A Hybrid Curvelet Transform and Genetic Algorithm for Image Steganography

Heba Mostafa Mohamed  
Information System  
Faculty of Computer and Informatics  
Suez Canal University  
Ismailia, Egypt

Ahmed Fouad Ali  
Computer Science  
Faculty of Computer and Informatics  
Suez Canal University  
Ismailia, Egypt

Ghada Sami Altaweel  
Computer Science  
Faculty of Computer and Informatics  
Suez Canal University  
Ismailia, Egypt

Abstract—In this paper, we present a new hybrid image steganography algorithm by combining two famous techniques which are curvelet transform and genetic algorithm GA. The proposed algorithm is called Hybrid Curvelet Transform and Genetic Algorithm for image steganography (HCTGA). Curvelet transform is a multiscale geometric analysis tool, its main advantage is that it can solve the important problems efficiently and other transforms are not that ideal. Genetic algorithm is a famous optimization algorithm with the aim of finding the best solutions to a given computational problem that maximizes or minimizes a particular function. In the proposed algorithm the cover and secret images are passed through a preprocessing process by applying four different filters to them in order to remove the noise and achieve a better quality to both images before the hiding process. Then the curvelet transform is applied to the cover image to find the curvelet frequencies of the image, and the secret image is hided at the Least Significant Bits (LSB) of the curvelet frequencies of the cover image to reconstruct the stego image. Finally genetic algorithm operations are employed to find different scenarios for the hiding process by rearranging the hiding bits and finally choose the best scenario that can reach a better image quality and a higher Peak Signal to Noise Ratio (PSNR) results.

Keywords—Image steganography; curvelet transform; least significant bits; genetic algorithm; Peak Signal to Noise Ratio (PSNR)

I. INTRODUCTION

Because of the continuous progress in the communication technologies, it becomes necessary to protect the important information sending through any communication facility especially the internet. So, image steganography which is the art of concealing vital data inside a cover which can be image, video or audio, becomes one of the most important fields.

There are many steganographic techniques that are used and developed through times. For example, substitution technique by least significant bits LSB [1], which is the simplest data hiding technique, it works by changing the least significant bits of the cover image by the secret information. This technique is simple and effective and it doesn’t influence the quality of the images, however it is good at resisting the steganalysis attacks when it is used alone.

Transform domain technique which consists of different transforms such as: Discrete Cosine Transform (DCT) and Discrete wavelet transform (DWT). In DCT [2], the cover medium is usually converted to its frequency domain and secret data is hided into the cover image frequencies without causing any significant changes in the cover image.

Discrete wavelet transforms DWT, is the most famous technique in the steganography field. Wavelet has been the most important technique used in this field, because of its ability to hide the secret images without affecting the quality of the image and because of its robustness against many steganalysis attacks, it works by converting the domains from spatial to frequency domains and it can be used in steganography by isolating the high frequencies from the low frequencies on each pixel, so the image is decomposed into two bands, these bands are detailed and approximation bands which referred to as the sub-bands [3]. Detailed band is the band that contains the high frequency components of images in which the insignificant features of the image exists. Approximation band contains the low frequency components; it contains all the significant features of the image. The important information that defines the image usually exists in the approximation band. So in image steganography, the secret information is usually hided in the detailed band.

Wavelet transform is the best in capturing zero-order singularities which called point singularities of the image and it cannot deal with the features along edges [4]. Since there are images with higher order singularities, wavelet transform won't have points of interest in such manner. To defeat the shortcoming of wavelet transform in the high dimensions, and to deals with curves better, Candes and Donoho proposed curvelet transform [5].

Spread spectrum technique [6], in which the secret information is distributed over a wide frequency bandwidth. Hence, it is very difficult to completely remove the message without destroying the cover image.

In statistical technique [6], the secret messages are encoded by the change of some numerical properties of the cover image.

Distortion technique [6], in this method the secret messages are stored by the distortion of signals. The sender usually makes a specific change to the cover image and the receiver recovers the secret information by recording the differences between the original and the stego images.

In this paper, we propose a novel image steganography algorithm that merges least significant bit and curvelet
transform to hide the secret messages in the curvelet frequencies of the cover image for a better image quality, and we employ the genetic algorithm technique, to choose the best embedding plan.

