

UNIVERSIDADE FEDERAL DE GOIÁS
PROGRAMA DE PÓS-GRADUAÇÃO EM
ENGENHARIA ELÉTRICA
E DE COMPUTAÇÃO

APLICAÇÃO DE TRANSFORMAÇÃO CONFORME EM
CODIFICAÇÃO E DECODIFICAÇÃO DE IMAGENS

Alan Henrique Ferreira Silva

[UFG] & [EMC]
[Goiânia - Goiás - Brasil]
13 de julho de 2016

UNIVERSIDADE FEDERAL DE GOIÁS
PROGRAMA DE PÓS-GRADUAÇÃO EM
ENGENHARIA ELÉTRICA
E DE COMPUTAÇÃO

APLICAÇÃO DE TRANSFORMAÇÃO CONFORME EM
CODIFICAÇÃO E DECODIFICAÇÃO DE IMAGENS

Alan Henrique Ferreira Silva

Dissertação apresentada à Banca Examinadora como exigência parcial para a obtenção do título de Mestre em Engenharia Elétrica e de Computação pela Universidade Federal de Goiás (UFG), Escola de Engenharia Elétrica, Mecânica e de Computação (EMC), sob a orientação do Prof. Dr. Wesley Pacheco Calixto.

[UFG] & [EMC]
[Goiânia - Goiás - Brasil]
13 de julho de 2016

Dados Internacionais de Catalogação na Publicação (CIP)
Sistemas da Bibliotecas da UFG, GO - Brasil

F368t Silva, Alan Henrique Ferreira.

Aplicação de transformação conforme em codificação e decodificação de imagens [manuscrito]/ Alan Henrique Ferreira Silva. – [Goiânia - Goiás - Brasil]: [UFG] & [EMC], 13 de julho de 2016.

82 f. : il.

Orientador: Prof. Dr. Wesley Pacheco Calixto.

Dissertação (Mestrado) - Universidade Federal de Goiás - UFG, Escola de Engenharia Elétrica, Mecânica e de Computação - EMC, Goiânia

Bibliografia.

Inclui siglas, abreviaturas, símbolos, lista de figuras.

1.Transformação Conforme. 2.Codificação e Decodificação de Imagem. 3.Criptografia Visual. 4.Decodificação de imagem impressa. 5.Segurança de Dados. I. Calixto, Wesley Pacheco. II. Título

CDU 621.3

Copyright © 13 de julho de 2016 by Federal University of Goias - UFG, Brazil. No part of this publication may be reproduced, stored in a retrieval system, or transmitted in any form or by any means, electronic, mechanical, photocopying, microfilming, recording or otherwise, without written permission from the Library of UFG, with the exception of any material supplied specifically for the purpose of being entered and executed on a computer system, for exclusive use of the reader of the work.

TERMO DE CIÊNCIA E DE AUTORIZAÇÃO PARA DISPONIBILIZAR AS TESES E DISSERTAÇÕES ELETRÔNICAS (TEDE) NA BIBLIOTECA DIGITAL DA UFG

Na qualidade de titular dos direitos de autor, autorizo a Universidade Federal de Goiás (UFG) a disponibilizar, gratuitamente, por meio da Biblioteca Digital de Teses e Dissertações (BDTD/UFG), sem ressarcimento dos direitos autorais, de acordo com a Lei nº 9610/98, o documento conforme permissões assinaladas abaixo, para fins de leitura, impressão e/ou *download*, a título de divulgação da produção científica brasileira, a partir desta data.

1. Identificação do material bibliográfico: **Dissertação** **Tese**

2. Identificação da Tese ou Dissertação

Autor (a):	Alan Henrique Ferreira Silva		
E-mail:	alanhfs@gmail.com		
Seu e-mail pode ser disponibilizado na página?	<input checked="" type="checkbox"/> Sim	<input type="checkbox"/> Não	
Vínculo empregatício do autor			
Agência de fomento:		Sigla:	
País:	UF:	CNPJ:	
Título:	Aplicação de transformação conforme em codificação e decodificação de imagens		
Palavras-chave:	1.Transformação Conforme. 2.Codificação e Decodificação de Imagem. 3. Criptografia Visual. 4.Decodificação de imagem impressa. 5.Segurança de Dados.		
Título em outra língua:	Conformal mapping applied to images encoding and decoding		
Palavras-chave em outra língua:	1.Conformal Mapping. 2.Image encode and decoding. 3.Visual Cryptography. 4.Decoding printed image 5.Data security		
Área de concentração:	Engenharia Elétrica e de Computação		
Data defesa: (dd/mm/aaaa)	31/03/2016		
Programa de Pós-Graduação:	Programa de Pós-Graduação em Engenharia Elétrica e de Computação		
Orientador (a):	Wesley Pacheco Calixto		
E-mail:	wpcalixto@gmail.com		
Co-orientador (a):*			
E-mail:			

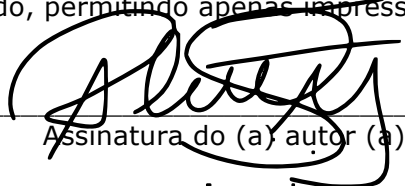
*Necessita do CPF quando não constar no SisPG

3. Informações de acesso ao documento:

Concorda com a liberação total do documento SIM NÃO¹

Havendo concordância com a disponibilização eletrônica, torna-se imprescindível o envio do(s) arquivo(s) em formato digital PDF ou DOC da tese ou dissertação.

O sistema da Biblioteca Digital de Teses e Dissertações garante aos autores, que os arquivos contendo eletronicamente as teses e ou dissertações, antes de sua disponibilização, receberão procedimentos de segurança, criptografia (para não permitir cópia e extração de conteúdo, permitindo apenas impressão fraca) usando o padrão do Acrobat.



 Assinatura do (a) autor (a)

Data: 12/07/2016

¹ Neste caso o documento será embargado por até um ano a partir da data de defesa. A extensão deste prazo suscita justificativa junto à coordenação do curso. Os dados do documento não serão disponibilizados durante o período de embargo.



MINISTÉRIO DA EDUCAÇÃO
UNIVERSIDADE FEDERAL DE GOIÁS
ESCOLA DE ENGENHARIA ELÉTRICA, MECÂNICA E DE COMPUTAÇÃO
COORDENAÇÃO DE PÓS-GRADUAÇÃO



FOLHA DE APROVAÇÃO

"Aplicação de Transformação Conforme em Codificação e Decodificação de Imagens"

ALAN HENRIQUE FERREIRA SILVA

Dissertação defendida e aprovada pela banca examinadora constituída pelos senhores:



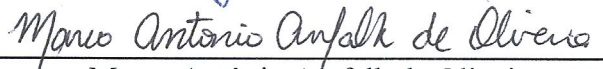
Wesley Pacheco Calixto – Orientador (IFG)



José Luiz de Freitas Júnior – PUC/FATESG-Go



Jesus Carlos da Mota – IME/UFG



Marco Antônio Assfalk de Oliveira – EMC/UFG

Goiânia, 31 de março de 2016

*“Ando devagar porque já tive pressa
E levo esse sorriso porque já chorei demais.”*

ALMIR SATER E RANATO TEIXEIRA
em “Tocando em frente”.

*As mulheres de minha vida: Marilene, Alana, Emanuele e
Helena.*

AGRADECIMENTOS

Mesmo percorrendo caminhos desconhecidos e cheios de obstáculos, encontrei e pude contar com a bondade de muitas pessoas. Apesar dos momentos de incerteza, estas pessoas sempre estiveram ao meu lado me auxiliando durante o percurso para que pudesse chegar ao final. Meus agradecimentos aos que contribuíram indiretamente na construção e finalização deste trabalho. Meus agradecimentos à Coordenação de Aperfeiçoamento de Pessoal de Nível Superior (CAPES) pelo suporte financeiro. Meus agradecimentos ao meu orientador e amigo Pacheco pela dedicação e orientação. Meus agradecimentos à Dona Maria pelo apoio e dedicação. Meus agradecimentos à minha esposa Alana pela dedicação, ajudas e conselhos. Meus infinitos agradecimentos à minha mãe por ter dedicado a saúde para ensinar os verdadeiros valores da vida e a importância dos estudos e da educação de qualidade.

RESUMO

Este trabalho propõe método que utiliza transformações conformes para codificar e decodificar imagens. As transformações conformes modificam os domínios em estudos sem modificar as características físicas entre eles. As imagens reais são transformadas entre estes domínios utilizando chaves, que são funções transformadoras. O diferencial desta metodologia é a capacidade de transportar a mensagem contida na imagem em meio impresso codificado e depois, decodificá-la.

CONFORMAL MAPPING APPLIED TO IMAGES ENCODING AND DECODING

ABSTRACT

This work proposes method to encode and decode images using conformal mapping. Conformal mapping modifies domains without modifying physical characteristics between them. Real images are processed between these domains using encoding keys, also called transforming functions. The advantage of this methodology is the ability to carry the message as an encoded image in printed media for posterior-decoding.

SUMÁRIO

Pág.

LISTA DE FIGURAS

LISTA DE SÍMBOLOS

LISTA DE ABREVIATURAS E SIGLAS

CAPÍTULO 1 INTRODUÇÃO	23
CAPÍTULO 2 TRANSFORMAÇÕES CONFORMES	27
2.1 Cartografia	27
2.2 Números complexos	28
2.2.1 História	28
2.2.2 Definição	29
2.2.3 Função complexa	30
2.3 Transformações Conformes	31
2.3.1 Funções transformadoras elementares	32
2.3.1.1 Translação	32
2.3.1.2 Rotação	33
2.3.1.3 Dilatação ou Contração	34
2.3.1.4 Inversão	34
2.3.1.5 Linear	35
2.3.1.6 Bilinear	36
2.4 Considerações finais	36
CAPÍTULO 3 IMAGENS	39
3.1 Composição de imagem digital	39
3.2 Criptografia de imagens	40
3.3 Processo de codificação e decodificação de imagem	44
3.4 Considerações finais	46
CAPÍTULO 4 METODOLOGIA	49
4.1 Aquisição de imagem	49
4.2 Escolha da função conforme transformadora e codificação de imagem	49

4.2.1	Processo de decodificação	52
4.3	Considerações finais	53
CAPÍTULO 5 RESULTADOS		55
5.1	Segurança da Chave	55
5.2	O Software	56
5.3	Estudo de Caso 1: Codificação e Decodificação de imagens digitais	58
5.3.1	Codificação	59
5.3.2	Decodificação	60
5.3.3	Comparativo entre imagens originais e decodificadas	62
5.4	Estudo de Caso 2: codificação e decodificação de imagens com inserção de ruídos	64
5.5	Estudo de Caso 3: codificação e decodificação de imagens impressas	67
CAPÍTULO 6 CONCLUSÃO		71
6.1	Contribuições do Trabalho	71
6.2	Sugestões para Trabalhos Futuros	73
REFERÊNCIAS BIBLIOGRÁFICAS		75
GLOSSÁRIO		81

LISTA DE FIGURAS

	<u>Pág.</u>
2.1	Conceito de mapa conforme. 27
2.2	Projeção de pontos da esfera no plano. 28
2.3	Conjuntos numéricos. 30
2.4	Plano complexo. 30
2.5	Curvas A_1 e A_2 com suas respectivas imagens e o ângulo α preservado. . . 32
2.6	Domínio e Contradomínio. 33
2.7	Função transformadora por translação. 33
2.8	Função transformadora por rotação. 34
2.9	Função transformadora por dilatação e por contração. 35
2.10	Função transformadora por inversão. 35
2.11	Função transformadora linear. 36
3.1	Composição do pixel para esquema de cores <i>RGB</i> 39
3.2	Posicionamento de <i>pixels</i> no plano- <i>xy</i> 40
3.3	Processo de encriptação e decriptação de texto simples. 41
3.4	Criptografia visual: (a) Imagem original e (b) Imagem criptografada. . . 42
3.5	Codificação de imagem binária. 43
3.6	Esquema de cores: (a) <i>RGB</i> e (b) <i>CMYK</i> 44
3.7	Codificação em quatro canais distintos: (a) Imagem original, (b) Canal <i>C</i> , (c) Canal <i>M</i> , (d) Canal <i>Y</i> e (e) Canal <i>K</i> 45
3.8	Processo genérico de codificação de imagem. 45
3.9	Processo genérico de decodificação de imagem. 46
4.1	Aquisição de imagem e composição de <i>pixel</i> 50
4.2	Posicionamento dos pixels na codificação. 50
4.3	Posicionamento dos pixels na codificação. 51
4.4	Geração de arquivo em formato PNG. 51
4.5	Processo de decodificação da imagem. 52
4.6	Imagem codificada simples e com marcas de impressão. 53
5.1	Funções transformadora com embaralhamento ineficaz. 55
5.2	Imagem da tela principal do <i>software</i> CODITRAC. 56
5.3	Fluxo de codificação. 57
5.4	Fluxo de decodificação. 58
5.5	Imagens codificadas, (a) colorida com mensagem e (b) código QR. 59

5.6	Imagens codificadas utilizando a Fig. 5.5 (a) e as expressões (5.1), (5.2) e (5.3).	60
5.7	Imagens codificadas utilizando a Fig. 5.5 (b) e as expressões (5.1), (5.2) e (5.3).	60
5.8	Imagem original e imagens decodificadas utilizando a Fig. 5.6 e as expressões (5.4), (5.5) e (5.6).	61
5.9	Imagem original e imagens decodificadas utilizando a Fig. 5.7 e as expressões (5.4), (5.5) e (5.6).	62
5.10	Mapa de diferenças entre imagem original e imagens decodificadas das Fig. 5.8 de (b) a (d).	63
5.11	Mapa de diferenças entre imagem original e imagens decodificadas das Fig. 5.9 de (b) à (d).	64
5.12	Imagem colorida contendo código binário.	65
5.13	Resultado da codificação das Fig. 5.12: (a) sem ruído (apenas (5.7)), (b) com ruído de <i>pixels</i> , (c) com ruído de desfoque e (d) em escala de cinza.	65
5.14	Resultado da decodificação das Fig. 5.13: (a) sem ruído (apenas (5.8)), (b) com ruído de <i>pixels</i> , (c) com ruído de desfoque e (d) em escala de cinza.	66
5.15	Mapa de diferenças entre imagem original e decodificadas: (a) sem ruído (apenas (5.8)), (b) com ruído de <i>pixels</i> , (c) com ruído de desfoque e (d) em escala de cinza.	67
5.16	Imagem contendo mensagem a ser transmitida.	67
5.17	(a) Imagem codificada digital. (b) Imagem codificada com marcas para impressão.	68
5.18	Resultado da decodificação da imagem impressa.	69

LISTA DE SÍMBOLOS

(x, y)	–	Coordenadas do ponto no plano cartesiano
R_e	–	Valores reais no plano complexo
I_m	–	Valores imaginários no plano complexo
\mathbb{C}	–	Conjunto dos números complexos
\mathbb{R}	–	Conjunto dos números reais
\mathbb{Q}	–	Conjunto dos números racionais
\mathbb{Z}	–	Conjunto dos números inteiros
\mathbb{N}	–	Conjunto dos números naturais
z	–	Plano complexo z
w	–	Plano complexo w
φ	–	Constante real que define dilatação ou contração dos valores de z
θ	–	Constante real que define ângulo de rotação dos valores de z
i	–	Parte complexa de uma expressão ou simplesmente $\sqrt{-1}$
(r, g, b)	–	Trio de valores que definem a cor de um <i>pixel</i> para esquema de cores <i>RGB</i>
M	–	Quantidade de linhas da matriz de dados da imagem
N	–	Quantidade colunas da matriz de dados da imagem
P	–	Quantidade de cores de um <i>pixel</i> da matriz de dados de uma imagem
(c, m, y, k)	–	Valores que definem a cor de um <i>pixel</i> para esquema de cores <i>CMYK</i>
F_A	–	Fator de ampliação da imagem codificada
M_{do}	–	Matriz de dados original
M_{dc}	–	Matriz de dados codificada
M_{dd}	–	Matriz de dados decodificada

LISTA DE ABREVIATURAS E SIGLAS

- 3D – Tridimensional
- RGB – *Red, Green and Blue* (esquema de cores de imagens)
- CMYK – *Cyan, Magent, Yellow and Key* (esquema de cores de imagens)
- dpi – Pontos por polegada quadrada (*dots per square inch*)
- QR – *Quick Response* (tipo de código de barras)
- JPEG – *Joint Photographics Experts Group* (formato de arquivo de imagem)
- JPG – Mesmo significado de *JPEG*
- PNG – *Portable Network Graphics* (formato de arquivo de imagem)
- SSIM – *Structural SIMilarity* (índice de similaridade entre duas imagens)

CAPÍTULO 1

INTRODUÇÃO

Uma das formas mais utilizadas de transmitir mensagens sigilosas é a criptografia, que é a transformação da mensagem de sua forma original em outra forma ilegível. A mensagem somente poderá ser decifrada pelo portador da chave que transformou a mensagem original na mensagem ilegível, que foi cifrada (STINSON, 2006). A técnica para ocultar a existência de uma mensagem dentro de outra é conhecida como esteganografia, que é o ramo particular da criptologia que consiste em fazer com que dados possam ser camuflados dentro de outros dados, a fim de esconder a sua verdadeira essência (ARTZ, 2002). Esta ocultação da essência dos dados, pode ser realizado transformando os dados entre domínios diferentes. Existem várias formas de transformar mensagens entre domínios, de forma a recuperá-las posteriormente. Uma das formas está na área da matemática, que é o ramo de pesquisa que estuda as mudanças entre domínios complexos, a teoria das transformações conformes. Tais transformações alteram as geometrias sem modificar os ângulos.

