBirthday,
        maritalStatus,
        work,
        workplace,
        home,
        district,
        neighborhood,
        avenue,
        phone,
        referencePlace,
        referencePerson,
        referenceRelation,
        referencePhone
    });

    return response.status(201).send();
}

async list(request: Request, response: Response): Promise<void> {
    const mothers = await this.mothersRepository.findAll();

    return response.render('pages/mothers', {
```

```
            title: 'Mães',
            mothers
        });
    }

    async showById(request: Request, response: Response): Promise<void> {
        const { id } = request.params;
        const mother = await this.mothersRepository.findById(Number(id));
        return response.render('pages/mother-details', {
            mother,
            title: 'Detalhes da mãe'
        });
    }
}

export default () => {
    const motherController = new MotherController();
    return motherController;
}
```

6.2.1.3 Anexo 3. **Código de microcontrolador Esp86822**

```
#include <SPI.h>
#include <Wire.h>
#include <WiFiClient.h>
#include <ESP8266WiFi.h>
#include <SoftwareSerial.h>
#include <ESP8266HTTPClient.h>
#include <Adafruit_GFX.h>
#include <Adafruit_SSD1306.h>
#include <Adafruit_Fingerprint.h>

#define Finger_Rx 14 //D5
#define Finger_Tx 12 //D6
// Declaration for SSD1306 display connected using software I2C
#define SCREEN_WIDTH 128 // OLED display width, in pixels
#define SCREEN_HEIGHT 64 // OLED display height, in pixels
#define OLED_RESET     0 // Reset pin # (or -1 if sharing Arduíno reset pin)
Adafruit_SSD1306 display(SCREEN_WIDTH, SCREEN_HEIGHT, &Wire, OLED_RESET);

SoftwareSerial mySerial(Finger_Rx, Finger_Tx);
Adafruit_Fingerprint finger = Adafruit_Fingerprint(&mySerial);
//************************************************************************
/* Set these to your desired credentials. */
#ifndef STASSID
#define STASSID "CONTACTA DTICS"
#define STAPSK "80624172"
#endif

String postData ;
```

```
String link = "192.168.7.186:3333";
int FingerID = 0;
uint8_t id;
//************************Biometric Icons*********************************
#define Wifi_start_width 54
#define Wifi_start_height 49
const uint8_t PROGMEM Wifi_start_bits[] = {
};
#define Wifi_connected_width 63
#define Wifi_connected_height 49
const uint8_t PROGMEM Wifi_connected_bits[] = {
};
#define FinPr_start_width 64
#define FinPr_start_height 64
const uint8_t PROGMEM FinPr_start_bits[] = {};
//-----------------------------------------------------------------
#define FinPr_valid_width 64
#define FinPr_valid_height 64
const uint8_t PROGMEM FinPr_valid_bits[] = {};
//-----------------------------------------------------------------
#define FinPr_invalid_width 64
#define FinPr_invalid_height 64
const uint8_t PROGMEM FinPr_invalid_bits[] = {};
//-----------------------------------------------------------------
#define FinPr_failed_width 64
#define FinPr_failed_height 64
const uint8_t PROGMEM FinPr_failed_bits[] = {};
//-----------------------------------------------------------------
#define FinPr_scan_width 64
```

```
#define FinPr_scan_height 64

const uint8_t PROGMEM FinPr_scan_bits[] = {};

//**************************************************************************

void setup() {

  Serial.begin(115200);

  if (!display.begin(SSD1306_SWITCHCAPVCC, 0x3C)) {

    Serial.println(F("Falha no Display SSD1306"));

    for (;;);

  }

  display.display();

  delay(2000);

  display.clearDisplay();

  Serial.print("Ligando a rede: ");

  Serial.println(STASSID);

  WiFi.begin(STASSID, STAPSK);

  finger.begin(57600);

  Serial.println("\n\nTeste do Sensor Biométrico");

  if (finger.verifyPassword()) {

    Serial.println("Sensor Biométrico encontrado!");

    display.clearDisplay();

    display.drawBitmap(    34,    0,    FinPr_valid_bits,    FinPr_valid_width,
FinPr_valid_height, WHITE);

    display.display();

