نظام الوكيل المساعد لتقنيـة الإخفاء

رسالة مقدمة

إلى مجلس كلية العلوم - جامعة بابل
كجزء من متطلبات نيل درجة الماجستير في علوم الحاسبات

من

نه وين نجاة محمد

بإشراف

د. ستار بدر سد خان

د. عباس محسن البكري

ذي القعدة ١٤٢٨ هـ **شباط ٢٠٠٧ م**

USE AN AGENT SYSTEM IN STEGANOGRAPHY

A Thesis

Submitted to the Council of College of Science University of Babylon in Partial Fulfillment of the Requirements for the Degree of Master of Science in Computer Science

By

Naween Najat Mohammed

Rabea-١ ١٤٢٨ **April-٢٠٠٧**

Acknowledgment

First of all, thanks to Allah for his guidance that enables me to complete my research.

I would like to express my appreciation and sincere gratitude to my father and mother for their patience, encouragement, guidance and advice they gave to me through out my study.

Special thanks to my supervisors, Dr. Sattar B. Sadkhan & Dr. Abbas M. Al-Bakry.

My deep appreciation and respect go to chief of Babylon University Dr. Nabeel H. Al-A'araji, department of computer science, specially the head of department Dr. Abbas M. Al-Bakry, and the Dean of college of science, Dr. Oda Mizi'l Yasser Al-Zamely.

Grateful thanks for all my friends especially Nidhal & Fatimah. I wish to them success and happiness in their life.

I would like to say "Thanks" to every one who support and help me through these tough years.

Naween

الملخـص

يعد آل (*Agent*)الوكيل في الغالب جيل من الأدوات التي تساعد على الإدارة الفعالة للمعلومات.خلال هذه الدراسة ما نعني بمصطلح آل (*Agent*) الوكيل يمثل عنصراً برمجياً الذي يخدم المستخدم بعدة طرق: أل(*Steganography*) هو تطبيق الإخفاء آو تمويه البيانات السرية بإخفائها في وعاء مقلد غير مؤذٍ. عندما يتم إخفاء البيانات فانه من المحتمل آن تنقل عبرخطوط غير آمنة آو توضع في مكان عام .لذلك يجب آن يكون الوعاء المقلد مناسب و غير مؤثر (برئ)في كل الاختبارات. في هذا البحث تم استخدام طريقتين للإخفاء *Steganography*: طريقة *LSB –Steganography*و طريقة *DCT-Steganography* وان دور آل(*Agent*) في الإخفاء حيث إن صورة التغطية آو الوعاء تعتبر ذات أهمية من خلال تأثيرها على أمنية النظام .لذلك فأن النظام الوكيل المساعد الفرعي يصنع القرار الذي يساعد على اختيار أ فضل صورة غطاء من قاعدة البينات الصور الخاصة بصور الغطاء. وأن قاعدة بيانات الصور تم تصميمها باستخدام ((*Thumb-plus software* . بالإضافة إلى ذلك آن نظام الوكيل المساعد يعمل على مساعدتنا في اتخاذ القرار المناسب في استخدام طريقة الإخفاء المناسبة للصورة السرية المختارة. يمكن ل (*Agent*)آن يستثمر ويصور من خلال عدة طرق. في النظام المقترح نقوم بتصوير نظام الوكيل المساعد من خلال تحرير نص.

أجهزة الحاسوب المستخدمة (*Hardware*) في النظام المقترح هي عبارة عن شبكة حاسبات ((*Client\server* . آن لغة البرمجة المستخدمة في هذا النظام هي (*object oriented programming*) وان أول نظام للوكيل المساعد تم تصميميها باستخدام لغة (*C*) والنظام المقترح نفذ باستخدام لغة (*Visual C++*) الذي يسمح بوصف قواعد السيطرة و إدارة الاتصالات بأدوات برمجية .

Abstract

gent is often claimed to become a new generation of tools facilitating efficient management of information. Throughout this thesis ,what we mean with the term agent is a software component that guid the user .to choose the best way

Steganography is the practice of hiding or camouflaging secret data in an innocent looking dummy container. Once the data has been embedded, it may be transferred across insecure lines or posted in a .public place

Therefor the dummy container should seem innocent under most examinations. In this work ,two steganography methods are implemented, the LSB-steganography method and DCT-steganography method. The Agent helps us in Steganography, since the cover image is important which influencing the security of the system ,So an agent-subsystem makes decisions that help us with choosing the best cover image from the image database, and the image database in this work is designed by using thumbs-plus software, also Agent helps us with making decisions by choosing the suitable steganography method for the chosen Cover image to embed the specified secret image. Agent can be implemented and visualized in several ways, in the proposed system, .we visualize our agent by generating a text

The proposed system hardware requires computers (server and client), in which Client \Server connection is implemented. The Programming tool used in this system is the object oriented programming (OOP). This is so because the first agent system is designed by using "C programming language". The proposed system is implemented by using "Visual C++" which allows the description of control and communication management as programming tool

Appendix A

BMP Image –file format

The BMP file format divides a graphics file into four major parts , these are:

١- **BMP file header**: the bitmap file header is ١٤-byte long and is formatted as follow :

UNIT bfType *(holds the signature value ٠xD٤٤٢,which identifies the file as BMP)*

DWORD bfSize (*holds the file size).*

UNIT bfReserved *(not used set to zero).*

UNIT bfReserved *(not used , set to zero).*

DWORD bfOffBits (*specifies the offset , relative to the begging of the file , where the data representing the bitmap itself begins).*

٢- **Bitmap Information Header** : The bitmap information contain important information about the image .the windows format for this header is :

DWORD bfSize *(holds the header length in byte).*

LONG biWidth *(identify the image width).*

LONG biHeight *(identify the image height).*

WORD biplane

WORD bibitCount (*identify number of bits/pixels in the image and thus the maximum number of colors that the bitmap can contain).*

BWORD biCompression *(identifies the compression scheme that the bitmap employ . it will contain zero if the bitmap uncompressed)*

DWORD biSizeimage *(Set to zero for uncompressed image ,else it holds the size (in bytes) of the bits representing*

the bitmap image for compressed images)

LONG biPelsperMeter.

LONG biYpelsperMeter.

DWORD biClrUsed.

DWORD biClrimportant.

٣-Palette(Color table containing RGB quad or RGB triple structure):the color table specified the colors used in the bitmap.the BMP files come in four color format.

١. ٢-color *one-bit per pixel.*

٢. ١٦-color *four –bit per pixels.*

٣- ٢٥٦-color *eight –bit per pixels.*

٤- ١٦.٧ million-color *٢٤-bits per pixel.*

The number of bits per pixels – and hence the color format-can be determined from the biBitCount shown above. in the ٢-color, ١٦-color and ٢٥٦-color BMP format, the color table contains one entry for each color. Each entry specifies the intensities of a color's red, green , and blue component and it is of ٤-byte long as shown below.

Byte rgbBlue.

Byte rgbGreen.

Byte rgbRed.

Byte rgbReserved.

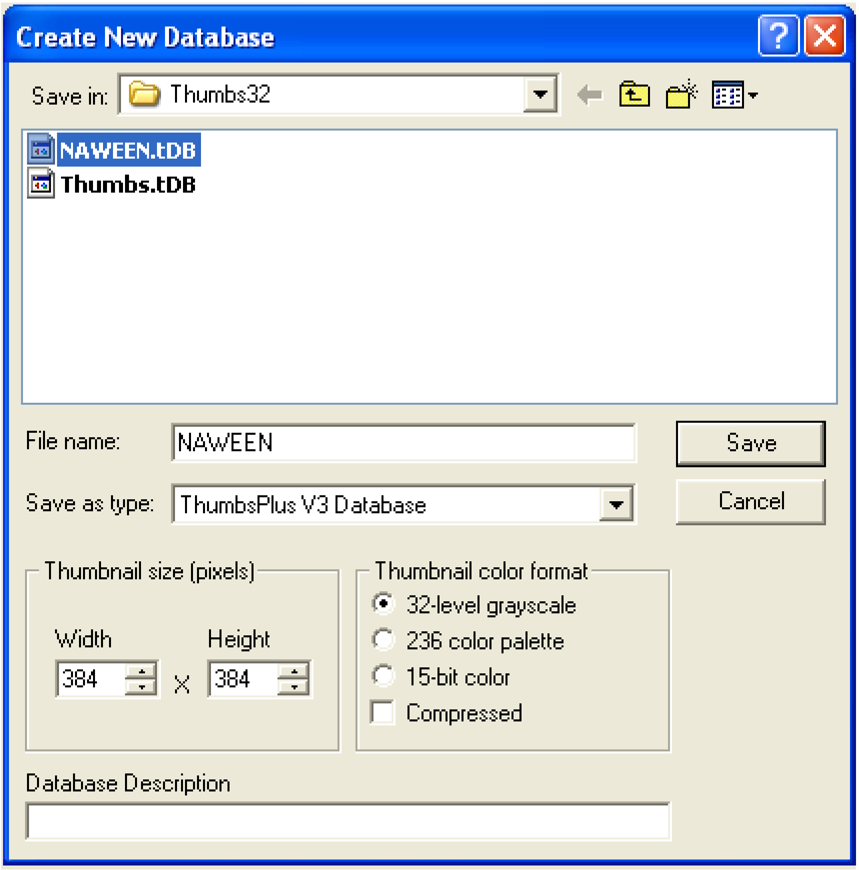
Each color –table entry can specify a range of red , green,and blue values from ٠ to ٢٥٥.True –color BMP files do not contain color tables , because a single color table with ١٦.٧ million entries of ٤-bytes each would require ٦٤MB of storage space.

٤-Bitmap Bits: The bitmap bits is the set of bits defining the image –the bitmap itself .In the ٢-color, ١٦-color BMP formats , each entry in the bitmap is an index to color table. In a ١٦.٧ million –color bitmap , where there is no color table , each bitmap table directly specifies a color. The first ٣-bytes in each ٢٤-bit entry specifies the pixels color red component,the second specifies green component and third specifies blue.

Appendix B

Image Database

If we have a lot of graphic files , we may want to organize them into separate databases,. we can create new database by using thumbs plus software in which from file /New database option you can create new database. There are several options you can set for the database, including the size of the thumbnails and their color depth.



Create New Database

Save in: Thumbs32

NAWEEN.tDB
Thumbs.tDB

File name: NAWEEN

Save as type: ThumbsPlus V3 Database

Thumbnail size (pixels)
Width 384 × Height 384

Thumbnail color format
● 32-level grayscale
○ 236 color palette
○ 15-bit color
□ Compressed

Database Description

we create A cover images database with size of (٣٨٤ x٣٨٤) pixels composed of gray scale image , BMP format.

List of Abbreviation

Abbreviate	Means
٢D	Two Dimension
AI	Artificial intelligent
BMP	Bit Maps Image format
CD	Compact Disk
COR	Correlation
DB	Data Base
db	Decibel
DCT	Discrete Cosine Transform
GIF	Graphical Image Format
H	Height
HVS	Human vision system
Internet	International NetWork
JPEG	Joint photographic Expert
LSB	Leas Significant Bit
MAS	Multi agent system
MSE	Mean Square error
OOP	Object oriented programming
PSNR	Peak- Signal- to- Noise Ratio
QC	Quantization coefficient
RGB	Read Green Blue
SS	Spread spectrum
W	Width

List of Contents

list of figures

List of Tables

Abstract

Agent is often claimed to become a new generation of tools facilitating efficient management of information. Throughout this thesis ,what we mean with the term agent is a software component that guid the user to choose the best way.

Steganography is the practice of hiding or camouflaging secret data in an innocent looking dummy container. Once the data has been embedded, it may be transferred across insecure lines or posted in a public place.

Therefor the dummy container should seem innocent under most examinations. In this work ,two steganography methods are implemented, the LSB-steganography method and DCT-steganography method. The Agent helps us in Steganography, since the cover image is important which influencing the security of the system ,So an agent-subsystem makes decisions that help us with choosing the best cover image from the image database, and the image database in this work is designed by using thumbs-plus software, also Agent helps us with making decisions by choosing the suitable steganography method for the chosen Cover image to embed the specified secret image. Agent can be implemented and visualized in several ways, in the proposed system, we visualize our agent by generating a text.

The proposed system hardware requires computers (server and client), in which Client \Server connection is implemented. The Programming tool used in this system is the object oriented programming (OOP). This is so because the first agent system is designed by using "C programming language". The

proposed system is implemented by using "Visual C^{++}" which allows the description of control and communication management as programming tool.

Supervisors Certification

We certify that this thesis was prepared under our supervision at the Department of Computer Science/ College of Science/ Babylon University, by ***Naweeen Najat Muhammad*** as partial fulfillment of the requirement for the degree of Master of Science in Computer Science.

Signature:		**Signature:**	
Name:	Dr.Eng Sattar B. Sadkhan	**Name:**	Dr. Abbas M. Al-Bakry
Title:	Asst Pro	**Title:**	
Date:	/ /٢٠٠٦	**Date:**	/ /٢٠٠٦

In view of the available recommendation, I forward this thesis for debate by examination committee.

Signature:	
Name:	Dr. Abass M. Al-Bakry
Title:	Head of the Department of Computer Science, Babylon University.
Date:	/ /٢٠٠٦

Chapter One

INTRODUCTION

١.١ Preface

The prevalence of the internet as a mass communication means and the proliferation of digital multi media circulate via the web have brought the ancient art of steganography into digital area[١].

Steganography is the art of invisible communication. Its purpose is to hide the very presence of the communication by embedding a message into innocuous-looking cover object. In today's digital world, invisible ink and paper have been replaced by much more versatile and practical covers for hiding message–digital documents, images, videos, and audio files. As long as an electronic document contain perceptual irrelevant or redundant information, it can be used as a cover for hiding secret messages[٢].

Data hiding method for image can be categorized in two categories, they are spatial-domain and frequency-domain. In the spatial domain, the message are embedded in the image pixels directly, while in frequency domain, however, the secrete image is first transformed to frequency domain, then the message is embedded in the transformed coefficients[٣]. For many applications the problem of information hiding can be considered as a trade-off between three aspects: *minimizing the distortion in the host image due to embedding*, maximizing the robustness of information hiding to attack, maximizing the embedding capacity of the scheme[٤]. Learning a new method for storing data is of fundamental importance to us. Science constantly seeks novel ways of retaining and laying claim to information storage medium which could be of more profound importance than the one that details the construction of life as we know it. To hide data, we need one of three things: the ability to insert sequence to alter an existing innocuous sequence and leveraging it to hide data or to find redundancy in an existing sequence and leveraging it to hide data [٥].

People have done business for long time. The only intelligent agent that people had was another human agent. Human being is currently the finest agent technology in the world and, as it appears from current research, will continue to be so for quite awhile[٦].