O primeiro registro da utilização das transformações conformes é datada do ano 150 *d.C.*, quando Claudius Ptolemy utiliza para representar projeção estereográfica da esfera do globo terrestre. Estudos relacionados às transformações conformes foram desenvolvidos por matemáticos ao longo dos anos, sendo utilizadas nas mais diversas áreas (BROWN; CHURCHILL, 2009). As transformações conformes auxiliam na solução analítica de problemas que envolvam a forma geométrica, transferindo os dados de um domínio a outro, sem alterar os ângulos das geometrias (KYTHE, 2012).

A definição de transformações conformes, na área de engenharia, esta ligada à capacidade de sintetizar soluções de problemas, de forma simplificada (PORTER, 2005). As áreas de destaque na utilização das transformações conformes são: engenharia geológica (SILVA et al., 2015), engenharia de telecomunicação (LI et al., 2013), engenharia elétrica (CALIXTO et al., 2011), computação gráfica (GONG et al., 2015) e outros (BRENNAN et al., 2004; AUBRY et al., 2010). Existem estudos utilizando transformações conformes como ferramenta de processamento e formação de imagens (XIONG et al., 2015; LIU et al., 2015).

A utilização das transformações conformes como ferramenta de processamento de imagens, surgiu por volta da década de 1980, através de pesquisa relacionada a re-

conhecimento de objetos bidimensionais, utilizando técnicas de memória associativa distribuída (WECHSLER; ZIMMERMAN, 1988). Ainda nesta época, Schwartz (1984) conduz estudo de análise de imagens do córtex cerebral estriado, utilizando transformações conformes.

Frederick e Schwartz (1990) avaliam a possibilidade de transformar imagens de geometrias tridimensionais (como imagens nas faces das pirâmides) em imagens bidimensionais utilizando as transformações conformes. Frederick e Schwartz ainda realizam trabalho que une as técnicas de processamento digital de imagem com as transformações conformes para distorcer imagens. Yadong et al. (2009) apresentam método de recuperação e preenchimento de imagens deterioradas pelo tempo. Rojer e Schwartz (1990) estudam a percepção da visão humana com o intuito de projetar sensor de visão, onde regiões das imagens eram mapeadas utilizando transformações conformes, mapeando círculos em elipses.

Mais recentemente, Ramadas et al. (2010) apresentam estudos relacionados ao mapeamento conforme para análise e processamento de imagens geradas por exames ultrassônicos. Hamdy et al. (2013) utilizam as transformações conformes para compressão de arquivo digital JPG. Xiong et al. (2015) utilizam a teoria das transformações conformes, aplicada à construção de classificador multiclases, utilizado no reconhecimento de imagens.

Imagens digitais tem seu franco desenvolvimento na década de 1920, pela necessidade das indústrias de jornais. Os arquivos de imagem precisavam ser transmitidos sob oceano Atlântico entre as cidades de Londres, Inglaterra e Nova York, Estados Unidos (MILNOR, 1941). A imagem transmitida era simplificada, com quantidade reduzida de cores. Utilizava no máximo cinco tons de cinza para compor toda imagem. O processamento efetuado foi batizado como método de Bartlane (GONZALEZ; WOODS, 2001; MCFARLANE, 1972).

Roberts (1962) conduz estudo no intuito de melhorar a transmissão de imagens de televisão, usando código binário. Os processos de melhoramento de cores e redimensionamento são algumas das primeiras aplicações no campo do processamento digital de imagens e que ainda são largamente pesquisados (HSU et al., 2013). O processamento de imagem pode ser utilizado como padrão de composição de imagem para calibração de auto-focagem de laser de alta precisão (HSU et al., 2013), reconhecimento de padrões em imagens de exames de ultrassom (KIM et al., 2001), aplicações

mais específicas como a codificação visual de imagens contendo mensagens secretas (NAOR; SHAMIR, 1994), e muitas outras.

Mensagens secretas codificadas sempre foram utilizadas para transmitir informações sigilosas entre transmissor e receptor. Técnicas de criptografia para repasse de informação foram iniciadas em Roma, por volta do ano 100 *a.C.*, utilizando técnicas primitivas de ocultação de mensagens em textos simples (ZIMMERMANN, 2000). A transmissão de mensagens secretas geralmente é acompanhada de aplicações de cunho militar (VERNAM, 1926).

Com o avanço das tecnologias e formatos de mídia, houve o aumento na exposição das informações sobre pessoas e empresas. Visando manter em sigilo determinadas informações, estudos são realizados na busca de novas formas de garantir a segurança da mensagem. Naor e Shamir (1994) propõem método de transmissão de mensagens secretas, baseado na inserção de mensagens de texto dentro de imagens. A imagem é posteriormente submetida a processo de criptografia visual, tendo seus dados embaralhados.

Vários métodos de codificação e decodificação de mensagens, na forma de imagens contendo textos, são descritos na literatura (XIONG et al., 2015; GAYATHRI; NAGARAJAN, 2015; NAOR; SHAMIR, 1994). No entanto, estudos abordando a utilização de transformações conformes como ferramenta de codificação e decodificação visual de imagens, contendo mensagens, ainda são incipientes.

Portanto, como hipótese tem-se que, se as transformações conformes podem modificar imagens, levando-as de determinado domínio A para outro domínio B , utilizando expressão matemática e se, através de manipulação algébrica, pode-se construir expressão inversas, logo é possível, reconstruir a imagem de B em A novamente. O processamento de imagens é cada vez mais presente no mundo atual, devido ao avanço tecnológico de dispositivos e do compartilhamento global de informações através dos mais diversos meios de comunicação. Cada vez mais se compartilha informações pessoais através da internet. A segurança dos dados é extremamente importante. O volume atual de estudos e pesquisas sobre os temas de criptografia, transporte de mensagens e dados justificam este trabalho.

O objetivo geral deste trabalho é o desenvolvimento de metodologia utilizando as transformações conformes aplicadas no processamento de imagens, sejam estas ima-

gens originalmente digitais ou imagens digitais extraídas de material físico impresso criando novo método de codificação visual de imagens. Ainda como objetivos tem-se: i) desenvolver metodologia de codificação e decodificação de imagens utilizando as transformações conformes, ii) desenvolver metodologia de transporte de mensagem impressa de forma a recuperá-la, iii) construir *software* utilizando a metodologia desenvolvida, iv) avaliar os ruídos gerados na codificação e decodificação das imagens digitais modificadas pelas transformações conformes.

Este trabalho está estruturado de forma a abordar toda a teoria envolvida no desenvolvimento do método proposto. No Capítulo 2 são definidas algumas transformações conformes e descrita de forma sucinta a teoria por trás destas transformações com breve histórico. O Capítulo 3 descreve alguns conceitos de imagens e apresenta alguns métodos de processamento digital e mecanismos de codificação e decodificação de imagens. No Capítulo 4 é descrita toda a metodologia aplicada no desenvolvimento do método proposto. O Capítulo 5 dispõe os resultados obtidos e no Capítulo 6 as conclusões e sugestões para trabalhos futuros.

CAPÍTULO 2

TRANSFORMAÇÕES CONFORMES

Neste capítulo será sucintamente apresentada a teoria de transformações conformes. Para o entendimento destas transformações, inicialmente será necessário realizar histórico e revisão conceitual sobre números complexos, base fundamental da teoria.

2.1 Cartografia

Desde o início dos tempos, o homem tem a necessidade de representar e identificar determinadas regiões onde vive ou deseja explorar. Para auxiliar nesta identificação e localização surgiram os mapas, que são representações gráficas de várias regiões (KRANTZ, 2010).

Evidências históricas relatam o surgimento dos mapas em diversas sociedades antigas, datadas desde 6000 *a.C.* (HARLEY; WOODWARD, 1987). Ainda na Idade Média, os navegadores perceberam a dificuldade em representar distâncias de pontos da esfera terrestre em mapas planos. Apesar das distâncias não poderem ser mantidas, foi observado a possibilidade de se manter os ângulos entre as linhas. Observou-se que ao transferir linhas latitudinais e longitudinais da esfera da Terra para o mapa plano, conseguia-se preservar os ângulos entre as linhas curvas. Desta forma constrói-se o mapa conforme (KRANTZ, 2010), como ilustrado na Fig. 2.1.

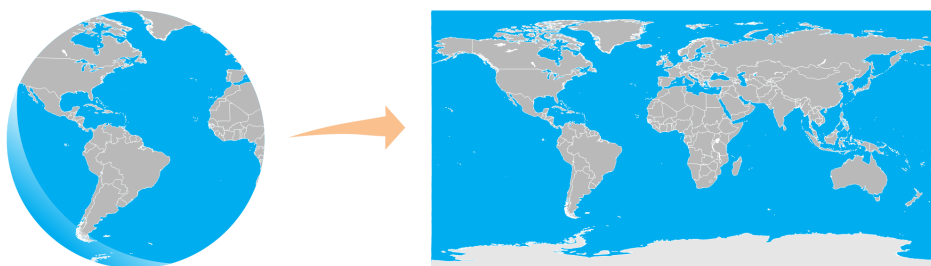


Figura 2.1 - Conceito de mapa conforme.

As projeções cartográficas já eram conhecidas e utilizadas anterior ao ano 200 *a.C.*, na Grécia antiga, e eram necessárias para auxiliar na criação de mapas para delimitação de território e de navegação (HARLEY; WOODWARD, 1987).

A projeção cartográfica trata-se do processo de transformação das coordenadas de determinados pontos da superfície do globo ou esfera, pontos estes compostos por coordenadas de latitude e longitude, que deverão ser mapeados no plano de coordenadas (x, y) em mapa bidimensional. Na Fig. 2.2 é apresentada a projeção dos pontos da esfera mapeados no segmento do mapa plano.

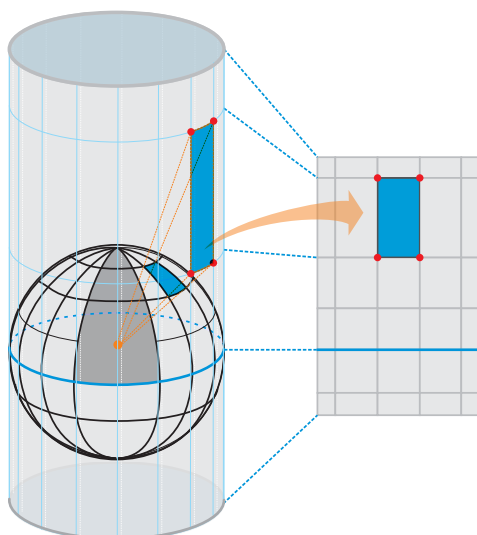


Figura 2.2 - Projeção de pontos da esfera no plano.

2.2 Números complexos

2.2.1 História

Ao longo da história da humanidade, a solução de equações sempre fascinou os matemáticos. Antigos matemáticos da Babilônia conseguiam resolver equações de segundo grau perfeitamente quadradas. Gregos conseguiam resolver equações semelhantes através de compasso e régua. No fim do Império Romano, os estudos matemáticos saíram do domínio dos europeus ficando sob domínio dos árabes e hindus (MERINO, 2006).

A expressão de resolução de equações do segundo grau, foi descoberta pelo hindu Sridhara, ainda no século XI (KREYSZIG, 2011). Através desta expressão, dada a equação $ax^2 + bx + c = 0$, sendo $a \neq 0$, tem-se duas raízes calculadas.

Na solução da expressão desenvolvida por Sridhara aparece: $\sqrt{b^2 - 4ac}$, em deter-

minados casos, pode ocorrer que o resultado $b^2 - 4ac < 0$. Nesta época, quando se deparava com tal situação, os matemáticos simplesmente determinavam que o problema não tinha solução.

No século XVI a Europa voltou a realizar estudos da Matemática. Nesta época percebe-se que o conjunto dos números reais não era suficiente para resolver os problemas matemáticos existentes, tal como raízes de números negativos e equações do terceiro grau, surgindo o conjunto dos números complexos.

A concepção de existência dos números complexos foi explicada pelo matemático italiano Gerolamo Cardano, no século XVII, ao constatar que a solução de equações cúbicas gerais podem conter raízes quadradas de números negativos (BROWN; CHURCHILL, 2009).

Em 1776, com créditos a Leonhard Euler, foi possível a realização dos primeiros estudos dirigidos a problemas de análise, hidrodinâmica e cartografia (KRANTZ, 2010; SPIEGEL, 1972). Os estudos de Euler possibilitaram demonstrar condições necessárias para a diferenciabilidade de função complexa (KRANTZ, 2010). As condições encontradas resultam em funções lineares complexas, desde que a diferenciabilidade no ponto possa ser aproximada através de função linear na vizinhança do ponto em questão. Euler chamou $\sqrt{-1}$ de i , sendo instituída então i como a unidade imaginária.

2.2.2 Definição

Um número completo é definido por:

$$z = x + yi \tag{2.1}$$

onde x e y são números reais, sendo x a parte real e y a parte imaginária de z , denotadas por:

$$x = R_e(z) \quad e \quad y = I_m(z) \tag{2.2}$$

O conjunto dos números complexos, denotado por \mathbb{C} , é dado por:

$$\mathbb{C} = \{z = x + iy, x \in \mathbb{R} \quad e \quad y \in \mathbb{R}\} \tag{2.3}$$

e a composição dos conjuntos numéricos pode ser ilustrada na Fig. 2.3.

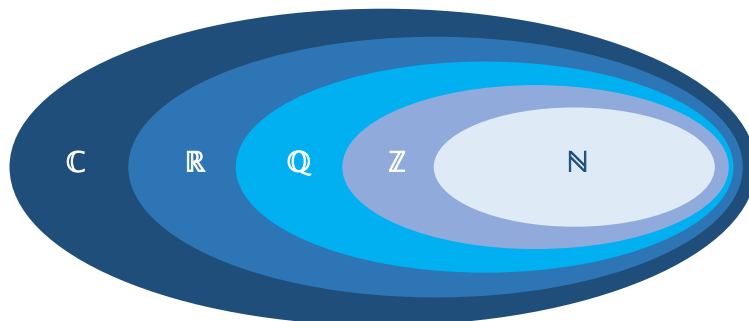


Figura 2.3 - Conjuntos numéricos.

Qualquer equação polinomial com grau n sendo $n \geq 1$ e que possua coeficientes reais ou imaginários, sempre possuirá solução em \mathbb{C} . Sendo possível afirmar que possui pelo menos uma solução complexa. Esta afirmação é conhecida como Teorema Fundamental da Álgebra (FERNANDEZ; JR, 2006).

A Fig. 2.4 ilustra o número complexo $z = x + yi$ no ponto P com as coordenadas $x; y$.

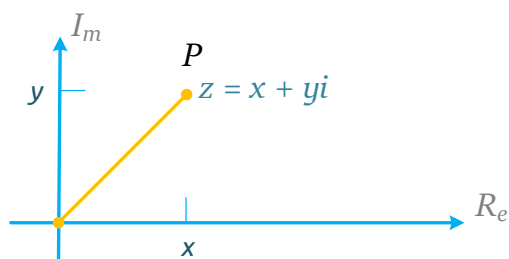


Figura 2.4 - Plano complexo.

2.2.3 Função complexa

A análise complexa tem foco em funções complexas diferenciáveis em algum domínio. A definição de uma função real f definida num conjunto C de números reais, é uma

regra que associa cada valor de x em C a um elemento real $f(x)$, chamado de valor de f em x . Uma função f definida em C é uma regra que associa um número w complexo a cada valor de z em C . Portanto, a função complexa pode ser escrita na forma:

$$w = f(z) \tag{2.4}$$

onde z em C é chamado de variável complexa. O conjunto C é chamado domínio de f .

O conjunto de valores da função f é chamado de intervalo de f , onde w é complexo e definido por $w = u + vi$, onde u é a parte real e v a parte imaginária. Como w depende diretamente de z onde $z = x + yi$, u é função real de x e y , desta forma tem-se:

$$w = f(z) = u(x, y) + v(x, y)i \tag{2.5}$$

que apresenta a função $f(z)$ equivalente ao par de funções reais $u(x, y)$ e $v(x, y)$, sendo que cada elemento depende diretamente das variáveis reais x e y em z .

2.3 Transformações Conformes

Transformações conformes, ou mapeamento conforme, é ferramenta importante na resolução de problemas que envolvem geometrias. Estes problemas normalmente são solucionados utilizando métodos numéricos (CALIXTO, 2008).

Além da utilização na cartografia, são vários os campos de aplicação de transformações conformes. Como exemplos da utilização, na área de análise médica foi utilizada para mapeamento de imagens 3D resultantes de exames médicos (SHI et al., 2011) e como método de mapeamento de estrutura cerebral (GU et al., 2004). Problemas na área da engenharia elétrica (SYCHEV et al., 2014) como parte de método para construção de condutores de faixa estreita, associado ao cálculo de capacitâncias parciais ou mesmo como apresentado na criação de formulação matemática para cálculo do fator de Carter, baseado nas ranhuras de máquinas elétricas (CALIXTO, 2008).

Na área da computação existem soluções de problemas utilizando captação de som (UPTON et al., 2008) para mapeamento de superfícies. Na área da matemática esta

teoria é utilizada como técnica de mapeamento de superfícies através de funções matemáticas simples (FERNANDÈZ, 2012) ou como técnica para solucionar problemas matemáticos envolvendo geometrias poligonais de difícil resolução, que exigem utilização de métodos numéricos, como o método de elementos finitos (SILVESTER; FERRARI, 1996).

Transformações conformes são funções $f(z) = w$ que preservam os ângulos em valor absoluto e sentido entre pares de curvas para cada ponto do domínio do plano- z , onde $f'(z) \neq 0$ (BROWN; CHURCHILL, 2009). Uma transformação conforme é capaz de preservar os ângulos de curvas entre os domínios, como mostra a Fig. 2.5, onde curvas ortogonais de um domínio são transformadas em curvas ortogonais em outro domínio.

