A REVIEW OF ARTIFICIAL INTELLIGENCE TECHNIQUES IN IMAGE STEGANOGRAPHY DOMAIN

H. S. HANIZAN¹, ROSHIDI DIN²*, HAFIZA A. S.,¹ RUKHIYAH A.¹, NOOR MAIZATULSHIMA S.¹

¹Faculty of Computing and Tech. Science, KUPTM, Taman Shamelin Perkasa, 52100 Cheras Kuala Lumpur
²School of Computing, UUM CAS, Universiti Utara Malaysia, 06000 Sintok, Kedah, Malaysia
*Corresponding Author roshidi@uum.edu.my

Abstract

This paper reviews major work focusing on three main artificial intelligence techniques, which are neural network, genetic algorithm, and fuzzy logic. This review is based on the several general criterias, i.e. types of field, main goal, types of hidden-information, image domain, implementation stages, secret-key and localization of artificial intelligence techniques. Then, the summary of these reviews is discussed. The findings suggest that all these works should apply artificial intelligence techniques either during pre-processing, embedding or extracting stages or more than one of these stages. Therefore, the presence of artificial intelligence techniques with their diverse approaches and strengths can help researchers in future work to attain excellent quality of image information hiding that comprises both imperceptibility and robustness.

Keywords: Neural network, Genetic algorithm, Fuzzy logic.

1. Introduction

The increased sophistication and capability of computers and the Internet has resulted in the increased demand and the role of information security. As such, the use of technology of information hiding; a technology where information is hidden in other files and among the popular files are images, also increased [1]. Image information hiding has emerged as an exciting and important research field. Image steganography is a process which involves hiding information called a hidden-information in an appropriate cover-image and the output is carrier-image [2]
whereas watermarking is a process to place the hidden-information in images, music and software for copyright protection purposes [3]. The embedding and extracting are two main stages involved in the generic image information hiding model. These two stages are normally used to embed and extract a hidden-information in and from a cover-image. Consequently, a carrier-image from the embedding process is sent through public channel and normally together with a secret-key. The embedding and extracting stages in the generic image information hiding model has illustrated in Fig. 1. These two processes are used to embed and extract the hidden-information M respectively in and from a cover-image C together with a secret-key K. As a result, there is a carrier-image S called either stego-image in steganography or watermarked-image in watermarking. The extracting process will involve the reversion of the embedding algorithm.

![Fig. 1. The generic image information hiding model.](image)

There are three main goals that must be considered in designing an excellent quality of image information hiding namely imperceptibility, robustness and payload capacity. Imperceptibility is to preserve the details of the cover-image when the hidden-information is being embedded. Robustness is the ability of the carrier-image to uphold its' content from attacking (e.g. image manipulation such as rotating and cropping) while the payload capacity indicates the maximum number of bits that can be hidden with an acceptable resultant carrier-image quality [4-5]. Thus, a trade-off between these goals becomes one of the main issues and challenges in order to obtain an excellent quality of image information hiding [6]. Another critical challenge for image information hiding comes from steganalysis or watermark attacks. Up until now, there is a lot of techniques that have been developed in image information hiding to offset the offensive from steganalysis. Steganalysis is the art of detecting the hidden-information and the most popular steganalysis technique is statistical method (i.e. active or passive steganalysis) [7-9]. Thus, new techniques have been proposed to counter both challenges and among them are the techniques that exploit the advantages of artificial intelligence. Among the preferred and employed artificial intelligence techniques in image steganography and watermarking are neural network (NN), genetic algorithm (GA), and fuzzy logic (FL). The recent trend shows that the artificial intelligence technique is
not only applied in the embedding but also in the extracting stages. Some of the works even utilize the strength of artificial intelligence technique in the pre-processing stage as well. The pre-processing stage is a stage before the embedding process which an image is being prepared and classified.

There are few criteria used to review all the artificial intelligence techniques in image information hiding. Among the criteria used to review for each work are types of fields, the main goal, types of hidden-information, image domain, implementation stages, secret-key and localization. For each criterion, there are corresponding types to be further used and discussed in this article. Table 1 summarizes the review criteria and its’ corresponding types whereas the Symbol Representations shows symbols representing the criteria types.

