PEOPLE'S DEMOCRATIC REPUBLIC OF ALGERIA

Ministry of Higher Education and Scientific Research

University of Larbi Tébessi -Tébessa-

Faculty of Exact Sciences and Sciences of Nature and Life

Department of maths and informatics

MASTER MEMORY

Domain: Mathematics and Computer Science

Speciality : informatic

Option: Systems and Multimedia

Theme

Steganography of uncompressed images based on Arnold's chaotic map

Presented by

Djedouani Med Bachir

In front of the jury

Akram Bennour	MCB	University of Tebessa	Président
Rafik Menassel	MCB	University of Tebessa	Examiner
Lakhdar Laimeche	MCB	University of Tebessa	Supervisor
Abdalah Merawmia	MCA	University of Tebessa	Vice Supervisor

DATE OF GRADUATION : 08/07/2019

Note: Mention:

Acknowledgements

In the name of God and after many thanks to our God:

The work presented in this thesis has been carried out in the university of cheikh larbi TEBESSI. Faculty of Exact Sciences and Sciences of Nature and Life Mathematics and informatics department .

First of all, we would like to thank all our teachers for having given us the necessary knowledge in recent years.

We would also like to thank Mr. Lakhdar LAIMECHE, my assets framed and supported to accomplish this project. I would also like to thank Mr akrem BENNOUR , Mr. Rafik MENASSEL and Mr Abdallah MERAOUMIA .

I wish to associate these thanks to my colleagues, my friends from the university and all of us who are in my hearts.

ملخص

يمكن تعريف , الستيغانوغرافيا على أنها تقنية تسمح لنا بإدخال معلومات رقمية في حامل رقمي والذي بدوره يمكن أن يكون عبارة على صورة, نص أو فيلم, بطريقة غير مرئية. بالإضافة إلي المهام الأولي للستيغانوغرافيا وهي إخفاء المعلومات, يمكن استعمالها أيضا للمحافظة على سرية نقل المعلومات بين الأشخاص.

في هذا العمل، نقترح طريقة لإخفاء المعلومات في الصور غير المضغوطة داخل مناطق عشوائية معتمدين علي مولد الأعداد العشوائية (الجذور الأولية) و ذلك لاختيار المكان المناسب لإخفاء المعلومات .

تعتمد هذه الطريقة على خطوتين أساسيتين :نقوم أولا بالبحث علي المناطق التي يمكن أن نخفي فيها المعلومة معتمدين على مولد الأعداد العشوائية : الجذور الأولية. ثانيا نستعمل خريطة ارنولد و هذا لخلط بيكسال الصورة. الهدف من استعمال خريطة ارنولد هو إيجاد مجموعة من البيكسال في نفس المواضع التي تقلص من تشويه الصورة .

الكلمات المفتاحية: إخفاء المعلومات- ستيغانوغرافي- البت الأقل أهمية- الجذور الأولية- خريطة ارنولد.

Abstract

Steganography can be defined as a technique to insert information into a digital format that can be an image, video, sound or text, in an imperceptibly way. In addition to its applications in the embedding of information, steganography tends increasingly to be used to perform other security functions.

In this work, we propose a novel method of steganography in uncompressed images using a Pseudo Random Number Generator to generate a sequence of positions in the cover image and the Arnold's Cat Map method.

The method that we propose involves two main steps: firstly, selection of the areas that can be including the information based on the primitive root technique. Then, we apply the Arnold's cat map to shuffle the cover image pixels to obtain a novel sequence of pixels in the same selected positions that minimize the visual degradation.

Keywords: Data hiding, steganography, least significant bits, primitive root, Arnold's cat map.

Résumé

La stéganographie des images numériques peut être défini comme étant une technique qui permet d’insérer des informations dans un support numérique qui peut être une image, vidéo, son ou un texte, de manière imperceptible. En plus de ses applications dans la dissimulation d’information, la stéganographie tend de plus en plus à être utilisé pour remplir d’autres fonctions de sécurité.

Dans ce travail, nous proposons une méthode de stéganographie des images non compressées en utilisant un générateur des nombres aléatoire pour la sélection des zones capables pour l’insertion de l’information et un système chaotique basée sur la technique la carte chaotique de Arnold.

La méthode que nous avons proposé se fait en deux étapes principales: dans une première étape, nous choisissons les zones capables pour l’insertion de l’information en se basant sur la méthode des racines primitives. Après avoir terminé l’opération de sélection, la deuxième étape consiste à utiliser la carte chaotique d’Arnold pour mélanger les pixels. L’objectif de cette opération est d’obtenir une nouvelle séquence de pixels dans les mêmes positions qui minimises la distorsion entre l’image de couverture et l’image stéganographiée.

Mots clés: dissimulation d'information, stéganographie, les bits de poids faible, racines primitives, carte chaotique d’Arnold.

List of figures

List of tables

List of symbols

- AVI : Audio Video Interleave
- BMP : bitmap picture
- BPP : bits per pixel
- DCT : Discrete Consinus Transform
- DCT : Discrete Cosine Transform
- DCVT : Discrete Curvelet Transform
- DWT : Discrete Wavelet Transform
- EBE :Edges based data embedding method
- GIF : Graphics Interchange Format
- JFIF : JPEG File Interchange Format
- JPEG2000 : Joint Photographic Experts Group committe in 2000
- JPEG : Joint Photographic Experts Group
- LSB : Least Significant Bit
- MPEG : Moving Picture Experts Group
- MSE : Mean Squared Error
- PMMm : Mapping pixel to hidden data method
- PNG : Portable Network Graphics
- PSNR: Peak Signal to Noise Ratio
- PVD :Pixel value differencing
- RGB : Red, Green, and Blue
- RPE: Random pixel embedding method
- TIFF : Tagged Image File Format
- WBMP : Windows Bitmap
- WPSNR : Weighted Peak Signal to Noise Ratio
- PRNG: pseudorandom number generator

CONTENTS

Chapter I: Information Security

Chapter II: images steganography

chapter III proposed method and experimental results

general introduction

Introduction

The development of communication networks and digital media has facilitated the sharing and transfer of digital data, also introducing new forms of data piracy and new security challenges. New techniques have been developed, it is consist of cryptography and data hiding.

The confidentiality of communications is often provided by cryptography, data are undergoes a particular treatment in order to making it incomprehensible by any unauthorized person. This information, once encrypted, can be freely transmitted through a channel that can be listened to: its confidentiality is not exposed since its meaning has been completely hidden. Encrypted data attracts attention in a mass of data in the clear. It is obvious to a hacker that encrypted data is the most interesting data. In addition, the problem of protecting the content of cover medium does not yet have satisfactory solutions. It has become easy to modify or reproduce a cover medium and even claim its exploitation rights.

In order to reduce the replication of multimedia works, protect the confidentiality of a transmission, protect the integrity of data, and to contribute to the protection of copyright, new methods have been developed to enhance the security of digital data: this is the case of data hiding.

Data hiding aims is to embed secret data of any type in another cover medium that can be text, image, audio or video. The applications of data hiding are distinguished by their aims. In steganography, the goal is to hide a secret message in a cover medium to allow partners to communicate in a secret way; the cover medium has no relation with the message to send. Digital watermarking consists to insert a watermark that is related to cover medium. It is used for copyright protection, copy protection, indexing, and data integrity verification. If the embedded watermark is different for all copies of the basic cover medium, then we speak of the fingerprinting, the main purpose of the latter is to trace the source of illegal copies.

Although the objectives are distinct, these three approaches share similarities: a cover medium for hiding (its importance is related to the application), data to be hidden (secret message, watermark or sequential number) and a secret key for insertion and extraction/ detection. The difference between steganography and watermarking is that in watermarking we try to embed a watermark in the cover medium to protect the copyright or to demonstrate data integrity. Another important difference is at the level of attacks. In steganography the pirate tries to extract the hidden message in the cover medium, while in the watermarking, the pirate aims is to remove the embedded watermark form the cover medium.

In order to reduce the replication of multimedia works, protect the confidentiality of a transmission, protect the integrity of data, and to contribute to the protection of copyright, new methods have been developed to enhance the security of digital data: this is the case of steganography.

The main goal of our work is using steganography to allow persons to communicate without it being seen.

In other words, conceal the existence of the embedded secret messages in a trivial medium. In this work, we propose a steganography technique in uncompressed images using LSB technique and based on a novel pixels selection in the cover medium.

This manuscript consists of three chapters which are as follows:

- ☞ In the first chapter, we present the terminology and objectives of data hiding. Steganography, watermarking and fingerprinting are detailed to better understand the difference between these three techniques of data hiding.

Next, we describe the process of information hiding, which usually has two functions: insertion and extraction process, and then we define the criteria for information hiding. We conclude this chapter by comparing the data hiding techniques (steganography, watermarking and fingerprinting).

- ☞ In the second chapter we present the basic concepts of images. This will enable us in the remain of this chapter, to understand the application of steganography in this type of medium. Next, we present some relevant images steganography techniques in the spatial domain. We finish this chapter by presenting some metrics for evaluating the steganography techniques.
- ☞ We present in the last chapter our proposed method of steganography in uncompressed images. In a first part, we introduce the general principle of pixels selection capable for hiding data, based on the primitive root method. Then we explain how these pixels can be used to hiding secret messages and computing the secret key used in the extraction process.

Chapter I
Information Security

1.1.introduction

Is it not all about securing information from unauthorized access? Information Security is basically the practice of preventing unauthorized access, use, disclosure, disruption, modification, inspection, recording or destruction of information. Information can be physical or electrical one. Information can be anything like your details or we can say your profile on social media, your data in mobile phone, your biometrics etc. Thus Information Security spans so many research areas like Cryptography and data hiding[01].This chapter aims is to present the two domain of information security including Cryptography and data hiding and gives the differences between these two domains of information security.

