Relatório Final trabalho Sistemas Distribuídos - “ColorTorra”

Grupo:

Bruno Henrique Firmino

Gabriel Furtado Teixeira

Lucas de Castro Nizio

Rhuan Campideli Borges

LAVRAS - MG

2025

Sumário

Introdução

O presente trabalho tem como objetivo a implementação de uma solução para um setor de pesquisas cafeeiras da Universidade Federal de Lavras (UFLA).

O governo federal estabeleceu diretrizes para a classificação de torras de café a partir da cor, de modo que tal categorização passasse a ser explícita nas embalagens de café. No entanto, percebeu-se uma certa dificuldade dos produtores em registrar corretamente a tonalidade da torra através de registros fotográficos, visto que, a depender dos dispositivos utilizados e da iluminação presente no ambiente, a fotografia capturada poderia apresentar coloração diferente da real.

Além disso, é importante uma precisa identificação da coloração da torra de café, pois cada classificação implica numa taxa de impostos diferente sobre os produtos embalados. Com isso, essa divergência nas colorações devido às distorções provocadas pelos dispositivos tornou-se um problema urgente dentro do setor de pesquisa, em busca de tal precisão.

A partir dessa problemática, portanto, o grupo procurou desenvolver uma aplicação com agentes inteligentes que recebem as fotografias das torras de café, registradas junto com uma paleta de cores para calibragem, e, a partir da identificação das cores de calibragem, aplicar a correção de cor sobre a que foi coletada da torra de café.

Dessa forma, construiu-se a aplicação denominada ColorTorra, que obtêm imagens fotográficas da torra de café disposta de maneira específica e efetua a calibragem e correção das cores. Assim, com as cores calibradas e corrigidas, a torra de café passa a ser devidamente classificada conforme as diretrizes governamentais.

Desenvolvimento

Relatório de Impacto à Proteção de Dados Pessoais (RIPD)

Para identificar e avaliar os riscos relacionados à proteção de dados pessoais na aplicação ColorTorra, utilizamos a modelagem de ameaças baseada na estrutura STRIDE (Spoofing, Tampering, Repudiation, Information Disclosure, Denial of Service, Elevation of Privilege), bem como a construção de diagramas de fluxo de dados. Essa abordagem permitiu mapear possíveis vulnerabilidades e ameaças associadas ao tratamento dos dados pessoais dos usuários.

Nossa aplicação não depende da autenticação de usuários, de modo que um risco de **Spoofing** direto pudesse ocorrer. No entanto, como se baseia em requisições HTTP para um servidor FastAPI, um invasor pode mandar requisições HTTP falsas ou simular comportamentos de funcionalidades/componentes internos da aplicação.

- Para mitigar esse tipo de ameaça, que, dentro do contexto, apresenta baixa probabilidade, seria importante utilizar requisições certificadas.

Ainda no contexto das requisições, pode haver ameaças do tipo **Tampering**, consistindo na alteração de imagens que são enviadas via HTTP, o que pode atrapalhar a eficácia na extração das cores, além do risco de manipulação das funcionalidades de correção de cor, que podem retornar dados incorretos.

- Um uso de requisições mais seguras, como HTTPS, pode proteger as interações entre cliente e servidor.

No que tange a ameaças do tipo **Repudiation**, é possível a ocorrência de uma dificuldade de rastrear as requisições e respostas do servidor, de modo que um usuário pode negar ter feito uma ação irregular.

- Isso pode ser mitigado com a implementação e registro de logs detalhados, a fim de que seja possível entender com detalhes os procedimentos que são tomados e acessados na aplicação.

Ameaças de **Information Disclosure** podem ocorrer no cenário em que metadados de imagens são vazados, o que pode revelar informações pessoais ou dos dispositivos que registraram as fotografias, além de divulgação dos algoritmos utilizados para correção de cor (o que, de fato, não chega a ser tão perigoso para o sistema).

- A implementação de criptografia nos dados pode mitigar o vazamento de dados, de modo que se tornem acessíveis e compreensíveis de forma não autorizada.

Ameaças do tipo **Denial of Service** podem ser bem comuns, pelo fato da aplicação ser uma aplicação web. É fato que a implementação realizada é executada localmente, mas em um contexto em que essa aplicação seja colocada em produção, aberta na web, ela pode sofrer tentativas de sobrecarregar o servidor.