<table>
<thead>
<tr>
<th>Criteria</th>
<th>Criteria type</th>
<th>Symbol representation</th>
</tr>
</thead>
<tbody>
<tr>
<td>Image Field (S/W)</td>
<td>Steganography/Watermarking</td>
<td>S/W</td>
</tr>
<tr>
<td>Goal</td>
<td>Robustness</td>
<td>R</td>
</tr>
<tr>
<td></td>
<td>Imperceptibility</td>
<td>I</td>
</tr>
<tr>
<td></td>
<td>Payload capacity</td>
<td>P</td>
</tr>
<tr>
<td>Types of Hidden Information</td>
<td>Text</td>
<td>T</td>
</tr>
<tr>
<td></td>
<td>Image</td>
<td>M</td>
</tr>
<tr>
<td>Image Domain</td>
<td>Spatial</td>
<td>S_p</td>
</tr>
<tr>
<td></td>
<td>Transform</td>
<td>T_r</td>
</tr>
<tr>
<td>Implementation Stage</td>
<td>Preprocessing</td>
<td>P_r</td>
</tr>
<tr>
<td></td>
<td>Embedding</td>
<td>E_m</td>
</tr>
<tr>
<td></td>
<td>Extracting</td>
<td>E_x</td>
</tr>
<tr>
<td>Secret Key</td>
<td>Yes/No</td>
<td>Y/N</td>
</tr>
<tr>
<td>Localization</td>
<td>Yes/No</td>
<td>Y/N</td>
</tr>
</tbody>
</table>

Symbol Representations show how the symbols represent the criteria types. Firstly, there are two types of image information hiding fields, either image steganography or watermarking. These two types of fields are selected because the image information hiding literature has shown that these two are major employed and interesting research fields of late [10-12]. Secondly, the main goal from each work is identified from each artificial intelligence technique employed; it is either robustness, imperceptibility or payload capacity. The main goal of each technique is determined based on the main aims of the author, types of artificial intelligence techniques applied and the way that experimental work is done. Next, there are two types of hidden-information that are identified, either text or image. Furthermore, the type of image domain is identified from each work that can either be applied in a spatial or transform domains making use of few types of images such as GIF, BMP or JPEG, to name a few.

2. Review on Artificial Intelligence Techniques
In this section, artificial intelligence works in image steganography will be presented.
2.1. Neural network

Neural network (NN) technique has been applied in image information hiding since 2003 when Lou [13] introduced NN to enhance the embedding process in his technique called an adaptive digital watermarking.

Fig. 2. Summary NN techniques in image steganography.

Since then, more NN techniques have been actively developed and utilized in both fields in steganography and watermarking as shown in Fig. 2. All of the works that involve NN focus on the robustness as the main goal and most of them use the back-propagation algorithm (BP) for embedding and some even apply it in extracting process [14-21]. Watermarking is preferably used to transform domain images unlike steganography that uses both. Vertally, in watermarking, applying BP together with transform domain images can improve the rate of learning and reduce the error [20]. The most common transforms applied to images in NN is Discrete Cosine Transform (DCT). Watermarking also seems to work well with the image rather than text as hidden-information. Unlike others, Kavita [14], Zhou [17] and Naoe [18], mentioned that improving the technique performance by applying NN is not only in the embedding but also in extracting processes. Furthermore, in increasing the robustness of the carrier-image, the secret-key is applied in almost all work. In relation to that, the localization is also applied to utilize the human visual system (HVS), for example, started with Lou [15] that utilizes four properties of HVS model i.e. entropy, frequency, luminance, and texture sensitivity to obtain the local characteristics of an image. Huang [19] localizes the embedding positions by considering the texture and edge areas as a hidden-information and selected cover-images from an image database. As summary, NN is good on generalization capabilities. However, the major problem with NN is to determine the appropriate number of layers and number of neurons.
2.2. Genetic algorithm

The major work, genetic algorithm (GA), is mostly employed to increase the payload capacity and exploited in steganography field [22-30] as illustrated in Fig. 3. A popular technique with three basic operations of selection, cross over and mutation was first introduced by Fard in 2006. Then, Ji introduced an optimal block mapping LSB method based on GA in looking for more suitable embedding positions between cover-image and hidden-information image blocks [22] while Chang [23] attempted to increase the payload capacity by using two-level of quantization values in which three additional bits could be hidden in a bitmap if it is a non-smooth block. Subsequently, he enhanced his work in [24] by using common bitmap generation procedure to not only increase the payload but also speed up the hiding process. Meanwhile, Yu came up with a technique called blockiness strategy [27] while Maity [28] introduced an optimal set of points using GA in order to increase the payload capacity. Later, in the year 2012, Ghasami [26] employed a GA based mapping function to embed data in discrete wavelet transform coefficients using 4 X 4 blocks. Akin to NN, there is a number of work that utilized GA technique in both embedding and extracting processes and all in the spatial domain [22-25]. Localization approach has been done here through a few work such as in [27] applying the genetic algorithmic operators to find the best combination of hidden-information and carrier-image to be used. Meanwhile, Chang has first determined the smooth and the non-smooth blocks and also quantization values to find the best substitution [24]. On the other hand, Yu moved with minimizing blockiness to preserve and localize the image characteristics [30]. As summary, GA technique is good on finding the best embedding position in image steganography and watermarking. However, the major problem with GA technique is relatively poor in finding the precise local optima solution in the region in which the algorithm converges and very slow in term of search speed in any image.

