NAIARA CRISTINA MATIELO

**Cifragem óptica de imagens utilizando máscara binária
aleatória**

Dissertação apresentada à Escola de
Engenharia de São Carlos da
Universidade de São Paulo para obtenção
do título de Mestre em Ciências,
Programa de Engenharia Elétrica.

Área de Concentração:
Telecomunicações

Orientador: Prof. Dr. Luiz Gonçalves
Neto

São Carlos
2011

Trata-se da versão corrigida da dissertação. A versão original se encontra disponível na EESC/USP que aloja o Programa de Pós-Graduação de Engenharia Elétrica.

AUTORIZO A REPRODUÇÃO E DIVULGAÇÃO TOTAL OU PARCIAL DESTE TRABALHO, POR QUALQUER MEIO CONVENCIONAL OU ELETRÔNICO, PARA FINS DE ESTUDO E PESQUISA, DESDE QUE CITADA A FONTE.

Ficha catalográfica preparada pela Seção de Tratamento
da Informação do Serviço de Biblioteca – EESC/USP

M433c Matielo, Naiara Cristina
 Cifragem óptica de imagens utilizando máscara binária
 aleatória / Naiara Cristina Matielo ; orientador Luiz
 Gonçalves Neto. -- São Carlos, 2011.

 Dissertação (Mestrado-Programa de Pós-Graduação em
Engenharia Elétrica e Área de Concentração em
Telecomunicações) -- Escola de Engenharia de São Carlos
da Universidade de São Paulo, 2011.

 1. Telecomunicações. 2. Modulação de fase.
3. Modulação de amplitude. 4. Método de contraste de
fase. 5. Transformada de Fourier. I. Título.

FOLHA DE JULGAMENTO

Candidato(a): Bacharel **NAIARA CRISTINA MATIELO**.

Dissertação defendida e julgada em 01/04/2011 perante a Comissão Julgadora:

Prof. Associado **LUIZ GONÇALVES NETO** – (Orientador)
(Escola de Engenharia de São Carlos/USP)

Aprovada

Prof. Dr. **GIUSEPPE ANTONIO CIRINO**
(Universidade Federal de São Carlos/UFSCar)

APROVADA

Prof. Dr. **JOSÉ CARLOS PIZOLATO JUNIOR**
(Universidade Federal de São Carlos/UFSCar)

Aprovada

Prof. Titular **DENIS VINÍCIUS COURY**
Coordenador do Programa de Pós-Graduação em
Engenharia Elétrica

Prof. Associado **PAULO CÉSAR LIMA SEGANTINE**
Presidente da Comissão da Pós-Graduação da EESC

AGRADECIMENTOS

Agradeço a Deus por ter me dado força e ter me ajudado a não desistir diante das dificuldades encontradas durante a realização deste trabalho.

Agradeço aos meus pais, Vania e José Carlos, pelo amor, incentivo, paciência e compreensão, não apenas durante o desenvolvimento deste trabalho, mas por toda a vida. E também pela certeza da vitória da conclusão deste.

Agradeço a minha irmã Naila por ter tido paciência comigo nos momentos de desespero e também pelas ajudas nas leituras de artigos em inglês.

Agradeço as minhas amigas, Ana Maria Vasconcelos, Daiane de Souza e Natália Costa de Lima, pelos momentos de conversa, desabafos e principalmente pelos incentivos para eu terminar este trabalho.

Agradeço ao Prof. Dr. Luiz Gonçalves Neto, meu orientador e amigo, por ter me recebido tão bem e ter acreditado na minha capacidade para realizar este trabalho.

Agradeço ao Prof. Dr. Wagner Vieira Leite Nunes, pela amizade, apoio, incentivo e ensinamentos passados ao longo da minha formação acadêmica.

Agradeço ao generoso auxílio de incontáveis pessoas que compartilharam comigo seus conhecimentos e experiências obtidos durante a fase de dissertação de seus respectivos mestrados.

RESUMO

MATIELO, N. C. Cifragem óptica de imagens utilizando máscara binária aleatória. 2010. Dissertação (Mestrado) – Escola de Engenharia, Universidade de São Paulo, São Carlos, 2010.

Várias técnicas de cifragem óptica de imagens surgem a todo o momento devido à necessidade que se tem de transmitir informações de uma maneira segura e confiável. Nessas técnicas a informação é criptografada de tal modo que para conseguir recuperar a informação criptografada é necessário ter um conhecimento prévio da mesma chave que a criptografou, sendo esta chave única. Isto faz com que as técnicas sejam robustas. Estes processos de cifragem de imagem trabalham com a distribuição de fase obtida diretamente da imagem que se deseja criptografar e conseqüentemente a imagem decodificada também está em modulação de fase. Porém imagens em distribuição de fase não são visíveis ao olho humano. Para transformá-las em modulação de amplitude, a qual é visível ao olho humano, é utilizado o método de contraste de fase de Zernike. Propôs-se então um método para cifrar imagem binária apenas em modulação de amplitude. Após o processo de decodificação, a imagem obtida é reconhecida graças à capacidade do olho humano em discernir regiões contínuas de regiões aleatórias. Este método é de fácil implementação, podendo ser obtido utilizando apenas materiais de baixo custo como papéis, filmes plásticos, etc. Vários ataques foram realizados contra o processo de cifragem óptica de imagens utilizando máscara binária aleatória para analisar a robustez de tal processo. Este processo de cifragem não é robusto ao ataque do texto conhecido e ao ataque das cifras conhecidas.

Palavras-chave: modulação de fase, modulação de amplitude, método de contraste de fase, transformada de Fourier.

ABSTRACT

MATIELO, N. C. Optical image encryption using random binary mask. 2010. Dissertação (Mestrado) - Escola de Engenharia, Universidade de São Paulo, São Carlos, 2010.

Several optical encryption techniques have been developed due to the need to transmit information in a secure and reliable way. In these techniques the information is encrypted in a way that to recover the encrypted information is necessary to have a previous knowledge of the same mask that encrypted it, being this mask unique. Because of this, the techniques are robust. These image encryption methods work with the phase distribution obtained directly from the image that is intended to encrypt and consequently the decrypted image will also be in the phase modulation. But, images in a phase distribution are not visible for the human eyes. To transform them in an amplitude modulation, that is visible for the human eyes, it is used the Zernike phase contrast method. Then, it is proposed a method for encryption and decryption of information processed in a binary form in an amplitude modulation. After the decryption process, the image obtained is recognized because the human eyes are able to differentiate continuous, periodical regions to random pattern. This method has an easy implementation and it can be obtained using regular and inexpensive materials, like paper, plastic films, etc. Many attacks were realized against the proposed method to analyse if this method is robust. This method can not resist the known-plaintext attack and the known-ciphertext attack.

Key-words: amplitude modulation, phase modulation, phase-contrast technique, Fourier transform.

LISTA DE FIGURAS

- FIGURA 1 - Processos de modulação de uma frente de onda planar luminosa. (a) representa a frente de onda luminosa com fase e amplitude constante, (b) representa uma frente de onda luminosa que atravessa um objeto de amplitude e tal frente de onda sofre uma variação de amplitude e (c) representa uma frente de onda luminosa que atravessa um objeto transparente e é modulada em fase. 8
- FIGURA 2 - Estrutura do microscópio de contraste de fase criado por Zernike. 9
- FIGURA 3 - Estrutura de um correlator óptico 4f. O correlator óptico 4f é composto por duas lentes, tendo cada uma delas o comprimento focal f . As lentes são posicionadas entre si a uma distância de $2f$. A primeira lente efetua a primeira transformada de Fourier da imagem localizada no plano de imagem, decompondo-a em suas frequências espaciais. A segunda lente efetua a segunda transformada de Fourier, recuperando a imagem original. 12
- FIGURA 4 - Frentes de onda luminosa após atravessarem um objeto de fase. A onda vermelha é a onda direta, a azul é a onda difratada e a onda verde é a interferência da onda direta pela onda difratada. 14
- FIGURA 5 - Estrutura do correlator óptico 4f com a aplicação da lâmina de fase. A onda luminosa não difrata ao passar pela lâmina de fase sofre um desvio de fase $\pi/2$, que ao sofrer interferência com a onda difratada gera uma onda luminosa modulada em amplitude no plano imagem. 15
- FIGURA 6 - Interferência das ondas luminosas. (a) interferência construtiva e (b) interferência destrutiva. 16
- FIGURA 7 – Método de cifragem de imagem em distribuição de fase utilizando a estrutura do correlator óptico 4f. Coloca-se no plano de entrada do correlator a imagem que se deseja cifrar em distribuição de fase e a chave de fase do processo. Um feixe de ondas ao atravessar tais imagens no plano de entrada sofrerá duas transformadas de Fourier, uma transformada em cada lente do correlator, resultando no plano imagem do correlator óptico 4f a imagem em fase da multiplicação entre as imagens colocadas no plano de entrada. 19

FIGURA 8 – Decodificação de imagem utilizando o método de contraste de fase e um correlator óptico 4f. A decodificação da imagem cifrada se dá através da multiplicação entre a imagem cifrada e a chave de fase do processo. Para que a imagem recuperada após a multiplicação esteja em modulação de amplitude é colocada uma lâmina de fase no plano de Fourier do correlator óptico 4f, conforme a técnica de contraste de fase de Zernike.	21
FIGURA 9 – Imagem do número cinco após o processo de decodificação. O número cinco é visualizado pois a imagem decodificada apresenta uma região periódica, que é o próprio número cinco, e uma região aleatória, que é a parte externa.	23
FIGURA 10 – Operação XOR: multiplicação da chave por uma região de pixels pretos (inversão de bit).....	26
FIGURA 11 – Operação XOR: multiplicação da chave por uma região de pixels brancos.	26
FIGURA 12 - Cifragem binária utilizando máscara binária aleatória. (a) imagem binária original do número “5”. (b) máscara binária aleatória, ruído branco. (c) imagem cifrada.....	29
FIGURA 13 - Imagens após o processo de decodificação. (a) imagem recuperada com a chave correta. (b) imagem recuperada com a chave incorreta.	31
FIGURA 14 – Distribuição de fase contínua da imagem com sua respectiva distribuição em nível de cinza.....	34
FIGURA 15 - Distribuição de fase da imagem com sua respectiva distribuição em nível de cinza.....	34
FIGURA 16- Uma imagem recuperada ao sobrepor a imagem cifrada do número 5 com uma chave aleatória qualquer. A imagem recuperada foi a do número um enquanto a imagem original é o número cinco.	38
FIGURA 17 - Imagem dos números 2, 4 e 5 e suas respectivas imagens cifradas. Todas as imagens foram cifradas por uma única chave binária.....	41
FIGURA 18 – Multiplicação entre as imagens cifradas nos números 2 e 5 e dos números 2 e 4 respectivamente.	42

