Steganography Genetic Algorithm Hyperparameter Tuning through Response Surface Methodology

Warley Gramacho da Silva[1], Rafael Lima de Carvalho[1] and Glêndara Aparecida de Souza Martins[2]

[1] *Federal University of Tocantins - UFT, Computer Science Department, Palmas-TO, Brazil*
[2] *Federal University of Tocantins - UFT, Food Engineering Department, Palmas-TO, Brazil*

Reception date of the manuscript: 27/02/2020
Acceptance date of the manuscript: 28/02/2020
Publication date: 09/03/2020

Abstract— Steganography consists of hidding bits of an information source into a host source. In image processing, a common way of doing the hiding process is to break each byte from the message information and embbed into the message bytes in a way that the differences among the original host and the embedded one are minimized. A Genetic Algorithm (GA) can be used to find the proper combination of bits in order to minimize such differences, but some hyperparameters need to be optimized in order to get an optimized performance. This work investigates the application of Response Surface Methodology (RSM) to find the best hyperparameters of a genetic algorithm applied to image steganography. As a result, RSM was able to point out fine-tuning hyperparameters for the GA.

Keywords—RSM, Steganography, Genetic Algorithms, Hyperparameter Optimization

I. INTRODUÇÃO

A esteganografia é a arte de ocultar informações digitais, a fim de impedir a detecção de mensagens ocultas, ou seja, o objetivo da esteganografia é evitar a suspeita na transmissão de uma mensagem secreta. Inclui-se técnicas para ocultar uma imagem, um arquivo de texto, um arquivo de áudio e até mesmo um programa executável dentro de uma imagem de cobertura sem distorção visual da imagem [1, 2]. Como apresentado em [3], esteganografia pode ser formalmente definida como o processo de incorporação que descreve um mapeamento de $E : C \times M \rightarrow C$, em que C é o conjunto de coberturas possíveis e M é o conjunto de possíveis mensagens. O processo de extração consiste em um mapeamento de $D : C \rightarrow M$, extraindo a mensagem secreta de uma imagem de cobertura.

Definição I.1 *O quádruplo* $\Psi =< C,M,D,E >$*, onde* C *é o conjunto de coberturas possíveis,* M *o conjunto de mensagens secretas com* $|C| \geq |M|$*,* $E : C \times M \rightarrow C$ *a função de mapeamento e* $D : C \rightarrow M$*, a função de extração, com a propriedade que* $D(E(c,m)) = m$ *para todos os* $m \in M$ *e* $c \in C$ *[3].*

O processo de mapeamento é definido de forma que a imagem de cobertura e o objeto “stego" correspondente sejam perceptivamente semelhantes. O esquema de esteganografia pode ser visto na Figura 1.

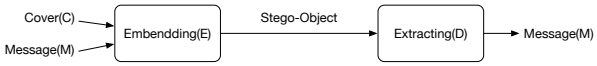

Fig. 1: Fluxograma de esteganografia

De acordo com [2], existem seis categorias de esteganografia, a saber: técnicas de sistema de substituição, técnicas de transformação de domínio, técnicas de espectro de espalhamento, técnicas de método estatístico, técnicas de distorção e técnicas de geração de cobertura. Na técnica do sistema de substituição, os *bits* redundantes ou desnecessários são subistituidos de uma imagem de cobertura pelos *bits* da mensagem secreta usando, por exemplo, o método *Bit* Menos Significativo (LSB, do inglês, *Least Significant Bit*) para codificar a mensagem secreta. No entanto, a esteganografia do LSB é suscetível as técnicas de análise de esteganização [4]. Para evitar a instalação de detecção de esteganografia através do uso do método LSB, em [5], foi proposta uma nova estratégia de substituição dos *bits*. Com o objetivo de otimizar o desempenho desse esquema proposto, foi utilizado um Algoritmo Genético (GA).