The paper is organized as follows: In Section 2; we give a brief description of the related work done on the steganography area. In Section 3, we highlight the principles of the curvelet transform and its implementation techniques. In Section 4, we explain how the genetic algorithm works and we give a brief description of its famous operations. Section 5 contains a detailed description of our proposed algorithm which called Hybrid Curvelet Transform and Genetic Algorithm for image steganography (HCTGA). In Section 6, 50 cover and secret images are tested and analyzed by the new algorithm and the numerical results of the experiments are recorded, then a comparison between our proposed algorithm and other famous techniques is done. Finally, a brief summary and conclusion is given.

II. RELATED WORK

In 2007, Yuan-Yu Tsai and Chung-Ming Wang [7] have applied a data hiding criteria for color images by using the Binary Space Partitioning (BSP tree). It results in high capacity steganography system with low visual distortion. They found that using the tree can enhance the security, making it troublesome for any unapproved user to extract the secret messages without the known of the secret key.

In 2008, L.Y. Por, W.K. Lai, Z. Alireza, T.F.Ang, M.T.Su and B.Delina, [8] have integrated three LSB insertion algorithms in one steganography system. The unauthorized users can’t detect the secret data during a communication because this method implements a public key infrastructure that is only the sender and the receiver can know it.

In 2008, M. A. Bani Younes and A. Jantan [9] introduced a steganography technique that depends on hiding secret data inside an encrypted image by using the LSB insertion. In this approach, they randomly overwrite the LSB of the encrypted image by the binary representation of the secret data. The receiver can easily extract the secret data by applying the inverse of the transformation and encryption processes to the stego image.

In 2008, Chang-Chu Chen and Chin-Chen Chang [10] have introduced a steganography method that modifies the regular steganography based LSB method by the use of reflected gray code rule. In this method, the hiding criteria and the distortion level are similar to the simple LSB method, but the two methods differs in the change of the secret bits before and after embedding; the LSB substitution keeps them equally, unlike this method where the stego and the secret images are not always the same.

In 2009, Babita Ahuja and Manpreet Kaur [11] have proposed a steganography technique using LSB method with the aim of providing high capacity for the hiding process. In this technique four least significant bits are replaced by the secret data, and a filtering criterion and two level high securities are employed to remove the distortions that can cause suspicions.

In 2010, Ekta Walia, Payal Jain and Navdeep [12] have analyzed two different schemes of steganography the least significant bit (LSB) and the discrete cosine transform (DCT), and they compared the two methods and found that steganography by using DCT method is better than steganography by using LSB, because the DCT method provides a better image quality with little image distortion as compared to LSB. Although LSB can hide a big amount of secret data way more than the amount of secret information that can be hidden using DCT technique.

In 2011, E. Ghasemi, J. Shanbehzadeh and N. Fassihi [13] have applied the wavelets and genetics based mapping function in a new steganographic technique. The frequency domain where the secret message is embedded improves the robustness of the steganography process and genetic algorithm is used to acquire the best mapping function that reduces the errors between the cover and the reproduced images, to enhance the capacity of the hiding process.

In 2012, M. R. Garg and M. T. Gulati [1] focuses on applying steganography by using two methods, Least Significant Bit (LSB) and Most Significant Bit (MSB), and they compared the two methods and found that LSB based steganography is much better than MSB based steganography for hiding the message.

In 2015, D. Babya, J. Thomasa, G. Augustine, E. Georgea and N.R. Michaela [14] have employed the discrete wavelet transform DWT to create a new steganography method, in which the cover is divided into three planes R, G and B planes and the secret messages are inserted into the frequency domain of these planes. They found that the resulted image has high general security and a less recognizable distortion when compared to the original cover image.

In 2015, Z. Yin and B. Luo [15] have proposed a large capacity steganography technique in light of two methods, the pixel pair matching and the modification direction exploitation (MDE). They modified the cover pixel pair implying one or two 9-ary digits as indicated by various payloads. Experimental results of this method show high embedding capacity in addition to great quality and security.