  } else {

    Serial.println("Sensor Biométrico encontrado :(");

    display.clearDisplay();

    display.drawBitmap(    32,    0,    FinPr_failed_bits,    FinPr_failed_width,
FinPr_failed_height, WHITE);

    display.display();

    while (1) {
```

```
      delay(1);
    }
  }
  finger.getTemplateCount();
  Serial.print("Sensor contains ");
  Serial.print(finger.templateCount);
  Serial.println(" templates");
  Serial.println("Waiting for valid finger...");
}
void loop() {
  if (WiFi.status() != WL_CONNECTED) {
    Serial.print("Ligando a rede: ");
    Serial.println(STASSID);
    WiFi.begin(STASSID, STAPSK);
  }
  FingerID = pesquisarImpressao();
  delay(50);
  DisplayFingerprintID();
  ChecktoAddID();
}
void DisplayFingerprintID() {
  if (FingerID > 0) {
    display.clearDisplay();
    display.drawBitmap(    34,    0,    FinPr_valid_bits,    FinPr_valid_width,
FinPr_valid_height, WHITE);
    display.display();
    enviarPesquisa( FingerID );
  }
  else if (FingerID == 0) {
```

```
    display.clearDisplay();

    display.drawBitmap(     32,     0,     FinPr_start_bits,     FinPr_start_width,
FinPr_start_height, WHITE);

    display.display();

  }

  else if (FingerID == -1) {

    display.clearDisplay();

    display.drawBitmap(    34,    0,    FinPr_invalid_bits,    FinPr_invalid_width,
FinPr_invalid_height, WHITE);

    display.display();

  }

  else if (FingerID == -2) {

    display.clearDisplay();

    display.drawBitmap(    32,    0,    FinPr_failed_bits,    FinPr_failed_width,
FinPr_failed_height, WHITE);

    display.display();

  }

}

void enviarPesquisa( int finger ) {

  WiFiClient client;

  HTTPClient http;

  postData ="http://192.168.7.186:3333/fingers/search/";

  http.begin(client, postData);

  http.addHeader("Content-Type", "application/json");

  int httpCode = http.POST({String(finger)});

  String payload = http.getString();


  Serial.println(httpCode);

  Serial.println(payload);

  Serial.println(postData);
```

```
  Serial.println(finger);
  http.end();
}
int pesquisarImpressao() {
  uint8_t p = finger.getImage();
  switch (p) {
    case FINGERPRINT_OK:
      Serial.println("Image taken");
      break;
    case FINGERPRINT_NOFINGER:
      Serial.println("No finger detected");
      return 0;
    case FINGERPRINT_PACKETRECIEVEERR:
      Serial.println("Communication error");
      return -2;
    case FINGERPRINT_IMAGEFAIL:
      Serial.println("Imaging error");
      return -2;
    default:
      Serial.println("Unknown error");
      return -2;
  }
  // OK success!
  p = finger.image2Tz();
  switch (p) {
    case FINGERPRINT_OK:
      Serial.println("Image converted");
      break;
    case FINGERPRINT_IMAGEMESS:
```

```
    Serial.println("Image too messy");
    return -1;
  case FINGERPRINT_PACKETRECIEVEERR:
    Serial.println("Communication error");
    return -2;
  case FINGERPRINT_FEATUREFAIL:
    Serial.println("Could not find fingerprint features");
    return -2;
  case FINGERPRINT_INVALIDIMAGE:
    Serial.println("Could not find fingerprint features");
    return -2;
  default:
    Serial.println("Unknown error");
    return -2;
}
// OK converted!
p = finger.fingerFastSearch();
if (p == FINGERPRINT_OK) {
  Serial.println("Found a print match!");
} else if (p == FINGERPRINT_PACKETRECIEVEERR) {
  Serial.println("Communication error");
  return -2;
} else if (p == FINGERPRINT_NOTFOUND) {
  Serial.println("Did not find a match");
  return -1;
} else {
  Serial.println("Unknown error");
  return -2;
}
```

O