The concept of an agent was originated from the area of artificial intelligence (AI). Naturally agent needs to execute some where. Computer host a platforms also provide additional service, such as communication facilities to agent it is hosting. Decision that we are asked to make today at work and at home require greater information content and analysis. This change has been brought about empowerment, competition, and decision making. Ten years ago if you wanted to buy a car you would wander down to a local dealer. Today through internet car tendering system, you can specify, the make, model, color, and trim that you require to fit your life style and actually many dealers from all over the (world) bid to get your business. It is at this point computer agent can help, by doing the searching and soon even doing negotiation, only when they complete their task you will be asked to look at the results and make decisions. It is a bit like having team of highly component staff members assemble the facts and the options on your behalf except the staff - work ٢٤- hours a day. Computer agent in our entertainment world will help us with decision, and provide intelligent quality options and choices[٧].

It is important to realize that like other software technologies such as objects, agent is not a magic they are an approach to structure and develop software that offers certain benefits and it is very well suited to certain types of applications[٨].

١.٢ Literature Survey

Although we can not find literature that matches directly the exact research area, i.e. the collection of the steganography technique, the agent systems and image features , we concerned with the following research area are:

- Chin–Chen Chang, Ju-Yuan Hsiao and Chi-Shiang Chan, they developed an optimal least significant bit substitution in image hiding. The processing of simple least significant bit (LSB) substitution embeds the secret image in the least significant bits of the pixels in the host image. The processing may degrade the host image quality. So significantly that grabbers can detect that there is something that is going on in the image that interests them. To over come this drawback, an exhaustive least significant-bit method that uses a genetic algorithm to search approximate optimal solution, and computation time is no longer so huge[٤١].
- Chi–Kwong Chan, and L.M Cheng, they proposed a system for hiding data in images by using simple least significant bit substitution, by applying an optimal pixels adjustment process to the STEGO image obtained by the simple LSB substitution method. The image quality of the STEGO image can be greatly improved with low extra computational complexity. The worst case of mean square error between the STEGO image and cover image is derived. The excremental results show that the STEGO image is visually indistinguishable from the original cover – image[٣٨].
- Tao Zhang and Xijian Ping, designed a new approach to reliable detection of least significant bit LSB-Steganography in natural image. A physical quantity is derived from the transition coefficient between different image histograms of an image and it is processed version produced by setting all

bits in the LSB plane to zero. It appears that this quantity is a good measurement of the weak correlation between successive bit planes. It can also be used to discriminate STEGO image from the cover-images. Further studies indicate that there exists a functional relationship between this quantity and the embedded message length[٣١].

- Najla abed Hamza, she designed a robust technique for information hiding in which image steganography is proposed using DCT transformation technique. The proposed system depends on substituting the similar blocks of the embedded image with in a cover image, the system composed of a number of stages: transformation stage, matching stage, substitution stage and inverse transformation stage[٢٨].
- Chin–Chen Chang and Tung–Shou Chen, LOU-Zo Chung, proposed a novel steganographic method based on the joint photographic expert group (JPEG).The proposed method modifies the quantization table first. Next, the secret message is hidden in the cover image with its middle frequency of the quantized DCT coefficient modified. Finally a JPEG STEGO image is generated. JPEG is a standard image and popularly used in the internet[٣].
- V. Rodin ***et al***, presented a parallel image processing system based on the concept of reactive agents. The system describes finely and simply the agents behaviors to detect image feature. They proposed an approach to continuity perception based on multi agent system. Each agent can move around on its environment which consists of an image made up of light and dark rings set out concentrically. The agents are named darkening agent and lightening agent. On the other hand, a higher level of communication requires that the objects (or agents) have the ability to exchange messages on an asynchronous way with management of a

message box in order to increase the flexibility and liability of service demands, proposition, and negotiation[٣٩].

- Sabu.M Thampi and Dr.k.Chandra sekaran, presented an image retrieval system based on image feature, steganography, mobile agents. By utilizing the information hiding technique (DCT based information hiding technique), the valuable image attribute can be hidden in an image without degrading the image quality. Mobile agents manage the query phase of the system based on the simulation results. The proposed system not only shows the efficiency in hiding the attributes but also provides other advantages such as:
  ١. Fast transmission of the retrieval image to the receiver.
  ٢. No need to extract the attribute separately for other applications.
  ٣. Searching made easy[٣٦].
- Tobais Samuel Gabriel Salem, designed an agent based recommender systems that relieve the user of managing large set of information and helping to find relevant objects in an area of interest. The main context is of regular customer at a vendor with offerings of product. The performance for these product could be possible to formalize. Through out this thesis the term agent is a software component that acts through out representative and an authority acting as a representative means that should perform the tasks that we wish it to perform, it also can perform better or faster than we can. This can for example be searching one thousand online–store for best price of CD which you want to consider the fee for package and postage, any bonus –system, etc[٣٢].
- Qi Dunsworth and Robert K. Atkinson, research suggests that students learn better when studying a picture coupled with narration rather than on–screen text in a computer based multimedia learning environment. Moreover,combining narration with the visual presence of an animated

pedagogical agent may also encourage student to process information deeper than narration or on screen text alone. The current study was designed to evaluate three effects among students learning about the human cardiovascular system: the modality effect (narration vs. on screen text), the embodied agent effect (narration + agent vs. on screen text), and the image effect (narration+agent vs. narration).Overall, the results suggest that incorporating an animated pedagogical agent-programme to coordinate narration with gaze and pointing in to science focused multimedia learning environment can foster learning[٣٥].

- Ido Omer and Michael Werman, built a system of image specific feature similarities in which calculating a reliable similarity measure between pixel features is essential for many computer vision and image processing application. They propose a similarity measure (affinity) between pixel features which depends on the feature space histogram of an image. They use the observations that cluster in the feature space histogram are typically smooth and roughly convex. Given two feature points they adjust their similarity according to the bottleneck in the histogram values on the straight line between them[٤٠].

- Jane Yau, Tharam Dillon and Edwige Pissaloux, presented anew approach to content – based image retrieval by addressing these primary issues: image feature extraction and representation, similarity measure, and search methods. Astatically based feature selection scheme is introduced to guide the selection of the most appropriate image feature for dynamic image indexing and similarity measures. In addition, a fractional discrimination function is proposed to enhance image feature points in conjunction with image decompositions and contextual filtering for image classification[٣٣].

١.٣ Aim of Thesis

The present work aims to develop a system for achieving an agent system in steganography by make decision for the best cover image in cover image database that holds the specific selected secrete message (image) and agent depend on the numbers of specific image features & some measurement for cover image, and achieving the suitable steganography method .So the client will obtain or receive a better STEGO image quality from the server.

١.٤ Thesis Layout

The reminder of this thesis is organized as follows:

- **Chapter Two**: defines the agent concept, agent property, and available steganography systems.
- **Chapter Three**: presents the proposed Agency system for steganography , in which the agent searches for the best cover image in image database and the suitable steganography method for selected secret message on server. The client will receive the best STEGO image.
- **Chapter Four:** describes system implementation and the objective test results tested on number of images.
- **Chapter Five:** includes a discussion, some limitations and suggestion for future work.

Chapter Two
STEGANOGRAPHY

Two areas of research are generally referred to as (information hiding) watermarking that is originated from the need for copyright protection of digital media, where steganography studies the ways to make communication invisible by hiding secrets in innocuous message[٩].

٢.١ Digital Watermarking

Digital watermarking is a technology proposed to address the issue of copyright protection for digital content. With the development of the internet and digital technology, digital watermark technique is getting more and more attention to the copyright of multimedia content application[١٠].

Conventional cryptographic systems permit only valid key holders access to encrypted data, but once such a data is decrypted, there is no way to track its reproduction and retransmission. Conventional cryptography ,therefore ,provides a little protection against data piracy, in which the publisher is confronted with unauthorized reproduction of information.

A digital watermark is intended to complement the cryptographic process. It is a visible, or preferably invisible, identification code that is permanently embedded in the data ,i.e, it remain present within the data after any decryption process[١١].

All watermarking methods show the same generic building block:
A watermark embedding system and a watermark recovery system. The watermark can be any nature such as a number ,a test, or an image. And public or secret key may be used to enforce security[٩].

٢.٢ Steganography

Steganography and data embedding are increasing gaining importance in secure and robust communication of vital information. the low sensitivity of human visual system to luminance enables embedding large amount of data in a still image or video without causing any discernible difference between the resulting signal or data embedded signal, and original image[١٣].

There is now a substantial body of literature on techniques of steganography particularly in the case when a covering medium is formed of digital images, and an increasing amount of steganalytic techniques for uncovering the presence of steganography[١٤]. In conventional cryptography, even if the information content is protected by encryption the existence of encrypted communication is known, In view of this, steganography provides an alternative approach in which it conceal even the evidence of encrypted message. Generally, steganography is defined as the art and science of communicating in a cove fashion، it utilizes the typical digit media such as text, image, audio, video and multimedia as carrier called (host or cover signal) for hiding private information in such a way that the third parties (unauthorized person) cannot detect or even notice the presence of communication[١٥].

The goal of image steganography is to embed information in a cover image using modification that is undetectable. In actual practice, however, most technique produce STEGO images that *are perceptually identical to the covered images*[١٦].

٢.٣ Steganalysis

Steganalysis is the art of discovering hidden data in covered objects· as in cryptoanalysis, we assume that steganographyic is publicly known with the exception of a secret key[٢]. The steganalyst is one who applies steganalysis in an attempt to detect the existence of hidden information and/ or render it useless·

Two aspects of steganalysis involve the detection and distortion of embedded message·

- Detection requires that the analyst observe various relationships between combinations of a cover, message, STEGO–media, and steganography tool·
- Distortion attacks require that the analyst manipulates the STEGO-media to render the embedded usless information or remove it altogether. In essence, the activities of observation and manipulation describe two classifications of attack: passive attacks and active attacks respectively·

Hiding information in digital media requires an alternation of the media properties, which may introduce some forms of degradation or unusual characteristics.

Manipulating digital media in an effort to disable or remove embedded messages is a simpler task than detecting the messages. Any image can be manipulated with an intent of destroying some hidden information whether an embedded image exists or not. Detecting the existence of a hidden message will save time in the activity to disable or remove messages by guiding the analyst to process only media that contains hidden information[١١].

٢.٤ Steganography Types

Steganography is divided into three main types. These types are described in the following sections:

- Pure steganography.
- Secret key steganography.
- Public key steganography.

٢.٤.١ Pure Steganography

A steganography system, which does not require a prior exchange of some secret information (like a STEGO-key) is called a pure steganography. Formally, the embedding process can be described as a mapping $E:C \times M \rightarrow C$.where C is the set of possible covers, and M the set of possible message. The extraction process consists of a mapping $D:C \rightarrow M$, extracting the secret messages out of a cover. Clearly it is necessary that $|C| \geq |M|$· both sender and receiver must have access to the embedding and the extraction algorithm, but the algorithm should not be public[١٧].

٢.٤.٢ Secret key Steganography

A secret key steganography system is similar to a symmetric cipher. The sender chooses a cover C and embeds the

secret message using a secret key. If the key ^{K} used in the embedding process is known to the receiver، he can reverse the process and extract the secret message. Any one who does not know the secret key can not obtain an evidence of the encoded information. A gain the cover C and the STEGO-object can be perceptually similar. Formally, the embedding process is a mapping E_k:C×M×K→C and the extracting process is a mapping D_k:C×K→M where k is the set of all possible secret key.

٢.٤.٣ Public key Steganography

The public key steganography system requires the use of two keys, one private and one public. The public key is stored in a public database.

Whereas the public key is used in the embedding process ،the secret key is used to reconstruct the secret message.

One way to build a public key steganography system is the use of a public key crypto system. The public key steganography utilized the fact that decoding function D in a steganography system can be applied to any cover C (recall that D is a function on the entire set C). In the latter case, there is a random element of M as results, which is called the "natural randomness" of the cover. If one assumes that this natural randomness is statically indistinguishable from cipher text produced by some public key cryptosystem. A secure steganography can be built by embedding cipher text rather than unencrypted secrete message[١٧].

٢.٥ Classification of Steganography Techniques

There are several approaches to the classification of steganography techniques. One of these approaches is to categorize them according to the cover modification applied in the embedding process. Mainly, stegano-graphic techniques may be grouped into six categories as follows:

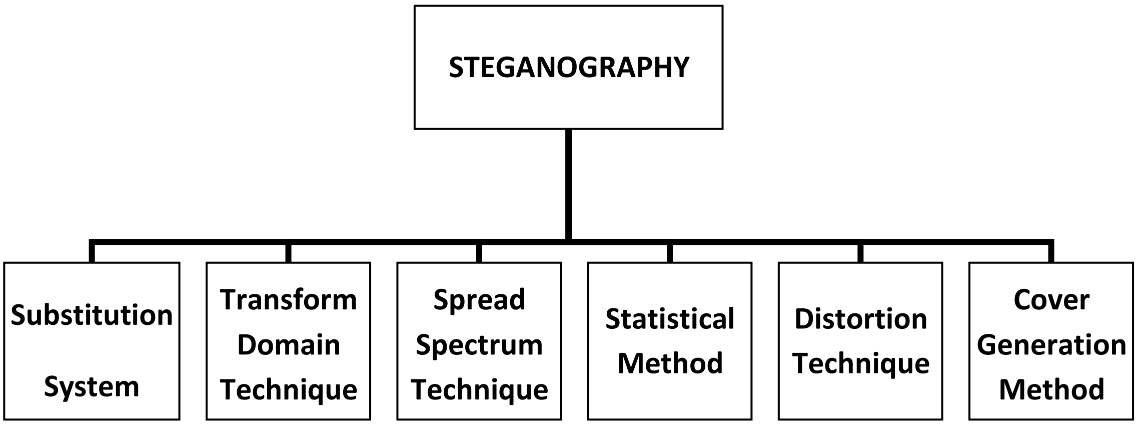


Figure (٢.١): Steganography Classification.

١. **Substitution System:** It substitutes redundant parts of cover with secret messages.

٢. **Transform Domain:** Technique embed secret information in a transform space of the signal (e.g in the frequency domain).

٣. **Spread Spectrum Technique:** They adopt ideas from spread spectrum communication.

٤. **Statistical Method:** it Encodes information by several statistical properties of a cover and uses hypothesis testing in the extraction process.

٥. **Distortion Technique:** it tore information by signal distortion and measure the deviation from the original cover in the decoding step.

٦. **Cover Generating Methods:** it encodes information in the way that a cover for secrete communication is created.

٢.٥.١ Substitution Systems

Basic substitution systems try to encode secret information by substituting insignificant parts of the cover by a secret message bit. The receiver can extract the information if he has knowledge of the positions where secret information has been embedded. Since only minor modifications are made in the embedding process, the sender assumes that he will not be noticed by an attacker. It consists of several techniques[١٧].

٢.٥.١.١ Least Significant Bit Substitution (LSB)..

A basic and well known steganography technique for hiding Message into uncompressed digital image is the least significant bit (LSB) embedding methods. In the least significant

embedding،image pixels are traversed in a predetermine – often pseudo – random – order and LSB. Each pixel is modified to reflect the corresponding bits in the message payload. LSB embedding is preferred in many cases for its simplicity and high embedding rate. The process amounts to introduce a small amplitude noise signal and resulting STEGO-image are visually identical to the cover image[١٦]. The popularity of the (LSB) embedding is most likely. This is due to its simplicity as well as the [false] early belief that modifications of pixels value by ١ in randomly selected pixels are undetectable because of the noise commonly present in all digital images of natural scenes[١٨]. The least significant bit technique takes the advantage of random noise present in the acquired media data, such as images, video, and audio. Embedding message bits in the least significant bit plane will not cause any discernible difference from the original visual[١].