In 2016, M. Saidi, H. Hermassi, R. Rhouma and S. Belghith [16] have introduced a steganography technique depending on chaotic map in DCT domain. In this method the DCT is applied on the original image, the coefficients is scanned in a zigzag order from the least to the most significant bits, as a result of this scan, the embedding positions are determined by the chaotic function in addition to the maximum allowed payload. The results of the experiments demonstrate that this algorithm gives a great imperceptibility and flexibility.

III. CURVELET TRANSFORM

Curvelet transform is a multiscale geometric analysis tool most appropriate for objects with curves. Candes and Donoho created this transform [5] with a goal of representing edges along curves more efficient than the traditional transformations. It differs from other transforms in that aside from location and scale, orientation decomposition is likewise applied for the signals; along these lines the coefficients acquired by the

www.ijacsa.thesai.org
curvelet show location, scale and angle data of the image features [4].

Curvelet transform is the best in representing the curves in images because it takes image edges as the essential representation elements [4]. The experiments of many researchers proved that the curvelet’s small scale coefficients can beat the wavelet’s high frequency coefficients, because of the orientation sensitive property of the curvelet coefficients.

Curvelet transform can be applied by two methods [17]:

Using Wrapping method.

Using Fast Fourier Transformation algorithm (FFT).

The two implementations of curvelet basically differ by the spatial grid choice that is utilized to interpret curvelet coefficients at every angle and scale. Both ways give back a table of digital curvelet coefficients listed by spatial location, orientation and scale parameters [17].

In this paper, we used the second method to apply the curvelet, cover image is transformed using the Fast Fourier Transformation algorithm and the secret message was embedded with that transformed image. Then the inverse FFT is applied to propose the stego image.

We choose FFT algorithm because it is very effective and very easy to study its function as it can be expressed as a sum of series of sine and cosines.

The benefits of using FFT algorithm can be listed and summarized as follows [17]:

- Elements of digital contents can be used directly and the secret data can be embedded in them directly.
- Elements that changes over time should be transformed into the frequency domain before the embedding process, this makes processing easier.
- The changes of the quality of digital content before and after embedding are minimized.
- Processing required for steganography and detection is simple.
- The secret information embedded in digital content can be detected as required.

IV. GENETIC ALGORITHM

Genetic Algorithm is a famous optimization algorithm proposed by John Holland in 1975 [18]. Its fundamental goal is to discover the optimal solutions of a given computational problem that maximizes or minimizes a particular function. Genetic algorithm based steganography developed to generate several stego images or several solutions by inserting the secret message in different blocks of the cover and choose the order that leads to the best PSNR value.

The steps of the GA process are listed below and summarized in Fig. 1:

1) Define the initial population with a specific number of individuals.

2) Produce the next generations by applying the GA operations such as crossover and mutation.

3) Select the best solutions by using the fitness function and repeat Step 2 to produce better solutions, and continue until the best solution is reached.

Fig. 1. Genetic algorithm process.

So, the main process of GA can be described as follows:

The initial population, selection process, crossover operation, mutation operation and fitness function.

A. Initial Population

The basic term of the GA process is the chromosome which is the numerical value that represents an individual or a candidate solution to the problem. Chromosomes consist of discrete units referred to as genes. Every gene represents the chromosome features.

A group of chromosomes is referred to as a population. GA usually begins with a randomly chosen arrangement of chromosomes, which serves as the initial population.

B. Selection Process

In this process, two chromosomes are selected to produce two new offsprings. Generally, the fitness function of every individual decides the likelihood of its existence in the next generations. There exist many distinctive selection strategies in genetics, for example, tournament selection, ranking, and proportional selection.

C. Crossover Operation

This operation is the most vital operation in genetic algorithm. In this operation, usually two parent chromosomes are consolidated together and produce new chromosomes, referred to as offsprings. This is can be done by swapping the genes of the chosen parents to produce new solutions as shown in Fig. 2.

The parents are usually selected among other chromosomes according to their fitness value so that the produced offsprings are required to acquire the great genes that can make better generations.
D. Mutation Operation

Mutation operator works by making random changes to the attributes of the chromosome. It is usually applied to the gene level; it works by randomly flips individual bits in the new chromosomes.

The GA algorithm can get stuck at a local optimum before finding the global optimum. The mutation operator helps protect against this problem by maintaining diversity in the population, but it can also make the algorithm converge more slowly.