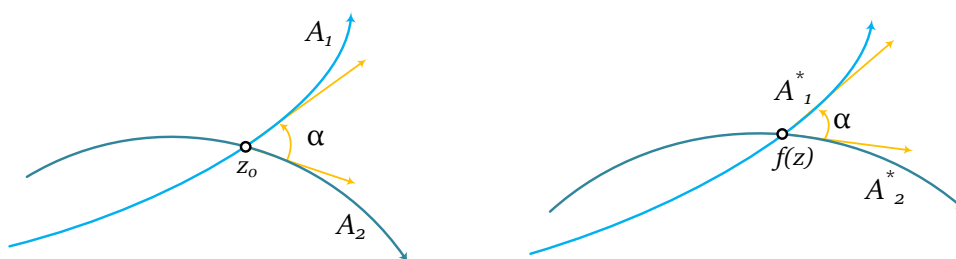


Figura 2.5 - Curvas A_1 e A_2 com suas respectivas imagens e o ângulo α preservado.

Dada função $f : D \rightarrow \mathbb{C}$, onde D é subconjunto de \mathbb{C} e a função f é função complexa de variável complexa. Sendo assim, é possível associar cada elemento de $z \in D$ a um elemento em w no plano- w complexo, dado em (2.5), onde $u(x, y)$ e $v(x, y)$ são funções reais de duas variáveis reais x e y , designada de R_e e I_m de f . O conjunto $D \subseteq \mathbb{C}$ é designado domínio de f e o conjunto das imagens é designado de conjunto imagem de f , como ilustra a Fig. 2.6.

2.3.1 Funções transformadoras elementares

2.3.1.1 Translação

A função transformadora por translação é dada por:

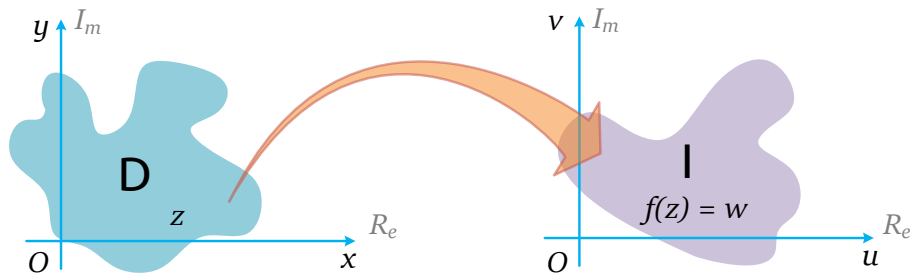


Figura 2.6 - Domínio e Contradomínio.

$$w = f(z) = z + b \quad (2.6)$$

onde b é constante complexa. Funções com esta estrutura possibilitam que pontos do plano- z sejam mapeados no plano- w em direção ao vetor b , tal como observado nas ilustrações das Fig. 2.7 (a) o plano- z e Fig. 2.7 (b) o plano- w transformado.

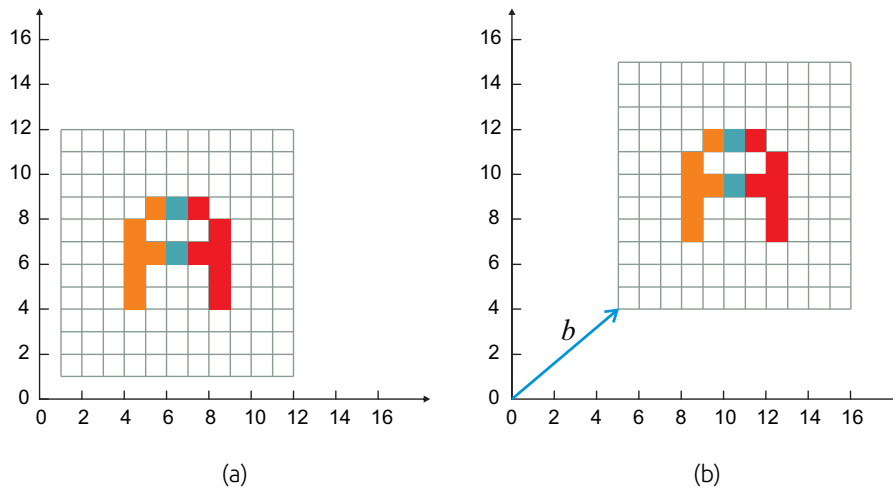


Figura 2.7 - Função transformadora por translação.

2.3.1.2 Rotação

A função transformadora por rotação é dada por:

$$w = f(z) = e^{\theta \cdot i} \cdot z \quad (2.7)$$

onde θ é constante real acompanhada de número complexo i . Funções deste tipo possibilitam rotacionar os pontos do plano- z com ângulo θ , com rotação no sentido horário quando $\theta < 0$ e no sentido anti-horário para $\theta > 0$. A Fig. 2.8 (a) ilustra o plano- z e a Fig. 2.8 (b) ilustra o plano- w transformado com rotação de $\theta = 18^\circ$.

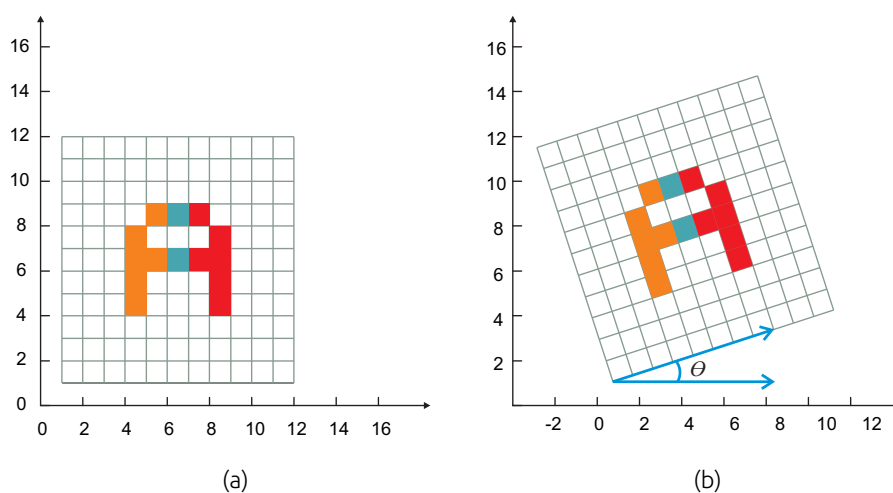


Figura 2.8 - Função transformadora por rotação.

2.3.1.3 Dilatação ou Contração

A função transformadora por dilatação ou contração é dada por:

$$w = f(z) = \varphi z \quad (2.8)$$

sendo φ constante real. Funções com esta estrutura possibilitam que pontos do plano- z sejam expandidos ou contraídos ao serem levados para o plano- w . Para $\varphi > 1$ ocorre a dilatação, enquanto para $0 < \varphi < 1$ ocorre contração, como ilustrado nas Fig. 2.9 (a) o plano- z e Fig. 2.9 (b) o plano- w transformado com $\varphi = 1, 2$ e Fig. 2.9 (c) o plano- w com $\varphi = 0, 5$.

2.3.1.4 Inversão

A função transformadora por inversão é dada por:

$$w = f(z) = \frac{1}{z} \quad (2.9)$$

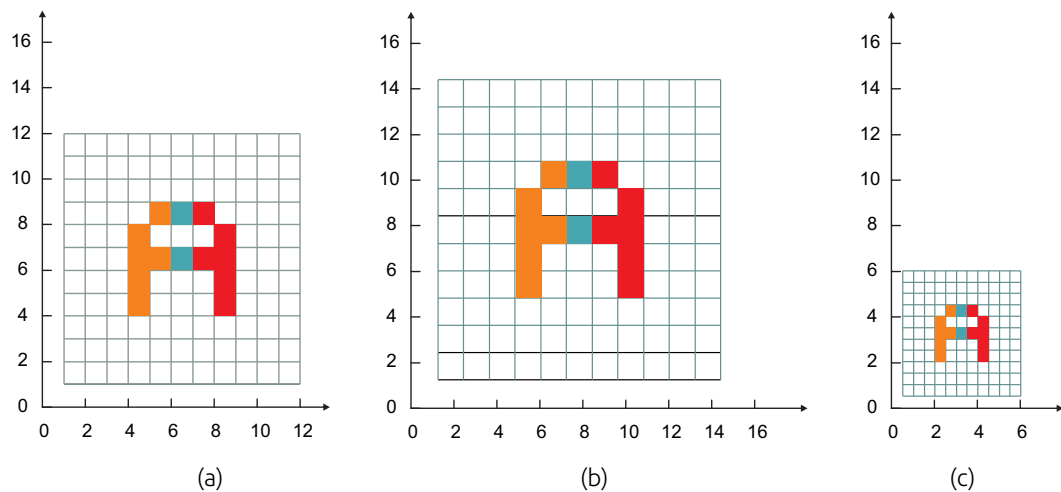


Figura 2.9 - Função transformadora por dilatação e por contração.

Esta função estabelece correspondência biunívoca entre os pontos do plano- z e do plano- w para todos os valores de z desde que $z \neq 0$. Funções transformadoras do tipo inversão levam linhas retas em círculos unitários e círculos em linhas retas (KREYSZIG, 2011). A Fig. 2.10 (a) ilustra uma letra A no plano- z e a Fig. 2.10 (b) ilustra a imagem da letra A no plano- w transformado.

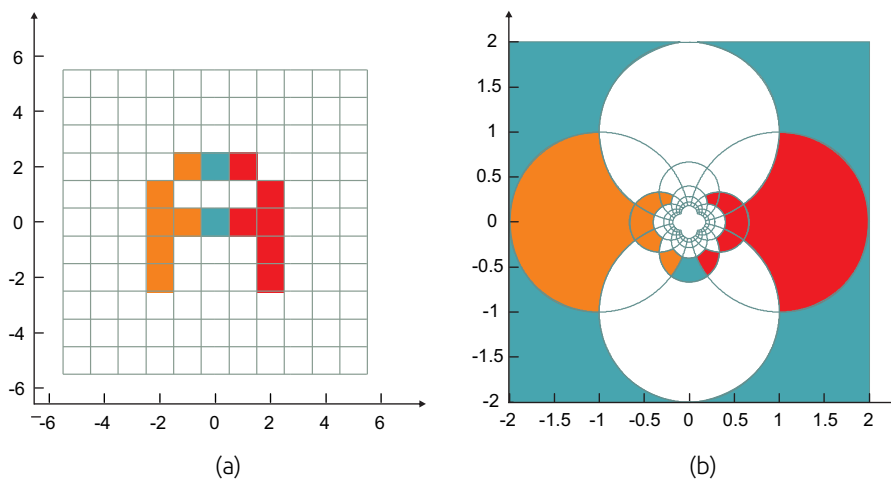


Figura 2.10 - Função transformadora por inversão.

2.3.1.5 Linear

A função transformadora linear é dada por:

$$w = f(z) = az + b \quad (2.10)$$

onde a e b são constantes complexas e $a = e^{\theta i}$. Esta transformação é a junção das transformações por translação (2.6), rotação (2.7) e dilatação ou contração (2.8). A Fig. 2.11 (a) ilustra o plano- z e a Fig. 2.11 (b) ilustra o plano- w transformado.

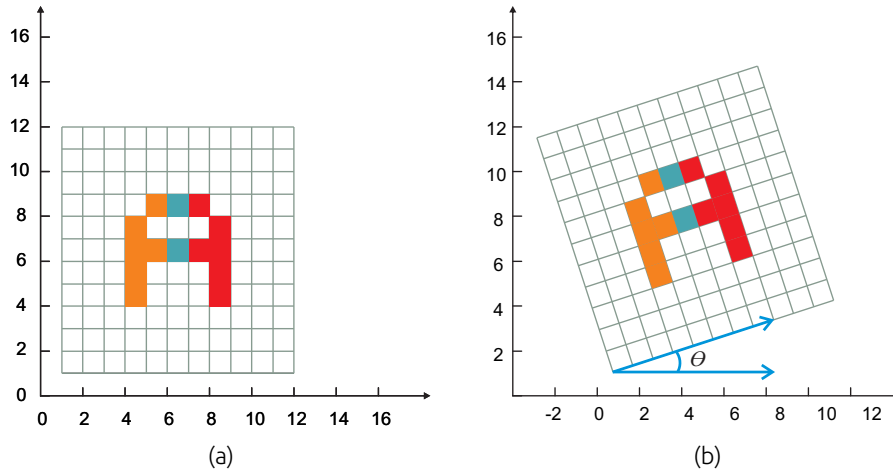


Figura 2.11 - Função transformadora linear.

2.3.1.6 Bilinear

A transformação bilinear ou transformação fracionária, também conhecida como transformação de Möebius é a combinação das transformações de translação (2.6), rotação (2.7), dilatação ou contração (2.8) e de inversão (2.9) e é dada por:

$$w = f(z) = \frac{az + b}{cz + d} \quad (2.11)$$

onde a , b , c e d são constantes complexas e a condição $ad - bc \neq 0$ é verdadeira (HENRICI, 1993). A partir das transformações elementares, várias transformações podem ser criadas.

2.4 Considerações finais

Os diversos tipos de transformação conforme apresentados neste capítulo ilustram a capacidade destas de modificar formas geométricas, transferindo dados de um domínio a outro. Tais transformações podem ser aplicadas também a imagens quando

estas são manipuladas de forma similar à manipulação de formas geométricas.

CAPÍTULO 3

IMAGENS

Neste capítulo será apresentada teoria relacionada às imagens. Serão abordado os conceitos de: composição, criptografia e mecanismos de codificação e decodificação de imagem digital.

3.1 Composição de imagem digital

Toda imagem, seja extraída de material impresso ou gerada digitalmente por dispositivo eletrônico ou por programa de computador, é composta basicamente por pontos de cores ordenados. Pontos estes que, dispostos através de coordenadas (x, y) , possuem dados relativos à sua cor.

De maneira geral, as informações de cores são representadas por vetor de dados com três componentes (r, g, b) . Os componentes (r, g, b) correspondem, respectivamente, às cores vermelho, verde e azul do esquema de cores *RGB*.

Cada valor das coordenadas do vetor (r, g, b) pode variar no intervalo $[0, 255]$. Através da combinação destes valores, é possível representar mais de 16 milhões de tonalidades diferentes. A Fig. 3.1 ilustra a disposição das cores no plano- xy .

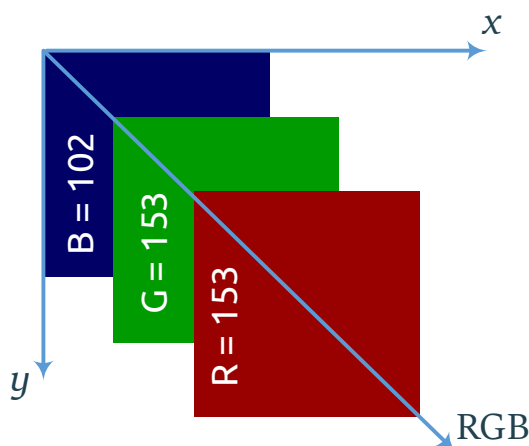


Figura 3.1 - Composição do pixel para esquema de cores *RGB*.

Pela definição de posicionamento dos pontos de cores no plano, cada imagem digital é composta de matriz multidimensional $M \times N \times P$, onde M representa quantidade de pontos de altura, N pontos de largura e P o vetor de três termos de cores do esquema *RGB*.

Cada ponto de cor é denominado *pixel*. O *pixel* é a menor unidade computacional de cor para imagem. Os *pixels* estão dispostos no plano de par ordenado, como ilustrado na Fig. 3.2.

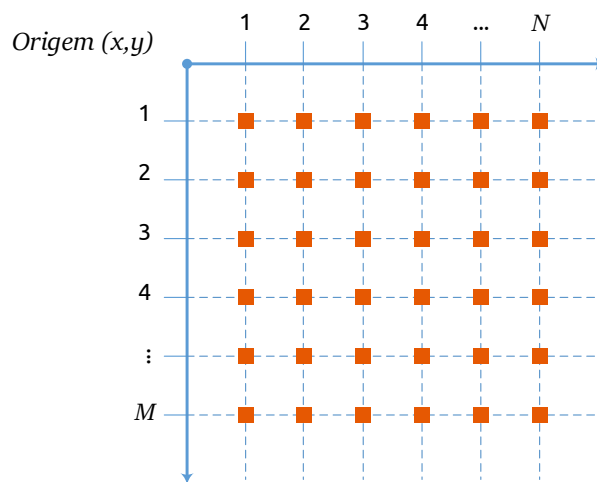


Figura 3.2 - Posicionamento de *pixels* no plano- xy .

Existem vários métodos de processamento digital de imagem. Cada método tem objetivo distinto. Alguns utilizam a manipulação de cores, afetando diretamente os valores do vetor (r, g, b) de cada pixel para conseguir inferir a distorção de cores desejada (CHANG; REID, 1996; HASNAT et al., 2015; TENG et al., 2016). Outros métodos utilizam a manipulação dos *pixels*, alterando as coordenadas (x, y) , reposicionando-os ou até mesmo eliminando determinadas faixas de *pixels* para redimensionamento da imagem (HARALICK et al., 1973; VANDERBRUG, 1975; PANG et al., 2016).

3.2 Criptografia de imagens

Quando o imperador romano Júlio César enviava mensagens a seus generais de guerra, não confiava em seus mensageiros. Então, para esconder o conteúdo real das mensagens, ele codificava os textos enviados. Substituíam as letras *A* por letras *D*, a

letra B pela letra E e assim sucessivamente para as demais letras do alfabeto. Porém, qualquer um que interceptasse as mensagens e soubesse a regra de deslocamento por três letras, conseguiria decifrar a mensagem (ZIMMERMANN, 2000).

Todo texto escrito que possa ser lido ou compreendido sem auxílio de métodos auxiliares, é considerado texto simples. Toda a manipulação de texto simples, para que este não possa ser lido ou compreendido senão por método auxiliar, é chamada de encriptação. Textos resultante da manipulação é chamado de texto cifrado. A fase ou processo de recuperação do texto encriptado é denominado de decifração. O processo de encriptação e decifração é ilustrado pela Fig. 3.3.