SUMÁRIO

RESUMO	vi
ABSTRACT	vii
LISTA DE FIGURAS	viii
Capítulo 1	1
1. Introdução	1
Capítulo 2	6
2. O método de contraste de fase de Zernike	6
Capítulo 3	17
3. Cifragem de imagem utilizando o método de contraste de fase.....	17
Capítulo 4	22
4. A técnica de cifragem óptica de imagens utilizando máscara binária aleatória.....	22
4.1. Observações do método empregado.....	25
4.2. Processo de codificação óptico de uma imagem binária.....	27
4.3. Processo de decodificação da imagem cifrada.....	30
Capítulo 5	33
5. Analogia entre o método de cifragem proposto e o método de contraste de fase	33
Capítulo 6	36
6. Ataque da força bruta	36
6.1 Ataque do texto conhecido	38
6.2 Ataque das cifras conhecidas	39
Capítulo 7	44
7.1 Resultados	44
7.2 Considerações Finais	45
Referências	46

Capítulo 1

1. Introdução

Várias técnicas de cifragem ópticas de imagens surgem a todo o momento devido à necessidade que se tem de transmitir informações de uma maneira segura e confiável. Nessas técnicas a informação é cifrada, ou criptografada, de tal modo que para conseguir recuperá-la é necessário ter um conhecimento prévio da mesma máscara ou chave que a criptografou, sendo esta chave única. Isto faz com que as técnicas sejam robustas.

Refregier e Javidi [1] foram os pioneiros nesta área propondo um algoritmo de cifragem óptica de imagens conhecido na literatura como codificação de fase dupla aleatória (*double random phase encoding*) DRPE. Este método utiliza duas máscaras de fase aleatórias distintas para cifrar a imagem. Tais máscaras convertem a imagem de entrada que está somente modulada em amplitude em um ruído branco estacionário. Para realizar a cifragem propriamente dita, estas duas máscaras de fase aleatórias distintas são colocadas no plano de entrada e no plano de Fourier de um correlator óptico $4f$ para que a imagem de entrada seja cifrada. A reconstrução da imagem de entrada cifrada deste modo também é feita utilizando o correlator óptico $4f$. A imagem cifrada é colocada no plano de entrada do correlator e no plano de Fourier é colocada a mesma chave utilizada no processo de cifragem e então a imagem é decodificada. Tal método é robusto ao efetuar a deconvolução.

Towghi et al. [2] notou que cifrar uma imagem totalmente em modulação de fase é bem mais seguro do que cifrar uma imagem em modulação de amplitude na presença de um ruído aditivo, pois a modulação em fase é um processo de cifragem não linear e a modulação em amplitude um processo de cifragem linear. Com isto ele aperfeiçoou o método de Refregier e Javidi [1] transformando, antes do processo de cifragem, a imagem de entrada, que está em nível de cinza e em modulação de amplitude representada por $a(x,y)$, com $0 \leq a(x,y) \leq 1$, em modulação de fase, representada por $\exp[i2\pi a(x,y)]$, no plano de entrada do correlator óptico $4f$. Após esta transformação da imagem em modulação de

amplitude para modulação de fase, o processo de cifragem continua exatamente como o anterior. O problema com esta cifragem totalmente em fase surge somente depois do processo de decodificação da imagem. Após o processo de decodificação, a imagem recuperada também está em modulação de fase, e tal modulação não é visível ao olho humano. Portanto é necessária a aplicação de um método de contraste de fase para converter a distribuição de fase da imagem decodificada em uma distribuição de intensidade tornando assim a imagem recuperada visível ao olho humano.

Uma análise numérica [3] na técnica de DRPE foi realizada para determinar como, em ambos casos de cifragem em amplitude [1] e de cifragem em fase [2], as duas máscaras de decodificação afetam na saída da imagem em nível de cinza quando elas estão com erro. Neste estudo provou-se que o método de cifragem em fase é menos sensível a valores de pixels incorretos na máscara de fase que o método de cifragem em amplitude.

Desde sua introdução em 1995, o método DRPE tem gerado muito interesse e tem sido o foco para muitos estudos [4]- [6].

Uma outra maneira de cifrar uma informação com segurança é combinando o método de codificação de fase dupla aleatória com a técnica holográfica digital [7]. Neste método a informação é cifrada opticamente através do método de codificação de fase dupla aleatória e armazenada como um holograma digital [8]. A chave óptica, que é a máscara de fase de Fourier, utilizada para cifrar a informação também pode ser armazenada como um holograma digital. Com isso o processo de decodificação da informação criptografada ocorre digitalmente tendo o holograma da chave óptica. A diferença deste processo com os anteriores é que este pode ser utilizado para o armazenamento e a transmissão de um vídeo seguro.

No método de implementação óptica de cifragem de imagem proposto por Refregier e Javidi [1] a máscara de fase aleatória é de banda limitada [9], matematicamente um sinal $f(s)$ é de banda limitada se existir um número finito p tal que $\mathcal{F} f(s) = 0$ para todo $|s| \geq p/2$, onde $\mathcal{F}$ é a transformada de Fourier. Como resultado, muitas informações poderão ser perdidas no sistema óptico e a imagem reconstruída terá um ruído *speckle* tão forte que a tornará indistinguível. Então, Neto e Sheng propuseram um novo método de cifragem de imagem [10] utilizando *kinoform*, uma representação diferente de holograma gerado por

computador [12], livre de *speckle* para uma máscara de fase aleatória suavizada. Nesta técnica, um holograma de Fourier gerado por computador livre de *speckle* é primeiro calculado usando a imagem a ser cifrada como uma reconstrução. A imagem então é cifrada multiplicando o holograma de fase gerado por computador por uma máscara de fase aleatória. A máscara de fase aleatória é suavizada para reduzir a sua largura de banda. Com isso a imagem cifrada poderá ser reconstruída. A imagem decodificada pode ser recuperada somente se o holograma cifrado for previamente multiplicado pela chave de fase correta, isto é, o complexo conjugado da máscara de fase aleatória usada na cifragem.

Neto também propôs uma técnica de cifragem de imagem em modulação de fase utilizando o método de contraste de fase [11]. Tal método é baseado na técnica de contraste de fase de Zernike [12] que faz a conversão de uma imagem em modulação de fase espacial para uma imagem em modulação de intensidade espacial. A informação criptografada é conseguida multiplicando a informação original, que está em modulação de fase, por uma distribuição de fase aleatória, denominada a chave do processo. Com isso tem-se a informação criptografada em modulação de fase. Esta informação criptografada é decodificada multiplicando-a por uma outra chave de fase, que é o complexo conjugado da mesma chave utilizada no processo de codificação. Esta multiplicação resulta na informação decodificada também em modulação de fase. Tal modulação não é visível ao olho humano. Para que a informação decodificada seja visualizada, aplica-se o método de contraste de fase de Zernike, convertendo-a em modulação de intensidade através de uma lâmina de fase. Esta lâmina de fase consiste em um substrato de vidro onde um pequeno ponto dielétrico transparente é depositado. Tal ponto é centralizado no eixo óptico do plano focal do correlator e tem a espessura e o índice de refração tal que retarda a fase da luz em $\pi/2$ radianos ou $3\pi/2$ radianos. A robustez deste método é garantida pela não-linearidade do método de contraste de fase e da largura de banda da distribuição de fase aleatória. A vantagem deste método comparado com os anteriores é a cifragem direta da imagem sem qualquer cálculo iterativo para gerar a máscara de fase. Essa abordagem permite aplicações práticas desde que a máscara de fase final possa ser implementada usando placas termoplásticas e moduladores espaciais de luz (*spatial light modulator*) SLM's. Uma desvantagem deste sistema é a precisão requerida para o alinhamento da lâmina de fase [13]

que é colocada na origem das coordenadas do plano de Fourier do sistema de contraste de fase de Zernike.

Um sistema de cifragem óptica de codificação de fase aleatória dupla que usa uma chave binária foi proposto por Nomura e Javidi [14]. Esta chave binária é um holograma gerado por computador binário. Este sistema renova as chaves de fases aleatórias em uma velocidade alta para cifragens diferentes de grupos diferentes de *frames* possibilitando uma maior segurança no método de cifragem.

Não só imagens binárias como também imagens coloridas possuem um método de cifragem. Joshi propôs [15] uma técnica de cifragem de fase digital baseado na DRPE para imagens coloridas no domínio de Fourier. Porém este método é extremamente sensível a alguns tipos de ataques.

Recentemente a segurança dos métodos de cifragem de imagens começou a ser cuidadosamente analisada e foi detectado que alguns métodos de cifragem eram parcialmente robustos. Frauel et al [16] mostraram que o método de cifragem de fase dupla aleatória é resistente a ataques de força bruta, mas susceptível a ataques em que se é conhecido algumas imagens a serem criptografadas e suas respectivas imagens criptografadas, todas criptografadas por uma mesma chave, e a partir destes conhecimentos consegue-se recuperar a chave utilizada no processo de cifragem das mesmas.

Neste trabalho mostrar-se-á um processo de cifragem no qual é possível codificar e decodificar uma imagem binária estando apenas em modulação de amplitude. A chave utilizada neste processo de cifragem é uma máscara binária aleatória também em modulação de amplitude. A decodificação da imagem é dada graças à capacidade do olho humano em discernir regiões contínuas de regiões aleatórias. Este método é de fácil implementação, podendo ser obtido utilizando apenas materiais de baixo custo, como papéis, filmes plásticos, etc.

