A Proposed Image Steganography System based on Mixing Matrix of Independent Components Analysis Technique

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

Natiq M. Abed Ali Al-Shemiry

Supervisor

Dr. Eng. Sattar B. Sadkhan

١٤٢٧ ٢٠٠٦

نظام اخفاء صور مقترح يعتمد على مصفوفة الخلط لتقنية تحليل العناصر المستقلة

رســـالة

مقدمة الى مجلس كلية العلوم - جامعة بابل

وهي جزء من متطلبات نيل درجة ماجستير في علوم الحاسبات

من قبل

ناطق مطشر عبدعلي الشمري

باشراف

الدكتور المهندس ستار بدر سدخان

١٤٢٧ ٢٠٠٦

بِسمِ اللهِ الرَحّمنِ الرحّيم

﴿ وَقُــلِ اعْمَلُــواْ فَسَــيَرَى اللّهُ عَمَلَكُــمْ وَرَسُــولُهُ وَالْمُؤْمِنُـونَ وَسَـتُرَدُّونَ إِلَـى عَـالِمِ الْغَيْـبِ وَالشَّـهَادَةِ فَيُنَبِّئُكُم بِمَا كُنتُمْ تَعْمَلُونَ﴾

صدق الله ألعلي العظيم

التوبة : ١٠٥

الخلاصــة

تعد تقنية اخفاء المعلومات من المواضيع المهمة التي تنال اهتماما كبيرا في العديد من المجالات ومنها الكتابة المخفية التي هي عملية إرسال رسالة سرية بين طرفين بطريقة تمنع المتطفل من اكتشاف وجودها .

يهدف النظام المقترح اخفاء صورة او أكثر داخل صورة بنفس الحجم . وقد استعملت طريقة مصفوفات المزج في عملية الإخفاء .

يتضمن النظام المقترح :- مرحلة الفحص ، مرحلة التحويل ، مرحلة انشاء مصفوفة الصور المراد خلطها ، مرحلة اختيار مصفوفة المزج المناسبة ،مرحلة ضرب مصفوفة الصور المراد مزجها بمصفوفة المزج ، مرحلة التحويل ، واخيرا مرحلة الفرق.

يعد النظام المقترح من طرائق الكتابة المخفية السرية حيث يكون المفتاح سريا بين المرسل والمستلم ويمثل هنا مصفوفة المزج وكذلك يعتبر من الطرائق التي عالجت مسألة سعة البيانات المخفية المرسلة حيث نجح النظام المقترح في عملية اخفاء (ولأول مرة) أكثر من صورة داخل صورة واحدة . وقد أعطى النظام نتائج جيدة ومقبولية لتلبية متطلبات الجودة والسعة والأمنية والتحصين ومقاومة الاكتشاف.

لقد تم تنفيذ النظام المقترح باستعمال لغة (Mathlab) الإصدار ٦.٥ .

Abstract

The steganography technique can be considered as one of the important subjects that obtained a great interest in many fields, such as a hidden writing , that is considered as a process for transmission secret message between two sites in a way that prevent its existence .

The proposed system provides a hidden one image or more (simultaneously) inside the cover image with the same size. The proposed system used the mixing matrix as a method for information hidden (Steganography) .

The proposed system contains: Test stage, Dimension Transformation Stage, Mixing Image Matrix Formation Stage, Selection of Mixing Matrix Stage, the Mixing stage , Dimension Transformation Stage, and Difference Stage .

This system is considered as a method of secret writing, since the secret key is maintained between the transmitter and receiver. This key is represented by the mixing matrix. And also the system can be considered as a method of treating the problem of the capacity of the hidden message. The system is successful in the process of hiding (for the first time) of more than one image inside the cover, and the result was very good and accepted to provide the requirements of goodness, security, robust, capacity and resistance to attack..

The system was implemented by using MATHLAB version ٦.٥ .

Supervisor Certification

I certify that this thesis was prepared under my supervision at the department of computer science/college of science/Babylon University, by **Natiq M. Abed Ali** as partial fulfillment of requirements for the degree of Master of Science in Computer Science.

Signature:

Name : **Dr. Eng. Sattar B. Sadkhan**

Title : **Assistant Professor**

Date : / /٢٠٠٦

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

Signature:

Name : **Dr. Abbas M. Albakry**

Title : **Assistant Professor**

Date : / /٢٠٠٦

(**Head of Computer Science Department)**

Certification of the Examination Committee

We chairman and members of the examination committee, certify that we have studied the thesis entitled (**A Proposed Image Steganography System based on Mixing Matrix of Independent Components Analysis Technique**) presented by the student **Natiq M. Abed Ali** and examined him in its content and in what is related to it, and we have found it worthy to accepted for the degree of Master of Science with (very good) degree.

Signature:

Name : Dr. Nabeel Hashem Kaghad

Title : Professor

Date : / /٢٠٠٦

(Chairman)

Signature:

Name : Dr. Abbas Muhson Al-Bakry

Title : Assistant Professor

Date : / /٢٠٠٦

(Member)

Signature:

Name :

Title : Lecture

Date : / /٢٠٠٦

(Member)

Signature:

Name : Dr. Eng. Sattar B. Sadkhan

Title : Assistant Professor

Date : / /٢٠٠٦

(Supervisor)

Signature:

Name : Dr. Oda Mizi'l Yasser Alzamely

Title : Professor

Date : / /٢٠٠٦

(Dean of College of Science – Babylon University)

List of Abbreviations

Abbreviations	Meaning
HTML	Hyper Text Markup Language
TCP/IP	Transmission Control Protocol / Internet Protocol
NTFS	New Technology File System
SS	Spread Spectrum
SSIS	Spread Spectrum Image Steganography
DCT	Discrete Cosine Transform
DWT	Discrete Wavelet Transform
BMP	Windows Bitmap
JPEG	Joint Photographic Experts Group
GIF	Graphics Interchange Format
LSB	Least Significant Bit
PCX	Windows Paintbrush
WNA	White Noise Storm
ICA	Independent Components Analysis
HVS	Human Visual System
PSNR	Peak Signal to Noise Ratio
RMSE	Root Mean Square Error
SNR	Signal to Noise Ratio

Contents

١.١ ***Overview***

The idea of Information Hiding can be traced back to a few thousands years ago . In many rivalry environments, concealing the existence of communication is desirable to avoid suspicion from adversaries [١].

Data hiding represents a class of processes used to embed data into various forms of media such as image , audio , or text . The embedded data should be invisible to a human observer [٢].

Information hiding techniques have recently become important in a number of application areas.

Digital audio, video , and image are increasingly furnished with distinguished but imperceptible marks which may contain a hidden copyright notice or a serial number or even help to prevent unauthorized copying directly . Military

communication systems make an increasing use of traffic security techniques which, rather than merely concealing the content of a message using encryption , seek to conceal its sender , its receiver or its existence [٣].

Techniques and applications of Information Hiding have been increasingly more sophisticated and widespread[٤]. Information Hiding can be classified as shown in figure (١.١).

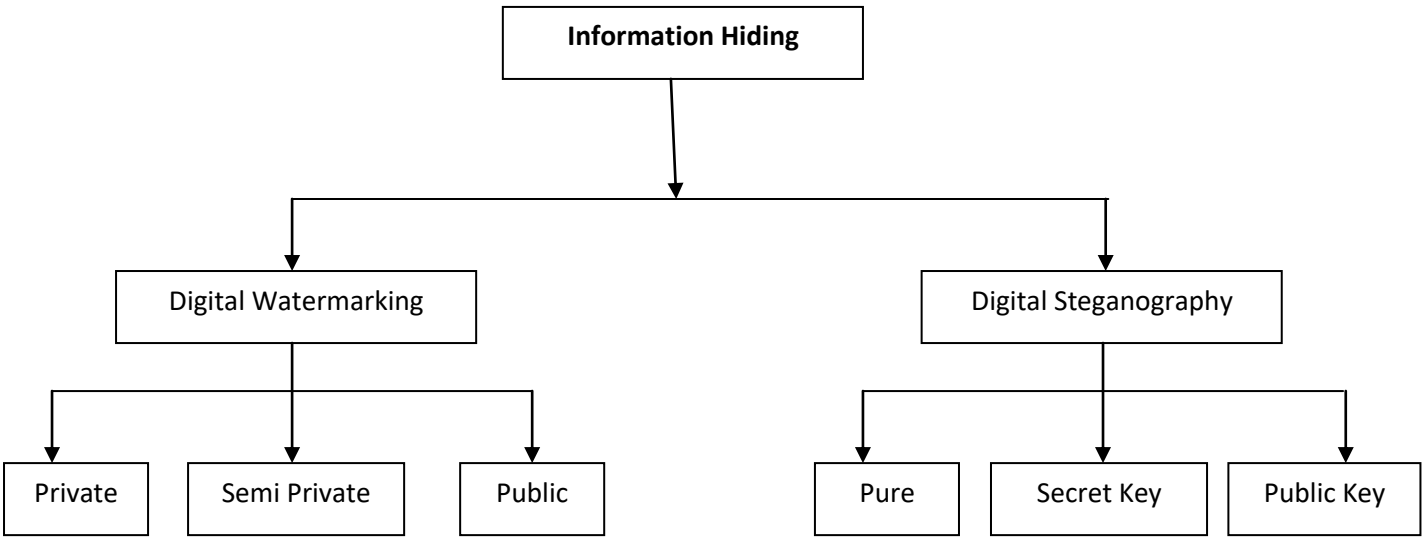


Figure (١. ١) Information hiding classification

Digital steganography is an ancient art of conveying message in a secret way that only the receiver knows the existence of message [٥] . Steganography,derived from Greek, literally means "covered writing" [٦].

Digital watermarking is employed in an attempt to provide a proof of ownership and identify illicit copying and distribution of multimedia information [٧].

Data hiding techniques should be capable of embedding data in a host signal with the following restrictions and features:

١. The host signal should be nonobjectionally degraded and the embedded data should be minimally perceptible. (The goal is for the embedded data to remain *hidden*. As any magician will tell you, it is possible for something to be hidden while it remains in plain sight; you merely keep the person from looking at it. We will use the words *hidden*, *inaudible*, *imperceivable*, and *invisible* to mean that an observer does not notice the presence of the data, even if they are perceptible.)

٢. The embedded data should be directly encoded into the media , rather than into a header or wrapper, so that the data remain intact across varying data file formats.

٣. The embedded data should be immune to modification ranging from intentional and intelligent attempts at removal to anticipated manipulations, e.g., channel noise , filtering , cropping ,etc.

٤. Asymmetrical coding of the embedded data is desirable , since the purpose of data hiding is to keep the data in the host signal , but not necessarily to make the data difficult to access.

٥. Error correction coding should be used to ensure data integrity . It is inevitable that there will be some degradation to the embedded data when the host signal is modified.

٦.The embedded data should be self-clocking or arbitrarily re-entrant. This ensures that the embedded data can be recovered when only fragments of the host signal are available, e.g., if a sound bite is extracted from an interview, data embedded in the audio segment can be recovered. This feature also facilitates automatic decoding of the hidden data, since there is no need to refer to the original host signal [٢].

١. ٢ ***Information Hiding Methods*** [٦]:-

The onset of computer technology and the Internet have given new life to steganography and to the creative methods with which it is employed.

Computer-based steganographic techniques introduce changes to digital carriers to embed information foreign to the native carriers.

Steganography encompasses methods of transmitting secret messages in such a manner that the existence of the embedded messages is undetectable. Carriers of such message may resemble innocent sounding text, disks, network traffic and protocols, the way software or circuits are arranged, audio, images, video, or any other digitally represented code or transmission.

a- Hiding in Text

Documents may be modified to hide information by manipulating positions of lines and words. HTML files can be used to carry information since adding spaces , tabs ,"invisible" characters and extra line breaks are ignored by web browsers . The "extra" spaces and lines are not perceptible until revealing the source of the web page.

b- Hiding in Disk Space

Other ways to hide information rely on finding unused space that is not readily apparent to an observer. Taking advantage of unused or reserved space to hold covert information provides a means of hiding information without perceptually degrading the carrier. The way operating systems store files typically results in unused space that appears to be allocated to files. This " allocated " but available space is known as *stack* space.

Another method of hiding information in file system is to create a hidden partition. These partitions are not seen if the system is started normally. However , in many cases , running a disk configuration utility exposes the hidden partition . These concepts have been expanded in a novel proposal of a steganographic file system. If the user knows the file name and password, then access is granted to the file; no evidence of the file exists in the system of the hidden files .

c- Hiding in Network Packets

Characteristics inherent in network protocols can be taken advantage of to hide information . An uncountable number of data packets are transmitted daily over the Internet .Any of which can provide an excellent covert communication channel. For example , TCP/IP packets can be used to transport information across the Internet. These headers have unused space and other features that can be manipulated to embed information. See Appendix A for an illustration of hiding information TCP/IP packet headers [٦].

d- Hiding in Software and Circuitry

Data can also be hidden on the physical arrangement of a carrier. The arrangement itself may be an embedded signature that is unique to the creator. An example of this is in the layout of code distributed in a program or the layout of electronic circuits on a board . This type of " marking " can be used to uniquely identify the design origin and cannot be removed without significant change to the work .

e- Hiding in Audio and Images

Many different methods for hiding information in audio and images exist. These methods may include hiding information in unused space in file headers to hold "extra" information. Embedding techniques can range from the placement of information in imperceptible levels (noise), manipulation of compression algorithms, to the modification of carrier properties . In audio , small echoes or slight delays can be added or subtle signals can be masked by sounds of higher amplitude .

In images , modifying properties such as luminance , contrast, or colors can be used . These methods hide information in audio and images with virtually no impact on the human sensory system.

١.٣ ***Literature Survey:-***

A.Tumoas (١٩٩٦)[٨], proposed an algorithm for hiding bit selection in digital image. The basic idea is to use a pseudorandom permutation of the cover bit .This kind of hiding system is called substitution method of invisibility. An experimentation of the algorithm on grayscale images .

W.Bender,D.Gruhi,N.Morimoto and A.Lu(١٩٩٦)[٢], introduced several methods to embed data into digital media ,one of these methods is called "Patchwork" . Two patches are chosen pseudorandomly , the first A, the second B . The image data in patch A are lightened while the data in patch B are darkened . This unique statistic indicates the presence or absence of a signature .Patchwork is independent of the contents of the host image . It shows reasonably high resistance to most nongeometric image modifications.

S.Joshua and C.Barrett (١٩٩٦)[٩], introduced several spread spectrum data – hiding method. These techniques used the message data to modulate a carrier signal , which is then combined with the cover image in section of non overlapping blocks. The message is extracted via cross correlation between the stegoimage and the regenerated carrier , hence , cover image escrow is not necessary. A threshold operation is then performed on the resulting cross correlation to determine the binary value of the embedded data bits.

W.Andreas and W. Gritta (١٩٩٨)[١٠] presented a steganography system which embeds a secret message in a video system. A signal path is transferred by a Discrete Cosine Transformation(DCT) based. The result is the technical realization of a steganography algorithm whose security is established by indeterminism within the signal path.

M.Lisa and B.Charles (١٩٩٨)[١١] , employed a method for reliable blind image steganography that can hide and recover a message of substantial length within digital imagery while maintaining the original image size and dynamic range . The message embedded by this method can be in the form of text , imagery , or any other digital signal .