Os GAs possuem alguns parâmetros de entrada que são, geralmente, definidos manualmente após várias tentativas de ajustes. Uma técnica usada para definir um ajuste para os parâmetros dos AGs é a técnica da Metodologia da Superfície de Resposta (RSM). O RSM é uma combinação de técnicas matemáticas e estatísticas adequadas para modelagem e análise de problemas nos quais a variável resposta é afetada por várias variáveis de entrada, que visam otimizar as respostas [6].

Contact data: Warley Gramacho da Silva, 109 Norte, Av. NS15, Câmpus Universitário de Palmas, wgramacho@uft.edu.br

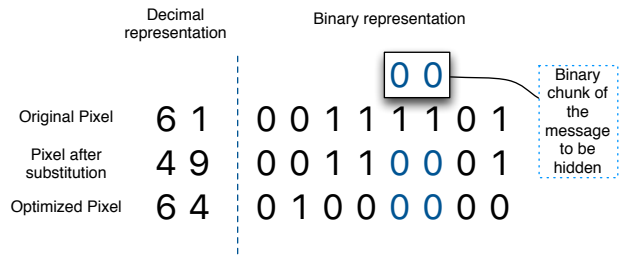

Fig. 2: Modelo de otimização adotado. Na imagem, o pixel original (valor 61 em decimal) recebe o par de pixels (00). Após a substituição, o valor do pixel otimizado se torna 64.

Neste artigo, propõe-se o uso da MRS para melhor ajuste dos parâmetros do AG para otimizar a esteganografia de imagens usando uma estratégia de substituição dos *bits* conforme proposto por [5].

II. Algoritmo Genético para o Problema de Esteganografia

Algoritmos Genético é uma metahaurística de otimização bio-inspirada, proposta por John Holland nos anos 1960 [7]. O GA é um método de busca e otimização que simula os processos naturais da evolução que consistem basicamente nos processos de cruzamento, mutação, mapeamento de fenótipo e calculo de aptidão (*fitness*) [8].

A idéia básica do GA é mostrada no Algoritmo 1 e funciona da seguinte maneira. Uma população inicial é gerada. Depois disso, o *loop* do algoritmo genético começa com a etapa de cruzamento, onde dois indivíduos são selecionados para serem os pais de um novo indivíduo, essa etapa é repetida até que não haja mais pais. Logo após a mutação ocorrer, é necessária uma baixa taxa de mutação nesta etapa para não comprometer a geração. E, finalmente, o processo de seleção natural. Para concluir o *loop*, um critério de parada é avaliado (número máximo de iteração).

Algoritmo 1 *Basic Genetic Algorithm [8]*

```
1: inicializa a população
2: repeat
3:     repeat
4:         Aplica crossover
5:         Aplica mutação
6:         Calculo da função fitness
7:     until população completa
8: until número de geração atingido
```

O princípio de otimização usado neste trabalho segue o proposto em [5]. Nesta abordagem, cada *byte* de destino deve passar por uma fase de verificação. Para ilustrar como isso funciona, considere um *byte*, como ilustrado na Figura 2. Na figura, o primeiro *byte* (61) é o valor original do pixel encontrado na imagem de destino. Neste exemplo, a mensagem será colocada na terceira e quarta posição do pixel de destino. Ao fazer a substituição, o valor do pixel se torna 49, o que fornece uma diferença de luminância de 12. Depois de otimizar o valor do pixel, pode ser visto que o valor 64 está mais próximo do valor original, enquanto o bloco de mensagens a ser oculto permanece incorporado.

Fig. 3: Imagem-alvo utilizada nos experimentos.

A representação binária do pixel favorece uma escolha natural para abordagem de otimização tais como Algoritmos Genéticos. Neste artigo, a função de aptidão (*fitness*) é uma função quadrática que contabiliza a diferença entre os *pixels* originais e os otimizados. Esta função pode ser conforme.

$$\sum_{i}^{N}(pixel_i - optimizedPixel_i)^2 \tag{1}$$

A solução ótima para o problema é a mais próxima do conjunto original de *pixels*, a população do Algoritmo Genético é gerada tendo pontos aleatórios ao redor da imagem original. Depois disso, a população inicial é atualizada para manter os *bits* da mensagem oculta. Em sequência, o *fitness* de cada individuo é calculado para prosseguir com o restante do algoritmo AG.