1.2.Data hiding

1.2.1. Terminology

In the remainder of this manuscript, we use the terminology defined above in order to distinguish between the different data hiding schemes [02].

- ☞ Cover-medium: it is a digital medium in which data will be hidden. It can be a text, an image, a sound, a video...
- ☞ Stego-medium: once data is hidden, the cover medium becomes a stego medium.
- ☞ Data: it is the information that will be hidden in the cover medium. It can be a secret message, watermark or fingerprinting.
- ☞ Stego Key: it is an additive secret information, but essential in all the process of data hiding process.

1.2.2. *Data hiding definition*

Data hiding is a discipline that modify a given cover medium, in a prescribed manner so that secret information can be embedded in the resulting cover medium without creating noticeable artifacts [03]. The recipient can correctly extract the embedded information from the resulting medium, while other people are unaware of the existence of the secret behind the resulting medium.

Data hiding techniques can be exploited for many applications, such as covert communication, data authentication, annotation association, etc., and so have been extensively investigated in recent years [04].

1.2.3. *Data hiding classification*

Data hiding domain is composed of three techniques as shown in figure 1.

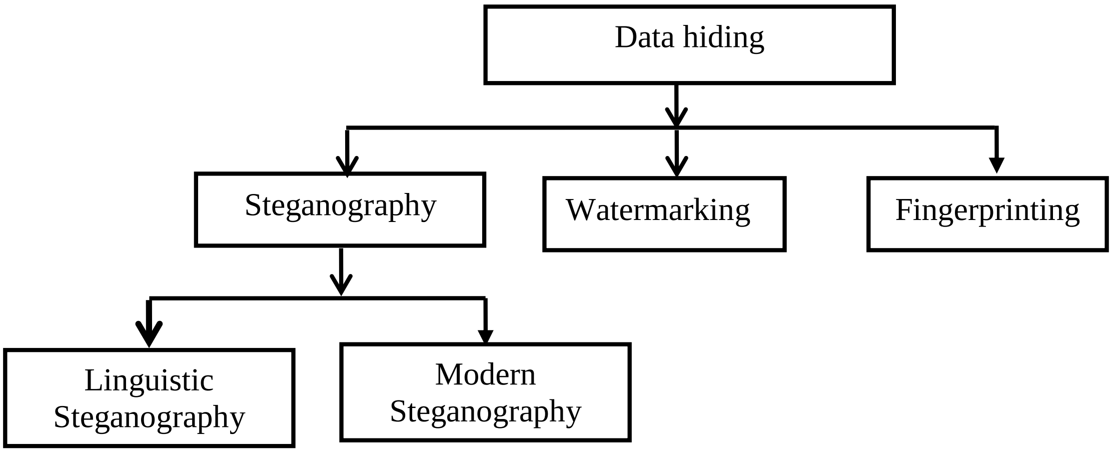


Figure 1.1 : Data hiding techniques[05]

1.2.3.1. *Steganography*

The term steganography is derived from the Greek words “steganos “(covered) and “graphy” (writing). The intention of steganography is to provide the secret transmission of data. Steganalysis provides a way of detecting the presence of hidden information[06].

A) History

The appearance of steganography, art of data hiding, is very old, and almost contemporaneous with cryptography. The first written record is found in the Histories of Herodotus (biography), published around 445 BC, through two stories. The first relates the story of Histiaeus, former tyrant of Miletus, and son-in-law of Aristagoras, the new tyrant of Miletus. Advisor of King Darius to the court of Persia, he wanted to organize a revolt against the Persians around 500 BC To convey his message to Aristagoras, he had the idea to shave the head of his most trustful slaves, to tattoo his message on their skulls and wait for the hair to grow back before sending the slaves to Miletus, with instructions to shave their hair. Of course, you should not be too eager to convey the message! [07].

Another passage in the History tells the story of Demaratus, former king of Sparta, who had taken refuge with the king of the Persians, Xerxes V, who had succeeded Darius. Demaratus was made aware of a plan to invade Greece. He then decided to prevent Sparta in all discretion using the following ploy”He took a double tablet, scraped the wax, then wrote on the wood even the plans of Xerxes, then he covered his message with wax: so the holder of a blank tablet was not in trouble [08].

The tablets having arrived at Sparta , Queen Gorgo had the wax scratched and thus discovered the message of Demaratus. These stories told by Herodotus already illustrate the two main methods of steganography used over the centuries. We can try to physically hide the existence of a message, as on the skull of a slave. Or we will hide the message on a medium that already transmits information, such as tablets of wax. These two methods have always coexisted, although the second was undoubtedly more popular.

B) Linguistic Steganography

The best known steganography process is probably the use of invisible inks, mentioned by Pliny the Elder from the 1st century BC. In the middle of the texts written in ink, a message is written to using lemon juice, milk, some chemicals, or even urine! It is invisible to the eye, but a simple flame, or a bath in a chemical reagent, reveals the message. The following example, shown in figure 2, was made using milk.

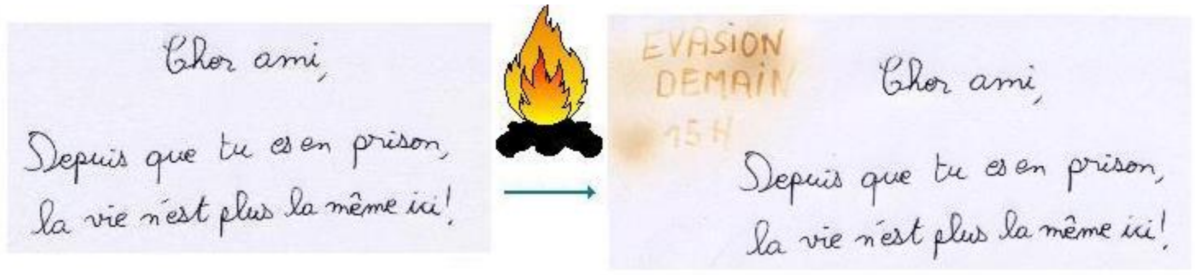
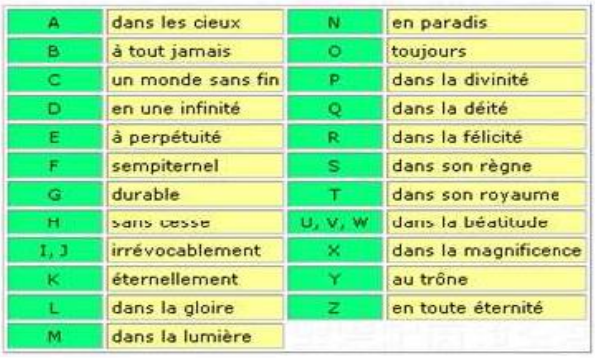

Cher ami,
Depuis que tu es en prison,
la vie n'est plus la même ici!
EVASION
DEMAIN
15 H
Cher ami,
Depuis que tu es en prison,
la vie n'est plus la même ici!

Figure 1.2: Example for using invisible ink [09]

Another widely used method of steganography is to conceal the message in the text itself. One of the masters in this field was Father Jean Tritheme. What is more common for an abbot than to write religious litanies in the slightly obscure sense, John Tritheme substituted for each letter a religious phrase as shown in figure 3. The final meaning is obscure, but what is merely a substitution is amplified by dissimulation [10].



A	dans les cieux	N	en paradis
B	à tout jamais	O	toujours
C	un monde sans fin	P	dans la divinité
D	en une infinité	Q	dans la déité
E	à perpétuité	R	dans la félicité
F	sempiternel	S	dans son règne
G	durable	T	dans son royaume
H	sans cesse	U, V, W	dans la béatitude
I, J	irrévocablement	X	dans la magnificence
K	éternellement	Y	au trône
L	dans la gloire	Z	en toute éternité
M	dans la lumière		

Figure1.3: Example of John Tritheme substitution [11].

The Second World War saw many forms of steganography. The methods were sometimes rather rudimentary, like this message sent by a German spy [12]:

> Apparently neutral's protest is thoroughly discounted and ignored. Ismam hard hit. Blockade issue affects pretext for embargo on by-products, ejecting suets and vegetable oils.

This seems quite trivial. Now, taking the second letter of each word, we get: Pershing sails from NY June 1 (the Pershing leaves New York on June 1). This explains why the Americans, who were very afraid of the use of steganography, have censored many communications, up to the demands of broadcasting of records on the radio. For its part, Radio-London has made great use of personal messages, like the famous verses Trenet, very close to those of Verlaine, "Rock my heart / A languor / Monotonous", which announce the landing in Normandy.

C) Modern steganography

With the advent of computers and the development of electronic exchanges, the possibilities of hiding a message have multiplied: we can hide a message in image, a website, a program, music. Steganography has also found commercial applications, with digital watermarking. We hide a message in an image or music, to identify its origin, and also to prevent it from being duplicated without the knowledge of its owner. Some have argued that steganography played a role in the preparations for the attacks of 11 September 2001 in the United States [13]. The terrorists would have exchanged various messages and plans hidden in pornographic photos. We do not know if this is true, or if it is about rumors propagated by people wishing to see passing a law limiting the use of steganography.

D) Types of cover medium

Almost all digital file formats can be used for steganography, but the image and audio files are more suitable because of their high degree of redundancy [14].

☞ *Hiding in Audio Files*

The techniques that are used to hide information inside Audio files may be listed as follows [15]:

- ✓ *Low bit encoding*, which is somewhat similar to LSB that is generally used in images. The problem with low bit encoding is that it is usually noticeable to the human ear, so it is a rather risky method for someone to use if they are trying to mask information inside of an audio file.
- ✓ *Spread Spectrum* is another method which adds random noises to the signal the information and spreads across the frequency spectrum.
- ✓ *Echo data hiding* which uses the echoes in audio files and. adds extra sound to an echo.
- ✓ *Differential phase variation* in which the file is divided into blocks and using the embedded message, block's initial phase is transformed.

