 **INSTITUTO POLITÉCNICO DE BEJA **

**Escola Superior de Tecnologia e Gestão**

**Mestrado em Engenharia de Segurança Informática**

**Tecnologias Biométricas –**

**Implementação de um Sistema Biométrico**

Luís Miguel Berenguer, 23695

Pedro Pita, 19933

Tomás Ferreira, 19934

2024

**INSTITUTO POLITÉCNICO DE BEJA**

**Escola Superior de Tecnologia e Gestão**

**Mestrado em Engenharia de Segurança Informática**

**Tecnologias Biométricas –**

**Implementação de um Sistema Biométrico**

Elaborado por:

Luís Miguel Berenguer, 23695

Pedro Pita, 19933

Tomás Ferreira, 19934

Orientado por:

Pedro Moreira

Relatório de projeto de Tecnologias Biométricas apresentado na

Escola Superior de Tecnologia e Gestão do Instituto Politécnico de Beja

2024

Índice

[1. Introdução 3](#_Toc155464964)

[2. Implementação de um Sistema Biométrico 4](#_Toc155464965)

[2.1. Explicação Procedimento Experimental 4](#_Toc155464966)

[2.2. Segurança 6](#_Toc155464967)

[2.3. Eficiência 11](#_Toc155464968)

[2.4. Eficácia 14](#_Toc155464969)

[2.5. Privacidade 16](#_Toc155464970)

[3. Conclusão 17](#_Toc155464971)

**Lista de Figuras**

Figura 2‑1 - Estrutura BD 4

Figura 2‑2 - Exemplo execução sistema autenticação 5

Figura 2‑3 - encryption\_module: Cifragem de ficheiro 6

Figura 2‑4 - encryption\_module: Decifragem de ficheiro 6

Figura 2‑5 - Cifragem da pasta dos ficheiros de impressões digitais 7

Figura 2‑6 - Resultado cifragem das imagens das impressões digitais 7

Figura 2‑7 - Criação de utilizadores e cifragem da impressão digital 8

Figura 2‑8 - Criação de ficheiros temporários seguros 8

Figura 2‑9 - Eliminação do ficheiro temporário 8

Figura 2‑10 - Incrementa o número de tentativas falhadas e o tempo bloqueado 9

Figura 2‑11 - Verifica se o utilizador existe ou está bloqueado 9

Figura 2‑12 - Exemplo utilizador bloqueado 9

Figura 2‑13 - Execução de comandos BD e armazenamento de log 10

Figura 2‑14 - Obtenção de todos os logs 10

Figura 2‑15 - Logs BD 10

Figura 2‑16 - Reconhecimento Impressão digital (Não otimizado) 11

Figura 2‑17 - Extração de minúcias de Impressões digitais (Original) 11

Figura 2‑18 - Comparação Impressões digitais (Original) 12

Figura 2‑19 - Extração de minúcias de Impressões digitais (Otimizado) 12

Figura 2‑20 - Comparação Impressões digitais (Otimizado) 12

Figura 2‑21 - Reconhecimento Impressão digital (Otimizado) 13

Figura 2‑22 - Distância de Euclides 14

Figura 2‑23 - Definição do threshold 14

Figura 2‑24 - Comparação das impressões digitais com a distância de euclides 14

Figura 2‑25 - Validação da comparação das impressões digitais 14

Figura 2‑26 - Eficácia sistema autenticação 15

Figura 2‑27 - Execução sistema autenticação 15

# Introdução

No âmbito da disciplina de Tecnologias Biométricas, foi nos proposto a realização de um projeto focado na "Implementação de um Sistema Biométrico". Este projeto visa explorar aplicações práticas de tecnologias biométricas, abordando aspetos cruciais como eficácia, eficiência, segurança e privacidade.

Com isso em vista, decidimos, a partir do código desenvolvido em aula, focarmo-nos na impressão digital analisando e melhorando a eficiência será analisada em termos de tempo de resposta e utilização de recursos do sistema, para além de verificarmos a sua eficácia quanto à sua capacidade de identificar e autenticar indivíduos. A segurança será reforçada com medidas para proteger os dados biométricos, através da implementação de criptografia, e a privacidade será garantida através da adoção de práticas específicas.

# Implementação de um Sistema Biométrico

Para este projeto, concentrámo-nos na análise e otimização do código referente à tecnologia biométrica de impressão digital, desenvolvido durante as aulas.