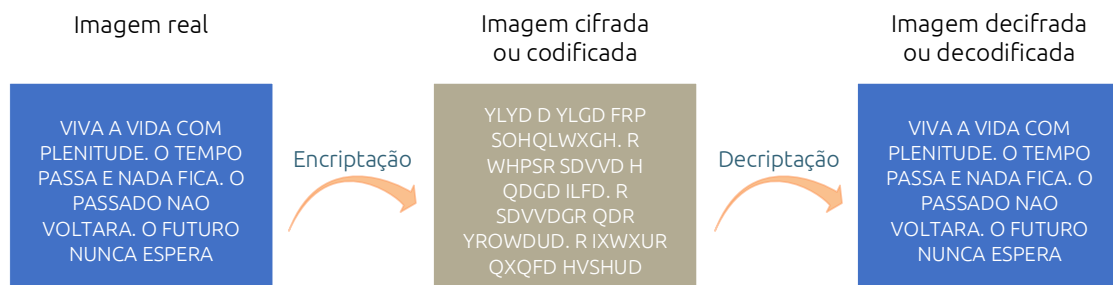


Figura 3.3 - Processo de encriptação e decifração de texto simples.

O processo de criptografia computacional sempre conta com um algoritmo, dotado de função matemática utilizada nos processos de encriptação e decifração de mensagens. Algoritmos utilizados para encriptação funcionam combinados a uma chave (palavra, número ou frase). A qualidade do processo de criptografia depende de duas condições distintas: a confidencialidade da chave e força do algoritmo de encriptar e decifrar (ZIMMERMANN, 2000).

Desde a criação da Internet, vários tipos de conteúdos como textos, imagens, vídeos e áudio podem ser transmitidos pela rede (SUBRAMANIAN; LOGANATHAN, 2011). Para garantir a confidencialidade na transmissão e compartilhamentos das imagens, várias técnicas de codificação tem sido estudadas. A metodologia de criptografia de mensagens de texto simples pode ser utilizada para codificar imagens.

A técnica de codificação de imagens é a capacidade de ocultar os conteúdos visuais que necessitem ser mantidos em sigilo. Podem ser criadas imagens criptografadas em arquivos codificados que possam ser transmitidos como texto ou imagens codificadas

em novos arquivos de imagem.

A encriptação de imagem que gera uma ou mais imagens codificadas, é chamada de Criptografia Visual. A Fig. 3.4 ilustra imagem digital original e ao seu lado a imagem gerada através de processo de encriptação.

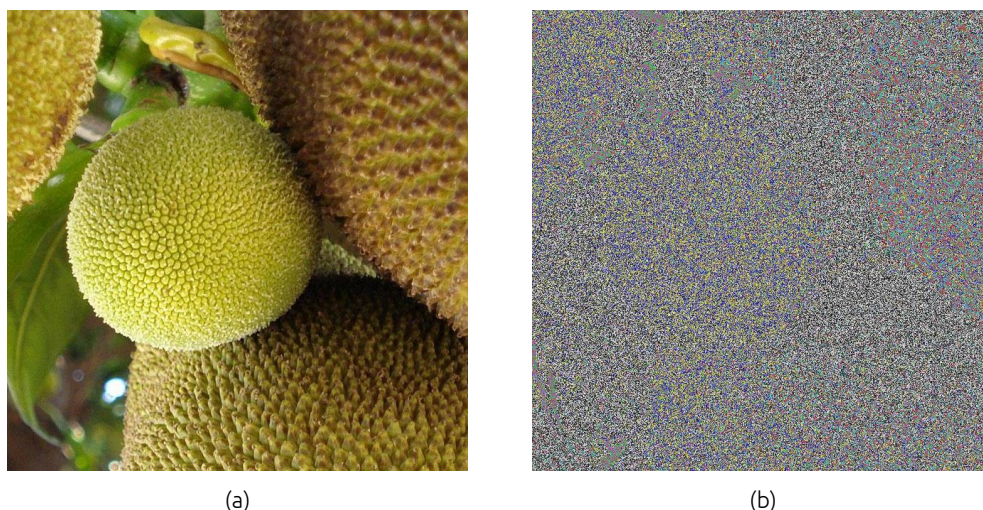


Figura 3.4 - Criptografia visual: (a) Imagem original e (b) Imagem criptografada.

O conceito e o método de codificação visual de imagens foi introduzida em 1994, afim de proteger mensagens secretas contidas em imagens. Foi proposta criptografia visual por limite $(k; n)$, onde, a imagem codificada em n partes tem k ou mais variações que podem ser recuperadas (NAOR; SHAMIR, 1994).

Dentre as possibilidades de se trabalhar com encriptação de imagens, pode-se citar técnicas aplicadas a três tipos diferentes de imagens: i) imagens binárias, ii) imagens em escala de cinza e iii) imagens coloridas.

Imagens binárias são aquelas que possuem estrutura $M \times N \times P$, como definido na Seção 3.1, porém com a diferença de que, ao invés de P receber faixa de valores de $[0,255]$, P assume os valores 0 ou 1.

O método de criptografia visual utilizando imagens binárias elaborado por Naor e Shamir (1994), gera n imagens à partir da imagem original e utiliza filtro de super-exposição de tons para recuperar a mensagem codificada. O esquema desenvolvido

é ilustrado na Fig 3.5.

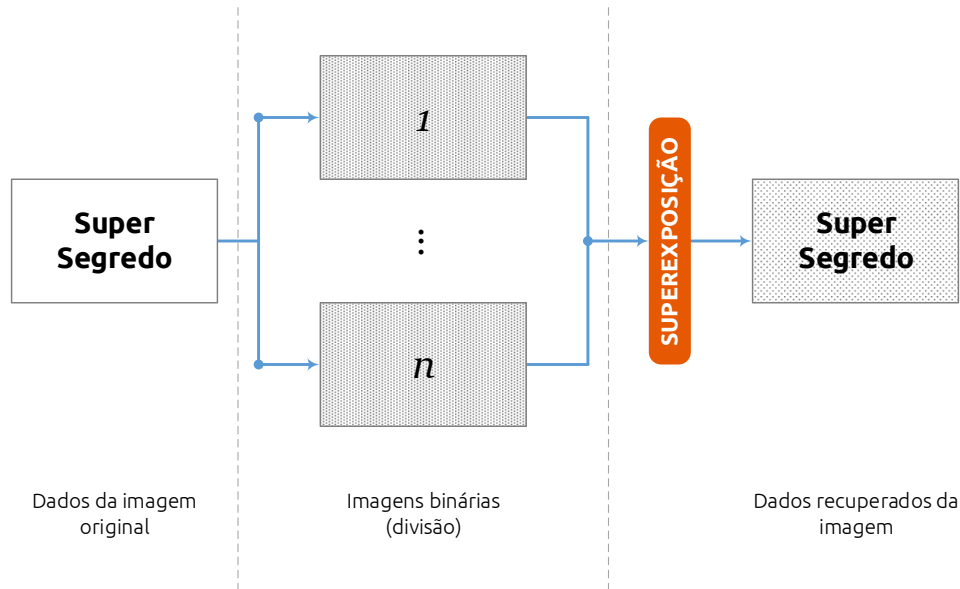


Figura 3.5 - Codificação de imagem binária.

Imagens em escala de cinza tem estrutura de dados $M \times N \times P$, com P assumindo apenas um valor inteiro no intervalo $0 \leq P \leq 255$ para cada posição da imagem. A criptografia de imagem em escala de cinza, proposta por [Dhole e Janwe \(2013\)](#), decompõe a imagem em códigos binários de oito bits, o que equivale a oito imagens binárias. Através de cálculo matemático e combinação de bits, é gerado plano de compartilhamento, onde este é o conjunto de imagem binária que contém as informações da imagem original.

Assim como a codificação de imagens binárias e em escala de cinza, a codificação de imagens coloridas utiliza variações de imagens compartilhadas baseadas no sistema de cores *CMYK*. O método converte a imagem colorida para o esquema de tons *CMYK* na geração de imagens intermediárias para compartilhamento ([HOU, 2003](#)).

Os esquemas de cores *RGB* e *CMYK* diferem-se pela forma com que fazem a quantificação de cores. A estrutura de cores *RGB* e *CMYK* podem ser visualizadas na Fig. 3.6. Para o esquema *RGB*, Fig 3.6 (a), as cores são obtidas pela combinação dos tons *vermelho*, *verde* e *azul*, não existindo unidade para determinar a tonalidade das

cores *preto* e *branco*, que são determinados pela combinação dos três tons anteriores.

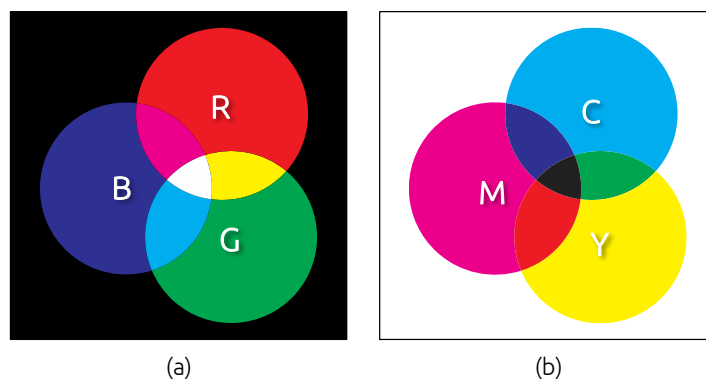


Figura 3.6 - Esquema de cores: (a) *RGB* e (b) *CMYK*.

No esquema de cores *CMYK*, Fig. 3.6 (b), as cores são obtidas através da combinação dos tons *ciano*, *magenta*, *amarelo* e *preto*. Os valores de cada uma das tonalidades do vetor (c, m, y, k) está no intervalo percentual $[0, 100]\%$.

Caso a imagem se encontre no esquema de cores *RGB*, existe a necessidade de realizar a conversão para *CMYK*. Após realizada a conversão do esquema de cores *RGB* para *CMYK*, o método de criptografia de imagem colorida gera quatro imagens de compartilhamento. Cada imagem contém um dos canais *C*, *M*, *Y* e *K*, com os dados criptografados através de função matemática (HOU, 2003). As imagens de compartilhamentos são separadas nos quatro canais de cor: *ciano/cyan*, *magenta/magenta*, *amarelo/yellow* e *preto/black(key)*.

A partir da imagem original, Fig. 3.7 (a), é realizado processo de codificação separando em imagens codificadas dos canais (c, m, y, k) , gerando imagem codificada relacionada a cada componente de cor: Fig. 3.7 (b) do canal da cor ciano, Fig. 3.7 (c) do canal da cor magenta, Fig. 3.7 (d) do canal da cor amarelo e Fig. 3.7(e) do canal da cor preto e branco.

3.3 Processo de codificação e decodificação de imagem

No processo de criptografia de imagem, a codificação e decodificação podem ser considerados como o processo de ida e processo de volta, respectivamente, dentro do

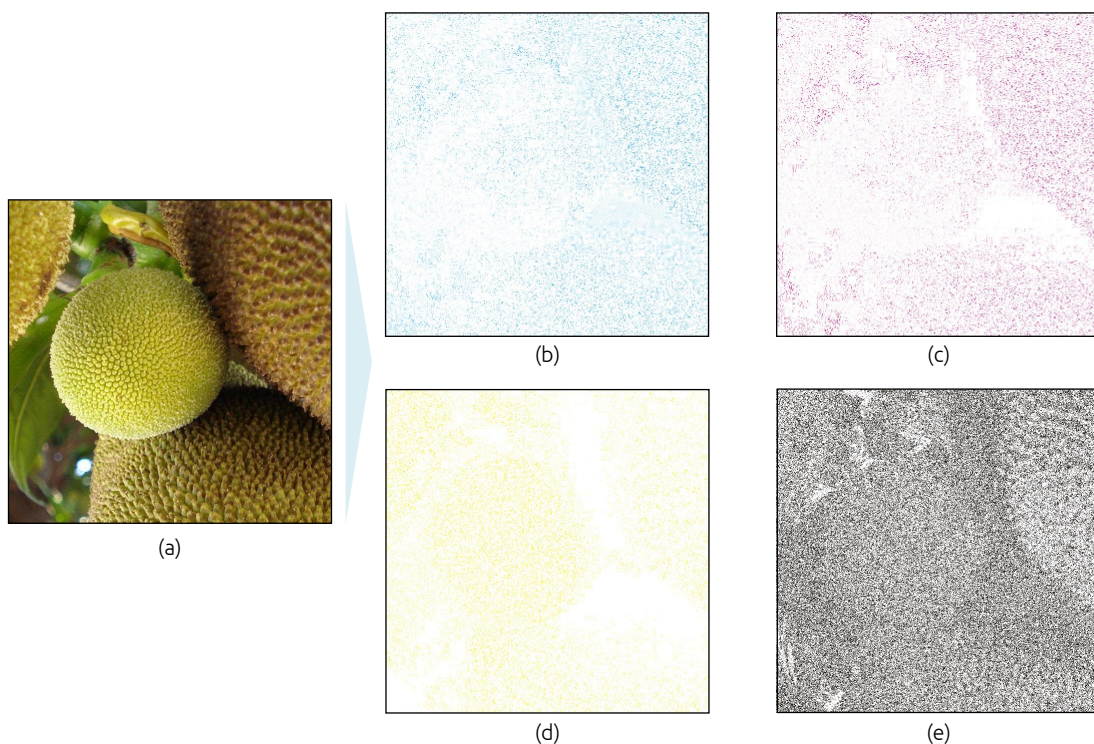


Figura 3.7 - Codificação em quatro canais distintos: (a) Imagem original, (b) Canal C , (c) Canal M , (d) Canal Y e (e) Canal K .

processo total de criptografia.

As características de cada processo dependerão do método, da quantidade de processos intermediários e da quantidade de chaves utilizadas. O que diferencia cada processo de codificação de imagens é o algoritmo, a Fig. 3.8 ilustra o processo genérico de codificação.



Figura 3.8 - Processo genérico de codificação de imagem.

O processo de decodificação é o inverso do processo de codificação. Assim como na codificação, as características do processo de decodificação dependem do método ou algoritmo utilizado na codificação. Na Fig. 3.9 encontra-se ilustrado o processo genérico de decodificação.



Figura 3.9 - Processo genérico de decodificação de imagem.

Quanto se trata de processo de decodificação utilizando somente o meio digital como transmissão, geralmente os arquivos codificados a serem transmitidos não tem seu conjunto de dados modificado por ruído do meio. Porém, quando as imagens codificadas passam, por exemplo, por conversão de formato de imagem ou até mesmo compactação através de algoritmo, tem-se problema na recuperação e reconhecimento da imagem após o processo de decodificação (SHIMOBABA et al., 2015).

Como a maioria das criptografias visuais trabalha diretamente com manipulação das cores e deslocamentos de bits, qualquer interferência de posicionamento pode impedir que a imagem seja decodificada corretamente. Tal característica impede que uma imagem gerada através destes métodos tradicionais existentes, possa, por exemplo, ser transmitida através de meio que não seja digital.

Todos os métodos listados, independentemente do algoritmo ou método utilizado só funcionam com imagens digitais. Se a imagem for impressa e posteriormente digitalizada, por mais criterioso que seja o processo de impressão e digitalização, inviabiliza a decodificação dos dados codificados.

3.4 Considerações finais

A composição de imagens digitais foi definida assim como a técnica de criptografia visual. Esta técnica de criptografia e a definição de método para manipulação de

dados de uma imagem formam a base para construção do método de criptografia visual utilizando transformações conformes.

CAPÍTULO 4

METODOLOGIA

Neste capítulo será apresentada a metodologia utilizada para o desenvolvimento e a formatação do método proposto. Serão descritas as etapas para captura da imagem, codificação e decodificação utilizando as transformações conformes.

4.1 Aquisição de imagem

A aquisição deverá ser realizada através de arquivo digital. Mesmo que a imagem a ser codificada esteja impressa, esta deverá inicialmente passar por escâner, onde os dados visuais impressos são convertidos em arquivo digital de imagem. Não haverá limite de dimensões da imagem a ser codificada. O único critério condicionante será que a imagem possua resolução de $72dpi$, que corresponde a 72 pontos de cor para cada polegada quadrada de área da imagem. Os formatos que serão trabalhados são JPEG e PNG. Ambos os formatos representam tipos de arquivos de imagem digital. O JPEG é formato de arquivo e método de compressão. É largamente utilizado para armazenar imagens em arquivos. Possui capacidade de representar imagens coloridas, porém não possui capacidade de representar transparência. O PNG também é formato de arquivo e método de compressão de imagens. Além da capacidade de armazenar imagens com vasta gama de cores, também representa a transparência presente na imagem.

Definidos os formatos de imagens a serem utilizados, procede-se com a aquisição do arquivo. Deverá ser realizada leitura do arquivo digital convertendo sua estrutura de dados no formato de imagem em matriz de dados $M \times N \times P$. A Fig. 4.1 ilustra a forma que deverá ocorrer o processo de aquisição e o detalhamento das informações de cores para cada *pixel* da imagem lida.

4.2 Escolha da função conforme transformadora e codificação de imagem

Para a escolha da função transformadora, será utilizado a teoria das transformações conformes. Para que o método proposto funcione corretamente, a função transformadora deverá ser totalmente invertível, ou seja, deverá ter inversa de forma a poder transitar os pontos da imagem entre os plano- z e plano- w complexos.