III. Experimentos

Para execução do AG, a Figura 3 foi utilizada para realização dos testes juntamente com uma mensagem de texto aleatória a ser oculta na imagem de destino.

Para ilustrar a abordagem de ajuste dos parâmetros do AG, selecionou-se um conjunto de parâmetros para observação das respectivas influências no desempenho do AG, independentemente do problema estudado. Neste caso, os seguintes parâmetros foram analisados: probabilidade de mutação ($pMut$), probabilidade de cruzamento ($pCros$), tamanho da população ($sPop$) e número de gerações ($nGen$).

Empregou-se nesse projeto o planejamento fatorial completo 2^k, com $k = 4$ parâmetros do AG (fatores principais) e três níveis. Os níveis são mostrados como -1, quando o fator está em um nível mínimo, 0, quando o fator esta no nível central, e $+1$, quando o fator pretendido está em um nível máximo [9]. Os parâmetros e seus níveis correspondentes podem ser vistos na Tabela 1.

Os experimentos realizados têm por objetivo buscar o melhor ajuste dos parâmetros de entrada do Algoritmo Genético de tal modo que sejam encontradas as melhores respostas médias para a função *fitness*. Desta forma, foram executadas

TABLE 1: VALORES PARA OS PARÂMETROS DO AG.

Parâmetros do AG	Codificado	pCros	pMut	sPop	nGen
Mínimo	−1	0.01	0.01	10	10
Central	0	0.50	0.50	105	105
Máximo	1	0.99	0.99	200	200

3 repetições e para cada repetição o algoritmo genético foi executado 10 vezes, retornando a resposta média. Os valores encontrados podem ser observados na Tabela 2.

TABLE 2: VALOR DE *fitness* PARA DIFERENTES AJUSTES DE PARÂMETROS DO AG.

ponto	pCros	pMut	sPop	nGen	fitness
1	0.01	0.01	10	10	14530.9
2	0.01	0.01	10	105	14514.9
3	0.01	0.01	10	200	14491.5
4	0.01	0.01	105	10	14045.6
5	0.01	0.01	105	105	14046.5
6	0.01	0.01	105	200	14039.6
7	0.01	0.01	200	10	13874.72
8	0.01	0.01	200	105	13884.2
9	0.01	0.01	200	200	13897.6
10	0.01	0.5	10	10	14581.6
11	0.01	0.5	10	105	14387.1
12	0.01	0.5	10	200	14496.5
13	0.01	0.5	105	10	14089.0
14	0.01	0.5	105	105	14023.7
15	0.01	0.5	105	200	14051.5
16	0.01	0.5	200	10	13937.5
17	0.01	0.5	200	105	13957.8
18	0.01	0.5	200	200	13925.5
19	0.01	0.99	10	10	14538.6
20	0.01	0.99	10	105	14447.3
21	0.01	0.99	10	200	14548.1
22	0.01	0.99	105	10	14097.0
23	0.01	0.99	105	105	14040.8
24	0.01	0.99	105	200	14050.5
25	0.01	0.99	200	10	13918.7
26	0.01	0.99	200	105	13950.9
27	0.01	0.99	200	200	13941.3
28	0.5	0.01	10	10	14375.9
29	0.5	0.01	10	105	14134.8
30	0.5	0.01	10	200	14235.5
31	0.5	0.01	105	10	13641.1
32	0.5	0.01	105	105	13644.1
33	0.5	0.01	105	200	13570.2
34	0.5	0.01	200	10	13609.0
35	0.5	0.01	200	105	13417.7
36	0.5	0.01	200	200	13426.0
37	0.5	0.5	10	10	14423.0
38	0.5	0.5	10	105	14554.0
39	0.5	0.5	10	200	14503.7
40	0.5	0.5	105	10	13885.1
41	0.5	0.5	105	105	13851.6
42	0.5	0.5	105	200	13886.9
43	0.5	0.5	200	10	13730.6
44	0.5	0.5	200	105	13763.2
45	0.5	0.5	200	200	13820.1
46	0.5	0.99	10	10	14456.4
47	0.5	0.99	10	105	14460.0
48	0.5	0.99	10	200	14486.2
49	0.5	0.99	105	10	13787.9
50	0.5	0.99	105	105	13890.6
51	0.5	0.99	105	200	13926.5
52	0.5	0.99	200	10	13801.2
53	0.5	0.99	200	105	13844.6
54	0.5	0.99	200	200	13787.7
55	0.99	0.01	10	10	14135.3
56	0.99	0.01	10	105	14309.5
57	0.99	0.01	10	200	14275.4
58	0.99	0.01	105	10	13675.3
59	0.99	0.01	105	105	13469.5
60	0.99	0.01	105	200	13527.2
61	0.99	0.01	200	10	13532.2
62	0.99	0.01	200	105	13332.5
63	0.99	0.01	200	200	13322.0
64	0.99	0.5	10	10	14351.8
65	0.99	0.5	10	105	14458.8
66	0.99	0.5	10	200	14415.6
67	0.99	0.5	105	10	13872.5
68	0.99	0.5	105	105	13790.7
69	0.99	0.5	105	200	13756.7
70	0.99	0.5	200	10	13663.3
71	0.99	0.5	200	105	13681.0
72	0.99	0.5	200	200	13581.2
73	0.99	0.99	10	10	14336.7
74	0.99	0.99	10	105	14346.1
75	0.99	0.99	10	200	14389.2
76	0.99	0.99	105	10	13843.0
77	0.99	0.99	105	105	13820.1
78	0.99	0.99	105	200	13817.9
79	0.99	0.99	200	10	13632.4
80	0.99	0.99	200	105	13695.3
81	0.99	0.99	200	200	13670.6