Nosso objetivo principal foi aprimorar a eficácia do sistema, assegurando uma identificação precisa e eficiente dos utilizadores. A revisão do código incluiu também medidas para reforçar a segurança dos dados biométricos, bem como a implementação de práticas que respeitam a privacidade dos indivíduos envolvidos.

## Explicação Procedimento Experimental

Para conseguirmos obter uma evolução notória deste projeto, realizamos procedimento experimental por fases, em que desenvolvemos exemplos com cada implementação de melhoria do trabalho, a fim de podermos fazer comparações. O procedimento passou da seguinte forma:

1. Cifragem das imagens Biométricas
2. Otimização da performance na comparação das impressões digitais
3. Implementação de sistema de base de dados, e na identificação de utilizadores

O seguinte código representa o esquema da base de dados criada, que providencia uma tabela para armazenar os utilizadores do sistema, uma tabela que se liga com os utilizadores, que armazena todas as impressões digitais de cada utilizador, e por fim uma tabela que guarda os logs do sistema para garantir maior segurança e privacidade nas operações realizadas na BD.

A computer screen shot of a computer code

Description automatically generated

Figura ‑ - Estrutura BD

1. Implementação de sistema de autenticação segura de utilizadores

Desenvolvemos um sistema de autenticação seguro, em que o utilizador necessita de inserir a sua sigla e a sua impressão digital, permitindo apenas o acesso às informações biométricas apenas ao utilizador, e caso a mesma esteja incorreta é incrementado o número de tentativas incorretas para aquele utilizador, e passado o limite de tentativas possíveis, o utilizador fica bloqueado durante (x tentativas / limite) minutos, impedidas tentativas de brute force, e só ao acesso da impressão digital do utilizador em específico.

A screen shot of a computer

Description automatically generated

Figura ‑ - Exemplo execução sistema autenticação

## Segurança

Como foco inicial, procedemos com a implementação de segurança nos dados biométricos para não puderem ser acedidos por utilizadores externos, com isso em vista, decidimos aplicar criptografia nos dados biométricos dos utilizadores, através da cifra de Fernet nas imagens das impressões digitais dos utilizadores. Esta escolha estratégica visa garantir a integridade e confidencialidade dos dados biométricos, assegurando uma camada adicional de proteção.

A cifra de Fernet, conhecida pela sua robustez e eficiência, revela-se uma opção ideal para criptografar as imagens das impressões digitais. Ao utilizar um algoritmo simétrico de chave secreta, proporciona uma segurança sólida, garantindo que apenas os utilizadores autorizados possam aceder e interpretar os dados biométricos. Esta medida não apenas impede acessos não autorizados, mas também eleva o nível de resistência do sistema a possíveis tentativas de ataques externos.

Criamos um módulo de cifragem e decifragem dos ficheiros, em que é só necessário o caminho do ficheiro (cifrado/decifrado) e a chave da cifra. A criação de módulos permite que as funções possam ser utilizadas em todos os ficheiros que as necessitassem.

A computer screen shot of a computer code

Description automatically generated

Figura ‑ - encryption\_module: Cifragem de ficheiro

A computer screen shot of a code

Description automatically generated

Figura ‑ - encryption\_module: Decifragem de ficheiro

Na primeira parte do projeto, usamos um sistema de armazenamento em ficheiros, em que a partir da pasta com as imagens das impressões digitais, gerávamos uma pasta com as impressões digitais cifradas.

A computer screen shot of text

Description automatically generated

Figura ‑ - Cifragem da pasta dos ficheiros de impressões digitais

A screenshot of a computer

Description automatically generatedA screenshot of a computer

Description automatically generated

Figura ‑ - Resultado cifragem das imagens das impressões digitais

Já na segunta fase, para armazenamento das impressções digitais na base de dados, guarda-mos os dados cifrados, e criamos os utilizaadores, de forma randomizada, por cada impressão digital, sendo que poderiamos ter que um utilizador pode ter mais que uma impressão digital pela forma como o sistema foi desenvolvido.

