Ministry of Higher Education
and Scientific Research
University of Diyala- College of Science
Department of Computer Science

Image Steganography Based on Behavior of Particle Swarm Optimization

A Thesis

Submitted to the Department of Computer Science\ College of Science\ University of Diyala in a Partial Fulfilment of the Requirements for the Degree of Master in Computer Science

By

Inaam Rabah Mohammad

Supervised by

Prof. Dr. Ziyad Tariq Al_Ta'i

September 2017

بِسْمِ اللَّهِ الرَّحْمَٰنِ الرَّحِيمِ

وَمَا مِن دَابَّةٍ فِي الْأَرْضِ وَلَا طَائِرٍ يَطِيرُ بِجَنَاحَيْهِ إِلَّا أُمَمٌ أَمْثَالُكُم ۚ مَّا فَرَّطْنَا فِي الْكِتَابِ مِن شَيْءٍ ۚ ثُمَّ إِلَىٰ رَبِّهِمْ يُحْشَرُونَ

الأية 38 من سورة الأنعام

صدق الله العظيم

الإهداء

أهدي جهدي المتواضع هذا

إلى النور الذي ينير لي درب النجاح
..... أبي الحبيب

إلى من كان دعائها سر
نجاحي.....أمي الغالية

إلى من كانوا يضيئون لي الطريق ويساندوني
.....عائلتي

إلى من أنار لي طريق العلم
والمعرفة..... اساتذتي

إنعام رباح محمد

Supervisor Certification

I certify that the thesis entitled “Image Steganography Based the Behavior of Particle Swarm Optimization" was prepared by "Inaam Rabah Mohammad” under my supervision at University of Diyala – Collage of Science – Department of Computer Science, as a partial fulfilment of the requirements for the degree of master in computer science.

Supervisor

Signature:

Name: prof. Dr. Ziyad Tariq Al_Ta'i

Date: \ \ 2018

وزارة التعليم العالي والبحث العلمي

جامعة ديالى - كلية العلوم

قسم علوم الحاسوب

إخفاء الصور بإستخدام سلوك خوارزمية PSO

رسالة

مقدّمة الى قسم علوم الحاسوب – كلية العلوم – جامعة ديالى كجزء من متطلبات نيل درجة الماجستير في إختصاص علوم الحاسوب

من قبِل

إنعام رباح محمد

بإشراف

أ.د. زياد طارق مصطفى

أيلول 2017

الخلاصة

فرضت الإمكانيات المتزايدة للإتصالات الحديثة والنمو الهائل لتكنولوجيا المعلومات تطور وسائل امنية المعلومات, تقنية إخفاء المعلومات بالصور هي فئة من وسائل أمنية المعلومات. في الوقت نفسه ، يهتم الباحثون بتقنيات التحسين مثل تحسين السرب. لذلك يقدم العمل تحسين لأمنية المعلومات في مجال إخفاء الصور بالآعتماد على سلوك خوارزمية PSO . على وجه التحديد, SPSO تمثل السلوك القياسي لخوارزمية PSO. QPSO تمثل السلوك الكمّي لخوارزمية PSO, HPSO تمثل السلوك البشري لخوارزمية PSO.

وفي هذا العمل، تم اقتراح نظام لإخفاء الصور باستخدام خوارزميات (SPSO, QPSO, HPSO) . هذه الخوارزميات تستخدم لتحديد أفضل المواقع في بكسل صورة الغطاء لتضمين رسالة نصية سرية باستخدام تقنية LSB.

تم اختبار قوة الخوارزميات الثلاث (SPSO , QPSO , HPSO) باستخدام ثماني دوال قياسية (benchmark optimization functions). وأظهرت نتائج هذا الاختبار أن خوارزمية QPSO أفضل من (SPSO, HPSO) باعتبارها البحث الأمثل.

وقد تمت مقارنة نتائج النظام المقترح مع بعضها البعض، ومع الأعمال المماثلة السابقة. وقد بينت النتائج ان نسبة PSNR لنظام الإخفاء المقترح بإستخدام خوارزمية QPSO هي (81.41 dB) ، نسبة PSNR لنظام الإخفاء المقترح بإستخدام خوارزمية HPSO هي (81.21 dB) , نسية PSNR لنظام الإخفاء المقترح بإستخدام خوارزمية SPSO هي (80.91 dB) . وبالتالي، فإن النظام المقترح باستخدام خوارزمية QPSO هو أفضل أداء من وجهة نظر الإخفاء.

بالإضافة الى ذلك تم إختبار النظم الثلاثة المقترحة وفقا لمنهجية الإخفاء. وأوضحت اختبارات هذه المنهجية أن جميع الأنظمة المقترحة قوية ضد اختبار الضغط، ولكنها ليست قوية بما فيه الكفاية ضد

إختبارات (التحويل والطباعة / المسح الضوئي). ومع ذلك، هذا ليس نقص في النظم المقترحة، حيث أن المهاجم لا يمكن أن تستفيد من الرسائل المستخرجة المدمرة.

Chapter One

□□□□□□□□□□

□□□ □ □□□□□□□

The Internet as a whole does not use secure links, thus information in transit may be vulnerable to interception as well. The important of reducing a chance of the information being detected during the transmission is being an issue now days. Some solution to be discussed is how to hide information in a manner that the very existence of the message is unknown in order to repel attention of the potential attacker. Besides hiding data for confidentiality, this approach of information hiding can be extended to copyright protection for digital media [1].

Information hiding is the method of hiding the amount of data called secret message or water mark into a cover media that may be audio, video or image in an imperceptible way to build a covert channel for secret communication for the purpose of verifying integrity, copyright protection, or other purposes [2].

