Data Hiding Based on Intelligent Optimized Edges for Secure Multimedia Communication

Raniyah Wazirali and Zenon Chaczko
Faculty of Engineering and Information Technology (FEIT)
University of Technology, Sydney (UTS)
Australia, NSW, Sydney
Raniyah.wazirali@gmail.com

Abstract—Recently, image steganography has received a lot of attention as it enables for secure multimedia communication. Payload capacity and stego image imperceptibility are a critical factors of any steganographic technique. In order to receive maximum embedding capacity with a minimum degradation of stego images, secret data should be embedded carefully in a specific regions. In this paper, data hiding is considered as an optimization problem related to achieving optimum embedding level of the cover image. Embedding data in edge area provide high imperceptibility. However, the embedding capacity of edge region is very limited. The work attempt to improve the edge based steganography by incorporates edge detection and vision science research. Genetic Algorithm that uses human visual system characteristics approach for data hiding is presented. Primarily, the approach applies Differences of Gaussian detector which closely resembles the human visual behavior. Secondly, the edge profusion indicates the level of threshold visibility with the help of Genetic Algorithm training. The suggested solution uses Contrast Sensitivity Function (CSF) which produces the edges based on the size of the embedding information. The authors of this paper compared their technique with other classical and recent works. The quality of the steganography is measured based on various quality metrics such as PSNR, wPSNR, SSIM and UIQI. These metrics declare the stability between imperceptibility and large embedding capacity.

I. INTRODUCTION AND BACKGROUND

Large quantities of information are spread over public networks with a wide area of internet facilities which then give users an ease of accessibility of information. Some of this data contains secret information and involves a certain level of security. Cryptography is one of the most common method which is used for many years and it represents useful techniques for securing messages by transfer its content to an unreachable and unreadable format or text called “cipher text”. Thus only the authorized person will be able to extract the secret message by entering a key. On the other hand, cryptography also has some weaknesses as a result of the presence the cipher text. Therefore in the recent years, steganography has been of interest to many researchers as it involves hiding the existence of the secret information rather than hiding its content.

There are broadly two substantial features of steganography which are payload capacity and stego image quality, both act as trade off. When one wants to hide the delicate elements in his image which thereafter yields added relics to it and then extra distortion to photo, hence makes the quality of stego image to decline. Besides, it would be infeasible to rely upon increased system security and potential. Nevertheless, it straight away implies an inculcated trade off by the quantity of relics brought into carrier file; safeguard aligned with alteration in the stego image and embedded data quantity.

Most of spatial domain Approaches presume that the least significant bits of the cover image is insignificant. Thus, the Pseudo Random Number Generator (PRNG) is mostly utilized for selecting pixels targeting to embed data. The concept of LSB is not always accurate particularly for the kind of images that have higher proportion of smooth areas than sharp areas. These jagged edge areas have extra complex features in turn making it further complex to notice alterations in the areas of an image. Although edge based steganographic approaches provide high stego image imperceptibility, they have issued with low payload capacity as per inadequacy of the edge areas.

Therefore, the secret data needed to be embedded carefully in certain areas of the carrier file in consideration to its features. This is to attain high payload capacity and having least alteration in it. While the edge detection technique is simple as compared to the above, it offers the vigorous hiding approach to safeguard against threats of rapid and instant change in the image file. Wu and Tasi (2003) projected the aspect of pixel-value differencing (PVD) which pertain the size of embedding capacity by subtracting the value of two pair of pixels [20]. However the focal point of using PVD is to pop in the secret message to an image, supported by making use of differences between pixels couple values. The secret message is determined by difference of value and this value remains same after embedding data. The PVD approach groups the values of all differences in terms of grades. A high disparity value means a high grade and low value means low grade. It is certain that the high difference between two sequential pixels would be more feasible for embedding information in an image. If these two pixels attain a little difference, only little message is embedded since there is an even area and the quality of image can be corrupted. Next to this, Singh et al. (2010) anticipated an approach to hide secret data in digital colored picture [12]. This scheme altered some color values which took advantage of certain pixels to show characters and not the color value, hence facilitating the high quality of image stego file.