```
  // found a match!
  Serial.print("Found ID #");
  Serial.print(finger.fingerID);
  Serial.print(" with confidence of ");
  Serial.println(finger.confidence);

  return finger.fingerID;
}
void ChecktoAddID() {
  //  if ((WiFi.status() == WL_CONNECTED)) {
  WiFiClient client;
  HTTPClient http;

  if (http.begin(client, "http://192.168.7.186:3333/fingers/save/last")) {
    int httpCode = http.GET();
    if (httpCode > 0) {
      Serial.printf("[HTTP] GET... code: %d\n", httpCode);
      if (httpCode == HTTP_CODE_OK || httpCode == HTTP_CODE_MOVED_PERMANENTLY) {
        String payload = http.getString();
        Serial.println(payload);
        if (payload.substring(0, 6) == "add-id") {
          String add_id = payload.substring(6);
          Serial.println(add_id);
          id = add_id.toInt();
          getFingerprintEnroll();
        }
        else {
          Serial.printf("[HTTP]      GET...      failed,      error:      %s\n",
http.errorToString(httpCode).c_str());
```

```
        }
      }
    }
    http.end();
  }
  else {
    Serial.printf("[HTTP} Unable to connect\n");
  }
}
uint8_t getFingerprintEnroll() {
  int p = -1;
  display.clearDisplay();
  display.drawBitmap(     34,     0,     FinPr_scan_bits,     FinPr_scan_width,
FinPr_scan_height, WHITE);
  display.display();
  while (p != FINGERPRINT_OK) {
    p = finger.getImage();
    switch (p) {
      case FINGERPRINT_OK:
        Serial.println("Image taken");
        display.clearDisplay();
        display.drawBitmap(   34,   0,   FinPr_valid_bits,   FinPr_valid_width,
FinPr_valid_height, WHITE);
        display.display();
        break;
      case FINGERPRINT_NOFINGER:
        Serial.println(".");
        display.setTextSize(1);             // Normal 2:2 pixel scale
        display.setTextColor(WHITE);        // Draw white text
        display.setCursor(0, 0);            // Start at top-left corner
```

Q

```
        display.print(F("scanning"));
        display.display();
        break;
      case FINGERPRINT_PACKETRECIEVEERR:
        display.clearDisplay();
        display.drawBitmap(  34,  0,  FinPr_invalid_bits,  FinPr_invalid_width,
FinPr_invalid_height, WHITE);
        display.display();
        break;
      case FINGERPRINT_IMAGEFAIL:
        Serial.println("Imaging error");
        break;
      default:
        Serial.println("Unknown error");
        break;
    }
  }

  p = finger.image2Tz(1);
  switch (p) {
    case FINGERPRINT_OK:
      display.clearDisplay();
      display.drawBitmap(   34,   0,   FinPr_valid_bits,   FinPr_valid_width,
FinPr_valid_height, WHITE);
      display.display();
      break;
    case FINGERPRINT_IMAGEMESS:
      display.clearDisplay();
      display.drawBitmap(  34,  0,  FinPr_invalid_bits,  FinPr_invalid_width,
FinPr_invalid_height, WHITE);
```

```
    display.display();
    return p;
  case FINGERPRINT_PACKETRECIEVEERR:
    Serial.println("Communication error");
    return p;
  case FINGERPRINT_FEATUREFAIL:
    Serial.println("Could not find fingerprint features");
    return p;
  case FINGERPRINT_INVALIDIMAGE:
    Serial.println("Could not find fingerprint features");
    return p;
  default:
    Serial.println("Unknown error");
    return p;
}
display.clearDisplay();
display.setTextSize(2);
display.setTextColor(WHITE);
display.setCursor(0, 0);
display.print(F("Retire"));
display.setCursor(0, 20);
display.print(F("O dedo"));
display.display();
Serial.println("Remova o dedo");
delay(2000);
p = 0;
while (p != FINGERPRINT_NOFINGER) {
  p = finger.getImage();
}
```

```
  Serial.print("ID ");
  Serial.println(id);
  p = -1;
  display.clearDisplay();
  display.drawBitmap(     34,     0,     FinPr_scan_bits,     FinPr_scan_width,
FinPr_scan_height, WHITE);
  display.display();
  while (p != FINGERPRINT_OK) {
    p = finger.getImage();
    switch (p) {
      case FINGERPRINT_OK:
        Serial.println("Image taken");
        display.clearDisplay();
        display.drawBitmap(   34,   0,   FinPr_valid_bits,   FinPr_valid_width,
FinPr_valid_height, WHITE);
        display.display();
        break;
      case FINGERPRINT_NOFINGER:
        Serial.println(".");
        display.setTextSize(1);
        display.setTextColor(WHITE);
        display.setCursor(0, 0);
        display.print(F("scanning"));
        display.display();
        break;
      case FINGERPRINT_PACKETRECIEVEERR:
        Serial.println("Communication error");
        break;
      case FINGERPRINT_IMAGEFAIL:
        Serial.println("Imaging error");
```

