Arquiteturas NTT e INTT de baixo consumo de energia para criptografia de imagens

ELOISA BARROS[1]; MORGANA DA ROSA[1];RAFAEL SOARES[1]

[1]Universidade Federal de Pelotas – elbarros@inf.ufpel.edu.br; morganamacedoazevedodarosa@gmail.com; rafael.soares@inf.ufpel.edu.br

1. INTRODUÇÃO

Nos últimos anos, o avanço tecnológico tem impulsionado o surgimento de importantes paradigmas computacionais, como a Computação em Nuvem, *machine learning* (ML) e Internet das Coisas (IoT). No entanto, à medida que esses sistemas se tornam mais sofisticados e complexos, a demanda por segurança de dados torna-se cada vez mais crítica. Esse cenário tem levado ao desenvolvimento de técnicas e algoritmos robustos, incluindo esquemas voltados para a criptografia de imagens. A segurança de imagens digitais envolve processos fundamentais, como a criptografia e descriptografia, realizados com o uso de chaves específicas. Esses processos podem ser implementados por diferentes métodos, sendo que os algoritmos baseados em operações polinomiais têm se mostrado particularmente eficazes. Entre as abordagens mais adotadas no campo da aritmética polinomial e processamento digital de imagens, destaca-se a *Number Theoretic Transform* (NTT) (Lima et al., 2015; Oliveira Neto et al., 2020), uma variação da *Discrete Fourier Transform* (DFT) que opera sobre anéis de inteiros que serão módulo um número primo, além de sua inversa, a INTT. A NTT/INTT possui características que a tornam promissora para esquemas criptográficos, principalmente devido à sua menor complexidade computacional, $O(n \log n)$, em comparação com outras abordagens como os algoritmos *schoolbook*, *Karatsuba*, *Toom-Cook* e a própria DFT (Liang, Zhao, 2022). Essa eficiência, aliada à sua estrutura algébrica, torna a NTT uma escolha frequente em esquemas de criptografia baseados em *lattices* (*Lattices-Based Cryptography*), que incluem diversas primitivas criptográficas como *Digital Signature*, *Public Key Encryption* (PKE), *Homomorphic Encryption*, entre outras. Embora a NTT acelere significativamente as multiplicações polinomiais, um dos principais desafios para sua aplicação é o alto consumo de memória durante a execução, o que limita seu uso em determinados cenários (Di Matteo et al., 2023), principalmente para sistemas com recursos limitados. A multiplicação de dois polinômios de grau muito alto envolve operações que podem se tornar computacionalmente intensivas, especialmente à medida que o grau dos polinômios aumenta. Nessas aplicações, multiplicações com polinômios representam a parte mais exigente em termos de tempo e memória. Este obstáculo tem gerado diversos estudos na busca por otimizações que mitiguem o impacto desse consumo, mantendo a eficiência das operações polinomiais e a integridade dos resultados. Este estudo realiza uma análise utilizando como caso de estudo o processamento de imagens para avaliar a aplicação e a eficácia da NTT e da INTT no contexto da criptografia e descriptografia de imagens. Neste trabalho, propomos uma implementação da NTT/INTT de baixo consumo, visando a eficiência do sistema em termos de desempenho, consumo de energia e área, enquanto garante a confiabilidade das imagens, buscando explorar novas abordagens na otimização das operações críticas dessas transformadas.

2. METODOLOGIA

A síntese das arquiteturas em VHDL é realizada com a ferramenta Cadence Genus, utilizando uma biblioteca de células comerciais de 65nm, com baixo consumo de energia e tensão de 1,25 V. A ferramenta gera o arquivo Gate-Level Netlist, que contém a estrutura lógica do design, e o arquivo Standard-Delay Format (SDF), que registra atrasos em portas e redes, falhas temporais, propagação de sinal, caminho crítico, área de célula e dissipação de potência. As arquiteturas foram sintetizadas a 400 MHz para permitir uma análise comparativa com a literatura. Esse processo foi realizado separadamente para a NTT, INTT e as arquiteturas integradas, visando avaliar a contribuição individual e conjunta de cada componente no desempenho geral. Após o processo de síntese lógica, é realizada a simulação do design a partir de estímulos de entrada através da ferramenta Cadence Xcelium. A partir dos arquivos *Gate-Level Netlist* e SDF gerados anteriormente, esse processo simula de maneira precisa a atividade de chaveamento do circuito, obtendo o arquivo *dump* e o arquivo de transição *Value Change Dump* (VCD), gerando relatórios precisos de dissipação de energia e permitindo a extração de estimativas precisas e detalhadas sobre o consumo de energia, área e potência. Como metodologia de verificação, este trabalho utiliza um método de co-simulação a partir das ferramentas *Matlab-Modelsim*, que consiste em um modelo de referência descrito em *Simulink* e o *Design Under Test* (DUT) representado a níveis de *netlist* após a síntese lógica. No ambiente *Matlab*, essa etapa compara as estruturas propostas neste trabalho com estruturas NTT/INTT exatas implementadas na ferramenta. Esse método executa múltiplas simulações com vetores de imagem para alcançar um comportamento realista do hardware na estimativa de desempenho. Para analisar e garantir a qualidade do projeto, serão empregadas métricas conhecidas para avaliação de erros, tais como: *Mean Absolute Error* (MAE), definida como a média de todos os erros absolutos, *Mean Relative Error Distance* (MRED), definida como a diferença entre um resultado exato e o resultado aproximado, a distância de Hamming, utilizada para comparar duas cadeias de dados binários, definida pelo número de posições de bits nas quais os dois bits se diferem, e o erro quadrático médio (MSE), também utilizado para obter métricas como a relação sinal-ruído de pico (*Peak Signal-to-Noise Ratio* - PSNR). Essas métricas possibilitam definir e analisar uma relação entre energia e qualidade do projeto.

