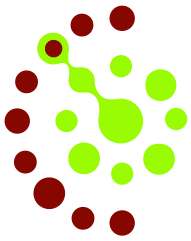

IPBeja

INSTITUTO POLITÉCNICO DE BEJA

Escola Superior de Tecnologia e Gestão

Mestrado em Engenharia de Segurança Informática

ABORDAGEM INOVADORA PARA A SEGURANÇA DA INFORMAÇÃO EM DOCUMENTOS IMPRESSOS

Pedro Miguel Clemente Dias Moreira

Beja, 14 de Fevereiro de 2022

Assinado por: **PEDRO MIGUEL CLEMENTE DIAS MOREIRA**
Num. de Identificação: 10352606
Data: 2022.02.15 14:07:35+00'00'

INSTITUTO POLITÉCNICO DE BEJA

Escola Superior de Tecnologia e Gestão

Mestrado em Engenharia de Segurança Informática

ABORDAGEM INOVADORA PARA A SEGURANÇA DA INFORMAÇÃO EM DOCUMENTOS IMPRESSOS

Pedro Miguel Clemente Dias Moreira

Orientado por :

Doutor Rui Miguel Soares Silva

Dissertação apresentada na
Escola Superior de Tecnologia e Gestão do Instituto Politécnico de Beja

2022

Resumo

ABORDAGEM INOVADORA PARA A SEGURANÇA DA INFORMAÇÃO EM DOCUMENTOS IMPRESSOS

É inevitável a impressão em papel de documentos com informações confidenciais. A partir do momento que seja impresso, o seu rastreamento é praticamente impossível. Este trabalho apresenta um sistema capaz de proteger a informação contida em documentos impressos, limitando o acesso apenas a utilizadores credenciados para tal, através da utilização de um sistema de realidade aumentada. É possível manter um rastreamento dos acessos à informação e revogar o acesso anteriormente concedido. São apresentadas duas abordagens, utilizando Reconhecimento de Caracteres e Reconhecimento de padrões. O sistema funciona através da criação de um documento cifrado e codificado que, posteriormente, através da utilização de óculos de realidade aumentada possibilita a visualização da informação por parte do utilizador.

Palavras-chave: *Confidencialidade em documentos impressos, espião de ombro, reconhecimento de caracteres, reconhecimento de padrões, realidade aumentada, sistema de gestão de mensagens.*

Abstract

INNOVATIVE APPROACH TO INFORMATION SECURITY IN PRINTED DOCUMENTS

Printing documents containing classified information on paper is inevitable. From the moment it is printed, its practically untraceable. This work presents a system capable of protecting information contained in printed documents, limiting access only to credentialed users, through the use of an augmented reality system. It is possible to keep track of accesses to information and revoke the access previously granted. Two approaches are presented, using Character Recognition and Pattern Recognition. The system works by creating an encrypted and encoded document that subsequently, through the use of augmented reality glasses makes it possible for the user to visualize the information.

Keywords: *Confidentiality in printed documents, shoulder spy, character recognition, pattern recognition, augmented reality, message management system.*

Agradecimentos

Não posso deixar de agradecer ao meu grande amigo e mentor, Professor Rui Miguel Soares Silva, de quem surgiu a brilhante ideia para implementar esta solução.

Estou eternamente grato pela forma como orientou a minha dissertação, paciência, empenho, contributo e forma como me motivou para conseguir levar a bom porto este trabalho.

Índice

Índice de Figuras

Índice de Tabelas

Capítulo 1

Introdução

Há séculos que as nações necessitam de ocultar mensagens de inimigos ou mesmo do seu povo por forma a evitar que os seus segredos cheguem ao conhecimento de quem não é suposto aceder a tais informações. Apesar da aparente contrariedade face a um regime democrático, o segredo é necessário em muitas áreas.

A evolução tecnológica possibilitou enormes avanços na transmissão de informação classificada de forma digital, mas existem situações onde poderá não ser possível a utilização de redes informáticas para a sua entrega, seja por restrições físicas, tecnológicas ou por questões de confidencialidade[1]. Em tais situações é preferível a utilização de documentos em papel.

Os documentos classificados impressos podem ser lidos por qualquer pessoa não autorizada, desde que tenha acesso físico aos documentos, o que pode dar origem a fugas de informação.

No sentido de minimizar o risco do acesso a informações confidenciais por quem não estiver autorizado para tal, é proposto neste trabalho um sistema alternativo para a distribuição e acesso a informação classificada impressa.

A base do sistema proposto consiste na distribuição de um documento que possa ser interpretado por um equipamento com câmara e com capacidade para processar a informação capturada. Neste caso foram utilizados óculos de realidade aumentada da marca Epson (modelo MOVERIO BT-200).

Apesar de ser possível a implementação em outros equipamentos, como smartphones ou tablets, a utilização dos óculos de realidade aumentada diminui consideravelmente a possibilidade do acesso à informação por parte de quem não tiver autorização para tal. Desde logo porque a informação cifrada fica visível apenas para o utilizador dos óculos, evitando assim o ataque conhecido como *espião de ombro*.

A técnica abordada neste documento permite utilizar tanto texto, como fotos, áudio ou vídeo.

[1] Por vezes é necessário que seja ocultada a transmissão de dados. A transmissão via digital poderá expor o destinatário (e.g. espiões).

O restante documento é composto pelo Capítulo 2 onde é feito um enquadramento teórico acerca do tema apresentado, abordando a segurança em sistemas de gestão de mensagens, segurança em documentos classificados, reconhecimento de caracteres, reconhecimento de padrões e autenticação biométrica.

Devido ao facto de não terem sido encontrados sistemas com a funcionalidade do sistema aqui proposto, optou-se por substituir o Estudo do Estado da Arte por um Enquadramento das Tecnologias de suporte ao sistema desenvolvido.

No Capítulo 3 é feita uma apresentação do sistema proposto, a sua avaliação no Capítulo 4 e no final as conclusões no Capítulo 5.

Capítulo 2

Enquadramento

Maret, S. & Goldman, J [26] apresentam um estudo sobre o segredo governamental, no seu livro destacam os principais tipos de segredo: bancário, burocrático, contratual, ambiental, executivo, íntimo, relacionado com invenções, militar, estado, nuclear, justiça, policial, entre outros.

Existem várias técnicas para garantir a confidencialidade das mensagens, Singh, Simon [38] apresenta técnicas utilizadas ao longo da história para ocultar mensagens por meio de cifras.

Existem alguns estudos que utilizam realidade aumentada para implementação de sistemas de criptografia visual[15] [2], no entanto estes tipos de sistemas apresentam riscos de segurança da informação, Bao Tianyou e Ok, Hurriyet[6] apresentam um estudo com possíveis soluções de mitigação desses riscos.

Neste capítulo é feito um enquadramento teórico sobre algumas das técnicas utilizadas, passíveis de serem aproveitadas para a implementação do trabalho proposto.

2.1 Sistemas de Gestão de Mensagens

A International Telecommunication Union - ITU, na sua recomendação F.400/X.400 [45] enumera ameaças existentes para sistemas de gestão de mensagens.

2.1.1 Ameaças ao Sistema

O acesso por utilizadores não autorizados é uma das maiores ameaças a sistemas de gestão de mensagens. Outros tipos de ameaças surgem por via de agentes externos à comunicação e podem manifestar-se das seguintes formas:

- Através do disfarce, tentado falsear o rementente da mensagem;
- Alteração da mensagem por um agente não autorizado;
- Captura da mensagem para ser reenviada mais tarde, podendo confundir o receptor;

- Espião de ombro, alguém conseguir observar parte ou a mensagem na totalidade.

No que diz respeito aos intervenientes na comunicação podem manifestar-se através do:

- Repúdio - negação do envio da mensagem;
- Violação do nível de segurança, encaminhando a mensagem para quem não tenha o nível de classificação de segurança que o autorize ao seu acesso.

Existem ainda outros tipos de ameças que envolvem a:

- Intercepção da mensagem e bloqueio no envio;
- Fabrico de novas mensagens para iludir o destinatário.

2.1.2 Capacidades do Sistema

Um sistema de gestão de mensagens deve:

- Garantir a autenticação do rementente e permitir que o destinatário comprove essa autenticidade;
- Fazer prova do envio e prova da recepção da mensagem;
- Garantir segurança no acesso à mensagem de acordo com o nível de segurança do meio de transporte;
- Garantir a integridade e a confidencialidade da mensagem;
- Garantir a confidencialidade e integridade da sequência de mensagens;
- Garantir o não repúdio do envio da mensagem;
- Correta etiquetagem da mensagem para que seja seguida a política de segurança em vigor.

2.2 Classificação da Informação

Em Portugal no sentido de proteger os segredos da Aliança NATO foram definidas as normas para a segurança nacional, salvaguarda e defesa das matérias classificadas, segurança industrial, tecnológica e de investigação — SEGNAC 2 [8] e as normas para a segurança nacional, salvaguarda e defesa das matérias classificadas, segurança informática — SEGNAC 4 [9].

A SEGNAC 2 identifica 4 graus de confidencialidade:

- Muito Secreto;
- Secreto;
- Confidencial;
- Reservado.

É também definido um conjunto de regras, procedimentos e processos necessários para garantir a segurança dos documentos classificados.

2.3 Criptografia

Tendo em conta que, em vários estudos, o algoritmo AES é considerado o mais seguro e eficiente [14] e o mais adequado para aplicações onde a integridade e confidencialidade são os fatores mais importantes [30], é sugerido que seja utilizado este algoritmo para a cifra da mensagem.

2.4 Identificação de Erros

Uma função de hash recebe uma entrada de qualquer dimensão e retorna uma saída de dimensão fixa. Qualquer alteração na entrada dará origem a uma resultado completamente diferente. Esta funcionalidade permite implementar o Serviço de Integridade, contra alterações intencionais ou inadvertidas, derivadas de erros de transmissão, por exemplo.

Como exemplos de funções de hash tradicionais podem referir-se o MD5 ou o SHA-1 que são actualmente desaconselhados por serem alvo de Ataques de Colisão; estes ataques derivam da propriedade das funções de hash de mapeamento de muitos para um, dado que a entrada pode ter qualquer dimensão e a saída tem dimensão fixa.

A identificação de Erros pode contudo recorrer ao Cyclic Redundancy Check (CRC), nomeadamente nos sistemas de comunicação, onde o processo se realiza pacote a pacote.

2.5 Reconhecimento de Padrões

Existem várias formas de proteger o acesso a imagens por utilizadores não autorizados através de cifra. Mishra and Gupta [28] classificam os métodos existentes, com base em sistemas para decifra pelo sistema visual humano – Criptografia Visual, e Sistemas Matemáticos.