Após a escolha da chave de codificação, através da função transformadora, deverá

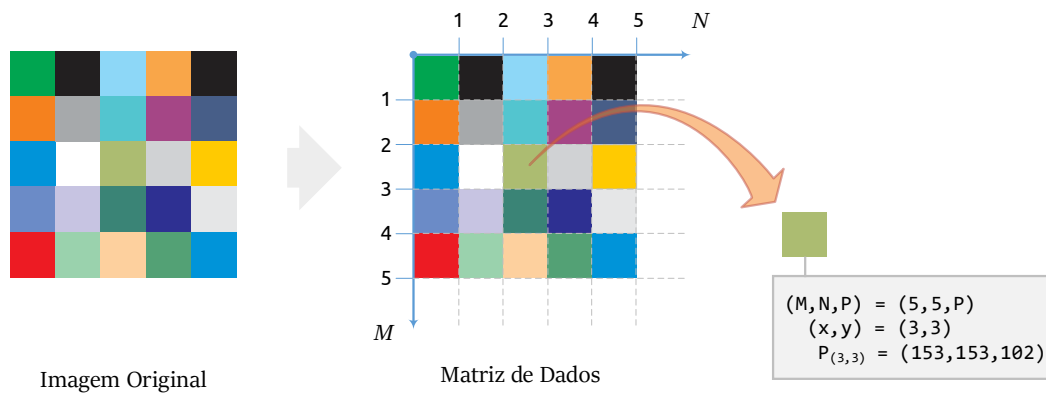


Figura 4.1 - Aquisição de imagem e composição de *pixel*.

proceder com a codificação da imagem previamente adquirida e armazenada na matriz de dados. A imagem será submetida ao processo de cálculo de reposicionamento de cada *pixel* baseado na função transformadora, levando o plano- z no plano- w , como exemplo ilustrado na Fig. 4.2, onde foi utilizado como chave de transformação, a função (4.1).

$$f(z) = 2z + 2i \quad (4.1)$$

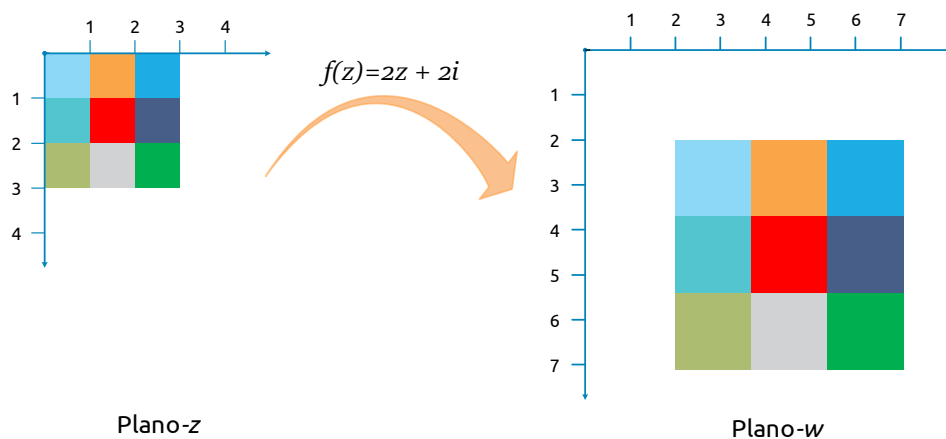


Figura 4.2 - Posicionamento dos pixels na codificação.

Devido a natureza de algumas funções transformadoras, a imagem codificada deverá possuir altura e largura superior ao da imagem original. Este aumento no tamanho da imagem codificada será chamado de fator de ampliação, ou simplesmente F_A . Para determinar o valor de F_A , deverão ser realizados testes com imagens e fun-

ções transformadoras em conjunto com o método de determinação da qualidade de imagem *Structural SIMilarity* (SSIM), que é a métrica de avaliação objetiva da qualidade de referência completa para imagens e que verifica *pixel a pixel* a similaridade entre duas imagens (WANG et al., 2004). A Fig. 4.3 ilustra o processo de ampliação por F_A , partindo da matriz M_{do} que contém os dados originais até a geração da nova matriz M_{dc} , que contém os dados de cores no plano- w , imagem codificada.

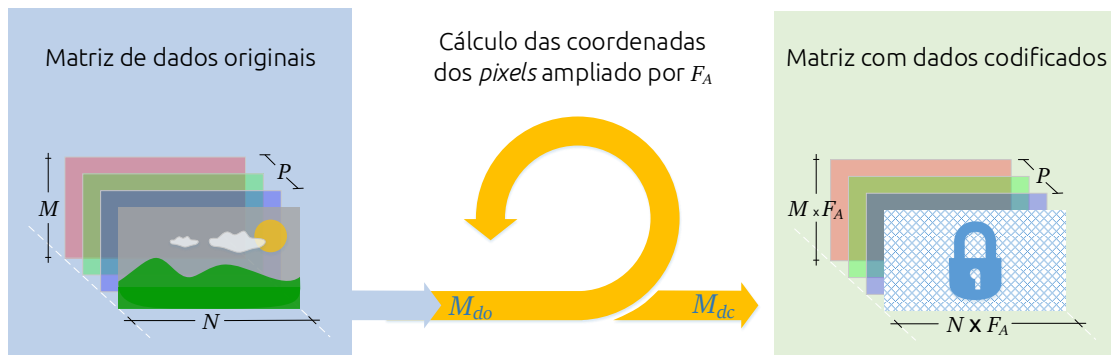


Figura 4.3 - Posicionamento dos pixels na codificação.

O processo de geração da imagem codificada será o inverso do processo de aquisição da imagem. A matriz M_{dc} contendo os dados da imagem codificada deverá ser convertida em arquivo de imagem PNG, como ilustrado na Fig. 4.4.

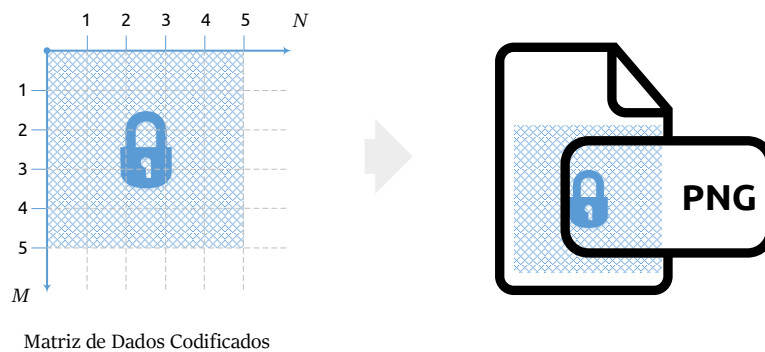


Figura 4.4 - Geração de arquivo em formato PNG.

4.2.1 Processo de decodificação

No processo de decodificação da imagem, poderá ser necessário realizar o escaneamento, caso a imagem codificada tenha sido impressa. A sugestão é que o escâner seja de alta precisão de cores, para que o escaneamento seja realizado com alta resolução, garantindo maior fidelidade na decodificação.

Para codificar a imagem, houve a necessidade de indicar a chave que é função invertível. Desta forma, para decodificar a imagem, será necessário calcular a inversa da função transformadora utilizada. Portanto, de posse da função transformadora inversa e da matriz M_{dc} , contendo os dados codificados, obtém-se a matriz M_{dd} , contendo os dados da imagem decodificada, reposicionando os pixels novamente, no plano- z complexo.

Como na codificação, na decodificação também haverá a necessidade da utilização do fator de ampliação F_A , que deverá reduzir a imagem na mesma proporção da ampliação utilizada na codificação. O processo de decodificação é ilustrado na Fig. 4.5.

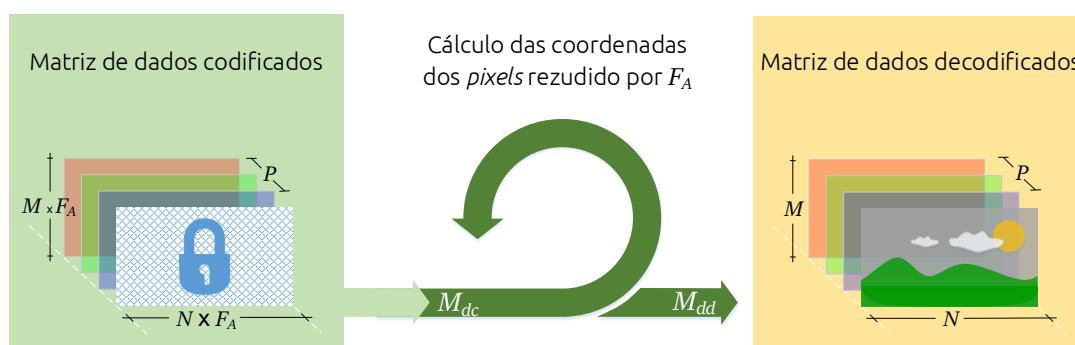


Figura 4.5 - Processo de decodificação da imagem.

Gerada a matriz M_{dd} contendo os dados decodificados, restará converter os dados de M_{dd} em imagem no formato PNG.

Considerando que todas as imagens codificadas serão impressas, será sugerido que contenham marcas de impressão ou balizamentos. As marcas de impressão serão utilizadas apenas no ajuste de escaneamento. Estas marcas não deverão possuir cores específicas e deverão ser inseridas na imagem codificada, seguindo apenas a delimitação dos vértices. A Fig. 4.6 (a) ilustra a imagem codificada sem a marca e a

Fig. 4.6 (b) ilustra a imagem codificada com a inserção das marcas em seus vértices.

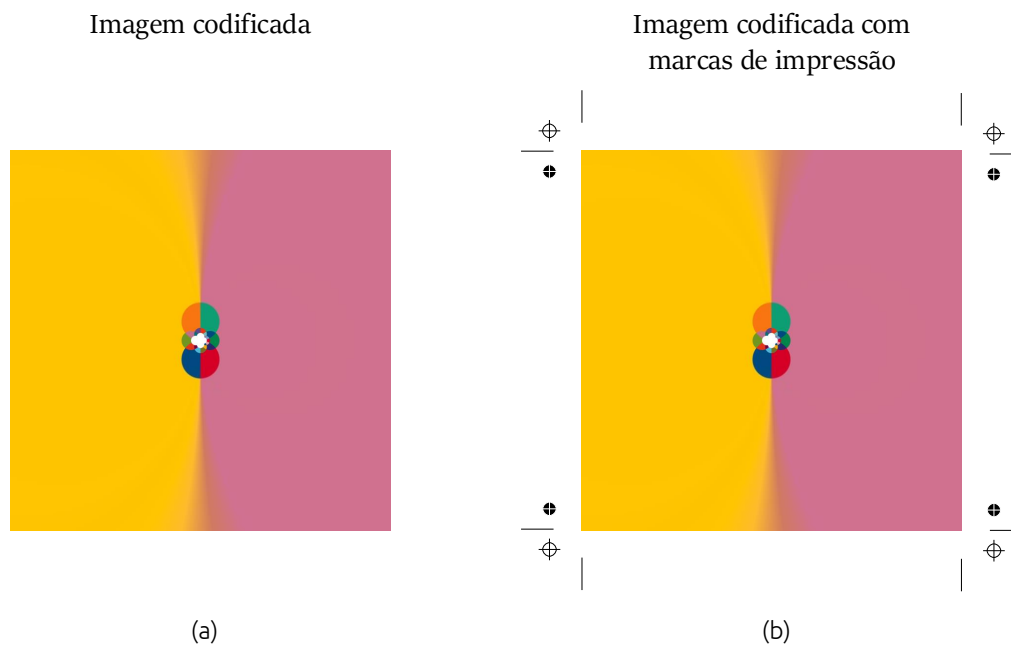


Figura 4.6 - Imagem codificada simples e com marcas de impressão.

4.3 Considerações finais

Diferentemente dos métodos já estudados, o método proposto utiliza como ferramenta de criptografia a mudança de um domínio a outro através de transformações conformes. O metodologia garante a possibilidade de codificar os dados de uma imagem, gerando imagem codificada, podendo esta ser impressa e posteriormente escaneada e decodificada através de função transformadora inversa. Dada a metodologia de criptografia visual, é necessário realizar testes para avaliar as capacidades do método proposto.

CAPÍTULO 5

RESULTADOS

Neste capítulo é apresentado o *software* que foi construído com o intuito de realizar o processo de codificação e decodificação de imagens utilizando as transformações conformes. São apresentados ainda os resultados obtidos através de estudos de casos. Os estudos de casos apresentados são: i) codificação e decodificação de imagens digitais, ii) codificação e decodificação de imagens com inserção de ruídos e iii) codificação e decodificação de imagens impressas. Todas as imagens utilizadas foram produzidas exclusivamente para o trabalho e não possuem restrição de uso ou exibição.

5.1 Segurança da Chave

A escolha da chave na criptografia é algo importante. Normalmente o termo utilizado é força da chave. A força da chave, em criptografia, depende do seu tamanho. No método proposto, a força da chave depende exclusivamente da função transformadora. Caso a função transformadora não produza o embaralhamento eficaz, a mensagem codificada pode ser facilmente interpretada. As transformações elementares, por exemplo, dadas pelas expressões (2.7), (2.6) e (2.8), quando utilizadas sozinhas não produzem resultados satisfatórios, como apresentado na Fig. 5.1.

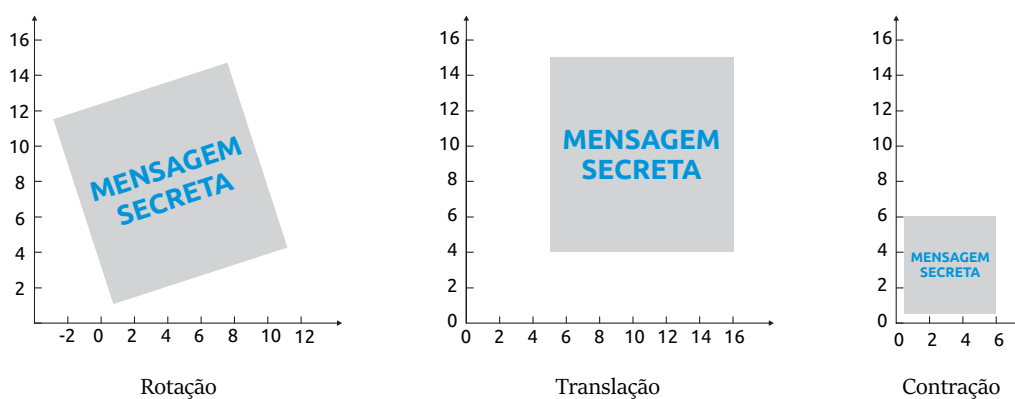


Figura 5.1 - Funções transformadora com embaralhamento ineficaz.

Vários testes foram realizados com o intuito de encontrar funções transformadoras capazes de produzir embaralhamento eficaz. Após os testes com as funções transformadoras, produziu-se testes para encontrar o valor ideal de F_A . Nestes novos testes

foram avaliados os resultados das imagens decodificadas e comparadas com as imagens originais. Utilizando o método de determinação de qualidade de imagem SSIM, escolhe-se o valor que produz o menor erro com a menor ampliação, encontrando empiricamente para este trabalho, $F_A = 15$.

5.2 O Software

Com o intuito de simular, testar e validar o método proposto, foi desenvolvido *software* capaz de realizar a codificação e a decodificação de imagens utilizando as transformações conformes. A Fig. 5.2 apresenta a interface do *software* com cada uma de suas funcionalidades.

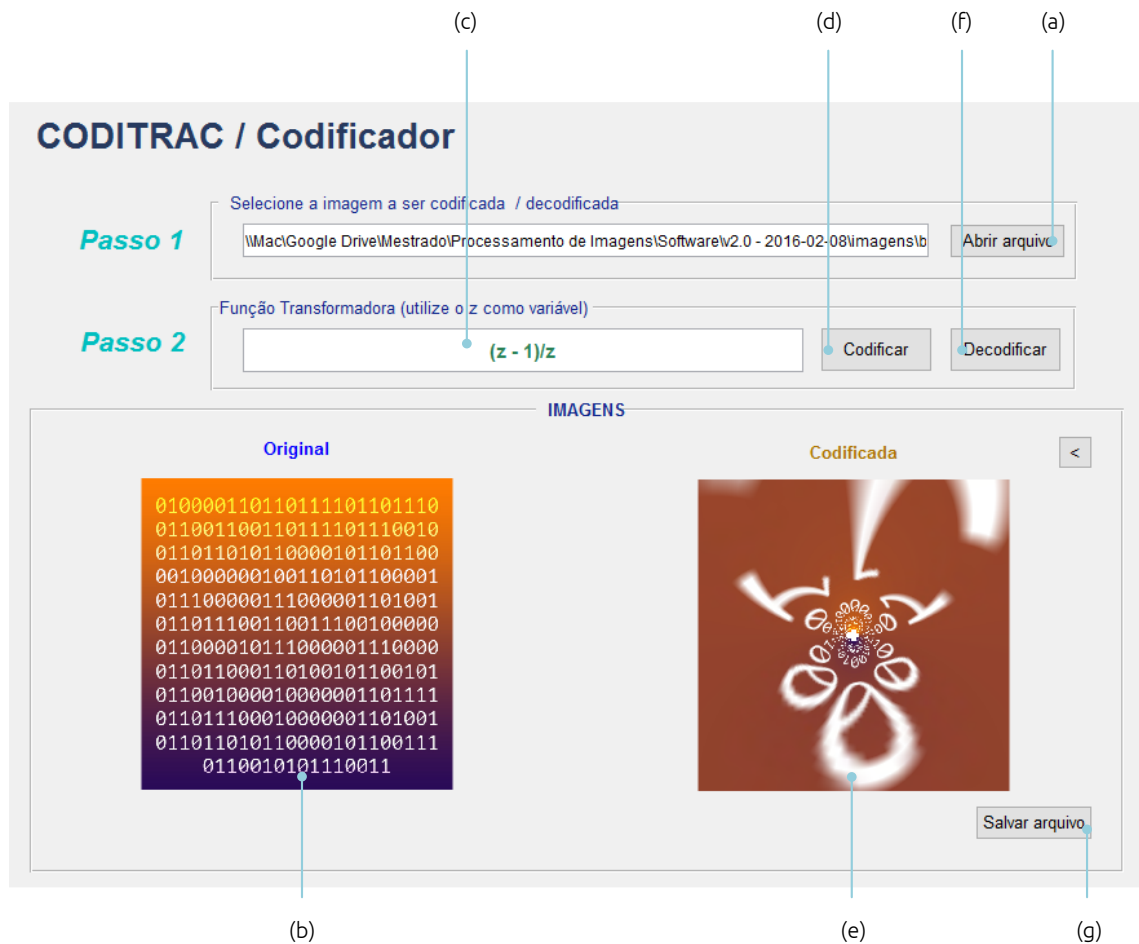


Figura 5.2 - Imagem da tela principal do *software* CODITRAC.