LEAST SIGNIFICANT BIT INSERTION: Is a common, simple approach to embedding information in a cover. Converting an image from a format like GIF or BMP, reconstructs the originated message exactly, to JPEG, which does not، and back could destroy the information in the LSBs.

٢٤-BIT IMAGES: To hide an image in the least significant bits (LSB) of each byte of a ٢٤-bit image, one can store ٣ bits in each

pixel. A ١٠٢٤x٧٦٨ image has the potential to hide a total of ٢,٣٥٩,٢٩٦ bits (٢٩٤.٩١٢ byte) of information. To the human eye the resulting STEGO – image will look identical to the cover image. For example, the letter Z can be hidden in three pixels (assuming no compression). The original raster data for ٣ pixel (٩ byte) may be:

(٠٠١٠١١ ١ ١١١٠١٠٠١ ١١٠٠١٠٠٠)
(٠٠١٠٠١١١ ١١٠٠١٠٠٠ ١١١٠١٠٠١)
(١١٠٠١٠٠٠ ٠٠١٠٠١١١ ١١١٠١٠٠١)

The binary value of A is ١٠٠٠٠٠١١. Inserting the binary value for A in the three pixels would result in:

(٠٠١٠٠١١١ ١١١٠١٠٠٠ ١١٠٠١٠٠٠)
(٠٠١٠٠١١٠ ١١٠٠١٠٠٠ ١١١٠١٠٠٠)
(١١٠٠١٠٠٠ ٠٠١٠٠١١١ ١١١٠١٠٠١)

The underlined bits are the only three actually changed in the ٨ bytes used. On average, LSB requires only half the bits in an image be changed. Data can also be hidden in more significant bits and still the human eye would not be able to discern it.

٨-BIT IMAGES: ٨-bit images are not as forgiving to LSB manipulation because of color limitations. When information is inserted into the LSBs of the raster data, the pointers to the color entries in the pallet are changed.

IMPLEMENTING–LSB: Steganography software processes LSB insertion to make the hidden information is less detectable.

Several approaches have been applied in steganography software, some are more successful than other–to hide information in ٨-bit images.

Applying steganography to the lower bits of image pixels is not limited to the LSB. Depending upon the image، the lower bits of image could encompass the lower four bits of each color byte. How much information can actually be hidden in an image? depends on the composition of an image٠ An image that contains high frequency areas (such as grass) can be manipulated more than an image containing primarily low frequency areas (such as clear blue sky).

LSB manipulation is a quick and easy way to hide information but is vulnerable to small changes resulting from image processing or lossy compression٠

Another way to hide information is in more significant areas of an image. This can be accomplished by manipulating image properties such as luminance[١١].

٢.٥.٢ Spread Spectrum Technique (SST)

The main principle of spread spectrum is to transmit a narrow band signal over a much larger bandwidth such that the power spectral density is very low and the signal in the channel looks like noise. Two well-known spread spectrum techniques are direct sequence and frequency hopping[١٩]. In the information hiding technique the direct either sequence spread spectrum used or frequency hoping. In a direct sequence scheme, the secret signal is spread by constant called "chip rate" modulated with

pseudorandom signal and added to the cover. In the frequency hopping scheme, the frequency of the carrier signal is altered widely used in the context of watermarking[١٧].

٢.٥.٣ Statistical Steganography

Statistical steganography technique utilizes the existence of "١-bits" steganographyic schemes, which embed one bit of information in a digital carrier. This is done by modifying the cover in such a way that some statistical characteristics changed significantly if a "١" is transmitted. Otherwise, the cover is left unchanged· So, the receiver must be able to distinguish the unmodified cover from the modified one.

A cover is divided into *l(m)* disjoint blocks $B_{١}...B_{l(m)}$. A secret bit m_i, is inserted in to i^{th} block by placing "١" into B_i if m_i = ١ otherwise, the block is not changed in the embedding process[١٧].

٢.٥.٤ Distortion Technique

In contrast to substitution systems, distortion requires the knowledge of the original cover in the decoding process. The sender applies a sequence of modification on the cover in order to get a STEGO-system. A sequence of modification is chosen in such a way that it corresponds to a specific secret message wanted to be transmitted. The receiver measures the difference to the original cover in order to reconstruct the sequence of modification applied by the sender which corresponds to the secret message. In

many applications, such systems are not useful, since the receiver must have access into the original cover[١٧].

٢.٥.٥ Cover Generation Technique

In contrast to all embedding methods presented above، when secret information is added to a specific cover by applying an embedding algorithm, some steganographyic applications generate a digital object only for the purpose of being a cover for secret communication[١٧].

٢.٥.٦ Transform Domain Technique

The substitution modification techniques are easy ways to embed information, but they are highly vulnerable to even small cover modification. An attacker can simply apply signal processing technique in order to destroy the secret information entirely.

It has been noted early in the development of steganography systems that embedding information in the frequency domain of a signal can be much more robust that the embedding rule operating in the time domain most robust steganography system known today actually operate in the same sort of transform domain[٢٠].

Transform domain methods hide messages in the significant area of the cover image which makes them more robust to attacks، such as adding noise, compression, filtering, cropping and some image processing, than the substitution approach. However, while they are more robust to various kinds of signal processing, they remain imperceptible, which mean that the HVS has no sense that there exists a STEGO-image. Many transform variations exist one method which is to use the discrete cosine transform (DCT), and the other is to be the wavelet transform.

Transformation could be applied over the entire image, to blocks throughout the image. One popular method of encoding secret information in the frequency domain is modulating the relative size of two (or more) DCT coefficient within one image block.

During the encoding process, the sender splits the cover image in ٨×٨ pixel blocks, each block encodes exactly one secrete message bit. The embedding process starts with selecting a pseudorandom block bi which will be used to code the i^{th} message bit. Let B_i = *DCT (bi)* be the discrete cosine transformed image blocks[٢٠].

٢.٥.٦.١ Discrete Image Transform

The concept of a transform is familiar to mathematicians. It is a standard mathematical tool used to solve problems in many area. The idea is to change a mathematical quantity to another form, where it may look unfamiliar but it may exhibit a useful feature[٢١].

Originally, transforms are defined in their continues forms· The discrete form of these transforms is created by sampling the continues form of the function on which these transformes are based, i.e, the basis functions and if it is extended in to two-dimension, as in images, they are basis image[٢٢].

The general form of the transform equation for N × N image is given by:

$$T(u,v)=\sum_{r=0}^{n-1}\sum_{c=0}^{n-1} I(r,c)B(r,c;u,v) \qquad ...(٢.١)$$

Where *I(r,c)* is the original image, *T(u,v)* is the transform coefficient, *B(r,c;u,v)* correspond to the basis images, *r* and *c* are the spatial domain variable and *u, v* are the frequency domain variable. The transform coefficients *T(u,v)* are the projection of *I(r,c)* onto each *B(u,v)*. These coefficients tell how similar the image is to the basis image. By applying the inversed transform, one can obtain the image from the transform coefficients as follow:

$$I(r,c)=\sum_{u=0}^{n-1}\sum_{v=0}^{n-1}T(u,v)B^{-1}(r,c;v,u) \qquad ...(٢.٢)$$

Here $B^{-١}$*(r,c; u,v)* represents the inversed basis image· In many cases they are the same as the forward ones، but they possibly weighted by a constant[٢٢].

٢.٥.٦.٢ Fourier Transform

The Fourier transform is the most well know, and the most widely used transform. It allows for decomposition of an image into a weighted sum of ٢-D sinusoidal term[٢٢].

Assuming an N x N image, the ٢-D Discrete Fourier Transform (DFT) pair is given by:

$$T(u,v)=1\big/N\sum_{r=0}^{n-1}\sum_{c=0}^{n-1}I(r,c)e^{-2j\pi\frac{(ur+ve)}{N}} \qquad ...(٢.٣)$$

$$...(٢.٤)\ I(r,c)=1/N\sum_{r=0}^{n-1}\sum_{c=0}^{n-1}T(u,v)e^{-2j\pi\frac{(ur+ve)}{N}}$$

By using Euler's identity,

$$e^{ix}=\cos(x)+j\sin(x),$$

Equation (٢.٣) can be rewritten as follows:

$$T(u,v)=1/N\sum_{r=0}^{n-1}\sum_{c=0}^{n-1} I(r,c)\left[\cos(2\pi/N(ur+ve))-j\sin(2\pi/N(ur+ve))\right]$$

$$=R(u,v)+jIm(u,v) \qquad \textit{...(٢.٥)}$$

Where *R (u, v)* is the real part, *Im (u, v)* is the imaginary part of complex spectrum, and *j* is the imaginary coordinate for complex number. At this point, one can define the magnitude and the phase of that spectrum as:

$$|T(u,v)|=\left[\cos(2/N(ur+ve))\right] \qquad \textit{...(٢.٦)}$$

$$\phi(u,v)=\tan^{-1}\frac{Im(u,v)}{R(u,v)} \qquad \textit{...(٢.٧)}$$

The magnitude of a sinusoidal is simply its peak value, and the phase determine where the origin is or where sinusoid starts, in other words, the phase contains information about where object are in the image and the magnitude gives their contrast[٢٢], [٢١].

٢.٥.٦.٣ Discrete Cosine Transform

The discrete cosine transform (DCT), like the Fourier transform’ uses sinusoidal basis function. The difference is that the cosine transform bases are not complex. They use only cosine functions. Assuming N×N image, the DCT (Discreet Cosine Transform) function is given by:

$$T(u,v)=\alpha(u),\alpha(V)\sum_{r=0}^{N-1}\sum_{c=0}^{N-1}I(r,c)\cos\left[\frac{(2r+1)u\pi}{2N}\right]\cos\left[\frac{(2c+1)v\pi}{2N}\right] \qquad \textit{...(٢.٨)}$$

The inverse cosine transform is given by:

$$I(r,c)=\sum_{r=0}^{N-1}\sum_{c=0}^{N-1}\alpha(u),\alpha(v)T(u,v)\cos\left[\frac{(2r+1)u\pi}{2N}\right]\cos\left[\frac{(2c+1)v\pi}{2N}\right] \qquad ...(٢.٩)$$

$$\text{Where}\ \alpha(u),\alpha(v)=\begin{cases}\sqrt{\frac{1}{N}} & \text{if}\ \alpha(u),\alpha(v)=0\\ \sqrt{\frac{2}{N}} & \text{if}\ \alpha(u),\alpha(v)=1,2,3,\ldots N\end{cases}$$

Given this interpretation of the DCT, the way to lose the unimportant image information is to reduce the size of the ٦٤ numbers. There is a chance that this won't degrade the image quality much. This does not always work. So, generally, each of the ٦٤ numbers is divided by the different Quantization Coefficient (QC) in order to reduce its size.

QUANTIZATION: After each ٨×٨ matrix of DCT coefficient calculated it is quantized. This is the step of information loss. Each numbers in the DCT coefficient matrix is divided by the corresponding number from particular quantization table used and the result is rounded to the nearest integer.

A simple quantization table *Q* is computed, based on one parameters R supplied by the user. A simple expression such as Q_{ij} = ١ + *(I + j) / R* guarantees that *QCs* start small at the upper left corner and get bigger toward the bottom right corner[٢١].

The (DCT) is applied not to the entire image but to the data image units (blocks) to reduce the arithmetic operation and then speed the algorithm up[٢١].

One can remembering that transform coefficients are the projection of the Original image onto each basis image· One can conclude the following:

- The origin coefficient represent the lowest frequency· in other word, the DC component of the entire image or sub image.
- The first raw of coefficient matrix increasingly show the frequency component of the image rows and in the same manner the first column shows the frequency component of the image column.
- The rest of the coefficients reflect the change in the frequencies in both raw and column that correspond with each basis images.

Chapter Four

Use An AgentSystem In Steganography

٤. Introduction

Steganography is the art of hiding a message in other message, or hiding message in host media. Several types of media could be used and the image is one of these types. We have two methods of steganography used in this work the first one is the discrete cosine transform (DCT) Steganography method, and the second is least significant bit (LSB) steganography method. Our approach makes an assumption about agent, in this chapter we dedicate to present

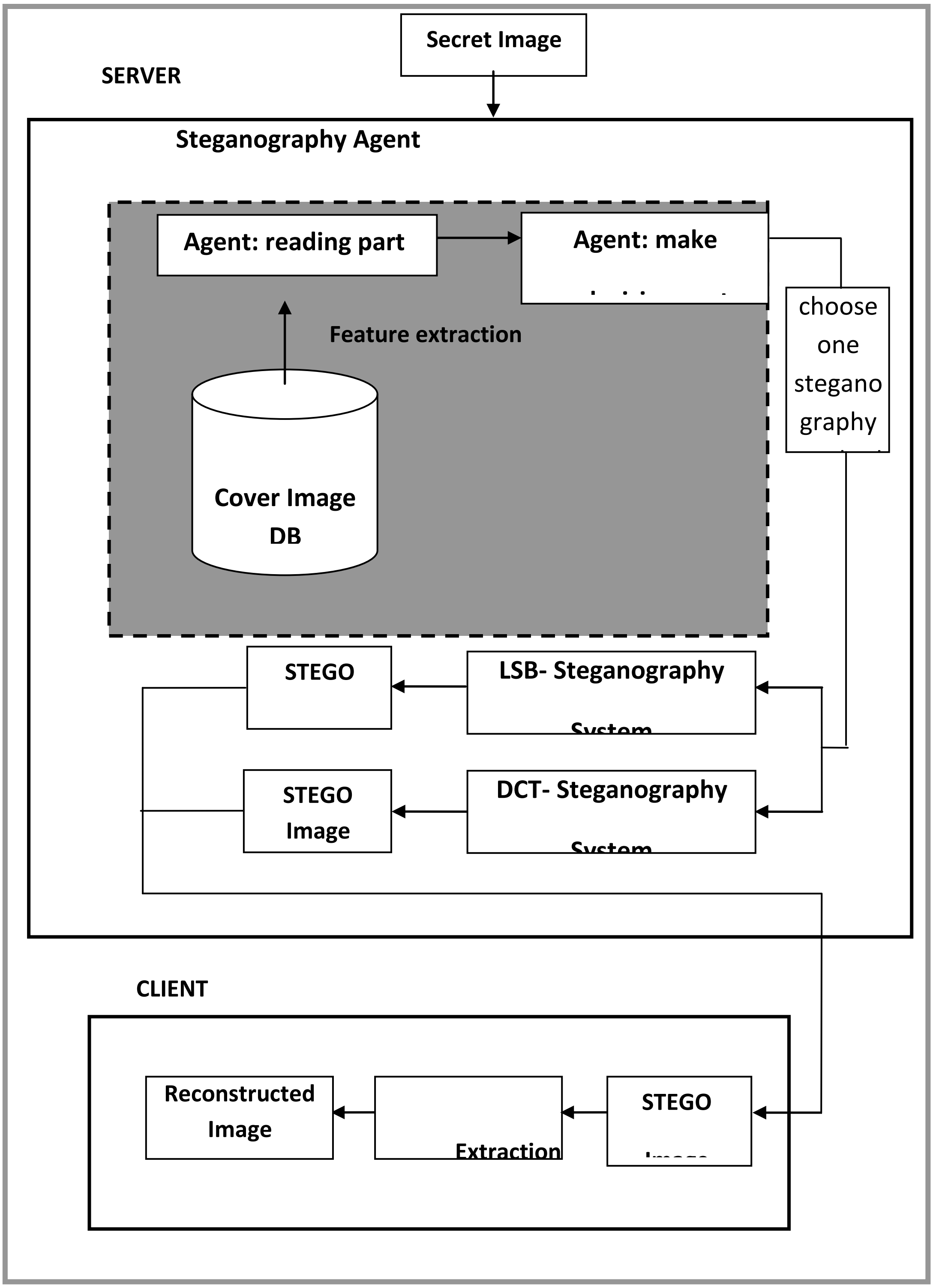
cover image database which are used by the agent . According to some features of media (image), when we select the secret image the agent will recommend you for the best cover (image) in image database to hold the secret message and the suitable image steganography method for embedding process.