☞ ***Hiding in Image Files***

Image steganography techniques can be divided into two groups: those in the Image (Spatial) Domain and those in the Transform (Frequency) Domain.spatial domain techniques embed messages in the intensity of the pixels directly. Frequency domain techniques first transform the image and then embed the message in more significant areas of cover image. Most suitable image types are uncompressed and lossless compressed images for spatial domain steganography methods [16].

☞ ***Hiding in Video Files***

Hiding a message in video files such as .avi and .mpeg is similar to hiding in images. Mostly of steganography techniques use Discrete Cosine Transform (DCT) to hide message rounding a value in a part of frame [17].

1.2.3.2. Digital Watermarking

It seems that digital watermarking is a good way to protect intellectual property from illegal copying. It provides a means of embedding a message in a piece of digital data without destroying its value. Digital watermarking embeds a known message in a piece of digital data as a means of identifying the rightful owner of the data. These techniques can be used on many types of digital data including still imagery, movies, and music [18].

☞ ***Digital watermarking application***

Watermarking has been proposed in the literature as a means for different applications. The four main digital watermarking applications are:

1. Copyright protection
2. Image authentication
3. Data hiding
4. Covert communication

1.2.3.3. Fingerprinting

Data hiding is proposed or tracing images in the event of their illicit redistribution. The need for this has arisen because modern digital networks make large-scale dissemination simple and inexpensive. In the past, infringement of copyrighted documents was often limited by the unfeasibility of large-scale photocopying and distribution.

1.2.4. Comparison between data hiding techniques

Despite the distinct objectives of data hiding techniques, it is easy to notice, that these three approaches require common parameters :

- ☞ Each approach requires information which can be a secret message, a watermark or a fingerprint.
- ☞ A medium to hide this information, its importance depends on the application, none for steganography, capital for watermarking and fingerprinting.
- ☞ Using a secret key to insert or extract / detect information, the extraction / detection function depends on the application, detection in steganography and extraction for watermarking and fingerprinting.

1.2.5. Data hiding systems

Generally, data hiding systems for digital media involve two distinct stages: data embedding and data detection/extraction to identify the owner or to extract the hidden message. Embedding a data requires three functional components: a cover medium, a secret message and an embedding algorithm. A cover medium is a list of data elements, selected from the cover medium, which are modified during the encoding of a sequence of secret message. The embedding algorithm adds the secret message to the selected carrier.

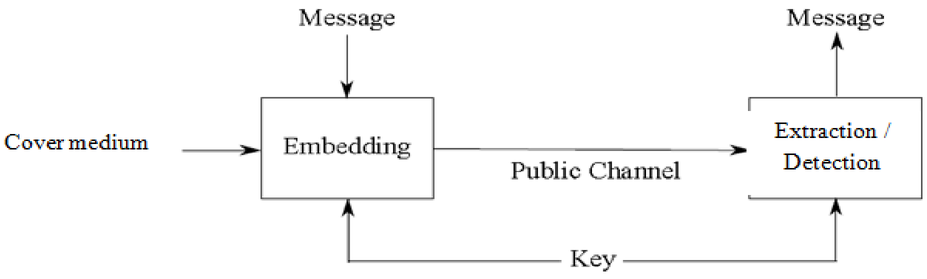


Figure1. 4: General data hiding systems.

1.2.6. Data hiding properties

Each data hiding technique must have certain properties that are dictated by the intended application. The most important properties of data hiding schemes are robustness, undetectability, invisibility, security, complexity, and capacity. We present definitions of those concepts below [19].

☞ ***Robustness***

Robustness determines the algorithm behavior towards data distortions introduced through standard and malicious data processing. 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 of modification are linear and nonlinear filters (blurring, sharpening, median filtering), lossy compression, contrast adjustment, gamma correction, recoloring, resampling, scaling, rotation, small nonlinear deformations, noise adding, cropping, printing / copying / scanning, D/A and A/D conversion, pixel permutation in small neighborhood, color quantization (as in palette images), skipping rows / columns, adding rows / columns, frame swapping, frame averaging (temporal averaging), etc. 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.

☞ ***Undetectability***

Undetectability is typically required for secure covert communication. The embedded information is undetectable if the image with embedded data is consistent with a model of 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 cover-object source. If an attacker has a more detailed model of the source, he may be able to detect presence of a hidden message. This means that the attacker is not automatically able to read hidden message. The concept of undetectability is different from that one of invisibility [20].

☞ ***Invisibility***

Invisibility is based on properties of human visual system or human hearing system. The embedding information should not introduce any perceptible artifacts, that is, if an average human subject is unable to distinguish between carriers that contain hidden information and those that do not. This problem can be solved by applying human perceptual modeling in embedding process. A commonly accepted experimental arrangement, the blind test, frequently used in psycho-visual experiments is based on randomly presenting a large number of carriers with and without hidden information and asking subjects to identify which cover-objects contain hidden information . Success ratio close to 50%, demonstrates that subjects cannot distinguish carriers with hidden information. The blind test is a test for visibility of artifacts caused by data embedding schemes. If the visibility of artifacts was tested by presenting both covers with or without embedding information, a concept of invisibility would result [21].

☞ ***Conflicting Requirements***

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, it is not possible, at the same time, to reach absolute undetectability and large robustness. Thus, there must be a trade-off between undetectability and robustness. On the other hand, if robustness to large distortion is an issue, the message that can be reliably hidden cannot be too long. This observation is schematically depicted in the figure below.

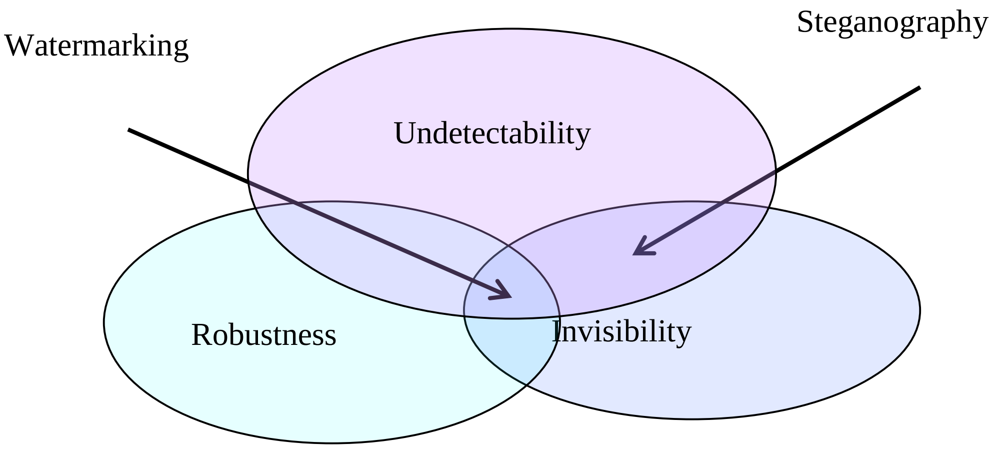


Figure 1.5: Trade-off among undetectability, capacity and robustness

1.3.Cryptography

Cryptography is a method of protecting information and communications through the use of codes so that only those for whom the information is intended can read and process it. The pre-fix "crypt" means "secret" and the suffix "graphy" stands for "writing."

In computer science, cryptography refers to secure information and communication techniques derived from mathematical concepts and a set of rule-based calculations called algorithms to transform messages in ways that are hard to decipher. These deterministic algorithms are used for cryptographic key generation and digital signing and verification to protect data privacy, web browsing on the internet and confidential communications such as credit card transactions and emails [22].

Cryptographic algorithms can be classified by the type of key used and also by their application and their uses , The three types of algorithms are :

1. Secret key Cryptography: uses a single key for both encryption and decryption,
2. Public Key Cryptography: uses one key for encryption and another for decryption,
3. Hash Functions: uses a mathematical transformation to irreversibly "encrypt" information.

1.4.Differences Between Data Hiding And Cryptography

Data hiding and Cryptography are two popular ways of sending vital information in a secret way. Data hiding is the art and science of communicating in a way which hides the existence of the communication while cryptography scrambles a message so it cannot be understood.

The main differences between data hiding and cryptography are:

1. Data hiding means cover writing. Cryptography means Secret writing.
2. Data hiding hides a secret message within a cover such as image, video, or audio file. In cryptography, encrypted message is scrambles and cannot be understood.
3. In data hiding, structure of data cannot be altered while in cryptography; structure of data can be altered.
4. In cryptography The degree of security is measured by the key length, Conversely there is no such thing in steganography

1.5.Conclusion

We have presented in this chapter the basic concepts of data hiding and theirs techniques which used to secure the communication transfer, verify the integrity and trace the illegal copies of digital media.

As the main objective of our work is images steganography, the following chapter describes the basic concepts of images and the steganography technique

Chapter II
Images steganography

Images steganography

2.1. *Introduction*

Steganography is one of the most data hiding techniques that used to protect the confidentiality of information transfer. This technique can be used in several digital media including image, video, sound, text, network protocol and executable file. The digital media used in steganography must support various modifications made in the embedding process. In other words, the stego medium remains authentic to the cover medium, has a height capacity and the most important that resist to the various manipulations. The image is one of the most digital media used by steganography techniques with over 836 image steganography tools [23].

2.2. *General Concepts*

An image is a collection of numbers that constitute different light intensities in different areas of the image [24]. The smallest component of a digital image is called as pixel. Each pixel has own coordinates. Pixels are displayed horizontally row by row. Number of row and columns gives the dimension of an image. The number of the bits per pixel (bpp) represents the color of a pixel, which describes the color depth or bit depth of an image. If each pixel represented by 1-bpp, called as monochrome. There are 2 colors for 1-bpp to represent pixels. 8-bpp generally uses for grayscale images to display 256 different shades of gray, or uses for color images. 16-bpp color depth images are called as “High color” images, 5 bits represents red color channel, 5 bits for blue color channel, and 6 bits for green color channels. 24-bpp is called as “True color”. These images can show almost 16.8 million different colors. Each primary color (red, green, and blue) is represented by 8-bits [25].