O *software* possui sete funcionalidades em sua interface. Estas funcionalidades são

indicadas pelas letras de “a” à “g” da Fig. 5.2. A seleção da imagem a ser codificada, é realizada no botão identificado pela letra “a”. Após a seleção da imagem a ser codificada, esta aparecerá no lado esquerdo da interface gráfica do *software*, letra “b”. A função transformadora é inserida na caixa identificada pela letra “c”. O botão identificado pela letra “d” inicia o processo de codificação. A imagem codificada é apresentada no lado direito da interface gráfica, identificada pela letra “e”. O processo de decodificação é realizado pressionando o botão “f”. O botão identificado pela letra “g” fornece interface para salvar arquivo em formato PNG das imagens, codificadas ou decodificadas, geradas pelo *software*.

Na Fig. 5.3 é ilustrado o processo completo da codificação, desde a aquisição da imagem até a geração do arquivo para impressão com a mensagem codificada. Na Fig. 5.4 é ilustrado o fluxo do processo de decodificação, desde o escaneamento da imagem impressa até a geração do arquivo final, contendo a imagem com a mensagem decodificada. As Fig. 5.3 e Fig. 5.4, juntas, ilustram de maneira geral o funcionamento do método proposto.

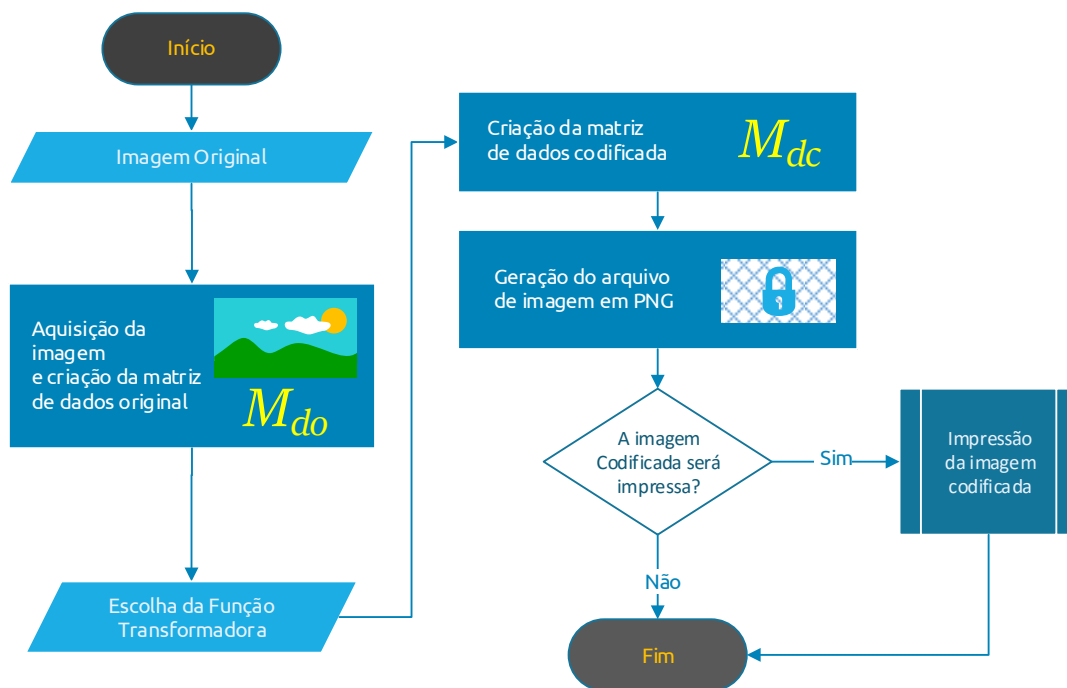


Figura 5.3 - Fluxo de codificação.

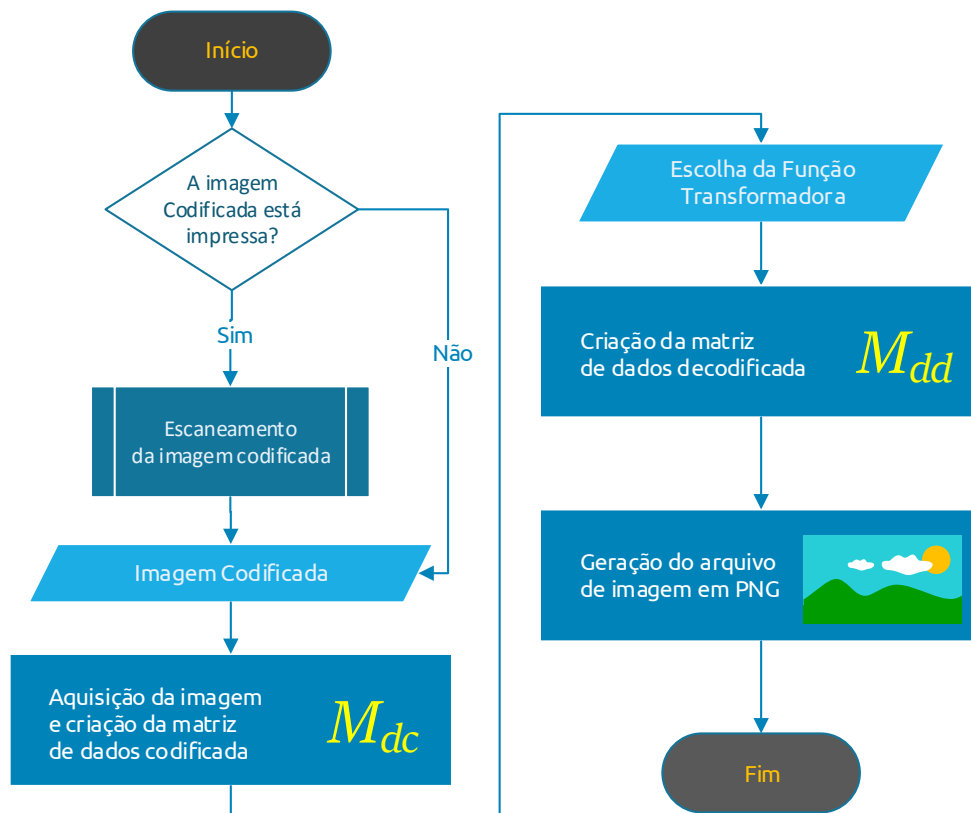


Figura 5.4 - Fluxo de decodificação.

5.3 Estudo de Caso 1: Codificação e Decodificação de imagens digitais

Neste estudo de caso foram realizadas codificação e decodificação de duas imagens com conteúdos diferentes. As imagens são apresentadas na Fig. 5.5, onde na Fig. 5.5 (a) é apresentada imagem colorida contendo mensagens e na Fig. 5.5 (b) é apresentada imagem no formato de Código *Quick Response* (QR), com a mensagem *Transformação Conforme*.

A Fig. 5.5 (a) foi escolhida por apresentar elementos visuais diferentes, como cores, geometrias e mensagens. A Fig. 5.5 (b) foi escolhida por conter mensagem escrita em código de barra bidimensional, que pode ser facilmente escaneada e convertida em texto, usando dispositivo eletrônico equipado com câmera e leitor de código QR. Desta forma, a mensagem pode ser lida na imagem original e depois na imagem decodificada. Na codificação das imagens da Fig. 5.5, foram utilizadas três chaves, definidas pelas expressões (5.1), (5.2) e (5.3). A escolha das chaves foi realizada visando explorar a capacidade de embaralhamento visual das transformações con-



Figura 5.5 - Imagens codificadas, (a) colorida com mensagem e (b) código QR.

formes.

$$w = f(z) = \frac{z}{z + 1} \quad (5.1)$$

$$w = f(z) = \frac{1 - zi}{z} \quad (5.2)$$

$$w = f(z) = e^{z \cdot \frac{\pi}{4}} \quad (5.3)$$

5.3.1 Codificação

As imagens resultantes da codificação das Fig. 5.5 (a) e Fig. 5.5 (b) estão apresentadas nas Fig. 5.6 e Fig. 5.7. As Fig. 5.6 (a), Fig. 5.6 (b) e Fig. 5.6 (c) correspondem as codificações utilizando as expressões (5.1), (5.2) e (5.3), respectivamente, da Fig. 5.5 (a). As Fig. 5.7 (a), Fig. 5.7 (b) e Fig. 5.7 (c) correspondem às codificações utilizando as expressões (5.1), (5.2) e (5.3), respectivamente, da Fig. 5.5 (b). Por serem imagens diferentes (Fig. 5.5 (a) e Fig. 5.5 (b)) e por terem sido utilizadas funções diferentes, apresentam imagens codificadas (Fig. 5.6 e Fig. 5.7) diferentes. É possível observar que a imagem codificada não tem semelhança com as imagens originais. A mensagem, contida na Fig. 5.5 (a), não pode ser decifrada nas Fig. 5.6 (a) e Fig. 5.6 (b), no entanto, pode ser parcialmente decifrado na Fig. 5.6 (c). A mensagem na Fig. 5.5 (b) que poderia ser lida por leitor de código QR, não pode ser

decifrada na Fig. 5.7 codificada.

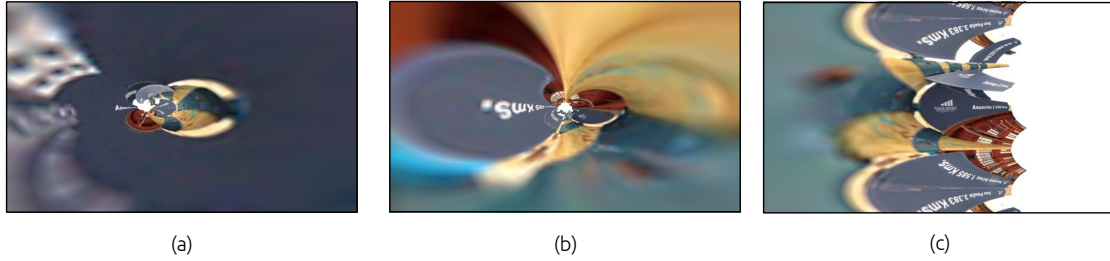


Figura 5.6 - Imagens codificadas utilizando a Fig. 5.5 (a) e as expressões (5.1), (5.2) e (5.3).

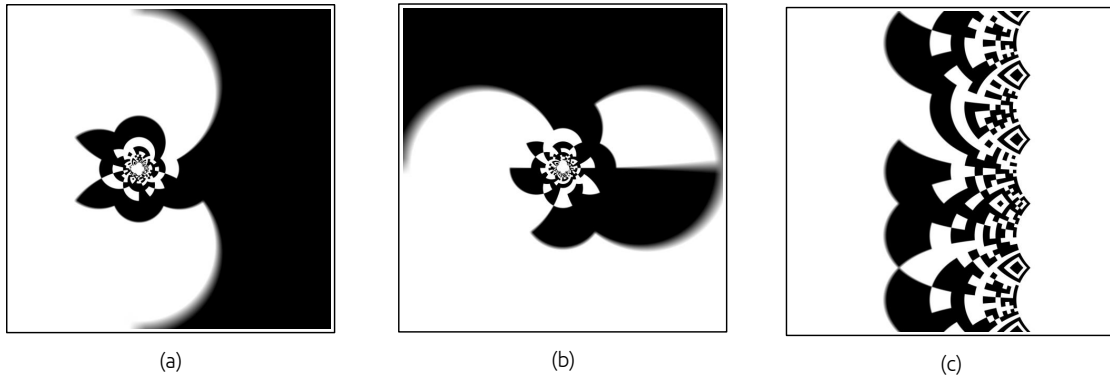


Figura 5.7 - Imagens codificadas utilizando a Fig. 5.5 (b) e as expressões (5.1), (5.2) e (5.3).

5.3.2 Decodificação

Após o processo de codificação, as Fig. 5.6 e Fig. 5.7 foram submetidas ao processo de recuperação das informações, através da decodificação. Neste processo são utilizadas as funções inversas de (5.1), (5.2) e (5.3), dadas por:

$$z = f(w) = \frac{-w}{w - 1} \quad (5.4)$$

$$z = f(w) = \frac{1}{w + i} \quad (5.5)$$

$$z = f(w) = \frac{4 \cdot \log(w)}{\pi} \quad (5.6)$$

As expressões (5.4), (5.5) e (5.6) serão as chaves para o processo de decodificação. Portanto, de posse das Fig. 5.6 e Fig. 5.7 e das funções transformadoras inversas (chaves), pode-se realizar o processo de decodificação. As Fig. 5.8 e Fig. 5.9 apresentam os resultados da decodificação. Observa-se nas Fig. 5.8 (b), Fig. 5.8 (c) e Fig. 5.8 (d), que são a decodificação da Fig. 5.5 (a), que ocorreu a recuperação dos dados codificados quase em sua totalidade (observe a Fig. 5.5 (a), imagem original), apresentando leitura das mensagens inseridas nas placas.

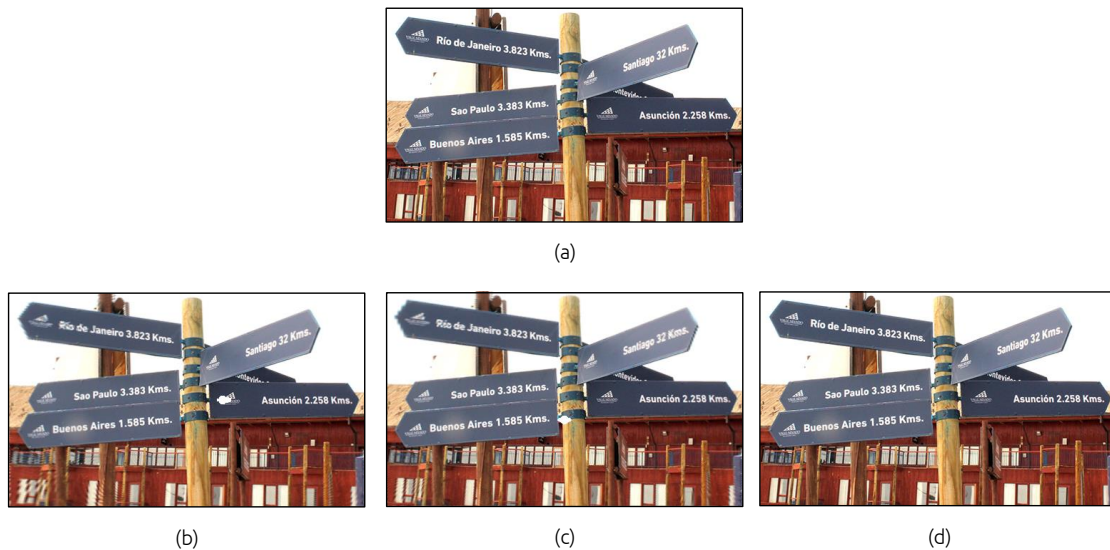


Figura 5.8 - Imagem original e imagens decodificadas utilizando a Fig. 5.6 e as expressões (5.4), (5.5) e (5.6).

Analisando as Fig. 5.9 (b), Fig. 5.9 (c) e Fig. 5.9 (d), que são a decodificação da Fig. 5.5 (b), observa-se que ocorreu a recuperação dos dados codificados quase em sua totalidade (observe a Fig. 5.9 (a), imagem original) e que os dados decodificados podem novamente serem lidos através de leitor de código QR. Os processos de codificação e decodificação produziram perda de dados nos centros das imagens. Isto ocorre devido ao operador de divisão nas funções transformadoras, que quando as coordenadas do plano- z ou plano- w são pequenos, próximos de *zero*, produz o efeito de perda. Cada tipo de função transformadora produz tipo diferente de imagem codificada, produzindo também efeito de perda diferente na imagem decodificada.

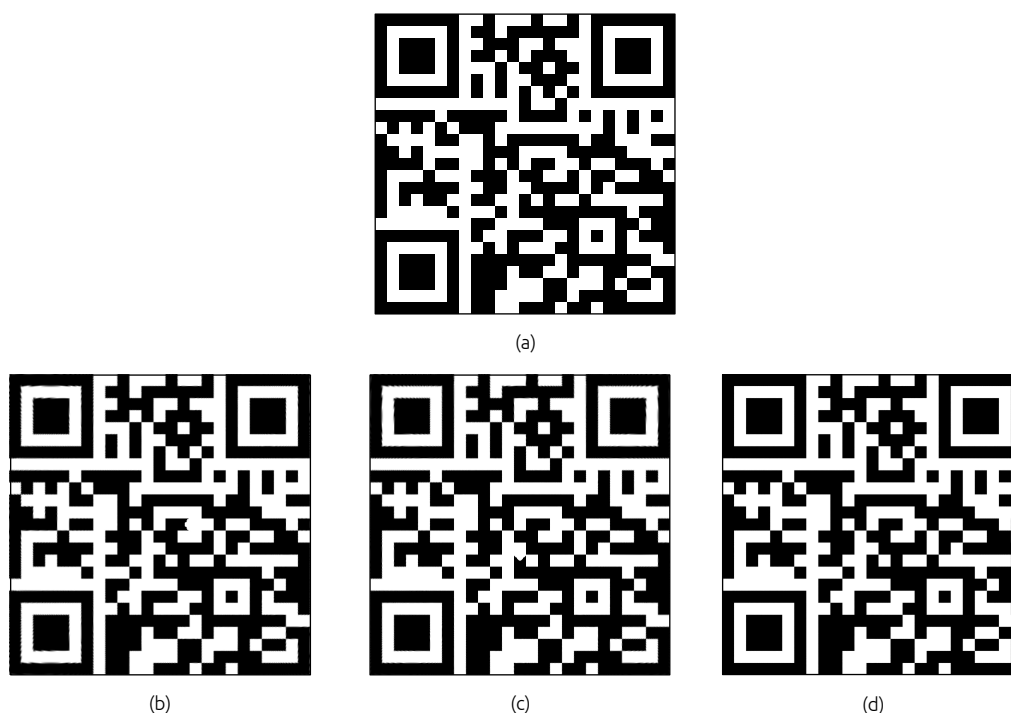


Figura 5.9 - Imagem original e imagens decodificadas utilizando a Fig. 5.7 e as expressões (5.4), (5.5) e (5.6).