E. Fitness Function

This function is one of the most vital steps of the GA process as it determines how the chromosomes will change over time and it determines the direction that the population will take. Peak Signal to Noise Ratio (PSNR) is a famous fitness function that is utilized widely in the image processing field. It is generally used to analyze quality of the image by describing the similarity degree between images. When the PSNR function gives higher results, this is indicating a better quality for the resulted image.

V. PROPOSED ALGORITHM (HCTGA)

The proposed algorithm presents a new image steganography algorithm that combines three famous and effective techniques; which are the discrete curvelet transform, the least significant bit (LSB) [19] and uses the genetic algorithm to achieve a better image quality and security.

A. Input Images

The proposed algorithm uses two input images with size 512 x 512. One of them is referred to as the cover image into which the required secret messages are embedded. The other is referred to as the secret image that needs to be hidden inside the cover image; it is also called the payload.

We test our proposed algorithm on 30 cover and secret images.

B. Preprocessing Step

This step is very important step in any image processing technique; its main goal is to enhance the image data to get rid of the unwanted distortions or enhance the features that is important for the next operations.

In our method, a preprocessing technique is done by applying four famous filters to the cover and the stego images, these filters are gaussian, average, motion, unsharp, each filter plays a great role in removing the noise from images while keeping its features and enhancing the images quality before applying the steganography process.

C. Embedding Process

In this step, the steganography process which is the most important step in our algorithm is applied as follows:

First the cover is divided into 16 equally blocks, each block consists of 128 x 128 pixels.

Then the discrete curvelet transform DCT is performed into the cover image. The DCT can be performed by the steps shown in Fig. 3 as produced by J. Starck, E. Candes, and D. Donoho [20]:

1) Subband filtering

The cover is divided into three subbands P0, Δ1 and Δ2 (see Fig. 4).

![Fig. 2. Example of the crossover operator.](image1)

![Fig. 3. Curvelet decomposition.](image2)

![Fig. 4. Curvelet subbands.](image3)
2) **Tiling**

The subbands $\Delta 1$ and $\Delta 2$ are tiled to make the curved edges become linear singular, so that the Ridgelet transform can handle it well. Fig. 5 illustrates the tiling process.

![Tiling Illustration](image)

**Fig. 5.** Smooth partitioning (tiling).

3) **Ridgelet transform**

Applying the Discrete Ridgelet transform is the final step of the process.

After applying the curvelet to the cover, the secret message should be embedded into the LSB of the curvelet subbands.

**D. Applying Genetic Algorithm GA**

The genetic algorithm is utilized to insert the secret image by different ways and scenarios and test the quality of the image at every scenario to choose the one that result in a better image quality. The cover image is divided into blocks and the secret data are embedded at a different arrangement of these blocks every time to create different embedding scenarios.

Two GA operators are used: Crossover and Mutation operators. We used the crossover operation to merge two scenarios together to create a new better one. The mutation operation is utilized to change some data when the resulted scenarios become similar to each other.

Finally, the stego image is generated by applying the Inverse Curvelet Transform on the modified coefficients.

To test the quality of the reconstructed image, PSNR is used as the GA fitness function. It works by computing the difference between the original image and the resulted stego image by applying the following equation:

$$PSNR = 20 \log_{10} \frac{255}{\sqrt{MSE}} \quad (1)$$

Where the MSE is the Mean Square Error that computes error difference between two images by the following equation:

$$MSE = \sum_{i=1}^{255} \sum_{j=1}^{255} \frac{(Cover(i,j) - Stego(i,j))^2}{255 \times 255} \quad (2)$$

The steps of our proposed algorithm are summarized in Algorithms 1 and 2 and Fig. 6.

![Proposed HCTGA Algorithm](image)

**Fig. 6.** Proposed HCTGA algorithm.

**Algorithm 1** The Embedding Algorithm of the Proposed HCTGA

- a. Get the cover image with size 512 x 512. (Input cover image)
- b. Apply the denoising technique. (Preprocessing operation)
- c. Divide the cover & secret images into 16 blocks.
- d. Rearrange the cover image blocks randomly.
- e. The curvelet transform is applied on the cover image.
- f. Embed the secret image by using LSB technique. (Hide secret image into cover image)
- g. Rearrange the cover image blocks to the original pattern.
- h. Apply the GA operations such as Crossover & Mutation, to generate a better stego images.
- i. Apply the fitness function (PSNR) that can measure the stego image quality.
- j. Choose the best stego image.
VI. EXPERIMENTAL RESULTS

A. Parameter Settings

There are three important parameters in the GA process, which are the population size, the crossover probability and the mutation probability. The values of these parameters are listed in Table 1.