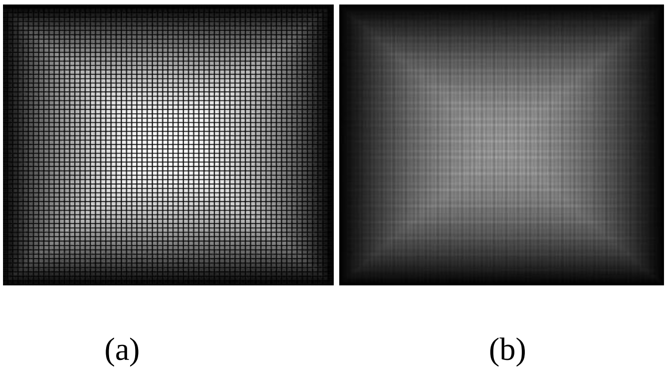
Digital images can be stored using different techniques. Some of them compresses image to reduce data size but it defects the quality of an image, called as lossy compression. Some of these techniques reduce data size, but not as much as lossy compression methods, by not changing pixel values, called as lossless compression.

2.2.1. *Image Types*

2.2.1.1. *Grayscale Images*

Grayscale images carry on a series of shades from white to black at each pixel. Generally, each pixel stores 8-bit integer, giving 256 different grayscale intensities.

For medical imaging use, more details are needed. So, some image formats as JPEG2000, GIF, and PNG support 16-bpp (65,536 tones) grayscale images. Binary representation of color black is 0 for different pixel depths and white is the maximum value. White is 255 for 8-bit pixel depth and 65,535 for 16-bit pixel depth. Figure 2.1 shows 8 and 16-bit shades of gray [26].



(a) (b)

Figure 2.1: (a) 8-bit Shades of Gray (b) 16-bit Shades of Gray [27]

To convert any color to grayscale representation, firstly the color is converted to RGB format if it is not. Then, typically adding %30 of the red value, %59 of the green value, and %11 of the blue value give the grayscale tone of the color [28].

2.2.1.2. *RGB Color Space*

The RGB color model is a mixture of different tones of red, green, and blue colors, and light spectra to produce tones of other colors. Zero intensity gives the black color, and full intensity of each color spaces gives the white color [29]. If the tones of color channels are close to each other, mixture of them gives the shade of gray depending on the intensity. If a color channel has the strongest value and there is a big difference between other color channels, the color is close to this primary color. If two color channels have the strongest value, the color is close to mixture of these two primary colors (cyan: green and blue, magenta: red and blue, yellow: red and green). Figure 2.2 shows the RGB color space.

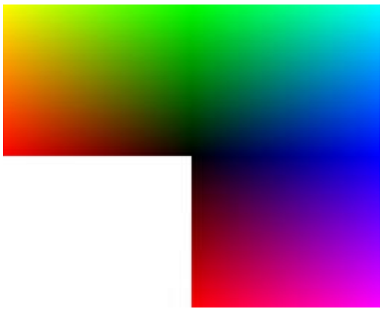


Figure 2.2. Color Space

2.2.1.3. ***Images Palette***

These images are coded using one number to represent a pixel color. Each image file contains its own palette. This palette is the list of used colors in image. For example, if a color image dimensions are 10x10, an uncompressed image carries 24 bit per pixel and totally 2400 bits (300 byte). If the palette image represents each pixel by 8 bits, this file contains 800 bits (100 byte) for pixels and 768 bits (256x3) for palette. These 768 bits (96 byte) define the RGB values of used 256 colors. While this uncompressed image needs 300 bytes, palette image needs 196 bytes. Limited number of distinct colors is the disadvantage of palette images[30]. But it can be useful for images or drawings which do not need more color than the number of colors supported by palettes as shown in figure 2.3.

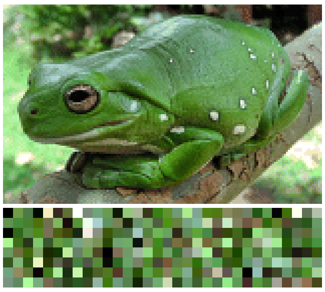


Figure 2.3 : Sample Image Palette

2.2.2. ***Image file formats***

Choosing the right file format is important, and can be critical depending on the level of quality, and also the level of post-processing in steganography.There are many different types of file formats, which can be retrieved and edited using a photo editing software. The most commonly used ones are shown in figure 2.4.

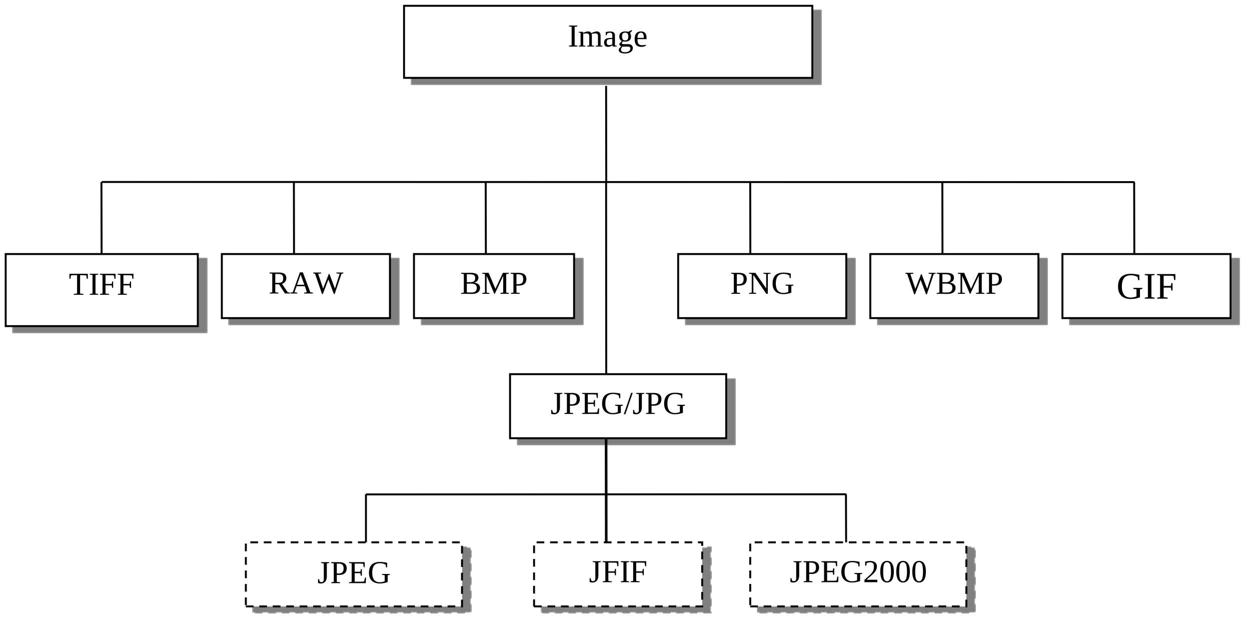


Figure 2.4 Image file format

2.3.*Components Of Image Steganography*

The easiest way of describing the components of image steganography is to consider the first invisible communication model of the prisoners problem proposed In this model, Alice and Bob are two criminals confined in two separate jail cells who want to develop a runaway plan. The warden, called Wendy, will let Alice and Bob communicate, but she monitors all their communications. Thus Alice and Bob will not be able to use encryption methods, as Wendy will stop their message exchange if she notices any suspicious communication.

Thus, they need to use a covert communication method like steganography. Hence, Alice tries to exchange a secret message with Bob by embedding it into a cover image. A secret key could be used by the embedding process. Alice then sends the stego image over an insecure channel to Bob, hoping that Wendy will not notice the embedded message. Then, Bob can extract the secret message from the stego image, since he knows the embedding method used by Alice and has access to the key used in embedding process [31]. The extraction process should be possible without referring to the cover image. This is illustrated in Figure 2.5.

2.3.1. *Embedding Process*

The embedding process usually has three inputs; cover object, secret data, and an optional stego key. It uses a particular method, for example LSB replacement, to embed the secret data into the cover object and create the stego object as an output.