There are numerous steganographic approaches which can be measured as per human vision susceptibility and features.
of local texture[4], [20]. Half decade back, Chen had been utilizing hybrid edge detector which mingled fuzzy edge detection approach with that of canny edge [19]. The canny edge detection technique has been also taken up in further researches by which the edge areas are being taken then inserting embedded message via k LSBs [10], [21]. The approaches gives high imperceptibility[1] which relies upon edge detection’s 3x3 window with secret data embedded (used human vision component). It is observed that a technique produces diverse outcomes of cover file and secret message which uses factors: size of Gaussian mask, low threshold value and finally high threshold [21]. Wazirali had second-hand on score matrix using Genetic Algorithm so that we can get best plot linking carrier file and secret data[18]. Then in 2015, it was invention of hyper edge detector using the features of gradient, 9x9 mask of Laplacian of Gaussian (LOG) and zero crossing with clustering, exhibiting effective edge detector so as to categorize a picture to edge as well as non-edge regions. The detection of edge regions would be having diverse quantity of secret message hidden in each cluster [17]. Thus, stego image imperceptibility and high payload capacity equilibrium would be attained by it.

As to acquire best embedding level with minimum alteration, there should be supposition of optimizing the steganography problem. The likely optimized search processes are Genetic Algorithm (GA). This means that GA is linked with natural collection and genetics. Therefore, GA is taken from concept of evolution of biological practice. The process of GA includes to develop a group of pupils answers for the required problems, then develop these repeatedly via use of stochastic operators. A role of fitness is crafted to evaluate each pupil answer. The fitted answers have high supposition to produce offspring. The number of cycles would execute till the time best resolution/answer or predefined set is evaluated.

In this paper, a novel edge based steganographic approach is projected to expand the capacity of steganography relied upon edge with least modification in stego file. This is foundation of new edge visibility, Contrast Sensitivity Function (CSF) and Genetic Algorithm (GA) usage. This scheme second hands the difference of Gaussians (DoG) detectors which just impersonates the performance of human visual system. The adaptation to the perceptibility of gratings gave similar outcome of this approach as of CSF. The edge emplacement is calculated by measuring the total zero crossing of DoG, which is more close to HVS [7], [15], than Laplacian of Gaussians (LoG). [9]. An improved framework can be achieved by the copying of perceptibility of edge from the DoG which directs to consolidated the framework. Supplementary, the usage of both CSF and GA facilitated the optimization of embedding capacity via developing the irregular edge visibility depending upon size of secret data.

The organization of this paper as follow; section two describes the proposed method. Then, section three shows the experimental results include imperceptibility evaluation, capacity evaluation and detectability evaluation.

II. PROPOSED SCHEME

The proposed technique presented in this paper reveals the perception of hiding data in intelligent edge visibility level using HVS characteristics in term of Contrast Sensitivity Function (CSF) and Genetic Algorithm (GA). The work combines edge detection and vision science research. Firstly, it is used Differences of Gaussian detector instead of Laplacian of Gaussian which is more closer to the human visual behavior. Secondly, the edge profusion indicates the threshold visibility with the help of Genetic Algorithm training in significance of HVS utilizing (CSF) which is produce the edges based on the size of the embedding information.

For a cover image C, GA produces a candidate solution to hide the secret message. A candidate expression principally recovers the optimized options for each selected coefficient. Fitness function is used to measure the performance of each candidate expression. It is based on measuring the imperceptibility and providing optimized high payload capacity at lowest distortion.

During GA training, the best individuals are maintained to engage in the operation of materialization. However, the weak individuals are excluded. Materialization are generated prospectively employing GA’s processes which are select the individuals, mutation and crossover. The operation move ahead repeatedly until stopping criteria achieved. The finest individual of the last generation is protected which will consequently be used for embedding secret data in the images. GA operations essentially precedes the threshold of edge visibility Th which indicate embedding rate for each region of the cover image based on the size of the secret message. Figure 1 shows the embedding process of the proposed method. The cover image C is split into non-overlapping sub-blocks and then the model detect the edges of the object using DoG filters in order to inaugurate the vision of CSF utilizing GA operator to produce the most proper edges. The GA determines the proper embedding rate threshold using the visibility of SDS(C) for each block based on the fitness function. The following sections will describe the theoretical concept of the proposed scheme.