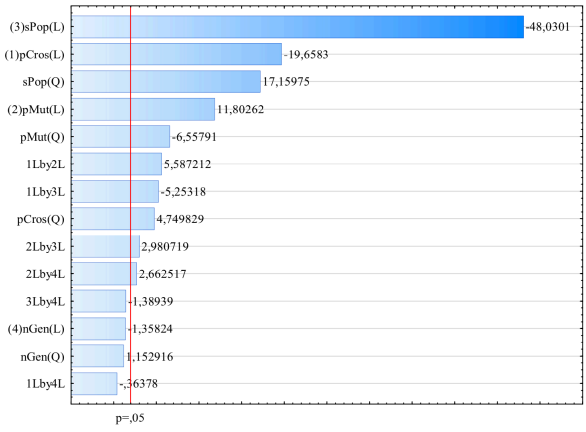

Fig. 4: Diagrama de Pareto.

IV. Resultados e discussões

O diagrama de Pareto apresentado na Figura 4 mostra que os parâmetros que mais influenciaram na minimização do *fitness* são o tamanho da população (*sPop*) e o percentual de crossover (*pCros*) quando avaliados separadamente. No entanto, quando combinados os parâmetros, o *pCros x pMut* associado ao *pCros x sPop* exerceram maior influência sob o *fitness*.

A relação entre os valores preditos e os valores ajustados (Figura 5) mostram alta correlação entre as variáveis estudadas. Não obstante, destaca-se, ainda, que o valor do coeficiente de determinação encontrado para os modelos estudados foi de $93,48\%$, fato esse que, conforme descreve [10], indica elevada confiabilidade do modelo, uma vez o R^2 é o valor que mede o efeito da variável independente na variação dependente e, quanto mais próximo de 1, maior a correlação.

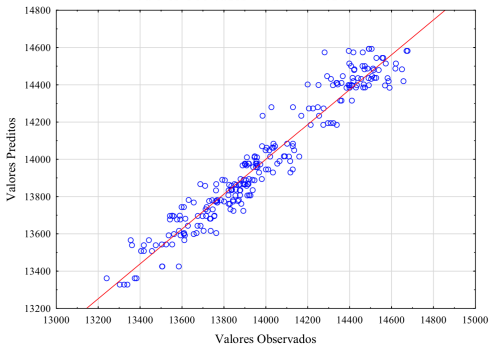

Fig. 5: Valores observados x Valores preditos.