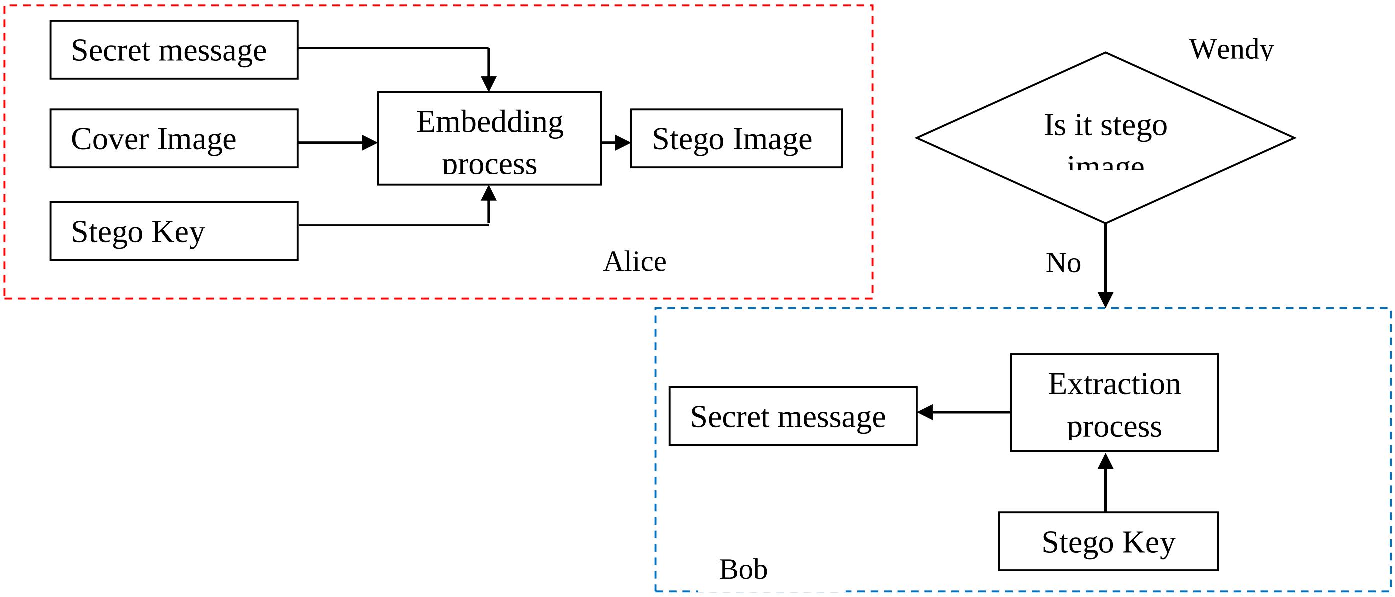


Figure 2.5: Schematic description of Image Steganography

2.3.2. *Stego Key*

The stego key is a secret key used in the embedding process to make the secret data computationally infeasible to extract by the extraction process without having access to that secret key. It can be a number generated via a pseudo-random number generator, or just a password for decoding the embedding location. The secret data may also be encrypted before embedding; in this case the recipient needs two keys to get the secret data, one for extracting and the other for decrypting the secret data [32].

2.3.3. *Extraction Process*

This is an opposite function of the embedding process; it takes the stego object and an optional stego key as an input and extracts the secret message as an output. This process could be achieved without referring to the original cover. However, it is possible to extract the hidden message by comparing both stego and cover object.

2.4. *Image Steganography Techniques*

The steganographic algorithms proposed in literature can broadly be classified into two categories: Spatial Domain Techniques and Transform Domain Techniques.

2.4.1. *Spatial domain techniques*

The spatial domain steganography technique refers to the methods in which the data hiding is performed directly on the pixel values of the cover image in such a way that the effect of the message is not visible (at least for the human vision perception) on the cover image. To perform such an embedding many techniques are used but common amongst all is they all utilize the direct pixel embedding although the pixel selection criterion varies. The common methods used in this domain are:

1. Least Significant Bit (LSB)
2. Pixel value differencing (PVD)
3. Edges based data embedding method (EBE)
4. Random pixel embedding method (RPE)
5. Mapping pixel to hidden data method (PMM)
6. Texture based method
7. Histogram based methods
8. Spread Spectrum based methods
9. Color Palette based methods.

2.4.2. *Transform Domain*

The transform based techniques utilizes the domain specific characteristics of image to embed data on it and for performing it the image firstly transformed to that domain like frequency domain (DCT, DFT), wavelet domain (DWT), Curvelet domain etc. in these techniques the data is embedded on the transformed image instead of direct pixels (as in spatial domain) and then the image is retransformed to spatial domain the advantage of the algorithm is that the information can be embedded in areas of the image that are less exposed to compression, cropping, and image processing also the information in one component of transformed domain spreads over larger number of pixels or even in whole image. This reduces the possibility of removal of information by any attack or operation. Although this is a more complex way of hiding information in an image. Transform domain techniques are broadly classified into:

- Discrete Cosine transform (DCT) based technique
- Discrete Fourier transform (DFT) based technique.
- Discrete Wavelet transform (DWT) based technique.
- Discrete Curvelet Transform (DCVT) Based techniques

In the literature, various steganographic techniques have been proposed [33]. The most frequently used and simplest that works in the spatial domain is Least Significant Bit (LSB) embedding, approaches of which can be classified into two categories: LSB replacement and LSB matching. The former; embeds data in a cover image by replacing the least significant bits of the cover image with secret message bits [34]. LSB matching, however, does not simply replace the LSBs of the cover image as LSB replacement does. If the message bit does not match the LSB of the cover image, then one is randomly either added or subtracted from the value of the cover pixel. To attain higher security data hiding and higher capacity, many successful LSB steganography methods have been proposed [35] for the case of $M \geq 2$ (M is the number of Least Significant Bits the secret message is embedded in). In these methods, it is shown that the LSB planes could be used to accommodate additional secret data by selecting suitable operations of addition/subtraction.

2.5. *Least Significant Bit Description*

Least Significant Bit (LSB) is a simple strategy for implementing steganography. Such as all steganographic methods, it embeds the data into the cover, so that it cannot be detected by a casual observer. The technique works by replacing some of the information in a given pixel with information from the data in the image. Normally, An LSB algorithm replaces the most-right bits of a cover files bytes. In case a bit of the cover image C(i,j) is equal to the bit of a secret massage (SM) that to be embedded, C(i,j) stay untouched, otherwise C(i, j) is set to bit of a secret massage.

2.5.1. *One least significant bits steganography algorithm*

One LSB algorithm consists of following steps:

Step 1 : convert the cover image and data to binary

Step 2 : substitute the Least Significant Bit of the image with the bit of the data

Step 3 : convert the stego image from binary to their pixel format

Step 4 : compress the stego image with using lossless method

Exemple : embedded the letter B'=01000010' in the following pixels :

117	211	50	01110101	11010011	00110010
25	140	7	00011001	10001100	00000111
30	12	18	000011110	00001100	10110100

01110100	11010011	00110010	116	211	50
00011000	10001100	00000110	24	140	6
00011110	00001101	10110100	30	13	180

2.5.2. *Two Least Significant Bits Steganography*

Embedding in 2LSB has been divided into two main categories, excluding the random selection of bit positions that could be applied in both cases. The 2LSB replacement, directly replaces the 2LSB of the cover image's pixel value with 2-bits of the secret message. And Independent 2LSB, known as I2LSB, which independently replaces the 2LSB of the cover pixel values; for instance, it starts with replacing the second-LSB of the pixel values with the secret message, then replaces the first-LSB of pixel values or vice versa.

2.5.2.1. *Independent two least significant bits steganography*

As an alternative scheme in the two LSBs, bits can be embedded in the cover image by selecting pixels and replacing only the second LSB of each pixel then repeating with a new selection of pixels of which only the LSB is used. Therefore, changes occur in the first and second LSB planes independently. We will abbreviate this as I2LSB embedding (letter "I" signifies the independence of the effects on the two lowest bit planes).

2.5.2.2. *Single mach two least significant bits steganography*

SM2LSB (Single Mach Two Least Significant Bits) is another alternative of 2LSB which employs a minor modification to 2LSB replacement. It considers the Match and Mismatch between 2LSB of the cover image and 2-bits of the secret message for embedding. It always assumes a single mismatch (SM) in embedding and changes the third-LSB of the cover image's pixel value in certain cases to point to the index of the mismatch. In the case of Match-Match and Mismatch-Mismatch, the embedding process changes one of the 2LSB of the selected pixel value to get Match-Mismatch or Mismatch-Match according to the binary value of the third least significant bit. If the third LSB of the selected pixel value was 0, then the mismatch would be in the first-LSB and the result after embedding would be (Match-Mismatch). If it was 1, the mismatch would be in the second-LSB and the result after embedding would be (Mismatch-Match).

For the other two cases (Match- Mismatch and Mismatch-Match), the embedding method changes the third LSB of the selected pixel value according to the index of the mismatch. It sets the third LSB to 0 for (Match- Mismatch) and sets it to 1 for (Mismatch-Match) cases. However, there is a probability of 50% that the third LSB already have a right index value and therefore no change would be done to the pixel value.

2.5.3. *Three least significant bits steganography*

The obvious advantage of using more LSBs is increased storage space for secret data. Stego three bits is capable of storing up to three times more secret data than stego one bit LSB approach [36]. Unfortunately, the stego image quality suffers more detectable degradation in this approach than stego two bits.

2.5.4. *Four least significant bits steganography*

The stego image quality degrades even more than stego three bits after secret data is embedded, experiencing a disadvantage consistent with the practice of using more LSBs to store secret data.

2.6. Image Analysis

Differences between two images can be calculated using MSE, PSNR, and WPSNR formulas to have an idea if these images are identical or manipulated. Histograms show the frequency distribution on color or grayscale images. Comparing histograms of two same looking images can give an idea if there is any modification on image.

2.6.1. *Mean Squared Error (Mse)*

MSE is the ratio of sum of the square of the differences in the pixel values between the corresponding pixels of the two images over total pixel number. MSE can be calculated if two images‟ dimensions are equal. If two images are identical MSE value is 0. Formula (1) shows how to calculate MSE value. I1 and I2 are images with same dimensions. M and N are the dimensions of images.

$$MSE = \frac{1}{MN}\sum_I \sum_J (I(i,j) - I_w(i,j))^2 \qquad (1)$$

2.6.2. *Peak Signal to Noise Ratio (PSNR)*

The peak signal-to-noise ratio (PSNR) is the ratio between maximum power of a signal and the power of the signal's noise. After lossy compressing an image to reduce data size or changing quality of image, pixel values changes. Calculating PSNR value defines the changes on image. PSNR is usually expressed in decibels. MSE and PSNR values can be calculated separately for each color channel. If two images are identical the PSNR value is infinite.

$$PSNR = 10.\,log_{10}(\frac{d^2}{EQM}) \qquad (2)$$

d is the maximum pixel value for the image. 2^n-1 gives the maximum pixel value for an image. d value is 2^8-1=255 if pixels are represented by 8-bits for image.