٤.١ Use an Agent System in Steganography

This Model of agents, Steganography agent, can be classified as server agent. ***A server agent can provide services to others, but it not need to know whom it will provide to*[٢٧]. Since the Client\ Server connection provided in this project, the server will send to the client the STEGO.bmp file, which it's contain the secret image. The Steganography agent or agent subsystem that it work on the server, detect several features of the cover image and compute some measurements then provide recommendation for "the best cover image since our steganography method is (Image Steganography)" the image (Cover image) can be used as:**

media for embedding the secret message (image), also, the suitable steganography method recommended for selected secret image .

The agency of steganography system structure is as follows:



Figure(٤.١) : The Agent sytem in Steganography Diagram

٤.١.١ Agent Subsystem

In this project we have image processing based on agent . An agent can be used to denote hardware or software - based computer system situated in specific environment, The agent will be placed at random on Cover image (The environment) and compute the number of features of cover Image since,

***The choice of cover image is important because it is significantly influences the design of the STEGO system and it is security*[٢]. The image features that agent detects are:**

١. **Histogram:** Is a plot of gray level value versus the number of pixels. At that value the histogram feature that we use are statically based feature where histogram used as probability distribution of gray level.

$$P(g)=\frac{N(g)}{M} \qquad \text{...(٤.١)}$$

where:

M: is number of pixels in image.

N(g): is number of pixels at gray level g.

٢. **Mean:** Is the average value, so it tell us something about agent general brightness of the image.

$$\bar{g}=\sum_{r}\sum_{c}\frac{I(r,c)}{M} \qquad \text{...(٤.٢)}$$

٣. **Standard deviation:** Which is known as square root of variance, tell as something about contrast, describe the spread in the data.

$$\sigma_g=\sqrt{\sum_{g=0}^{i-1}(g-\bar{g})^2 \;\; p(g)} \qquad \text{...(٤.٣)}$$

٤. **Entropy:** The entropy is a measure that tells us how many bits we need to code the image data. as the pixels value in the image are distributed among more gray level, the entropy increase[٢٢].

$$\text{Entropy} = -\sum_{g=0}^{i-1} P(g)\log_2[P(g)] \qquad ...(٤.٤)$$

Agent computes the previous features, after picking up an image from image database, then agent make a decisions and a choice, detecting a suitable cover to hold the secret image and specified steganography method for the detected cover image. Agent subsystem try to find or detect an image with highest variance, maximum contrast, and high entropy, energy image also an agent subsystem recommends a grayscale uncompressed image.

The choice of image format that makes a very big impact on the design of secure steganography system[٢].

Raw, uncompressed format such as BMP provide biggest space for secure steganography. One should avoid to choose decompressed JPEG images for spatial steganography method such as LSB[٢].

Also , agent choose cover image from images database for DCT steganography that is similar to selected secret image, and the size of cover image and secret image is important since embedding of the secret image must be in cover image larger than the secret image. computing the similarity and dissimilarity measurement between the secrete image and the cover image, similar images recommended for our technique of DCT-steganography.

Similarity and dissimilarity (S&D) computed according to these equation:

$$S\{H(E),H(C)\}=\sum_{j=0}^{n}\frac{\min hj(E),hj(C)}{M_c \times N_c} \qquad ...(٤.٥)$$

$$D\{H(E),H(C)\}=\sum_{j=0}^{n}\left|\frac{h_j(E)}{M_c \times N_c}-\frac{hj(C)}{M_c \times N_c}\right| \qquad ...(٤.٦)$$

Equation (٤.٥) used to measure the similarity between the histogram of the embedded image (E) and cover image (C).

Where:

h ، (E): is a number of element which have the color (J) in the Embed image.

h ١(C): is a number of element which have the color (J) in the Cover image[٢٨].

If Agent fails to find the suitable cover image for DCT-steganography when a secret message is selected then agent make a choice of cover image in image database which is the best one for LSB- steganography method. What we mean by best one, the cover image which decrease the distortion in STEGO file when specific steganography method implement. Depending on previous features variance, contrast, entropy.. ,and (randomness) .

The algorithm theory of randomness is well developed when underlying space is the set of finite or infinite sequence and underlying probability distribution are the uniform distributions[٤٠]**.**

Randomness, the concern in the generation of a sequence of numbers be random in some well–defined statistical sense.

Uniform distribution, the distribution of numbers in sequence should be uniform. Independence, no one value in the sequence can be inferred from other[٢٩].

agent Determine No. of ٠ 's and ١ 's as following:

$$r_0 = \frac{n_0}{n_1 + n_0}$$ ...(٤.٧)

$$r_1 = \frac{n_1}{n_1 + n_0}$$ ...(٤.٨)

where:

n٠: No. of Zero's in Cover Image.

n١: No of one's in Cover Images.

r٠ - ٠.٥ ≤Err and r١ – ٠.٥ ≤Err.

And agent also determine the transition coefficient as follows:

$$r_{00} = \frac{n_{00}}{n_{00} + n_{10} + n_{01} + n_{11}}$$ ...(٤.٩)

$$r_{10} = \frac{n_{10}}{n_{00} + n_{10} + n_{01} + n_{11}}$$ ...(٤.١٠)

$$r_{01} = \frac{n_{01}}{n_{00} + n_{10} + n_{01} + n_{11}}$$ ...(٤.١١)

$$r_{11} = \frac{n_{11}}{n_{00} + n_{10} + n_{01} + n_{11}}$$ ...(٤.١٢)

Where:

n٠٠: no. of ٠٠ in the Cover Image.

n٠١: no. of ٠١ in the Cover Image.

n١٠: no. of ١٠ in the Cover Image.

$n_{١١}$: *no. of* ١١ *in the Cover Image.*

$r_{٠٠} - ٠.٢٥ \leq Err,\ r_{١٠} - ٠.٢٥ \leq Err.$

$r_{١١} - ٠.٢٥ \leq Err,\ r_{٠١} - ٠.٢٥ \leq Err.$

Agent Subsystem Algorithm

Input:	**Input Secret image and the database directory for Cover image.**
Output:	*Recommendation for the best steganography method (LSB & DCT steganography) and the most suitable Cover image from the DB to hold the selected Secret image.*
Step٠:	*Set N= ٠;*
Step١:	*For I = ١ to No of Cover image in DB do steps (٢- ٩).*
Step٢:	*If cover image [I] is not bmp file where the signature of the image file violates 'B'&'M', then go to step ١.*
Step٤:	*If Cover image [I]size and the secret image size is not violate the following condition Secret image size*٨ <= cover image size Then go to step ١.*
Step٤:	*If cover image [I] is Compressed then go to step ١.*
Step٥:	*Compute the similarity(S) and dissimilarity (D)between Cover image [I], and the secret image according to equation (٤.٥) and (٤.٦).*
Step٦:	*If one of the following condition:* *(S > ٠ and D < ٠.٥) is satisfied then go to step ١.*
Step٧:	*Compute the Entropy and the Contrast for the Cover image [I].*
Step٨:	*If Entropy < = ١ and Entropy >٨.٠ then go to step ١.*
Step٩:	*Append the contrast of Cover image [I] to the accepted cover file and Set N = N+ ١, then go to step ١.*
Step١٠:	*If N = ٠ the go to step ١٤.*
Step١١:	*Find the maximum contrast from accepted Cover file then recommendation will set as follow "Use DCT steganography method for embedding the selected secrete image inside the best cover image that is chose by the Agent".*
Step١٢:	*Go to step ١٦.*
Step١٤:	*Compute the stationary probability distribution of No. of ١'s and ٠'s. according to equations (٤.٧), (٤.٨). Of cover image [I],* $r_{٠} – ٠.٥ \leq Err$ *and* $r_{١} – ٠.٥ \leq Err$*, then go to step ١.*
Step١٤:	*Compute the stationary probability distribution of transition*

```
          coefficient of cover image [I] according eq. (٤.٩), (٤.١٠), (٤.١١),
          (٤.١٢), then go to step ١.
Step١٥:   Set recommendation "Use LSB steganography method for
          embedding the selected secret image inside the suitable Cover
          image that chose by agent"
Step١٦:   End.
```

٤.١.٢ Steganography

We use two steganography methods as shown below:

١. LSB Steganography Method.

٢. DCT Steganography Method.

٤.١.٢.١ LSB Steganography

٤.١.٢.١.١ LSB - Embedding

The LSB steganography approach is considered to be one of the most popular and easily implemented steganography system. Each byte in the cover image can hold one bit of secret data in its least significant bits. Therefore, hiding a byte of secrete data needs eight bytes from a cover image. Then the user on Server sends the STEGO file to the Client.

The sequential least significant bit replacement can be implemented more conveniently but has serious security problem in that there is an obvious statically difference between modified part and unmodified part of STEGO image.

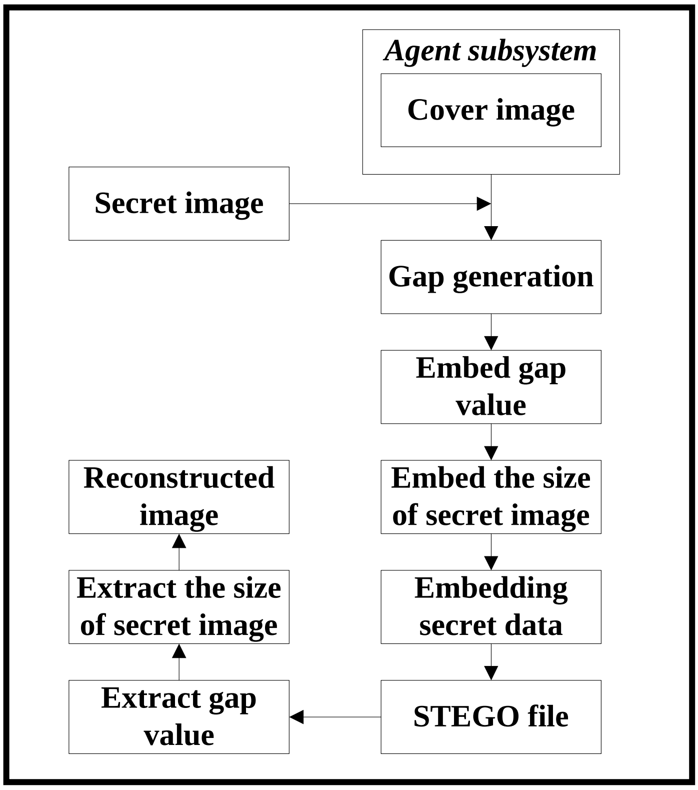


Figure (٤.٢): **LSB-Steganography System**

Through the random LSB embedding, secret message (image) can be randomly scattered, which improves the steganograophic security[٤١]. Secret bit scattered according to following equation[٢٨]:

$$\mathrm{Gap} = \mathrm{int}\,(\mathrm{CH}\times\mathrm{CW})/(\mathrm{L}\times 8) \qquad ...(٤.١٣)$$

where:

CH: is the height of Cover Image.

CW: is the width of Cover image.

L: Secret image size.

LSB Embedding Algorithm

Input:	*Secrete data (image), the cover image.*
Output:	*The STEGO image*
Step١:	*Compute the size of secret image file (L).*
Step٢:	*Generate Gaps according to Gap equation (٤.١٣)*
Step٤:	*Copy the header information and RGB palette from cover image in to STEGO image*
Step٤:	*Distributed secrete image data according to gap equation (٤.٤).*
Step٥:	*Embed the gap value in (LSB) of ٨ –consecutive, Bytes of STEGO file.*
Step٦:	*Embed L value inside the next ٤٢ gapped bytes of STEGO file.*
Step٧:	*Read the first byte of secret data.*
Step٨:	*While not (EOF) secret data do the following steps*
Step٩:	*Embed the secret bit in the LSB of cover image byte and append it to STEGO file.*
Step١٠:	*Copy image data between gaps to STEGO file without change from cover image.*
Step١١:	*Get the next secret bit then go to step ٧.*
Step١٢:	*End*

٤.١.٢.١.٢ LSB – Extraction

It is the art of extracting the hidden data embedded in the image.To accomplish this task the user who receive the STEGO image must has enough and sufficient information about the approach used to embed data.

