UMA ARQUITETURA EFICIENTE EM TERMOS DE ENERGIA PARA A TRANSFORMADA HAAR APROXIMADA PARA CRIPTOGRAFAR E DESCRIPTOGRAFAR IMAGENS

MORGANA MACEDO AZEVEDO DA ROSA[1]; RAFAEL SOARES[1]; EDUARDO DA COSTA[2]

[1]*Universidade Federal de Pelotas – mmarosa@inf.ufpel.edu.br; rafael.soares@inf.ufpel.edu.br*
[2]*Universidade Católica de Pelotas – eduardo.costa@ucpel.edu.br*

1. INTRODUÇÃO

Nesta era digital de comunicação de dados, a transmissão de informações privadas por meio de um canal seguro é a principal preocupação de pesquisadores e provedores de segurança. A segurança da informação emprega diferentes estratégias para ocultar informações, entre elas é possível citar a criptografia e a esteganografia, visando atingir três objetivos: confidencialidade, integridade e disponibilidade (Forouzan, 2015). A criptografia oculta informações de usuários não autorizados por meio do embaralhamento de dados, tendo muitas aplicações tais como nas forças armadas, sistemas de comunicação e aeroespacial.

Uma metodologia para ocultar informações, baseada na Transformada Wavelet Discreta (DWT) foi introduzida por (Balaji, 2011) onde dados secretos são embutidos em quadros de vídeos. Em (Thakur, 2015), examina-se um novo método de criptografia aplicada a vídeos usando DWT e transformada de Arnold onde um alto valor de PSNR é alcançado. Em (Gao, 2008), apresenta-se um esquema de criptografia de imagem, que emprega uma matriz de embaralhamento total da imagem para embaralhar as posições dos pixels e então usa um sistema hiper-caótico para confundir a relação entre a imagem original e a imagem cifrada. Em (Parthasarathy, 2015), usa-se a transformada Wavelet Haar para criptografar imagens e a transformada Haar inversa para descriptografar as imagens.

Neste trabalho, explora-se uma nova forma de criptografar e descriptografar imagens. O método proposto aplica a Transformada Discreta Wavelet Haar (DWHT) com quatro níveis de decomposição. A solução proposta DWHT é implementada em hardware empregando conceitos de computação aproximada e explorando circuitos somadores consolidados da literatura como o Carry Lookahead, Ripple Carry, Brent Kung, Kogge Stone, Ladner Fischer, Han Carlson e Sklansky. A DWHT utiliza o coeficiente de aproximação $\frac{1}{\sqrt{2}}$, que introduz um acréscimo de dissipação de potência. Entretanto, como observado por (Seidel, 2020; Rosa, 2021), torna-se possível reduzir as operações aritméticas implementando o coeficiente $\frac{1}{\sqrt{2}}$ com multiplicações por constantes simples (*Single Constante Multiplication - SCS*). No entanto, para a arquitetura proposta aproxima-se o coeficiente da Haar para 1, não havendo assim, a necessidade de circuitos multiplicadores. Para criptografar as imagens, usa-se a transformada Haar aproximada até o quarto nível de decomposição. Para descriptografar as imagens, a arquitetura Haar proposta fornece o coeficiente de aproximação igual a 2, além do coeficiente de aproximação igual a 4. O grande diferencial do trabalho proposto é usar uma transformada Haar aproximada que embaralha os pixels da imagem original em maior grau em relação à transformada Haar original.

O processo inverso de recuperação da imagem no destino aumenta a qualidade da imagem. O aumento da qualidade da imagem em relação à DWHT original ocorre devido ao fato do hardware para a criptografia usar a mesma essência da descriptografia.