De acordo com Asif et al. [4] a origem do Reconhecimento de Padrões data de 1870, por Carey, com a invenção de um leitor de retina.

2.5.1 Criptografia Visual

Criptografia Visual permite a cifra de informação visual de forma a que possa ser decifrada pelo sistema visual humano sem auxílio de um computador.

Esta técnica foi apresentada em 1994 por Naor and Shamir [31] e consiste na cifra de uma imagem em várias partes de forma a que esta seja decifrável apenas sobrepondo as várias partes. O modelo básico consiste numa cifra impressa num papel e um acetato ou mais cifras que servirão de chaves. Qualquer destas páginas é indecifrável por si só. Apenas a sua sobreposição, correctamente alinhada, permite obter a imagem secreta.

A simplicidade desta técnica permite que seja utilizada por alguém que não tenha conhecimentos de criptografia, além de não necessitar de operações computacionais para a operação de decifra.

Raju and Tech&Science em [36] identificam oito tipos de Criptografia Visual (optou-se por não traduzir a descrição das técnicas por se entender que neste caso se perderia o contexto):

- Visual cryptography for gray level images
- Visual cryptography for general access structures
- Halftone visual cryptography
- Recursive threshold visual cryptography
- Visual cryptography for color images
- Regional incrementing Visual Cryptography
- Extended visual cryptography for natural images
- Progressive visual cryptography

Anuradha and Rani[3] separam em três os tipos de esquemas:

- Traditional Visual Cryptography
- Extended Visual Cryptography
- Color Visual Cryptography

Segundo o seu estudo, o esquema *Color Visual Cryptography* apresenta a performance mais satisfatória.

Revenkar et al. em [37] separam os tipos de esquemas em Criptografia Visual para imagens a preto e branco e a cores. No seu estudo efectuam uma comparação entre vários esquemas de entre estes tipos, tanto na utilização de apenas uma chave como de várias

chaves. Por fim sugerem os esquemas ideiais, de entre os estudados, para aplicação em várias situações.

Borchert and Reinhardt[7] sugerem a utilização de Criptografia Visual em transacções financeiras online.

Um dos problemas na criptografia visual está na necessidade da sobreposição exacta das várias partes do criptograma. Para resolver esse problema Yan et al. [50], sugerem a utilização uma técnica de inclusão de marcas de alinhamento (Walsh Transform) para que as partes da cifra sejam correctamente alinhadas.

2.5.2 Sistemas Matemáticos

G.A.Sathishkumar et al [17] criaram um algoritmo para cifrar / decifrar imagens utilizando a técnica *multiple chaotic based circular mapping*. Esta técnica mostrou-se computacionalmente rápida, económica e permite a utilização de chaves simétricas.

Em 2014, Zhang et al [53], criaram um algoritmo baseado num sistema *spatio temporal chaotic* que apresenta uma elevada taxa de segurança e se mostrou mais eficiente que a maior parte das técnicas utilizadas para cifra de imagens.

Outro esquema, publicado por Mirzaei et al [27], cifra imagens com base em permutações e cifra paralela. O algoritmo é rápido, pois utiliza funções XOR e tem uma ampla gama de chaves possiveis (2^{296}).

Já Ye & Zhou [51], através de um algoritmo baseado em operações de difusão conseguem reduzir a redundância computacional apresentada noutras arquitecturas tradicionais.

2.5.3 Esteganografia

Esteganografia deriva do grego, onde estegano "stegos" significa esconder, mascarar, e, grafia significa escrita.

De acordo com Anderson and Petitcolas[1] a esteganografia remonta à antiguidade. Existem relatos em que os gregos receberam um aviso das intenções hostis de Xerxes numa mensagem escondida com uma tinta secreta. No entanto o primeiro estudo científico, a esta técnica, foi apresentado em 1984 por Simmons[5].

Subhedar and Mankar[43] classificam os tipos de esteganografia em quatro modelos:

- Spatial Domain;
- Transform Domain;
- Spread Spectrum;
- Model Based Steganography.

No seu trabalho identificaram as técnicas utilizadas em cada um dos modelos e sugerem o procedimento a tomar para obter uma boa segurança contra ataques.

É possivel utilizar cifras gráficas para proteger ou ocultar informação. Estas técnicas podem ser utilizadas, não só para proteger informação, como também para que possa ser possivel identificar o utilizador que decifrou um determinado documento. Um exemplo dessa possíbilidade é apresentado por Dixit et al. [11] que propõem uma forma de ocultar dados dentro de uma imagem com uma distorção mínima, aumentando a probabilidade de sucesso na ocultação de dados.

Existe uma solução que dá pelo nome de "papel inteligente", Dymetman e Cooperman [13] apresentam possiveis aplicações desta técnica. Trata-se de um papel físico onde além do conteúdo visível são também impressas marcas com tinta invisível ao olho humano. Tocando nessas marcas com um apontador é possível interpretá-las. Nestes exemplos o resultado consiste na obtenção de conteúdos relacionados, na internet, e apresentação num dispositivo associado ao apontador.

2.6 Reconhecimento Óptico de Caracteres

Asif et al. [4] indicam que o Reconhecimento Óptico de Caracteres (OCR) surgiu em 1900 através de Tyurin na tentativa de auxiliar pessoas com deficiência visual. No entanto, é conhecido[5] que em 1809 foi registada uma patente para um sistema de auxilio de leitura para deficientes visuais, com base em OCR.

O OCR tem sido alvo de estudo ao longo do tempo. Recentemente, T.C.Wei, et al.[48] apresentam um sistema aperfeiçoado de OCR com uma rede neural profunda onde conseguiu atingir uma melhoria significativa na eficácia do reconhecimento de texto em imagems com baixa qualidade, obtendo uma redução de 21,5% de erros comparativamente com outras soluções OCR existentes.

Existem várias soluções open source para OCR, Y. Leydier, et al,[23] apresentaram libcrn, uma biblioteca open source de processamento de imagens.

A versão moderna de OCR surgiu em meados dos anos 1940, com o nascimento da computação digital. David Shepard foi considerado o pioneiro no desenvolvimento de equipamentos OCR, comercializando-os para o público em geral nos anos 1950.

Ray Smith[40] apresentaram uma análise a uma ferramenta muito utilizada em OCR - Tesseract[41][44], esta solução foi criada pela Hewlett-Packard Laboratories Bristol e Hewlett-Packard Co, entre 1985 e 1994, foram feitas alguma alterações em 1996 para compatibilidade com o sistema operativo Windows, e migração de algum código para C++ em 1998. Em 2005 tornou-se open source e entre 2006 e 2018 foi mantido pela Google.

O algoritmo Tesseract começa por converter a imagem de entrada para binária e segmentar o documento em linhas de texto. Dessas linhas é feita a segmentação dos caracteres em palavras, o reconhecimento é feito através de classificadores adaptativos, sendo possível utilizar dados de treino de acordo com a linguagem pretendida. Após a fase de

reconhecimento dos caracteres é feita uma análise mais apurada das palavras existentes no documento corrigindo eventuais erros no reconhecimento de alguns caracteres.

OCR pode ser dividido em três fases: Pré-Processamento, Segmentação e Classificação de Características.

2.6.1 Pré-Processamento

A entrada para um sistema de OCR, normalmente, é uma imagem colorida ou em tons de cinza. Para que o reconhecimento seja feito é necessário identificar as áreas onde o texto está contido. Dentro dessas áreas é aplicada uma redução de ruído e normalização para posterior segmentação de linhas e caracteres.

Vishwanath et al., [46] melhoraram esse reconhecimento convertendo a imagem para tons de cinza, efetuando uma comparação entre as duas versões e alterando os valores das cores para um intervalo de 0 a 100. Ambas as versões são reduzidas e, por fim, os píxeis com maior valor (20% do total) são multiplicados por 2.55. Esta técnica melhora a visualização dos caracteres, que se destacam com maior visibilidade do fundo do documento.

2.6.2 Segmentação

Patel et al. [35] fizeram um estudo dos métodos utilizados para segmentação de matrículas de automóveis. Neste trabalho estudaram os resultados apresentados por Ying et al. [52], Lee et al. [22] e Vishwanath et al. [46].

Para segmentação de caracteres em imagens binárias, é suficiente fazer a verificação vertical da existência de pixeis coloridos. No entanto o ruído e caracteres que se unem podem causar erros neste tipo de abordagem. Lee et al. [22] apresentam uma solução muito eficaz para este problema.

Manikandan et al. [25] apresentam um algoritmo que melhora a segmentação utilizando Hough Transform. No seu artigo é proposta a utilização de uma versão DSL - "Digital Straight Line" de Hough Transform. Esta proposta começa o processamento por segmentar o documento, já convertido em imagem binária, em linhas, seguida pela segmentação em colunas. Após as fases iniciais, é calculado o grau de rotação do documento e, por último a segmentação dos caracteres.

Vishwanath, et al. [46] consideram que conhecendo características exatas do tipo de documento a analisar aumenta consideravelmente a eficácia no reconhecimento de caracteres. No seu trabalho fazem a prova desta teoria, com um sistema baseado em Hough Transform para reconhecimento de matrículas de automóveis. Neste caso as características são:

- Dimensão da matrícula;
- Dimensão dos caracteres;

- Espaçamento entre os caracteres.

Ying et al. [52] tentam a identificação de um objecto de referência para facilitar a segmentação dos caracteres em matrículas de automóveis.

Jain, A et al. [18] utilizam MSER - Maximally Stable Extremal Regions para a identificação de áreas de texto com o auxílio de Support Vector Machines.

2.6.3 Extração de Características

Esta fase é, provavelmente, a mais importante para o reconhecimento de alta performance e pode ser dividida em duas partes:

- Seleção de Caraterísticas;
- Classificação.

O método de extração irá definir o tipo de características resultantes. Também o pré-processamento tem de ter este factor em conta. Alguns métodos apenas funcionam com imagens em tons de cinza, enquanto que outros com imagens binárias, contornos exteriores binários ou vectores (Vector Skeleton).

O método de classificação também depende destas variantes, já que o formato das características extraídas deve respeitar os requisitos do classificador.

A extração de características pode ser feita diretamente em imagens em tons de cinza, vectorizando a imagem num símbolo compacto, onde cada píxel tem os valores 0 ou 1, tornando o contorno da simplificação da forma ou objeto num vector (backbone).

Øivind Due Trier et. al [12] concluem que muitas vezes a utilização de apenas um método de extração não é suficiente para atingir bons resultados.

A obtenção de imagens binárias a partir da versão em escala de cinza permite uma maior compressão pois cada píxel apenas será representado pelos valores 0 ou 1 ao contrário de 256 tons de cinza. Desta conversão podem surgir alguns problemas, especialmente em caracteres que estejam unidos a outros em alguns pontos.