LSB Extraction Algorithm

```
Input:    The STEGO image.
Output:   The hidden data or Secret i image.

Step١:    Retrieve the value of gap from ٨-consecutive bytes. After reading
          the offset of data.
Step٢:    Retrieve from the next ٤٢-gapped value secret file size(L),
          Set j= ٠
          While (j <L) do these steps (٥- ١٤)
Step٤:    Extract the secret data from LSB of STEGO file.
Step٤:    Extract the header of the reconstructed image.
Step٥:    Set sum= ٠, base= ١, i= ٠.
Step٦:    While (i< ٨) do the following steps (٧- ١٢).
Step٧:    Read the next byte (B) from STEGO file.
Step٨:    Extract the secret bit value from LSB of B.
Step٩:    Add the (LSB×base) to sum value.
Step١٠:   Set base =base× ٢.
Step١١:   Read image data between gaps, set i = i + ١ then go to step ٦.
Step١٢:   Append sum value to the reconstructed image file.
Step١٤:   goto step ٤
Step١٤:   End.
```

٤.١.٢.٢ DCT Steganography

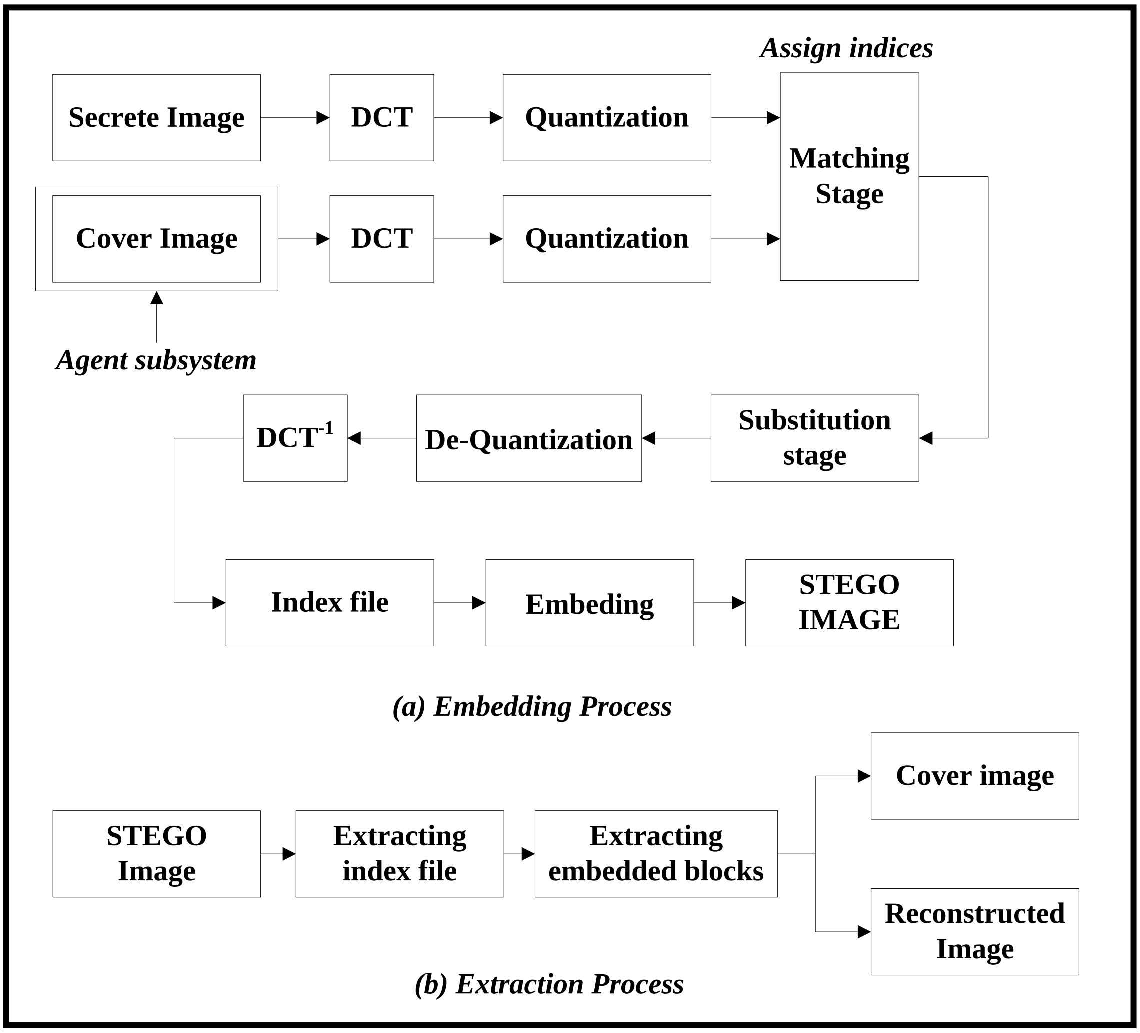
This steganography method is based on DCT transformation technique, the cover image and the embedded image are partitions into blocks of (n×n) pixels. In this method the value of (n) represents either (٢, ٤ or ٨). When the size of blocks decreases, distortion in the stego image will be less, or the STEGO Image quality is better.

٤.١.٢.٢.١ Transformation

These block will be transformed using DCT to get on blocks of (n×n) coefficient of real numbers. The equation (٤.١) is used to calculate DCT transformation for images:

$$T(u,v)=\alpha(u)\alpha(v)\sum_{i=0}^{n-1}\sum_{j=0}^{n-1}s(u,v)\cos\frac{(2i+1)u\pi}{2N}\cos\frac{(2j+1)v\pi}{2N} \qquad ...(٤.١٤)$$

Where:



$$\alpha(u)\alpha(v)=\begin{cases}\dfrac{1}{\sqrt{n}} & \text{if } \alpha(u),\alpha(v)=0\\[2ex]\dfrac{2}{\sqrt{n}} & \text{if } \alpha(u),\alpha(v)=1,2,\dots,n-1\end{cases}$$

Figure (٤.٤): The Structure of DCT Steganography System

And the inverse DCT computation perform according to this equation:

$$I(r,c)=\sum_{u=0}^{N-1}\sum_{v=0}^{N-1}\alpha(u)\alpha(v)C(u,v)\cos\left[\frac{(2r+1)u\pi}{2N}\right]\cos\left[\frac{(2c+1)v\pi}{2N}\right] \qquad ...(٤.١٥)$$

where:

$$\alpha(u)\alpha(v)=\begin{cases}\frac{1}{\sqrt{n}} & \text{if } \alpha(u),\alpha(v)=0\\[2ex] \frac{2}{\sqrt{n}} & \text{if } \alpha(u),\alpha(v)=1,2,...,n-1\end{cases}$$

After each (n×n) block of DCT coefficient is calculated, it is quantized to transform the real number to integer number. Each number in the DCT coefficient block is divided by the corresponding number (quantize number) and the result rounded to nearest integer.

The quantize is based on parameter R that is supplied by the user the equation (٤.٢) measure the quantization number:

$$Q_{ij} = ١ + (i + j) / R \qquad ...(٤.١٦)$$

Where:

i, j range from ١ to n.

R value is chosen as small value, so we get better STEGO image quality.

Transformation Algorithm

```
Input:    A Cover Image, the Secret Image.
Output:   Image contain $(n\times n)$ quantized coefficient.
step١:    Read block size (n).
step٢:    Split the Cover (embedded) image into blocks of $(n\times n)$.
step٤:    Set i, for I = ١ to Secret image blocks No. do steps (٤-٥).
step٤:    Calculate the DCT Coefficients for blocks [i] by performing equation
          (٤.٢).
Step٥:    Quantize each DCT coefficient results from step ٤ by using Equation
          (٤.٤)
Step٦:    Set I, for i= ١ to Cover image blocks No. do steps (٤-٥).
Step٧:    End.
```

٤.١.٢.٢.٢ Matching Stage

In this stage the position of embedded blocks of secret image inside the cover image are found by matching between blocks of secret and cover image, using the goodness of fit equation (٤.٤):

$$S = \sum_{i=1}^{n} \frac{(E_i - C_i)^2}{C_i} \qquad ...(٤.١٧)$$

where:

E: represent value of embedded image pixels.

C: represent value of cover image pixels.

n: represent the block size.

All blocks of the cover image will be searched and when the suited block will found to hold the embedded one it will be assigned, by a flag and will not be used again.

The algorithm start by assigned all the blocks as true, we select the first block from embedded image blocks and perform the equation ٤.٤ to find the best block among the cover block (that find similar blocks or that converge to it).

First we start searching to block that may have the same value, if it fail then will search to block with nearest value, and then it will save the position of block in a file.

Matching Algorithm

```
Input: The DCT quantize coefficients for Secret and Cover image.
Output: The index file that contain assigned blocks.

Step ١: Initialize all cover blocks to be unassigned.
Step٢: Set i, for i= ١ to Secret image blocks No. do steps (٤-٥).
Step٤: Set j, for j= ١ to Cover image blocks No. do steps (٤- ٦).
Step٤: Compute the fitness between blocks [i] and blocks [j] according to equation (٤. ١٧) for the unassigned blocks [j].

Step٥: Search for greater match from step ٤ by finding the smaller value of s then save it's location to loc.
Step٦: Set the Cover image blocks state at loc to be assigned.
Step٧: Append the indices of Cover image blocks to index file.
Step٨: End.
```

٤.١.٢.٢.٤ Substitution Stage

After we determine the fit blocks, substituted the blocks of secret image with cover image blocks (putting secret image blocks instead of cover image blocks).

Substitution Algorithm

Input:	*The DCT quantize coefficients for Secret and Cover image with index file.*
Output:	*The DCT quantize coefficients for Cover image with substituted DCT quantized Secret image blocks.*
Step١:	*Get the first index from the index file (Cx,Cy)*
Step٢:	*Set i, For i = ١ to secret image blocks No. do steps (٤-٥).*
Step٤:	*Set Sx, Sy to indexes for Secret image blocks.*
Step٤:	*Substitute Cover image index (Cx, Cy) by secret image blocks [i] of index (Sx,Sy).*
Setp٥:	*Get the next index from index file (Cx,Cy)***.**
Step٦:	*End.*

٤.١.٢.٢.٤ Hiding Stage

In this stage, the algorithm will hide the index file. Data hiding is method of hiding information, and the most common method is based on manipulating of least significant bit by directly replacing the LSBs of cover image with secret message in our approach the cover image is the STEGO image file.

Hiding Stage Algorithm

Input:	*Secret image, Cover image quantize DCT coefficient and index file.*
Output:	*The STEGO image.*
Step١:	*Create the secret information data file which consist of the header and RGB palette of secret image respectively.*
Step٢:	*Append the index file to the end of secret information data file.*
Step٤:	*Compute the size of secret information data file and append it to the Secret information file*
Step٤:	*For the embedding procedure repeat steps (٢- ١٢) from LSBs embedding algorithm.*
Step٢:	*Generate Gaps according to Gap equation (٤. ١٣)*
Step٤:	*Copy the header information and RGB palette from cover image in to STEGO image*
Step٤:	*Distributed secrete image data according to gap equation (٤. ٤).*
Step٥:	*Embed the gap value in (LSB) of ٨ –consecutive, Bytes of STEGO file.*
Step٦:	*Embed L value inside the next ٤٢ gapped bytes of STEGO file.*
Step٧:	*Read the first byte of secret data.*
Step٨:	*While not (EOF) secret data do the following steps*
Step٩:	*Embed the secret bit in the LSB of cover image byte and append it to STEGO file.*
Step١٠:	*Copy image data between gaps to STEGO file without change from cover image.*
Step١١:	*Get the next secret bit then go to step ٧.*
Step١٢:	*End*

٤.١.٢.٢.٥ Extraction Process

The extractor know all the important information to extract information, the algorithm will extract the embedded block by using the hidden locations, for each embedded blocks in cover image.

Extraction Process Algorithm

Input:	*The STEGO image file.*
Output:	*The reconstructed image or secret image file.*
Step١:	*Retrieve the value of gap from ٨ consecutive byte.*
Step٢:	*Retrieve from the next ٤٢ – gapped byte the value of secret image file size (L).*
Step٤:	*Reconstruct the header & RGB palette of reconstructed image from the next gapped Byte.*
Step٤:	*Reconstructed the block size H, and the block size W.*
Step٥:	*Reconstructed the index file in order to know the hidden location equivalent to each embedded block inside the stego image.*
Step٦:	*Transfer the embedded blocks from the Stego image to get on reconstructed image.*
Step٧:	*End.*

Chapter Six
CONCLUSION AND FUTURE WORK

٦.١ Introduction

In this chapter, a list of remarks derived from the investigation of case results shown in chapter four will presented. Also, some suggestions for a future work, that may enhance the system efficiency, are presented.

٦.٢ Conclusion

From the case study results conducted on the proposed system, the following remarks were derived.

٥. **The use of agent which indicates what part of system should be treated as agent, and links between agent and other part of non agent software. The agent subsystem help to identify component which is offer benefit.**

٦. **The agent make a decision. In this work we have analyzed different parameters ruling the agent . The agent we dealt with have information about cover image and can adapted to BMP type of cover image.**

٧. **The goal of steganography is to avoid attacker from discovering the secret messages embedded in the cover image. to improve security**

level we must obtain acceptable STEGO image quality. Overall, the proposed system match the requirement to obtain acceptable STEGO image.**agent subsystem which make a decision for the suitable steganography method and best cover-image to hold the secret image, since the choice of the cover-image is important. and according to the condition that is ruled the agent behavior we get the most acceptable STEGO image quality which is clear from the objective test measurement, for these two steganography methods the LSB-steganography and the DCT- steganography methods.**

٦.٣ Future Work

During the development of the proposed system, many suggestion for future work was emerged to increase the system efficiency, among these suggestion are the following:

١. **Analyzing more image features that may effect on the STEGO image quality.**

٢. **Using mobile agent which help us to manage request of the image and Finding an image more effectively and efficiently. Searching made easy, or providing image from internet, by determine the address of the URL .**

٣. **develop the system to make the agency architecture "multi –agent " model to develop the efficiency of the system .**

Chapter Four

AGENT PRINCIPLE

٤.introducton

The advantage of software agents gave arise to much discussion of just what such an agent is, and of how they differ from programs in general. The agent should strive to act in our best interest. what does this mean ," to act in our best interest"?, that it should do its best to satisfy our information need, And an agent knows what services its capable of providing. The agent can be implemented and visualize in several way, it should not be restricted to one type of media. Finding the best type of visualization and suitable interface is a research area in its self. One agent might be visualize with high-quality video animation while another *just generating text* .

٤.١ What is Agent?

As is to be expected from a fairly young area of research. There is not yet a universal consensus definition of an agent. However, the Wooldridge and Jennings definition:

As Agent is a computer system that is situated in some environment and that is capable of autonomous action in this environment in order to meet it design objective.

This definition is increasingly adopted, and it is probably fair to say that most researchers, in the field when asked to provide their definition will mention various properties.

Let us note that we are talking about (software agent) whenever or any other researchers in the field say (agent), we really mean software agent. The typical dictionary definition of the agent, as an entity having the authority to act on behalf of another[٨].

Number of definitions of agent have been propounded over the years. Some definitions emphasize the agent in user interface typically with some sort of persona, typically represented in some suitable graphical manner. Such a kind of agent is not of direct relevance to the present topics. The more promising class of definitions state that an agent is "capable of interacting with other parties".

Some definitions were tied to specific implementation technology such as being based on theorem provers, or using internal data structure corresponding to the so-called mentalist concepts, such as beliefs or knowledge، goal or desires, intention, and so on.

So , a good working definition of agent is that[٧]:

It is a persistent computational entity that can perceive، reason, Act, and communicate.

٤.٢ Agent Property

The basic properties of software agent are :

- **Autonomous:** being autonomous, mean that agents are independent and make their own decision, this is one property that distinguish agent from object.

The second property:

- **Situated ness:** dose not constrain the notion of an agent very much since virtually all software's can be considered to be situated in an environment[٨].
- **Flexibility:** can be defined to include the following property:
  i. **Responsive**: Refer to agent ability to perceive its environment and respond in a timely fashion to change that occur in it.
  ii. **Pro-active**: Agent are able to exhibit opportunistic, goal –driven behavior, and takes initiative where appropriate
  iii. **Social**: Agent should be able to interact, where appropriate, with other agent or human in order to solve their own problem and help others with their activities.

٤.٤ Agent Classification

The various definition discussed above involves a host properties of an agent. Having settled on a much less restricted definition of an agent, this property may help us further to classify agents in useful ways.