```
      break;
    default:
      Serial.println("Unknown error");
      break;
  }
 }
 p = finger.image2Tz(2);
 switch (p) {
  case FINGERPRINT_OK:
    Serial.println("Image converted");
    display.clearDisplay();
    display.drawBitmap(    34,    0,    FinPr_valid_bits,    FinPr_valid_width,
FinPr_valid_height, WHITE);
    display.display();
    break;
  case FINGERPRINT_IMAGEMESS:
    Serial.println("Image too messy");
    return p;
  case FINGERPRINT_PACKETRECIEVEERR:
    Serial.println("Communication error");
    return p;
  case FINGERPRINT_FEATUREFAIL:
    Serial.println("Could not find fingerprint features");
    return p;
  case FINGERPRINT_INVALIDIMAGE:
    Serial.println("Could not find fingerprint features");
    return p;
  default:
    Serial.println("Unknown error");
```

```
      return p;
  }
  // OK converted!
  Serial.print("Creating model for #");
  Serial.println(id);

  p = finger.createModel();
  if (p == FINGERPRINT_OK) {
    Serial.println("Prints matched!");
    display.clearDisplay();
    display.drawBitmap(    34,    0,    FinPr_valid_bits,    FinPr_valid_width,
FinPr_valid_height, WHITE);
    display.display();
  } else if (p == FINGERPRINT_PACKETRECIEVEERR) {
    Serial.println("Communication error");
    return p;
  } else if (p == FINGERPRINT_ENROLLMISMATCH) {
    Serial.println("Fingerprints did not match");
    return p;
  } else {
    Serial.println("Unknown error");
    return p;
  }
  Serial.print("ID ");
  Serial.println(id);
  p = finger.storeModel(id);
  if (p == FINGERPRINT_OK) {
    Serial.println("Stored!");
    display.clearDisplay();
```

```
    display.drawBitmap(     34,     0,     FinPr_valid_bits,     FinPr_valid_width,
FinPr_valid_height, WHITE);
    display.display();
  } else if (p == FINGERPRINT_PACKETRECIEVEERR) {
    Serial.println("Communication error");
    return p;
  } else if (p == FINGERPRINT_BADLOCATION) {
    Serial.println("Could not store in that location");
    return p;
  } else if (p == FINGERPRINT_FLASHERR) {
    Serial.println("Error writing to flash");
    return p;
  } else {
    Serial.println("Unknown error");
    return p;
  }
}
void ligarWiFi() {
  Serial.print("Ligando a rede: ");
  Serial.println(STASSID);
  WiFi.begin(STASSID, STAPSK);

  display.clearDisplay();
  display.setTextSize(1);
  display.setTextColor(WHITE);
  display.setCursor(0, 0);
  display.print(F("Ligando a rede: \n"));
  display.setCursor(0, 50);
  display.setTextSize(2);
```

```
  display.print(STASSID);

  display.drawBitmap(     73,     10,     Wifi_start_bits,     Wifi_start_width,
Wifi_start_height, WHITE);

  display.display();


  while (WiFi.status() != WL_CONNECTED) {

    delay(500);

    Serial.print(".");

  }

  Serial.println("");

  Serial.println("Ligado");

  display.clearDisplay();

  display.setTextSize(2);

  display.setTextColor(WHITE);

  display.setCursor(8, 0);

  display.print(F("Ligado \n"));

  display.drawBitmap(   33,   15,   Wifi_connected_bits,   Wifi_connected_width,
Wifi_connected_height, WHITE);

  display.display();

  Serial.print("Endereco IP: ");

  Serial.println(WiFi.localIP());