B. General Performance of HCTGA

The performance of the proposed algorithm is shown in Fig. 7 and Table 2.

C. Comparison between HCTGA Algorithm and other Algorithms for Image Steganography

We compared the proposed HCTGA algorithm with three famous steganography techniques to test the efficiency of our algorithm. These methods are: the LSB, the wavelet transforms and the curvelet transform method without using genetic algorithm.

1) LSB
Least significant bit (LSB) is a spatial domain technique; it is usually used for steganography for hiding the secret messages by replacing the cover's least significant bits by the secret image bits. This technique makes steganography very easy mission to accomplish, it is fast, effective, enables high capacity embedding and the changes in the cover after steganography would be unnoticeable. The drawback of this technique is its weakness against attacks, but this is can be solved by using other image transformation with LSB.

2) Wavelet Transform
It is a frequency domain transform; steganography based wavelet transform was the most popular and frequently used technique over the last few years. It works by converting the cover from spatial to frequency domains, then hiding the secret message in the wavelet coefficients of this cover image [3].

Steganography based wavelets is very effective method, because it is resistent against the attacks unlike the LSB, and it provides a better capacity and robustness for the steganography process.

The drawback of wavelet transform is its representation of image edges and higher order singularities. To represent edges by wavelet transform, too many wavelet coefficients are needed to repeat edges at scale after scale in order to reconstruct the edges properly [4]. So it is not the best method for capturing higher order singularities for images. To overcome the shortage of wavelet transform in higher dimensions, and to represent the curves better, Candes and Donoho proposed curvelet transform [5].

3) Curvelet Transform
The steganography based curvelet was described in Section 3.

<table>
<thead>
<tr>
<th>Test No.</th>
<th>MSE</th>
<th>PSNR</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>6.47</td>
<td>40.02</td>
</tr>
<tr>
<td>2</td>
<td>7.10</td>
<td>39.62</td>
</tr>
<tr>
<td>3</td>
<td>8.21</td>
<td>38.99</td>
</tr>
<tr>
<td>4</td>
<td>7.58</td>
<td>39.33</td>
</tr>
<tr>
<td>5</td>
<td>7.52</td>
<td>39.37</td>
</tr>
<tr>
<td>6</td>
<td>6.91</td>
<td>39.74</td>
</tr>
<tr>
<td>7</td>
<td>6.37</td>
<td>40.09</td>
</tr>
<tr>
<td>8</td>
<td>7.12</td>
<td>39.61</td>
</tr>
<tr>
<td>9</td>
<td>8.31</td>
<td>38.93</td>
</tr>
<tr>
<td>10</td>
<td>10.53</td>
<td>37.91</td>
</tr>
<tr>
<td>11</td>
<td>5.97</td>
<td>40.37</td>
</tr>
<tr>
<td>12</td>
<td>6.29</td>
<td>40.14</td>
</tr>
<tr>
<td>13</td>
<td>6.75</td>
<td>39.84</td>
</tr>
<tr>
<td>14</td>
<td>5.37</td>
<td>40.83</td>
</tr>
<tr>
<td>15</td>
<td>9.33</td>
<td>38.43</td>
</tr>
<tr>
<td>16</td>
<td>9.19</td>
<td>38.50</td>
</tr>
<tr>
<td>17</td>
<td>7.99</td>
<td>39.11</td>
</tr>
<tr>
<td>18</td>
<td>7.12</td>
<td>39.61</td>
</tr>
<tr>
<td>19</td>
<td>5.11</td>
<td>41.05</td>
</tr>
<tr>
<td>20</td>
<td>8.97</td>
<td>38.60</td>
</tr>
<tr>
<td>21</td>
<td>4.98</td>
<td>41.16</td>
</tr>
<tr>
<td>22</td>
<td>5.61</td>
<td>40.64</td>
</tr>
<tr>
<td>23</td>
<td>8.41</td>
<td>38.88</td>
</tr>
<tr>
<td>24</td>
<td>7.95</td>
<td>39.13</td>
</tr>
<tr>
<td>25</td>
<td>7.13</td>
<td>39.60</td>
</tr>
<tr>
<td>26</td>
<td>6.29</td>
<td>40.14</td>
</tr>
<tr>
<td>27</td>
<td>6.59</td>
<td>39.94</td>
</tr>
<tr>
<td>28</td>
<td>6.91</td>
<td>39.74</td>
</tr>
<tr>
<td>29</td>
<td>7.10</td>
<td>39.62</td>
</tr>
<tr>
<td>30</td>
<td>7.37</td>
<td>39.46</td>
</tr>
</tbody>
</table>