2. METODOLOGIA

A métrica PSNR (*Peak Signal-to-Noise Ratio*) calcula a relação sinal-ruído de pico, em decibéis, entre duas imagens. Essa proporção é usada como uma medida de qualidade entre a imagem original e uma imagem reconstruída. Quanto maior o PSNR, melhor será a qualidade da imagem reconstruída. Para adquirir os resultados de PSNR com a arquitetura proposta, utiliza-se o software MATLAB no processo de cossimulação vinculado à ferramenta MODELSIM. Inicialmente as imagens passam por um processo de transformação de duas dimensões para uma dimensão. A seguir, as imagens são processadas pelo hardware da Haar aproximada até os coeficientes de detalhe de nível 4, resultando no processo de criptografia. O resultado da transformada Haar é processado com o hardware da Haar inversa aproximada até os coeficientes de detalhe de nível 2, resultando no processo de descriptografia. Por fim, a saída $\hat{X}(n)$ é transformada de uma dimensão para duas dimensões.

3. RESULTADOS E DISCUSSÃO

Os resultados de PSNR, descritos na Tabela I, são comparados com a Haar-4 nativa do MATLAB que apresenta melhores resultados em relação ao estado-da-arte (Parthasarathy, 2015). A Tabela I mostra que a arquitetura proposta apresenta os melhores resultados de PSNR para todas as imagens testadas em tons de cinza e com diferentes dimensões: a) Cameraman (256x256 pixels), b) Lena (256x256 pixels), c) Barco (512x512 pixels), d) Woman (566x402 pixels), todas nos processos de criptografia e descriptografia. Esses resultados se consolidam, pois o embaralhamento dos pixels nas imagens é maior devido à aproximação e o processo de descriptografia apresenta resultados promissores no processo de reconstrução, uma vez que o hardware inverso cancela o embaralhamento dos pixels adicionados no processo de criptografia.

Tabela I: Resultados de PSNR do teste com várias imagens padrão, imagens criptografadas e descriptografadas. Criptografada - PSNR entre imagens originais e criptografadas. Descriptografada - PSNR entre imagens originais e descriptografadas.

	Imagens	Criptografada	Descriptografada
MATLAB	Cameraman	7,7394	29,1529
	Lena	7,8975	39,5931
	Boat	7,6143	32,4829
	Woman	8,9801	29,6188
Aproximada	Cameraman	2,9784	98,1087
	Lena	2,0021	99,9100
	Boat	1,3023	98,1711
	Woman	3,6845	97,0254

Os resultados de síntese referem-se à área, dissipação de potência e energia por operação (EPO). As estruturas Haar foram descritas em VHDL usando o somador inferido pela ferramenta de síntese lógica (operador '+' em VHDL) e explorando os somadores CLA, RCA e PPAs (*Parallel Prefix Adders*). A ferramenta Cadence Genus™ realizou a síntese com *netlist* ao nível de portas RTL. As estruturas Haar foram mapeadas para células padrão de 65 nm com tensão de alimentação de 1,25 V, na frequência máxima do relógio (*slack* zero) atingindo 250 MHz. Utiliza-se a ferramenta Cadence Incisive para realizar as simulações considerando os atrasos da porta para um atraso preciso de propagação do sinal e *glitches* temporais. Gera-se um arquivo *Toggle Count Format* (TCF) e carrega-o na ferramenta de síntese para realizar uma extração de energia baseada em dados. A metodologia de estimativa de energia utiliza a ferramenta de síntese Genus no modo PLE (*Physical-aware Layout Estimation*) para gerar os resultados. Estimulam-se as *netlists* pós-síntese usando a imagem Lena com 65.536 amostras para os resultados de dissipação de potência com estímulos de entrada realísticos. A Tabela II mostra que a estrutura mais eficiente em termos de área e energia é a arquitetura Haar aproximada e Haar inversa usando o somador PPA Ladner Fischer. A arquitetura aproximada elimina o coeficiente $\frac{1}{\sqrt{2}}$ da arquitetura original, reduzindo o uso de multiplicadores para compor os coeficientes. A arquitetura com uso do somador PPA Ladner Fischer apresenta uma redução de 58.662% na área total da célula e 1,32 vezes no consumo de energia.