Outro método de extração passa pela obtenção do contorno binário da imagem. Os contornos são analisados e criadas funções periódicas para cada segmento identificado.

As características também podem ser extraídas pela representação vectorial do caracter. Estas podem ser obtidas através da redução da forma do caracter até que a linha do caracter apresente a espessura de 1 píxel. Esta vectorização pode ser obtida diretamente da sua representação em escala de cinza.

Narasimha Reddy Soora e Parag S. Deshpande [42] apresenta uma revisão de métodos de extração de características para OCR. No seu trabalho classificam estas técnicas em dois grupos:

- Não baseadas em formas

- Centroids
- Special dots
- End points
- Intersection Points
- Cross Correlation
- Template Matching
- Statistical Features

- Baseadas em formas
  - Geometrical Features
  - Moment Based Features
  - Local Features
  - Spatial Relational Features

2.6.4 Classificação das Características Extraidas

Podem ser classificadas em três grupos: Statistical, Global Transformation e Series Expansion Features and Structural. Todavia existem dois outros tipos de classificadores que funcionam como combinadores de métodos de extração e, simultâneamente, como classificadores estatísticos.

- **Classificadores Estatísticos**

  Derivam da distribuição estatística dos pontos. Podem ser utilizados para reduzir a quantidade de elementos no conjunto de estatísticas. Os mais significantes são:

  (i) Zoning;

  (ii) Characteristic Loci;

  (iii) Crossing and Distances.

- **Transformadores Globais e Séries de Expanção de Características**

  Características que não variam com deformações como rotações ou outras. Exemplos:

  (i) Fourier Transforms;

  (ii) Walsh Hadamard Transform;

  (iii) Rapid Transform;

  (iv) Hough Transform;

  (v) Gabor Transform;

  (vi) Wavelets;

(vii) Karhunen Loeve Expansion;

(viii) Moments. Mori et al., Cite 156468 concluíu que estes classificadores apenas são úteis para caracteres impressos (machine-printed).

- **Classificadores Estruturais**

  Podem representar características locais ou globais e apresentam grande tolerância a distorções e variações de estilo. Neste grupo estão incluídas linhas, linhas e direções de fendas, Cadeias de Códigos, intersecções em segmentos de linha e loops, bem como relações entre linhas e propriedades de ângulos.

  Mori et al., [29], no seu estudo, abordam:

  (i) Análise de Redução de Linhas;

  (ii) Decomposição em Massa;

  (iii) Análise de Fendas Consecutivas / Seguimento de Fluxo;

  (iv) Análise de Seguimento de Contornos;

  (v) Análise de Background.

- **Redes Artificiais Neurais (RNAs)**

  Podem ser vistas como uma combinação de métodos e extração e classificadores de características. Nielsen apresenta uma introdução [32] a este método com exemplos práticos.

  São as mais utilizadas em reconhecimento de texto escrito à mão. É criada uma base de dados de exemplos para comparações. As RNAs criam automaticamente regras para o reconhecimento, e mais exemplos são adicionados à base de dados à medida em que o reconhecimento for executado. Desta forma o reconhecimento vai sendo aperfeiçoado e a sua eficácia enriquecida. Os pesos deste método são associados a determinadas características. As decisões são tomadas através da avaliação dos pesos das respetivas características.

- **Máquinas de Vectores de Suporte (MVS)**

  Classificador baseado em estatísticas, onde é definido um hiperplano que separa as classes dos dados fornecidos para treino antecipado. A biblioteca OpenCV suporta a utilização deste classificador [34].

- **Modelos Ocultos de Markov (MOM)**

  É uma ferramenta estatística poderosa para modelação de situações para que seja estudada a sua natureza ou auxiliar na predição de observações futuras [10]. É também bastante utilizada na segmentação.

De acordo com Luiz de Oliveira [33], inicialmente, este modelo era aplicado em reconhecimento de voz, no entanto tem também sido utilizado em reconhecimento de texto manuscrito.

2.7 Autenticação Biométrica

Para proteger o acesso à informação, por quem tiver acesso físico ao equipamento que irá decifrar a mensagem, a Autenticação Biométrica é fundamental.

Recentemente houve melhorias relevantes na área de autenticação em dispositivos móveis [21], ou autenticação em sistemas de realidade aumentada [16]. Existem várias opções disponíveis, como autenticação por impressão digital, reconhecimento facial, reconhecimento de voz e de retina.

Neste trabalho sugerimos a utilização de smart glasses com implementação de reconhecimento de retina. Este tipo de reconhecimento pode ser dividido em três categorias, nomeadamente:

- Utilização de sistemas integrados nos equipamentos;
- Conexão a dispositivos externos;
- Conexão a câmaras Near-Infrared (NIR) com iluminadores [20]. Estas câmaras são dispositivos poderosos com a capacidade de capturar imagens da iris com padrões espectrais nítidos mesmo em iris com cores escuras[19].

Yung-Hui Li and Po-Jen Huang[24] afirmam serem pioneiros na implementação de reconhecimento de iris em smart glasses.

2.8 Proposta de Investigação

Considerando os métodos e tecnologias apresentadas, e existindo já atualmente dispositivos que permitem a captura de imagens e o seu processamento, e admitindo a sua evolução e aperfeiçoamento, será possível desenvolver um sistema composto por duas partes, sendo uma que cifre e codifique a informação a imprimir em papel, e, outra que capture, descodifique e decifre o que foi impresso, e apresente o seu resultado no visor de um dispositivo de realidade aumentada? Sendo portanto este sistema capaz de proteger informação classificada em documentos impressos?

Capítulo 3

Sistema Proposto

Para ler o conteúdo de um documento classificado por alguém sem autorização basta ter acesso ao documento, o que pode levar a fugas de informação. Para minimizar o risco de acesso a informação confidencial por utilizadores não autorizados é apresentado, neste trabalho, um sistema alternativo para distribuição e acesso a documentos classificados em documentos impressos.

Neste capítulo é apresentada a solução proposta para reduzir o risco de fuga de informação e, em simultâneo conseguir um rastreio de quem acede, ao quê, e quando, limitando o acesso a utilizadores autorizados.

A base deste sistema é a impressão de um documento que pode ser lido por um dispositivo equipado com uma câmara capaz de processar a informação presente no documento. Apesar de ser possível utilizar o sistema em outros dispositivos, a utilização de óculos de realidade aumentada reduz significativamente o acesso à informação por utilizadores não autorizados.

Neste trabalho foram utilizados óculos de realidade aumentada Epson MOVERIO BT-200. A informação decifrada apenas é visível ao utilizador. A técnica utilizada permite a transmissão de documentos de texto, fotos, áudio ou vídeo.

O sistema proposto é constituido por três componentes: cifra, autenticação e decifra e são apresentadas duas abordagens alternativas para a criação e processamento do documento:

- Com base em Reconhecimento Óptico de Caracteres;
- Utilizando Reconhecimento de Padrões (cores).

3.1 Processo de Cifra

Foram utilizadas duas abordagens, Reconhecimento Óptico de caracteres e Reconhecimento de Padrões. Em ambas as situações podem ser impressas várias folhas para armazenamento da informação.

É necessário um bom controlo de erros pois, neste tipo de operações um erro no reconhecimento invalida a totalidade da mensagem. Neste sistema foi implementado o controlo de erros tanto na totalidade do documento, como nas linhas, através de cabeçalhos. Nos cabeçalhos das linhas, é indicada a sua numeração, possibilitando a impressão de forma não sequencial, ou mesmo a utilização de uma linha como elemento chave para a decifra do documento, partilhada por outra via.

Figura 3.1: Processo de Cifra

O algoritmo de cifra é transparente no sistema proposto, ou seja, não é perceptível ao utilizador. Sugere-se que seja utilizado um sistema híbrido de criptografia simétrica e assimétrica, tendo cada documento uma chave simétrica que será partilhada com os utilizadores através da sua encriptação com a chave pública desse mesmo utilizador. Consideram-se duas situações possíveis de utilização do sistema proposto, nomeadamente:

- Sistema Online

  Vantagens: (i) possibilidade de revogar o acesso a utilizadores; (ii) possibilidade de saber quando e quem acedeu ao documento;

  Desvantagens: (i) A chave do documento terá de ser solicitada a um servidor online, o que poderá expor esse mesmo utilizador; (ii) Em caso de incapacidade de comunicação com o servidor não será possível obter a chave para abertura do documento;

- Sistema Offline

  Vantagem: (i) Não é necessária qualquer ligação a um servidor online;

  Desvantagem: (ii) Impossibilidade de saber quem e quando acede aos documentos;

Após a cifra, segue-se o processo de codificação, que apresenta diferenças nas duas situações de utilização indicadas.

3.2 Processo de Decifra

Os documentos impressos protegidos assumem, naturalmente, a forma de um conjunto de folhas de papel, cujo conteúdo não é entendível às pessoas. Para visualizar o conteúdo, o utilizador deve estar equipado com óculos de realidade aumentada e, após autenticação,

olhar para cada uma das folhas impressas através do óculos. Após o processamento de todas as páginas, a informação é apresentada nos óculos, evitando ataques de espião de ombro. Na Figura 3.2 apresenta-se o processo de decifra

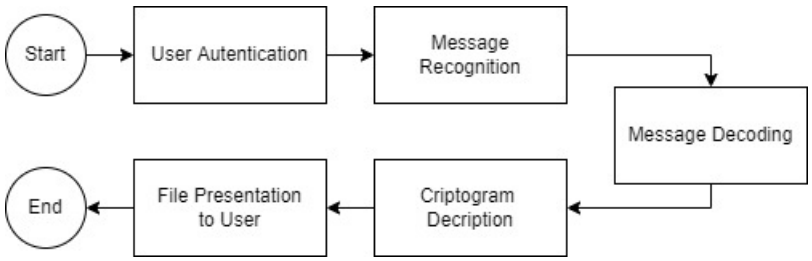

Figura 3.2: Processo de Decifra

3.3 Composição dos Documentos

A base seguida no desenvolvimento do sistema proposto para estrutura do documento segue o exposto na Recomendação F.400/X.400 da ITU [45] como estrutura de uma mensagem IP. (Figura 3.3).