}
```

6.2.1.4 Anexo 4: Datasheet do Oled

OLED SPECIFICATION

Model No:

REX012864DWPP3N00F00

1.General Specification

The Features is described as follow:

- Module dimension: 26.7 × 19.26 × 1.26 mm
- Active area: 21.738 × 10.858mm
- Dot Matrix: 128 × 64
- Dot size: 0.148 × 0.148 mm
- Dot pitch: 0.17 × 0.17mm
- Display Mode：Passive Matrix
- Duty: 1/64 Duty
- Display Color: OLED , White
- Interface: 6800,8080,SPI,I2C
- Controller IC: SSD1306BZ
- SIZE: 0.96 inch

Interface Pin Function

<table>
<tr><th>No.</th><th>Symbol</th><th>Function</th></tr>
<tr><td>1</td><td>N.C.
(GND)</td><td>Reserved Pin (Supporting Pin)
The supporting pins can reduce the influences from stresses on the function pins. These pins must be connected to external ground.</td></tr>
<tr><td>2</td><td>C2N</td><td rowspan="4">Positive Terminal of the Flying Inverting Capacitor Negative Terminal of the Flying Boost Capacitor The charge-pump capacitors are required between the terminals. They must be floated when the converter is not used.</td></tr>
<tr><td>3</td><td>C2P</td></tr>
<tr><td>4</td><td>C1P</td></tr>
<tr><td>5</td><td>C1N</td></tr>
<tr><td>6</td><td>VBAT</td><td>Power Supply for DC/DC Converter Circuit
This is the power supply pin for the internal buffer of the DC/DC voltage converter. It must be connected to external source when the converter is used. It should be connected to VDD when the converter is not used.</td></tr>
<tr><td>7</td><td>NC</td><td>NC</td></tr>
<tr><td>8</td><td>VSS</td><td>Ground of Logic Circuit
This is a ground pin. It acts as a reference for the logic pins. It must be connected to external ground.</td></tr>
<tr><td>9</td><td>VDD</td><td>Power Supply for Logic
This is a voltage supply pin. It must be connected to external source.</td></tr>
<tr><td>10</td><td>BS0</td><td rowspan="3">Communicating Protocol Select
These pins are MCU interface selection input. See the following table:
<table>
<tr><th></th><th>BS0</th><th>BS1</th><th>BS2</th></tr>
<tr><td>I2C</td><td>0</td><td>1</td><td>0</td></tr>
<tr><td>3-wire SPI</td><td>1</td><td>0</td><td>0</td></tr>
<tr><td>4-wire SPI</td><td>0</td><td>0</td><td>0</td></tr>
<tr><td>8-bit 68XX Parallel</td><td>0</td><td>0</td><td>1</td></tr>