5.3.3 Comparativo entre imagens originais e decodificadas

A imagem decodificada deve ser, no melhor dos casos, idêntica a imagem original. No entanto, no processo de codificação e decodificação há as perdas que são diferentes, dependendo da função transformadora, da imagem e outros fatores. Foi realizada análise para avaliar numericamente os resultados obtidos, comparando o desempenho de cada função transformadora (5.1), (5.2) e (5.3). O tamanho dos arquivos originais e decodificados foram avaliados assim como a similaridade, utilizando o método de determinação de qualidade de imagem SSIM, que indica em percentual o quanto a imagem decodificada é similar à imagem original. A Tabela 5.1 dispõe o comparativo entre o tamanho do arquivo original e o tamanho do arquivo decodificado.

Na comparação entre o arquivo de imagem original e os decodificados na Fig. 5.8, observa-se que a diferença máxima foi obtida utilizando as expressões (5.1) e (5.2) como chave de codificação, com 4,68% de diferença entre as imagens. Quando comparado a mesma imagem original e a decodificada utilizando a expressão (5.3), obtém-se o valor de 1,28% de diferença. O índice de similaridade encontrado utilizando o SSIM foi superior a 94,5% para todas as imagens da Fig. 5.8. As diferenças visuais

Tabela 5.1 - Comparativo imagem original \times imagem decodificada.

Imagem	Chave	SSIM
Fig. 5.8 (b)	(5.1)	94,56%
Fig. 5.8 (c)	(5.2)	96,22%
Fig. 5.8 (d)	(5.3)	99,85%
Fig. 5.9 (b)	(5.1)	96,59%
Fig. 5.9 (c)	(5.2)	96,53%
Fig. 5.9 (d)	(5.3)	99,92%

de similaridade entre a imagem original e as imagens decodificadas são ilustradas na Fig. 5.10.

A relação entre as imagens são: Fig. 5.10 (a) diferença entre original e Fig. 5.8 (b) e expressão (5.1), Fig. 5.10 (b) diferença entre original e Fig. 5.8 (c) e expressão (5.2), Fig. 5.10 (c) diferença entre original e Fig. 5.8 (d) e expressão (5.3). Os mapeamentos das diferenças entre as imagens são ilustradas na cor cinza, onde a localização das tonalidades mais escuras representam a localização da maior diferença entre as imagens.

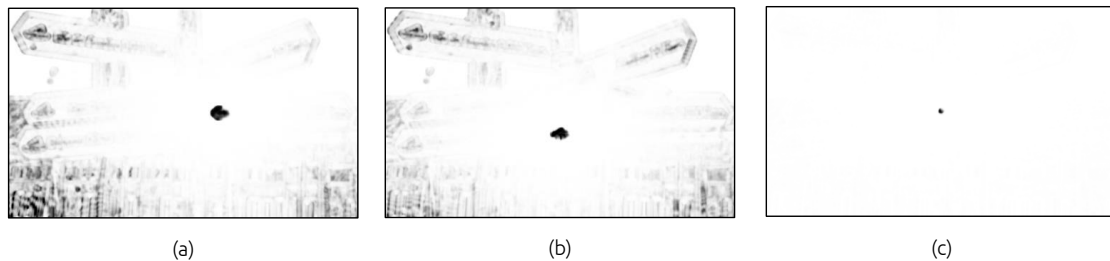


Figura 5.10 - Mapa de diferenças entre imagem original e imagens decodificadas das Fig. 5.8 de (b) a (d).

Na comparação entre o arquivo de imagem original e os decodificados na Fig. 5.9, observa-se que a diferença máxima, foi obtida utilizando a expressão (5.2) como chave de codificação, com valor 2.266,68% de diferença entre as imagens. Quando comparado a mesma imagem original e decodificada utilizando a expressão (5.3), obtém-se o valor de 1.333,33% de diferença. Relacionando estes resultados com os resultados obtidos nas imagens da Fig. 5.10, pode-se abstrair que, não somente a função transformadora contribui para a perda de qualidade no processo de decodi-

ificação, mas as características das imagens também.

O índice de similaridade encontrado utilizando o SSIM, para as Fig. 5.9 de (b) à (d) foi superior a 96,5%. A diferença visual de similaridade entre a imagem original e as imagens decodificadas da Fig. 5.9 são ilustradas na Fig. 5.11. A relação entre as imagens são: Fig. 5.11 (a) diferença entre original e Fig. 5.9 (b) e expressão (5.1), Fig. 5.11 (b) diferença entre original e Fig. 5.9 (c) e expressão (5.2), Fig. 5.11 (c) diferença entre original e Fig. 5.9 (d) e expressão (5.3).

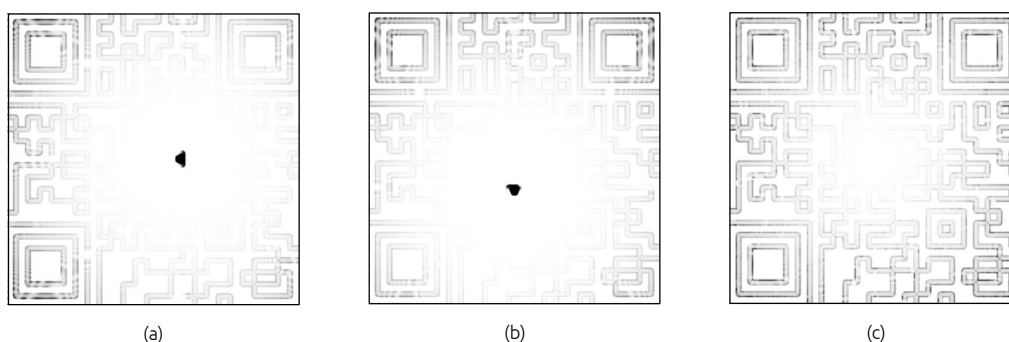


Figura 5.11 - Mapa de diferenças entre imagem original e imagens decodificadas das Fig. 5.9 de (b) à (d).

5.4 Estudo de Caso 2: codificação e decodificação de imagens com inserção de ruídos

O intuito deste estudo de caso é analisar o processo de codificação e decodificação proposto, inserindo diferentes tipos de ruídos na imagem. O objetivo é observar a sensibilidade das transformações conformes com relação aos ruídos inseridos no processo. Os ruídos foram inseridos nos arquivos gerados na codificação, acrescentando três tipos diferentes de modificação na imagem codificada. A Fig. 5.12 ilustra imagem original contendo código binário. Na tradução deste código binário tem o texto: *Conformal Mapping applied on images* e plano de fundo colorido.

Foi utilizada como chave para codificação a função transformadora (5.7). A Fig. 5.13 (a) apresenta resultado da codificação sem inserção de ruídos, a Fig. 5.13 (b) apresenta resultado da codificação com inserção de ruídos de *pixels* na cor preta e branca. Na Fig. 5.13 (c) é apresentado resultado da codificação com inserção de ruído de desfoque e a Fig. 5.13 (d) apresenta imagem resultante da codificação convertida



Figura 5.12 - Imagem colorida contendo código binário.

para escala de cinza.

$$w = f(z) = \tan z \quad (5.7)$$

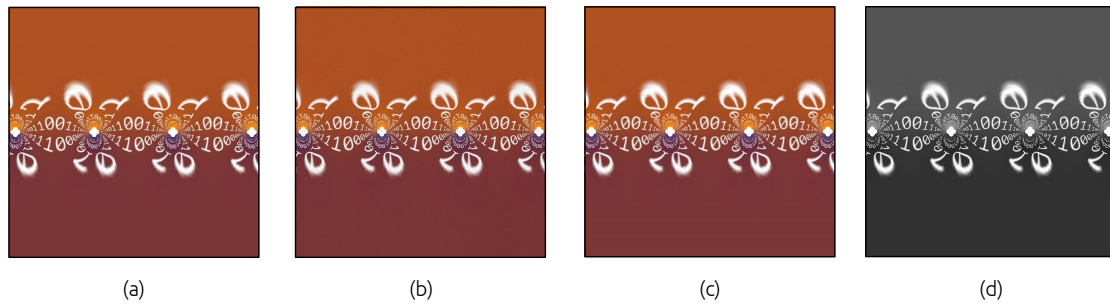


Figura 5.13 - Resultado da codificação das Fig. 5.12: (a) sem ruído (apenas (5.7)), (b) com ruído de *pixels*, (c) com ruído de desfoque e (d) em escala de cinza.

Utilizando a expressão (5.8), produz-se a decodificação das imagens codificadas da Fig. 5.13. As Fig. 5.14 (a) e Fig. 5.14 (b), são resultados da decodificação das Fig. 5.13 (a) e Fig. 5.13 (b), respectivamente, apresentando a mensagem binária completamente recuperada, com alguma perda na Fig. 5.14 (b). Na Fig. 5.14 (c), que é o resultado da decodificação da Fig. 5.13 (c), a imagem foi recuperada apresentando distorções próximas das bordas, com perda da mensagem. Na Fig. 5.14 (d), resultado da decodificação da Fig. 5.13 (d), a imagem foi recuperada em sua totalidade.

$$z = f(w) = \arctan w \quad (5.8)$$

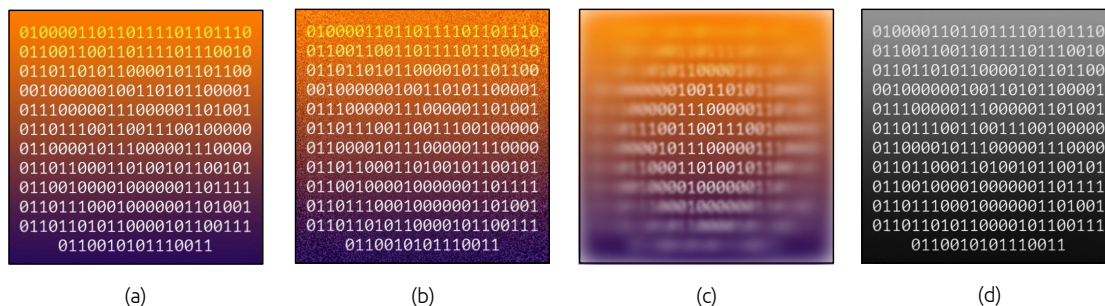


Figura 5.14 - Resultado da decodificação das Fig. 5.13: (a) sem ruído (apenas (5.8)), (b) com ruído de *pixels*, (c) com ruído de desfoque e (d) em escala de cinza.

Para avaliar o nível de interferência de cada tipo de ruído, as imagens das Fig. 5.14 de (a) à (d) foram comparadas com a imagem original Fig. 5.12, utilizando o índice de similaridade SSIM. A Fig. 5.15 (a) apresenta o resultado da comparação da Fig. 5.14 (a), que utilizou apenas as transformações conformes sem inserção de ruídos, com a imagem original. Esta comparação apresentou índice de similaridade de 98,04%. A Fig. 5.15 (b) é o resultado da comparação da Fig. 5.14 (b), que foi inserido ruído de *pixels* e a imagem original. Esta comparação apresentou índice de similaridade de aproximadamente 62,00% e mesmo com valor de índice de similaridade baixo, é possível decifrar a mensagem. A Fig. 5.15 (c) apresenta o resultado da comparação da Fig. 5.14 (c), onde foi inserido ruído de desfoque, com a imagem original. Esta comparação apresentou índice de similaridade de aproximadamente 45,00%. Com este valor de índice de similaridade não é possível decifrar a mensagem. Na Fig. 5.15 (d) é ilustrado o resultado da comparação da Fig. 5.14 (d), que utilizou ruído em escala de cinza e a imagem original. Esta comparação apresentou índice de similaridade de 92,49% e modificação na imagem para escala de cinza.

Os métodos tradicionais de codificação digital não possuem robustez quando submetidos a ruídos. Qualquer tipo de alteração de posicionamento, conteúdo e de coloração afeta o resultado final a ponto de não ser possível recuperar o conteúdo após a decodificação. O método proposto apresenta robustez com relação a inserção de ruídos.

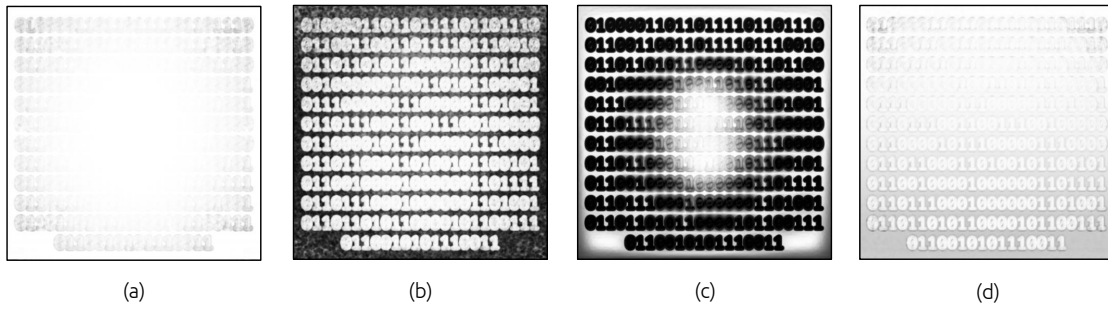


Figura 5.15 - Mapa de diferenças entre imagem original e decodificadas: (a) sem ruído (apenas (5.8)), (b) com ruído de *pixels*, (c) com ruído de desfoque e (d) em escala de cinza.

5.5 Estudo de Caso 3: codificação e decodificação de imagens impressas

O intuito deste estudo de caso é analisar a proposta de inserção de mensagem escrita em meio físico, como fotografia impressa. Portanto, de posse da imagem contendo mensagem, como ilustrada na Fig. 5.16, produz-se o processo de codificação. Neste caso foi utilizado a função transformadora (5.9).

$$w = f(z) = \frac{z - 1}{z} \quad (5.9)$$

```

20OVh8_N9/x6#7dWC:27D
L8&8r7p: BIOV1.a*!S643YI/
pX8DMENSAGEM2DAT7
>9p627B99OIASN{.DO424C
CE43E552B2S0MZEN70R7Jj
kkoMjY05m1u8UCkK77&R4
2UioK2Ei$9Z^K]ES3sIxZ.Jda
w7Z1233SSECRETA#z2eH
D;k2Ei$9Z^K]ES3sIR7i39`g:
a5C]!Q69hL22]aG2+Gw95L6
ZWUhEyV95L6ZWUhEy20

```

Figura 5.16 - Imagem contendo mensagem a ser transmitida.

A imagem da Fig. 5.16, contém vários caracteres gerados aleatoriamente e duas palavras com o texto: *MENSAGEM SECRETA* na cor vermelha. No processo de codificação, a imagem da Fig. 5.16 é transformada na imagem da Fig. 5.17 (a). A imagem da Fig. 5.17 (a) é impressa com marcas de balizamento como ilustrado na Fig. 5.17 (b). A impressão foi realizada por impressora jato de tinta em papel sulfite

comum e resolução 300dpi.

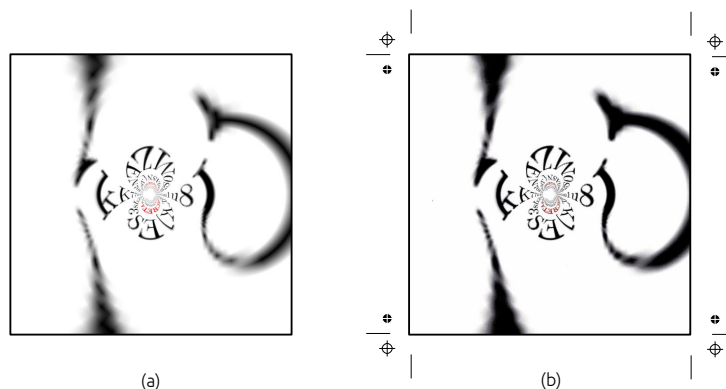


Figura 5.17 - (a) Imagem codificada digital. (b) Imagem codificada com marcas para impressão.

A imagem impressa foi escaneada em equipamento com resolução de 600dpi. A imagem resultante deste escaneamento foi submetida ao *software* para decodificação. A função inversa de (5.9) é dada por:

$$z = f(w) = \frac{-1}{w - 1} \quad (5.10)$$

A função em (5.10) é a chave para a decodificação. O resultado da decodificação é apresentado na Fig. 5.18. Devido ao processo de impressão, a imagem codificada sofreu adição de ruídos, desde o momento da inserção das marcas para impressão (balizamento) até chegar na imagem decodificada. O problema é que os ruídos são inseridos e o resultado da diferença na similaridade entre a imagem original e a decodificada, será a soma destes ruídos. Mesmo utilizando equipamento e papel de baixa qualidade, foi possível resgatar a mensagem inserida na imagem da Fig. 5.16. Os métodos tradicionais de codificação e decodificação de imagens são restritos ao meio digital, não podendo ser utilizados no processo de decifrar, quando a mensagem está em meio físico.