A. Contrast Sensitivity Function

The CSF describes the observing trend of humans to the visibility of sine gratings. In fact, this is great instrument whereby a picture can be crack into rasing using Fourier decomposition in the linear systems. Thereafter, illustration schemes act as a linear schemes as when the fluorescence version is set. As a result, the sensitivity to square rasing is guessed via the sensitivity to sine gratings [7].

Mannos and Sakrisson [8] had anticipated a logical and eminent form of the CSF to the field of computer. Subsequently, it was the turn of Barten [3] who united accessible psycho-visual information to carry out the absolute model of CSF which is most up-to-date. Below is the employed Barten’s CSF:

\[
CSF(f) = a f e^{-b f} \sqrt{1 + e^{bf}}
\]
where \( f \) denotes frequency in cycle per degree, \( c = 0.06, b = 0.3(1 + 100/L)^{0.15} \), furthermore
\[ a = \frac{540(1 + 0.7/L)^{-0.2}}{1 + \frac{12}{(1 + f/3)^{-2}}} \]  

(B. 1.2 The Detection of Edges)

Difference of Gaussians (DoG) is one of the logical models which was anticipated in vision science in the approachable area of X- cubicles in the Lateral Geniculate Nucleus (LGN)\cite{7}, \cite{15}. We deployed the CSF in band pass filters within frequency domain, basically called weighted sum of DoG (or SDoG). Thereby making DoG as the creator of transmission capacity of the CSF-taking the illustration scheme as a multistage analyzer, and ON/OFF cubicles along with sympathetic sphere of a required mass \cite{7}. The equation referring slanted computation of DoG has been represented below:

\[ \text{SDoG}(C) = \sum_k T_h (G_{\sigma^+} - G_{\sigma^-})(C) \]  

Here \( C \) is taken as the cover picture (in luminance units), \( G_{\sigma} \) as the standardized Gaussian function, Standard Deviation (SD) \( \sigma, \sigma^+ \) and \( \sigma^- \) are the SD of the optimistic and pessimistic elements of a DoG (\( \sigma^- = \lambda \sigma^+ \)), and \( T_h \) is taken as embedding threshold wherein the illustration is in next part.

A DoG is not viewed as a subsequent derived but it achieves the ends revealing is with the same superiority as with \( \nabla^2 G \) expressed in the forms of localization and factors of the optimistic and pessimistic masses are to be identical as per equation 3.

(C. Optimized Edges Using Genetic Algorithm)

After obtaining the image with edges from previous subsection, evolutionary training will begin to optimized the edges based on the size of embedding data. Figure 3 illustrates the diagram of edge training flowchart.

In GA training system, chromosome is performed by a list of 64 \times 64 bit string. The initial chromosomes are generated randomly from the previous step (SDoG). The chromosome value can be either zero or one where zero express non edge pixel and one indicates an edge pixel. The chromosome of pixel \( P(x,y) \) can be generated as follow

\[ \text{Chromosome}(x,y) = E_1 \times \text{Integer}(P(x,y) + E_2) \]  

where \( E_1 \) is a random integer to be either 0 or 1 and \( E_2 \) is a random number range between 0 to 0.99

Many factors should be consider during GA training for optimum data embedding which include maximum fitness function \( wPSNR \), diversity of edges \( C_d \), thickness of edges \( C_t \), fragmentation of edge \( C_f \) and the total number of edge pixel \( C_e \).

where

Function of Fitness: Herein, we take weighted Peak Signal to Noise Ratio \( wPSNR \) as function of fitness and \( wPSNR \) considers entire HVS properties pertaining by the theory of less sensitivity of human eye modifies the texture areas rather than smooth areas. Besides, \( wPSNR \) is taken as an alternative quality metric which is developed by Voloshynovskiy et al., it is relied upon the calculation of Noise Visibility
Function (NVF) as a correction factor. It is constituted as
the picture property found on textured as well as edge area
since embedding information of this area could conceal extra
information efficiently and will have less distortion [14].
NVF is approximately 1 whereas for the edge areas, it is
approximately 0, which reflects that for smooth area. wPSNR
takes out extra good and true results than PSNR relatively the
methods that are edge detection schemes.