<tr><td>8-bit 80XX Parallel</td><td>0</td><td>1</td><td>1</td></tr>
</table></td></tr>
<tr><td>11</td><td>BS1</td></tr>
<tr><td>12</td><td>BS2</td></tr>
<tr><td>13</td><td>CS#</td><td>Chip Select
This pin is the chip select input. The chip is enabled for MCU communication only when CS# is pulled low.</td></tr>
<tr><td>14</td><td>RES#</td><td>Power Reset for Controller and Driver
This pin is reset signal input. When the pin is low, initialization of the chip is executed.</td></tr>
<tr><td>15</td><td>D/C#</td><td>Data/Command Control
This pin is Data/Command control pin. When the pin is pulled high, the input at D7~D0 is treated as display data.
When the pin is pulled low, the input at D7~D0 will be transferred to the command register. For detail relationship to MCU interface signals, please refer to the Timing Characteristics Diagrams.
When the pin is pulled high and serial interface mode is selected, the data at SDIN is treated as data. When it is pulled low, the data at SDIN will be transferred to the command register. In I2C mode, this pin acts as SA0 for slave address selection.</td></tr>
</table>

Z

6.2.1.5 Anexo 5: Datasheet do Esp86822

Pin	Name	Type	Function
4	VDD3P3	P	Amplifier Power 2.5 V – 3.6 V
5	VDD_RTC	P	NC (1.1 V)
6	TOUT	I	ADC pin. It can be used to test the power-supply voltage of VDD3P3 (Pin3 and Pin4) and the input power voltage of TOUT (Pin 6). However, these two functions cannot be used simultaneously.
7	CHIP_EN	I	Chip Enable High: On, chip works properly Low: Off, small current consumed
8	XPD_DCDC	I/O	Deep-sleep wakeup (need to be connected to EXT_RSTB); GPIO16
9	MTMS	I/O	GPIO 14; HSPI_CLK
10	MTDI	I/O	GPIO 12; HSPI_MISO
11	VDDPST	P	Digital/IO Power Supply (1.8 V – 3.6 V)
12	MTCK	I/O	GPIO 13; HSPI_MOSI; UART0_CTS
13	MTDO	I/O	GPIO 15; HSPI_CS; UART0_RTS
14	GPIO2	I/O	UART TX during flash programming; GPIO2
15	GPIO0	I/O	GPIO0; SPI_CS2
16	GPIO4	I/O	GPIO4
17	VDDPST	P	Digital/IO Power Supply (1.8 V – 3.6 V)
18	SDIO_DATA_2	I/O	Connect to SD_D2 (Series R: 20 Ω); SPIHD; HSPIHD; GPIO9
19	SDIO_DATA_3	I/O	Connect to SD_D3 (Series R: 200 Ω); SPIWP; HSPIWP; GPIO10
20	SDIO_CMD	I/O	Connect to SD_CMD (Series R: 200 Ω); SPI_CS0; GPIO11
21	SDIO_CLK	I/O	Connect to SD_CLK (Series R: 200 Ω); SPI_CLK; GPIO6