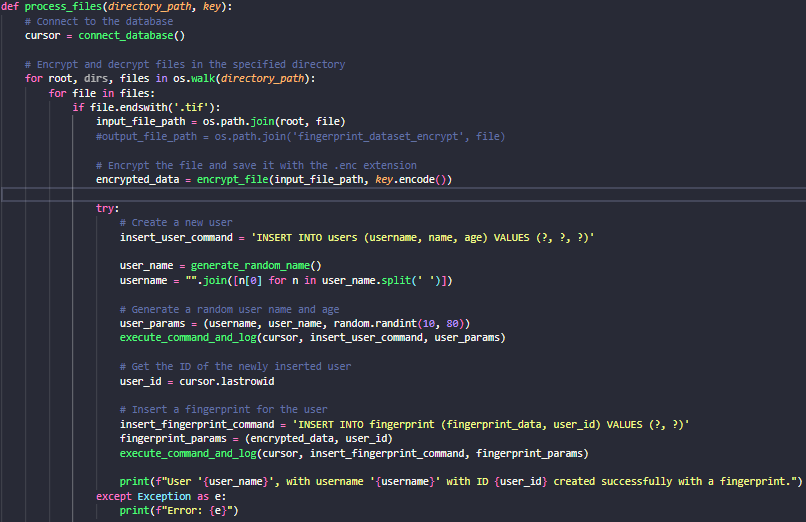


Figura ‑ - Criação de utilizadores e cifragem da impressão digital

Além da cifragem dos ficheiros, ao decifrar os ficheiros para serem analisados, utilizamos um sistema de ficheiros temporários seguros, para que mesmo que os ficheiros das impressões digitais decifrados sejam intercetados durante a execução do programa, estes não possam ser lidos.

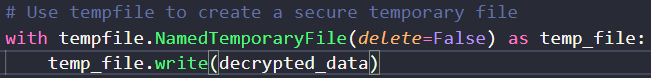


Figura ‑ - Criação de ficheiros temporários seguros

A close up of a text

Description automatically generated

Figura ‑ - Eliminação do ficheiro temporário

Também desenvolvemos um sistema de autenticação seguro, em que o utilizador necessita de inserir a sua sigla e a sua impressão digital, e caso a mesma esteja incorreta é incrementado o número de tentativas incorretas para aquele utilizador, e passado o limite de tentativas possíveis, o utilizador fica bloqueado durante (x tentativas / limite) minutos, impedidas tentativas de brute force, e só ao acesso da impressão digital do utilizador em específico.

A computer code on a black background

Description automatically generated

Figura ‑ - Incrementa o número de tentativas falhadas e o tempo bloqueado

A screenshot of a computer program

Description automatically generated

Figura ‑ - Verifica se o utilizador existe ou está bloqueado

A screen shot of a computer

Description automatically generated

Figura ‑ - Exemplo utilizador bloqueado

Por fim, o nosso sistema de base de dados oferece um sistema de logs dos comandos que nos permite verificar todas as operações que foram realizadas na BD, podendo assim visualizar que tipo de acessos foram realizados.

A computer screen with text and images

Description automatically generated

Figura ‑ - Execução de comandos BD e armazenamento de log

A screenshot of a computer program

Description automatically generated

Figura ‑ - Obtenção de todos os logs

A screen shot of a computer code

Description automatically generated

Figura ‑ - Logs BD

## Eficiência

Como segunda fase, procedemos com a análise do tempo de resposta do sistema e o consumo de recursos. O computador usado para testes, por ter cerca de 7 anos e ser mais antigo, conseguimos perceber a lentidão que um sistema não otimizado pode levar a processar as imagens, sendo o primeiro sistema desenvolvido o seguinte:

A screenshot of a computer

Description automatically generated

Figura ‑ - Reconhecimento Impressão digital (Não otimizado)

Com este print, conseguimos perceber que só para comparar uma impressão digital leva 118 segundos e consome imensos recursos do sistema. Após uma análise do código, percebemos que o problema se encontrava na extração de minúcias e na comparação das duas impressões digitais.

A computer screen shot of text

Description automatically generated

Figura ‑ - Extração de minúcias de Impressões digitais (Original)

A computer screen shot of code

Description automatically generated

Figura ‑ - Comparação Impressões digitais (Original)

Percebemos que poderíamos aproveitar a biblioteca do numpy para nos fornecer cálculos mais eficientes.