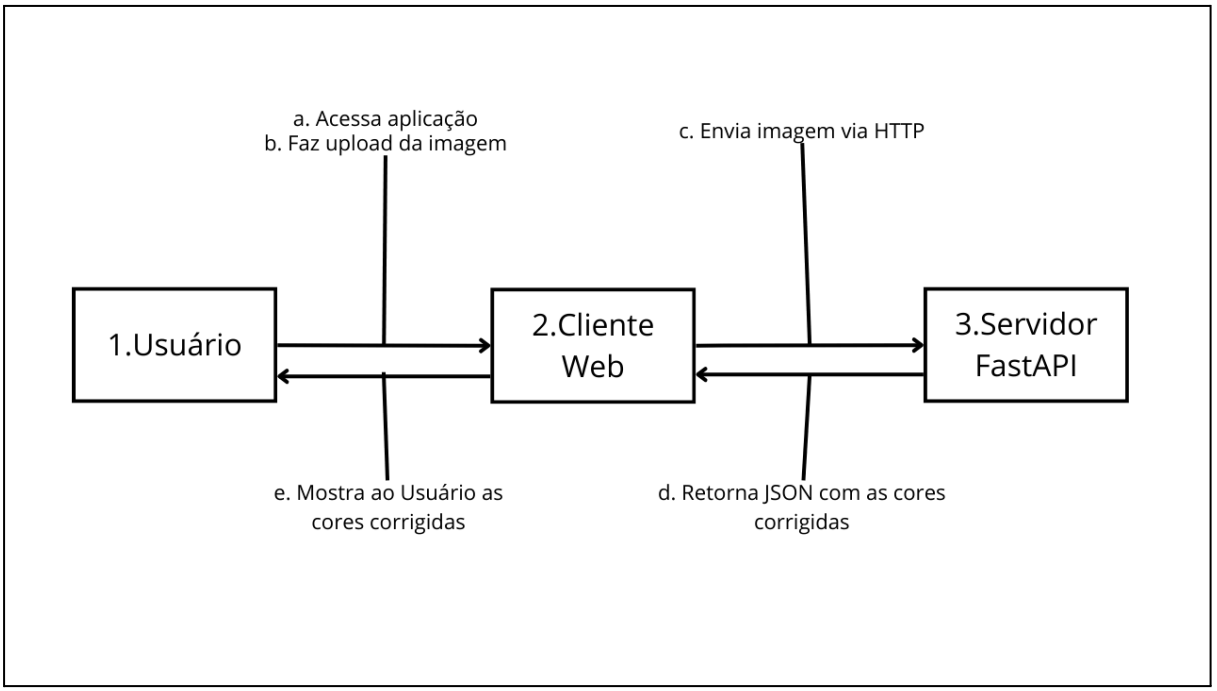
- Com isso, pode-se pensar em uma adoção de limite de uploads ou um monitoramento rigoroso do uso dos recursos computacionais do servidor, com a possibilidade de realizar balanceamento de carga.

Elevation of Privilege pode ocorrer com menor probabilidade, visto que a aplicação não apresenta funcionalidades tão restritas. Porém, se enquadraria como ameaças desse tipo tentativas de acessar áreas internas do sistema para explorar vulnerabilidades das bibliotecas e framework utilizados para compor a aplicação.

- Sendo assim, acredita-se que uma realização periódica de segurança da aplicação, além de manter as bibliotecas atualizadas, pode ajudar a manter o controle de acesso.

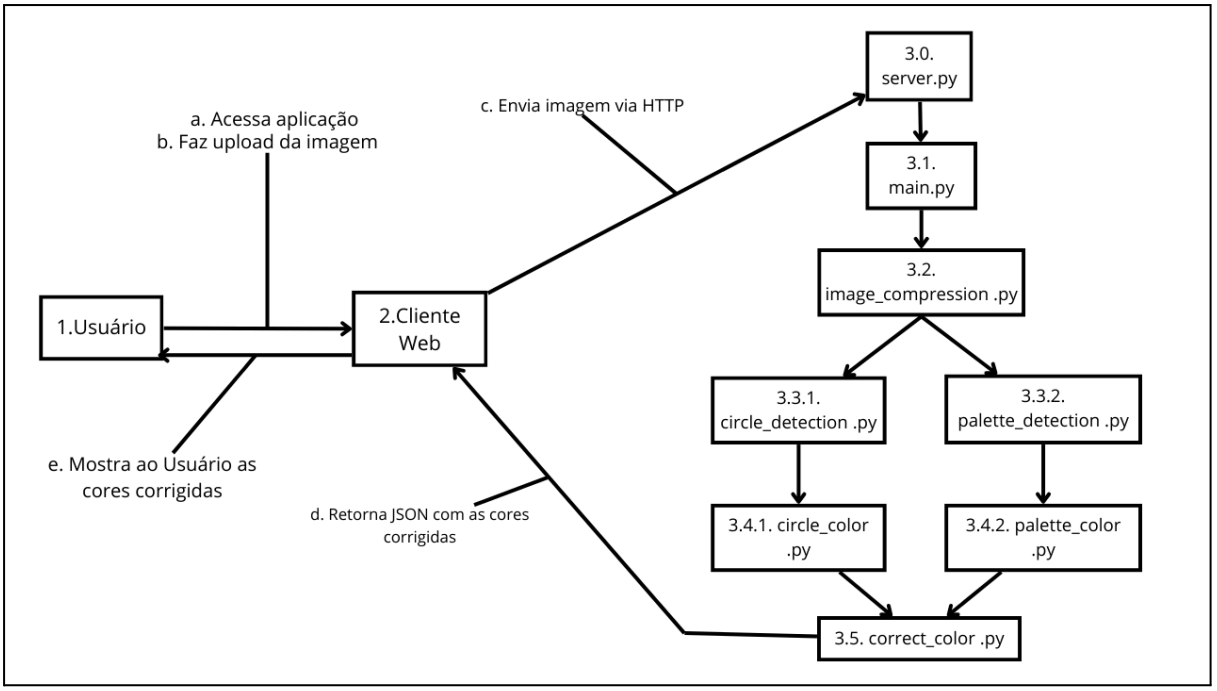
Diagramas de Fluxo de Dados (DFDs)