3. RESULTADOS E DISCUSSÃO

Esta seção aborda os conceitos básicos das transformadas NTT/INTT aplicadas à criptografia e descriptografia, além dos resultados obtidos em eficácia e segurança. A aplicação da NTT envolve transformar um par de polinômios para o domínio da frequência, permitindo que o produto seja calculado por multiplicação ponto a ponto em $O(n)$, conforme Zhang et al. (2020). A NTT/INTT opera gradualmente obtendo a forma transformada a partir da sequência original, organizando os elementos de acordo com a ordem inversa dos bits de seus índices provenientes. Cada etapa incrementalmente aproxima a sequência de sua fase final transformada, conduzidas pelas estruturas chamadas *butterflies*. A partir de uma sequência de entradas, cada *butterfly* realiza as operações de soma e subtração em paralelo, ambas utilizando operação de módulo, resultando nas saídas das estruturas. Ao final desse processo, a INTT é aplicada à sequência

resultante para obter os coeficientes do polinômio resultante de volta ao domínio original, correspondendo ao processo de descriptografar uma imagem.

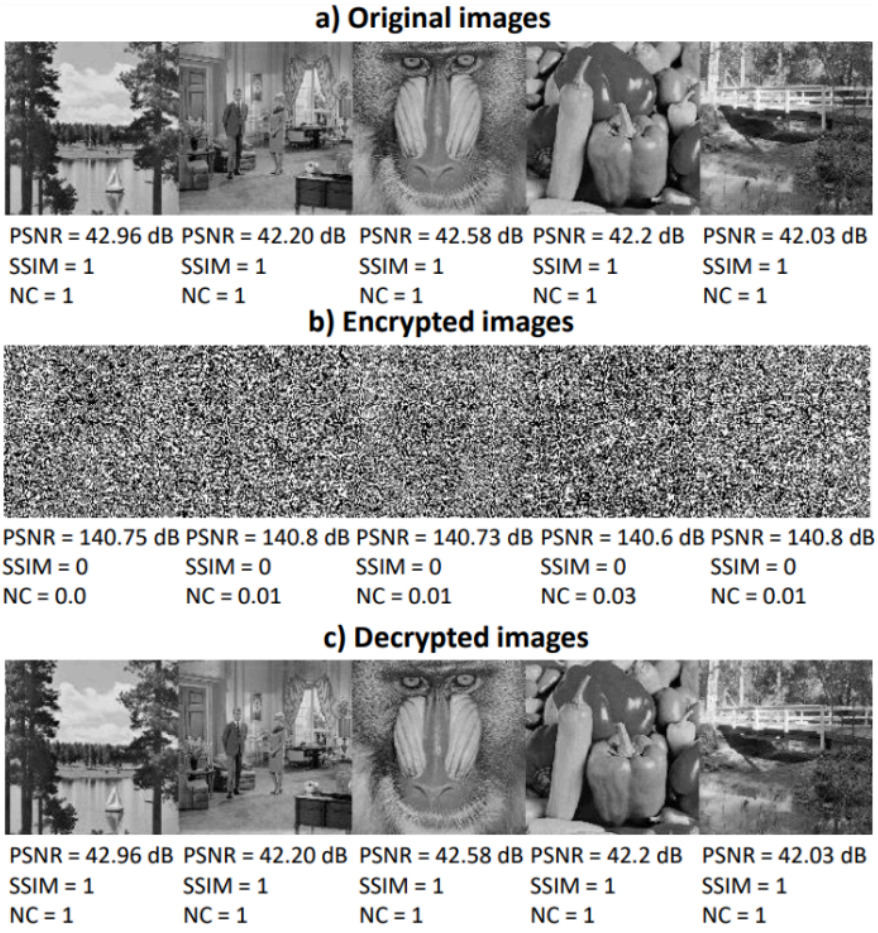

Figura 1. Métricas de precisão e qualidade para criptografia (NTT) e descriptografia (INTT). PSNR, SSIM e NC analisados.