22	SDIO_DATA_0	I/O	Connect to SD_D0 (Series R: 200 Ω); SPI_MISO; GPIO7
23	SDIO_DATA_1	I/O	Connect to SD_D1 (Series R: 200 Ω); SPI_MOSI; GPIO8
24	GPIO5	I/O	GPIO5
25	U0RXD	I/O	UART Rx during flash programming; GPIO3
26	U0TXD	I/O	UART TX during flash programming; GPIO1; SPI_CS1
27	XTAL_OUT	I/O	Connect to crystal oscillator output, can be used to provide BT clock input
28	XTAL_IN	I/O	Connect to crystal oscillator input
29	VDDD	P	Analog Power 2.5 V – 3.6 V
30	VDDA	P	Analog Power 2.5 V – 3.6 V

Pin	Name	Type	Function
31	RES12K	I	Serial connection with a 12 kΩ resistor and connect to the ground
32	EXT_RSTB	I	External reset signal (Low voltage level: active)

📖 ***Note:***

1. *GPIO2, GPIO0, and MTDO are used to select booting mode and the SDIO mode;*
2. *U0TXD should not be pulled externally to a low logic level during the powering-up.*

6.2.1.6 Anexo 6: Datasheet FingerPrint Display GT511C3

Technical Specification

Item	Value
CPU	ARM Cortex M3 Core
Sensor	optical Sensor
Effective area of the Sensor	14 x 12.5(mm)
Image Size	202 x 258 Pixels
Resolution	450 dpi
The maximum number of fingerprints	200 fingerprints
Matching Mode	1:1, 1:N
The size of template	496 Bytes (template) + 2 Bytes (checksum)
Communication interface	UART, default baud rate = 9600bps after power on USB Ver1.1, Full speed
False Acceptance Rate (FAR)	< 0.001%
False Rejection Rate(FRR)	< 0.1%
Enrollment time	< 3 sec (3 fingerprints)
Identification time	< 1.0 sec (200 fingerprints)
Operating voltage	DC 3.3~6V
Operating current	< 130mA

Operating environment	Temperature	-20℃ ~ +60℃
	Humidity	20% ~ 80%
Storage environment	Temperature	-20℃ ~ +60℃
	Humidity	10% ~ 80%

BB

6.2.1.7 Anexo 7: Fotografias dos componentes

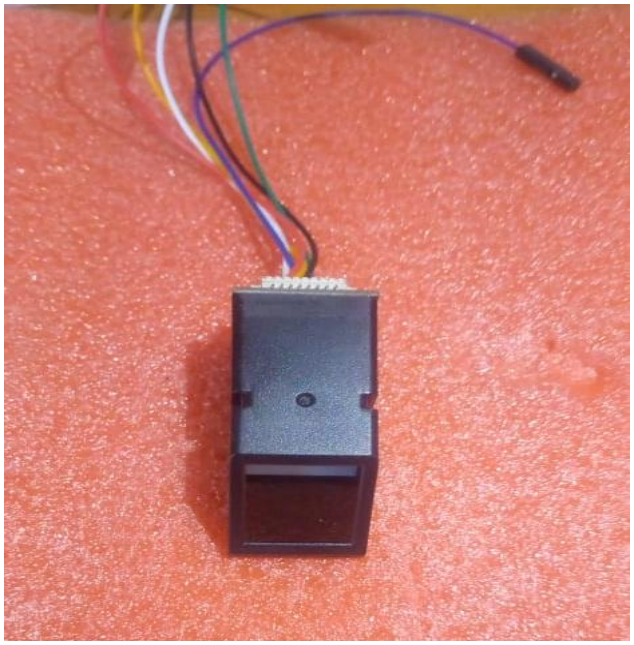

Figura 32: FingerPrint display GT511C3 (Fonte: o autor)

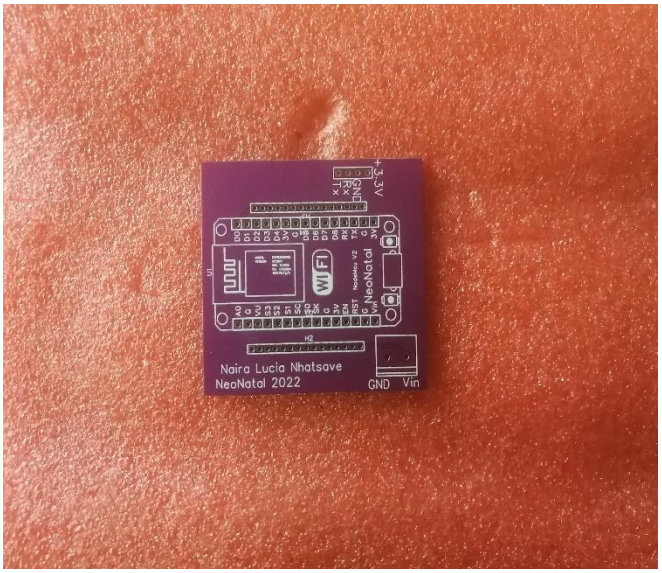

Figura 33: Placa do circuito impresso desenhado no easyeda **(**Fonte: o autor)

CC

Figura 34: Esp8286**(**Fonte: o autor)

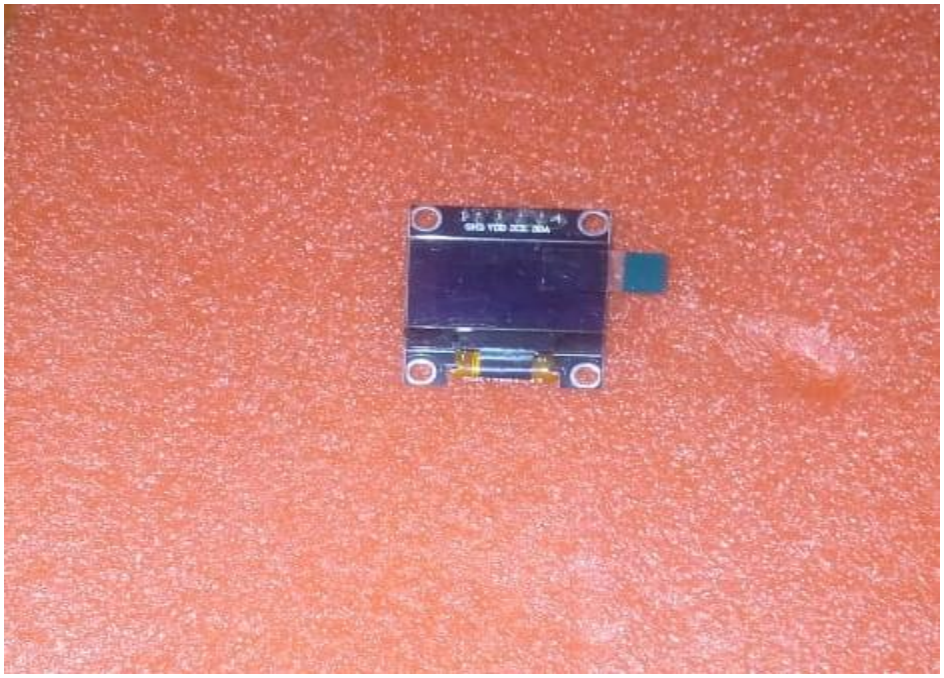

Figura 35: Oled Display **(**Fonte: o autor)

DD

Figura 36: Soldadura e Montagem do dispositivo(Fonte: o autor)

Figura 37: bebe sendo registado em um scanner biométrico (fonte: https://natosafe.com.br)