Tabela II: IHDWT – Transformada Wavelet Haar inversa, Original – precisa IHDWT, Aproximada – aproximada IHDWT, *Tool* -- é o somador selecionado automaticamente pela ferramenta de síntese. Total é a dissipação de potência total em (µW), Área é a área do circuito em (µm²), Gates - contagem de portas (k gates), EPO é a Energia por operação (fJ / op).

IHDWT	Somador	*Gates* (k gates)	Área (μm^2)	Power dissipation (μW)			EPO (fJ/op)
				Estática	Dinâmica	Total	
Original	*Tool*	821	4102,100	4,325	5,940	10.265	41,060
Aproximada	BK	592	2920,320	3,155	3,904	7,060	28,240
	HC	646	3076,320	3,315	3,680	6,995	27,980
	KS	707	3211,520	3,408	4,235	7,643	30,572
	LF	407	2585,440	1,647	2,785	4,432	17,728
	SK	506	2773,680	1,872	2,825	4,697	22,784
	CLA	594	2920,840	3,160	3,889	7,049	28,196
	RCA	565	2869,360	3,071	3,675	6,746	26,984
	Tool	581	3302,320	3,106	4,873	7,979	31,916

4. CONCLUSÕES

Este trabalho propõe a implementação em hardware da transformada Wavelet Haar obtendo baixo consumo energético para criptografar e descriptografar imagens no processo de esteganografia. Explora-se a transformada Wavelet Haar aproximada com nível de decomposição igual a 4, no processo de criptografia. Para a reconstrução ou para descriptografar imagens é

usada a Haar aproximada com nível de decomposição igual a 2. Para melhorar a eficiência energética do hardware proposto, explora-se o uso de somadores consolidados da literatura nas transformadas Haar direta e inversa. Em comparação com o estado da arte, para todas as imagens de teste a arquitetura proposta apresentou os melhores resultados de PSNR (*Peak Signal-to-Noise Ratio*) no processo de criptografar e descriptografar. Em termos de dissipação de potência, a arquitetura proposta com uso do somador Ladner Fischer apresenta uma redução de 1,32 vezes, em relação com a arquitetura Haar original.

5. REFERÊNCIAS BIBLIOGRÁFICAS

FOROUZAN, Behrouz A.; MUKHOPADHYAY, Debdeep. **Cryptography and network security**. New York, NY: Mc Graw Hill Education (India) Private Limited, 2015.

COX, Ingemar et al. **Digital watermarking and steganography**. Morgan kaufmann, 2007.

BALAJI, R.; NAVEEN, Garewal. Secure data transmission using video Steganography. In: **2011 IEEE International Conference on Electro/Information Technology**. IEEE, 2011. p. 1-5.

THAKUR, Abhinav; SINGH, Harbinder; SHARDA, Shikha. Secure video steganography based on discrete wavelet transform and Arnold transform. **International Journal of Computer Applications**, v. 123, n. 11, 2015.

GAO, Tiegang; CHEN, Zengqiang. A new image encryption algorithm based on hyper-chaos. **Physics Letters A**, v. 372, n. 4, p. 394-400, 2008.

SEIDEL, Henrique et al. Energy-Efficient Haar Transform Architectures Using Efficient Addition Schemes. In: **2020 IEEE 11th Latin American Symposium on Circuits & Systems (LASCAS)**. IEEE, 2020. p. 1-4.

DA ROSA, Morgana M. et al. An Energy-Efficient Haar Wavelet Transform Architecture for Respiratory Signal Processing. **IEEE Transactions on Circuits and Systems II: Express Briefs**, v. 68, n. 2, p. 597-601, 2020.

PARTHASARATHY, M. B.; SRINIVASAN, B. Increased security in image cryptography using wavelet transforms. **Indian Journal of Science and Technology**, v. 8, n. 12, p. 1-8, 2015.