Para analisarmos a segurança de tal processo de cifragem aplicaremos dois tipos de ataques conhecidos na literatura, [17] e [18]. Um ataque é chamado de ataque de força bruta, que é a busca extensiva por todas as possíveis chaves do sistema. O outro é o ataque do texto conhecido, em que se é conhecida a imagem original, a imagem decodificada e o processo de cifragem e pretende-se descobrir a chave utilizada em tal processo.

Uma contribuição deste trabalho foi o desenvolvimento de um novo ataque contra métodos de cifragem óptica de imagens para analisar a robustez do mesmo. O novo tipo de ataque foi nomeado como ataque das cifras conhecidas. Neste ataque são conhecidas várias imagens cifradas de um mesmo processo de cifragem, e essas imagens cifradas foram criptografadas por uma única chave. Através destes conhecimentos tenta-se descobrir a chave utilizada no processo.

Este trabalho está dividido da seguinte maneira. No Capítulo 2 é explicado detalhadamente o método de contraste de fase de Zernike. Já no Capítulo 3 é mostrado um processo de cifragem de imagem no qual utiliza o método de contraste de fase de Zernike para obter a visualização da imagem após o processo de decodificação. Um novo método de cifragem de imagem binária apenas em modulação de amplitude é apresentado no Capítulo 4. A analogia entre o processo de contraste de fase que utiliza o método de Zernike e o processo de cifragem desenvolvido no Capítulo 4 é apresentada no Capítulo 5. Ataques contra o processo de cifragem óptica de imagens utilizando máscara binária aleatória são apresentados no Capítulo 6, inclusive o novo ataque desenvolvido. Os resultados e as considerações finais encontram-se no Capítulo 7.

Capítulo 2

Neste capítulo será apresentado alguns conceitos para a interpretação do método de contraste de fase de Zernike. Tal método também será detalhado neste capítulo. Para a implementação deste método é necessário a utilização de um mecanismo óptico. Zernike utilizou como mecanismo um microscópio óptico, o qual junto com o método de contraste de fase ficou conhecido como microscópio de contraste de fase. Além do microscópio óptico pode-se utilizar também como mecanismo óptico um correlator óptico 4f.

2. O método de contraste de fase de Zernike

Um objeto qualquer pode ser “visto” quando está em destaque com o fundo que o rodeia, seja através da cor, da tonalidade ou da ausência de cor. Tais características criam de algum modo um contraste do objeto com o fundo. Objeto deste tipo constitui um objeto de amplitude [19], pois só é observável por causa das variações que provoca na amplitude da onda luminosa. A amplitude da onda refletida ou transmitida diz-se modulada pelo objeto. A FIGURA 1(b) representa uma frente de onda luminosa que ao atravessar um objeto é modulada em amplitude .

Muitas vezes é necessário visualizar objetos de fase [19], objetos transparentes, que não contrastam com o fundo ou com o ambiente em que estão e que alteram a fase da onda detectada. Como o olho humano é incapaz de detectar variações de fase de uma frente de onda luminosa, estes objetos são de fato invisíveis. Os biólogos, muitas vezes tendo que analisar microorganismos transparentes, criaram técnicas de coloração do microorganismo para que pudessem analisá-los. Porém esta técnica é pouco sucedida porque muitas vezes o corante utilizado afeta o microorganismo cujo metabolismo se pretende analisar microscopicamente.

Quando uma parte da frente de onda luminosa (sobre a qual a fase é constante) é obstruída de algum modo, isto é, quando a amplitude ou a fase da frente de onda luminosa se altera ocorre o fenômeno da difração. Quando uma onda inicialmente plana incide e

atravessa uma partícula transparente, o efeito predominante é a geração de um desvio de fase da onda luminosa. A onda emergente não é mais plana, e foi alterada pela própria partícula transparente. Diz-se então que o objeto modulou a fase da onda luminosa. A FIGURA 1(c) representa uma frente de onda luminosa que ao atravessar um objeto transparente é modulada em fase.

A FIGURA 1 ilustra os processos de modulação de uma frente de onda luminosa. Uma frente de onda plana luminosa com a fase e a amplitude constante está representada na FIGURA 1(a). Após esta frente de onda plana luminosa atravessar um objeto de amplitude, a amplitude de tal onda sofre uma alteração causada pelo objeto. Tal alteração é a frente de onda luminosa modulada em amplitude. A FIGURA 1(b) mostra a alteração de amplitude da frente de onda sem que a mesma sofra qualquer modificação na fase. E se a frente de onda plana luminosa atravessar um objeto transparente, a frente de onda luminosa torna-se modulada em fase como ilustra a FIGURA 1(c), que preserva a amplitude da onda.

FIGURA 1 - Processos de modulação de uma frente de onda planar luminosa. (a) representa a frente de onda luminosa com fase e amplitude constante, (b) representa uma frente de onda luminosa que atravessa um objeto de amplitude e tal frente de onda sofre uma variação de amplitude e (c) representa uma frente de onda luminosa que atravessa um objeto transparente e é modulada em fase.

O microscópio de contraste de fase ilustrado na FIGURA 2, inventado pelo físico holandês Fritz Zernike em 1935 [12], é uma técnica óptica de melhoramento de contraste que pode ser utilizado para produzir imagens com um alto contraste de espécimes transparentes, convertendo uma modulação de fase espacial em uma modulação de intensidade espacial.

FIGURA 2 - Estrutura do microscópio de contraste de fase criado por Zernike².

Zernike estava em seu laboratório analisando a estrutura de um microscópio óptico simples na intenção de descobrir algum método que o fizesse observar objetos de contraste de fase [20]. Após muitos estudos, tentativas e testes, criou-se o microscópio de contraste

² Imagem retirada de: LODISH, H. et al. **Molecular Cell Biology**. New York: W. F. Freeman, 2000.

de fase. Tal aparelho é importante no estudo das células microscópicas, pois, desde então, não houve mais a necessidade de pigmentar as células e conseqüentemente matando-as para que fossem estudadas.

A descoberta de Zernike não obteve o reconhecimento merecido até 1941, época em que as forças alemãs ocupavam os países baixos. Neste ano, as forças alemãs fizeram um inventário de todas as invenções e criações que poderiam ser úteis na guerra. Um rudimentar microscópio de contraste de fase foi apresentado para tal inventário, o que possibilitou os cientistas a visualizar e estudar os detalhes de células vivas e sem corantes. Como consequência descobriu-se a cura para muitas epidemias existentes na época, evitando assim a morte de muitos soldados presentes na guerra. Depois da guerra, a importância de tal invenção foi realmente reconhecida e Zernike ganhou o Prêmio Nobel de Física em 1953.

Várias técnicas para a visualização de objetos de fase surgiram, porém todas as técnicas apresentam defeitos similares: as variações de intensidade observadas não estão linearmente relacionadas ao desvio de fase e, portanto não podem ser consideradas como um indicativo direto da variação de espessura do objeto. Já a técnica de Zernike [12] se apóia nos princípios de filtragem espacial e tem a vantagem que a intensidade observada está linearmente relacionada ao desvio de fase introduzido pelo objeto.

O microscópio óptico simples baseia-se no princípio de que a densidade de um corpo determina a velocidade com que a luz o atravessa e, conseqüentemente, o seu índice de refração. Quando uma partícula transparente, cujo índice de refração é próximo do meio envolvente, é atravessada por um raio luminoso, uma parte do raio atravessa sem se desviar, enquanto que outra parte se difrata e desvia. Nas preparações biológicas, a diferença de fase entre as ondas é de $\frac{1}{4} \lambda$ aproximadamente, onde λ é o comprimento de onda.

O microscópio de contraste de fase é dotado de um sistema óptico especial que transforma diferença de fase dos raios de luz em diferença de intensidade luminosa. Um objeto transparente é composto por estruturas distintas, podendo ter espessuras diferentes por todo o seu comprimento. Esta variação de espessura que um objeto transparente pode ter causa atrasos diferentes na luz que o atravessa. Isto gera diferenças de fase na luz

emergente, que, por interferência, são transformadas em diferenças de amplitude, gerando diferenças de intensidade luminosa as quais a retina é sensível.

No microscópio de contraste de fase, mostrado na FIGURA 2, o raio mais lateral que passa através da objetiva, conjunto de lentes que permite a ampliação do objeto, é adiantado de $\frac{1}{4} \lambda$ em relação à luz central, pela introdução de uma placa anelar na objetiva. Também no condensador, que distribui regularmente no campo visual do microscópio a luz refletida pelo espelho, se introduz um diafragma anelar. A placa anelar é um disco transparente com um sulco em forma de anel, que coincide com a imagem direta do condensador. O efeito de fase decorre da interferência entre a imagem geométrica fornecida pela parte central da objetiva e a imagem difratada, dada pelos raios laterais, adiantada de $\frac{1}{4} \lambda$. Isto gera diferenças de fase que são transformadas em diferenças de intensidade luminosa.

Como o desenvolvimento da técnica de contraste de fase aplicado em um microscópio óptico ou em um correlator óptico 4f é o mesmo, mostrar-se-á com maior detalhe a técnica de contraste de fase aplicada em um correlator óptico 4f como ilustrado na FIGURA 3.

FIGURA 3 - Estrutura de um correlador óptico 4f. O correlador óptico 4f é composto por duas lentes, tendo cada uma delas o comprimento focal f . As lentes são posicionadas entre si a uma distância de $2f$. A primeira lente efetua a primeira transformada de Fourier da imagem localizada no plano de imagem, decompondo-a em suas frequências espaciais. A segunda lente efetua a segunda transformada de Fourier, recuperando a imagem original.