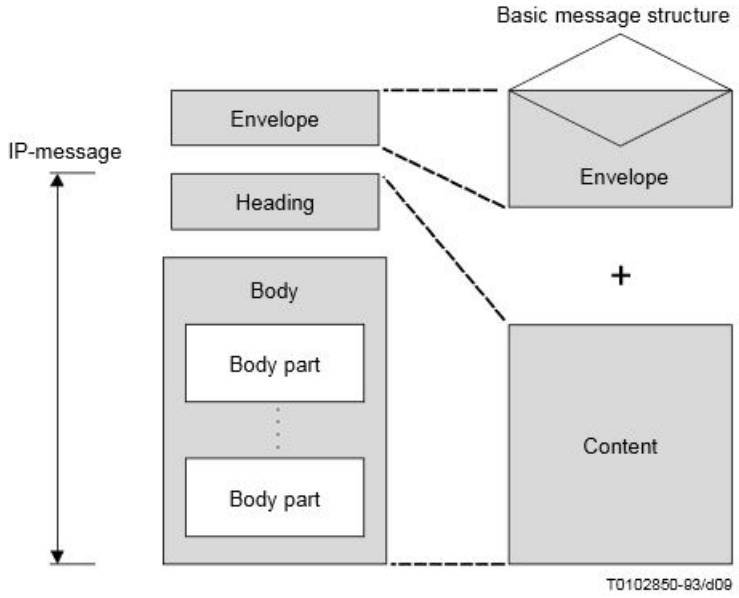

Figura 3.3: Estrutura de uma mensagem IP - Recomendação ITU F.400/X.400

Seguindo o exemplificado na recomendação (Figura 3.3), o Documento (Figura 3.4) é constituído por um cabeçalho e um payload (Mensagem) encapsulando várias linhas de texto, cada uma delas também com um cabeçalho e respetivo payload. O conteúdo final

pode ser constituído por texto ou imagem impressos no documento, que poderá ter várias folhas.

Neste trabalho foi utilizada a função CRC16 para o cálculo dos checksum, assim são utilizados 16 bits por linha (Figura 3.7) e 32 bits no cabeçalho do documento (Figura 3.5) para checksums.

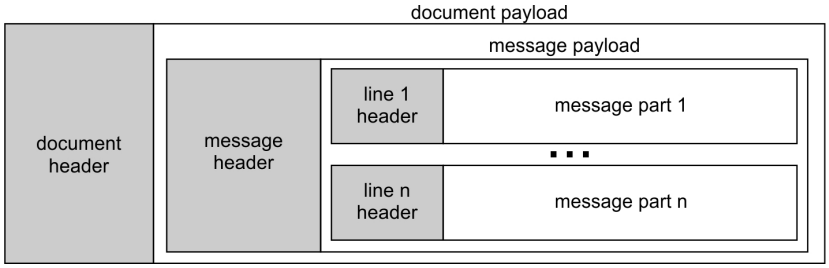

Figura 3.4: Estrutura Global do Documento

O cabeçalho do Documento (Figura 3.5) é constituído por três partes:

- Header Checksum - Cálculo CRC do Number of LInes e Message Checksum
- Number of Lines - Número total de linhas que compõe o documento (excluíndo o cabeçalho)
- Message Checksum - Cálculo CRC da mensagem final

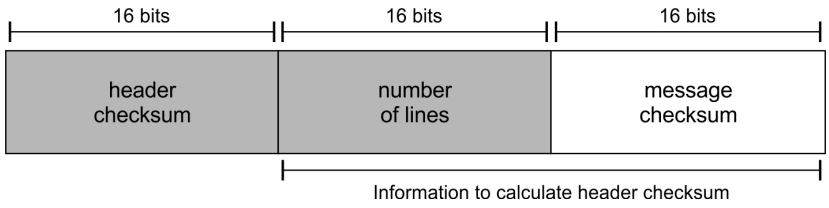

Figura 3.5: Cabeçalho do Documento

O cabeçalho da Mensagem (Figura 3.6) está também dividido em três partes:

- Number of Padding Bits - Quantidade de bits necessários para a operação de padding
- Padding Bits - Bits de padding gerados aleatoriamente
- Message - Payload da Mensagem, constituído por uma ou mais Linhas

Cada Linha da Mensagem está dividida em três partes constituídas pelo cabeçalho da Linha (Figura 3.7) e pela parte correspondente da Mensagem :

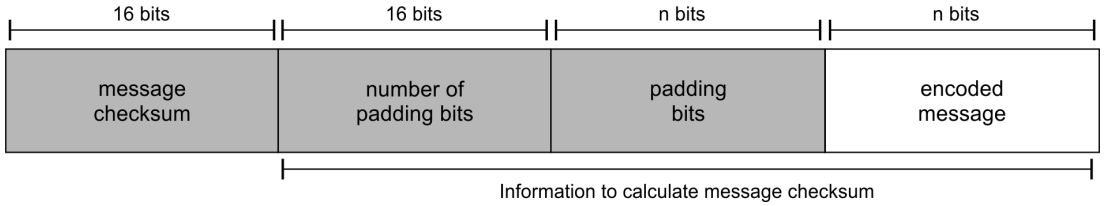

Figura 3.6: Cabeçalho da Mensagem

- Line Checksum - Cálculo CRC do Line Number e Message Part da Linha atual
- Line Number - Número de ordem da linha
- Message Part - Parte da Mensagem, para reconstrução final

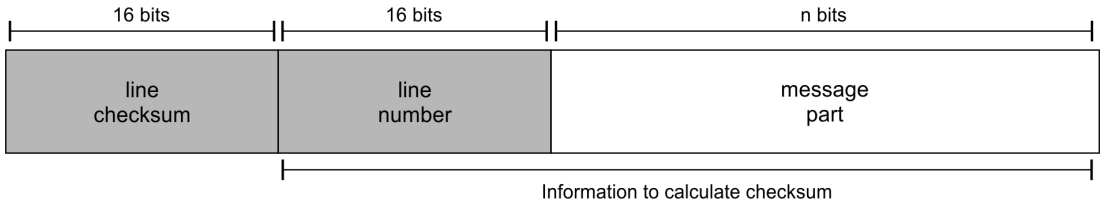

Figura 3.7: Cabeçalho das Linhas

3.4 Reconhecimento Óptico de Caracteres

Tal como indicado no início deste capítulo, uma das abordagens para criação e processamento dos documentos recorre ao Reconhecimento Óptico de Caracteres e, portanto, os documentos impressos são constituídos por caracteres. É necessário garantir que o reconhecimento dos caracteres não tem erros, já que invalidaria a totalidade do documento. Aqui a qualidade da câmara utilizada é fulcral para a eficácia do reconhecimento.

Nesta abordagem, o documento é constituído por séries de caracteres que representam código binário, de acordo com a informação cifrada. O número de bits possíveis de armazenar num carácter pode variar, consoante a quantidade de diferentes caracteres a utilizar: $qt = lg(X)$ onde qt é o total de bits possíveis de armazenar em um carácter pertencente a um conjunto de dimensão X.

O documento a imprimir é gerado a partir do criptograma, passando pelo processo de codificação com base no conjunto de caracteres definido inicialmente (Figura 3.1).

Para obter o documento original, o utilizador deve equipar-se com os óculos de realidade aumentada, autenticar-se no sistema e, se tiver autorização para tal, dá-se início ao processo de reconhecimento. Após a conclusão do reconhecimento, o documento é descodificado, decifrado e apresentado ao utilizador, tal como se ilustra na Figura 3.2.

No cabeçalho do documento é indicado o número de linhas total e o checksum do documento. Por sua vez, os cabeçalhos das linhas indicam o número de linha e o checksum do seu payload. Após a leitura de todas as linhas, os payloads são concatenados, calculado o checksum e, se coincidir com o indicado no cabeçalho, o processo continua com a abertura do documento para apresentação ao utilizador.

Seguidamente apresenta-se um exemplo de codificação de um documento com a mensagem "HELLO WORLD"na Secção 3.4.1, e depois na Secção 3.4.2 descreve-se o processo de descodificação.

3.4.1 Processo de Codificação

A semelhança entre caracteres distintos é um dos principais problemas no reconhecimento. Num sistema deste tipo a falha no reconhecimento de um carácter invalida toda a linha e, consequentemente, todo o documento.

Tendo em conta este constrangimento, neste trabalho, foi realizada uma Prova de Conceito, tendo-se decidido utlizar um conjunto reduzido de caracteres escolhendo os menos propícios a este tipo de erros. Com a dimensão do conjunto escolhida é possível armazenar $int(log2(X))$ bits de informação em cada carácter, onde X é o número de caracteres a utilizar na operação de codificação.

Um conjunto de 32 caracteres (Tabela 3.1) permite o armazenamento individual de 5 bits de informação.

O processo de codificação começa por transformar a mensagem na sua representação binária, de acordo com o conjunto de caracteres utilizado.

Neste trabalho é exemplificado o processo, tendo como base um documento com a mensagem "HELLO WORLD!". A sua representação em binário (Tabela 3.2) dá origem à sequência "01001000 01000101 01001100 01001100 01001111 00100000 01010111 01001111 01010010 01001100 01000100 00100001".

De seguida é executada uma operação de padding, adicionando os bits necessários para que a dimensão da mensagem seja múltiplo de $int(log2(X))$ (X = universo de caracteres utilizados na codificação).

É necessário predefinir a quantidade de caracteres que irão ser impressos por linha, para esta definição há que ter em conta a qualidade da câmara que vai ser utilizada no reconhecimento, pois tendo de ser reconhecida a totalidade da linha, quanto mais caracteres a compuserem maior será a linha e, consequentemente, menor será a dimensão dos caracteres na imagem capturada.

Neste exemplo utilizou-se um conjunto de 32 caracteres, que permite armazenar cinco bits cada *(bits_caracter = 5)*. Dada a fraca qualidade da câmara, são utilizados 15 caracteres por linha *(caracteres_linha = 15)*. Cada linha necessita de 32 bits para o seu cabeçalho *(len_cab_linha = 32)* O número de bits armazenáveis por linha *(bits_linha)* é calculado como:

CARÁCTER	VALOR BINÁRIO CODIFICADO
a	00000
b	00001
d	00010
m	00011
n	00100
A	00101
B	00110
D	00111
E	01000
F	01001
G	01010
H	01011
K	01100
L	01101
M	01110
N	01111
R	10000
T	10001
1	10010
3	10011
4	10100
5	10101
2	10110
#	10111
+	11000
&	11001
@	11010
g	11011
%	11100
J	11101
p	11110
7	11111

Tabela 3.1: Caracteres utilizados na codificação

CARÁCTER	VALOR DECIMAL ASCII	VALOR BINÁRIO
H	72	01001000
E	69	01000101
L	76	01001100
L	76	01001100
O	79	01001111
	32	00100000
W	87	01010111
O	79	01001111
R	82	01010010
L	76	01001100
D	68	01000100
!	33	00100001

Tabela 3.2: Representação Binária da Frase "HELLO WORLD!"

```
bits_linha = caracteres_linha * bits_caracter - len_cab_linha
<=>
bits_linha = 43
```

A dimensão da mensagem a transmitir é de 96 bit acrescida de 16 bit para o número de padding bits e os padding bit necessários, logo o número de linhas no documento será:

```
numero_linhas = (len_mensagem + 16) / bits_linha
+ ((len_mensagem + 16) % bits_linha > 0)
<=>
numero_linhas = 3
```