J. Fridrich (١٩٩٨)[١٢],presented steganographic technique for embedding message in palette –based images, such as GIF files. The technique embeds one message bit into one pixel . The pixels for message embedding are randomly chosen using a pseudo-random number generator seeded with secret key . For each pixel at which one message bit is to be embedded , the palette is searched for closest colors. Indeed, numerical experiments indicate that the technique introduces approximately four times less distortion to the carrier image than EZ Stego. A technique that introduces less distortion to the carrier image will generally cause changes that are more difficult to detect, and will therefore provide more security.

J.J.Chae and B.S.Manjunath (١٩٩٩)[١٣], presented a technique for embedding image data that can be recovered in the absence of the original host image. The data to be embedded, referred to as the signature data , is inserted into the host image in the DCT domain. The signature DCT coefficients are encoded using a lattice coding scheme before embedding. Each block of host DCT coefficients is first checked for its texture content and the signatured codes are appropriately inserted depending on a local texture measure. Experimental results indicate that high quality embedding is possible , with no visible distortions. Signature images can be recovered even when the embedded data is subject to significant lossy JPEG compression.

N.K.Abdulaziz, K.K. Pang (١٩٩٩)[١٤], presented a technique for robust data embedding , which uses a source and channel coding framework for data hiding. The data to be embedded , referred to as the signature data, is source coded by vector quantization and the indices obtained in the process are embedded in the transform coefficients of the host image. Transform

coefficients of the host are grouped into vectors and perturbed using error-correcting codes derived from BCH codes. Compared to prior work in digital watermarking, the proposed scheme can handle a significantly large quantity of data such as a gray scale images.

J.J Chae and B.S Manjunath (١٩٩٩)[١٥],proposed a video data embedding scheme in which the embedded signature data is reconstructed without knowing the original host video. The proposed method enables high rate of data embedding and is robust to motion compensated coding, such as MPGE-٢. Embedding is based on texture masking and utilizes a multi-dimensional lattice structure for encoding signature information. Signature data is embedded in individual video frames using the block DCT. The embedded frames are then MPEG-٢ coded . At the receiver, both the host and signature images are recovered from the embedded bit stream.

E.T.Lin and E. J.Delp (١٩٩٩)[١٦], presented overview the use of data hiding techniques in digital images. They described how one can use steganography to hide information in a digital images.

L. Yeuan and C. Ling (٢٠٠٠)[٥], presented an image steganographic model and proposed a new high-capacity embedding / extracting module that is based on the variable – sized LSB insertion . In the embedding part , based on the contrast and luminance property , these use three components to maximize the capacity , minimize the embedding error and eliminate the false contours.

S. Areepongsa, N. Kaewkamnerd, Y. F. Syed, and K. R. Rao (٢٠٠٠)[١٧], presented a method to image retrieval by using steganography technique . They extract some image features as shape, color and texture

,then hidden in database images are compressed by using CHC-RIOT Wavelet based coder.

S.Abdullah (٢٠٠١)[١٨], presented a method to hide small Arabic texts in two cover types : the first cover is another Arabic text , where the embedding depends on the natural feature of Arabic , the second cover is an image ; the process uses three methods : Hiding by modulo ٢ of LSB block , Hiding by modulo ٢ with Encryption and hiding in blue channel of pixel .

A. Jafer (٢٠٠٢)[١٩], presented a method for hiding an image inside another image , and this method involves Wavelet Transformation Techniques .

H.Al Khafaji (٢٠٠٣)[٢٠], employed a method for hiding an image with different color levels (True color , color-٢٥٦, gray) inside another image with the same size , using five different methods : Image Downgrading method , Least Significant Bit Insertion , Modulo Mechanism , Hybrid Method and Similar – blocks method.

C.julio, L.Ignacio,T.Juan and G.Arturo (٢٠٠٥)[٢١], presented and analyzed a novel methodology that illustrates how games (such as Chess, Backgammon, Go, etc.) can be used to hide digital contents. They also look at some of its possible advantages and limitations when compared with other techniques, discussing some improvements and extensions. Finally, they present the results of a first implementation of an open-source prototype, called StegoGo, for hiding digital contents in Go games.

H.Ewa, B.Derek and W.Cheong Kai (٢٠٠٦) [٢٢], examined the methods of hiding data in the NTFS file system. Further they discuss the analysis techniques which can be applied to detect and recover data hidden using each

of these methods. They focus on sophisticated data hiding where the goal is to prevent detection by forensic analysis. Obvious data hiding techniques , for example setting the hidden attribute of a file , will not be included . Hidden data can be further obfuscated by file system independent approaches like data encryption and Steganography . This paper is only concerned with the methods which are made possible by the structure of the NTFS file system, and with the recovery of hidden data, not its interpretation.

١.٤ ***Aim of the Thesis:-***

The aim of this thesis is to design and test an algorithm to hide one or more images inside one image without affecting of cover image to avoid drawing suspicion to transmitted image.

١.٥ ***The Contents of Thesis:-***

The remain of this thesis :-

- **Chapter Two:** includes a background to steganography theory, applications of images steganography, including the types of

steganography, steganography tools, methods for hiding information , and finally a background to the independent component analysis .

- **Chapter Three:** presents the new proposed image steganography system in its two parts: the embedding part and the extracting part.
- **Chapter Four:** deals with the results of the proposed system.
- **Chapter Five:** gives the conclusions and some recommendations for future work.

٢.١ *Introduction*

Steganography (literally , covered writing) is the art of hiding information in ways that prevent the detection of hidden message [٦].It includes a vast array of secret communication methods that conceal the very existence message [٢٣].

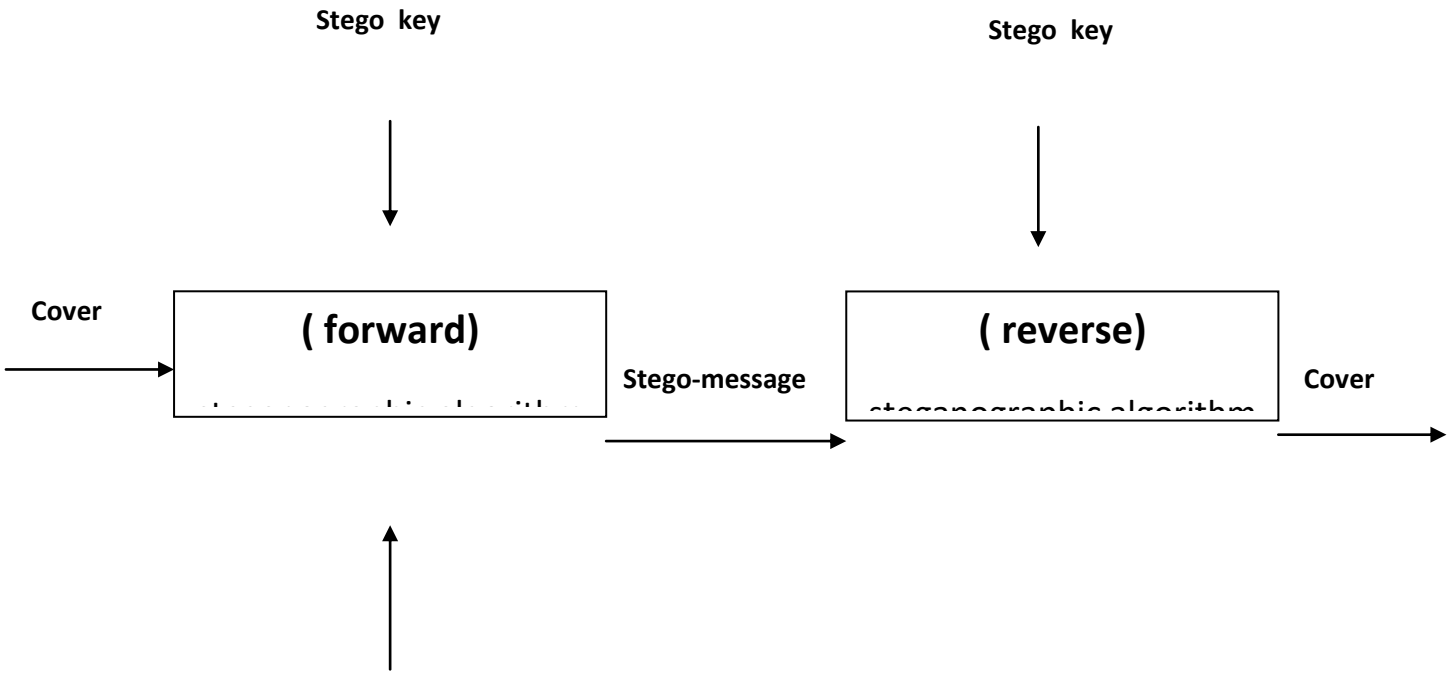
Steganography has its place in security . It is not included to replace cryptography but supplement it . Hiding a message with steganography methods reduces the chance of a message being detected . If the message is also encrypted then it provides another layer of protection [٢٤]. Therefore , some steganographic methods combine traditional cryptography with steganography , the sender encrypts the secret message prior to the overall communication process , as it is more difficult for an attacker to detect embedded cipher text in a cover .

This chapter is organized in the following manner. In section ٢ Steganography System is described. Then, Characterization of Steganography System is introduced in section ٣ . In section ٤, Applications of Images Steganography are explained. Steganography types is introduced in section ٥. In section ٦, Classification of Steganography Techniques is described. Then, Steganography

Tools is described in section ٧. In section ٨, Independent Components Analysis(ICA) is explained. Fidelity Criteria is introduced in section ٩ .

٢. ٢ ***Steganography System*** [٢٥] *:-*

A general steganography system is shown in figure (٢.١).



Embedded (hidden) message **Extracted (hidden) message**

Figure (٢.١) General Steganography System

It is assumed that the sender wishes to send , via steganographic transmission , a message to a receiver. The sender starts with a cover message , which is an input to the stego-system, in which the embedded message will be hidden. The hidden message is called the embedded message .

The algorithm may , or may not , use a steganographic key (Stego key), which is additional secret data that may be needed in the hidden process. The same key (or related one) is usually needed to extract the embedded message again . The output of the steganographic algorithm is the stego message .The cover message and stego message must be of the same data type , but the embedded message may be of another data type. The receiver reverses the embedding process to extract the embedded mess-age.

٢.٣ ***Characterization of Steganography System*:-**

Steganographic techniques embed a message inside a cover. Various features characterize the strengths and weaknesses of the methods. The relative importance of each feature depends on the application [١٦].

a- Robustness:-

The embedded information is said to be robust if its presence can be reliably detected after the image has been modified but not destroyed beyond recognition. Examples are linear and nonlinear filters (blurring, sharpening, median filtering), lossy compression, scaling, rotation, noise adding , color quantization (as in palette images), etc.

We emphasize that robustness does not include attacks on the embedding scheme that are based on the knowledge of the embedding algorithm or on the availability of the detector function. Robustness means resistance to “blind”, non-targeted modifications, or common image operations [٢٦,١٦].

b- Undetectability:-

This property is typically required for secure covert communication. That is mean, the embedded information is undetectable if the image with the embedded message is consistent with a model of the source from which images are drawn. For example, if a steganographic method uses the noise component of digital images to embed a secret message, it should do so while not making statistically significant changes

to the noise in the carrier. The concept of Undetectability is inherently tied to the statistical model of the image source. If an attacker has a more detailed model of the source, he may be able to detect the presence of a hidden message. It is worth mentioning that the ability to detect the presence does not automatically imply the ability to read the hidden message [٢٦].

c- Invisibility (Perceptual Transparency):-

The act of hiding the message in the over necessitates some noise modulation or distortion of the cover image. It is important that the embedding occurs without significant degradation or loss of perceptual quality of the cover. In a secret communications arouses suspicion of the presence of hidden data in a stego-image, the steganographic encoding has failed even if the attacker is unable to extract the message. Preserving perceptual transparency in an embedded watermark for copyright protection is also of paramount importance because the integrity of the original work must be maintained.

For applications, where the perceptual transparency of embedded data is not critical, allowing more distortion in the stego-image can increase hiding capacity, robustness, or both[١٦].

d- Security :-

The embedding algorithm is said to be secure if the embedded information cannot be removed beyond reliable detection by targeted attacks based on a full knowledge of the embedding algorithm and the detector (except the secret key), and the knowledge of at least one carrier with hidden message [٢٦].

e- Capacity:-

The above requirements are mutually competitive and cannot be clearly optimized at the same time. If we want to hide a large message inside an image, we cannot require at the same time absolute Undetectability and large robustness. A reasonable compromise is always a necessity. On the other hand, if robustness to large distortion is an issue, the message that can be reliably hidden cannot be too long [٢٦].

٢.٤ ***Applications of Images Steganography*** [١٦]:

There are many applications for digital steganography of images , including copyright protection, feature tagging, and secret communications.

a- Copyright Protection:-

A secret copyright notice or watermark can be embedded inside an image to identify it as intellectual property. This is the watermarking scenario where the message is the watermark. The “watermark” can be a relatively complicated structure. In addition, when an image is sold or

distributed, an identification of the recipient and time stamp can be embedded to identify potential pirates. A watermark can also serve to detect whether the image has been subsequently modified. Detection of an embedded watermark is performed by a statistical, correlation, or similarity test, or by measuring other quantity characteristic to the watermark in a stego-image. The insertion and analysis of watermarks to protect copyrighted material is responsible for the recent surge of interest in digital steganography and data embedding.

b- Feature Tagging:-

Captions, annotations, time stamps, and other descriptive elements can be embedded inside an image, such as the names of individuals in a photo or locations in a map. Copying the stego-image also copies all of the embedded features and only parties who possess the decoding stego-key will be able to extract and view the features. In an image database, keywords can be embedded to facilitate search engine. If the image is a frame of a video sequence, timing markers can be embedded in the image for synchronization with audio. The number of times an image has been viewed can be embedded for "pay-per-view" applications.

c- Secret Communications:-

In many situations, transmitting a cryptographic message draws unwanted attention. The use of cryptographic technology may be

restricted or forbidden by law. However, the use of steganography does not advertise covert communication and therefore avoids scrutiny of the sender, message, and recipient. A trade secret, blueprint, or other sensitive information can be transmitted without alerting potential attackers or eavesdroppers.

٢.٥ ***Steganography types*:-**

Steganography is divided into three main types as described in the following section:

a- Pure Steganography :-

A steganography system that 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× → M , extracting the secret message out of a cover. Clearly , it is necessary that /C/ ≥ /M/ . Both sender and receiver must have access to the embedding and extraction algorithm , but the algorithm should not be public [٢٧].

b- 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 into C , using a secret key K . If the key used in the embedding process is known to the receiver , he can reverse the process and extract the secret message . Anyone who does not know the secret key should not be able to obtain evidence of the encoded information . Again , 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 keys [٢٨].

c- Public Key Steganography

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

Whereas it 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 . Public key steganography utilizes the fact that the 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 are random elements of M which will be results , which will be called the " natural randomness " of the cover . If one assumes that this natural randomness is statistically indistinguishable from the cipher text produced by some public key cryptosystem , a secure steganography can be built by embedding cipher text rather than unencrypted secret mess-age [٧].