2.6.3. *Weighted Peak Signal to Noise Ratio (WPSNR)*

Quality measurement function Weighted Peak Signal to Noise Ratio uses different approach than PSNR. WPSNR calculates different weights for different blocks of image while PSNR uses same weight for all images. Using different weights gives better results about changes in the perceptual quality more accurately than PSNR. HVS is less sensitive for to changes in highly textured areas. So, WPSNR uses Noise Visibility Function (NVF) , which uses a Gaussian model to estimate how much texture exists at different blocks of the image. NORM is a normalization function and δ is the luminance variance of block at formula (3) and Formula (4) shows how to calculate WPSNR

$$NVF(i,j) = \frac{1}{1+\theta\delta_x^2\,(i,j)} \qquad (3)$$

$$WPSNR = 10\log(\frac{L_{max}^2}{MSE^*\,NVF^2}) \qquad (4)$$

2.7.*Conclusion*

The key concerns and considerations of steganographers have been explained in this chapter. Any steganographic scheme is considered broken when the existence of the hidden message is detected, thus the statistical undetectability of the embedded data is the most important property for any steganographic system. Regarding the embedding methods, LSB embedding is the most common steganographic method in spatial domain because it has a reasonable capacity, is easy to implement, and visually imperceptible.

Chapter III
Proposed method
and
Experimental results

3.1. Introduction

The least-significant-bit (LSB)-based approach is a popular type of steganographic algorithms in the spatial domain. However, we find that in most existing approaches, the selection of positions for data embedding within a cover image mainly depends on a pseudorandom number generator without considering the relationship between the LSBs of the cover image and the embedded data. In order to minimize visual distortion of the stego image, in this manuscript, we propose a new positions selection approaches of LSBs based steganography based on the primitive roots and Arnold's Cat Map (PR-ACM). The proposed approach is not a steganographic algorithms by them self but rather a universal enhancement to any existing steganographic techniques. Our new works generalize the LSBs based approaches to improve the embedding efficiency, that is to say, select the suitable cover image's pixel value that minimize the expected number of modifications per pixel and the visual distortion.

3.2.Preliminary

The chaos phenomenon is a deterministic and analogously stochastic process appearing in a nonlinear dynamical system [37]. Because of its properties, such as unpredictability, similar randomness, aperiodicity, sensitive dependence on initial conditions and parameters, these properties make chaotic systems become popular in information hiding to increase security [38].Primitive roots and Arnold's cat map are one of the simplest chaotic maps.

*3.2.1. Arnold's Cat Map (AC*M)

Arnold's Cat Map (ACM), usually called cat mapping, proposed by Vladimir Arnold in 1960, is a chaotic map which when applied to a digital image randomizes the original organization of its pixels and the image becomes imperceptible or noisy [39].
It can be mathematically expressed as:

$$\Gamma\begin{bmatrix}x\\y\end{bmatrix}=\begin{bmatrix}1&1\\1&2\end{bmatrix}\begin{bmatrix}x\\y\end{bmatrix} mod\ 1 \qquad (1)$$

Where,$\Gamma\begin{bmatrix}\mathrm{x}\\\mathrm{y}\end{bmatrix}$gives the Cat Map transform over the original pixels *x* and *y*. Generally for an *n*×*n* image,

$$\Gamma\begin{bmatrix}x\\y\end{bmatrix}=\begin{bmatrix}1&a\\b&ab+1\end{bmatrix}\begin{bmatrix}x\\y\end{bmatrix} mod\ N \qquad (2)$$

Where $\mathrm{a},\mathrm{b}\in\mathbb{z}$ and $\mathrm{a},\mathrm{b}\geq 1$.

Thus, it is evident that (1) is a special case of (2) when *a*=*b* =*N*=1.

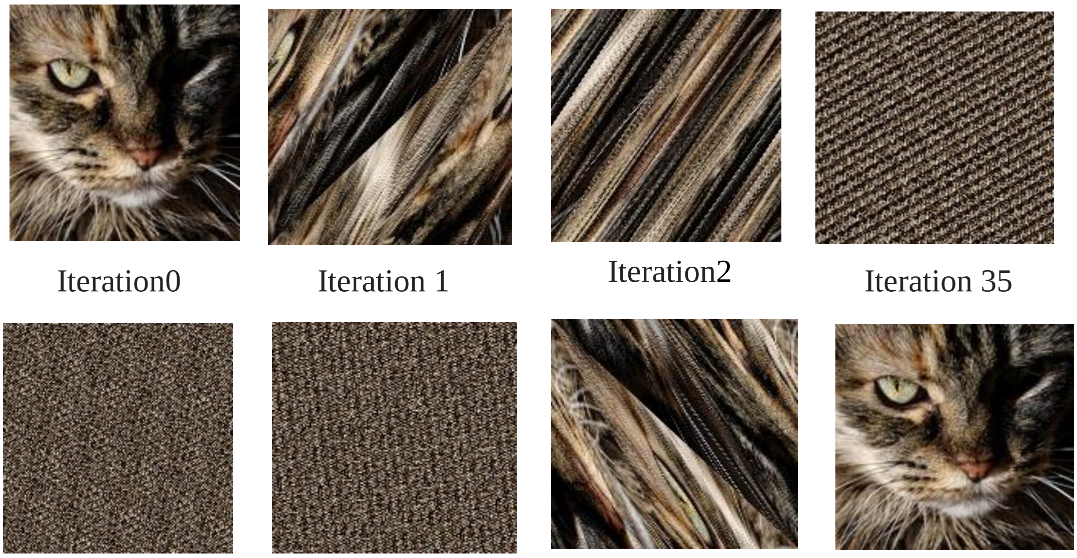
Transformation given by Equation (2) is periodic as abs (det (A)) is 1 in both the cases where, A = [1, a; b, ab+1] is the Arnold transform matrix. It has a period τ and if iterated *t* number of times, the original image reappears.

There are no known formulae to calculate the period of Arnold mapping from the image dimension. However some special case rules for the period τ were found as:

$$\tau = 3n \, if \ and \ only \ if \ n = 2 \times 5^k k = 1,2, \ldots.$$

$$\tau = 2 \, n \, if and \ only \ if \ n = 5^k orn = 6 \times 5^k k = 1,2, \ldots.$$

$$\tau \leq \frac{12n}{7} for \ all \ other \ choice$$



Iteration0 Iteration 1 Iteration2 Iteration 35

Iteration65 Iteration 83 Iteration298 Iteration300

Figure 3.1: Samples from Arnold's cat map application on the image 'Cat'

The image 'Cat' with a size of 150×150 has a period of 300, after 300 times the shuffled image is reduced back to the original image.

3.2.2. Pseudo Number Random Generator

Before introducing the pseudo number random generator used in our proposed steganography method, in this section we present some mathematical concept :

3.2.2.1.Number order

Definition

Let *n* be an integer positive number and let gcd(p,n) = 1 the order of *p* modulo *n* denoted $Ord_n(p)$ is the smallest positive integer m such that $\mathrm{p}^{\mathrm{m}} \equiv 1(\mathrm{mod\ n})$.

For example

$Ord_7(2) = 3$

$2^1 \equiv 2 (mod\ 7)$, $2^2 \equiv 4\ (mod\ 7)$ $2^3 \equiv 8 \equiv 1\ (mod\ 7)$ ⇨ *Ord7*(2) = 3.

3.2.2.2.Euler's phi function

The Euler's phi function is defined as the number of positive integers $\leq n$ that are relatively prime to *n*, where 1 is counted as being relatively prime to all numbers. Since a number less than or equal to and relatively prime to a given number is called a $\varphi\ (n)$ or

$\phi\ (n)$, $\varphi(n)$ can be simply defined as the number of integers k in the range 1 ≤ k ≤ n for which the greatest common divisor gcd(n, k) is equal to 1.

For example φ(24) = 8 numbers (1, 5, 7, 11, 13, 17, 19, and 23). You can verify that gcd(24, 5) = gcd (24, 7)= gcd (24, 11) = gcd(24, 13) =gcd(24, 19) = gcd(24, 23) =1.

Primitive root

Suppose *p* is prime and *n* is an integer such that *p* does not divide *n* we say *n* is primitive root modulo *p* if $ord_p(n) = \varphi(p) = p - 1$

For example $ord_{13}(2) = 12,\ \varphi(13) = 12$

2 is a primitive root modulo 13

Theorem: there are $\varphi\ (\varphi(n))$ primitive roots modulo *n*

For example, how many primitive roots are there modulo 7?

$\varphi(\varphi(7)) = \varphi(6) = \varphi(3 * 2) = \varphi(3) * \varphi(2)$ = (3-1)(2-1)=2*1=2, so there are two primitive roots modulo 7

If *a* is a primitive root of the prime number *p*, then the numbers *a* mod *p*, a^2mod *p*, …, a^{p-1}mod *p* are distinct and consist of the integers from 1 through (*p* – 1) in some permutation. Therefore, if *n* is the primitive root of *p*, then its powers $n, n^2 \ldots n^{p-1}$

are all relatively prime to p with distinct numbers. For any integer y and a primitive root n of prime number p, a unique exponent i is determined so that $Y = n^{i} mod\ p$

3.2.3. Proposed embedding algorithm

In this the proposed method, we have used the primitive root to generate a sequence of positions in the cover image, while the Arnold' cat map it is used to shuffle the cover image pixels to obtain a novel sequence of pixels in the same selected positions that minimize the visual degradation. The process of using primitive root and Arnold's cat map in an embedding procedure is stated as follows.

1) Choose a prime number between message length and image size.
2) Calculate the primitive roots of the prime number and choose one of them.
3) Define map pixels.
4) The secret massage bits are embedded in the obtained positions using the steganographic methods based LSBs.
5) Calculate the PSNR between the cover image and the stego image.
6) Shuffle the cover image pixels according to Equation (1).
7) The secret massage bits are embedded in the obtained positions using a steganographic method based LSBs.
8) Reverse Arnold's transform to compute and compare the new obtained PSNR with previous one and keep the max with its iteration.
9) Steps 6-8 are repeated until the cover image is constructed.
10) Repeat all the previous steps with another position map until we get the higher PSNR.