Há a necessidade de adicionar bits padding para completar a mensagem, então:

```
len_padding_bits = numero_linhas * bits_linha - (len_mensagem + 16)
<=>
len_padding_bits = 17
```

São criados 17 bit aleatórios e pode calcular-se a totalidade da mensagem:

```
padding_bits = 1
M = len_padding_bits || padding_bits || message
<=>
M =
0000000000010001 ||
10101010101010101 ||
01001000 01000101 01001100 01001100
01001111 00100000 01010111 01001111
01010010 01001100 01000100 00100001
```

Após a concatenação é possível calcular o checksum:

```
message_checksum = CRC16(M)
<=>
message_checksum = 0001000001001000
```

É então possível calcular o checksum do cabeçalho do documento

```
header_checksum = CRC16(numero_linhas || message_checksum)
<=>
header_checksum = 0100100110111001
```

É necessário que toda a linha do cabeçalho fique preenchida, neste caso cada linha terá capacidade de armazenamento de 75 bits. Para terminar a capacidade da linha é necessário preencher 27 bits adicionais com valores aleatórios Finalmente o cabeçalho fica definido:

```
doc_header = 0100100110111001 ||
0000000000000011 ||
0001000001001000 ||
011011011000101011001011101
```

Para a codificação do cabeçalho, primeira linha do documento, é necessário segmentar o seu valor binário de acordo com a capacidade de cada carácter e escrever a sua representação (Tabela 3.3) :

```
F B % R a a + R F b 2 + 5 1 J
```

A construção das linhas seguintes consiste na divisão da mensagem, já preparada com os bits de padding, pelo número de linhas já identificado:

VALOR BINÁRIO	CARACTERE
01001	F
00110	B
11100	%
10000	R
00000	a
00000	a
11000	+
10000	R
01001	F
00001	b
10110	2
11000	+
10101	5
10010	1
11101	J

Tabela 3.3: Cabeçalho da Codificação da Frase "HELLO WORLD!"

```
M1 = 0000000000010001101010101010101010100100001
M2 = 0001010100110001001100010011110010000001010
M3 = 1110100111101010010010011000100010000100001
```

Para cada linha é calculado o checksum do número da linha concatenado com a parte da mensagem:

```
line_checksum_x = CRC16( line_number_x || M_x)
L_X = line_checksum_x || line_number_x || M_x

line_checksum1 = 0100111111011101
line_checksum2 = 0110011010000101
line_checksum3 = 0101011100101001

L1 = 01010 11100 10100
10000 00000 00000 01000
00000 00010 00110 10101
01010 10101 01001 00001

L2 = 01100 11010 00010
10000 00000 00000 10000
10101 00110 00100 11000
```

```
10011 11001 00000 01010

L3 = 01010 11100 10100
10000 00000 00000 11111
01001 11101 01001 00100
11000 10001 00001 00001

L1 = G % 4 R a a E a d B 5 G 5 F b
L2 = K @ d R a a R 5 B n + 3 & a G
L3 = G % 4 R a a 7 F J F n + T b b
```

Finalmente o resultado é impresso em papel, pronto para distribuição.

```
F B % R a a + R F b 2 + 5 1 J
G % 4 R a a E a d B 5 G 5 F b
K @ d R a a R 5 B n + 3 & a G
G % 4 R a a 7 F J F n + T b b
```

3.4.2 Processo de Descodificação

O processo de descodificação, nesta abordagem de Reconhecimento Óptico de Caracteres, foi implementado com o auxílio de uma API open source para reconhecimento de texto, Tessaract[39].

Dada a fraca qualidade da câmara utilizada, para a escolha do universo de caracteres a utilizar foi necessário identificar os menos susceptíveis de gerar confusão no seu reconhecimento. Por exemplo a utilização dos caracteres 0(*zero*), o *o* e *O* (maiúsculo), entre outros.

O processo está ilustrado na Figura 3.8. O equipamento começa por procurar uma linha com o cabeçalho de um documento. Essa linha é identificada quando o cálculo CRC16 dos bits da posição 16 até à posição 48 coincide com primeiros 16 bit da mesma linha.

Após a identificação do cabeçalho, a aplicação inicia o processo de reconhecimento do número total de linhas indicado no cabeçalho.

Para cada linha é calculado o CRC16 de todos os seus bits, a partir da posição 16 e comparado o valor com os primeiros 16 bits da mesma linha. Se este valor coincidir a linha é armazenada para a reconstrução final da mensagem.

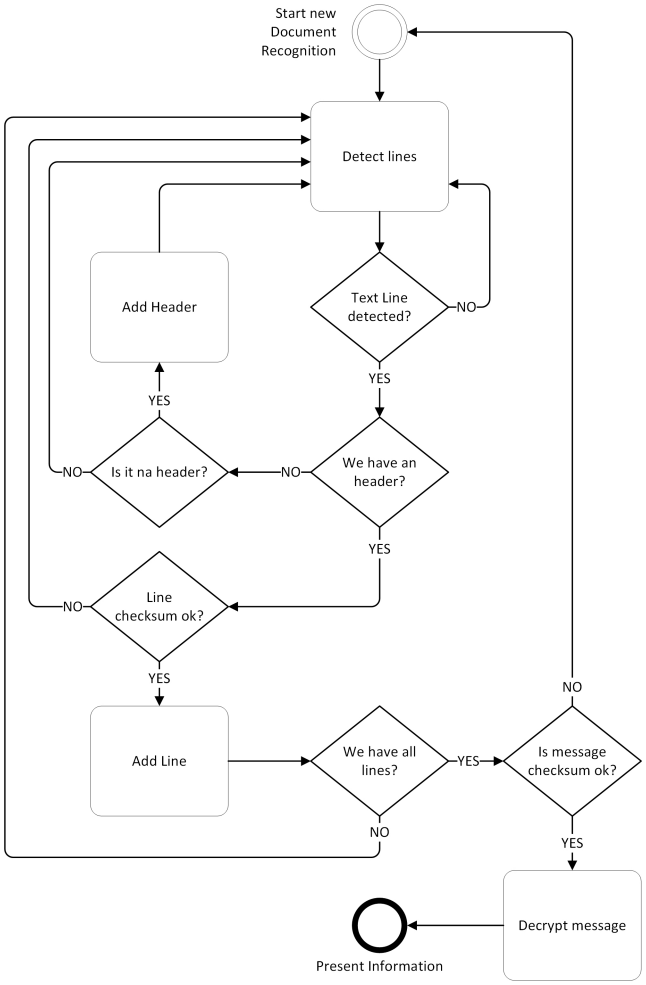

Figura 3.8: Diagrama de fluxo do processo de decifra por OCR

Este processo é repetido até que todas as linhas sejam identificadas. À medida que o reconhecimento é feito, o utilizador é notificado das linhas em falta para que o processo termine.

Quando todas as linhas estão armazenadas, a mensagem é reconstruída, é calculado o CRC16 e comparado com o checksum indicado no cabeçalho, se os valores coincidirem os bits de padding são removidos e a informação decifrada para ser apresentada ao utilizador através dos óculos de realidade aumentada.

3.5 Reconhecimento de Padrões

Existem várias formas de proteger o acesso a imagens por utilizadores não autorizados. Mishra and Gupta [28] classificam os métodos de cifra existentes, com base no sistema de decifra, em sistemas para decifra pelo sistema visual humano – Criptografia Visual, e Sistemas Matemáticos.

A técnica proposta consiste em codificar a mensagem em blocos de cores (pseudo-píxeis). No topo do documento é colocada uma linha com a escala de cores e tons utilizados na criação do documento. As duas linhas seguintes são constituidas por 14 blocos cada onde constam o checksum do cabeçalho, checksum da mensagem, total de linhas, total de blocos que constituem o documento e a dimensão de cada um deles.

Para ultrapassar as variações na identificação da cor capturada, o sistema fará o varrimento de cada um dos blocos, píxel a píxel, calculando a média da cor neles prensente. O valor obtido é então comparado com a escala de cores existente no cabeçalho da página. O valor mais próximo é utilizado como o binário para o corpo da mensagem.

Figura 3.9: Reconhecimento de padrões - Exemplo de folha em ambiente com ruído

Seguidamente apresenta-se um exemplo de codificação de um documento com a mensagem "HELLO WORLD" na Secção 3.5.1, e depois na Secção 3.5.2 descreve-se o processo de descodificação.

3.5.1 Processo de Codificação

O processo utilizado para Reconhecimento de Padrões consiste na criação de pseudo píxeis que poderão variar na sua dimensão para facilitar o reconhecimento pelo dispositivo. Foi decidido, neste trabalho, o desenvolvimento de uma Prova de Conceito com a utilização de apenas quatro padrões em escala de cinza, o que permite o armazenamento de 2 bits de informação por pseudo pixel.

O processo de codificação é semelhante ao utilizado no Reconhecimento Óptico de Caracteres, mas neste caso a representação da informação é feita em quadrados de cor sólida, correspondente ao valor desejado.

Utilizando o exemplo anterior da frase "HELLO WORLD!", a sequência a codificar é "01001000 01000101 01001100 01001100 01001111 00100000 01010111 01001111 01010010 01001100 01000100 00100001".

No início do documento é impressa uma escala de cores (Figura 3.10) com o universo de blocos utilizado na codificação. Esta escala serve para auxiliar na correta identificação do valor dos blocos para o processo de descodificação, tendo em conta a possíveis variações de luminosidade do ambiente.

Figura 3.10: Escala de Cores para Cabeçalho em Reconhecimento de Padrões

A mensagem é codificada em vários blocos de acordo com a sua dimensão, é feito um cálculo apurando a quantidade de blocos necessários para apresentar a mensagem na folha, e são organizados os blocos ao longo da mesma. No final são impressos blocos com valores aleatórios para preencher a totalidade do documento.

No cabeçalho do documento (Figura 3.11) é incluido o checksum do próprio, checksum da mensagem, total de linhas e total de blocos da mensagem e o número de bits utilizados no final da mensagem para padding.