٢. ٦ ***Classification of Steganography Techniques***:-

There are several approaches to the classification of steganographic techniques . One of these approaches is to categorize them according to the cover modifications applied in the embedding process. Mainly, steganographic techniques may be grouped into six categories as follows [٧]:

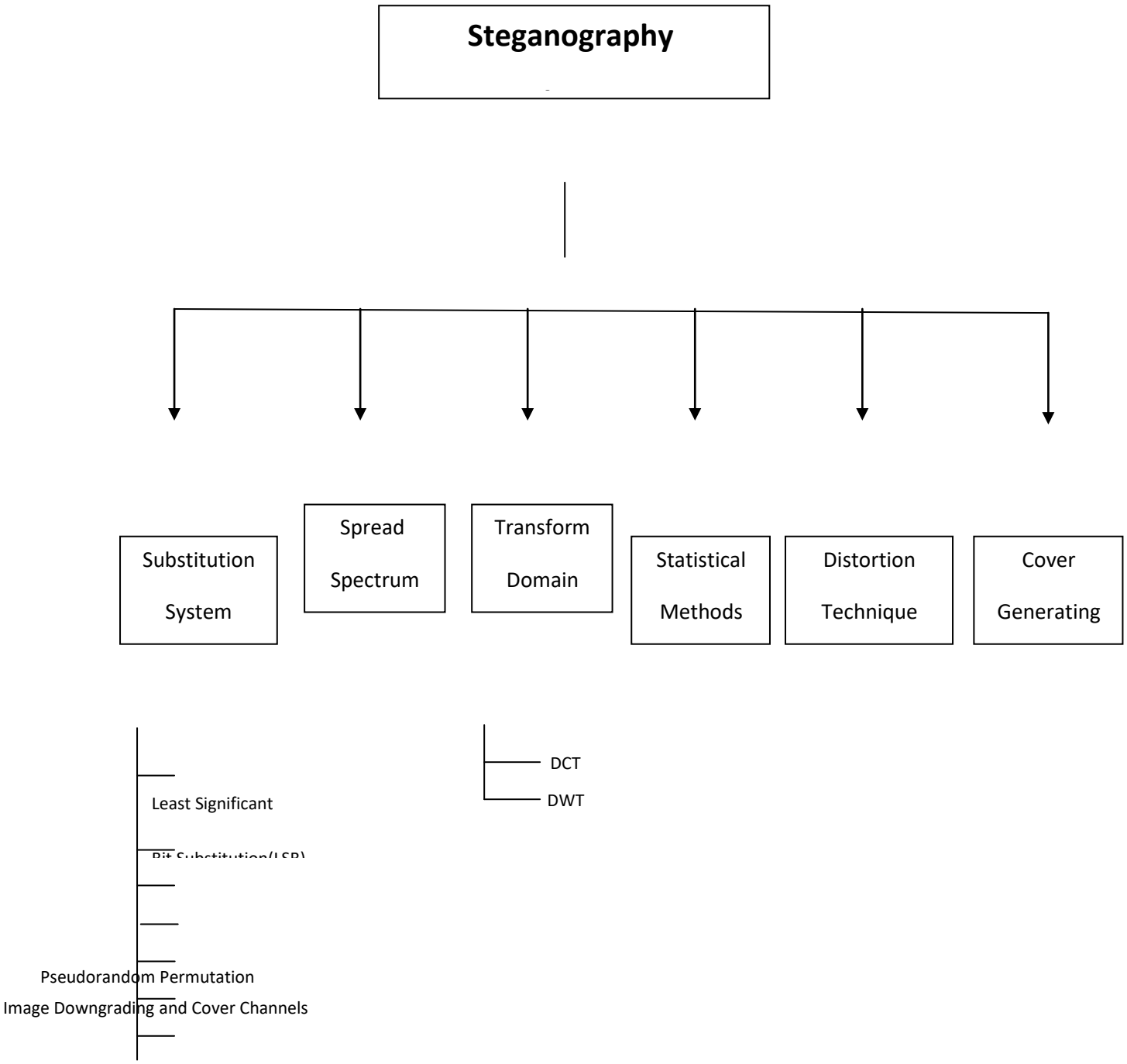

Steganography
Substitution System
Spread Spectrum
Transform Domain
Statistical Methods
Distortion Technique
Cover Generating
DCT
DWT
Least Significant
Pseudorandom Permutation
Image Downgrading and Cover Channels
Cover Regions and Parity Bits
Palette-based Image
Quantization and Dithering

Figure (٢.٢) Steganography Classifications.

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

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

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

٤. **Distortion Techniques**:They store information by signal distortion and measure the deviation from the original cover in the decoding step.

٥. **Statistical Methods**: They encode information by changing several statistical properties of a cover and use hypothesis testing in the extraction process.

٦. **Cover Generating Methods**:They encode information in the way that a cover for secret communication is created.

٢. ٦. ١ ***Substitution System*** :-

Basic substitution system tries to encode secret information by substituting insignificant parts of the cover by secret message bits . The receiver can extract the information if it 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 they will not be noticed by an attacker. It consists of several techniques that will be discussed in more detail.

a- Least Significant Bit Substitution(LSB):-

The embedding process consists of choosing a subset$\{J_1 \ldots J_{l(m)}\}$ of cover elements and performing the substitution operation $c_{ji} \leftrightarrow m_i$ on them, which exchanges the LSB of c_{ji} by m_i (m_i can be either ١ or ٠). In the extraction process , the LSB of the selected cover-element is extracted and lined up to reconstruct the secret message .

In order to be able to decode the secret message , the receiver must get access to the sequence of elements indices used in the embedding process. In the simplest case , the sender uses all cover elements for information transfer , starting at the first element . Since the secret message will normally have less

bits then *I(c)* , the embedding process will be finished long before the end of the cover , in which case , the sender can leave all other elements unchanged. This can , however, lead to a serious security problem ; the first part of the cover will have different statistical properties than the second part , where no modifications have been made [١٨].

b- Pseudorandom Permutation :-

If all cover can be access in the embedding process, the cover is a random access cover, and the secret message bits can be distributed randomly over the whole cover . This technique further increases the complexity for the attacker , since it is not guaranteed that the subsequent message bits are embedded in the same order.

The embedding process starts with creating pseudorandom number generator , a sequence $j_{١},\ldots,j_{١(m)}$ of element indices and storing the kth message bit in the element with the index j_k , Note that one index could be appearing more than once in the sequence , so collision will occur. If the message is quite short compared with the number cover elements , the probability of collisions is negligible and that the corrupted bits could be reconstructed using error correcting code [١٨,٢٩].

c- Image Downgrading and Cover Channels:

Image downgrading is a special case of a substitution system in which image acts both as a secret message and a cover . Given cover-image and secret image of equal dimensions , the sender exchanges the four least significant bits of the covers grayscale(or color) values with the four least significant bits out of the stego-image, thereby gaining access to the most significant bits of the stego-image. Whereas the degradation of the cover is not visually noticeable in many cases. Four bits are sufficient to transmit a rough approximation of the secret image [٧,٢٠].

d- Cover Regions and Parity Bits:-

Any nonempty subset of $\{c_1,\ldots,c_{l(c)}\}$ is called a cover-region. By dividing the cover into several disjoint regions , it is possible to store one bit of information in a whole cover-region rather than in a single element. A parity bit of a region I can be calculated by :

$$B(I) = \sum_{j \in I} LSB(C_j) \bmod 2 \qquad (٢.١)$$

In the embedding step, $I(m)$ disjoint cover-regions I_i ($1 \le i \le I(m)$) are selected , each encodes one select bit m_i in the parity bit $B(I_i)$. If the parity bit of one cover-region I_i does not match with secret bit m_i to encode , one LSB of the value I_i is flipped. This will result in $B(I_i)=m_i$.

In the decoded process , the parity bits of all selected regions are calculated and lined up to reconstruct the message . Again , the cover-region can be constructed pseudo randomly using the stego-key as a seed.

Although the method is not more robust than simple bit substitution , it is conjectured to be more powerful in many cases [١٩].

e- Palette-based Image :-

There are two ways to encode information in a palette-based image , either the palette or the image data can be manipulated . The LSB of the color vectors could be used for information transfer , just like the substitution methods presented . Alternatively , since the palette does not need to be stored in any way , information can be encoded in the way the colors are stored in the palette. For N colors since there are N! different ways to sort the palette, there are enough capacity to encode a small message . However , all methods which use the order of a palette to store information are not robust, since an attacker can simply sort the entries in a different way and destroy the secret message.

f- Quantization and Dithering:-

Dithering and quantization of digital images can be used for embedding secret information. Some steganographic systems operate on quantizes images . The difference e_i between adjacent pixels χ_i and χ_{i+1} is calculated and fed into a quantizer φ which output a discrete approximation Δ_I of the difference

signal $\chi_i - \chi_{i+1}$. Thus in each quantization step a quantization error is introduced .

For a steganographic purpose, the quantization error in a predictive coding scheme can be utilized , specifically, when the difference signal Δ_I is adjusted in such a way so that it transmits additional information. In this scheme, the stego-key consists of a table which assigns a specific bit to every possible value of Δ_I .

In order to store the ith message bit in the cover-signal, the quantized difference signal Δ_I is computed. If, according to the secret table, Δ_I does not match with the secret bit to be encoded, Δ_I is replaced by the nearest Δ_I where the associated bit equals the secret message bit. The values Δ_I are those fed into the entropy coder. At the receiver side, the message is decoded according to the difference signal Δ_I and the stego-key [٧].

g- Information Hiding in Binary Images:-

Binary images contain redundancies in the way black and white pixels are distributed. Although the implementation of a simple substitution scheme is possible , these systems are highly susceptible to transmission errors and therefore not robust.

A binary image is divided into rectangular image blocks B_{ij}. Let $P_0(B_i)$ be the percentage of black pixels in the image, block B_i and $P_1(B_i)$ the percentage of white pixels, respectively. Basically, one block embed a ١ , if

$P_1(B_i)$ >٥٠٪ and a ٠ if $P_0(B_i)$>٥٠٪. In the embedding process, the color of some pixel is changed so that the desired relation can be held. Modifications are carried out of those pixels whose neighbors have the opposite color, in sharply contrasted binary image, and these modifications are carried out at the boundaries of black and white pixels. These rules assure that the modifications are not generally notice- able [٢٠].

h- Unused or Reserved Space in Computer Systems:-

Taking advantage of an unused or reversed space to hold covert information provides a means of hiding information without perceptually degrading the carrier. For example , the way operation systems store files typically results in an unused space that appears to be allocated to a file.

Another method of hiding information in file system is to create hidden partitions. These partitions are not seen if the system is normally started [٧].

٢. ٦. ٢ ***Transform Domain Techniques:-***

It has been seen that the substitution modification techniques are easy ways to embed information ,but they are highly vulnerable to even small modification . An attacker can simply apply signal processing techniques in order to destroy the secret information . In many cases, even the small changes resulting out of lossy compression system yield total information loss.

It has been noted in the development of steganographic systems that embedding information in the frequency domain of a signal can be much more robust than embedding rules operating in the time domain. Most robust steganographic systems known today actually operate in some sort of transform domain.

Transform domain steganographic methods hide message in a significant area of the cover image which makes them more robust to attack, such as adding noise, compression, cropping some image processing . However , whereas they are more robust to various kinds of signal processing , they remain imperceptible to the human sensory system. Many transform domain variations exist. One methods is to use the Discrete Cosine Transform (DCT) as a vehicle to embed information in image . Another method would be the use of Wavelet transform [٧].

Transform Domain Method embeds a message by modification (selected) transform (e.g, frequency) coefficients of the cover message . Ideally , transform embedding has an effect in the spatial domain to apportion the hidden information through different order bits in a manner that is robust , but yet hard to detect . Since an attack, such as image processing , usually affects a certain band of transform coefficient , the remaining coefficient would remain largely intact.

Hence , transform embedding is , in general, more robust than other embedding methods [٣٠].

٢. ٦. ٣ *Spread Spectrum(SS) Techniques:-*

Spread Spectrum Techniques are defined as " means of transmission in which the signal occupies a bandwidth in excess of the minimum necessary to send the information" . The band spread is accomplished by means of a code which is independent of the data , and a synchronized reception with the code at the receiver is used for dispreading and subsequent data recovery. Although the power of the signal to be transmitted can be large, the signal –to-noise ratio in every frequency band will be small , even if parts of the signal could be removed in several frequency band, enough information should be present in the other bands to recover the signal. This situation is very similar to a steganography system which tries to spread a secret message over a cover in order to make it impossible to perceive. Since spread signals tend to be difficult to remove , embedding methods based on SS should provide a considerable level of robustness.

In information hiding, two special variants of SS are generally used : direct sequence, and frequency-hopping scheme. In direct-sequence scheme, the secret signal is spread by a constant called chip rate, modulated with a pseudorandom signal and added to the cover . On the other hand, in the frequency-hopping schemes the frequency of the carrier signal is altered in a way that it hops rapidly from one frequency to the another. SS are widely used in the context of watermarking [٢٣].

٢. ٦. ٤ ***Statistical Steganography :-***

Statistical Steganography techniques utilize the existence of " ١-bits " steganographic 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 characteristic changes significantly if a "١" is transmitted. Otherwise , the cover is left unchanged . So the receiver must be able to distinguish unmodified covers from modified ones.

A cover is divided into *I(m)* disjoint blocks $B_1,.....B_{I(m)}$. A secret bit m_i is inserted into the ith block by placing "١" into B_i if m_i=١. Otherwise , the block is not changed in the embedding process [٧].

٢. ٦. ٥ ***Distortion Techniques:-***

In contrast to substitution systems, distortion requires the knowledge of the original cover in the decoding process. The sender applies a sequence of modifications 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 want 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 to the original covers. If the attacker also has access to them, he/she can easily detect the cover modifications and has evidence for a secret communication. If the embedding and extraction functions are public and do not depend on a stego-key, it is also possible for the attacker to reconstruct secret message entirely [٢٩].

٢. ٦. ٦ ***Cover Generation Techniques:-***

In contrast to all embedding methods presented above, when secret information is added to a specific cover by applying an embedding algorithm, some steganographic applications generate a digital object only for the purpose of being a cover for secret communication [٧].