O fluxo de funcionamento da aplicação, bem como das possíveis ameaças a serem enfrentadas, podem ser melhor visualizados através dos Diagramas de Fluxo de Dados. A princípio, apresentamos um primeiro diagrama, mais geral:



Conforme explicado anteriormente, as requisições HTTP realizadas pelo cliente ao servidor FastAPI podem sofrer ameaças do tipo **Spoofing,** por meio de requisições falsas, e **Denial of Service,** por meio de uma tentativa de sobrecarregar o servidor.

Passando para um diagrama mais detalhado, principalmente dentro do contexto da aplicação, podemos observar mais detalhes:



Os componentes 3.3.1 e 3.3.2 constituem os modelos de agentes inteligentes, para a detecção do círculo e da paleta de cores nas imagens. Esses agentes podem sofrer ameaças do tipo **Tampering,** visto que as imagens recortadas podem vir alteradas, o que apresentaria inconsistências nos módulos subsequentes (3.4.1 e 3.4.2) que detectam as cores a partir das imagens recortadas.

- Em vista disso, é importante fazer a verificação periódica do funcionamento dos modelos e/ou a implementação de assinaturas de criptografia nas imagens para identificar as autênticas.

O componente 3.5 para correção de cor também pode sofrer **Tampering** e **Elevation of Privilege**, acessando e alterando os valores de rgb_target, provocando incoerências nas correções de cores.

De uma forma geral, os DFDs possibilitam a identificação dos pontos de interação entre processos e componentes, evidenciando onde os mecanismos de segurança devem ser aplicados para reduzir riscos. Assim, a modelagem de ameaças serve como base para o aprimoramento contínuo da segurança na aplicação e pode ser expandida conforme novas funcionalidades ou requisitos de segurança sejam identificados durante o desenvolvimento de novas versões da aplicação.

Implementação

No seguinte link, encontram-se reunidos os arquivos de implementação da ColorTorra:
https://github.com/GabrielFTgft/Correcao-de-Imagem-Sistemas-Distribuidos

Considerações finais

Em suma, a ColorTorra, a solução implementada neste trabalho, surgiu de uma demanda do setor cafeeiro para facilitar a classificação das torras de café, conforme novas diretrizes governamentais, a partir de fotografias registradas por produtores.

De fato, o simples registro fotográfico não permite, a olho nu, uma classificação correta da torra de café, visto que os dispositivos distorcem um pouco a luz do ambiente.

Com isso, o grupo buscou utilizar as fotografias das torras de café junto à paleta de cores para calibragem para fins de treinamento do modelo. Foi um processo trabalhoso e difícil a construção e implementação da solução, visto que exigiu uma aprendizagem ativa dos integrantes do grupo. Somado a isso, durante o processo de desenvolvimento, houve a ocorrência de muitas inconsistências a respeito da captura das cores na imagem, da correção da orientação das imagens, da captura da cor da torra de café (disposta em formato circular, ao invés de quadricular como da paleta de calibragem) e, principalmente, da eficaz correção das cores para os valores RGB reais.

Portanto, apesar da existência dos desafios, o grupo conseguiu construir uma primeira versão da solução, com pontos a serem melhorados, porém que já facilita bastante o trabalho dos produtores de café a se adequarem às diretrizes governamentais no que tange à correta classificação das torras de café nas embalagens dos produtos.