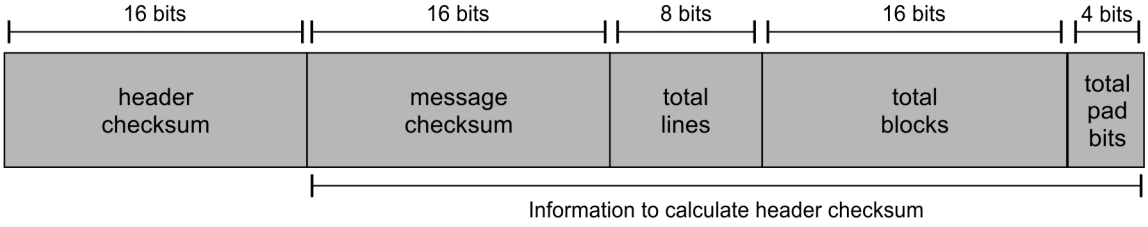

Figura 3.11: Cabeçalho em Reconhecimento de Padrões

```
len_mensagem = 96

bits_linha = blocos_linha * bits_bloco
<=>
bits_linha = 28

numero_linhas = len_mensagem/bits_linha + (len_mensagem%bits_linha > 0)
<=>
numero_linhas = 4
```

```
num_bits_padding = blocos_linha * numero_linhas - len_mensagem
<=>
num_bits_padding = 16

total_blocos = blocos_linha * numero_linhas
<=>
total_blocos = 56
```

Figura 3.12: Cabeçalho em Reconhecimento de Padrões para a frase "HELLO WORLD!"

A Figura 3.12 ilustra o cabeçalho para este documento de exemplo, as restantes quatro linhas são compostas com a mensagem e terminadas com os bits de padding, conforme ilustrado na Figura 3.13. O documento final encontra-se ilustrado na Figura 3.14

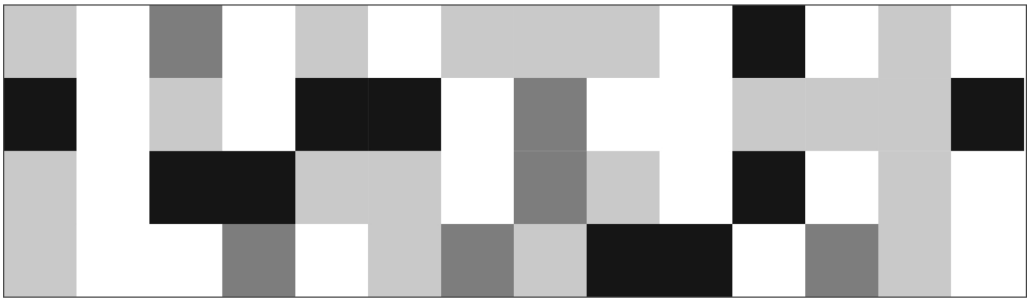

Figura 3.13: Mensagem em Reconhecimento de Padrões para a frase "HELLO WORLD!"

3.5.2 Processo de Descodificação

Esta abordagem foi implementada com o auxílio de uma API open source para computer vision e machine learning - OpenCV[1].

O processo começa por tentar identificar quadriláteros e, em cada um que encontre, é feito um ajuste na sua dimensão e forma para que fique proporcional com a forma de uma folha A4. A câmara utilizada não pode caputar imagens além de 480px de altura, no

[1] OpenCV - `https://opencv.org`

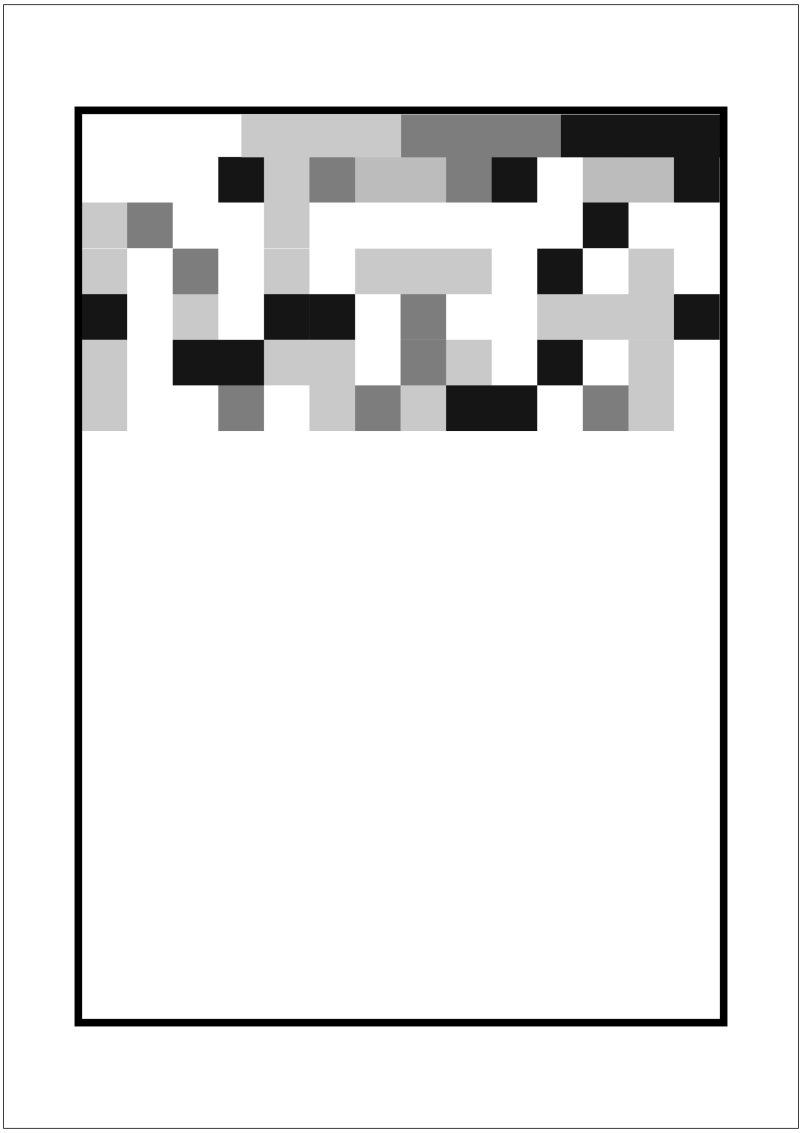

Figura 3.14: Documento a imprimir em Reconhecimento de Padrões para a frase "HELLO WORLD!"

entanto para este trabalho optou-se por redimensionar a imagem capturada para 1980px de largura por 3100px de altura. Dessa imagem são removidos 10px de cada lado para eliminar o contorno criado no documento. A imagem final é segmentada em quatro linhas, três para o cabeçalho, com 140px de altura cada e uma para o corpo da mensagem, com 2660px de altura.

É então iniciado o parsing do cabeçalho, que começa por identificar a quantidade de tons utilizados na primeira linha, que irá influenciar o valor de bits armazenado em cada um dos pseudo-píxeis ($2\hat{X}$). É feito o varrimento píxel a píxel de cada quadro para identificar a média das suas cores. As duas linhas seguintes são segmentadas em 14 colunas, os 28

blocos de 140px cada são também processados píxel a píxel e calculada a média da sua cor, que posteriormente é comparada com os valores do cabeçalho, o valor mais aproximado é o considerado para atribuição da informação contida. No final do processamento das duas linhas, os valores binários são concatenados e é validado o cabeçalho, onde os bits 0:15 constituem o CRC16 do cabeçalho, dos restantes bits presentes é calculado o CRC16, se os valores não coincidirem, o processamento da forma é descartado e o processo passa à próxima forma a identificar.

Quando o valor CRC16 do cabeçalho coincide, são processados os seus restantes bits, 16:31 consta o CRC16 da totalidade da mensagem, os bits 32:39 contêm a totalidade de linhas que compõem o documento, finalmente os bits 40:55 a totalidade de blocos a considerar no documento.

Terminado o processamento do cabeçalho é possível segmentar o restante da imagem dividindo a totalidade dos blocos pela quantidade de linhas, obtendo assim o valor da largura de cada pseudo pixel. Divide-se então a altura da área remanescente da imagem (2.660px) pelo valor da largura dos blocos, permitindo efetuar a correcta segmentação das linhas. Após esta segmentação são processados o número de blocos indicados no cabeçalho e os seus bits concatenados, terminada a concatenação a mensagem em bits é decifrada e apresentada a mensagem ao utilizador.

Capítulo 4

Avaliação

Neste capítulo é feita uma avaliação global do trabalho e das opções feitas na implementação do sistema proposto.

4.1 Equipamento Utilizado

Foram utilizados óculos EPSON MOVERIO BT-200, modelo com Sistema Operativo Android, ecrã transparente e visor de 0.42 polegadas que permite uma reprodução de 24 bits de cores e taxa de atualização de 60Hz. A sua câmara é de qualidade VGA (640x480 pixeis), muito sensível a variações de luminosidade, com forte impacto negativo na qualidade das imagens capturadas. Vem equipado com um CPU TI OMAP 4460 1.2GHz Dual Core, 1 GB de RAM e memória interna de 8GB.

À data, a versão mais recente, BT-40S, apresenta uma melhoria significativa na câmara. É possível capturar imagens com qualidade HDMI (1920x1080 pixeis). Vem equipado com 4 GB de RAM e 64GB de memória interna.

4.2 Reconhecimento Óptico de Caracteres

As características da câmara utilizada invalidam algumas opções, por exemplo, se utilizarmos 30 caracteres por linha, teriam na imagem processada 17 píxeis de dimensão, já descontando 130 pixeis para as margens da folha e espaçamento entre caracteres. Esta dimensão (17 pixeis) torna praticamente impossível o reconhecimento dos caracteres[1].

Numa primeira abordagem optou-se pelo reconhecimento de toda a folha. Devido à fraca qualidade da câmara presente no equipamento utilizado, foi necessário optimizar esta captura passando a fazer o processamento linha a linha. Esta abordagem limita

[1]Minimum Character Size for OCR - `http://stackoverflow.com/questions/27489735/minimum-character-size-for-ocr` é referenciado que para o reconhecimento de um carácter a altura mínima deverá ser de 20 pixels

a dimensão de dados possível de representar pela mesma quantidade de caracteres, no entanto apresenta um impacto bastante significativo na eficácia do processo.

Para aumentar a capacidade de armazenamento de uma mensagem é necessária a utilização de várias folhas. Neste trabalho dividimos o documento impresso em duas áreas: cabeçalho e corpo (header e body). O cabeçalho é constituído, por uma linha.

No sentido de optimizar o espaço disponível para armazenar os dados da mensagem, deve ocupar-se o menor espaço possível com checksums. É necessário encontrar um bom balanceamento entre o tamanho destes controlos e as colisões que possam ocorrer.

Com o avanço da tenologia, é esperado que num futuro próximo, esta qualidade aumente nos equipamentos disponibilizados ao público, como telemóveis, tablets ou óculos de realidade aumentada. Com estes avanços a quantidade de diferentes caracteres possíveis de utilizar aumentará, o que se traduzirá num forte aumento no desempenho deste sistema.

No sistema implementado foram utilizados 32 caracteres (Tabela 3.1) do alfabeto Inglês, o que permite um armazenamento individual de 5 bits.