Agent may be usefully classified according to the subset of these properties that they enjoy. Every agent by our definition, satisfies the first four properties. Adding other properties reduces

potentially useful classes of agents, for example, mobile, learning agent. Thus, a hierarchical classification based on set inclusion occurs naturally.

There are of course other possible classifying schemes, for example, we might classify software agent according to the tasks they perform, for example, information gathering agents or email filtering agent, or we might classify them according to their control architecture, sumpy, then would be fuzzy subsumption agent, while etzion and weld’s softbot would be planning agent, also agent could be classified by the range and sensitivity of their senses, or by the much internal state they possess.

٤.٤.١ A natural kind taxonomy of an agent

in thinking about a taxonomy of agents two possible model come to mind, the biological model and mathematical model. The biological taxonomy take the form of a tree with "living creatures " at the root and individual species at the leaves[٤٤]. At the kingdom level let's classify our agents as either biological , robotic or computational , as these seem to be natural kinds. every cultural and even very young children readily distinguish between animate organisms, artifact and abstract concept . We can reasonably sub classify computational into software agents and artificial life agent and we can sub classify software agent into task specific agent and entertainment agents, and computer viruses[٢٤].

٤.٤ Agent Environment

Typical agent environments are:

I. Dynamic.

II. Unpredictable.

III. Unreliable.

These environment are dynamic in that they change rapidly. By rapidly we mean that the agent can't assume that the environment remains static while trying to achieve a goal.

These environments are unpredictable in that it is not possible to predict the future states of an environment, often for agent is not possible to have perfect and complete information about its environment and because it is being modified in ways beyond the agent's knowledge and influence.

Finally the environment are unreliable in that the action the agent can perform may fail for some reasons that are beyond an agent's control. For example a robot attempting to lift an item may fail for wide range of reasons including the item being too heavy[٨].

٤.٤.١ Agent Operate on Local Data

The agent in this environment would be limited to operating on the local data but still be extremely useful. Such an agent might be an alert agent in banking environment for certain condition of liquidity or dept.

The agent might flash a warning on an officer's screen or perhaps when a stock price reaches a certain level and then it buys or sails[٢٤].

٤.٤.٢ Agent Operate on The Internet

As the number of computers in the network grows they become accessible to use agents to act on the distribution data to become more valuable. For that reason, the internet with its million of hosts is the ideal environment for agent to be useful and therefore to stimulate the growth of underlying technology that agent works[٢٤].

٤.٥ When To Use Agents

it is important to consider what part of a system should be treated as agents and designed using an agent oriented methodology(such as Prometheus). and also how the link between an agent sub-system and non agent software implemented.

Not all software components are best viewed , modeled and designed as agents. Some time , you will be designing a system where it make sense to model it entirely as a multi-agent system. However, this is not always the case. Some sub-system may not make sense or may not benefit from being viewed as a collection of agents. For example an image processing sub-system that extract the position of a ball from video frames will not benefit from being viewed as an agent or as a system of agent.

The following question can be used to help identify component that should be treated as agents

- Is it autonomous?
- Does it have a goal?
- Viewed as an object, is it active?
- Does it do multiple thing at once? if so does it need reason about interaction between different activities?
- Does it need to change the ways it need to do thing on the bases of changes in its environment?

If the answers to these question are: mostly

'yes' you should probably think of component as agents[٨].

٤.٦ Concept for Building Agents

We define agents as having a number of properties such as being situated, reactive and proactive. We being to look at how we can design and build a software that has these properties, by considering what concept leads to an agent having certain properties. For example in order for an agent to be proactive, it needs to have a goal. Thus the concept of a goal is an important one for designing and building a proactive agent[٨].

We began our definition of an agent with the basic property that an agent software that is situated in an environment. Two concept that capture the interface between an agent and its environment are :

PERCEPT: its from the environment.

ACTION: that the agent performs to effect the environment.

An important aspect of proactiveness is persistent of goals if a plan for achieving a goal fails, then the agent will consider alternative plans for achieving a goal in question، until it is believed impossible or it is no longer relevant.

AN EVENT: is a significant occurrence that the agent should respond to in some way. Events are often extracted from percept, although they may be generated internally by the agent.

For example, on the basis of a clock, an event can trigger a new goal, cause a change information about the environment and/ or cause an action to be performed immediately. an Action generates directly by an event·

Events are important in creating, reactive agent in that they identifies an important change that the agent needs to react to·

Percept can be seen as particular kinds of events that are generated with in the environment. We note that the percept may well have to be interpreted from the raw data available، in order to provide the percept/ event that has significance to the agent.

Particularly if the raw data is an image data, it is likely to require a significant process.

A PERCEPT: Is an item of information received from the environment by some sensor for example, a fire fighting robot

may receive information such as the location of a fire and indicate its intensity. An agent may obtain information about environment through sensing action.

AN ACTION: Is something an agent does, as moving north or squirt. Agent are situated, an action is basically the agent ability to effect its environment. In their simplest forms, actions are atomic and instantaneous and either fail or succeed.

Also we want our agent to be **proactive** and **reactive:**

The agent proactive ness implies the use of a goal .A reactive agent is one that will change its behavior in response to the change in the environment.

An important aspect in decision making is balancing proactive and reactive aspect. On one hand we want the agent to stick with its goal by default and on the other hand we want it to take the changes in the environment Into account.

The key to reconciling these aspects, thus making agent suitably reactive, is identifying significant changes in the situation. These are event.

A GOAL:I 's Variously called task, objective, aim or desire of something. The agent works on or towards, for example, extinguishing fire, or Rescuing – civilians. Often goal are defined as states of the world that the agent wants to bring about.

However, this definition does not allow some type of goal to be expressed such as maintenance goals (e.g maintain cruising altitude), Avoidance goal or safety constrain (e.g never move the table while the robot is drilling). Goals give the agent its autonomy and reactive ness[٨].

٤.٧ Trust

Agent need to be able to make decision based on information received and collected from other entities. In order to make these decision they need to be able to evaluate the trust worthiness of the information or the information source . A mobile agent need to decide whether or not to transfer to , and execute on, a particular host.

the issues surrounding trust with an agent systems are currently attracting much research with in an agent community. Various mechanism for agents to reason about trust have been proposed. trust mechanism based on reputation are one approach suggested by a number of author[٤٢].

٤.٨ Examples of Agent System and Application

From the practical perspective, intelligent agents are the most popular AI technology in recent years. Agent systems and applications are numerous, and agent-oriented software engineering opens a wide door to the analysis and design of many software systems using intelligent agents. Amongst the application domains, where agents have been applied so far, are electronic commerce, information gathering on internet, interface technology, network monitoring and control, business Process management, industrial system management, distributing sensing, factory process control, etc.

The following systems and applications are just a few recent examples that illustrate some characteristic application domains.

- **MARS–based searcher agents:** searcher agent applications typically send out mobile agent to remote internet sites to analyze HTML pages and extract information without transfering the pages over the network. For example, a searcher agent can find and return the URLs of pages containing a specific key word. In all such applications, appropriate coordination between an agent and other agents and resource in the execution environment is of a fundamental importance.

- **Fuzzy intelligent agents in eCommerce:** web advertising is essential in e-commerce، current visitors actions, and deciding about his/ her possible interest in the advertiser's service.On behalf of the advertiser, the agent determines a bid to make its ad appear to the visitor. The point is that all the advertising agents receive information about the visitor simultaneously. Each agent then processes the information using its own knowledge base and then bids to make its ad appear. These bids are converted into probability distribution that is used to determine which ad appears to the visitor. An advertising pays the web site not for fixed number of units but in proportion with bids. In the fuzzy rules in the agents knowledge bases, the antecedent variables (Vi) corresponds to characteristic useful in describing a site visitors[٢٥].

- **Microsoft agent:** Microsoft agent is a set of programmable software services that supports the presentation of interactive animated characters with in the Microsoft interface. Developer can use characters as interactive assistants to introduce, guide, entertain, or otherwise enhance their web pages or application in addition to the conventional use of windows, menus, and controls. Microsoft agent enables software developers and web authors to incorporates a new form of user interaction, known as *conversational interface* that leverages natural aspect of human social communication. In Addition to mouse and keyboard input, Microsoft Agent includes optional support for speech recognition so application can respond to voice commands. Characters can respond using synthesized speech, recorded audio, or text in cartoon word balloon[٢٦]

- **The Maes Agent :** Autonomous agents are computational systems that inhibit some complex dynamic environment, senses and act autonomously in this environment , and by doing so realize a set of goals or tasks for which they are designed. **Pettie Maes** Agent is one of the pioneer**s** of agent research **.**She adds a crucial elements to her definition of an agent : agent must act autonomously so as to " realize a set of goal [٢٤].

- **The IBM Agent :** intelligent agents are software entities that carry out some set of operation on behalf of a user or another program with some degree of independence or autonomy , and in so doing employ some knowledge or representation of user goal of the users goal or desires. This definition , from IBM's Intelligent agent strategy white paper , views as intelligent agent as acting for another with authority granted by another. atypical example might be an **information gathering agent**[٢٤].

- **The Hayes–Roth Agent:** intelligent agent continuously perform three function :perception of dynamic condition in the environment , action to effect condition in the environment; and reasoning to interpret perception ,solve problems, draw inferences, and determine action.

  Barbara hays Roth of Stanford 's Knowledge system Laboratory insist that agent reason during the process of action selection. If reason interpreted broadly, her agent architecture does allow for reflex action as well as planned action[٢٤].

Chapter Five
RESULTS AND CASE STUDY

٥ Introduction

There are two types of fidelity criteria, namely, the objective and the subjective criteria. The first one provides us with equations that can be used to measure the amount of the error in the reconstructed image, where as the second requires the definition of the qualitative scale to assess image quality.

the objective measures which are Commonly used include peak signal-to-noise ratio (PSNR), correlation test[٢٢].

٥.١ Peak Signal -To- Noise Ratio Test (PSNR db)

To describe the quality of the STEGO image precisely, we use the value of the peak signal -to- noise ratio (PSNR) to judge the similarity between the host image and the *STEGO* image. The (PSNR) function is defined as follows[٣٨]:

$$\mathrm{PSNR} = 10\log_{10}\frac{(\mathrm{L}-1)^2}{\mathrm{MSE}}\,\mathrm{db}$$ *...(٥.١)*

Where:

L = ١, ٢, ..., ٢٥٦

PSNR is measured in *decibel* (db). Here MSE is the mean square error. Subsequently, we define MSE as follow:

$$\mathrm{MSE} = \frac{1}{(\mathrm{WH})}\sum_{i=1}^{w}\sum_{j=1}^{H}\left(\alpha(\mathrm{I,J}) - \beta(\mathrm{I,J})\right)^2$$ *...(٥The*

symbol $\alpha(I,J)$ and $\beta(I,J)$ separately represent the pixels value of the host image and the STEGO image in position (I,J), and W and H represent the width and height of image separately[٢٨].

٥.٢ Correlation

This test measures the similarity between two image and can be defined as follows[٢٨]**:**

$$\mathrm{Cor} = \frac{\sum_{r=1}^{N}\sum_{c=1}^{M}(\mathrm{I}_1(r,c) - \bar{\mathrm{I}}_1)(\mathrm{I}_2(r,c) - \bar{\mathrm{I}}_2)}{\sqrt{\left[\sum_{r=1}^{N}\sum_{c=1}^{M}(\mathrm{I}_1(r,c) - \bar{\mathrm{I}}_1\right]\left[\sum_{r=1}^{N}\sum_{c=1}^{M}(\mathrm{I}_2(r,c) - \bar{\mathrm{I}}_2\right]}}$$ *...(٥.٣)*

Where:

Ī١: is the mean of the original image I١(r, c) that is:

$$\bar{\mathrm{I}}_1 = \frac{1}{\mathrm{M} \times \mathrm{N}}\sum_{r=1}^{N}\sum_{c=1}^{M}\mathrm{I}_1(r,c)$$ *...(٥.٤)*

Ī٢: is the mean of the modified image I٢(r, c) that is:

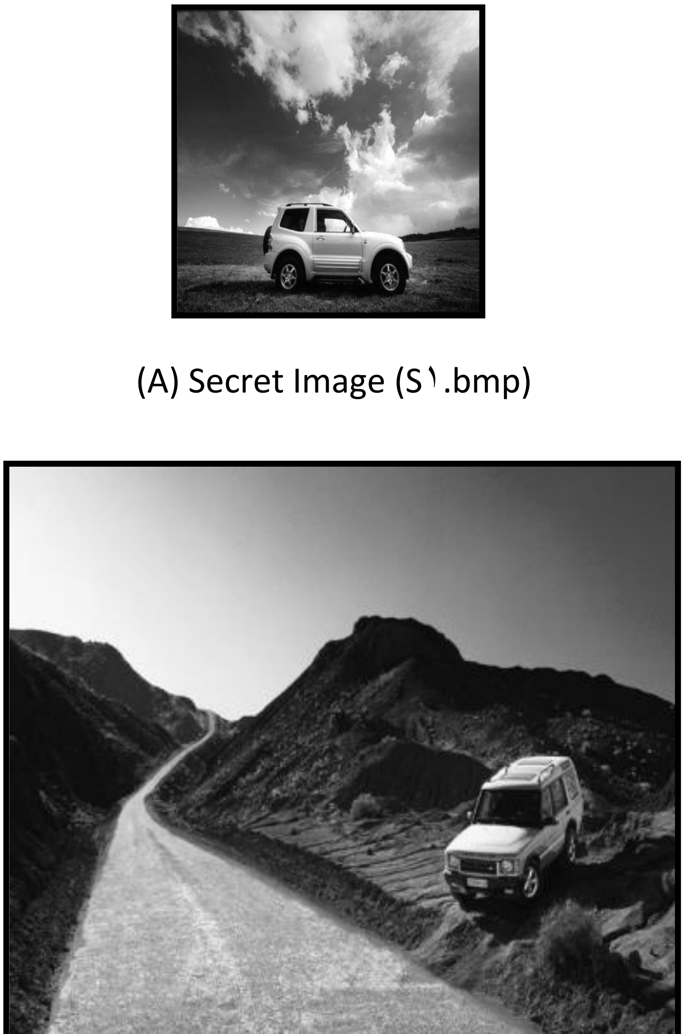
$$\bar{\mathrm{I}}_2 = \frac{1}{\mathrm{M} \times \mathrm{N}}\sum_{r=1}^{N}\sum_{c=1}^{M}\mathrm{I}_2(r,c)$$ *...(٥.٥)*

If the correlation is equal to ١; this means that the two image are perfectly similar.

٥.٣ Make Decision with Agent Subsystem for (DCT-Steganography)

The agent chooses one cover image from the image database and specified a DCT-steganography method for selected secret message (image) and then give the user a recommendation according to the features of cover image with similarities and dissimilarities measurement between the cover and secret image that the agent depend on . So , the agent select the specific steganography

method with the best cover for the selected secret message (Image). The results are as follows:



(A) Secret Image (S١.bmp)

Figure (٥.١)

The cover image (C١. bmp) is selected from the image database by an agent. The visual quality of STEGO image is much better than that obtained when we select the cover image arbitrary from image database.