Primeiramente tem-se que um correlador óptico 4f é um sistema de imagem composto por duas lentes, tendo cada uma delas o comprimento focal dado por f , daí a denominação de 4f. A análise da propagação da luz através das lentes deste sistema pode ser dividida em dois sub-sistemas de transformadas de Fourier. O primeiro sub-sistema, compreendido entre o plano objeto ou plano de entrada e o plano de Fourier (distância entre os planos de $2f$), realiza a primeira transformada de Fourier, e o segundo sub-sistema, compreendido entre o plano de Fourier e o plano de imagem (distância entre eles de $2f$), realiza outra transformada de Fourier. Esta segunda transformada é matematicamente conhecida como transformada de Fourier inversa desde que o sistema de coordenadas do plano de imagem seja invertido. Considerando $t(y,z)$ a transmitância (quantidade de luz que atravessa uma certa amostra) de amplitude complexa de uma transparência localizada no

plano de entrada e iluminada por uma onda plana, o primeiro sub-sistema de lentes analisa $t(y,z)$ em sua transformada de Fourier espacial e separa as componentes de Fourier para que cada ponto no plano de Fourier corresponda a uma frequência espacial simples. Essas componentes são então recombinaas pelo segundo sub-sistema de lentes e a distribuição do objeto é perfeitamente reconstruída. Este sistema pode ser utilizado com um filtro espacial no plano de Fourier, para que a imagem seja uma versão filtrada de $t(y,z)$. Existem vários tipos de filtros que podem ser colocados no plano de Fourier. Dependendo do filtro utilizado no plano de Fourier, após a transformada de Fourier inversa pode-se obter como resultado uma imagem mais suavizada ou mais nítida ou com mais contorno em relação à imagem original.

Suponha então que um objeto transparente tenha a transmitância de amplitude dada por

$$t(y,z) = \exp[j\phi(y,z)] \quad (1)$$

e que este mesmo objeto seja iluminado coerentemente em um sistema de formação de imagem, sendo este o correlator óptico 4f [12].

A frente de onda incidente do feixe de luz é dividida em duas componentes após atravessar o objeto transparente, o objeto de fase situado no plano de entrada. A primeira componente é uma frente de onda planar que não sofre desvio algum (ou seja, é uma onda não difratada, de ordem zero). Esta frente de onda passa através e ao redor do objeto, porém não interage com o mesmo, é uma onda direta. A outra componente é uma frente de onda que sofre um desvio de fase após atravessar o objeto transparente, é uma onda difratada. O desvio de fase $\Delta\phi$ sofrido pela onda difratada deve ser menor que 1 radiano, dado que o objeto de fase é muito fino. Assume-se que o objeto de fase não altera significativamente a amplitude da frente de onda incidente nele. Ao deixar o plano do objeto, a onda difratada e a onda direta recombinaam-se e ficam defasadas de $\pi/2$, conforme ilustrado na FIGURA 4, formando uma onda modulada em fase. Como a amplitude da onda reconstruída é constante no plano imagem, embora a sua fase varie de ponto para ponto, a imagem não é perceptível.

FIGURA 4 - Frentes de onda luminosa após atravessarem um objeto de fase. A onda vermelha é a onda direta, a azul é a onda difratada e a onda verde é a interferência da onda direta pela onda difratada.

Sendo assim, a transmitância de amplitude pode ser aproximada por

$$t(y,z) \approx 1 + j\Delta\phi(y,z). \quad (2)$$

O primeiro termo da aproximação (2) representa a luz que atravessa o objeto transparente sem sofrer qualquer desvio e o segundo termo representa a luz difratada, a onda que transporta consigo toda a informação relativa à estrutura óptica do objeto.

A imagem produzida pelo sistema é dada pelo cálculo da intensidade da imagem, I , que pode ser escrita como

$$I \approx |1 + j\Delta\phi|^2 \approx 1 \quad (3)$$

onde, para permanecer consistente com nossa aproximação, o termo $\Delta\phi$ é próximo de zero (a variação de fase é $\Delta\phi \ll 1$).

Zernike percebeu que a luz difratada resultante da estrutura de fase não é observável no plano imagem porque esta está em quadratura de fase, diferença de 90° , com a luz que não sofre desvio. Se fosse possível variar a diferença de fase entre a onda difratada e a onda direta de $\pi/2$ antes da recombinação, a coerência entre ambas não seria afetada e a interferência seria destrutiva ou construtiva. Em ambos os casos, portanto, a onda

reconstruída seria modulada em amplitude na região da imagem e esta sim seria visível ao olho humano.

Para que isto ocorra Zernike propôs o seguinte. Introduzir um filtro espacial no plano focal posterior da primeira lente conforme ilustrado na FIGURA 5, onde tem-se a transformada de Fourier óptica do objeto transparente. Obtém-se assim uma variação de fase da onda não difratada com a onda difratada de $\pi/2$. Note-se que a luz direta forma uma imagem da fonte na intersecção do eixo óptico com o plano de Fourier.

FIGURA 5 - Estrutura do correlador óptico 4f com a aplicação da lâmina de fase. A onda luminosa não difrata ao passar pela lâmina de fase sofre um desvio de fase de $\pi/2$, que ao sofrer interferência com a onda difratada gera uma onda luminosa modulada em amplitude no plano imagem.

O filtro espacial introduzido pode tomar a forma circular de uma pequena reentrância de profundidade d , aberta numa placa de vidro transparente de índice de refração n_g . Teoricamente, apenas o feixe direto passa através da reentrância, e a sua fase avança de $(n_g - 1)d$ (que deve ser igual a $\lambda/4$) relativamente ao feixe difratado. Um filtro deste tipo constitui uma lâmina de fase. O seu efeito está ilustrado na FIGURA 6 (b), interferência destrutiva: objetos de fase mais espessos ou com um índice superior

manifestam-se no plano imagem como escuros num fundo claro. No caso contrário, quando a lâmina de fase tem uma saliência e não uma reentrância no centro ocorre a situação oposta. No primeiro caso o contraste de fase é positivo e no segundo caso o contraste de fase é negativo.

FIGURA 6 - Interferência das ondas luminosas. (a) interferência construtiva e (b) interferência destrutiva.

Sendo assim, a transformada inversa de Fourier desempenhada pela segunda lente do correlator óptico $4f$ resulta na intensidade da imagem

$$I = | \exp[j(\pi/2)] + j\Delta\phi |^2 = | j(1 + \Delta\phi) |^2 \approx 1 + 2\Delta\phi \quad (4)$$

ou

$$I = | \exp[j(3\pi/2)] + j\Delta\phi |^2 = | -j(1 - \Delta\phi) |^2 \approx 1 - 2\Delta\phi. \quad (5)$$

Nas equações (4) e (5) a intensidade da imagem está linearmente relacionada com o desvio de fase $\Delta\phi$, produzindo assim variações observáveis de intensidade de imagem. O caso da equação (4) refere-se ao contraste de fase positivo (escuro) enquanto o caso da equação (5) refere-se ao contraste de fase negativo (claro).

Zernike após muitos estudos concluiu que introduzindo apenas uma lâmina de fase no plano de Fourier de um correlator óptico $4f$, conseguiria converter uma imagem em modulação de fase espacial para uma em modulação de intensidade espacial, criando o método de contraste de fase de Zernike conhecido na literatura.

Capítulo 3

Neste capítulo é mostrado a técnica de contraste de fase de Zernike aplicada em um método de cifragem de imagem. O objetivo da aplicação da técnica de contraste de fase é fazer com que a imagem decodificada após o processo de cifragem de imagem seja visível ao olho humano. Tal método de cifragem de imagem foi a motivação do método de cifragem óptica de imagem utilizando máscara binária aleatória apresentado neste trabalho.

3. Cifragem de imagem utilizando o método de contraste de fase

O ato de cifrar uma imagem corresponde em transmiti-la utilizando códigos secretos, transformando-a em uma imagem sem sentido. Esta imagem perturbada, a chamada imagem cifrada, somente terá algum sentido para quem tiver um prévio conhecimento do código utilizado para cifrá-la.

Vários métodos de cifragem de imagem em modulação de fase foram desenvolvidos [1]-[5]. Tais métodos de cifragem de imagem apresentam uma mesma característica, a de serem robustos, o que é de uma máxima importância para um processo de cifragem de imagem. Porém a imagem obtida após o processo de decodificação desses métodos é a imagem decodificada em modulação de fase. Como tal imagem está em modulação de fase, ela não é visível ao olho humano. O desafio estava então em desenvolver uma técnica de cifragem de imagem em modulação de fase na qual após o processo de decodificação, a imagem resultante fosse idêntica a inicial e que já estivesse em modulação de amplitude, sendo assim visível ao olho humano.

Neto, em 1998, propôs um método para cifrar imagens em modulação de fase contínua [11]. Tal método utiliza a técnica de contraste de fase de Zernike [12] e uma máscara de fase aleatória para cifrar a imagem.

A técnica aqui apresentada de cifragem de imagem utilizando o método de contraste de fase é robusta, ou seja, sem o conhecimento prévio da máscara de fase aleatória utilizada no processo de cifragem não é possível que a imagem cifrada em fase seja recuperada.

Suponha que o objeto transparente que se deseja cifrar tenha a transmitância de fase dada por

$$t(y,z) = \exp[j\phi(y,z)], \quad 0 \leq \phi(y,z) \leq 2\pi. \quad (6)$$

A transmitância é a quantidade de luz que atravessa uma certa amostra. Neste caso, a amostra é a imagem representada por $\phi(y,z)$.

Esta transmitância de fase foi gerada pela imagem em nível de cinza normalizada, $\phi(y,z)$ (a imagem em nível de cinza $\phi(y,z)$ é normalizada com o valor máximo 1 para garantir a condição de linearidade). O nível de cinza da imagem está linearmente relacionado ao valor de fase. O valor de nível de cinza 0 que representa a cor preta corresponde ao valor de fase 0, o valor de nível de cinza 255 que representa a cor branca corresponde ao valor de fase 2π e os outros valores de níveis de cinza correspondem a valores de fase intermediários entre 0 e 2π .

