A More Secure Image Hiding Scheme Using Pixel Adjustment and Genetic Algorithm

Omar Banimelhem, Department of Network Engineering and Security, Jordan University of Science and Technology, Irbid, Jordan

Lo'ai Tawalbeh, Department of Computer Engineering, Jordan University of Science and Technology, Irbid, Jordan

Moad Mowafi, Department of Network Engineering and Security, Jordan University of Science and Technology, Irbid, Jordan

Mohammed Al-Batati, Department of Computer Engineering, Jordan University of Science and Technology, Irbid, Jordan

ABSTRACT

This paper proposes a more secure image hiding scheme using Optimal Pixel Adjustment Process (OPAP) and Genetic Algorithm (GA). The security issues of key selection that is used in image hiding are addressed. Thus, a more secure scheme is proposed in order to improve the security as well as the quality of the stego-image. Since GA is a semi-blind algorithm, it may select a key that affects the security. Therefore, the authores improve the security by applying image transformation not only using the GA key, but also using a user key. The user key is used to disarrange the pixel locations of the secret image. Then, the GA, using OPAP, selects the key that maximizes the quality as well as the security of the stego-image. From implementation point of view, the scheme uses a simple and fast transformation method that increases the difference between the secret image and its transformed version. The results showed that the resultant disarranged image cannot be detected, and at the same time the stego-image quality is still high.

Keywords: *Genetic Algorithm (GA), Image Hiding, Optimal Pixel Adjustment Process (OPAP), Secure, Steganography*

INTRODUCTION

Image hiding is a kind of information hiding known as steganography that is usually used in convert communication. The difference between steganography and cryptography is that the goal of cryptography is to make the secret data unreadable by a third party (attackers); while steganography aims to hide secret data within cover data. Depending on the embedding domains, image steganographic methods are classified into two categories: spatial domain

DOI: 10.4018/jisp.2013070101

based methods and frequency domain based methods. The most popular steganography methods that fall into the spatial domain class are presented in (Adelson, 1990; Bender, Gruhl, Morimoto & Lu, 1996; Bender et al., 2000; Turner, 1989). The basic idea of these methods is to use the Least Significant Bits (LSBs) of image pixels to embed the secret data. For example, if the value of secret data is 5 $(101)_2$, and the pixel value of the cover image is 100 $(01100100)_2$, then the basic method is to embed the secret data into the pixel value in the three LSBs to be 109 $(01101101)_2$. The human eyes cannot detect such changes since the Most Significant Bits (MSBs) have not changed. Despite that the spatial domain based LSB methods are simple and have less computational complexity, they have weak resistance to attacks (Cheddad, Condell, Curran & Mc Kevit, 2010). In order to overcome this shortcoming and improve the security level, frequency domain based methods have been proposed. The main idea of this class of image steganographic methods is to convert the image into frequency domain using a transformer and embed the secret data there. There are several transformation methods that have been used for steganography. The most popular methods are the Discrete Cosine Transformation (DCT) method that was used in (Chang, Chen & Chung, 2002; Hashad, Madani & Wahdan, 2005), Discrete Fourier Transform (DFT) method that was used in (Mckeon, 2007; Raja, Chowdary, Venugopal & Patnaik, 2005), and Discrete Wavelet Transform (DWT) method that was used in (Xuan et al., 2002a; Xuan et al., 2002b). Further image hiding methods are discussed and analyzed in (Cheddad et al., 2010).

The efficiency of image hiding process can be improved by augmenting it with other approaches such as searching algorithms. One of the current approaches that has recently been adapted in order to improve image hiding is Genetic Algorithm (GA), which was proposed by Holland in 1962 (Davis, 1991; Goldberg, 1989). It is a search technique that is used to generate optimal or approximate solutions for a specific problem. The GA uses terms stimulated by biology's terms, such as inheritance, mutation, selection, and crossover. Basically, the algorithm starts from a population of randomly generated individuals, and the fitness for each individual in the population is evaluated. Then, based on the resultant fitness, new individuals will be mixed using one or more crossovers, randomly mutated, and finally selected to be a new generation. The new population will be used in the next iteration of the algorithm that will terminate by either reaching a maximum number of generations or by reaching a specific fitness level, depending on a defined objective function.

On the other hand, Optimal Pixel Adjustment Process (OPAP) (Chan & Cheng, 2004) is a technique that is used to reduce the distortion that might be caused by the LSB method. The OPAP is carried out after embedding the secret image where each pixel of the stego-image (containing the secret image) is adjusted to reduce the difference between the stego-image pixel value and the corresponding cover image pixel value in order to improve the quality of the stego-image.

GA has been used with OPAP to enhance the quality of the stego-image (Tseng, Chan, Ho & Chu, 2008). Before embedding the secret image using OPAP, the image is transformed (scrambled) using a key selected by GA that maximizes the quality of the stego-image. In such approach the security issues of key selection have not been addressed. This paper proposes a more secure image hiding scheme using OPAP and GA in order to improve the security as well as the quality of the stego-image. Unlike (Tseng et al., 2008), the proposed scheme applies secret image transformation using a user key in addition to the key selected by GA, and takes into consideration both the security and image quality in the GA evaluation (fitness) function. Moreover, a simple and fast secret image transformation method that increases the difference between the secret image and its transformed version is introduced.

The remaining of the paper is organized as follows. First, a review of the related work is provided. Next, the OPAP algorithm is presented, and image hiding using OPAP and GA