Quando associadas, as variáveis *nGen* e *sPop* (Figura 6), observa-se que, independente dos valores de *nGen*, quanto maior forem os valores de *sPop* melhor será a resposta, corroborando com o descrito no diagrama de pareto (Figura 4) que apresenta uma correlação direta entre a resposta e a variável *sPop*, ou seja, a medida que uma aumenta a outra possivelmente seguirá um comportamento semelhante.

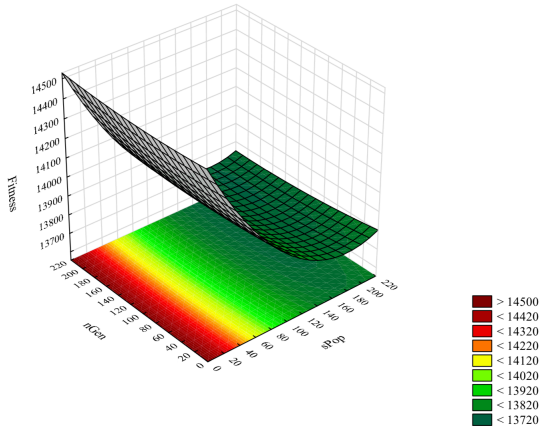

Fig. 6: Superfície de Resposta para a Interação dos parâmetros *nGen* x *sPop*

O valor de *fitness* observado durante a interação entre *sPop* x *pMut* (Figura 7) indica que as melhores condições de ação dessas variáveis são em faixas elevadas de *sPop* e reduzidas de *pMut*. Nesse sentido o diagrama de Pareto (Figura 4) também destaca a relação inversa entre a variável *pMut* e a resposta *fitness*, uma vez que o índice negativo indica que a redução de uma implicará no aumento da outra.

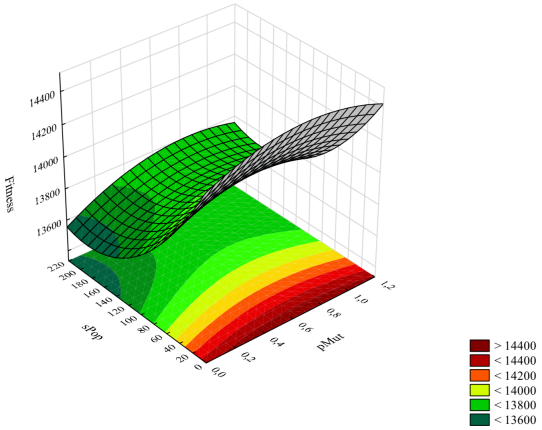

Fig. 7: Superfície de Resposta para a Interação dos parâmetros *nMut* x *sPop*.

Ao correlacionar as variáveis *nGen* e *pMut* (Figura 8) destaca-se que o *nGen* não exerce qualquer influência sobre a resposta, corroborando com o apresentado pelo Diagrama de Pareto (Figura 8). Por outro lado, a *pMut* apresentou o mesmo comportamento observado em outras interações das quais participou, ou seja, sua faixa desejável de atuação está em valores próximos ao parâmetro mínimo estudado (-1).

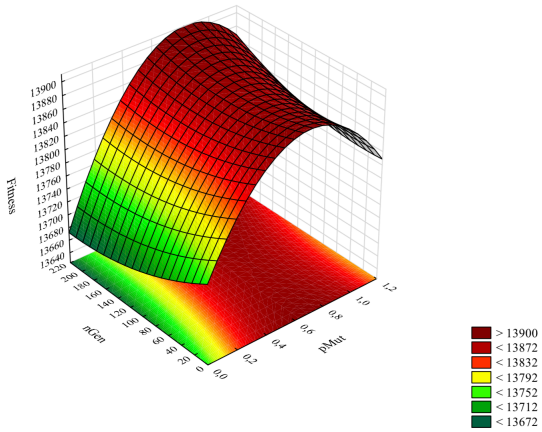

Fig. 8: Superfície de Resposta para a Interação dos parâmetros *nGen* x *pMut*.