٢. ٧ ***Steganography Tools :***

Various Steganography software tools explored throughout this project. The evaluation process was to determine limitations and flexibility of the software readily available to the public. This section provides description of their functionally [٦].

a- Hide and seek:-

This freeware is a MS DOS program that embeds and extracts data from (GIF) format image files. It will embed up to ١٩,٠٠٠ bytes in to a GIF file of maximum size ٣٢٠× ٤٨٠ pixels .It uses Least Significant Bit (LSB) replacement to encode, removing the LSB of the image byte and replacing it with a bit of message file data . It also uses IDEA to encrypt the program-specific header information [٣١].

b- Stego Dos :-

This collection of programs , also known as Black Wolf 's Picture Encoder, is also freeware. It encodes data files up to ٨kb in size within a picture file of maximum size ٣٢٠× ٤٨٠ pixels and of ٢٥٦ colors. It doesn't specify any specific image format; additionally, the user must supply the graphics file display and screen capture software to use this utility . It encodes the screen capture file with data using the LSB replacement method, and since it uses screen capture doesn't overwrite the original image. It is cumbersome to use, because it requires the user to perform multiple steps to encode and extract data [٣١].

c- White Noise Storm(WNS):-

The White Noise Storm tool is a set of software for DOS. Embedding the text message in the cover images was rather trivial and no degradation could be readily detected. WNS applies steganography to the LSBs of PCX files by extracting the LSBs from the cover image and storing them in a file . The message is encrypted and applied to these bits to create a new set of LSBs. The

modified bits are then injected into the cover image to create the new stego-image. The White Noise Storm tools are based on Spread Spectrum Technology and frequency hopping, which scatters the message throughout the image (similar to DES block encryption) [٦].

d- S-Tools :-

It encodes and extracts using LSB replacement on not only .BMP and GIF files , but on audio ,WAV files . It also has a utility to steganographically encode unused disk space on floppy disks. It supports ٢٤ bit BMP color and supports encryption of the input message file using (IDEA,DES) [٢٣].

٢.٨ ***Independent Components Analysis(ICA)***:

Independent Component Analysis is a method for finding underly-ing factors or components from multivariate (multidimensional) statistical data. What distinguishes ICA from other methods is that it looks for components that are both *statistical independent* and *nongaussian* [٣٢].

٢.٨.١ ***Definition of ICA***:

To rigorously define ICA (Jutten and Herault, ١٩٩١;Comon, ١٩٩٤), we can use a statistical"latent variables" model. Assume that we *observe n* linear mixtures $x_1, \ldots, x_n$ of *n* independent components

$x_j = a_{j1}s_1 + a_{j2}s_2 + ... + a_{jn}s_n$, for all j . (٢.٢)

They have now dropped the time index t; in the ICA model , assume that each mixture x_j as well as each independent component s_k is a random variable, instead of a proper time signal. The observed values $x_j(t)$, e.g., the microphone signals in the cocktail party problem , are then a sample of this random variable . Without loss of generality , can assume that both the mixture variables and the independent component have zero mean: if this is not true , then the observables x_i can always be centered by subtracting the sample mean, which makes the model zero-mean.

It is convenient to use vector-matrix notation instead of the sums like in the equation(٢.٢). Let us denote by **x** the random vector whose elements are the mixtures $x_1,....,x_n$, and likewise by **s** the random vector with elements $s_1,...,s_n$. Let us denote by **A** the matrix with elements a_{ij}. Generally , bold lower case letters indicate vectors and bold upper-case letters denote matrices. All vectors are understood as column vectors; thus $\mathbf{x}^T$, or the transpose of **x**, is a row vector. Using vector-matrix notation, the above mixing model is written as

$$\mathbf{x}=\mathbf{A}\mathbf{s} \qquad (٢.٣)$$

Sometimes we need the columns of matrix A; denoting them by $\mathbf{a}_j$ the model can also be written as

$$\mathrm{x}=\sum_{i=1}^{n}\mathrm{a}_i s_i \,. \qquad (٢.٤)$$

The statistical model in Eq.(٢.٣) is called Independent Component Analysis , or ICA model .The ICA model is a generative model, which means that it describes how the observed data are generated by a process of mixing the components s_i . The independent components are latent variables,

meaning that they cannot be directly observed. Also the mixing matrix is assumed to be unknown. All observe is the random vector **x** , and must estimate both **A** and **s** using it .This must be done under general assumptions as possible [۳۳].

۲.۸. ۲ ***Observing mixtures of unknown signals***:

Consider a situation where there are a number of signals emitted by some physical objects or sources. These physical sources could be, for example, different brain areas emitting electric signals; people speaking in the same room, thus emitting speech signals; or mobile phones emitting their radio waves. Assume further that there are several sensors or receivers. These sensors are in different positions, so that each records a mixture of the original source signals with slightly different weights.

For the sake of simplicity of exposition, let us say there are three underlying source signals, and also three observed signals. Denote by $x_1(t)$, $x_2(t)$ and $x_3(t)$, the observed signals, which are the amplitudes of the recorded signals at time point t , and by $s_1(t)$, $s_2(t)$ and $s_3(t)$ the original signals. The $x_i(t)$ are then weighted sums of the $s_i(t)$, where the coefficients depend on the distances between the sources and the sensors:

$$\left.\begin{aligned} x_1(t) &= a_{11}s_1(t) + a_{12}s_2(t) + a_{13}s_3(t) \\ x_2(t) &= a_{21}s_1(t) + a_{22}s_2(t) + a_{23}s_3(t) \\ x_3(t) &= a_{31}s_1(t) + a_{32}s_2(t) + a_{33}s_3(t) \end{aligned}\right\} \quad (۲.۵)$$

The a_{ij} are constant coefficients that give the mixing weights. They are assumed *unknown*, since we cannot know the values of a_{ij} without knowing all

the properties of the physical mixing system, which can be extremely difficult in general. The source signals s_i are *unknown* as well, since the very problem is that we cannot record them directly.

As an illustration, consider the waveforms in Fig.(٢.٣). These are three linear mixtures x_i of some original source signals. They look as if they were completely noisy, but actually, there are some quite structured underlying source signals hidden in these observed signals.

What we would like to do is to find the original signals from the mixtures x_1(t) , x_2(t) and x_3(t).This is the blind source separation (BSS) problem. *Blind* means that we know very little if anything about the original sources.

We can safely assume that the mixing coefficients a_{ij} are different enough to make the matrix that they form invertible. Thus there exists a matrix **W** with coefficients w_{ij} , such that we can separate the s_i as

$$\left.\begin{aligned} s_1(t) &= w_{11}x_1(t) + w_{12}x_2(t) + w_{13}x_3(t) \\ s_2(t) &= w_{21}x_1(t) + w_{22}x_2(t) + w_{23}x_3(t) \\ s_3(t) &= w_{31}x_1(t) + w_{32}x_2(t) + w_{33}x_3(t) \end{aligned}\right\} \quad (٢.٦)$$

Such a matrix W could be found as the inverse of the matrix that consists of the mixing coefficients a_{ij} in Eq.(٢.٥), if we knew those coefficie- nts a_{ij} .

Now we see that in fact this problem is mathematically similar to the one where we wanted to find a good representation for the random data in x_i(t), as :

$$\begin{pmatrix} x_1(t) \\ x_2(t) \\ \\ \end{pmatrix} \qquad \begin{pmatrix} s_1(t) \\ s_2(t) \\ \\ \end{pmatrix}$$

$$\begin{matrix} x_1(t) \\ . \\ . \\ . \\ x_n(t) \end{matrix} = A * \begin{matrix} s_1(t) \\ . \\ . \\ . \\ s_m(t) \end{matrix} \qquad (٢.٧)$$

Indeed, we could consider each signal x_i(t), t= ١….T as a sample of a random variable x_i , so that the value of the random variable is given by the amplitudes of that signal at the time points recorded [٣٢].

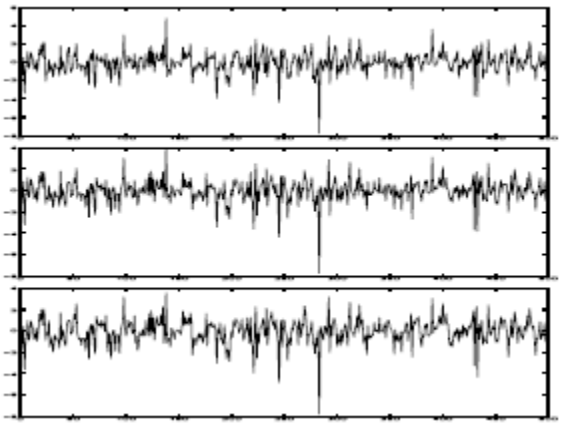


Figure (٢.٣) The observed signals that are assumed to be mixtures of some underlying source signals.

٢. ٩ ***Fidelity Criteria:***

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, Whereas the

second requires the definition of qualitative scale to assess image quality, and this scale can then be used by human test subjects to determine image fidelity.

In order to provide unbiased results, evaluation with subjective measure requires careful of the test subjects and carefully-designed evaluation experiments. The objective criteria are useful as relative measures in comparison with different versions of the same image.

a- Root Mean Square Error(RMSE):-

We can define the error between an original, uncompressed pixel value and the reconstructed(decompressed) pixel value as :

$$\text{Total Error} = \sum_{r=0}^{N-1}\sum_{c=0}^{M-1}[I^{'}(r,c) - I(r,c)] \qquad (٢.٨)$$

The root-mean-square error is found by taking the square root ("root") of the error squared ("square") divided by the total number of pixels in the image ("mean"):

$$\text{RMSE} = \sqrt{\frac{\sum_{r=0}^{N-1}\sum_{c=0}^{M-1}[I^{'}(r,c) - I(r,c)]^2}{(N \times M)}} \qquad (٢.٩)$$

The smaller the value of the error metrics , the better the reconstructed image [٣٤].

b- Signal to Noise Ratio(SNR):-

The (SNR) metrics consider the decompressed image to be the "signal" and the error to be "noise" . We can define the signal-to-noise ratio as [٣٤] :-

$$SNR= \sqrt{\frac{\sum_{r=0}^{N-1}\sum_{c=0}^{M-1}[I^{'}(r,c)]^2}{\sum_{r=0}^{N-1}\sum_{c=0}^{M-1}[I^{'}(r,c)-I(r,c)]^2}} \qquad (٢.١٠)$$

Another related metric is the Peak Signal-to-Noise Ratio, (PSNR) which is defined as

$$PSNR = ١٠ \log_{١٠} \frac{(L-1)^2}{\frac{1}{(N\times M)}\times\sum_{r=0}^{N-1}\sum_{c=0}^{M-1}[I^{'}(r,c)-I(r,c)]^2} \qquad (٢.١١)$$

Where :-

M: is the height of the two images(because the two images must be the same size).

N: is the width of the two image.

r and **c** : are row and column numbers.

L: is the number of the gray levels, L= ٢٥٦ .

I(r,c) : is the original image .

I'(r,c) : is the modified image.

٣.١ ***Introduction*** :-

In the proposed system , One or more images (color , Gray) are hidden in cover image and a mixing matrix technique is chosen for implementing the steganography technique .

The proposed system depends on choosing a mixing matrix for implementing the hidden principle of embedding images in cover .

The proposed system consists of two parts : the embedding process and the extraction process. In the embedding process , the algorithm takes as an input the embedded and the cover image which is either ٨ or ٢٤ bit per pixel and the result is the stego images as an output for this process. The proposed

system requires the inverse of mixing matrix to extract the embedded image from the stego image .

In the extraction process , the algorithm takes as its input the stego image and extract the embedded image from the stego image as an output for this process .

In this chapter , the main design steps for the proposed system and its algorithms are described in detail .

٣. ٢ ***The Embedding Process*** :

The embedding process of the proposed system consists of several stages: Test stage, Dimension Transformation Stage, Mixing Image Matrix Formation Stage, Selection of Mixing Matrix Stage, the Mixing stage , Dimension Transformation Stage, and Difference Stage .

The embedding process is illustrated in the Figure (٣.١)

a- Test – stage :-

In this test , the algorithm will check the size of the cover –image and the size of the embedded image , which must be equal to the size of the cover – image .

The size of both the cover –image and embedded image is calculated using the equation:

$$S_e = \text{embedded\_ height} \times \text{embedded\_wide}$$

$$S_c = \text{cover\_ height} \times \text{cover\_wide} \qquad (٣.١)$$

Where ,

S_e : is the size of the embedded image.

S_c : is the size of the cover image .

Size test Algorithm

Input : embedded image and cover image .

Output : Return false or true.

Step١ : Open bmp file (cover image and embedded image)

Step٢: Input the embedded image and the cover image .

Step٣: Calculate the sizes of the embedded image and the cover image by performing the equation (٣.١).

Step٤: Compare between two sizes :

If Se = Sc then

Well size:= true

Else

Well size:= false

Step٥: End.

b- Dimension Transformation- Stage :-

After selection the cover and embedded image on basis of the size, will transform the cover and embedded image from two dimensional matrix into a single dimensional (vector).

Dimension Transformation Algorithm
Input : The embedded images and cover image .
Output : Matrices of one dimension

Step١: x=١;
Step٢: For i=١ to cover_high do step٣ to step٩
Step٣: For j=١ to cover_wide do step٤ to step٨
Step٤: Vector١(x)=Cover-image(i , j);
Step٥: Vector٢(x)=Embedded-image١(i , j);
Step٦: Vector٣(x)=Embedded-image٢(i , j);
Step٧: Vectorn(x)=Embedded-imagen-١(i , j);
Step٨: x=x+١;
Step٩: End.

c- Mixing Image Matrix Formation-Stage :-

After completing the dimension transformation , will establish a matrix in which each row is a single dimensional matrix. Mean while the number of rows in it is the same as the input images to the system (for instance the first row of the new matrix is a single dimensional (vector) which is the cover image) .

The second row of the matrix is one dimensional which is the hiding image.

In case of hiding more than one image in the same time , the suitable mechanism which is supposed to be followed is adding the new image (second one ,i.e. the hiding image) after transformation it to a single dimensional (vector) as a third row of the established .

In the first case , the matrix consists of two rows and the number of columns of this matrix has the same size as the image (height × width) .

In the second case , the dimensions would be ; the number of rows of the matrix is the same as the input images (Cover and Hiding).

Mixing Image Matrix Formation Algorithm

Input : Matrices of one dimension (cover image and embedded images)

Output: Matrix of Images wanted mixing

Step١: f= cover_ height × cover_wide

Step٢: x=١;

Step٣: For j=١ to f do step٤ to step٨

Step٤: Matrix of images(١,j)= Vetor١(x)

Step٥: Matrix of images(٢,j)= Vetor٢(x)

Step٦: Matrix of images(٣,j)= Vetor٣(x)

Step٧: Matrix of images(n,j)= Vetorn(x)

Step٨: x=x+١

Step٩: End.

d- Selection of Mixing Matrix- Stage:-

After completing the transformation of input images into a single dimensional image (vector) , We will select the suitable mixing matrix which could give us a good mixing result.

There are two conditions to choose the mixing matrix:-

١. The mixing image must be a square.

٢. The mixing matrix multiplication by inverse matrix of mixing equal to union matrix .

For instance , if we input two images (cover image and hidden image) the size of the mixing matrix should be two rows and two columns.

In case of inputting three images (cover image and two hidden images) the size of mixing matrix (i.e. the dimensions) would be three rows and three columns .

The example of mixing matrix is given below :

$$\begin{bmatrix} ١ & ٠ \\ & \end{bmatrix}$$

S=

٠.٥ ٠.٥

e- Mixing –Stage :-

After establishing the mixing matrix as well as selection of the suitable mixing matrix .

In this stage , will multiply the mixing matrix with mixed image , For instance , If input two images (Cover and hiding) and forming the matrix of the mixed image which has the following dimensions

Number of rows = two

Number of columns = height × width .

In this case , the mixing matrix is a square one and it's dimensions (٢× ٢)

We will multiply the mixing matrix with the matrix of the mixed image .

This process would result in a matrix which its dimensions are :-

Number of rows = two.

Number of columns = height × width .