![Fig. 3. Summary GA techniques in image steganography.](image-url)
2.3. Fuzzy logic

Fig. 4 summarizes the work done on applications of FL in image steganography. Almost Fuzzy logic (FL) techniques attempt to preserve the imperceptibility of the cover-image and apply in watermarking except for Li [31] who did it in steganography where the main goal is robustness. Fuzzy approaches have been implemented in various ways, for example, Nobuhara [32] who introduced the fuzzy relational equation (ICF) where it treats an original gray scale image as a fuzzy relation by normalizing the intensity range of each pixel into [0, 1] and then the hidden-information is embedded based on least significant bit modification (LSBM) of a pixel of the compressed image. Then Comuo [33] employed FL to treat the texture and contrast features for embedding such that it is undetectable to the HVS because the imperceptibility is closely related to the HVS characteristics. Meanwhile Lou [34] also used FL but for this time the brightness and frequency features were selected and utilized. Li [31] used the fuzzy classification rules and defined according to the HVS characteristics.

Meanwhile, Kiani [36] introduced fuzzy c-means (FCM) clustering in his work to address the embedded bits by classifying the cover-image in transforming domain into four classes based on vertical and horizontal derivatives. His attempt was fruitful to conserve the unnoticeability of hidden-information compared to Li. Unlike stated in [33], Khursheed et al. [36] had transformed the cover-image and hidden-information into fuzzy domain for the embedding. The embedding is then performed based on the pre-determined threshold value and the membership’s difference value of the cover-image and hidden-information. Oueslati [38] used different textural and luminance features in fuzzy inference system to exploit the advantage of HVS in gaining the adaptive embedding algorithms. Likewise, Lande [39] utilized texture sensitivity in order to serve the same purpose. Almost all fuzzy works embed hidden-information in transform domain except Nobuhara [32] and Cuomou [33] in spatial domain. Meanwhile, there are four works that utilize fuzzy
in both embedding and extracting stages. Only Li [29] and Lande [36] were having pre-processing stage, while secret-key is not much used in FL technique and preferred only by Kiani [36] and Oueslati [37]. Comuo et al. in [33] applied the localization approach when first determining the amount of adjustment applied to the pixels based on the surrounding pixel element intensity characteristics whether it is a dark or bright area. The localization approach has been applied in [36] too when using the local search strategy where the consideration was made based on the values of horizontal and vertical of domain blocks before the hidden-bits were embedded. Another attempt was conducted by Zhou to consider the pixel values rather than the blocks of an image in order to localize the pixel selection and substitution [35]. As summary, FL technique is good on preserving the imperceptibility of the cover-image. However, one of the major problem with FL technique is that as the system complexity increases, it becomes more challenging to determine the correct set of rules to describe the watermarking and steganography system behaviour.

3. Preferred Criteria in Image Steganography

The preferred criteria are classified according to image information hiding fields, i.e. steganography or watermarking and in form of percentages. Among the criteria to be observed is the goal, the hidden-information, image domain, stages, secret-key and localization. The percentage values obtained are based on the 39-artificial intelligence works where 17 out of the total are steganography and the remaining is watermarking.

Table 2. Percentage use of each criterion for steganography and watermarking.