A obtenção da cifragem da imagem $\phi(y,z)$ é realizada multiplicando-se a sua transmitância $t(y,z)$, a qual está em modulação de fase, por uma distribuição de fase aleatória, que é expressa matematicamente por $\exp[j2\pi\psi(y,z)]$, onde $\psi(y,z)$ é um ruído branco aleatório distribuído uniformemente no intervalo $[0,1]$. Esta distribuição de fase aleatória é conhecida como a chave do processo de cifragem. Tal método está representado na FIGURA 7. A multiplicação do objeto transparente pela chave resulta na imagem cifrada, uma máscara de fase cifrada t^c dada por

$$t^c(y,z) = \exp[j(\phi(y,z) + 2\pi\psi(y,z))], \quad 0 \leq \psi(y,z) \leq 1. \quad (7)$$

Nota-se que a imagem cifrada também está em modulação de fase contínua.

FIGURA 7 – Método de cifragem de imagem em distribuição de fase utilizando a estrutura do correlador óptico 4f. Coloca-se no plano de entrada do correlador a imagem que se deseja cifrar em distribuição de fase e a chave de fase do processo. Um feixe de ondas ao atravessar tais imagens no plano de entrada sofrerá duas transformadas de Fourier, uma transformada em cada lente do correlador, resultando no plano imagem do correlador óptico 4f a imagem em fase da multiplicação entre as imagens colocadas no plano de entrada.

O conteúdo da imagem cifrada $t^c(y,z)$ não pode ser reconhecido por um detector de intensidade de luz e o processo de recuperação da imagem original através da deconvolução é de uma extrema dificuldade que se torna inviável. Logo, é impossível decodificar a imagem cifrada $t^c(y,z)$ sem o conhecimento prévio da chave de fase $\exp[j2\pi\psi(y,z)]$ que é a mesma chave que a criptografou.

Com o conhecimento prévio da mesma chave de fase utilizada na cifragem da imagem, o processo de decodificação da imagem cifrada é obtido multiplicando-se a imagem cifrada $t^c(y,z)$ pela chave de fase $\exp[-j2\pi\psi(y,z)]$. Esta chave de fase é a representação matemática do complexo conjugado da mesma chave de fase aleatória utilizada no processo de cifragem da imagem. Quando a imagem cifrada é multiplicada pela chave de fase $\exp[-j2\pi\psi(y,z)]$, o termo de fase aleatório $\exp[j2\pi\psi(y,z)]$ armazenado na imagem cifrada é cancelado resultando em uma outra máscara de fase $t^a(y,z)$ dada por

$$t^a(y,z) = \exp[j(\phi(y,z) + 2\pi\psi(y,z))] \cdot \exp[-j2\pi\psi(y,z)] = \exp[j\phi(y,z)]. \quad (8)$$

Esta máscara de fase resultante nada mais é que a imagem de fase decodificada. Pelo fato de a imagem recuperada estar em modulação de fase, não é possível que esta seja

visualizada pelo olho humano. Para que a intensidade da imagem decodificada seja recuperada opticamente é necessário aplicar a técnica de contraste de fase de Zernike.

A técnica de contraste de fase é aplicada sobre um correlator óptico $4f$ como ilustrado na FIGURA 8. Uma frente de onda monocromática ilumina a imagem cifrada que está alinhada ao modulador espacial de luz (SLM) em regime de modulação de fase. Quando a imagem cifrada é multiplicada pela chave de fase $\exp[-j2\pi\psi(y,z)]$ modulada pelo SLM, ambas no plano de entrada do correlator óptico, o termo de fase aleatório $\exp[j2\pi b_{mn}]$ armazenado na imagem cifrada é cancelado, resultando somente o termo de fase $t^a(y,z) = \exp[j\phi(y,z)]$. Este termo de fase carrega a informação decodificada somente em modulação de fase e é necessário estar em modulação de amplitude para que a informação possa ser detectada como um padrão de intensidade. Aplica-se então uma lâmina de fase no plano de Fourier do correlator óptico $4f$, como diz o método de contraste de fase de Zernike citado no Capítulo 2. Um padrão de intensidade é gerado no plano imagem do correlator óptico $4f$ e a imagem decodificada é visualizada.

FIGURA 8 – Decodificação de imagem utilizando o método de contraste de fase e um correlador óptico 4f. A decodificação da imagem cifrada se dá através da multiplicação entre a imagem cifrada e a chave de fase do processo. Para que a imagem recuperada após a multiplicação esteja em modulação de amplitude é colocada uma lâmina de fase no plano de Fourier do correlador óptico 4f, conforme a técnica de contraste de fase de Zernike.

A robustez deste método de cifragem de imagem é garantida pela aplicação da técnica de contraste de fase de Zernike e pela largura de banda da distribuição de fase aleatória. A vantagem deste método é a cifragem direta da imagem sem qualquer cálculo iterativo para gerar a chave de fase do processo.

Este método de cifragem de imagem foi a motivação para o desenvolvimento do método de cifragem de imagem utilizando máscara binária aleatória que será apresentado no capítulo seguinte.

Capítulo 4

No capítulo anterior foi apresentado um método de cifrar imagens em modulação de fase contínua, com a fase variando entre 0 e 2π . Também é possível cifrar imagens em modulação de fase descontínuas, com as fases assumindo apenas alguns valores, como 0 ou π , as imagens binárias. É mostrado agora um método de cifrar imagens estando estas apenas em modulação de amplitude e sendo imagens binárias. Tal método cifra e decodifica imagens na forma binária utilizando apenas uma máscara binária aleatória.

4. A técnica de cifragem óptica de imagens utilizando máscara binária aleatória

A técnica aqui apresentada refere-se a cifragem e decodificação de uma informação apresentada na forma de símbolos, números, logos, imagens, etc., processada na forma binária. O processo de cifragem da informação é dado por meio de uma operação multiplicativa ou comparativa entre imagens.

O método multiplicativo ou comparativo de imagens (também conhecido como inversão de bit) aplicado no processo de cifragem da informação é mais robusto do que os métodos de adição ou subtração de imagens.

A decodificação da informação deste processo resulta em uma imagem com pelo menos uma região contínua ou periódica como mostra a FIGURA 9. É por causa da existência desta região contínua que a imagem recuperada é obtida de uma forma clara e inteligível.

FIGURA 9 – Imagem do número cinco após o processo de decodificação. O número cinco é visualizado pois a imagem decodificada apresenta uma região periódica, que é o próprio número cinco, e uma região aleatória, que é a parte externa.

Quando duas telas, cujos conteúdos são imagens com nenhum significado visual, são sobrepostas, seguindo um alinhamento pré-determinado, uma imagem é reconstruída com relação a um observador. Esta imagem reconstruída é a imagem inicial do processo de cifragem, que não era reconhecida ou decifrada sem a sobreposição de pelo menos duas telas. Nesta reconstrução, pelo menos uma região da informação original reconstruída é periódica, ou seja, tem um padrão contínuo (ao invés de aleatório), o que faz com que o olho humano decifre, reconheça a imagem. O padrão de uma das telas é uma distribuição aleatória superficial arbitrária, chamada de elemento de cifrar ou chave do processo. Por ser aleatória, esta chave não tem significado algum, não representa nenhuma letra, número, caractere, símbolo, etc. A outra tela da sobreposição, independente da informação a ser cifrada, tem uma distribuição bi-dimensional resultante de uma operação multiplicativa entre a chave do processo citada anteriormente e a imagem binária a ser cifrada, ou seja, esta outra tela é a informação de origem cifrada. A informação cifrada, portanto, não é uma

distribuição aleatória e sim pseudo-aleatória, embora não tenha um aspecto discernível para um observador.

O processo de cifragem da informação é dado em uma série de passos que transforma a imagem original a ser cifrada, que está em seu formato inteligível podendo ser uma ou mais letras, números, símbolos, etc., em uma imagem sem qualquer significado para um observador. Esta transformação é dada aplicando a operação multiplicativa ou comparativa. O resultado deste processo é a informação cifrada.

O processo de decodificação da informação cifrada é realizado através de alguns passos consecutivos que recuperam a informação cifrada através da sobreposição de pelo menos duas telas, as quais individualmente não tem algum significado e sobrepostas reconstituem a informação original. Esta sobreposição tem que seguir um alinhamento pré-determinado para que produza efeito. A informação recuperada é composta por duas regiões na imagem, uma região com um padrão visual aleatório e uma outra com imagens periódicas (pontos, pequenas figuras, etc.), ou cores contínuas ou uma distribuição em nível de cinza. São estas duas regiões da imagem recuperada que torna a informação discernível ao olho humano.

Este processo de cifragem de imagem trabalha com a imagem em distribuição de amplitude. Com isso, a imagem recuperada após o processo de decodificação está também em modulação de amplitude, já sendo visível ao olho humano.

Uma das vantagens deste processo é exatamente o aspecto visual da imagem recuperada obtida através do processo de decodificação da informação que é composto por duas regiões, uma com um padrão visual aleatório e outra com imagens periódicas, ou cores contínuas ou uma distribuição em nível de cinza. Por estas duas regiões possuírem um grande contraste, a imagem recuperada é reconhecida facilmente pelo olho humano.

Um aspecto importante é que após o processo de cifragem, a imagem obtida está com o mesmo tamanho da imagem original, diferentemente de outros processos de cifragem de imagem em distribuição de amplitude [21][22].

Outra vantagem deste método é a sua fácil implementação, podendo ser obtida em materiais regulares e de baixo custo, como plásticos, papéis, etc.

4.1. Observações do método empregado

A imagem original a ser cifrada tem que estar em sua forma binária. Para que a imagem seja binária, é necessária a transformação desta em uma outra imagem formada apenas por duas cores que tenham um contraste considerável entre si. Esta transformação não tem restrição alguma, qualquer imagem pode ser transformada em uma imagem binária. Geralmente as cores utilizadas para o formato binário são o branco e o preto, podendo ser também o verde e o vermelho. Normalmente é associado à cor preta o valor de nível de cinza 0 e à cor branca o valor de nível de cinza 255, pois é comum que uma imagem em nível de cinza tenha 256 tons de cinza. Também é possível associar ao preto e ao branco os valores 0 e 1 ou -1 e 1 respectivamente. Neste trabalho serão utilizados os números -1 e 1 para associar às cores preto e branco respectivamente.