The prime number, its primitive root and the iteration ***i*** are used as a secret key, as shown in figure 2, which is used in the extraction procedure.

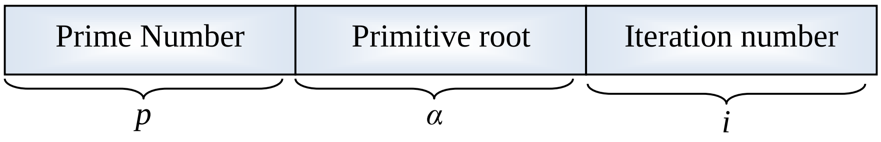


Figure 3.2: Secret key steganography based on the primitive root and ACM

The secret key that we used in the extraction process has the format of {p ,α ,i}, where ***p*** and ***α*** are used for generating the pixels positions and ***i*** is the iteration number of Arnold's cat map that gives the best PSNR.

3.3. Experimental Results

In this section, we demonstrate the performance of our proposed method using the embedding schemes: One LSB, 2-LSBs and 4-LSBs. For stego image evaluation, Peak Signal-to-Noise Ratio (PSNR) is considered and 200 standard gray-level with different sizes are used as cover.

3.3.1. Embedding methods

In the first step of our experiments, stego images are generated with different embedding rates from 10% to 50% with a step of 10% using the following embedding methods: One LSB, 2-LSBs and 4-LSBs.

3.3.2. Embedding distorsion

The PSNR metric is the most common and widely used full reference metrics for stego image evaluation. In particular, PSNR is used in many image processing applications and considered as a reference model to evaluate the efficiency of other objective image quality evaluation methods. PSNR as a metric computes the peak signal-to-noise ratio, in decibels, between two images. It is used in steganography to measure the peak signal-to-noise ratio in the original image and the stego image after embedding the hidden data.

3.3.3. Embedding distorsion analysis

As an example, Figure 3 shows the cover image ‘pepper’ its stego images, figures 3(b)-3(c)- 3(d) using One LSB, 2-LSBs and 4-LSBs techniques. The visual inspection (subjective test) does not find differences between the cover image and the stego images. The images are identical optically with no indication of hidden messages.

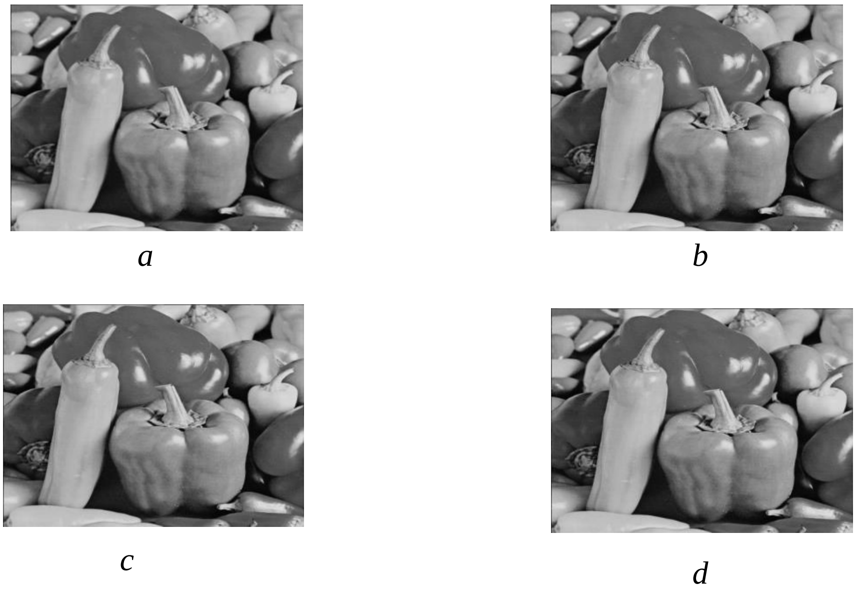


Figure 3. 3: Visual comparison of the cover image pepper(a), and the stego images obtained with One LSB (b), 2-LSBs (c), and 4-LSBs (d)

Figure 4 below shows the comparison of PSNR between the proposed method and the standard steganography methods (One LSB, 2-LSBs and 4-LSBs) at different embedding rates of the image 'pepper' .It is clear from this figure that the PR-ACM scenario provides better results in terms of PSNR regardless of the size of the secret message inserted.

In this case, the stego image distortion (PSNR) can achieve an average improvement of 61.7 db (One LSB), 57.04 db (2-LSBs), and 47.9 db for (4-LSBs).

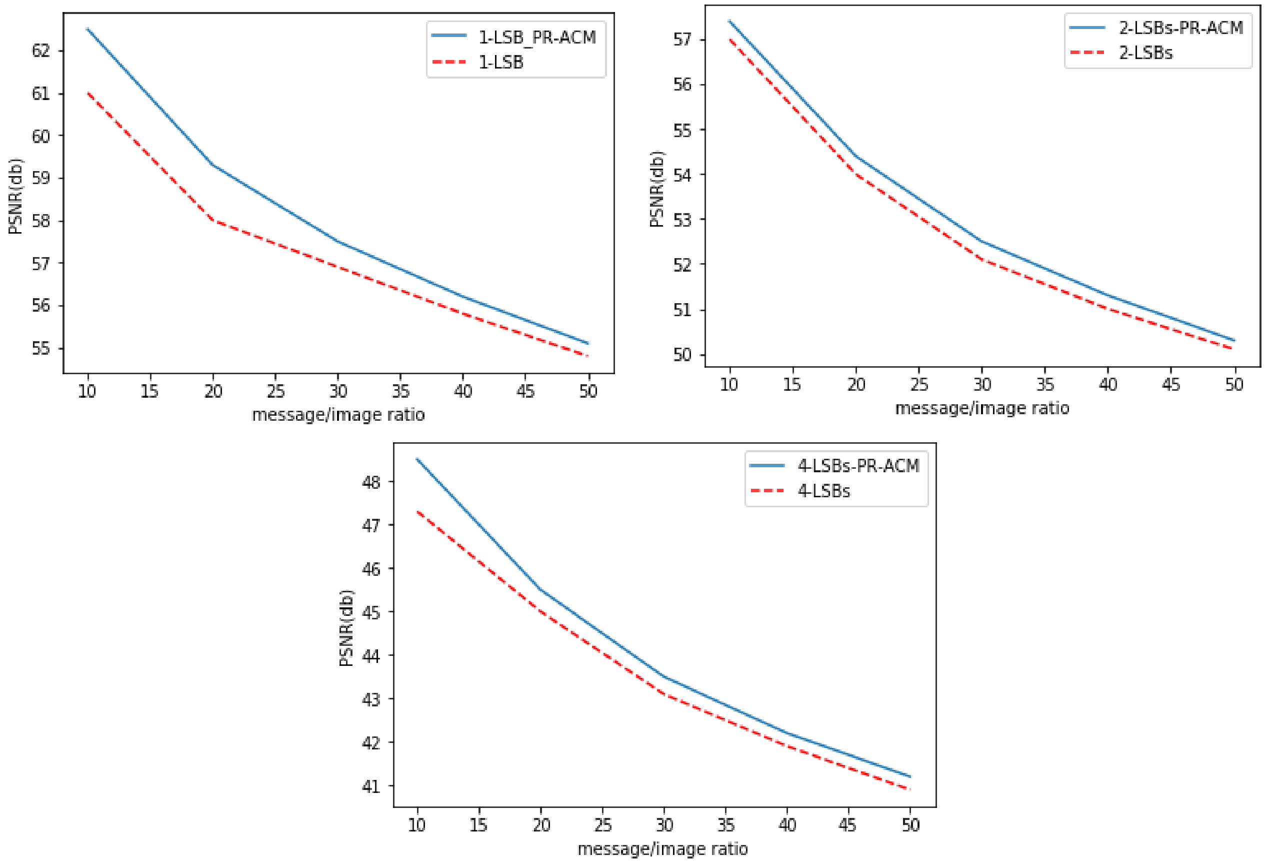


Figure 3. 4: PSNR comparison of our proposed PR-AC Mmethod and LSBs schemes

In Table 1, we provide the computed values for PSNR of the proposed method, One LSB, 2-LSBs, and 4-LSBs. Also, for each embedding rates the secret key and the PSNR are computed. It has been observed, from table 1, that the 2-LSB and 4-LSBs employs additional distortion than One LSB, which makes the value of PSNR in average **57.12%** more than the 2-LSB and 4-LSBs. It has also been observed that the proposed method improve the PSNR in comparison to One LSB, 2-LSBs, and 4-LSBs. It appears that the embedding rate have the better PSNR equal to **58.12%** for One LSB, equal to **53.1%** for 2-LSBs, and equal to **46.18%**for -LSBs, where it has been reduced about **1%, 0.51%, and 0.54%** for the proposed method.

embedding rate	10%	20%	30%	40%	50%
One-LSB	61	58	56.9	55.8	54.8
2-LSBs	57	53.8	52	51	50.1
4-LSBs	47.3	45	43.1	41.9	40.9
One-LSB-PR-CAT	62.5	59.3	57.5	56.2	55.1
2-LSB-PR-CAT	57.4	54.4	52.5	51.3	50.3
4-LSB-PR-CAT	48.5	45.5	43.5	42.2	41.2

Table 3.1 : PSNR values of the proposed method and the LSBs techniques

3.4.Conclusion

In this chapter, a new positions selection technique for image steganography in the spatial LSB domain is proposed. The selection step of positions used for data hiding is mainly determined by a PRNG based on the primitive roots method. To preserve the embedding visual distortions in cover images, we have used the Arnold's Cat Map method to shuffle the image pixels. The experimental results evaluated on 200 natural images using three embedding schemes show that the visual distortion of our stego images are improved significantly compared to One LSB, 2-LSBs, and 4-LSBstechniques.