A Figura 1 representa esses processos para uma sequência de imagens. Para validar a abordagem proposta, as seguintes métricas de erro foram mensuradas: (i) PSNR, que representa uma relação entre a potência do sinal (intensidade da imagem original) e a potência do ruído que afeta sua representação; (ii) similaridade estrutural (SSIM), indicando se as imagens são idênticas (1) ou se não possuem similaridade (0); (iii) Correlação cruzada normalizada (NC), também indicando a similaridade entre as imagens mas considerando a correlação linear entre os pixels. Nota-se que a imagem criptografada, apresentada na Figura 1-b, não é capaz de revelar informações confidenciais ou que possam comprometer a confiabilidade dos dados, resultando no valor 0 para as métricas SSIM e NC, o que indica que as imagens criptografadas não possuem nenhuma semelhança com a imagem original. Além disso, o valor elevado de aproximadamente 140db para a métrica PSNR das imagens criptografadas, sugere que as imagens tornaram-se irreconhecíveis, em comparação com os valores de aproximadamente 40db para as imagens antes desse processo, garantindo que os dados originais não podem ser reconhecidos sem a chave de descriptografia. Essa etapa é realizada através da NTT, a partir de uma chave específica e de valor superior a 2^{10} (valores inferiores não apresentam resultados satisfatórios), o processo de criptografia é realizado e a imagem é mascarada. Com a aplicação

da INTT, o processo de descriptografia é realizado e a imagem criptografada é convertida de volta ao seu domínio original, como mostrado na Figura 1-c, garantindo a recuperação fiel da imagem. A análise das métricas empregadas evidencia a integridade dos dados, demonstrando que não houveram bits corrompidos ou qualquer outro tipo de distorção que pudesse comprometer a qualidade da imagem após esses processos. Tanto a métrica NC quanto o SSIM apresentaram valor 1, indicando uma correspondência perfeita entre a imagem recuperada e a original, sem qualquer perda de informação visual ou semelhança comprometida.

4. CONCLUSÕES

Este trabalho propõe uma nova abordagem para a implementação das transformadas NTT e INTT no contexto da segurança de imagens. Diante das limitações físicas enfrentadas pelas tecnologias convencionais e da crescente demanda por eficiência energética em sistemas de hardware, a otimização das operações intensivas associadas à NTT tem sido amplamente discutida na literatura. Essa pesquisa visa não apenas melhorar o desempenho computacional dessas transformadas, mas também garantir a integridade e a confidencialidade das imagens, contribuindo para o avanço das soluções de segurança em aplicações que exigem processamento rápido e eficiente de dados, e/ou para sistemas com recursos limitados. Apesar dos avanços significativos já alcançados neste trabalho, etapas adicionais são necessárias para aprofundar a pesquisa e garantir a eficácia da implementação das transformadas NTT/INTT no contexto de segurança. Essas etapas incluem a avaliação da nossa proposta com as arquiteturas mais eficientes encontradas na literatura, bem como explorar a frequência máxima do circuito, a fim de compreender o seu funcionamento diante de condições extremas.

5. REFERÊNCIAS BIBLIOGRÁFICAS

J.B. Lima, F. Madeiro, F.J.R. Sales, Encryption of medical images based on the cosine number transform, **Signal Processing: Image Communication**, Volume 35, Pages 1-8, 2015.

J. R. de Oliveira Neto, J. B. Lima and D. Panario, The Design of a Novel Multiple-Parameter Fractional Number-Theoretic Transform and Its Application to Image Encryption, ***IEEE Transactions on Circuits and Systems for Video Technology***, vol. 30, no. 8, pp. 2489-2502, Aug. 2020

Liang, Z., Zhao, Y. Number theoretic transform and its applications in lattice-based cryptosystems: A survey. **arXiv preprint arXiv:2211.13546**, 2022.

S. Di Matteo, M. L. Gerfo and S. Saponara, VLSI Design and FPGA Implementation of an NTT Hardware Accelerator for Homomorphic SEAL-Embedded Library, ***IEEE Access***, vol. 11, pp. 72498-72508, 2023.

ZHANG, N., YANG, B., CHEN, C., YIN, S., WEI, S., LIU, L**.** Highly efficient architecture of NewHope-NIST on FPGA using low-complexity NTT/INTT. ***IACR Transactions on Cryptographic Hardware and Embedded Systems***, 2020.