TABLE. I. GA PARAMETERS

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Pop Size</td>
<td>16</td>
</tr>
<tr>
<td>Probability of Crossover Pc</td>
<td>Pc = 1</td>
</tr>
<tr>
<td>Probability of Mutation Pm</td>
<td>Pm = 0.001</td>
</tr>
</tbody>
</table>

TABLE. II. PERFORMANCE OF THE PROPOSED ALGORITHM
We apply the four methods on 10 images and the PSNR values of the methods are calculated and recorded in Table 3 and Fig. 8. This comparison illustrates that the proposed HCTGA algorithm can obtain better image quality than the other compared methods.

TABLE III. COMPARISON BETWEEN LSB, WAVELET, CURVELET AND THE PROPOSED HCTGA ALGORITHM

<table>
<thead>
<tr>
<th>Test No.</th>
<th>LSB</th>
<th>Wavelet</th>
<th>Curvelet</th>
<th>HCTGA</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>29.12</td>
<td>31.32</td>
<td>40.01</td>
<td>40.02</td>
</tr>
<tr>
<td>2</td>
<td>28.57</td>
<td>30.07</td>
<td>37.13</td>
<td>39.62</td>
</tr>
<tr>
<td>3</td>
<td>21.01</td>
<td>29.49</td>
<td>37.24</td>
<td>38.99</td>
</tr>
<tr>
<td>4</td>
<td>28.10</td>
<td>32.18</td>
<td>38.44</td>
<td>39.33</td>
</tr>
<tr>
<td>5</td>
<td>20.39</td>
<td>30.21</td>
<td>39.31</td>
<td>39.37</td>
</tr>
<tr>
<td>6</td>
<td>19.34</td>
<td>21.11</td>
<td>38.93</td>
<td>39.74</td>
</tr>
<tr>
<td>7</td>
<td>21.81</td>
<td>25.98</td>
<td>39.22</td>
<td>40.09</td>
</tr>
<tr>
<td>8</td>
<td>21.52</td>
<td>25.65</td>
<td>38.67</td>
<td>39.61</td>
</tr>
<tr>
<td>9</td>
<td>29.31</td>
<td>27.28</td>
<td>38.81</td>
<td>38.93</td>
</tr>
<tr>
<td>10</td>
<td>23.89</td>
<td>33.41</td>
<td>37.17</td>
<td>37.91</td>
</tr>
</tbody>
</table>

Fig. 8. Comparison between LSB, Wavelet, Curvelet and the proposed HCTGA algorithm.

VII. CONCLUSION AND FUTURE WORK

A new hiding algorithm has been illustrated in this paper by using the curvelet transform and genetic algorithm. Some filters are applied to the cover image as a preprocessing technique to remove the noise and enhance the quality of the images. Discrete curvelet transform is applied to cover images and the secret messages had been embedded in the curvelet coefficients by using LSB technique. Finally the genetic algorithm had been used to choose the best embedding criteria which lead to a high performance and unsuspected stego images.

Our proposed HCTGA algorithm has been tested and analyzed over fifty cover and secret images to test the performance of the proposed method and the results were promising.

Applying other evolutionary optimization algorithms besides genetic algorithm, such as, Differential Evolution (DE), Scatter Search (SS), Tabu Search (TS), Neighborhood search (NS) and Simulates Annealing (SA), is the main idea of the future work.

REFERENCES