Table (٥.١): C١.bmp features& (SD) measure

Mean	١١١.٥٨٥٨
Entropy	٧.٧٦٣٦١٨
Variance	٥٩١٨.٥٩١
Contrast	٧٠.١٣٢٦٧
Similarities	٢.١١٥٢٠٨e-٠٢١
Dissimilarities	٠.٥٥٥١٠٥٣

The Similarity measure between the pixels is a fundamental step in many image processing algorithm. Agent will measure the similarities and dissimilarities between the cover and the selected secret messages (images). If the conditions are satisfied then the cover image with the best features of variance, entropy, mean ,contrast, similarity and dissimilarity measure will be selected by the agent and then will specify the steganography method which it is DCT-steganography. Similarities is measured between the blocks of the cover image and the secret image is calculated.

The Image features that the agent subsystem depends on are the mean ,energy values, maximum contrast and variance since the cover image with maximum variance is recommend for image steganography. The agent also choose image in image database with high entropy value.

Table (٥.٢): The objective measures for S١.bmp & C١.bmp chosen by agent subsystem according to image feature

Block size	Quantize value R	PSNR(db)of	Correlation

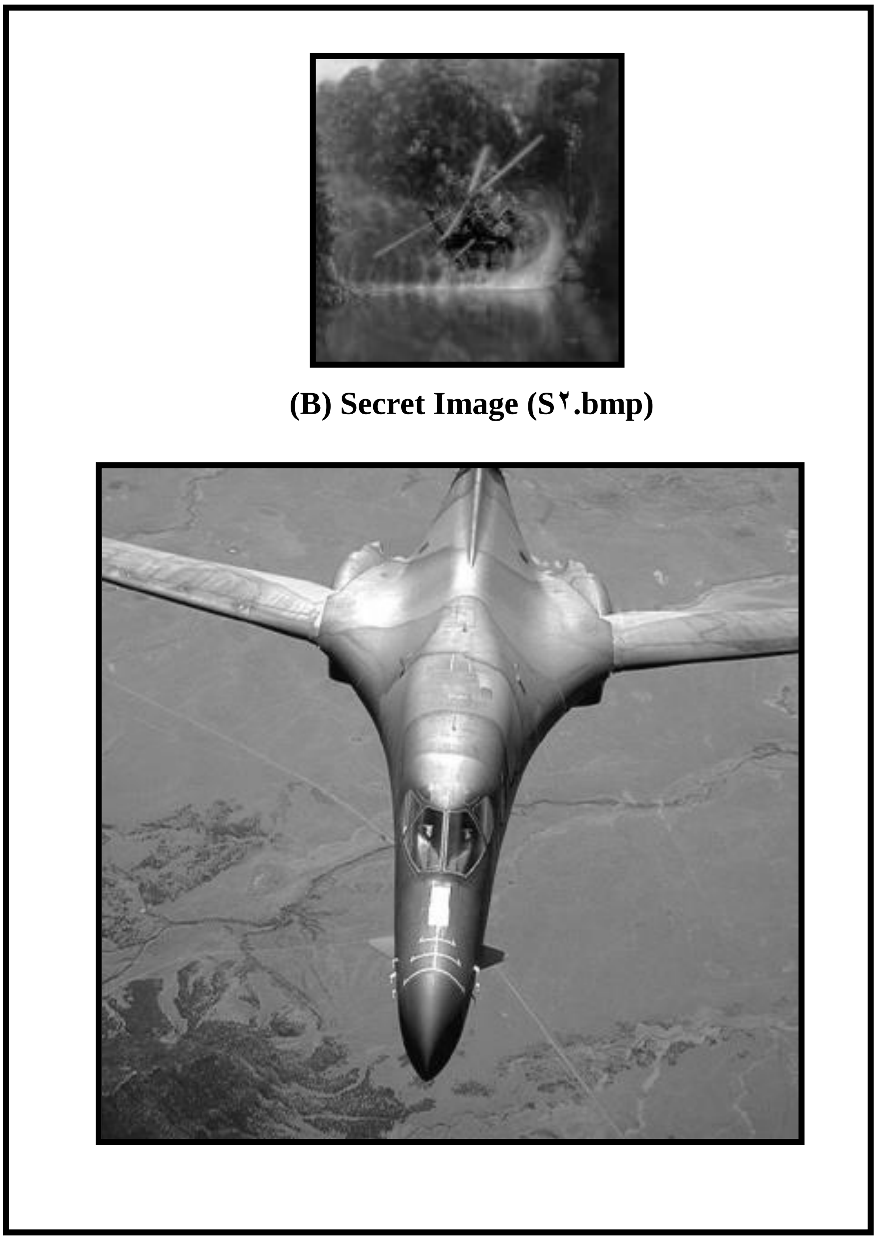
		Cover &STEGO	
٢	٠.١	٣٠.٥٩١٣	٠.٩٩٨٣٦٦
٥	٠.١	٢٥.١٨٣٧	٠.٩٩٥٣١٥
٨	٠.١	٢٢.٢٠٧٦	٠.٩٨٨٦٩٨

The block size, that is either (٢, ٥, ٨) affect the quality of STEGO image as we have mentioned and best result (maximum PSNR) is obtained when (n) or block size = ٢ and with R = ٠.١. From the previous example, although the block size chosen = ٢ and the R = ٠.١, the STEGO image has been distorted and it is distinguishable in the first case. The best STEGO image is obtained when the media (cover image) is chose, by the agent subsystem among the images in image database. The agent subsystem will select one cover image and it gives us a good STEGO image quality with maximum PSNR.

Figure (٥.٢): STEGO Image

٥.٥ Make Decision with Agent Subsystem for (LSB-Steganography)

When the agent fails to find best cover image for DCT-steganography for the selected secret image, the agent choose the cover image (best cover image) for the selected secret image that is satisfied for LSB steganography. Depending on agent selection, in which an agent determine the number of ٠'s and ١'s of the cover image and the transition coefficient and according to (Err) value that is equal to ٠.٠٠١ .In addition the features of cover image entropy ,contrast, variance,…etc is considered. The results are as follow:



(B) Secret Image (S٢.bmp)

(C) Cover image (C٢.bmp)

Figure (٥.٣)

Where S٢.bmp is the secret image that we want to embed it inside the host image (cover image), C٢. bmp will be chosen by the agent, as we noticed the image format is **BMP** since agent will reject any other format Like JPEG, JIF, …etc.

Table (٥.٥): C٢. bmp features& Randomness

Mean	١٢٩.٥٩٣١
Entropy	٦.٨٥٥١٠٨
Variance	١٣٣١.٨٩٣
Contrast	٣٦.٥٩٥١١
R٠٠	٠.٢٥٠٥٣٥٢
R٠١	٠.٢٥٩٨٥٣٦
R١٠	٠.٢٥٩٨١٦٥
R١١	٠.٢٥٩٩٠٥٨
R٠	٠.٥٠٥٠٣٥
R١	٠.٥٩٥٩٦٥

A further analysis for those transitional coefficients reveal that there exists a weak correlation between the LSB bit plane and the neighboring bit. So the probability of the occurrence of bit ١'s followed by bit ٠'s is approximately equal to ٠.٢٥ and the same for other transition that we notice from table(٥.٥) they are approximately equal to ٠.٢٥, since the probability of two "in depended" events equal to the probability of the first event multiplied by the probability of the second event. The probability distribution of number of ٠'s is approximately equal to ٠.٥ and probability distribution of ١'s is approximately equal to ٠.٥.

Figure (٥.٥): STEGO Image

Table (٥.٥): The Objective measures for S٢.bmp & C.bmp

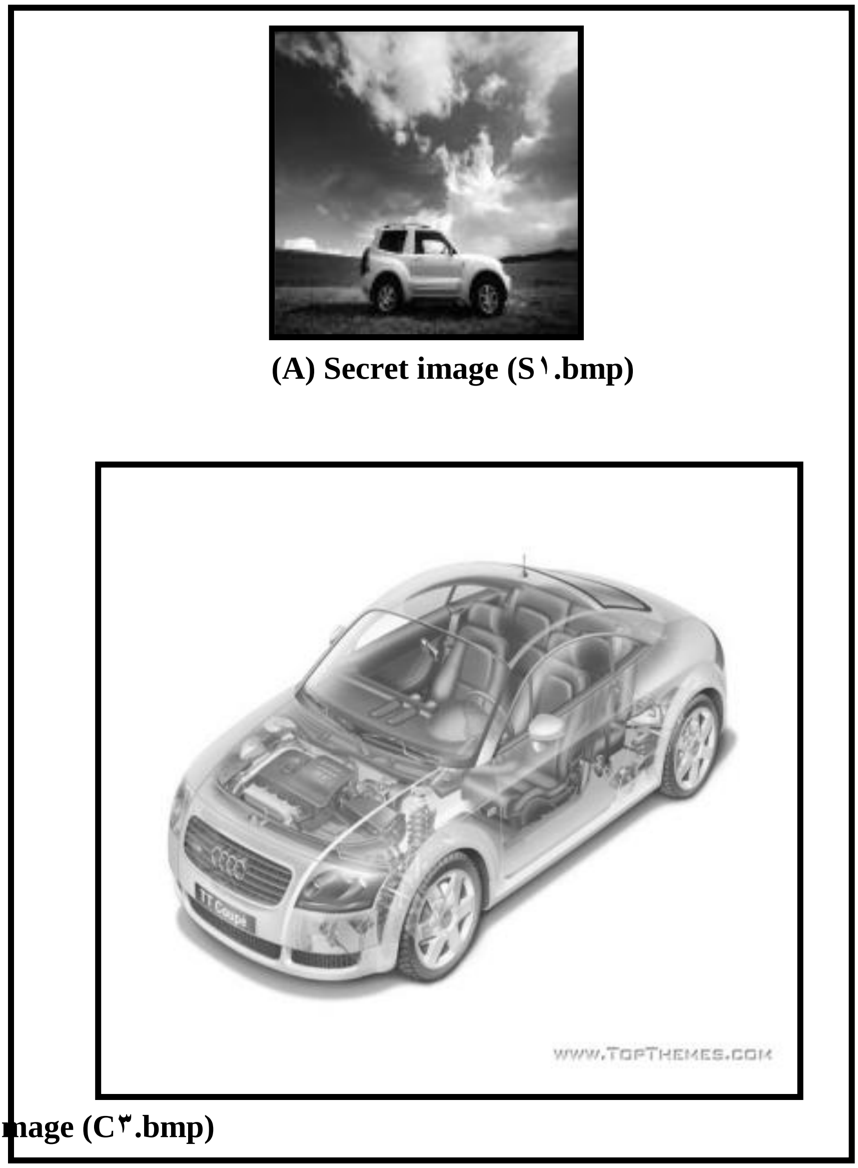
PSNR(db)	***CORELATION***
٥١.٣٩٥٦	٠.٩٩٩٩٨٧

As we have noticed ,PSNR value is better when the steganography agent chooses the (cover image and steganography method) for the selected secret message. The maximum PSNR is the best candidate.

٥.٥ Manual Using of DCT-Steganography System

First of all , a secret image is chosen, then the cover image is selected arbitrarily. after that the effect of block size and the quantized value R that is effect the STEGO image quality is tested, and we chose R value as small value .

Case ١:



(A) Secret image (S١.bmp)

(B) Cover Image (C٣.bmp)

Figure (٥.٥)

Table (٥.٥): C٣.bmp features

Mean	٢١٩.٧٥٦٥
Entropy	٥.٠٢٥٢٧١
variance	٢٦٧٥.٩٣٦
Contrast	٥١.٧٢٩٥٥

Figure (٥.٦): STEGO IMAGE

We choose the secret image (S١.bmp) that we want to embed inside the cover image, then we arbitrarily selecte a cover image (C٣.bmp) from image database .The features of the (C٣.bmp) is shown in table (٥.٥).

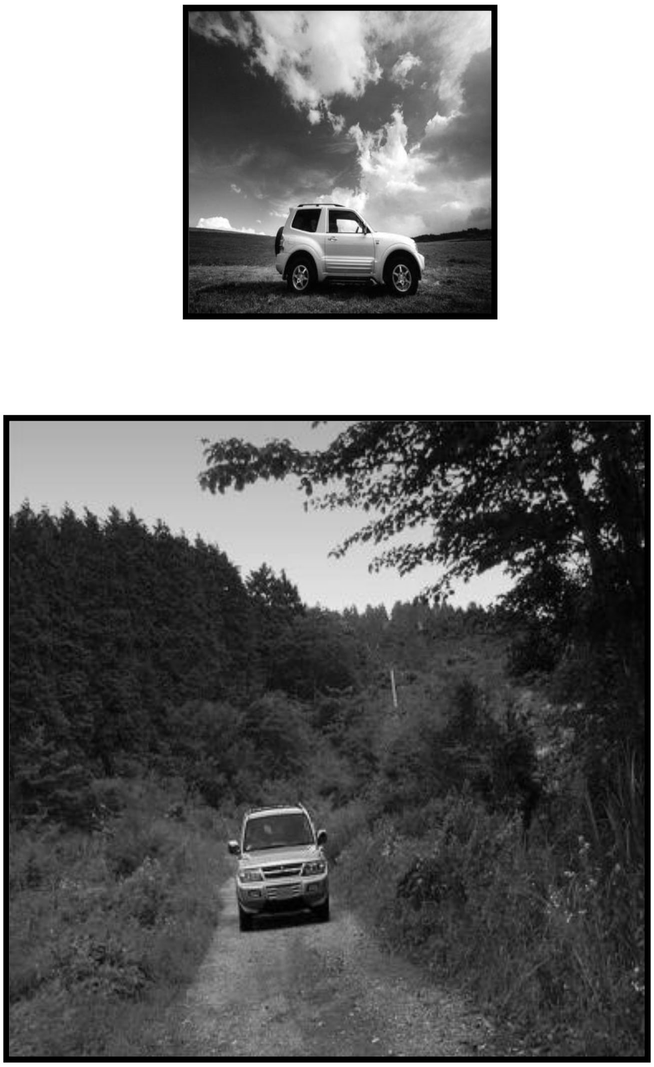
The results of the objective test are as follows:

Table (٥.٦): The objective measures for S١.bmp & C٣.bmp according to different block size n (i.e, n= ٢, ٥ or ٨) and R = ٠.١.

Block size	Quantize value R	PSNR(db)of STEGO & cover	Correlation
٢	٠.١	٢٥.٥٧٥٩	٠.٩٩٧٧٨١
٥	٠.١	٢١.٨٠٠٥	٠.٩٩٠٩٣٥
٨	٠.١	١٨.٥٩٢٦	٠.٩٩٠٩٣٥

The Maximal value among all values of PSNR, it's corresponding STEGO image is most similar to the host image (Cover image)[٣]. The block size = ٢. and quantize R value = ٠.١.