\[
\text{wPSNR} = 10 \log_{10} \frac{\text{MAX}^2}{||(C_{ij} - S_{ij})||^2_{\text{NVF}}}
\]

\[
wPSNR = 10 \log_{10} \frac{\text{MAX}^2}{||(C_{ij} - S_{ij}) \cdot \text{NVF}||^2}
\]

\[
\text{NVF}(i, j) = \frac{1}{1 + \theta \sigma^2_x(i, j)}
\]

Where \(\sigma^2_x(i, j)\) represents the limited alteration of the picture
in a windowpane dashed on the pixel with parameters \((i, j)\)
and \(\theta\) is a variation factor dependable to the precise image
which can be computed in equation 6 and 7.

\[
\tau(i, j) = \frac{1}{(2L + 1)^2} \sum_{k=-L}^{L} \sum_{l=-L}^{L} x(i + k, j + L)
\]

\[
\sigma^2_x(i, j) = \frac{1}{(2L + 1)^2} \sum_{k=-L}^{L} \sum_{l=-L}^{L} (x(i + k, j + L))^2
\]

The image based on alteration factors is specified as \(\theta = \frac{\text{D}}{\sigma^2_{\text{max}}}\). Where \(\sigma^2_{\text{max}}\) is the highest local variance for a fastidious
image and \(D \in [50, 100]\) is a calculated value.

Diversity of region \(C_d\)

\[
C_d = \begin{cases} 
0 & \text{if } p \text{ is an edge pixel} \\
D(p) & \text{otherwise}
\end{cases}
\]

Thickness of edges \(C_t\)

\[
C_t = \begin{cases} 
0 & \text{if } p \text{ is a thin edge pixel} \\
1 & \text{otherwise}
\end{cases}
\]

Fragmentation of edge \(C_f\)

\[
C_f = \begin{cases} 
1 & \text{if more than one neighboring edge pixel} \\
0.5 & \text{if only one neighboring edge pixel} \\
0 & \text{if no neighboring edge pixel}
\end{cases}
\]

Total number of edge pixels \(C_e\)

\[
C_e = \begin{cases} 
1 & \text{if more than 2 edge pixels} \\
0.5 & \text{if only one edge pixel} \\
0 & \text{if no edge pixel}
\end{cases}
\]

D. Data Embedding

Embedding secret message will depend upon the texture
of the cover image. Figure 4 illustrates the decision tree for
embedding evaluation which mainly examine the pixel whether
it place in edge and non-edge region. Follow by evaluate the neighbor pixel, the number of the edge pixels and the thickness of the edge. Various amount of data will be embedded based on the feature of pixel.

Non-edge pixel will hide less amount of bits while edge pixels will hide more bits. Figure 5 indicates the bits replacement of pixels based on its position.

### III. EXPERIMENTAL RESULTS

For demonstration purposes, a graphical user interface simulation was built using Matlab R2014a. The algorithm was implemented with help of Genetic Programing Toolbox (GALAB). Comprehensive experiments have been conducted on a 400 dataset of RGB images, however, five images such as Lenna, Pepper, Baboon, Tiffany and, Airplane are referred to in this chapter for imperceptibility, capacity and detectability evaluation. They are all RGB images with size $512 \times 512$. All the secret files were hide successfully in cover images and produced stego files using the best evolved expression. In order to get best evolved expression, several GA simulation should be generated. The best expression will be generated based on achieving the fitness function. Imperceptibility, capacity and detectability will be evaluated below.
A. Imperceptibility Evaluation

In order to evaluate the imperceptibility of the stego image, subjective and objective test have been performed. The output of subjective test have been prove that the proposed method provide high quality stego image with minimum distortion with low and high embedding capacity. Figure 5 shows Lenna cover image with 5 different stego images at various embedding rate. Obviously, the resulted stego images are very close to the cover image with indicate high visual quality. Moreover, PSNR, wPSNR, SSIM and UQI have been used to objectively measure the quality of stego images. Table I, shows the result of the objective measurements for the proposed method. In addition, to prove the efficiency of the proposed method, we have compared the results of the proposed technique with others. LSB, PVD and Hyper Edge detection which has been developed by the authors are used for the comparison. It is clearly from tables I that the proposed method provide better imperceptibility even with high embedding capacity.