CAPÍTULO 6

CONCLUSÃO

Este trabalho propôs método que utiliza transformações conformes para codificar e decodificar imagens. As imagens originais foram transformadas entre os domínios complexos utilizando chaves, que são funções transformadoras. A diferença desta metodologia com as demais, é a capacidade de decodificar a mensagem contida na imagem que está impressa. O método de codificação e decodificação de imagens utilizando a teoria de transformações conformes é eficiente. Os resultados obtidos apresentaram que, diferentes chaves produzem diferentes codificações e que para se obter resultados satisfatórios de codificação, a chave a ser utilizada deverá ser escolhida criteriosamente. A escolha da função transformadora é etapa importante no processo de codificação e pode resultar em codificação eficiente ou ineficiente para ocultar as mensagens a serem transmitidas. O método proposto apresentou robustez superior à outros métodos de criptografia visual por ter apresentado capacidade de recuperação das mensagens transmitidas mesmo com a presença de ruídos gerados digitalmente ou fisicamente através da impressão e escaneamento da imagem impressa. Este último é capacidade inédita entre os métodos de criptografia visual, pela capacidade de decodificar mensagens impressas. Existem algumas restrições observadas durante os experimentos: i) funções transformadoras elementares como a transformação por rotação, transformação por translação e a transformação por dilatação ou contração, não fornecem codificação com embaralhamento suficiente para não identificação da mensagem; ii) funções transformadoras com pontos críticos utilizando operador de divisão, podem ocasionar perda de informação visual, devendo ser observada esta limitação ao inserir mensagens na imagem; iii) o método é limitado quando a imagem codificada é submetida a mudança acentuada do posicionamento dos *pixels*.

6.1 Contribuições do Trabalho

Durante o desenvolvimento deste trabalho foram realizadas contribuições científicas através da publicação de trabalhos e registro de *software*:

- Artigos submetidos e aceitos em congresso:
 1. SILVA, A. H. F.; MAGALHÃES, A. S.; SILVA, U. F.; ALVES, A. J.; CALIXTO, W. P.; JÚNIOR, J. L. F. and OLIVEIRA, M. A. A. **Con-**

formal Mapping Applied to Encoding and Decoding Images. Florence, Italy: 16 IEEE International Conference on Environment and Electrical Engineering, 2016;

2. SILVA, A. H. F.; MAGALHÃES, A. S.; SILVA, U. F.; DOMINGUES, E. G.; ALVES, A. J. and CALIXTO, W. P. **Conformal Mapping Applied to Encoding and Decoding of Images.** Santiago, Chile: 2015 CHILEAN Conference on Electrical, Electronics Engineering, Information and Communication Technologies (CHILECON), 2015;
3. SILVA, U. F.; JÚNIOR, M. I. Q.; FURRIEL, G. P.; SILVA, A. H. F.; ALVES, A. J. and CALIXTO, W. P. **Application of Conformal Mapping in the Calculation of Geological Pressures.** Santiago, Chile: 2015 CHILEAN Conference on Electrical, Electronics Engineering, Information and Communication Technologies (CHILECON), 2015;
4. SILVA, A. H. F.; MAGALHÃES, A. S.; SILVA, U. F. and CALIXTO, W. P. **Codificação e Decodificação de Imagens via software utilizando Transformações Conformes,** Goiânia, Brasil. 12º Congresso de Pesquisa, Ensino e Pesquisa CONPEEX, 2015;
5. SILVA, U. F.; SILVA, A. H. F. and CALIXTO, W. P. **Uso das Transformações Conformes no Cálculo de Pressões Surge e Swab,** Goiânia, Brasil. 12º Congresso de Pesquisa, Ensino e Pesquisa CONPEEX, 2015;
6. SILVA, A. H. F.; MAGALHÃES, A. S.; SILVA, U. F.; DOMINGUES, E. G.; ALVES, A. J. and CALIXTO, W. P. **Cálculo de capacitância em capacitores de placas cilíndricas e semi-cilíndricas utilizando Transformações Conformes,** Goiânia, Brasil. 11º Congresso de Pesquisa, Ensino e Pesquisa CONPEEX, 2014.

- Registro de software:

7. Foi depositado, junto ao Instituto Nacional de Propriedade Industrial (INPI), sob protocolo número *BR 51 2016 00044 9*, como Registro de Programa de Computador, o registro do *software* CODITRAC desenvolvido durante o trabalho.

6.2 Sugestões para Trabalhos Futuros

Através dos experimentos o método desenvolvido apresentou capacidades a serem exploradas em trabalhos futuros, podendo ser listadas:

- a) Otimização da chave codificadora para conseguir melhor embaralhamento com menor distorção da imagem decodificada;
- b) Estudo da aplicação do método na recuperação informação de imagens impressas deterioradas ou desgastadas pelo tempo;
- c) Avaliar matematicamente a interferência da chave de codificação na distorção da imagem decodificada;
- d) Criar versão híbrida unindo o método proposto a outros métodos de criptografia visual;
- e) Avaliar capacidade de compressão de imagens utilizando o método proposto, minimizando a perda visual;
- f) Verificar capacidade de utilização do método como criptografia sonora;
- g) Avaliar a possibilidade de codificação e decodificação com mais de uma chave.

REFERÊNCIAS BIBLIOGRÁFICAS

ARTZ, D. **Digital Steganography: Hiding Data within Data**. IEEE Internet Computing: IEEE, 2002. [23](#)

AUBRY, A.; LEI, D. Y.; MAIER, S. A.; PENDRY, J. B. **Conformal transformation applied to plasmonics beyond the quasistatic limit**. American Physical Society: Physical Review B, 2010. [23](#)

BRENNA, M.; MARTINELLI, F.; ZICH, R. E. **Analysis of the electric field distribution on perfectly conducting wing sections by application of a conformal mapping**. Mathematical Methods in Electromagnetic Theory, 2004. 10th International Conference on: IEEE, 2004. [23](#)

BROWN, J. W.; CHURCHILL, R. V. **Complex variables and Applications**. 8. ed. New Your, USA: McGraw-Hill, 2009. [23](#), [29](#), [32](#)

CALIXTO, W. P. **Aplicação do mapeamento conforme no cálculo do fator de Carter**. Dissertação de Mestrado. Goiânia, Goiás, Brasil: Universidade Federal de Goiás - UFG, 2008. [31](#)

CALIXTO, W. P.; ALVARENGA, B.; MOTA, J. C. da; BRITO, L. C.; WU, M.; ALVES, A. J.; NETO, L. M.; ANTUNES, C. F. R. **Electromagnetic problems solving by conformal mapping: A mathematical operator for optimization**. Hindawi Publishing Corporation: Mathematical Problems in Engineering, 2011. [23](#)

CHANG, Y.; REID, J. F. **RGB calibration for color image analysis in machine vision**. Image Processing, IEEE Transactions on: IEEE, 1996. [40](#)

DHOLE, A. B.; JANWE, N. J. **Visual Cryptography in Gray Scale Images**. [S.l.]: International Journal of Engineering Research and Development, 2013. [43](#)

FERNANDEZ, C. S.; JR, N. C. B. **Introdução às Funções de uma Variável Complexa**. Rio de Janeiro, Brasil: SBM, 2006. [30](#)

FERNANDÈZ, D. P. **Parametrizaciones Conformes Elementales de Supercifres**. Cantoblanco, Madrid, Spain: Universidad Autonoma de Madrid, 2012. [32](#)

- FREDERICK, C.; SCHWARTZ, E. L. **Conformal Image Warping**. [S.l.]: Computer Graphics and Applications, IEEE, 1990. [24](#)
- GAYATHRI, R.; NAGARAJAN, V. **Secure data hiding using steganographic technique with Visual cryptography and watermarking scheme**. Communications and Signal Processing (ICCSP), 2015 International Conference on: IEEE, 2015. [25](#)
- GONG, W.; XIE, X.; MA, R.; WU, T. **Angle-Preserving Quadrilateral Mesh Parameterization**. IEEE Computer Society: IEEE, 2015. [23](#)
- GONZALEZ, R. C.; WOODS, R. E. **Digital Imaging Processing**. New Jersey, USA: Prentice hall Upper Saddle River, 2001. [24](#)
- GU, X.; WANG, Y.; CHAN, T. F.; THOMPSON, P. M.; YAU, S. **Genus Zero Surface Conformal Mapping and Its Application to Brain Surface Mapping**. Ambleside, UK: IEEE Transactions on Medical Imaging, 2004. [31](#)
- HAMDY, M. M.; MOSTAFA, A. A.; EL-SISI, A. B. **Image Compression Ratio Enhancement Based on Conformal Mapping**. [S.l.]: 8th International Conference on Computer Engineering & Systems (ICCES), IEEE, 2013. [24](#)
- HARALICK, R. M.; SHANMUGAM, K.; DINSTEN, I. H. **Textural features for image classification**. IEEE: Systems, Man and Cybernetics, IEEE Transactions on, 1973. [40](#)
- HARLEY, J. B.; WOODWARD, D. **Prehistoric Maps and the History of Cartography: An Introduction**. USA: The Mathematical Association of America, 1987. [27](#)
- HASNAT, M. A.; ALATA, O.; TRÉMEAU, A. **Joint Color-Spatial-Directional clustering and Region Merging (JCSD-RM) for unsupervised RGB-D image segmentation**. IEEE Computer Society: IEEE, 2015. [40](#)
- HENRICI, P. **Applied and Computational Complex Analysis**. [S.l.]: John Wiley & Sons, Inc., 1993. [36](#)
- HOU, Y. C. **Visual cryptography for color images**. Pattern Recognition 36: Elsevier, 2003. [43](#), [44](#)

HSU, Y.; HSU, W.; FAN, S.; LIN, H.; LIU, C.; JIANG, S. **Application of Image Processing to Laser Reflective Pattern for Multi-layer Auto-focusing System**. Wellington, New Zealand: Seventh International Conference on Sensing Technology (ICST), IEEE, 2013. [24](#)

KIM, J.; JEONG, H.; KIM, H.; KIM, C. **Adaptation of neural network and application of digital ultrasonic image processing for the pattern recognition of defects in Semiconductor**. Jeju Island, South Korea: Advances in Electronic Materials and Packaging, IEEE, 2001. [24](#)

KRANTZ, S. G. **An Episodic History of Mathematics: Mathematical Culture Through Problem Solving**. United States of America: The Mathematical Association of America, 2010. [27](#), [29](#)

KREYSZIG, E. **Advanced Engineering Mathematics**. 10. ed. Ohio, USA: John Wiley & Sons, Inc, 2011. [28](#), [35](#)

KYTHER, P. K. **Computational Conformal Mapping**. United States of America: Springer Science & Business Media, 2012. [23](#)

LI, S.; ZENG, W.; ZHOU, D.; GU, D. X.; GAO, J. **Compact conformal map for greedy routing in wireless mobile sensor networks**. IEEE Computer Society: IEEE, 2013. [23](#)

LIU, Y.; CHEN, H.; NAEEM, M. **Infinite Maxwell fish-eye in a finite area**. Advanced Electromagnetic Materials in Microwaves and Optics (METAMATERIALS), 2015 9th International Congress on: IEEE, 2015. [23](#)

MCFARLANE, M. D. **Digital pictures fifty years ago**. Proceedings of the IEEE: IEEE, 1972. [24](#)

MERINO, O. **A Short History of Complex Numbers**. Kingston, USA: University of Rhode Island, 2006. [28](#)

MILNOR, J. W. **Picture transmission by submarine cable**. Electrical Engineering: IEEE, 1941. [24](#)

NAOR, M.; SHAMIR, A. **Visual Cryptography**. Italy: Advances in Cryptology - EUROCRYPT 94, 1994. [25](#), [42](#)

PANG, J.; FANG, L.; ZENG, J.; GUO, Y.; TANG, K. **Subpixel-Based Image Scaling for Grid-Like Subpixel Arrangements: A Generalized Continuous-Domain Analysis Model**. IEEE: IEEE Signal Processing Society, 2016. [40](#)

PORTER, R. M. **History and recent developments in techniques for numerical conformal mapping**. IWQCMA05: Proceedings of the International Workshop on Quasiconformal Mappings and Their Applications, 2005. [23](#)

RAMADAS, S. N.; JACKSON, J.; TWEEDIE, A.; O'LEARY, R.; GACHAGAN, A. **Conformally mapped 2D ultrasonic array structure for NDT imaging application**. IEEE International Ultrasonics Symposium: IEEE, 2010. [24](#)

ROBERTS, L. G. **Picture coding using pseudo-random noise**. Information Theory, IRE Transactions on: IEEE, 1962. [24](#)

ROJER, A. S.; SCHWARTZ, E. L. **Design considerations for a space-variant visual sensor with complex-logarithmic geometry**. Pattern Recognition, 1990. Proceedings., 10th International Conference on: IEEE, 1990. [24](#)

SCHWARTZ, E. L. **Anatomical and physiological correlates of visual computation from striate to infero-temporal cortex**. Systems, Man and Cybernetics, IEEE Transactions on: IEEE, 1984. [24](#)

SHI, R.; ZHU, H.; GU, D. X.; LIANG, J. Z. **Efficient Colon Wall Flattening by Improved Conformal Mapping Methodologies for Computed Tomography Colonography**. Valencia, Spain: Nuclear Science Symposium and Medical Imaging Conference (NSS/MIC), IEEE, 2011. [31](#)

SHIMOBABA, T.; KAKUE, T.; ENDO, Y.; HIRAYAMA, R.; HIYAMA, D.; HASEGAWA, S.; NAGAHAMA, Y.; SANO, M.; SUGIE, T.; ITO, T. **Optical encryption for large-sized images using random phase-free method**. Optical Society of America: IEEE, 2015. [46](#)

SILVA, U. F.; JÚNIOR, M. I. Q.; FURRIEL, G. P.; SILVA, A. H. F.; ALVES, A. J.; CALIXTO, W. P. **Application of Conformal Mapping in the Calculation of Geological Pressures**. Santiago, Chile: 2015 CHILEAN Conference on Electrical, Electronics Engineering, Information and Communication Technologies (CHILECON), 2015. [23](#)

- SILVESTER, P. P.; FERRARI, R. L. **Finite Elements for Electrical Engineers**. 2. ed. Cambridge, UK: Cambridge University Press, 1996. 32
- SPIEGEL, M. R. **Variáveis Complexas com uma Introdução as Transformações Conformes e suas Aplicações**. São Paulo, Brasil: McGraw Hill do Brasil, 1972. 29
- STINSON, D. R. **Cryptography: Theory and Practice, Third Edition**. Canada: Chapman & Hall CRC, 2006. 23
- SUBRAMANIAN, G. K.; LOGANATHAN, D. **Color Image Cryptography Scheme Based on Visual Cryptography**. Thuckalay, India: International Conference on Signal Processing, Communication, Computing and Networking Technologies (ICSCCN), IEEE, 2011. 41
- SYCHEV, A. N.; CHEKALIN, M. A.; STRUCHKOV, S. M. **Combining the partial-capacitance and the conformal mapping techniques for analysis of the multiconductor microstrip lines**. Roma, Italy: 44th European Microwave Conference (EuMC), 2014. 31
- TENG, Y.; ZHANG, Y.; CHEN, Y.; TI, C. **Adaptive Morphological Filtering Method for Structural Fusion Restoration of Hyperspectral Images**. IEEE Geoscience & Remote Sensing Society: IEEE, 2016. 40
- UPTON, R.; HADDAD, K.; SØRENSEN, J. **Conformal Mapping Techniques for Consumer Products**. Cleveland, USA: Sound and Vibration, Bay Village, Ohio, Acoustical Publications, Inc., 2008. 31
- VANDERBRUG, G. J. **Line detection in satellite imagery**. IEEE: Laboratory for Applications of Remote Sensing, 1975. 40
- VERNAM, G. S. **Cipher printing telegraph systems: For secret wire and radio telegraphic communications**. AIEE, Journal of the: IEEE, 1926. 25
- WANG, Z.; BOVIK, A. C.; SHEIKH, H. R.; SIMONCELLI, E. P. **Image quality assessment: from error visibility to structural similarity**. Image Processing, IEEE Transactions on: IEEE, 2004. 51
- WECHSLER, H.; ZIMMERMAN, G. L. **2-D invariant object recognition using distributed associative memory**. Pattern Analysis and Machine Intelligence, IEEE Transactions on: IEEE, 1988. 24

XIONG, H.; YU, W.; YANG, X.; SWAMY, M. N. S.; YU, Q. **Learning the Conformal Transformation Kernel for Image Recognition**. IEEE TRANSACTIONS ON NEURAL NETWORKS AND LEARNING SYSTEMS: IEEE, 2015. [23](#), [24](#), [25](#)

YADONG, W.; YONGGUO, H.; HONGYING, Z. **Image Encoding and Decoding Scheme Based on Digital Image Inpainting Technology**. Kiev, Ukraine: International Conference on Information Technology and Computer Science, 2009. ITCS 2009, IEEE, 2009. [24](#)

ZIMMERMANN, P. **An Introduction to Cryptography**. Santa Clara, California, USA: Network Associates, Inc., 2000. [25](#), [41](#)

GLOSSÁRIO

Chave de Codificação - é o elemento alfanumérico utilizado para realizar uma criptografia.

Código QR - ou *QR Code* (sigla do inglês Quick Response Code) é um código de barras bidimensional que pode ser escaneado usando a maioria dos telefones celulares equipados com câmera.

CODITRAC - é o nome do software codificador e decodificador de imagens utilizando transformações conformes.

Criptografia - é o processo de ocultação de mensagem através de processos de embaralhamento dos dados.

Criptografia Visual - é o processo de ocultação do conteúdo de imagem através de processos de embaralhamento dos dados de cores.

Domínio - conjunto de valores possíveis das abscissas x para uma região onde uma função é definida.

Função Transformadora - é a função utilizada para levar os dados de um domínio a doutro.

Mapa de diferenças - é o mapa gerado pelo cálculo do *SSIM* que determina visualmente as diferenças encontradas entre na imagem avaliada em relação à imagem referência.

pixel - é a menor unidade computacional que contém as informações de cores do ponto de uma imagem digital.