Each row in this matrix is (Stego image) with one dimension .

Mixing Algorithm

Input : Matrix of Images wanted mixing

Output: Mixing Images

Step١: f= cover_ height × cover_wide

Step٢: For i=١ to n do step٣ to step٧

Step٣: For j=١ to f do step٤ to step٦

Step٤: For k=١ to n do step٥ to step٦

Step٥: Mixing Images(i,j) = Mixing Images(i,j) +S(i,k)× Matrix of images(i,j);

Step٦: j=j+١;

Step٧: End.

f- Dimension Transformation-Stage :-

After completing the multiplication of the mixing matrix with the mixed image , the result would be a matrix , every one of its row is (Stego image).

In this case , it would transform each row in the resulted matrix , which is (Stego image) from one dimension image into two dimensions image ; which represents the output and the number of the produced image after the transformation process is the same as the input images in the matrix of mixed image .

Dimension Transformation Algorithm

Input : Mixing Images(single dimension).

Output : Stego-Images(two dimension)

Step١: x=١;

Step٢: For i=١ to cover_high do step٣ to step٨

Step٣: For j=١ to cover_wide do step٤ to step٩

Step٤: Stego-image١(x)= Mixing Images(١,j);

Step٥: Stego-image٢(x)= Mixing Images(٢,j);

Step٦: Stego-image٣(x)= Mixing Images(٣,j);

Step٧: Stego-imagen(x)= Mixing Images(n,j);

Step٨: x=x+١;

Step٩: End.

g- Difference-Stage:

In this stage and after have more than one stego-image and to increase the security of the transmitted information to the receiver , we will calculate the difference among the stego-image١ and remnant stego-images by the following equations :-

$$\left.\begin{aligned} Diff_{١} &= Stego\text{-}image_{١} - Stego\text{-}image_{٢} \\ Diff_{٢} &= Stego\text{-}image_{١} - Stego\text{-}image_{٣} \\ Diff_{٣} &= Stego\text{-}image_{١} - Stego\text{-}image_{٤} \\ &\vdots \end{aligned}\right\} \quad (٣.٢)$$

$Diff_{n-١} = Stego\text{-}image_{١} - Stego\text{-}image_{n}$

Then we will save each difference in a single file .After that will send one file to the receiver side.

Difference Algorithm

Input : Stego-images

Output: Stego-image١ and file of difference

Step١: For i=١ to cover_ height do step٢ to step٤

Step٢: For j=١ to cover_wide do step٣ to step٥

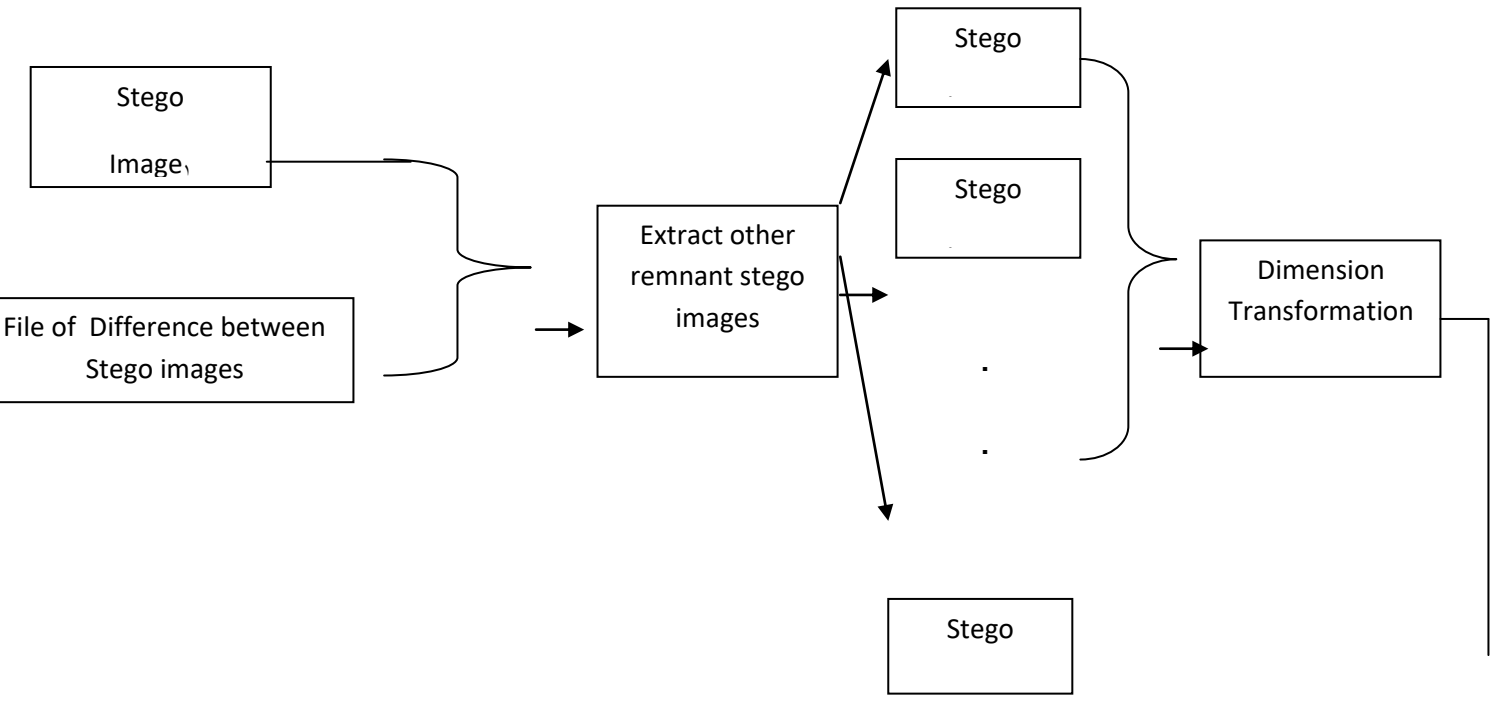
Step٣: Perform equation(٣.٢)

Step٤: save (Diff١ , Diff٢ ,..., Diffn-١) into single file format

Step٥: End.

٣.٣ ***Extraction process*** :-

To start the extraction process , the extractor must have the stego-images, and the inverse of mixing matrix to extract the original image. The extraction processes are described in Figure (٣.٢)



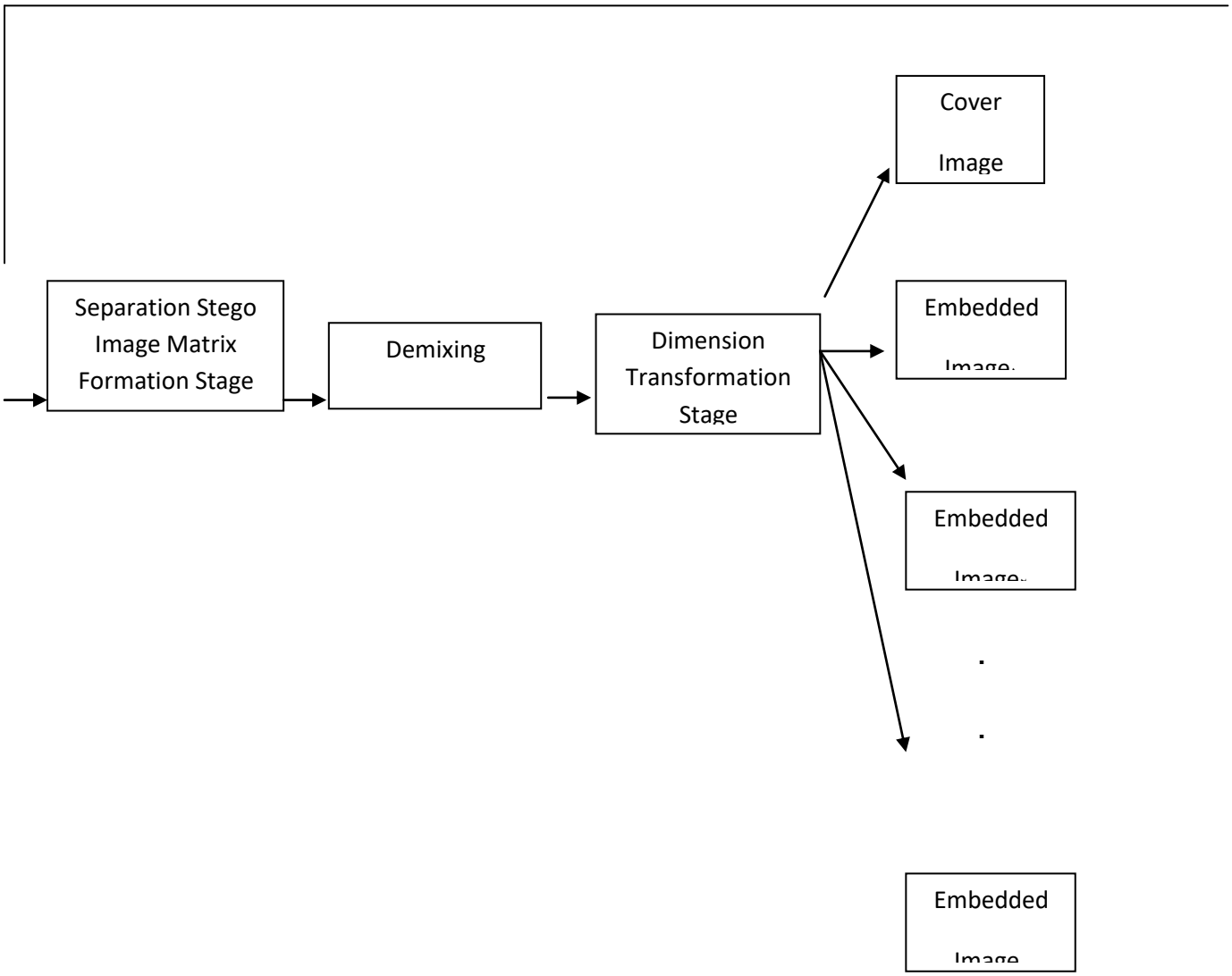


Figure (٣.٢) The Extracting Process

a- Extract remnant Stego-images – Stage:

After receiving the stego-image١ and file of difference which represent the difference among stego-image١ and other stego-images , and to get back

the remnant stego-images ($Stego_{١}$, $Stego_{٢}$,.., $Stego_{n}$) we will apply the following equation :

$$\left.\begin{array}{l} Stego\text{-}image_{٢}=Stego\text{-}image_{١}-Diff_{١} \\ Stego\text{-}image_{٣}=Stego\text{-}image_{١}-Diff_{٢} \\ \bullet \\ \bullet \end{array}\right\} \quad (٣.٣)$$

$$Stego\text{-}image_{n}=Stego\text{-}image_{١}-Diff_{n-١}$$

This will result in getting all the of stego-images without the need to send many stego-images to the receiving side (i.e. we could increase the capacity of the hiding information the over the same transmission channel).

Extract remnant Stego-images Algorithm

Input : Stego-image١ and the file of difference.

Output : Stego- images

Step١ : read from files and save to arrays

Step٢: For i=١ to stego_ height do step٣ to step٤

Step٣: For j=١ to stego_ wide do step٤ to step٥

Step٤: Perform equation(٣.٣)

Step٥: End.

b- Dimension Transformation-Stage :-

After reception the stego-images , will transform them from two dimensional matrix into a single dimensional (vector).

Dimension Transformation Algorithm

Input : The Stego-images.

Output : Matrices of one dimension

Step١: x=١;

Step٢: For i=١ to cover_high do step٣ to step٩

Step٣: For j=١ to cover_wide do step٤ to step٨

Step٤: Vector١(x)=Stego-image١(i , j);

Step٥: Vector٢(x)= Stego-image٢(i , j);

Step٦: Vector٣(x)= Stego-image٣(i , j);

Step٧: Vectorn(x)= Stego-image n-١(i , j);

Step٨: x=x+١;

Step٩: End.

c- Separation Stego Image Matrix Formation-Stage:-

In this stage , will create matrix of stego-images that will be separated; the result would be a matrix , every one of its row is (Stego image).

Separation StegoImage Matrix Formation Algorithm

Input : Matrices of one dimension (Stego-Images)

Output: Matrix of Stego-Images wanted Demixing

Step١: f= cover_ height × cover_wide

Step٢: x=١;

Step٣: For j=١ to f do step٤ to step٨

Step٤: Matrix of images(١,j)= Vector١(x)

Step٥: Matrix of images(٢,j)= Vector٢(x)

Step٦: Matrix of images(٣,j)= Vector٣(x)

Step٧: Matrix of images(n,j)= Vectorn(x)

Step٨: x=x+١

Step٩: End.

d- Demixing –Stage

In this stage , will multiply the matrix of stego-images and the inverse of mixing matrix ; the result would be a matrix , every one of its row is an image; these images are original image (Cover, hidden images).

Demixing Algorithm

Input : Matrix of Stego-images wanted Demixing

Output: Images of single dimension

Step١: W= inverse of mixing matrix;

Step٢: f= cover_ height × cover_wide

Step٢: For i=١ to n do step٣ to step٧

Step٣: For j=١ to f do step٤ to step٦

Step٤: For k=١ to n do step٥ to step٦

Step٥: Images(i,j) = Images(i,j) +W(i,k)× Matrix of images(i,j);

Step٦: j=j+١;

Step٧: End.

e- Dimension Transformation-Stage :-

After completing the multiplication of the inverse of mixing matrix with the matrix of stego- images , the result would be a matrix , every one of its row is (image) which resulted from separation of cover image and hidden images . In this case , each row in the resulted matrix will be transformed , which is the result of demixing of the covered and hiding images) which represents the output and the number of the produced image after the transformation process is the same as the input images in the matrix of stego- images .

Dimension Transformation Algorithm

Input: Images of single dimension.

Output : Original-Images(two dimension)

Step١: x=١;

Step٢: For i=١ to cover_high do step٣ to step٨

Step٣: For j=١ to cover_wide do step٤ to step٩

Step٤: Cover-image(x)= Images(١,j);

Step٥: Stego-image١(x)= Images(٢,j);

Step٦: Stego-image٢(x)= Images(٣,j);

Step٧: Stego-imagen-١(x)= Images(n,j);

Step٨: x=x+١;

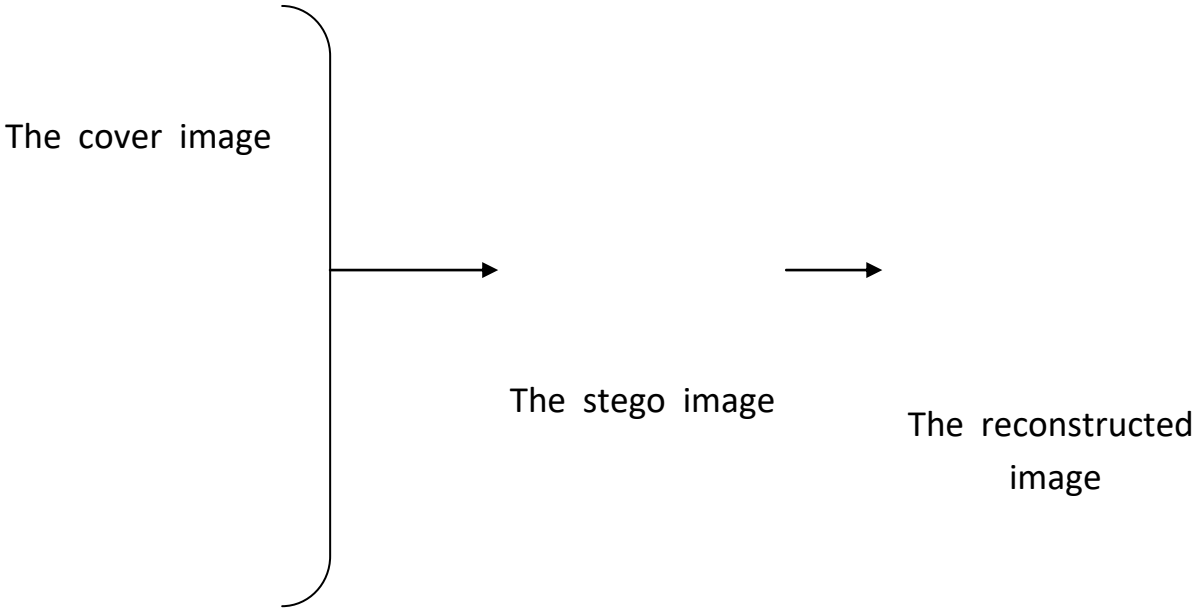
Step٩: End.