Fitness functions evaluate every possible solution. The solutions are selected randomly. Evolution starts from a set of random entities and it is repeated in other generations that will come after. Those considered more suitable, and not necessarily the best, are taken from each and every generation.

B. Capacity Evaluation

Steganographic limit is the vast majority of pieces that could be incorporated in a given secure information document with a negligible plausibility of distinguishing by an aggressor. Then again, the inserting limit is the majority of pieces that might be incorporated in a given secure information document. Along these lines, the inserting limit is prone to be greater than the steganographic limit [6]. Also, the measurement the undetectable data relative to the measurement the secure picture is known as implanting amount or limit [13]. Steganographic strategies, fundamentally utilized for key association, plan to enhance the steganographic limit and diminish the understanding of undetectable data in stego pictures [16]. [5] specified that "the more information you can conceal, the better the method". Then again, the steganographic limit has a tendency to be constrained by the measurement ensure information records [2], [11]. Along these lines, making a steganographic procedure ought to consider how to enhance the amount of
key information that might be imperceptible without affecting the characteristics of stego information documents.

Table II shows the embedding capacity with various threshold value. With the increase of the threshold value, the embedding capacity increased. Therefore, the model will choose the proper threshold based on the size of the secret message.

<table>
<thead>
<tr>
<th>Threshold</th>
<th>Embedding Capacity</th>
</tr>
</thead>
<tbody>
<tr>
<td>Lenna</td>
<td></td>
</tr>
<tr>
<td>2</td>
<td>573,587</td>
</tr>
<tr>
<td>5</td>
<td>758,954</td>
</tr>
<tr>
<td>9</td>
<td>985,587</td>
</tr>
<tr>
<td>13</td>
<td>1,089,587</td>
</tr>
<tr>
<td>Pepper</td>
<td></td>
</tr>
<tr>
<td>2</td>
<td>515,658</td>
</tr>
<tr>
<td>5</td>
<td>698,744</td>
</tr>
<tr>
<td>9</td>
<td>805,387</td>
</tr>
<tr>
<td>13</td>
<td>987,254</td>
</tr>
<tr>
<td>Baboon</td>
<td></td>
</tr>
<tr>
<td>2</td>
<td>577,548</td>
</tr>
<tr>
<td>5</td>
<td>748,584</td>
</tr>
<tr>
<td>9</td>
<td>975,587</td>
</tr>
<tr>
<td>13</td>
<td>1,087,954</td>
</tr>
<tr>
<td>Tiffany</td>
<td></td>
</tr>
<tr>
<td>2</td>
<td>548,255</td>
</tr>
<tr>
<td>5</td>
<td>715,845</td>
</tr>
<tr>
<td>9</td>
<td>948,398</td>
</tr>
<tr>
<td>13</td>
<td>1,025,733</td>
</tr>
<tr>
<td>Airplane</td>
<td></td>
</tr>
<tr>
<td>2</td>
<td>537,652</td>
</tr>
<tr>
<td>5</td>
<td>753,691</td>
</tr>
<tr>
<td>9</td>
<td>982,364</td>
</tr>
<tr>
<td>13</td>
<td>1,057,286</td>
</tr>
</tbody>
</table>

Table II: Various Threshold Vs Embedding Capacity

IV. CONCLUSIONS

For secure multimedia communication, an effective techniques are required. Image steganography has become increas-
ingly complex and the tradeoffs between high imperceptibility and large capacity face many challenges. Many researchers attempt to use edge regions to embed the secret message as the human visual system less sensitive to modification in edge regions. However, the payload capacity of these edge based steganography is very limited. In this paper, we developed a new idea of optimizing the embedding region in edge area using the characteristic of human visual system and Genetic Algorithm. The work uses background of edge detection and vision science research. A balanced substitute between security of edge detection based embedding and payload capacity of standard LSB can be achieved on the work based on a non-uniform data distribution algorithm with small computational requirements and improved data carrying surface. It is also worth adding non-linear data distribution to secure and provide reasonable resistance to statistical detection of hidden data. The experimental results indicate that not only high imperceptibility could achieve by this proposed method also makes certain high embedding rate.

REFERENCES