A utilização da biblioteca Tessaract mostrou-se não ser a ideal para este trabalho, pois no processo de reconhecimento, o algoritmo tenta adivinhar a palavra presente. Como as sequências de caracteres não têm qualquer correspondência com palavras existentes, esta API, por vezes, substitui alguns dos caracteres. Neste trabalho ultrapassou-se esse problema adicionando pontos finais após cada carácter.

Uma abordagem para ultrapassar este problema pode passar pela utilização de palavras, em vez de apenas caracteres. Esta abordagem resolveria a dificuldade do Tesseract e daria também uma maior discrição ao documento codificado, no entanto a quantidade de informação possível de armazenar por página iria reduzir.

Foram realizadas algumas experiências desta abordagem , tendo-se verificado ser vantajosa a utilização da API ABBYY, como alternativa ao Tessaract. Esta API não apresentou os mesmos problemas, no entanto surgiram outras dificuldades, como a área possível de reconhecimento e alguns problemas na gestão da memória do equipamento.

A Tabela 4.1 apresenta uma simulação da quantidade de informação possível de armazenar de acordo com a dimensão do conjunto de caracteres. Por exemplo, utilizando caracteres Chineses podemos ter um conjunto com 2,235 elementos em Simplified Chinese[2] ou 7,344 elementos em Traditional Chinese[3].

4.3 Reconhecimento de Padrões

Esta abordagem consiste no armazenamento da informação em valores RGB. Estima-se que, de futuro, a qualidade das câmaras neste tipo de equipamentos permita reconhecer a cor de um píxel numa imagem capturada. Nessa altura será possível utilizar imagens com grafismo complexo para esta abordagem.

[2]simplified chinese - `http://www.loria.fr/~roegel/chinese/list-simp-char.pdf`
[3]traditional chinese - `http://www.sayjack.com/traditional/chinese/characters/`

N. DE CARACTERES	LINHAS POR FOLHA	CARACTERES POR LINHA	BYTES ARMAZENADOS
32	15	15	80
	40	40	840
	90	90	4.702
128	15	15	136
	40	40	1.240
	90	90	6.727
256	15	15	165
	40	40	1.440
	30	30	7.740
2.235	15	15	252
	40	40	2.065
	90	90	10.905
7.287	15	15	300
	40	40	2.406
	90	90	12.631

Tabela 4.1: Quantidade de informação possível de armazenar numa página de acordo com o número de caracteres utilizados na operação de codificação

As condições de luminosidade do local onde a captura é feita e a capacidade da câmara em lidar com ambientes de fraca luminosidade são muito importantes para a eficácia do sistema. A eventual distorção causada pela lente da câmara ou curvatura da folha devido ao seu manuseamento podem causar um desiquilíbrio no seu conteúdo inviabilizando assim a descodificação da mensagem. Outro obstáculo à eficácia do sistema é a variação de luminosidade como reflexos de luz que podem ser minorados através da utilização de papel anti reflexo. As sombras também podem alterar significativamente os valores das cores existentes.

Na Tabela 4.2 é apresentada uma simulação da quantidade de informação possível de armazenar de acordo com o tamanho e quantidade de cores e tons utilizados.

CORES	TONS	BLOCOS/LINHA	TAMANHO BLOCO(mm)	BYTES ARMAZENADOS
1	4	10	20.8	33.89
		30	6,93	305
		50	4,16	847
		100	2,08	3.389
	8	10	20.80	51
		30	6,93	458
		50	4,16	1.271
		100	2,08	5.084
	16	10	20,80	68
		30	6,93	610
		50	4,16	1.695
		100	2,08	6.779
3	4	10	20,80	102
		30	6,93	915
		50	4,16	2.542
		100	2,08	10.168
	8	10	20,80	153
		30	6,93	1.373
		50	4,16	3.813
		100	2.08	15.252
	16	10	20,80	203
		30	6,93	1.830
		50	4,16	5.084
		100	2.08	20.337

Tabela 4.2: Quantidade de dados possível de armazenar numa página, de acordo com as cores, tons e dimensão dos blocos

Capítulo 5

Conclusão

Neste trabalho comprova-se que é possível desenvolver um sistema que cifre e codifique a informação a imprimir em papel. Permitindo a sua captura, descodificação e decifra, apresentando o seu resultado no visor de um dispositivo de realidade aumentada.

As metodologias apresentadas são também úteis na transmissão discreta de conteúdo classificado. É possível a utilização online e offline, sendo que a versão online permite um rastreamento dos acessos. Sendo portanto este sistema capaz de proteger informação classificada em documentos impressos. Com a presente solução é possível utilizar tanto texto, como fotos, áudio ou vídeo, transmitidos através de documentos impressos.

São apresentadas duas abordagens para atingir o objetivo: Reconhecimento Óptico de Caracteres e Reconhecimento de Padrões. Em ambas as abordagens foram identificadas algumas dificuldades, em grande parte pela fraca qualidade das imagens capturadas pela câmara do equipamento utilizado.

Relativamente ao Reconhecimento Óptico de Caracteres, há que optar por alguma solução alternativa à API Tesseract ou ABBYY. No que concerne ao Reconhecimento de Padrões a maior dificuldade prende-se com as variações de cores no ambiente particularmente sombras, daí surgiu a necessidade de calcular médias dos blocos de cores para que a solução possa adaptar-se automaticamente a esses ambientes.

Algumas ameaças a este tipo de sistemas, identificados pelo International Telecommunication Union - ITU, na sua recomendação F.400/X.400, são mitigadas em grande parte pela utilização de criptografia assimétrica. O sistema proposto mitiga a ameaça do espião de ombro, impossibilitando que o conteúdo seja visualizado por outra pessoa que não o verdadeiro destinatário da mensagem.

Existe trabalho a fazer para optimizar a solução no sentido de o tornar mais discreto, nomeadamente a utilização de texto normal na codificação ou, no caso da abordagem de Reconhecimento de Padrões, a utilização de fotos.

Em 2020 surgiu a primeira lente de contacto com realidade aumentada[47][49]. É de prever que num futuro próximo possam existir equipamentos deste género, equipados com câmaras de alta qualidade que permitam um processamento mais avançado e eficaz.

Também a autenticação biométrica neste tipo de equipamentos será um salto importante para este tipo de soluções.

Bibliografia

[1] Ross J Anderson e Fabien A P Petitcolas. ≪On the limits of steganography≫. Em: *Selected Areas in Communications, IEEE Journal on* 16.4 (1998), pp. 474–481 (citado na página 7).

[2] Sarah J Andrabi, Michael K Reiter e Cynthia Sturton. ≪Usability of augmented reality for revealing secret messages to users but not their devices≫. Em: *Eleventh Symposium On Usable Privacy and Security ({SOUPS} 2015)*. 2015, pp. 89–102 (citado na página 3).

[3] T Anuradha e K Usha Rani. ≪Comparative Analysis on Visual Cryptographic Schemes≫. Em: *International Journal of Computer Science and Mobile Computing* 3 (2014), pp. 134–140 (citado na página 6).

[4] Ali Mir Arif Mir Asif et al. ≪An Overview and Applications of Optical Character Recognition≫. Em: *International Journal of Advance Research In Science And Engineering* 3.7 (2014), pp. 261–274 (citado nas páginas 5, 8).

[5] S Baird Henry e Karl Tombre. ≪The Evolution of Document Image Analysis≫. Em: *Handbook of Document Image Processing and Recognition*. Ed. por David Doermann e Karl Tombre. Springer London, 2014, pp. 63–71. ISBN: 978-0-85729-858-4. DOI: 10.1007/978-0-85729-859-1_43. URL: http://dx.doi.org/10.1007/978-0-85729-859-1%7B%5C_%7D43 (citado nas páginas 7, 8).

[6] Tianyou Bao e Hurriyet Ok. ≪Secure Augmented Reality (AR) for Telehealth and Emergency Medical Services (EMS): A Survey≫. Em: (2021) (citado na página 3).

[7] Bernd Borchert e Klaus Reinhardt. ≪Applications of Visual Cryptography≫. Em: *Visual Cryptography and Secret Image Sharing* 4 (2011), p. 329 (citado na página 7).

[8] Presidência do Conselho de Ministros. *Normas para a Segurança Nacional, salvaguarda e defesa das matérias classificadas, segurança industrial, tecnológica e de investigação — SEGNAC2*. 1989. URL: https://dre.pt/web/guest/pesquisa/-/search/549396/details/normal?q=segnac2 (citado na página 4).

[9] Presidência do Conselho de Ministros. *Normas para a Segurança Nacional, Salvaguarda e Defesa das Matérias Classificadas, Segurança Informática — SEGNAC4*. 1990. URL: https://dre.pt/web/guest/pesquisa/-/search/307435/details/normal?q=segnac4 (citado na página 4).

[10] Luciana da Silveira Espindola. *Um Estudo sobre Modelos Ocultos de Markov HMM-Hidden Markov Model*. 2010 (citado na página 12).

[11] Pushkar Dixit, Nishant Singh e Jay Prakash Gupta. «Robust Lossless Semi Fragile Information Protection in Images». Em: *International Journal of Artificial Intelligence and Interactive Multimedia* 2.6 (2014), pp. 75–88 (citado na página 8).

[12] Øivind Due Trier, Anil K. Jain e Torfinn Taxt. «Feature extraction methods for character recognition-A survey». Em: *Pattern Recognition* 29.4 (1996), pp. 641–662. ISSN: 0031-3203. DOI: https://doi.org/10.1016/0031-3203(95)00118-2. URL: https://www.sciencedirect.com/science/article/pii/0031320395001182 (citado na página 10).

[13] Marc Dymetman e Max Copperman. «Intelligent paper». Em: *Electronic Publishing, Artistic Imaging, and Digital Typography*. Ed. por RogerD. Hersch, Jacques Andre e Heather Brown. Vol. 1375. Lecture Notes in Computer Science. Springer Berlin Heidelberg, 1998, pp. 392–406. ISBN: 978-3-540-64298-5. DOI: 10.1007/BFb0053286. URL: http://dx.doi.org/10.1007/BFb0053286 (citado na página 8).

[14] Mansoor Ebrahim, Shujaat Khan e UmerBin Khalid. «Symmetric Algorithm Survey: A Comparative Analysis». Em: *CoRR* abs/1405.0398 (2014). arXiv: 1405.0398. URL: http://arxiv.org/abs/1405.0398 (citado na página 5).

[15] Andrea G Forte et al. «EyeDecrypt—Private interactions in plain sight». Em: *International Conference on Security and Cryptography for Networks*. Springer. 2014, pp. 255–276 (citado na página 3).

[16] Ethan Gaebel et al. «Looks good to me: Authentication for augmented reality». Em: *Proceedings of the 6th International Workshop on Trustworthy Embedded Devices*. 2016, pp. 57–67 (citado na página 13).