٤. ١ ***The proposed System Results*** :-

In the following examples, it is shown that the embedded images , the cover images , the stego image, which results from the embedded process , and the reconstructed image which results from the extraction process which is used and tested in the proposed system :-

Case study ١:- In this case embedded one image BMP(٢٥٦)inside an image BMP(٢٥٦).

Example ١:-



The embedded image

PSNR between the embedded image and reconstructed image	٥١.١١٣٦
RMSE	٠.٧٠٩٣
Mixing matrix	١ ٠ ٠.٥ ٠.٥

Figure (٤.١) The cover image , the embedded image , the stego image and reconstructed image

Example ٢:-

The cover image

The stego image

The embedded image

PSNR between the embedded image and reconstructed image	٥١.١٩٣٤

RMSE	٠.٧٠٢٩
Mixing matrix	١ ٠ ٠.٥ ٠.٥

[ ]

Figure (٤.٢) The cover image , the embedded image , the stego image and reconstructed image

Example ٣:-

The cover image

The stego image

The reconstructed image

The embedded image

PSNR between the embedded image and reconstructed image	٥١.١٩١٨
RMSE	٠.٧٠٣٠
Mixing matrix	$\begin{bmatrix} ١ & ٠ \\ ٠.٥ & ٠.٥ \end{bmatrix}$

Figure (٤.٣) The cover image , the embedded image , the stego image and reconstructed image

Example ٤:-

The cover image

The stego image

The reconstructed image

The embedded image

PSNR between the embedded image and reconstructed image	٥١.١٣٩٨
RMSE	٠.٧٠٧٢

Mixing matrix	$\begin{bmatrix} ١ & ٠ \\ ٠.٥ & ٠.٥ \end{bmatrix}$

Figure (٤.٤) The cover image , the embedded image , the stego image and reconstructed image

Example ٥:-

The cover image

The stego image

The reconstructed image

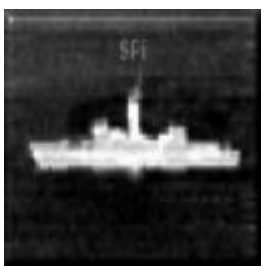
The embedded image

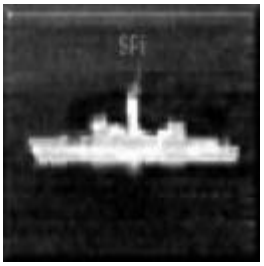
PSNR between the embedded image and reconstructed image	٥١.١٢٩٤
RMSE	٠.٧٠٨١
Mixing matrix	$\begin{bmatrix} ١ & ٠ \\ ٠.٥ & ٠.٥ \end{bmatrix}$

Figure (٤.٥) The cover image , the embedded image , the stego image and reconstructed image

Example ٦:-

The cover image





The embedded image

The stego image

The reconstructed image

PSNR between the embedded image and reconstructed image	٥١.١٩٥٠
RMSE	٠.٧٠٢٧
Mixing matrix	$\begin{bmatrix} ١ & ٠ \\ ٠.٥ & ٠.٥ \end{bmatrix}$

Figure (٤.٦) The cover image , the embedded image , the stego image and reconstructed image

Example [٧]:-

The cover image

The stego image

The reconstructed image

The embedded image

PSNR between the embedded image and reconstructed image	٥١.١٦١٨
RMSE	٠.٧٠٥٤
Mixing matrix	$\begin{bmatrix} ١ & ٠ \\ ٠.٥ & ٠.٥ \end{bmatrix}$

Figure (٤.٧) The cover image , the embedded image , the stego image and reconstructed image

Case study ٢: In the following example embedded one image RGB(true color)inside image RGB (true color).

Example ١:-

The cover image

The embedded image

The stego image

The reconstructed image

PSNR between the embedded image and reconstructed image	٥١.٣٥٩٣
RMSE	٠.٦٨٩٧
Mixing matrix	$\begin{bmatrix} ١ & ٠ \\ ١ & ٠.٥ \end{bmatrix}$

Figure (٤.٨) The cover image , the embedded image , the stego image and reconstructed image

Example ٢:-

The cover image

The stego image

The reconstructed image

The embedded image

PSNR between the embedded image and reconstructed image	٥١.١٥١٦
RMSE	٠.٧٠٦٣
Mixing matrix	$\begin{bmatrix} ١ & ٠ \\ ١ & ٠.٥ \end{bmatrix}$

Figure (٤.٩) The cover image , the embedded image , the stego image and reconstructed image

Example ٣:-

The cover image

The stego image

The reconstructed

The embedded image

PSNR between the embedded image and reconstructed image	٥٠.٦٠٣٦
RMSE	٠.٧٥٢٢
Mixing matrix	$\begin{bmatrix} ١ & ٠ \\ ١ & ٠.٥ \end{bmatrix}$

Figure (٤.١٠) The cover image , the embedded image , the stego image and reconstructed image

Example ٤:-

The cover image

The stego image

The reconstructed image

The embedded image

PSNR between the embedded image and reconstructed image	٥١.٣٤٥٣
RMSE	٠.٦٩٠٨
Mixing matrix	$\begin{bmatrix} ١ & ٠ \\ ١ & ٠.٥ \end{bmatrix}$

Figure (٤.١١) The cover image , the embedded image , the stego image and reconstructed image

Example ٥:-

The cover image

The stego image

The reconstructed image

The embedded image

PSNR between the embedded image and reconstructed image	٥١.١٣٩٠
RMSE	٠.٧٠٧٣
Mixing matrix	$\begin{bmatrix} ١ & ٠ \\ ١ & ٠.٥ \end{bmatrix}$

Figure (٤.١٢) The cover image , the embedded image , the stego image and reconstructed image

Example ٦:-

The cover image

The stego image

The reconstructed image

The embedded image

PSNR between the embedded image and reconstructed image	٥١.١٣٨٧
RMSE	٠.٧٠٧٣
Mixing matrix	$\begin{bmatrix} ١ & ٠ \\ ١ & ٠.٥ \end{bmatrix}$

Figure (٤.١٣) The cover image , the embedded image , the stego image and reconstructed image

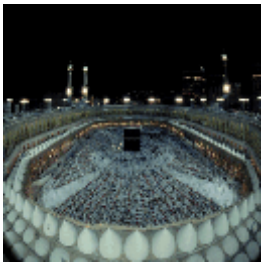
Case study ٣: In the following example embedded one image BMP(٢٥٦) inside an image RGB (true color).

Example ١:-

The cover image

The stego image

The reconstructed image



The embedded image

PSNR between the embedded image and reconstructed image	٥٢.٧٨٠٧

RMSE	٠.٥٨٥٥
Mixing matrix	$\begin{bmatrix} ١ & ٠ \\ ٠.٥ & ٠.٥ \end{bmatrix}$

Figure (٤.١٤) The cover image , the embedded image , the stego image and reconstructed image

Example ٢:-

The cover image

The embedded image

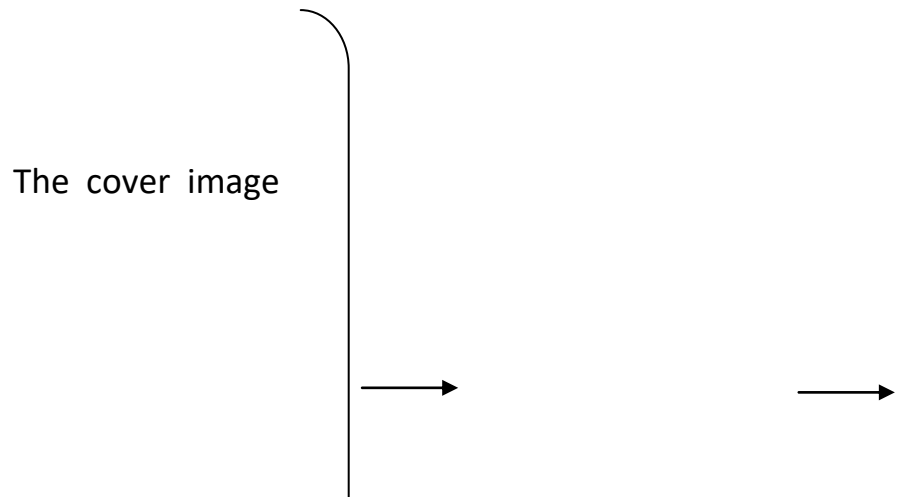
The stego image

The reconstructed image

PSNR between the embedded image and reconstructed image	٥١.١٩١٢
RMSE	٠.٧٠٣٠
Mixing matrix	$\begin{bmatrix} ١ & ٠ \\ ٠.٥ & ٠.٥ \end{bmatrix}$

Figure (٤.١٥) The cover image , the embedded image , the stego image and reconstructed image

Example ٣:-



The stego image

The reconstructed image

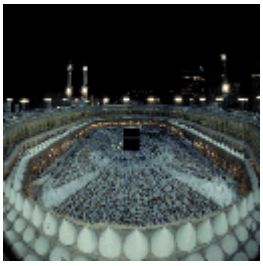
The embedded image

PSNR between the embedded image and reconstructed image	٥١.١٢٤٢
RMSE	٠.٧٠٨٥
Mixing matrix	$\begin{bmatrix} ١ & ٠ \\ ٠.٥ & ٠.٥ \end{bmatrix}$

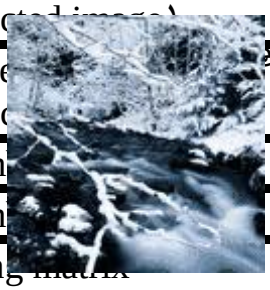
Figure (٤.١٦) The cover image , the embedded image , the stego image and reconstructed image

Case study ٤:- In the following example embedded two image BMP(٢٥٦)inside an image BMP (٢٥٦).

Example ١:-



The cover image	The embedded image.
PSNR between the embedded image and reconstructed image١	٥٢.٨٦٥٩
PSNR between the e and onstruc	٥١.٢٥١٢
of em	٠.٥٧٩٨
of em	٠.٦٩٨٢
Mixing matrix	٠ ٠ ٠ ٠.٥ ٠.٥ ٠.٠١



Example ٢:-


Figure (٤.١٧) The cover image , the embedded images , the stego image and reconstructed images

The cover image

The embedded image١

The embedded image٢

The reconstructed image١

The stego image

The reconstructed image٢

PSNR between the embedded image١ and reconstructed image١	٥١.٠٣٥٨
PSNR between the embedded image٢ and reconstructed image٢	٥٢.٠٨٩٤
RMSE of embedded image١	٠.٧١٥٧
RMSE of embedded image٢	٠.٦٣٤٠
Mixing matrix	١ ٠ ٠ ١ ٠ ٠.٥ ١ ٠.٥ ٠.٠١

Figure (٤.١٨) The cover image , the embedded images , the stego image and reconstructed images

Example ٣:-

The stego image

The reconstructed image١

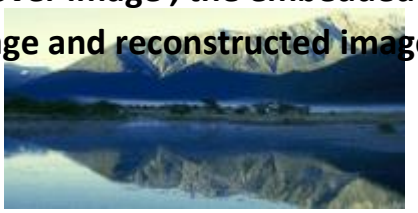
The reconstructed image٢

PSNR between the embedded image١ and reconstructed image١	٥١.١١٨١
PSNR between the embedded image٢ and reconstructed image٢	٥١.٣٠٠٣
RMSE of embedded image١	٠.٧٠٩٠
RMSE of embedded image٢	٠.٦٩٤٣
Mixing Matrix	١ ٠ ٠ ١ ٠ ٠.٥ ١ ٠.٥ ٠.٠١

***Example ٤*:-**

Figure (٤.١٩) The cover image , the embedded images , the stego image and reconstructed images

The cover image



The embedded image١

The embedded image٢

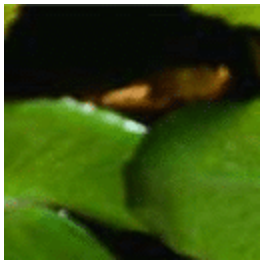
The stego image

The reconstructed image١ The reconstructed image٢

PSNR between the embedded image١ and reconstructed image١	٥١.٠٦٨٧
PSNR between the embedded image٢ and reconstructed image٢	٥١.٠٢٣٣
RMSE of embedded image١	٠.٧١٣٠
RMSE of embedded image٢	٠.٧١٦٨
Mixing matrix	١ ٠ ٠ ١ ٠ ٠.٥ ١ ٠.٥ ٠.٠١

Figure (٤.٢٠) The cover image , the embedded images , the stego image and reconstructed images

Case study ٥:- In the following example embedded two image(RGB)inside an image (RGB).


Example ١

The cover image

image١ The embedded image٢

The stego image

The reconstructed image٢

PSNR between the embedded image١ and reconstructed image١	٥١.٧٤١٥

PSNR between the embedded image٢ and reconstructed image٢	٤٣.٧٧٥٠
RMSE of embedded image١	٠.٦٦٠١
RMSE of embedded image٢	٣.٥٧٢٥
Mixing matrix The reconstructed image١	١ ٠ ٠ ١ ٠ ٠.٥ ١ ٠.٥ ٠.٠١

Example ٢:-



Figure (٤.٢١) The cover image , the embedded images , the stego image and reconstructed images

The cover image The ge١ The embedded image٢

The stego image

PSNR between the embedded image١ and reconstructed image١	٥١.٣٤٦٣
PSNR between the embedded image٢ and reconstructed image٢	
MSE of embedded image١	
MSE of embedded image٢	
Mixing matrix	٠ ٠.٢ ٠.٠١ ٠.٥ ٠.٩٠

Figure (٢.٢) The cover image, the embedded images, the stego image and reconstructed images

Case study ١:- In the following example embedded three image BMP(٣٢×٣٢) inside an image BMP (٤٠٠×٤٠٠).