A computer screen shot of text

Description automatically generated

Figura ‑ - Extração de minúcias de Impressões digitais (Otimizado)

A computer screen shot of a program

Description automatically generated

Figura ‑ - Comparação Impressões digitais (Otimizado)

**A screenshot of a computer

Description automatically generated**

Figura ‑ - Reconhecimento Impressão digital (Otimizado)

Após a otimização realizada, notamos uma melhoria significativa de performance, sendo que levou apenas 3 segundos, para encontrar a mesma impressão digital, para além de uma diminuição do uso de recursos, como o CPU e a RAM.

## Eficácia

A distância de Euclides [3] é frequentemente utilizada para comparar eficazmente duas impressões digitais no contexto de sistemas biométricos. Essa métrica de distância é aplicada para avaliar a similaridade ou dissimilaridade entre duas características biométricas, como as representadas pelas imagens das impressões digitais.

Ao utilizar a distância de Euclides na comparação de impressões digitais, os vetores que representam as características biométricas são tratados como pontos no espaço tridimensional (ou multidimensional, dependendo da dimensionalidade dos dados). A distância euclidiana entre esses pontos é então calculada através da fórmula matemática:



Figura ‑ - Distância de Euclides

Quando aplicada a impressões digitais, os pontos no espaço representam as características específicas das impressões, como minúcias ou pontos singulares. Quanto menor a distância euclidiana entre os pontos, maior é a similaridade entre as impressões digitais. Caso a distância seja pequena o suficiente, as impressões podem ser consideradas como provenientes da mesma fonte, no caso o threshold mais seguro que analisamos foi 4, que garante uma eficácia maior na validação das impressões digitais.

A blue and white text

Description automatically generated

Figura ‑ - Definição do threshold

A screenshot of a computer

Description automatically generated

Figura ‑ - Comparação das impressões digitais com a distância de euclides

A screen shot of a computer program

Description automatically generated

Figura ‑ - Validação da comparação das impressões digitais

Relativamente ao sistema de autenticação, o sistema será mais eficaz pelo facto de que para além da impressão digital, o sistema terá que também identificar o utilizador que pretende aceder.

**A screenshot of a computer program

Description automatically generated**

Figura ‑ - Eficácia sistema autenticação

A screen shot of a computer

Description automatically generated

Figura ‑ - Execução sistema autenticação

## Privacidade

A fim de garantir a privacidade do sistema, utilizamos cifragem dos dados com a cifra de Fernet [4], o que permite que cada utilizador tenha a sua chave e só esse utilizador pode aceder à sua biometria, isto poderia ser implementado se o utilizador tivesse de colocar a sigla e a sua password, e depois para se autenticar teria que adicionar a sua impressão digital também.

Para este projeto, só identificamos com uma chave de Fernet do sistema, porém garantimos a privacidade já que o utilizador precisa da sigla correta para aceder à sua biometria e compará-la para se autenticar, além de sistema de logs e proteção contra ataques brute force, como abordado no Ponto 2.2.

# Conclusão

Em conclusão, a aplicação da distância de Euclides na comparação de impressões digitais representa uma abordagem eficaz e amplamente utilizada em sistemas biométricos. Ao tratar as características biométricas como pontos no espaço, essa métrica possibilita a avaliação da similaridade entre duas impressões digitais de forma quantitativa. A utilização dessa medida de distância contribui para a eficácia na identificação e autenticação de indivíduos, permitindo que sistemas biométricos determinem a proximidade ou distância entre as características específicas das impressões digitais.

No entanto, é crucial reconhecer que a escolha da métrica de distância, seja ela de Euclides ou outra, deve ser feita considerando a natureza e as características específicas do sistema em questão. Além disso, a implementação eficaz de medidas de segurança, como a cifra de Fernet mencionada anteriormente, é vital para garantir a proteção adequada dos dados biométricos. A combinação cuidadosa desses elementos contribui para o desenvolvimento de sistemas biométricos robustos, seguros e capazes de atender aos requisitos rigorosos de identificação e autenticação.

**Bibliografia**

[1] Moodle – Tecnologia Biométricas, 2023, Pedro Moreira, <https://cms.ipbeja.pt/course/view.php?id=2062>.

[2] Python, <https://www.python.org>.

[3] Euclidean Distance | Calculation, Formula & Examples, 2023, Study.com, <https://study.com/academy/lesson/euclidean-distance-calculation-formula-examples.html>.

[4] What is Fernet? Secure data encryption in Python, 2023, JOSH LAKE, <https://www.comparitech.com/blog/information-security/what-is-fernet/>.