A major category of information hiding is steganography (literally, covered writing). Johnson et al. [3] defined steganography as the concealing secret data within another innocuous cover media.

Steganography become more important as more people join the cyberspace revolution. Steganography is the art of concealing information in ways that prevent the detection of hidden messages [1].

At the same time, nature provides inspiration to computer scientists in many fields. One source of such inspiration is the way in which natural organisms can behave when they are in groups. If the group itself is considered as an individual (the swarm) in some ways, the swarm seems to be more intelligent than any of the individuals within it [4]. Therefore, swarm intelligence is part of artificial intelligence. It is based on the study

of collective behavior in decentralized and self-organized systems. In this thesis, Particle swarm optimization (PSO) algorithm is used as powerful swarm intelligence search technique for finding best steganographic positions [5]. However, PSO has many modifications that can be used in different applications, we noticed that PSO and its modifications can be organized by the behavior of PSO. This organization starts by Standard Particle Swarm Optimization (SPSO), followed by quantum-behaved Particle Swarm Optimization (QPSO), then human behavior-based Particle Swarm Optimization (HPSO). Therefore, this thesis focuses on joining between image steganography and the behavior of PSO algorithm.

□□□ □ □□□□□□ □ □□□

□Xiaoxia Li and Jianjun Wang (2007) [6], they proposed a technique that can conceal large message as well as keeping the quality of stego image acceptable. Also, their proposed method derives an optimum substitution matrix by SPSO algorithm to change the secret data and then conceals a secret message into the cover image through a modified JPEG quantization table. Moreover, the proposed method helps to embed the secret messages with high level of security because one cannot recover the secret messages correctly without knowing the substitution matrix.

□Ruchika Bajaj et al. (2010) [7], developed a method for embedding secret messages of variable length with high embedding capacity based on SPSO. This method finds the best pixel positions in the cover image, which can be used to conceal the secret message. In the proposed method, M bits of the secret message are substituted into M least significant bits of the image pixel, such as M varies from 1 to 4 depending on the message length.

□Feno Heriniaina et. al (2011) [8], proposed a secure data hiding scheme for embedding secret message into a cover image with least significant bit

(LSB) substitution in discrete cosine transformation domain (DCT). Firstly, the secret message was divided into partitions, whereas the cover image is split into blocks of 2x2 size. The DCT was used to change the blocks from spatial to frequency domain. The proposed method results an increasing in efficiency, as well the security level, because SPSO algorithm is used for finding an optimal transformation matrix T.

Anu Garg and Navdeep Kaur (2014) [9], proposed a new method for data hiding that is using the hybrid algorithm of PSO with ACO. The results were calculated using PSNR and MSE values, providing increased security and quality of the stego image.

E. Divya and P. Rajmar (2015) [10], analyzed the embedding procedure using SPSO in spatial and transform domain. SPSO was analyzed for (100) iterations and obtained an increase in efficiency. SPSO finds pixel locations for hiding the data. The performance of both techniques was compared and the PSO gives best stego images. The PSNR value comparison showed that the PSO gave best PSNR after 100 iterations. Also, the DWT using PSO gave good PSNR but it took more computation compared to other methods.

*E. Divya and P. Rajmar (2016) [11], analyzed the steganographic data hiding using the least significant bit technique and PSO algorithm that provides the best pixel positions in the cover image that can be used to embed the secret message bits so that less image distortion occurs. Also, the image quality measures were calculated to compare the results of simple LSB hiding in random pixels without using PSO algorithm and with the method based on PSO. This method also analyses the modified particle swarm optimization on the spatial domain technique which improved the PSNR and also reduced the computation time.

- Vaddadi Swetha et. al (2016) [12], implemented biometric feature for skin tone region of images. Data hiding is done in detecting skin tone regions. A novel steganography scheme was proposed that uses particle swarm optimization algorithm (PSO) for data hiding. It assured high security, good invisibility and robustness. The secret data is embedded with a cover image to improve the security of stego images by means of PSO algorithm.

□□□ □□□□□□ □□□□□□ □□□

The previous related works show that image steganography using PSO algorithm is not a new field. However, these works did not take in consideration the effect of an individual's behavior in PSO algorithm. Also, the strength of PSO algorithm in finding optimal solutions was not evaluated. Many modifications of PSO algorithm are proposed through the last few years based on its behavior, such as quantum behaved PSO (QPSO) and human behavior based PSO (HPSO) algorithms. Therefore, the first problem of this thesis is to improve the security of image steganography using the behavior of PSO algorithm. The second problem is to evaluate the strength of the algorithms (SPSO, QPSO and HPSO) in the search space with a chosen set of benchmark functions.

□□□ □ □□ □□□□□ □ □□□□□

The aim of research is to evaluate the behavior of PSO algorithm classically, quantitatively and humanly using image steganography. The three types of PSO algorithm are used as powerful swarm intelligence search technique for finding random positions in the cover image to hide a secret text message. Also, a comparison between (SPSO, QPSO, and HPSO) algorithms will be investigated from the viewpoint of optimization by using a set of standard test benchmark functions.

The other chapters in this thesis are as follows:

This chapter gives the background and review of image steganography and PSO algorithm and its modifications: (Quantum behaved- particle swarm optimization (QPSO) and Human behavior based- particle swarm optimization (HPSO)).

This chapter describes the proposed steganography system with its design and implementation.

This chapter explains the results and evaluation that have been getting from the proposed system.

This chapter presents the conclusions of this work. Furthermore, it provides suggestions for future work.