General conclusion

Conclusion And Perspectives

In this manuscript, a new positions selection technique for image steganography in the spatial LSB domain are proposed. In most proposed steganographic schemes, the selection step of positions used for data hiding is mainly determined by a PRNG without considering the relationship between the characteristics of content regions and the size of the secret message to be embedded, which means that the smooth/flat regions will be contaminated by such a random selection. To preserve the embedding changes and visual distortions in cover images, we have proposed a novel positions selection method for data hiding which can first embed the data into the better regions according to a criteria metric function based on PSNR. The experimental results evaluated on 200 natural images using three embedding schemes show that visual distortion of our stego images are improved significantly compared to One LSB, 2LSBs and 4LSBs replacement. Furthermore, our proposed approaches can be applied to other steganographic methods such as audio/video steganography in the spatial domain.

For further improvement, we project in our future work to use, firstly, other chaotic systems like Tent map, Lorenz attractor and Rossler attractor and the use of optimization techniques like Bat algorithm and Genetic Algorithm.

References

1. P. P. Ray, “Towards an Internet of Things based Architectural Framework for Defence”, In: Proc. IEEE International Conference on Control Instrumentation Communication and Computational Technology, pp. 411-416 (2015).
2. J. Chambers, W. Yan, A. Garhwal et al, “Currency security and forensics: a survey”, In: Multimedia Tools Application, vol. 74, no. 11, pp. 4013-4043 (2015).
3. C.C. Chang, C.Y. Lin, and Y.Z. Wang, “New image steganographic methods using run length approach”, In: Information Sciences, vol. 176, pp. 3393-3408 (2006).
4. X. Zhang and S. Wang, “Vulnerability of pixel-value differencing steganography to histogram analysis and modification for enhanced security,” Pattern Recognition”, In: Signal Processing Letters, vol. 25, pp. 331-339 (2004).
5. http://sk.sagepub.com/reference/the-sage-encyclopedia-of-the-internet-3v/i3146.xml
6. J. Zujovic, T.N. Pappas, D.L. Neuhoff, “Structural texture similarity metrics for image analysis and retrieval”, In: IEEE Trans. Image Processing., vol. 22, no. 7, pp. 2545-2558(2013).
7. D. Lee, K. Plataniotis, “Towards a full-reference quality assessment for color images using directional statistics”, In: IEEE Trans. Image Process., vol. 24, no. 11, pp. 3950-3965 (2015).
8. A.D. Ker, R. Bohme, “Revisiting weighted stego-image steganalysis”, In: Electronic Imaging, Security, Forensics, Steganography, and Watermarking of Multimedia Contents X, San Jose, CA. Proceedings SPIE, January 2731, vol. 6819, pp. 5:1-5:17 (2008)
9. X. Li, B. Yang, D. Cheng, and T. Zeng, “A generalization of LSB matching”, In: Signal Processing Letters, IEEE, vol. 16, pp. 69-72 (2009).
10. C. H. Yang, C. Y. Weng, S. J. Wang, and H. M. Sun, “Adaptive data hiding in edge areas of images with spatial LSB domain systems”, In: IEEE transactions on informations on forensics and security, vol.3, no. 3, pp. 488-497 (2008).
11. W. Luo, F. Huang, and J. Huang, “Edge Adaptive Image Steganography Based on LSB Matching Revisited”, In: IEEE transactions on informations on forensics and security, vol. 5, no. 2 (2010).
12. D. Volkhonskiy, B. Borisenko and B. Evgeny “Generative adversarial networks for image steganography”. In: ICLR 2016, Open Review (2016).
13. H. Shi, J. Dong, W. Wang, Y. Qian, X. X. Zhang, “Secure Steganography Based on Generative Adversarial Networks. In: Advances in Multimedia Information Processing PCM 2017. PCM 2017. Lecture Notes in Computer Science, vol 10735. Springer (2018).
14. S. Baluja, “Hiding Images in Plain Sight: Deep Steganography”,In: Proceedings of Advances in Neural Information Processing Systems 30 (NIPS), pp.2069-2079 (2017).
15. N. Zhang, S. Ding, J. Zhang, Y. Xue“Research on point-wise gated deep networks”, Applied soft Computing, vol. 52, pp.1210-12221.
16. N. Zhang, S. Ding “Unsupervised and semi-supervised extreme learning machinewith wavelet kernel for high dimension data”, Memetic Computing, vol. 9, no. 2, pp. 129-139 (2107).
17. N. Zhang, S. Ding, J. Zhang, Y. Xue “An overview on restricted Boltzmann machines”, Neurocomputing, vol. 275, pp.1186-1199 (2018).
18. R. Bohme, J. Grossklags, “The security cost of cheap user interaction” In: Proceedings of the New Security Paradigms Workshop, ACM, New York, pp. 67-82 (2011).
19. M.K. Hani, M.K, M.N. Marsono, R. Bakhteri, “Biometric encryption based on a fuzzy vault scheme with a fast chaff generation algorithm”, In: Future Generation Computer. System. pp.800-810 (2013).
20. A.K. Verma, C. Patvardhan, C.V. Lakshmi, “Robust adaptive watermarking based on image contents using wavelet technique”, In: Journal Image, Graph Signal Process, vol. 2, pp. 48-55(2015).
21. A. Cheddad, J. Condell, K. Curran, P. McKevitt, “Digital image steganography: Survey and analysis of current methods”, Signal Processing, vol. 90, pp. 727-752 (2010).
22. L. Malina, L. Popelova, P. Dzurenda, J. Hajny, Z. Martinasek, “On Feasibility of Post-Quantum Cryptography on Small Devices”, In: IFAC-Papers On Line, vol.51, no. 6, pp. 462-467 (2018).

23. A. Abdul Manaf, A. Bouroujerdizade, S. Mojtaba, “Collusion-resistant digital video watermarking for copyright protection application”, In: Int. J. Appl. Eng. Res., vol. 11, pp.3484-3495 (2016)
24. A. Pradhan,K.R. Sekhar,G. Swain, “Digital image steganography based on seven way pixel value differencing”, In: Indian J. Sci. Technol., vol. 9, no. 37, pp. 1-11 (2016).
25. Y.P.Lee, J.C Lee, W.K. Chen, K.C. Chang, I.J. Su, C.P. Chang “High-payload image hiding with quality recovery using tri-way pixel-value differencing”, In: Inf. Sci., vol. 191, pp. 214-225 (2012).
26. O.M. Al-Shatanawi, N.N. El-Emam, “A new image steganography algorithm based on MLSB method with random pixels selection”, In: Int. J. Net. Security. Appl., vol. 7, no.2, pp. 37-53 (2015)
27. A.D. Ker, “A general framework for the structural steganalysis of LSB replacement”, In: Lecture Notes in Computer Science: 7th International Workshop on Information Hiding, Barcelona. Edited by: Barni M, Herrera-Joancomart J, Katzenbeisser S, Prez-Gonzlez F., Springer Berlin, pp. 296-311 (2005).
28. A. Westfeld and A. Pfitzmann, “High capacity despite better steganalysis (F5-a steganographic algorithm)”,In: Information Hiding, 4th International Workshop, pp. 289-302(2001).
29. Z. Liu and L. Xi, “Image information hiding encryption using chaotic sequence”, In: Proceedings of the 11th International Conference on Knowledge-Based Intelligent Information and Engineering Systems, pp. 202-208 (2007).
30. Y. Zhang, F. Zuo, Z. Zhai, and C. Xiaobin, “A new image encryption algorithm based on multiple chaos system”, In: Proceedings of the International Symposium on Electronic-Commerce and Security (ISECS ’08), pp. 347-350 (2008).
31. R. Munir, B. Riyanto, S. Sutikno, and W. P. Agung, “Secure spread spectrum watermarking algorithm based on chaotic map for still images”, In: Proceedings of the International Conference on Electrical Engineering and Informatics (2007).
32. Z. Dawei, C. Guanrong, and L. Wenbo, “A chaos-based robust wavelet-domain watermarking algorithm”, Chaos, Solutions and Fractals, vol. 22, no. 1, pp. 47-54 (2004).
33. O. Chergui, H. Bendjenna, A. Meraoumia, S. Patnaik, “Can a chaos system provide secure communication over insecure networks? Online automatic teller machine services as a case study”, In: J. Electron. Imaging 27(3), 033045 (2018),
34. G. Ye, K.W. Wong, “An efficient chaotic image encryption algorithm based on a generalized Arnold map”, in Nonlinear Dynamics vol. 69, no. 4, pp. 2079-2087(2012).
35. G. Komarasamy and A. Wahi, “An Optimized K-Means Clustering Technique using Bat Algorithm”, In: European Journal of Scientific Research, vol. 84, no. 2, pp.263-273 (2012).
36. X. S. Yang, “A New Metaheuristic Bat-Inspired Algorithm”, in Nature Inspired cooperative Strategies for Optimization (NISCO 2010), J. R. Gonzalez et al., Eds., Springer Press, vol. 284, pp. 65-74 (2010).
37. J. H. Holland, “Adaptation in Natural and Artificial Systems”, In: MIT Press, Cambridge, Mass, USA, (1992).
38. Y.-T. Wu and F. Y. Shih, “Genetic algorithm based methodology for breaking the steganalytic systems”, In: IEEE Transactions on Systems, Man, and Cybernetics B, vol. 36,no. 1, pp. 24-31 (2006).
39. L. Shao-Hui, C. Tian-Hang, Y. Hong-Xun, and G. Wen, “A variable depth LSB data hiding technique in images”, In: Proceedings of 2004 International Conference on Machine Learning and Cybernetics, vol.7, pp. 3990-3994 (2004).