Example ١

The cover image

The embedded

The embedded

The embedded image٣

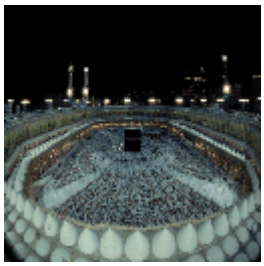
The reconstructed image١	The reconstructed image٢	The reconstructed image٣
PSNR between the embedded image١ and reconstructed image١	٣٨.٧٥٥٥	
PSNR between the embedded image٢ and reconstructed image٢	٣٨.٧٠٩٧	
PSNR between the embedded image٣ and reconstructed image٣	٤٤.٢٣٢١	
RMSE of embedded image١	٢.٩٤٢٨	
RMSE of embedded image٢	٢.٩٥٨٤	
RMSE of embedded image٣	١.٥٦٦٥	
Mixing matrix	١ ٠ ٠ ٠ ٠.٩٠ ٠.٠٢ ٠.٠١ ٠.٢٠ ٠.٩٠ ٠.١ ٠.٠١ ٠ ٠.٩٠ ٠.٠١ ٠.١ ٠	

Example ٢:-

The cover image

The embedded image١

The embedded image٢



The embedded image٣

Figure (٤.٢٣) The cover image , the embedded images , the stego image and reconstructed images

The stego image

PSNR between the embedded image١ and reconstructed image١	٣٧.٩١٥٦
PSNR between the embedded image٢ and reconstructed image٢	٣٨.٠١٨٠
PSNR between the embedded image٣ and reconstructed image٣	٤٤.٨٨٦٨
RMSE of embedded image١	٣.٢٤١٦
RMSE of embedded image٢	٣.٢٠٣٦
RMSE of embedded image٣	١.٤٥٢٨
Mixing matrix	١ ٠ ٠ ٠ ٠.٩٠ ٠.٠٢ ٠.٠١ ٠.٢٠ ٠.٩٠ ٠.١ ٠.٠١ ٠ ٠.٩٠ ٠.٠١ ٠.١ ٠

The reconstructed image١

The reconstructed image٢

The reconstructed image٣

٤.٢ ***Discussion the results***:-

In case study١, the mixing matrix

$$\begin{bmatrix} ١ & ٠ \\ ٠.٥ & ٠.٥ \end{bmatrix}$$

is considered good results because the PSNR between the embedded image and reconstructed image equal (٥١.١٩٣٤) and the embedded process will be invisible and less distortion in the stego and reconstructed image.

Figure (٤.٢٤) The cover image , the embedded images , the stego image and reconstructed images

In case study٢, the mixing matrix

$$\begin{bmatrix} ١ & ٠ \\ ٠.٥ & ٠.٦ \end{bmatrix}$$

is considered good results because the PSNR between the embedded image and reconstructed image equal (٥٣.٤٩٨٩) and the embedded process will be invisible and less distortion in the stego and reconstructed image.

In case study٣, the mixing matrix

$$\begin{bmatrix} ١ & ٠ \\ ٠.٥ & ٠.٥ \end{bmatrix}$$

is considered good results because the PSNR between the PSNR between the embedded image and reconstructed image equal (٥٢.٧٨٠٧) and the embedded process will be invisible and less distortion in the stego and reconstructed image.

In case study٤, the mixing matrix

$$\begin{bmatrix} ١ & ٠ & ٠ \\ ١ & ٠ & ٠.٥ \\ ١ & ٠.٥ & ٠.٠١ \end{bmatrix}$$

is considered good results because the PSNR between the embedded image١ and reconstructed image١ equal (٥٢.٨٦٥٩) and the PSNR between the embedded image٢ and reconstructed image٢ equal (٥١.٢٥١٢) and the embedded process will be invisible and less distortion in the stego and reconstructed image.

In case study٥, the mixing matrix

$$\begin{bmatrix} ١ & ٠ & ٠ \\ ١ & ٠.٠١ & ٠.٢ \\ ٠.٩٠ & ٠.٥ & ٠.٠١ \end{bmatrix}$$

is considered good results because the PSNR between the embedded image١ and reconstructed image١ equal (٥١.٧٤١٥) and the PSNR between the embedded image٢ and reconstructed image٢ equal (٤٣.٧٧٥٠) and the

embedded process will be invisible and less distortion in the stego and reconstructed image.

In case study٦, the mixing matrix

$$\begin{bmatrix} ١ & ٠ & ٠ & ٠ \\ ٠.٩٠ & ٠.٠٢ & ٠.٠١ & ٠.٢٠ \\ ٠.٩٠ & ٠.١ & ٠.٠١ & ٠ \\ ٠.٩٠ & ٠.٠١ & ٠.١ & ٠ \end{bmatrix}$$

is considered good results because the PSNR between the embedded image١ and reconstructed image١ equal (٣٨.٧٥٥٥) and the PSNR between the embedded image٢ and reconstructed image٢ equal (٣٨.٧٠٩٧) , the PSNR between the embedded image٣ and reconstructed image٣ equal (٤٤.٢٣٢١) and the embedded process will be invisible and less distortion in the stego and reconstructed image.

٥.١ ***Conclusions:-***

After having performed the proposed stegosystem, the following conclusions can be reached :-

١.The proposed system can be defined as a secret key steganography system .It is a secret key between the sender and the receiver.The stego key represented by mixing matrix .Without knowledge of the stego key , the receiver cannot extract the original message.

٢. The good quality of both stego and reconstructed images is achieved as shown when applying the PSNR test.

٣.The similarity between the cover image and stego images١ can be

	PSNR between the embedded image and reconstructed image	RMSE	Mixing matrix

considered very good because using a suitable mixing matrix .

٤.The embedded image that is used in proposed system is one or more images in cover image, this capacity can be considered good.

٥. The imperceptibility of stego image is achieved as shown when applying Peak Signal-to-Noise Ratio(PSNR) measure.

٦.The appropriate mixing matrix for images BMP (٢٥٦), it is not necessarily to be appropriate for images(RGB).

٥.٢ ***Suggestion for Future Work:***

١.Using another image file format rather than BMP format .

٢.Using genetic algorithm to choice a suitable mixing matrix .

٣.Applying the proposed system to hide sound and text inside image

٤.Compression file of difference, it using in our previous work .

Table (١) The tests for using difference Mixing Matrix to embedded image BMP i
an image BMP

Case Stady ١	٢١.١١٤	٠.٧٠٧١	١ ٠ ٠.٥ ٠.٥
	٤٢.٣٥٦٥	١.٩٤٤١	١ ٠ ٠.٥ ٠.٦
	٣٤.٨٠٨٦	٤.٦٣٥٧	١ ٠ ٠.٦ ٠.٦
	٢٠.٥٤٧٨	٢٣.٩٤١٤	١ ٠ ٠.٩ ٠.٦
	٣٣.٦٢٧٠	٥.٣١١٢	١ ٠ ٠.٩ ٠.١
	١٤.٦٧٣٣	٤٧.٠٨٤٤	١ ٠ ٠.٩ ٠.٠١
	٣٨.٤٦٢٤	١٦.٤٣٠١	١ ٠ ٠.٣ ٠.٣
	٣٣.٦٢٧٠	٥.٣١١٢	١ ٠ ٠.٩٠ ٠.١
	٢٨.٤٠٨٩	٩.٦٨٤٩	١ ٠ ٠.٩٠ ٠.٣
	٣٤.٤٤٠١	٤.٨٣٦٦	١ ٠ ٠.٩٠ ٠.٢

Table (٢) The tests for using difference Mixing Matrix to embedded image RGB inside an image RGB

	PSNR between the embedded image and reconstructed image	RMSE	Mixing matrix
Case Stady ٢	٥٢.٦٩٠٣	٠.٥٩١٦	١ ٠ ٠ ٠.٦ ٠.٥
	٥٣.٤٩٨٩	٠.٥٤٠٩	١ ٠ ٠ ٠.٥ ٠.٦
	٣٧.١٣٥١	٣.٦٦١١	١

			٠ ٠.٥ ٠.٩
	٢٨.٧٦٩٩	١٤.٣٠٠٣	١ ٠ ٠ ٠.٩
	٢٩.١٥١٨	١٣.٧٢٤٧	١ ٠ ٠.٠١ ٠.٩
	٣٧.٨٣٧٥	٩.٧١٤٦	١ ٠ ٠.٣ ٠.٣
	٤٨.٣٣٤٩	٠.٩٧٦٨	١ ٠ ٠.٩ ٠.٣
	١٧.٨٩١٨	٥٠.٩٦٠٦	١ ٠ ٠.٠٩ ٠.٣
	٢٤.٨٩٣٦	١٤.٥١٦٥	١ ٠ ٠.٥ ٠.٠٢

Table(٣) The tests for using difference Mixing Matrix to embedded image BMP inside an image RGB

	PSNR between the embedded image and reconstructed image	RMSE	Mixing ma
Case Stady ٣	٤٥.٣٣٨١	١.٣٧٩٢	٠ ٠.٥ ٠.٦
	١٤.١٥٥٧	٤٩.٩٧٥٤	١

A-٢

			٠ ٠.٩ ٠.٦
	١١.٢٨٥٢	٦٩.٥٤٧٦	١ ٠ ١ ٠.٦
	٥٢.٧٨٠٧	٠.٥٨٥٥	١ ٠ ٠.٥ ٠.٥
	٣٥.٣٦٩١	٤.٣٤٥٩	١ ٠ ٠.٩ ٠.١
	٣٥.٠١٨١	٤.٥٢٥٢	١ ٠ ٠.٧ ٠.١
	٤٠.٢٩٨٣	٢.٤٦٣٩	١ ٠ ٠.٧ ٠.٢
	٢١.١٠٠٠	٢٢.٤٦٦٦	١ ٠ ٠.٣ ٠.٦
	٣٥.٤٢٠٤	٤.٣٢٠٤	١ ٠ ٠.٨ ٠.١

difference Mixing Matrix to embedded two image BMP inside

e embedded onstructed ١	PSNR between the embedded image٢ and reconstructed image٢	RMSE١	RMSE٢	
٩٧	١٠.٤٩٧٠	١.٤١٢٧	٧٦.١٥٣٥	١ ١

A-٣

				١ ٠.٥ ٠.٠١
٦٢	١٩.٥٨٢٨	٦٢.٤٠٦٥	٢٦.٧٥٤٧	١ ٠ ٠ ١ ٠.٢ ٠.٥ ١ ٠ ٠.٠١
٠٥	٣١.٧٢٢٢	١١.٣٢٤٣	٦.٦١٣٥	١ ٠ ٠ ١ ٠.١ ٠.٥ ١ ٠.١ ٠.٢
٦٥	٥٢.٠٨٩٤	٢.٩١٨٩	٠.٦٣٤٠	١ ٠ ٠ ١ ٠ ٠.٥ ١ ٠.١ ٠.١
١٦	٤٩.٧٥٢٧	٢.٩٧١٤	٠.٨٢٩٧	١ ٠ ٠ ١ ٠ ٠.٤ ١ ٠.١ ٠.١
٥٧	٣٨.٠٧٩٢	٤.٣١٧٧	٣.١٨١١	١ ٠ ٠ ١ ٠ ٠.١ ١ ٠.١ ٠.١
٥٩	٥١.٢٥١٢	٠.٥٧٩٨	٠.٦٩٨٢	١ ٠ ٠ ١ ٠ ٠.٥ ١ ٠.٥ ٠.٠١

ing difference Mixing Matrix to embedded two image RGB inside

A-٤

embedded nstructed	PSNR between the embedded image٢ and reconstructed image٢	RMSE١	RMSE٢	
٦٩	٤٢.١٣٦٦	٠.٦٩٩٩	٢.١٢٠٥	١ ٠ ٠ ١ ٠.٠١ ٠.٢ ٠.٩٠ ٠.٥ ٠.٠١
٥٠	٤٢.١٤٢٣	١.١٢٢٠	٢.١١٨٨	١ ٠ ٠ ١ ٠.٠١ ٠.٢ ٠.٩٠ ٠.٧ ٠.٠١
٦٨	٤٣.٧٣٣٧	١.١٢٦٨	٣.٧٠٦٩	١ ٠ ٠ ١ ٠.٠١ ٠.٥ ٠.٩٠ ٠.٧ ٠.٠١
٦٢	٤٣.٧٢٥٧	١.٥٠٢٣	٣.٧٠٧٣	١ ٠ ٠ ١ ٠.٠١ ٠.٥ ١ ٠.٧ ٠.٠١
١٥	٤٣.٧٧٥٠	٠.٦٦٠١	٣.٥٧٢٥	١ ٠ ٠ ١ ٠ ٠.٥ ١ ٠.٥ ٠.٠١
٨٥	٢٠.٨٣٦٢	٥.٤٣٥٨	٣٠.٣٩٢٦	١ ٠ ٠ ١ ٠.٩ ٠.٥

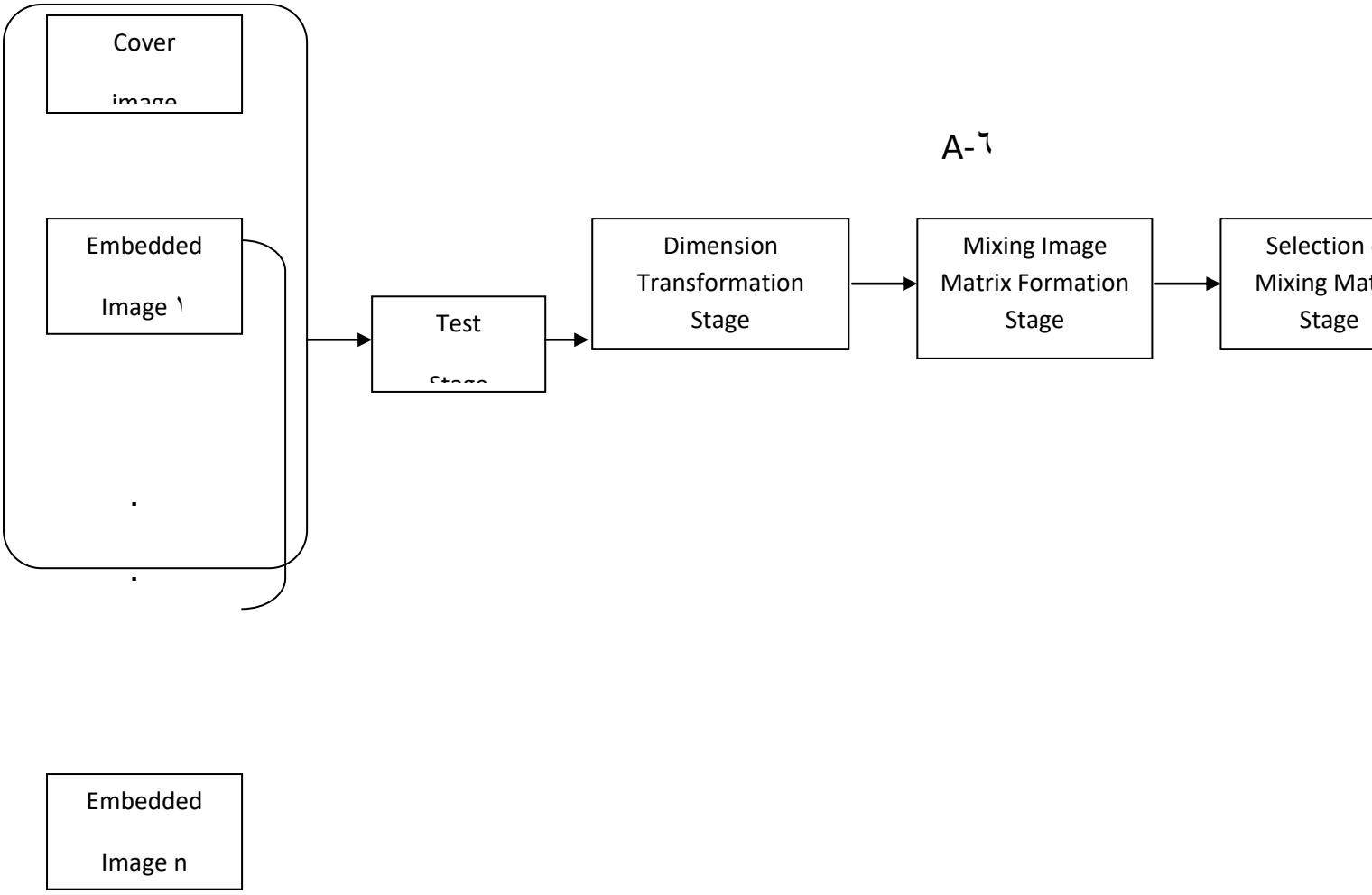
				١	٠.١	٠.٠١
٦٢	١٣.١٢٩٣	٣٩.٩١٦٦	٥٦.٥٩٤٩	١	٠	٠
				١	٠.٩	٠.٥
				١	٠.٠١	٠.٠١