No âmbito da correlação entre a *sPop* e a *pCros* (Figura 9) observa-se que a melhor faixa da variável resposta encontra-se em valores próximos ao parâmetro máximo (1) para ambas as variáveis independentes, confirmando, novamente, o comportamento descrito pelo Diagrama de Pareto (Figura 4).

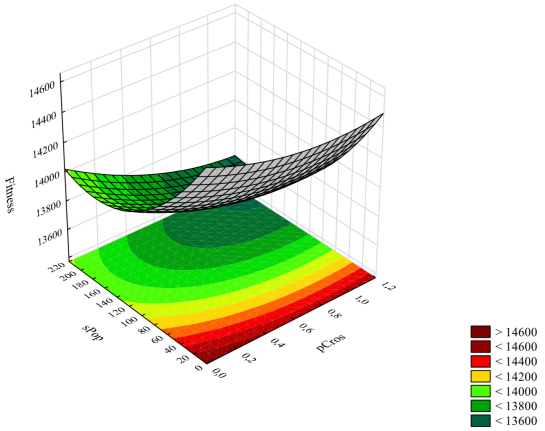

Fig. 9: Superfície de Resposta para a Interação dos parâmetros *nCros* x *sPop*.

V. Conclusões

Este trabalho apresentou a utilização de Algoritmos Genéticos (AG) para a área de Esteganografia, mostrando a aplicação da metodologia de Superfície de Resposta (MRS) como método de otimização de seus hiper-parâmetros. Um experimento foi conduzido de maneira a observar quatro hiperparâmetros do AG em questão. O experimento levou a concluir que a variável independente *nGen* não exerce influência significativa na variável resposta e que as melhores faixas de *fitness* encontram-se próximas ao parâmetro mínimo de *pMut* e máximo de *sPop* e *pCros*.

Neste sentido, conclui-se que após o uso da MSR, evitou-se, tanto quanto possível, os riscos e erros associados ao método de tentativa e erro na definição de parâmetros do AG avaliado. Como observado nos gráficos na seção IV, a MSR indicou a região de valores para melhor configuração de parâmetros que levaram a minimização do valor da função *fitness* em questão.

References

[1] F. Y. Shih, *Digital Watermarking and Steganography: Fundamentals and Techniques*, 1st ed. Boca Raton, FL, USA: CRC Press, Inc., 2007.

[2] G. Kipper, *Investigator's Guide to Steganography*. CRC Press, 2003.

[3] S. Katzenbeisser and F. Petitcolas, *Information Hiding Techniques for Steganography and Digital Watermarking*, ser. Artech House computer security series. Artech House, 2000.

[4] S. Mungmode, R. Sedamkar, and N. Kulkarni, "A modified high frequency adaptive security approach using steganography for region selection based on threshold value," *Procedia Computer Science*, vol. 79, pp. 912 – 921, 2016.

[5] Gangeshawar and J. Attri, "Optimizing image steganography using genetic algorithm," *International Journal of Engineering Trends and Technology (IJETT)*, vol. 24, no. 1, pp. 32–38, 2015.

[6] D. Montgomery, *Design and Analysis of Experiments, 6th Edition Set*. John Wiley & Sons, Limited, 2007.

[7] M. Mitchell, *An Introduction to Genetic Algorithms*, 1st ed., ser. Complex Adaptive Systems. The MIT Press, 1996.

[8] O. Kramer, *Genetic Algorithm Essentials*, ser. Studies in Computational Intelligence. Springer, 2017, vol. 679.

[9] T.-Y. Wang and K.-B. Wu, "A parameter set design procedure for the simulated annealing algorithm under the computational time constraint," *Computers & Operations Research*, vol. 26, no. 7, p. 665–678, Jun. 1999.

[10] P. R. M. de Azevedo, *Introdução à estatística*, 3rd ed. EDUFRN, 2016.