O processo de cifragem é feito então na seguinte ordem:

- Transformação binária da imagem a ser cifrada;
- Multiplicação entre a imagem binária e a chave do processo que também é binária.

A multiplicação entre as imagens é calculada multiplicando-se um pixel da imagem binária com o pixel correspondente da chave do processo. Esta operação é também conhecida como inversão de bit ou operação XOR [23].

Como a operação XOR tem a propriedade de inverso e identidade, pode ser utilizada no método de cifragem de imagem. Matematicamente temos as propriedades da operação XOR expressas como: para qualquer número binário x : $x \otimes 0 = x$ (propriedade inversa) e como esperado $0 \otimes x = x$ (identidade). No caso em estudo, $\otimes$ significa a operação multiplicação usual e o elemento identidade é o número 1. Contudo, no sistema de cifragem a operação XOR é aplicada entre a imagem binária a ser cifrada e a chave do processo, resultando na imagem codificada. O parágrafo seguinte explica na prática o mecanismo da operação XOR.

Suponha que a chave seja multiplicada pela imagem binária em uma região que seja totalmente preta. Os pixels coincidentes da chave serão invertidos, o pixel branco da chave tornará preto e o pixel preto da chave tornará branco após a multiplicação, conforme FIGURA 10. Matematicamente, $1 \text{ (branco)} \times (-1) = -1 \text{ (preto)}$ e $-1 \text{ (preto)} \times (-1) = 1$

(branco), onde o primeiro fator de cada operação representa o pixel da chave e o segundo fator representa o pixel correspondente da imagem binária.

FIGURA 10 – Operação XOR: multiplicação da chave por uma região de pixels pretos (inversão de bit).

Agora, com a chave sendo multiplicada por uma região totalmente branca da imagem binária, os pixels correspondentes da chave não sofrerão qualquer alteração na cor, pois multiplicação pelo número 1 (pixel branco) não altera o valor do outro fator, FIGURA 11. É através desta multiplicação que se cria a imagem cifrada.

FIGURA 11 – Operação XOR: multiplicação da chave por uma região de pixels brancos.

Os valores dos pixels da chave do processo são dados por uma distribuição aleatória bi-dimensional dos números -1 e 1, sendo estes representações das cores contrastantes preto e branco respectivamente. Esta distribuição aleatória pode ser gerada utilizando uma equação não-linear, tendo como exemplo a equação

$$x_{n+1} = r \cdot x_n(1 - x_n), \quad (9)$$

onde r varia entre 0 e 4, x_n varia entre 0 e 1, transformando todo valor abaixo de 0.5 em -1 e todo valor acima de 0.5 em 1, com x_n representando os pixels da imagem e n variando de 0 até a quantidade de pixels da imagem menos 1 [24].

O método de cifragem óptica de imagens utilizando máscara binária aleatória foi implementado utilizando o programa MatLab versão 7.1. Os valores dos pixels da chave do processo foram gerados aleatoriamente através da função *rand* disponível no programa.

As imagens da chave (uma distribuição aleatória bi-dimensional) e da máscara cifrada podem ser geradas sobre diferentes superfícies, plana ou esférica, porém a sobreposição alinhada das imagens é o que reconstitui a informação original. Desta maneira, qualquer superfície que permita ou suporte a geração de uma imagem pode ser utilizada, como papel, plástico, vidro, metal, etc. Estes materiais podem ser utilizados para diferentes aplicações em documentos, documentos de banco, cartões, tickets promocionais, televisões ou telas de vídeo, televisões a cristal líquido, ou qualquer outro suporte físico ou eletrônico que permita a visualização e/ou reconstituição da imagem.

4.2. Processo de codificação óptico de uma imagem binária

Este processo de codificação óptico pode ser aplicado em qualquer tipo de imagem, podendo esta ser um caractere, um número, uma letra, etc. Toda imagem em nível de cinza é formada por um conjunto de pixels, com cada pixel assumindo uma cor. Este conjunto de pixels pode ser representado por uma matriz A_{MN} de $M \times N$ pixels, com $M, N \in \mathbb{IN}$. Nesta matriz, a cor preta é representada pelo número 0, a cor branca pelo número 255 e as demais distribuições de níveis de cinza são representadas pelos outros números entre 0 e 255.

Como este método de codificação é melhor aplicado em imagens binárias, a informação original é então transformada em uma informação binária. Esta transformação pode ser feita escolhendo um nível de limiar, um número entre 0 e 255 onde as distribuições de níveis de cinza abaixo deste limiar tornam-se -1 (preto) e as distribuições acima deste limiar tornam-se 1 (branco), obtendo assim uma nova matriz B_{MN} que é a informação em sua forma binária.

Na sequência, cada elemento da matriz B_{MN} é multiplicado pelo respectivo elemento de uma nova matriz C_{MN} de tamanho $M \times N$ chamada elemento de cifrar ou chave do processo. Esta nova matriz C_{MN} é formada por uma distribuição aleatória bi-dimensional binária de -1's e 1's. Esta chave pode ser gerada por métodos numéricos computacionais ou por equações não-lineares que tenham um comportamento caótico. O resultado desta operação multiplicativa é uma matriz D_{MN} que representa a informação inicial cifrada.

A operação multiplicativa realizada entre as matrizes B_{MN} e C_{MN} é dada pela multiplicação de elemento por elemento de cada matriz e não pela operação usual de multiplicação entre matrizes. Considerando b_{mn} , c_{mn} e d_{mn} os elementos das matrizes B_{MN} , C_{MN} e D_{MN} respectivamente e m , n a linha e a coluna em que estes elementos estão localizados com $m, n \in \mathbb{IN}$, a multiplicação entre as matrizes é expressa por

$$d_{mn} = b_{mn} \times c_{mn}. \quad (10)$$

A matriz resultante desta operação, representada por D_{MN} , é composta por -1's e 1's, ou seja, por pixels pretos e brancos o que resulta na imagem criptografada.

Este método de cifragem é de fácil implementação, considerando que pode ser obtido usando materiais regulares e de baixo custo como papéis, filmes plásticos e outros.

A FIGURA 12 ilustra este processo de cifragem para a imagem do número “5”. A FIGURA 12(a) é a imagem binária original a ser cifrada. A FIGURA 12(b) é a chave do processo gerada por métodos numéricos computacionais. E a FIGURA 12(c) é a imagem cifrada, o resultado da multiplicação entre a imagem original e a chave. A multiplicação é dada pixel a pixel, cada pixel da imagem original é multiplicado pelo respectivo pixel da chave.

A imagem do resultado da codificação tem o aspecto de uma distribuição aleatória bi-dimensional, mas na verdade, é uma distribuição pseudo - aleatória bi-dimensional, ou seja, uma distribuição extremamente ruidosa com a informação da imagem inicial em uma forma inteligível.

FIGURA 12 - Cifragem binária utilizando máscara binária aleatória. (a) imagem binária original do número “5”. (b) máscara binária aleatória, ruído branco. (c) imagem cifrada.

4.3. Processo de decodificação da imagem cifrada

O processo de decodificação da imagem, a qual foi cifrada como citado anteriormente, é de fácil implementação. Para que a imagem criptografada seja recuperada basta sobrepor a mesma chave utilizada no processo de cifragem FIGURA 12(b) com a imagem cifrada FIGURA 12(c). Esta sobreposição tem que seguir um alinhamento pré-determinado para que se obtenha a imagem decodificada. A imagem decodificada contém uma região contínua e uma região aleatória.

A decodificação é feita pela sobreposição da chave e da imagem contendo a informação cifrada. Para que esta operação seja realizada com sucesso, é necessário que a máscara que sobrepõe a imagem cifrada tenha regiões substancialmente translúcidas ou transparentes permitindo a visualização da combinação das duas máscaras. Desta maneira, na região associada ao número -1, a luz é bloqueada pela cor preta, e a região associada ao número 1, a máscara é transparente ou translúcida, permitindo a passagem total ou parcial da luz respectivamente. Já na imagem contendo a informação cifrada, o número -1 refere-se também a cor preta, porém o número 1 é associado à cor branca. Assim, quando as imagens se sobreporem, a combinação entre elas resultará em uma imagem bem nítida.

As imagens decodificadas estão ilustradas na FIGURA 13. A FIGURA 13(a) mostra a imagem decodificada com a mesma chave utilizada no processo de codificação da imagem original. Nota-se que a imagem recuperada é composta por duas regiões, uma contínua e outra aleatória. O interior do número cinco é a região contínua e o fundo da imagem a região aleatória. É este contraste de regiões que faz com que o cérebro reconheça o número em questão. E é devido a características da percepção humana, que a imagem decodificada, mesmo contendo pequenas distorções, é identificada. Já a FIGURA 13(b) mostra a imagem decodificada da sobreposição da imagem cifrada com outra chave aleatória diferente da utilizada para a cifragem.

(a)

(b)

FIGURA 13 - Imagens após o processo de decodificação. (a) imagem recuperada com a chave correta. (b) imagem recuperada com a chave incorreta.

Após a sobreposição da imagem cifrada por uma chave aleatória qualquer não é possível recuperar a imagem original, como mostra a FIGURA 13(b). Deste modo temos que apenas se sobrepormos a imagem cifrada com a mesma chave utilizada no processo de codificação é que conseguimos recuperar a imagem inicial.

Nos métodos de cifragem de imagem apresentados anteriormente, a imagem obtida após o processo de decodificação de imagem está em distribuição de fase. Como uma imagem em distribuição de fase se torna invisível ao olho humano, após o processo de decodificação é necessário a aplicação da técnica de contraste de fase para que a imagem decodificada seja transformada em distribuição de amplitude e assim visível ao olho humano.

Já neste processo de cifragem de imagens trabalha-se com a imagem em sua distribuição de amplitude. Portanto, após o processo de decodificação, a imagem recuperada já se encontra em distribuição de amplitude, não necessitando assim a aplicação de qualquer outro método para que a imagem se torne visível ao olho humano.