Case ٢:



(A) Secret image (S١.bmp)

(B) Cover Image (C٥.bmp)

Figure (٥.٧)

Table (٥.٧): C٥.bmp features

Mean	٧٢.٨٨٢٥٣
Entropy	٧.٢٧٠٧٧
Energy	٧.٨٥٧١٨٥e-٠٠٣
Variance	٢٩٧٨.٩٥٣
Contrast	٥٥.٥٧٩٦٩

As we have noticed that the value of features variance, entropy and contrast is high for this selected cover image, but the similarity, and dissimilarity conditions are not satisfied .

Figure (٥.٨): STEGO Image

Table (٥.٨): The objective measures for S٢.bmp & C٥.bmp according to different block size n (i.e, n= ٢, ٥ or ٨) and R = ٠.١.

Block size	Quantize value R	PSNR(db) of STEGO&cover	Correlation
٢	٠.١	٢٨.٩٣٨٥	٠.٩٩٥٩٨٢
٥	٠.١	٢٣.٥٥٨٩	٠.٩٨٢٢٧٢
٨	٠.١	٢٠.٦٠٥١	٠.٩٦٥٧٨٨

The PSNR value results are better than the previous example due to the image feature.

٥.٦ Manual Using Of LSB – Steganography System

If agent subsystem fails to find the best cover image for DCT steganography method, then LSB steganography will be chosen by agent subsystem.

LSB STEGANOGRAPHY SYSTEM: We choose the cover image for the selected secret image arbitrarily first and we get the following results:

Case ١:

TT Coupé
WWW.TOPTHEMES.COM

(A) Secret image (s٢.bmp)

(B) Cover image (C٣.bmp)

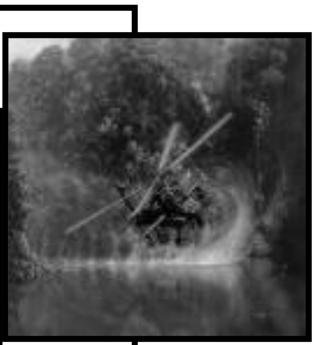
(C) STEGO image

Figure (٥.٩)

Table (٥.٩): The Objective measures for S٢.bmp & C١.bmp

PSNR(db) of STEGO&Cover	CORELATION
٥١.٠٨٦٣	٠.٩٩٩٩٩٦

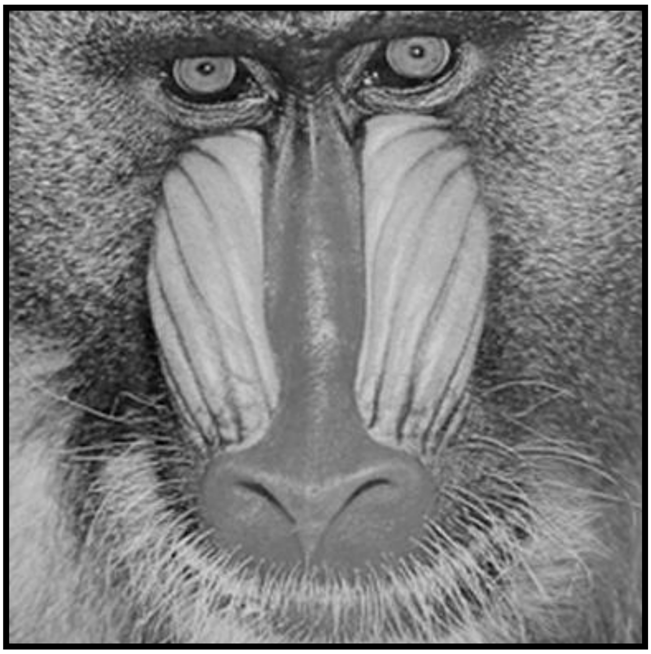
Case ٢:



WWW.TOPTHEMES.COM

(A) Secret image(S٢.bmp)

We choose baboon. bmp arbitrary selected as cover image .



(B) Cover image (C٥.bmp)

Figure (٥.١٠)

Table (٥.١٠): C٥.bmp features**&Randomness**

Mean	١٢٧.٥٨٥
Entropy	٧.٢٦٢٨١٦
variance	١٥٣٠.١٠٥
contrast	٣٩.١١٦٥٥
R٠	٠.٥٠٥٠٣٥
R١	٠.٥٩٥٩٦٥
R٠٠	٠.٢٢٧٥٣٥٨
R٠١	٠.٢٧٢٦٠٨
R١٠	٠.٢٧٢٦٢٨٥
R١١	٠.٢٢٧٢٢٨٨

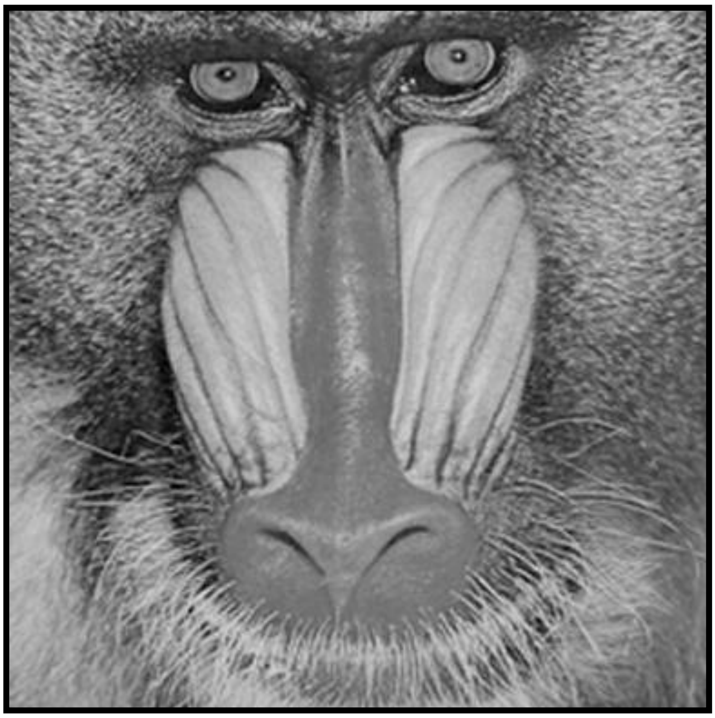


Figure (٥.١١): STEGO Image

Table (٥.٦): The Objective measures for S١.bmp & C٥.bmp

PSNR(db)of cover and STEGO	**CORELATION**
٥١.٣٩٣	٠.٩٩٩٩٨٧

Reference

١. Sorina D., Xiaolin W, and Zhe W., "*Detection of LSB-Steganography via sample pair analysis*", Electronic and computer engineering department, McMaster university Hamilton, Ontario, Canada L٨S ٤Ki, ٢٠٠٣.

٢. Jessica. F., MIroslav. G. , and Dorin H. , "*Steganalysis of JPEG Images: Breaking the F٥ Algorithm*", department of electric and computer engineering, SUNY Binghamton, NY ١٣٩٠٢-٦٠٠٠, USA, ٢٠٠٣.

٣. Chin-Chang, Tung-Shou C. and Lou-Zo C., "*A steganography method based upon JPEG and quantization table*", information engineering and computer science department, national Chung Cheng university, ١٤١, pp. ١٢٣-١٣٨, ٢٠٠٢.

٤. Ning L. and K. P. S. , "*Vector quantization based scheme for data embedding for image. "*Network and communication laboratory, department of computer and electronic engineering, Steven institute of technology, HOBOKEN, NJ٠٧٠٣٠, ٢٠٠٤.

٥. Boris Sh., Jessica F., and Moidring P, "*Hidding Data in DNA*", computer science department, university of California, Los angles, LNCS ٢٥٧٨, pp. ٣٧٣-٣٨٦, ٢٠٠٣.

٦. Bigus Joseph P. and Jennifer, "*Constructing Intelligent agent with java*", A programmer Guide to smart Application, New York, ١٩٩٨.

٧. Federico B., Marie-Pierre. G. and Franco. Z., "*Methodology and software engineering for agent system*", KLUWER ACADEMIC PUBLISHERS, ٢٠٠٤.

٨. Padgham & Michael Winikoff, "*developing intelligent agent system* "JHON WEILY & SONS, ٢٠٠٠.

٩. Katzenbeisser and F. A. P. Petitcolas," *information hiding techniques for steganography and digital watermarking*", ARTECH HOUSE, ٢٠٠٠.

١٠. Thia D. H. , Zensho K. , and Yen-Wei C. ," *ICA Based Robust logo image watermarking"*, department of EEE, faculty of engineering, University of RyuKus, Okinawa ٩٠٣-٠٢١٣, Japan, and institute of computational and engineering, Ocean university of china, ٢٠٠٤.

١١. Neil. F. Jhonson, Z Duric, and S. Jajodia, "*information hiding: steganography and watermarking*", KLUWER ACADEMIC PUBLISHERS ٢٠٠١.

١٢. Zaid. K. Ibrahim, "*Image based steganography system*", computer Science Department Al-Nahrain university, Baghdad, Iraq, MSc. thesis, ٢٠٠٢.

١٣. K. Gopalan, "*Cepstral Domain modification of audio signals for data embedding preliminary results"* department of engineering Purdue University Calumet, Hammond, IN ٤٦٣٢٣,٢٠٠٤.

١٤. Andrew D. Ker, "*Quantitative Evaluation of pairs and RS steganalysis"*, computing laboratory, Oxford university, England, ٢٠٠٤.

١٥. S. Areeponsga, Y. F. Syed, N. Kawamnerd, and K. R Rao, *"Steganography for low bit rate wavelet image coder",* http://issu. gmu. edu/~njohnson/steganography.

١٦. Mehmet U. C, Gaurav S. and A. Murat T. , *"Universal Image steganalysis using Rate-Distortion Curve"* ,university of Rochester, NY, USA, ٢٠٠٤.

١٧. Lala Z. Avedssian, "*Image in Image Steganography system*", computer science and information system department university of technology, Baghdad, Iraq, Ph. D. Thesis, ٢٠٠٠.

١٨. Jessica F. and Miroslav G. ,"*On Estimation of secret message Length in LSB-Steganography in Spatial Domain*", Department of electrical and computer engineering, SUNY, BINGHAMTON, NY ١٣٩٠٢-٦٠٠٠.

١٩. Jain ZH. and Eckard K. , "*A generic Digital Watermarking Model*", Fraunhofer Center for research in computer graphic, RI ٠٢٩٠٣,USA, vol. ٢٢, No. ٤, pp ٣٩٧-٤٠٣, ١٩٩٨.

٢٠. Katzenbeisser and F. A. P. Petitcolas, "*Information hiding techniques for steganography and digital watermarking*", ARTECH HOUSE, ٢٠٠٠.

٢١. David Salamon, "*Data compression*", SPRINGER-VERLAG New York,١٩٩٨.

٢٢. Scott E. Umborgh, "*computer vision and image processing a practical approach using CVIP tools*", PRENTIC HALL, ١٩٩٨.

٢٣. Stan Franklin and Art. G. "*It is An Agent or just a Program? A taxonomy for Autonomous Agent*" institute for intelligent system, university of Memphis, Springer-verlag, ١٩٩٦.

٢٤. Mariam. S. AL-braheem, "*Interface Agent for Database System*", computer science department university of technology, Baghdad, Iraq, M. Sc. thesis, ٢٠٠٥.

٢٥. Abeer T. AL-Obiady, "*Mobile intelligent agent for E-commerce Knowledge base building", *computer science department, University of technology, Baghdad, Iraq, M. Sc. thesis, ٢٠٠٥.

٢٦. Abass. M. ALbakry, "*Expert Systems Development using knowledge agent",* computer science and information system, university of technology, Ph. D. thesis, ٢٠٠٣.

٢٧. Wenpin J. and Zhongzhi S., "*A Dynamic architecture for multi agent system",* institute of computing technology, CAS,IEEE. ١٩٩٩.

٢٨. Najla'a H. M, "*New Robust information hiding technique*", information institute university of technology, Baghdad, Iraq, MSc. thesis, ٢٠٠٥.

٢٩. William Stalling, "*Cryptography and Network security: principle and practic",* PRINTIC–HALL, ١٩٩٩.

٣٠. Peter Gacs, "*Uniform test of algorithmic randomness over general space"*, COMPUTER SCIENCE DEPERATMENT, BOSTON UNVVERSITY, theoretical computer science, ٣٤١, pp. ٩١-١٣٧, ٢٠٠٥.

٣١. Tao Z. and Xijian P., "*A new approach to reliable detection of LSB steganography in natural images*", Signal Processing, (٨٣), pp. ٢٠٨٥-٢٠٩٣, ٢٠٠٣.

٣٢. Tabais S. G. G, "*Agent –Based recommendation systems*", Department of computer and system science, university of Stockholm, royal institute of technology, Msc. thesis, ١٩٩٩.

٣٣. Jane Y., Tharam D. and Edwige Pissaloux, "*Feature guide: A statistically based feature selection scheme"*, Laboratoire de perception University de Rouen, France, school of computing & Info. Tech., Griffith University QLD, Austeria ٤١١١, the Hong -Kong polytechnic University, IEEE, ٢٠٠١.

٣٤. V. Rodin, A. BenZinou, A. Guillaud, P. Ballet, F. Harrouet, J. Tissueau, and LE. B.,"*An immune oriented multi- agent system for biological image processing", pattern recognition*, (٣٧), pp. ٦٣١-٦٤٥, ٢٠٠٣.

٣٥. Qi D. and Robert K. A., "*Fostering multimedia learning of science: Exploring the role of an animated agent's image*". Computer and education, ٢٠٠٥.

٣٦. Sabu. M. Th. and K. Chandra S., "*Steganography based WWW distribution image retrieval with mobile agents"*, department of computer engineering national institute of technology, Karnataka, department of computer science and engineering L. B. S collage of engineering, Kasaragod, ٢٠٠٤.

٣٧. Niklas B., "*agent system security*", Information security group, royal Holloway University of London, UK, ٢٠٠٥.

٣٨. Chi-Kwong C. and L. M. Cheng, "*Hiding data in images by simple least significant bit*", department of computer Engineering and information technology, university of Hong Kong, pattern recognition, ٣٧, pp. ٤٦٩-٤٧٤, ٢٠٠٤.

٣٩. V. Rodin, A. BenZinou, A. Guillaud, P. Ballet, F. Harrouet, J. Tissueau, and LE. B., "*An immune oriented multi- agent system for biological image processing", pattern recognition*, (٣٧), pp. ٦٣١-٦٤٥, ٢٠٠٣.

٤٠. Ido O. and Michael W., "*Image Specific Feature Similarities*", School of Computers, the Hebrew University of Jerusalem, Jerusalem, ٩١٩٠٤, ٢٠٠٣.

٤١. Chin-Chen C., Ju-Yuan H. , and Chi-Shiang C., " *finding optimal least significant–bit substitution in image hiding by dynamic programming strategy",* department of computer science and information engineering,Taiwan, pattern Recognition, ٣٦, pp. ١٥٨٣-١٥٩٥, ٢٠٠٣.

٤٢. Niklas Borselius," *Agent System Security*", information security group ,Royall Holloway, University of London,UK,٢٠٠٢.