<table>
<thead>
<tr>
<th>Information Hiding Field</th>
<th>Goal R</th>
<th>I</th>
<th>P</th>
<th>M</th>
<th>T</th>
<th>Image Domain Sp</th>
<th>Tr</th>
<th>Stages Pre</th>
<th>Em</th>
<th>Ex</th>
<th>Secret-Key Location</th>
<th>Localization</th>
</tr>
</thead>
<tbody>
<tr>
<td>Steganography</td>
<td>53.3</td>
<td>13.3</td>
<td>33.3</td>
<td>52.9</td>
<td>47.1</td>
<td>64.7</td>
<td>35.3</td>
<td>10.3</td>
<td>58.6</td>
<td>31.0</td>
<td>64.7</td>
<td>70.6</td>
</tr>
<tr>
<td>Watermarking</td>
<td>41.7</td>
<td>58.3</td>
<td>0.0</td>
<td>77.3</td>
<td>22.7</td>
<td>22.7</td>
<td>77.3</td>
<td>18.9</td>
<td>56.8</td>
<td>24.3</td>
<td>50.0</td>
<td>63.6</td>
</tr>
</tbody>
</table>

Based on Table 2, robustness and payload capacity were the main goals in information hiding for steganography criterion with each 53.3% and 33.3%. On the other hand, with watermarking, the main goals were imperceptibility (58.3%) and robustness (41.7%) whereas payload capacity in watermarking was not used at all in any research using artificial intelligence technique at that time. As for the image domain, even though spatial domain is used in 2000 until 2005, there were evidences of reducing the usage of it and transform domain were used more in the middle of 2006 until now. This can be seen with the increase in percentage of the usage for watermarking with 77.3% and 35.3% for steganography. The type of hidden-information that was used frequently in watermarking was images with 77.3%. As for usage of images and text were almost the same in steganography, they value 52.9% and 47.1% respectively. For artificial intelligence technique application in stages, it showed both criterion, steganography and watermarking in which both are applied mostly in embedding stage, with the usage more than 50% and some of it used in extracting stage. What is fascinating is that the usage of artificial intelligence technique in pre-processing stage increased particularly in...
these recent years, based on Table 2 that shows the percentage of usage in this stage is 10.3% for steganography while for watermarking is 18.9%. If we take a look at localization, it shows that it has its place that is applied in most of the artificial intelligence work; more than 60% in terms of usage, in steganography alone is 70.6% and 63.6% in watermarking. Similarly, the use of secret-key that was widely used for the purpose of adding data security in which 64.7% was applied in steganography and 50% in watermarking. Hence, it can be concluded that, robustness and imperceptibility goals are attracting more attention and priority research in both steganography and watermarking when the criteria of transform domain, secret-key and localization were widely considered and applied in most of the artificial intelligence techniques of late.

4. Findings

This paper shows the artificial intelligence techniques that have been identified to be used for image information hiding in the previous ten years. Many authors have worked on it particularly on how to design an excellent quality of hiding algorithm in image information hiding. In literature survey, in addition to improvements in encryption algorithms and embedded techniques in spatial and transform domains, artificial intelligence techniques have been increasingly employed in image information hiding. As such, in information hiding, these are the significant findings that are made based on artificial intelligence techniques:

- Neural network (NN) is well known for its good generalization capability. Most of the NN works applied the back-propagation algorithm (BP) for embedding. BP is used because it is suitable especially for training the complex input patterns like input characteristic information of an image to generate robust outputs [15-16].

- Genetic algorithm (GA) is known for its strength in which no derivative information is required and it works well with populations of points, not individual points in the search space [40]. GA is using not only biological evolution operation, such as crossover and mutation, but also good at dealing with the noisy features on cover-images that can enhance the probability of spaces used for embedding [41-42].

- Fuzzy logic (FL) is able to improve the performance of system when dealing with image patterns that are very often inexact, ambiguous, or corrupted [43]. FL can also be successfully applied in information hiding mainly for two reasons. The first is ambiguity in the images can easily be recognized and second, the need for fast processing, that might be complicated formulas, may not be applicable for a real-time system. These are all essential in order to preserve the imperceptibility [41-43].

5. Conclusions

This paper studied a comprehensive overview of artificial intelligence techniques namely NN, GA, and FL. They have their own strength in attaining the main goals of information hiding; imperceptibility, payload capacity or robustness. They have been utilized based on their strengths in the stage of pre-processing, embedding, extracting or a combination of a few of them. In order to preserve imperceptibility many artificial intelligence works have applied the pre-processing, image features,
HVS and localization approaches. Meanwhile, for robustness most of the works use secret-key, blind techniques and transform domain. FL has been utilized at all stages and is used to preserve imperceptibility. GA is primarily used to increase the payload capacity while NN is mainly exploited for robustness in embedding and extracting. The significant findings have been clearly outlined to design an excellent quality of hiding algorithm in image information hiding that can preserve imperceptibility and at the same time increase robustness. Configurations with boattail have a higher wave drag but appreciably lower base drag with a resultant decrease of total drag. The decrease of the boattail angle increases the base drag but reduces the projectile wave drag with a resultant decrease of the total drag.

References