Capítulo 5

Neste capítulo será mostrado a analogia entre os dois métodos de cifragem de imagens apresentados nos capítulos anteriores, Capítulo 3 e Capítulo 4. No primeiro método de cifragem, a cifragem é aplicada na imagem em sua modulação de fase e no outro método a cifragem é feita diretamente na imagem original, que está em modulação de amplitude.

5. Analogia entre o método de cifragem proposto e o método de contraste de fase

Mostrar-se-á que o método de cifragem de imagem que utiliza a técnica de contraste de fase apresentado no Capítulo 3 é análogo ao método proposto no capítulo anterior. O método de cifragem de imagens utilizando máscara binária aleatória foi baseado no método de contraste de fase.

No processo de cifragem de imagem utilizando o método de contraste de fase, a cifragem da imagem é obtida pela multiplicação da distribuição de fase obtida diretamente da imagem em nível de cinza que se deseja criptografar por uma distribuição de fase aleatória, a chamada chave do processo. Tal multiplicação é expressa matematicamente por

$$t^c = \exp[j(\phi(y,z) + 2\pi\psi(y,z))], \quad 0 \leq \psi(y,z) \leq 1. \quad (11)$$

Pode-se dizer que a distribuição em nível de cinza da imagem está linearmente relacionada com o valor de fase da mesma, FIGURA 14. Ou seja, o valor de nível de cinza 0 (preto) corresponde ao valor de fase 0, o valor de nível de cinza 255 (branco) corresponde ao valor de fase 2π . Já os outros níveis de cinza com valores entre 0 e 255 correspondem a valores intermediários de fase entre 0 e 2π . Assim existe uma correspondência linear entre os níveis de cinza de uma imagem e os seus valores de fase.

Para o processo de decodificação da imagem multiplica-se a imagem criptografada que está em modulação de fase pelo complexo conjugado da mesma chave utilizada para cifrar a imagem. Após tal multiplicação aplica-se o método de contraste de fase para que a imagem decodificada seja convertida em modulação de amplitude e assim torna-se-á visível ao olho humano.

FIGURA 14 – Distribuição de fase contínua da imagem com sua respectiva distribuição em nível de cinza.

Já no processo proposto, o de cifragem óptica de imagem utilizando máscara binária aleatória, a cifragem se dá pela multiplicação da imagem binária que se pretende criptografar por uma máscara binária aleatória, a chave deste processo. A multiplicação é feita pixel a pixel, onde a cor preta é representada pelo número -1 e a cor branca pelo número 1. Este processo é aplicado diretamente na imagem, estando esta em modulação de amplitude. Porém, tem-se que a imagem binária também pode ser expressa por uma distribuição de fase, FIGURA 15, onde as fases são apenas o 0 (branco) e o π (preto). Da mesma forma pode-se expressar a distribuição de fase da máscara binária aleatória. Ou seja, $\exp[j0] = 1$ (branco) e $\exp[j\pi] = -1$ (preto).

FIGURA 15 - Distribuição de fase da imagem com sua respectiva distribuição em nível de cinza.

A multiplicação entre a imagem binária e a chave do processo é então expressa matematicamente, em modulação de fase, por

$$\exp[ja_1] \times \exp[ja_2] = \exp[j(a_1 + a_2)], \text{ onde } a_i = 0 \text{ ou } \pi, i = 1, 2 \quad (12)$$

que é a imagem criptografada.

O processo de decodificação é dado pela sobreposição da imagem criptografada com a mesma chave do processo. A imagem resultante já é a imagem decodificada.

Comparando as expressões (11) e (12) que são as imagens cifradas do processo de cifragem de imagem utilizando o método de contraste de fase e do processo de cifragem óptica de imagens utilizando máscara binária aleatória respectivamente, percebe-se que ambas são análogas, ou seja, que a maneira de cifragem óptica de imagem dos dois métodos são análogas.

Mesmo os dois métodos sendo análogos, no próximo capítulo será apresentado alguns ataques realizados contra o método de cifragem óptica de imagens utilizando máscara binária aleatória para verificar a robustez do processo.

Capítulo 6

Vários tipos de ataques são realizados contra métodos de cifragem de imagem para se analisar a segurança da cifragem de tais métodos e descobrir se há pequenas falhas nos mesmos [16], [17] e [18]. No método de cifragem óptica de imagens utilizando máscara binária aleatória será aplicado dois tipos de ataques já conhecidos na literatura, o ataque da força bruta e o ataque do texto conhecido, [16] e [25], para verificar a robustez do método. A contribuição deste trabalho está no desenvolvimento de um novo tipo de ataque para realizar contra métodos de cifragem e verificar a robustez do mesmo. O novo ataque foi nomeado de ataque das cifras conhecidas.

6. Ataque da força bruta

Para um sistema de cifragem de imagem ser ideal, uma pessoa tendo o conhecimento apenas da imagem cifrada e do método utilizado para cifrar a imagem teria que tentar todas as possíveis combinações de pixels de uma imagem para que uma dessas combinações seja a chave do processo utilizada para cifrar a imagem e assim conseguir recuperar a imagem original.

Seja uma imagem binária de tamanho $N \times N$, com $N \in \mathbb{N}$. Tal imagem sofreu o processo de cifragem óptica de imagens utilizando máscara binária aleatória resultando em uma imagem cifrada de mesmo tamanho. Para realizar a cifragem, utilizou-se uma chave binária com o mesmo tamanho da imagem original (Capítulo 4).

Tem-se que a chave binária do processo é do tamanho de $N \times N$ pixels e que para cada pixel exista apenas duas possibilidades de cores (branco ou preto). O número de tentativas para recuperar a chave do processo é da ordem de $2^{N \times N}$, pois existem $2^{N \times N}$ combinações possíveis da chave do processo. Tomando $N=100$, o número de tentativas é $2^{10000} \approx 10^{3000}$ que é uma quantidade de tentativas consideravelmente alta.

Para qualquer valor prático de $N \times N$, $2^{N \times N}$ é um valor muito alto, e o mais importante, este valor aumenta exponencialmente com o número de pixels da imagem. Este grau de

complexidade é considerado intratável computacionalmente. Assim, o método apresentado é resistente ao ataque da força bruta.

Além disso, na tentativa de descobrir a chave original do processo de cifragem, ao sobrepor qualquer chave binária aleatória na imagem cifrada pode-se obter uma outra imagem diferente da original. E não dá para saber se a imagem que foi descoberta é de fato a imagem original ou é uma outra imagem qualquer. A FIGURA 16 ilustra tal situação ao sobrepor a imagem cifrada do número cinco, conforme FIGURA 12(c), por uma chave aleatória qualquer. A imagem recuperada foi a do número um enquanto que a imagem cifrada era a do número cinco. Recuperou-se a imagem de um número, porém a do número incorreto.

Isto é possível porque a característica visual da percepção humana é tolerável a pequenos erros. E assim não saberemos se a imagem obtida é a imagem que realmente pretende-se descobrir ou uma outra imagem que foi recuperada sozinha ao utilizar uma chave qualquer, na tentativa de descobrir a chave correta.

Na busca da chave correta do processo de cifragem óptico de imagem pode-se recuperar qualquer imagem e sem saber se a imagem é a original e nem mesmo qual é a chave correta.

FIGURA 16- Uma imagem recuperada ao sobrepor a imagem cifrada do número 5 com uma chave aleatória qualquer. A imagem recuperada foi a do número um enquanto a imagem original é o número cinco.

Portanto o método de cifragem óptica de imagens utilizando máscara binária aleatória é robusto ao ataque de força bruta.

6.1 Ataque do texto conhecido

Um aspecto importante é a capacidade do processo de cifragem de imagem em resistir a um ataque onde são conhecidas a imagem original e sua respectiva imagem cifrada.

Assume-se que são conhecidas a imagem original e sua correspondente imagem cifrada e o método utilizado para cifrar a imagem em questão. Com apenas o conhecimento deste particular par de imagens não se pode ser capaz de decodificar uma outra imagem cifrada para o processo ser robusto. Em particular, para um processo de cifragem ser

resistente não pode ser possível recuperar a chave do processo de cifragem apenas tendo o conhecimento do par de imagens: imagem original e respectiva imagem cifrada.

O processo de cifragem óptica de imagens utilizando máscara binária aleatória apresentado no capítulo anterior tem uma propriedade que facilita este ataque. Esta propriedade vem da matemática empregada no método. Tal matemática utiliza o cálculo linear. A operação linear utilizada no processo de cifragem de imagem apresentado é a multiplicação ponto a ponto de pixels realizada entre a imagem original e a chave do processo.

O processo de cifragem é realizado através da fórmula $d_{mn} = b_{mn} \times c_{mn}$ onde b_{mn} são os pixels da imagem original, c_{mn} os pixels da chave do processo e d_{mn} os pixels da imagem cifrada. Neste ataque d_{mn} e b_{mn} são conhecidos e tenta-se recuperar a chave do processo que é representada por c_{mn} . Logo,

$$c_{mn} = d_{mn} / b_{mn} \quad (13)$$

que é uma operação matemática linear e simples. Através deste resultado se descobre quais são os valores exatos de c_{mn} .

Com isso conclui-se que é possível recuperar a chave exata utilizada no sistema para cifrar a imagem. A partir disso consegue-se decifrar qualquer outra imagem que tenha sido cifrada pelo mesmo processo de cifragem e desde que tenha sido utilizado a mesma chave de cifragem no processo.

Tem-se então que tal processo de cifragem é robusto ao ataque do texto conhecido desde que para cifrar cada imagem diferente seja utilizado uma nova chave. Com as chaves sendo distintas não se consegue recuperar a imagem original.

6.2 Ataque das cifras conhecidas

O ideal de um processo de cifragem de imagem é que este seja robusto a todos os tipos de ataques que possa existir, tornando-o o mais confiável e seguro possível. Então, um novo tipo de ataque que pode ser realizado contra um processo de cifragem de imagem será analisado.

Este novo tipo de ataque foi a contribuição deste trabalho para a área de cifragem de imagem. O ataque foi nomeado de ataque das cifras conhecidas.