Table(٦) The tests for using difference Mixing Matrix to embedded three image BMP an image BMP

	PSNR between the embedded image١ and reconstructed image١	PSNR between the embedded image٢ and reconstructed image٢	PSNR between the embedded image٣ and reconstructed image٣	RMSE١	RM	A-٥	ing rix
Case Stady ٦	٣٨.٦٧٩ ٨	٣٨.٦٨٤ ٠	٤٢.٨١٠ ٤	٢.٩٦٨ ٦	٢.٩٦٧١	١.٨٤٥١	١ ٠ ٠.٢٠ ٠.٠٧ ٠.٠٢ ٠.٩٠ ٠.٩٠ ٠.١ ٠.٠١ ٠ ٠.٩٠ ٠.٠١ ٠.١
	٣٨.٦٧٩ ٨	٣٨.٦٨٤ ٠	١٢.٦٨٥ ٥	٢.٩٦٨ ٦	٢.٩٦٧١	٥٩.١٩٢ ٢	١ ٠ ٠ ٠.٢٠ ٠.٠٧ ٠.٠٢ ٠.١ ٠.٩٠ ٠.١ ٠.٠١ ٠

٠.٩٠ ٠.٠١ ٠.١ ٠							
١ ٠ ٠ ٠.٢٠ ٠.٠١ ٠.٠٢ ٠.٩٠ ٠.٩٠ ٠.١ ٠.٠١ ٠ ٠.٩٠ ٠.٠١ ٠.٧ ٠	١.٦٧١١	٢٤.٤٢٢ ٣	٣.٥٣٠ ٩	٤٣.٦٧٠ ٥	٢٠.٣٧٥ ١	٣٧.١٧٣ ٠	
١ ٠ ٠ ٠.٢٠ ٠.٠١ ٠.٠٢ ٠.٩٠ ٠.٩٠ ٠.١ ٠.٠١ ٠ ٠.٩٠ ٠.٠٥ ٠.٧ ٠	١.٨٢٢٥	٢٨.٧٦٧ ٨	٣.٨٣٤ ١	٤٢.٩١٧ ٧	١٨.٩٥٢ ٧	٣٦.٤٥٧ ٤	
١ ٠	١.٥٦٦٥	٢.٩٥٨٤	٢.٩٤٢ ٨	٤٤.٢٣٢ ١	٣٨.٧٠٩ ٧	٣٨.٧٥٥ ٥	

							٠ ٠.٢٠ ٠.٠١ ٠.٠٢ ٠.٩٠ ٠.٩٠ ٠.١ ٠.٠١ ٠ ٠.٩٠ ٠.٠١ ٠.١ ٠



A-٦

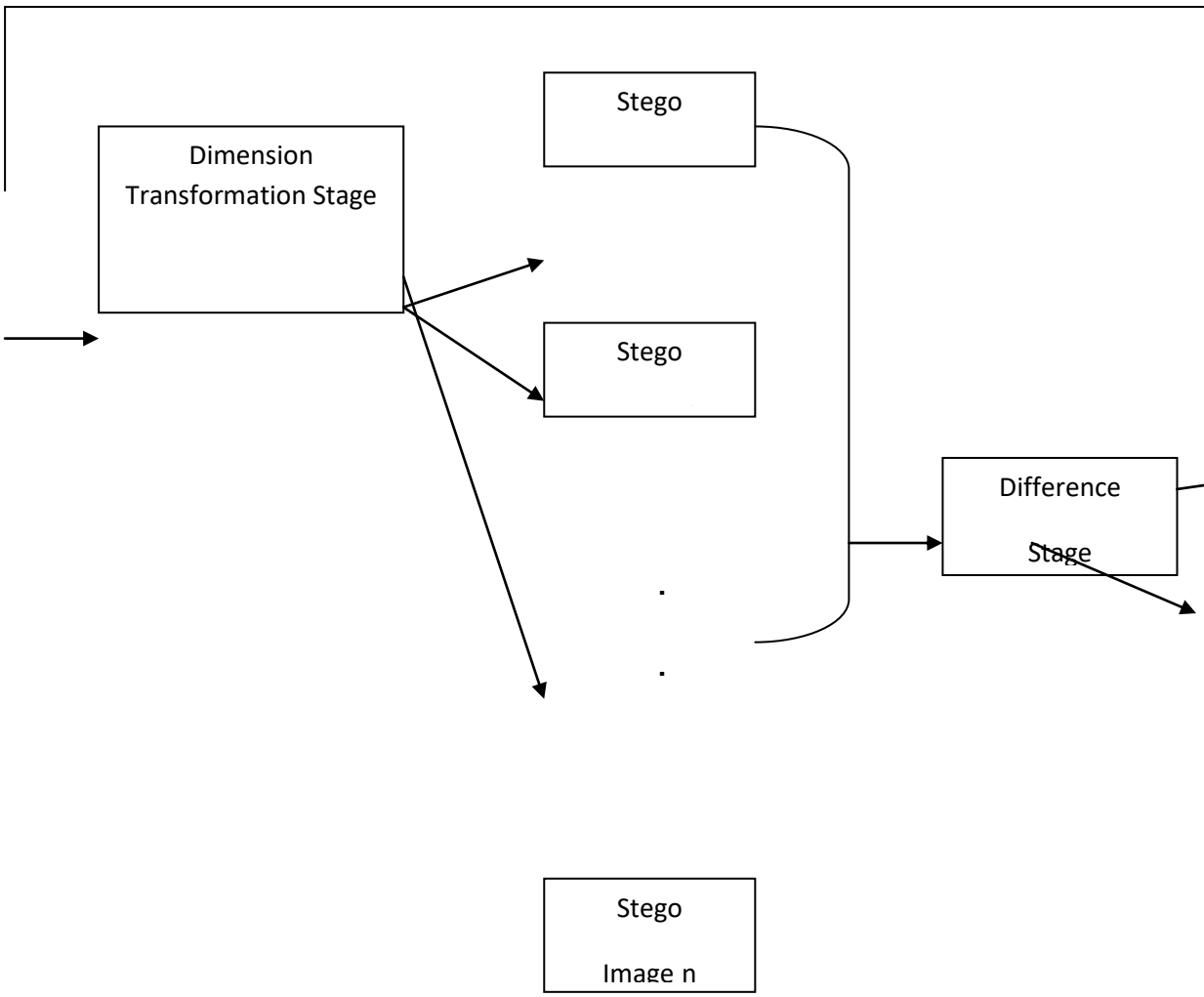


Figure (٣.١) The embedded Process of the Proposed System

References:-

[١] Min's, "**Multimedia Data Hiding**", ph. D.Thesis. Dissertation,

Princeton University , April ٢٠٠١.

[٢] W. Bender, D. Gruhal, N. Morimot and A.L.U., " **Techniques for Data Hiding** ", IBM System Journal,Vol.٣٥,No ٣ & ٤, ١٩٩٦.

[٣] F.Petitcolas, R.Anderson and M.Kuhn, "**Information Hiding- A survey** ",Proceeding of the IEEE, Special issue on protection of Multimedia Content, ٨٧(٧):١٠٦٢-١٠٧٨,jully,١٩٩٩.

[٤] H.Farid, "**Detecting Steganography Message In digital Images**", Department of Computer Science, Dartmouth College ,١٩٩٨.

[٥] L. Yeuan and C.Ling, "**High Capacity Image Steganographic Model**", IEEE Proceeding Vision, Image and Signal Processing, ١٤٧,٣,٢٨٨,(٢٠٠٠).

[٦] N.F.Johnson , S.Jajodia and Z.Dnric, "**Information Hiding: Steganography and Watermarking-Attacks and Countermeasures**", Center for Secure Information Systems, George Mason University, Boston/ Dordrecht/London,٢٠٠١.

[٧] S.Katzenbisser and F.A.Petitcolas, "**Information Hiding Techniques for Steganography and Digital Watermarking**", Artech House, USA, ٢٠٠٠.

[٨] A. Tumoas, "**Practical Invisibility In Digital Communication**", Information Hiding: First International Workshop, Proceedings, Vol. ١١٧٤ of Lecture Notes In Computer Science, Springer, ١٩٩٦,PP.٣٩-٤٨.

[٩] S. Joshua and C. Barrett, "**Modulation and Information Hiding In Images**", Information Hiding: First International Workshop, Proceedings, Vol. ١١٧٤ of Lecture Notes In Computer Science, Springer, ١٩٩٦, PP.٢٠٧-٢٢٦.

[١٠] W. Andreas and W. Gritta, "S**teganography In A Video Conferencing System**", Information Hiding: Second International Workshop, Proceedings, Vol.١٥٢٥ of Lecture Notes In Computer Science, Springer, ١٩٩٨, PP.٣٢-٤٧.

[١١] M. Lisa and B. Charles, "**Reliable Blind Information Hiding For Images**", Information Hiding: Second International Workshop, Proceeding, Vol. ١٥٢٥ of Lecture Notes In Computer Science, Springer, ١٩٩٨,PP.٤٨-٦١.

[١٢] J. Fridrich , "**A new Steganographic Method for Palette-Based**

Images", IS& TPICS conference, Savannah, Georgia, ٢٥,(١٩٩٨).

[١٣] J.J.Chae and B.S.Manjunath, "**A Technique for Image Data Hiding and Reconstruction without Host Image**", SPIEEI, ٩٩, Security and Watermarking Multimedia contents ,San Jose, California , (١٩٩٩).

[١٤] N. K. Abdulaziz, K. K. Pang, **"Robust Data Hiding for Images"**, Dept. of Electrical and Computer Systems Engineering, Monash University, Clayton, VIC ٣١٦٨, Australia, (١٩٩٦).

[١٥] J.J.Chae and B.S.Manjunath, **"Data Hiding in Video"**, Department of Electrical and Computer Engineering, University of California, Santa Barbara, CA ٩٣١٠٦-٩٥٦٠, (١٩٩٩).

[١٦] E. T. Lin and E. J. Delph, "**A Review of Data Hiding In digital Images**", PICS ٩٩, Ed., Apr.١٩٩٩.

[١٧] S. Areepongsa ,N. Kaewkamnerd,Y. F. Syed and K.R.Rao, **"Information Hiding in Image Retrieval Systems"**, ICCS,٢٠٠٠.

[١٨] S. B. Abdullah, **"Arabic Text Information Hiding"**, M.Sc. Thesis, Iraqi Commission For Computer and Informatics/ Informatics Institute for Postgraduate Studies, ٢٠٠١.

[١٩] A. M. Jafer, **"Image Steganography Using Wavelet Transform Techniques"**, M.Sc. Thesis , University of Baghdad, ٢٠٠٢.

[٢٠] هبــة محمد جعفــر الخفــاجي، نظــام لإخفــاء صــورة ملونــة داخــل صــورة ملونــة، رسالة ماجستير مقدمة إلى جامعة بابل ، كلية العلوم ،٢٠٠٣ .

[٢١] C.julio, L.Ignacio,T.Juan and G.Arturo , **"Steganography in games: A general methodology and its application to the game of Go "**, Computer Science Department, Carlos III University of Madrid, Avda. Universidad ٣٠, ٢٨٩١١ Leganés, Madrid, Spain.

[٢٢] H.Ewa, B.Derek and W.Cheong Kai , **"Data hiding in the NTFS file system "**, Department of Information Engineering and Computer Science, Feng Chia University, ١٠٠ Wenhwa Road, Seatwen, Taichung ٤٠٧٢٤, Taiwan, ROC.

[٢٣] N. F. Johnson and S. Jajodia, "**Exploring Steganography: Seeing The Unseen**", IEEE, computer,٣١ , ٢٦ , ١٩٩٨.

[٢٤] N. F. Johnson, **"Steganography In Images"**, Final Communication Report, Francesco Queirolo, ٢٠٠١.

[٢٥] L. S. Moskowitz, G. E. London and L. Chang, " **A New Paradigm Hiding in Steganography**", in New Security Paradigms , Proceeding, ACM press , ٤١ , ٢٠٠٠.

[٢٦] J. Fridrich, **"Applications of Data Hiding in digital Images"**, Tutuorial, ISPACS ' ٩٨ conference in Melbourne, Australia, (١٩٩٨).

[٢٧] N. F. Johnson, S. Jajodia, "**Steganalysis of Image Created Using Current Steganography Software**", Information Hiding: First International Workshop, Proceeding, Vol. ١٥٢٥ of Lecture Notes

In Computer Science , Springer, ١٩٩٨, PP.٢٧٣-٢٨٩.

[٢٨] A.J.Menezes, P.C.van Oorschot and S.A.Vanstone, "**Handbook of Applied Cryptography**"
http://www.cacr.math.uwaterloo.ca/hac/

[٢٩] L.Z. Avedissian, **"Image In Image Steganography System"**, Ph. D. Thesis, University of Technology, ٢٠٠٠.

[٣٠] L. Chang, "**Issues in Information Hiding Techniques**", Research supported By The Office of Naval Research,٢٠٠٢.

[٣١] W. David , **"A Graphic User Interface for Rapid Integration of Steganography Software"**, M.Sc. Thesis, Naval Postgraduate School, March, ١٩٩٦.

[٣٢] O. Hyvarinen, **"Independent Component Analysis"**

http://www.cis.hut.fi/projects/ica/book/

[٣٣] H. Aapo and O. Erkki , **"Independent Component Analysis:**

Algorithms and Applications ", Neural Networks Research Centre, Helsinki University of Technology, Finland , Neural Networks, (٢٠٠٠).

[٣٤] R. C. Gonzalez, R. E. Woods and A, Wesley, **"Digital Image Processing"**, Addison Wesley publishing Company INC., ١٩٩٢.