[17] «Image encryption based on diffusion and multiple chaotic maps». Em: 3.2 (2011), pp. 181–194 (citado na página 7).

[18] A Jain et al. «Text detection and recognition in natural scenes and consumer videos». Em: *Acoustics, Speech and Signal Processing (ICASSP), 2014 IEEE International Conference on*. 2014, pp. 1245–1249. DOI: 10.1109/ICASSP.2014.6853796 (citado na página 10).

[19] Yujin Jung et al. ≪An eye detection method robust to eyeglasses for mobile iris recognition≫. Em: *Expert Systems with Applications* 67 (2017), pp. 178–188. ISSN: 0957-4174. DOI: https://doi.org/10.1016/j.eswa.2016.09.036. URL: http://www.sciencedirect.com/science/article/pii/S0957417416305206 (citado na página 13).

[20] Dongik Kim et al. ≪An empirical study on iris recognition in a mobile phone≫. Em: *Expert Systems with Applications* 54 (2016), pp. 328–339. ISSN: 0957-4174. DOI: https://doi.org/10.1016/j.eswa.2016.01.050. URL: http://www.sciencedirect.com/science/article/pii/S0957417416300148 (citado na página 13).

[21] Douglas Kunda e Mumbi Chishimba. ≪A Survey of Android Mobile Phone Authentication Schemes≫. Em: *Mobile Networks and Applications* (ago. de 2018). ISSN: 1572-8153. DOI: 10.1007/s11036-018-1099-7. URL: https://doi.org/10.1007/s11036-018-1099-7 (citado na página 13).

[22] Seong-Whan Lee, Dong-June Lee e Hee-Seon Park. ≪A new methodology for gray-scale character segmentation and recognition≫. Em: *Pattern Analysis and Machine Intelligence, IEEE Transactions on* 18.10 (1996), pp. 1045–1050. ISSN: 0162-8828. DOI: 10.1109/34.541415 (citado na página 9).

[23] Y. Leydier et al. ≪libcrn, an Open-Source Document Image Processing Library≫. Em: *2016 15th International Conference on Frontiers in Handwriting Recognition (ICFHR)*. Ago. de 2016, pp. 211–215. DOI: 10.1109/ICFHR.2016.0049 (citado na página 8).

[24] Yung-Hui Li e Po-Jen Huang. ≪An Accurate and Efficient User Authentication Mechanism on Smart Glasses Based on Iris Recognition≫. Em: *Mobile Information Systems* 2017 (2017), p. 14. DOI: https://doi.org/10.1155/2017/1281020 (citado na página 13).

[25] V Manikandan et al. ≪An enhanced algorithm for Character Segmentation in document image processing≫. Em: *Computational Intelligence and Computing Research (ICCIC), 2010 IEEE International Conference on*. 2010, pp. 1–5. DOI: 10.1109/ICCIC.2010.5705728 (citado na página 9).

[26] Susan Maret e Jan Goldman. *Government secrecy*. Vol. 19. Emerald Group Publishing, 2011 (citado na página 3).

[27] Omid Mirzaei, Mahdi Yaghoobi e Hassan Irani. ≪A new image encryption method: parallel sub-image encryption with hyper chaos≫. Em: *Springer* (2011) (citado na página 7).

[28] Dr Dhirendra Mishra e Poonam Gupta. ≪Encryption techniques for security of images≫. Em: *International Journal of Engineering Science & Technology* 6.1 (2014) (citado nas páginas 5, 26).

[29] S Mori, C Y Suen e K Yamamoto. ≪Historical review of OCR research and development≫. Em: *Proceedings of the IEEE* 80.7 (jul. de 1992), pp. 1029–1058. ISSN: 0018-9219. DOI: 10.1109/5.156468 (citado na página 12).

[30] Muhammad Faheem Mushtaq et al. ≪A survey on the cryptographic encryption algorithms≫. Em: *International Journal of Advanced Computer Science and Applications* 8.11 (2017), pp. 333–344 (citado na página 5).

[31] Moni Naor e Adi Shamir. ≪Visual cryptography≫. Em: *Advances in Cryptology - EUROCRYPT'94*. Ed. por Alfredo De Santis. Vol. 950. Lecture Notes in Computer Science. Springer Berlin Heidelberg, 1995, pp. 1–12. ISBN: 978-3-540-60176-0. DOI: 10.1007/BFb0053419. URL: http://dx.doi.org/10.1007/BFb0053419 (citado na página 6).

[32] Michael A Nielsen. *Neural Networks and Deep Learning*. Ed. por Determination Press. \url{http://neuralnetworksanddeeplearning.com/}, 2015 (citado na página 12).

[33] Luiz Eduardo Soares de Oliveira e Marisa Emika Morita. ≪Introduçao aos modelos escondidos de markov (hmm)≫. Em: (2000) (citado na página 13).

[34] OpenCV. *Introduction to Support Vector Machines* (citado na página 12).

[35] Chirag Patel, Atul Patel e Dipti Shah. ≪A Review of Character Segmentation Methods≫. Em: *International Journal of Current Engineering and Technology* 3.5 (2013), pp. 2075–2078 (citado na página 9).

[36] P D Ratna Raju e Priyadarshini Instt Of Tech&Science. ≪An introduction to different types ov visual cryptography schemes≫. Em: () (citado na página 6).

[37] P S Revenkar, Anisa Anjum e W Z Gandhare. ≪Survey of visual cryptography schemes≫. Em: *International Journal of Security and Its Applications* 4.2 (2010), pp. 49–56 (citado na página 6).

[38] Simon Singh. *The Code Book: How to Make It, Break It, Hack It, Or Crack it*. Delacorte Press, 2002 (citado na página 3).

[39] R. Smith. ≪An Overview of the Tesseract OCR Engine≫. Em: *Ninth International Conference on Document Analysis and Recognition (ICDAR 2007)*. Vol. 2. Set. de 2007, pp. 629–633. DOI: 10.1109/ICDAR.2007.4376991 (citado na página 25).

[40] Ray Smith. ≪An Overview of the Tesseract OCR Engine≫. Em: *Proc. Ninth Int. Conference on Document Analysis and Recognition (ICDAR)*. 2007, pp. 629–633 (citado na página 8).

[41] Ray Smith. ≪An overview of the Tesseract OCR engine≫. Em: *Ninth international conference on document analysis and recognition (ICDAR 2007)*. Vol. 2. IEEE. 2007, pp. 629–633 (citado na página 8).

[42] Narasimha Reddy Soora e Parag S. Deshpande. «Review of Feature Extraction Techniques for Character Recognition». Em: *IETE Journal of Research* 64.2 (2018), pp. 280–295. DOI: 10.1080/03772063.2017.1351323. eprint: https://doi.org/10.1080/03772063.2017.1351323. URL: https://doi.org/10.1080/03772063.2017.1351323 (citado na página 10).

[43] Mansi S Subhedar e Vijay H Mankar. «Current status and key issues in image steganography: A survey». Em: *Computer Science Review* 13-14.0 (2014), pp. 95–113. ISSN: 1574-0137. DOI: http://dx.doi.org/10.1016/j.cosrev.2014.09.001. URL: http://www.sciencedirect.com/science/article/pii/S1574013714000136 (citado na página 7).

[44] Ahmad P Tafti et al. «OCR as a service: an experimental evaluation of Google Docs OCR, Tesseract, ABBYY FineReader, and Transym». Em: *International Symposium on Visual Computing*. Springer. 2016, pp. 735–746 (citado na página 8).

[45] ITU - International Tellecommunication Union. *F.400/X.400 - Message Handling Systems*. Consultado em 2021/08/30. 1999. URL: https://www.itu.int/rec/dologin_pub.asp?lang=e&id=T-REC-F.400-199906-I!!PDF-E&type=items (citado nas páginas 3, 17).

[46] N Vishwanath et al. «A hybrid Indian license plate character segmentation algorithm for automatic license plate recognition system». Em: *Computational Intelligence Computing Research (ICCIC), 2012 IEEE International Conference on*. 2012, pp. 1–4. DOI: 10.1109/ICCIC.2012.6510322 (citado na página 9).

[47] Kaixuan Wang et al. «Nanowire-Based Soft Wearable Human–Machine Interfaces for Future Virtual and Augmented Reality Applications». Em: *Advanced Functional Materials* 31.39 (2021), p. 2008347. DOI: https://doi.org/10.1002/adfm.202008347. eprint: https://onlinelibrary.wiley.com/doi/pdf/10.1002/adfm.202008347. URL: https://onlinelibrary.wiley.com/doi/abs/10.1002/adfm.202008347 (citado na página 37).

[48] T. C. Wei, U. U. Sheikh e A. A. A. Rahman. «Improved optical character recognition with deep neural network». Em: *2018 IEEE 14th International Colloquium on Signal Processing Its Applications (CSPA)*. Mar. de 2018, pp. 245–249. DOI: 10.1109/CSPA.2018.8368720 (citado na página 8).

[49] Mike Wiemer. «Mojo Vision: Designing Anytime, Anywhere AR Contact Lenses with Mojo Lens». Em: *SPIE AVR21 Industry Talks II*. Ed. por Conference Chair. Vol. 11764. International Society for Optics e Photonics. SPIE, 2021. DOI: 10.1117/12.2597476. URL: https://doi.org/10.1117/12.2597476 (citado na página 37).

[50] Wei-Qi Yan, Duo Jin e M S Kankanhalli. ≪Visual cryptography for print and scan applications≫. Em: *Circuits and Systems, 2004. ISCAS '04. Proceedings of the 2004 International Symposium on*. Vol. 5. 2004, V–572–V–575 Vol.5. DOI: 10.1109/ISCAS.2004.1329727 (citado na página 7).

[51] Guodong Ye e Junwei Zhou. ≪A block chaotic image encryption scheme based on self-adaptive modelling≫. Em: *Applied Soft Computing* 22.0 (2014), pp. 351–357. ISSN: 1568-4946. DOI: http://dx.doi.org/10.1016/j.asoc.2014.05.025. URL: http://www.sciencedirect.com/science/article/pii/S156849461400252X (citado na página 7).

[52] Hongwei Ying, Jiatao Song e Xiaobo Ren. ≪Character segmentation for license plate by the separator symbol's frame of reference≫. Em: *Information Networking and Automation (ICINA), 2010 International Conference on*. Vol. 1. 2010, pp. V1–438–V1–442. DOI: 10.1109/ICINA.2010.5636522 (citado nas páginas 9, 10).

[53] Xuanping Zhang, Zhongmeng Zhao e Jiayin Wang. ≪Chaotic image encryption based on circular substitution box and key stream buffer≫. Em: *Signal Processing - Image Communication* (2014). DOI: http://dx.doi.org/10.1016/j.image.2014.06.012i (citado na página 7).