O ataque das cifras conhecidas é descrito da seguinte forma: supõe-se que várias imagens cifradas diferentes são conhecidas. Tais imagens foram cifradas através do processo de cifragem de imagens óptica utilizando máscara binária aleatória, e as mesmas foram cifradas com uma mesma chave binária. Com apenas o conhecimento destas imagens cifradas tenta-se descobrir a chave binária utilizada no processo e conseqüentemente as imagens originais.

Como exemplo tem-se as imagens dos números 2, 4 e 5 de mesmo tamanho e suas respectivas imagens cifradas ilustradas na FIGURA 17. Tais imagens foram cifradas pelo método apresentado no Capítulo 4 e com uma mesma chave binária, a qual está representada pela FIGURA 12(b).

Na tentativa de descobrir a chave binária do processo multiplica-se então duas a duas as imagens cifradas dos números 2, 4 e 5. Como visto no processo, a multiplicação entre duas imagens ocorre pela multiplicação pixel a pixel das imagens e não pela multiplicação usual entre matrizes. Os resultados obtidos foram as imagens apresentadas na FIGURA 18.

FIGURA 17 - Imagem dos números 2, 4 e 5 e suas respectivas imagens cifradas. Todas as imagens foram cifradas por uma única chave binária.

FIGURA 18 – Multiplicação entre as imagens cifradas nos números 2 e 5 e dos números 2 e 4 respectivamente.

Para a multiplicação entre os pixels das imagens cifradas resultar na cor branca, os respectivos pixels entre as duas imagens que foram multiplicadas tem que ser da mesma cor,

ou ambos da cor branca ou ambos da cor preta, pois são as únicas possibilidades da multiplicação resultar no valor 1, $1 \times 1 = 1$ ou $-1 \times (-1) = 1$ respectivamente.

Os pixels sendo iguais conclui-se que na região branca obtida da multiplicação entre as imagens cifradas os pixels tem que ser coincidentes, ou seja, ou os pixels são pixels da chave do processo ou são pixels de valores opostos aos da chave.

Na região onde a multiplicação resulta na cor preta tem-se que os pixels são de valores opostos, pois a única forma da multiplicação resultar no valor -1 é $1 \times (-1) = -1$. Com isso os pixels referentes a região preta em uma das imagens cifradas, após a multiplicação, são pixels da chave do processo e os respectivos pixels da outra imagem cifrada são pixels da imagem cifrada.

Com estas análises, as possibilidades em encontrar a chave correta aumentam drasticamente, pois apenas tem-se que fazer as combinações por regiões de brancos e pretos e não mais a combinação pixel a pixel.

O processo de cifragem óptica de imagens utilizando máscara binária aleatória é robusto ao ataque das cifras conhecidas desde que não se repita a chave para cifrar as mais diversificadas imagens.

Capítulo 7

Neste capítulo é apresentado os resultados finais obtidos após várias análises e alguns ataques sofridos contra o processo de cifragem óptica de imagens utilizando máscara binária aleatória desenvolvido neste trabalho. Também é apresentado as considerações finais.

7.1 Resultados

Na presente era, é importante proteger uma informação quando esta é transmitida através de um canal inseguro. Um meio de prevenir tal proteção é converter a informação inteligível para uma forma não inteligível antes de transmiti-la. E é o método para se fazer tal conversão que é estudado há anos. Vários métodos diferentes foram desenvolvidos para a transmissão tornar-se cada vez mais segura. Em todos os métodos existe pelo menos uma chave para cifrar tal informação. Assim somente conseguirá identificar a informação original quem tiver um conhecimento prévio da chave que a criptografou.

Neste trabalho foi desenvolvido um método de cifragem óptica de imagens utilizando máscara binária aleatória. Pode-se dizer que tal método é análogo ao processo de cifragem de imagem que utiliza o método de contraste de fase de Zernike. Porém o método desenvolvido trabalha com a imagem em modulação de amplitude e o análogo em modulação de fase.

O processo de cifragem de imagem proposto apresenta várias vantagens. Uma delas é que o método é de fácil implementação podendo ser obtida em materiais regulares e de baixo custo. Uma outra é que a chave binária utilizada no processo de cifragem é fácil de ser gerada. Uma vantagem importante é que a imagem obtida após o processo de decodificação já está visível ao olho humano dispensando-se a aplicação de um outro método para poder identificá-la. E também, o tamanho da imagem cifrada é igual ao tamanho da imagem original.

Ao sofrer o ataque da força bruta o método é robusto. Nem tentando todas as possibilidades de chaves binárias é possível recuperar a imagem original pois nas tentativas

pode se recuperar uma imagem inteligível mas que não é a imagem original. E esta dúvida permanecerá, se a imagem inteligível que foi recuperada é ou não a imagem original.

Já nos ataques do texto conhecido e das cifras conhecidas o método de cifragem óptica de imagens utilizando máscara binária aleatória só é robusto se utilizar uma chave diferente para cada imagem que se pretender cifrar.

Esta característica de que o método de cifragem é robusto se utilizar para cada imagem que for cifrar uma chave diferente não é específica deste método.

7.2 Considerações Finais

O método de cifragem desenvolvido em modulação de amplitude utiliza apenas uma chave binária para efetuar a cifragem. Um próximo passo seria o estudo do mesmo método de cifragem, porém utilizando duas máscaras binárias aleatórias diferentes para o processo de cifragem. E analisar se desta maneira o processo seria resistente aos ataques apresentados no Capítulo 6.

Um outro ponto interessante é que ao realizar o ataque das cifras-conhecidas, os números utilizados como exemplo estavam todos no centro da imagem. Com isso, ao efetuar a multiplicação das respectivas imagens cifradas, as informações relevantes continuaram no centro da imagem, aumentando a probabilidade de descobrir a chave original. Sugere-se realizar o mesmo ataque, porém com informações que estejam em posições diferentes na imagem.

Referências

- [1] REFREGIER, P.; JAVIDI, B. **Optical image encryption based on input plane and Fourier plane random encoding.** Optics Letters, v. 20, n. 7, p. 767-769, 1995.
- [2] TOWGHI, N.; JAVIDI, B.; LUO, Z. **Fully phase encrypted imagem processor.** Journal of Optical Society of America, v. 16, n. 8, p. 1915-1927, 1999.
- [3] MONAGHAN, D. et al. **Role of phase key in the double random phase encoding technique: an error analysis.** Applied Optics, v. 47, n. 21/20, p. 3808-3816, 2008.
- [4] JAVIDI, B. et al. **Fault tolerance properties of a double phase encoding encryption technique.** Optical Engineering, v.36, n. 4, p. 992-998, 1997.
- [5] UNNIKRISHNAN, J.; JOSEPH, J.; SINGH, K. **Optical encryption by double-random phase encoding in the fractional Fourier domain.** Optics Letters, v. 25, n. 12, p. 887-889, 2000.
- [6] JAVIDI, B. et al. **Error-reduction techniques and error analysis for fully phase-and amplitude-based encryption.** Applied Optics, v. 39, n. 23, p. 4117-4130, 2000.
- [7] JAVIDI, B.; TAKANORI, N. **Securing information by use of digital holography.** Optics Letters, v. 25, n. 1, p. 28-30, 2000.
- [8] SALEH, B. E. A.; TEICH, M. C. **Fundamental of Photonics.** John Wiley & Sons, Inc., 1991.
- [9] BRACEWELL, R. **The Fourier Transform and its applications.** McGraw-Hill Book Company, 1965.
- [10] NETO, L. G.; SHENG, Y. **Optical implementation of image encryption using random phase encoding.** Optical Engineering, v. 35, n. 9, p.2459-2463, 1996.
- [11] NETO, L. G. **Implementation of Image Encryption Using The Phase-Contrast Technique.** In: SPIE, v. 3386, p. 284-290, 1998.
- [12] GOODMAN, J. W. **Introduction to Fourier Optics.** McGraw-Hill International Editions, 1996.
- [13] MOGENSEN, P. C.; GLUCKSTAD, J. **Phase-only optical decryption of a fixed mask.** Applied Optics, v. 40, n. 8, p. 1226-1235, 2001.

- [14] NOMURA, T.; JAVIDI, B. **Optical encryption system with a binary key code.** Applied Optics, v. 39, n. 26, p. 4783-4787, 2000.
- [15] JOSHI, M.; SHAKHER, C.; SINGH, K. **Phase image encryption of colored images using double random phase encoding technique in HSV color space.** Optical Review, v. 16, n. 5, p. 511-516, 2009.
- [16] FRAUEL, Y. et al. **Resistance of the double random phase encryption against various attacks.** Optics Express, v. 15, n. 16, p. 10253-10265, 2007.
- [17] FRAUEL, Y. et al. **Security analysis of optical encryption.** SPIE, v. 5986, p. 25-34, 2005.
- [18] GOPINATHAN, U. et al. **A known-plaintext heuristic attack on the Fourier plane encryption algorithm.** Optics Express, v. 14, n. 8, p. 3181-3186, 2006.
- [19] HECHT, E.; **Optics.** Addison-Wesley Publishing Company, Inc, 1984.
- [20] HOWARD, J. N. **Honorary members of the 1950's.** Optics and Photonics News, v. 19, n. 5, p. 24-25, 2008.
- [21] NAOR, M.; SHAMIR, A. **Visual cryptography.** Advances in Cryptology-Eurocrypt '94, Lecture Notes in Computer Science, v. 950, p.1-12, Springer-Verlag, 1994.
- [22] LUKAC, R.; PLATANIOTIS, K. **Bit-level based secret sharing for image encryption.** Pattern Recognition, v. 38, p. 767-772, 2005.
- [23] HAN, J-W; PARK, C-S; RYU, D-H; KIM, E-S. **Optical image encryption based on XOR operations.** Optical Engineering, v. 38, n. 1, p. 47-54, 1999.
- [24] KADANOFF, L.P.; **Road to Chaos.** Physics Today, p 46-53, 1983.
- [25] CHIN, Y.-C.; WANG, P.-C.; HWANG, J.-J. **Cryptanalysis on Schwartz graphical encryption method.** Journal of Cryptologia, v. 17, n. 3, p.301-304, 1993.