**A SECRET IMAGE DATA HIDING SCHEME FOR COPYRIGHT PROTECTION**

Abstract:

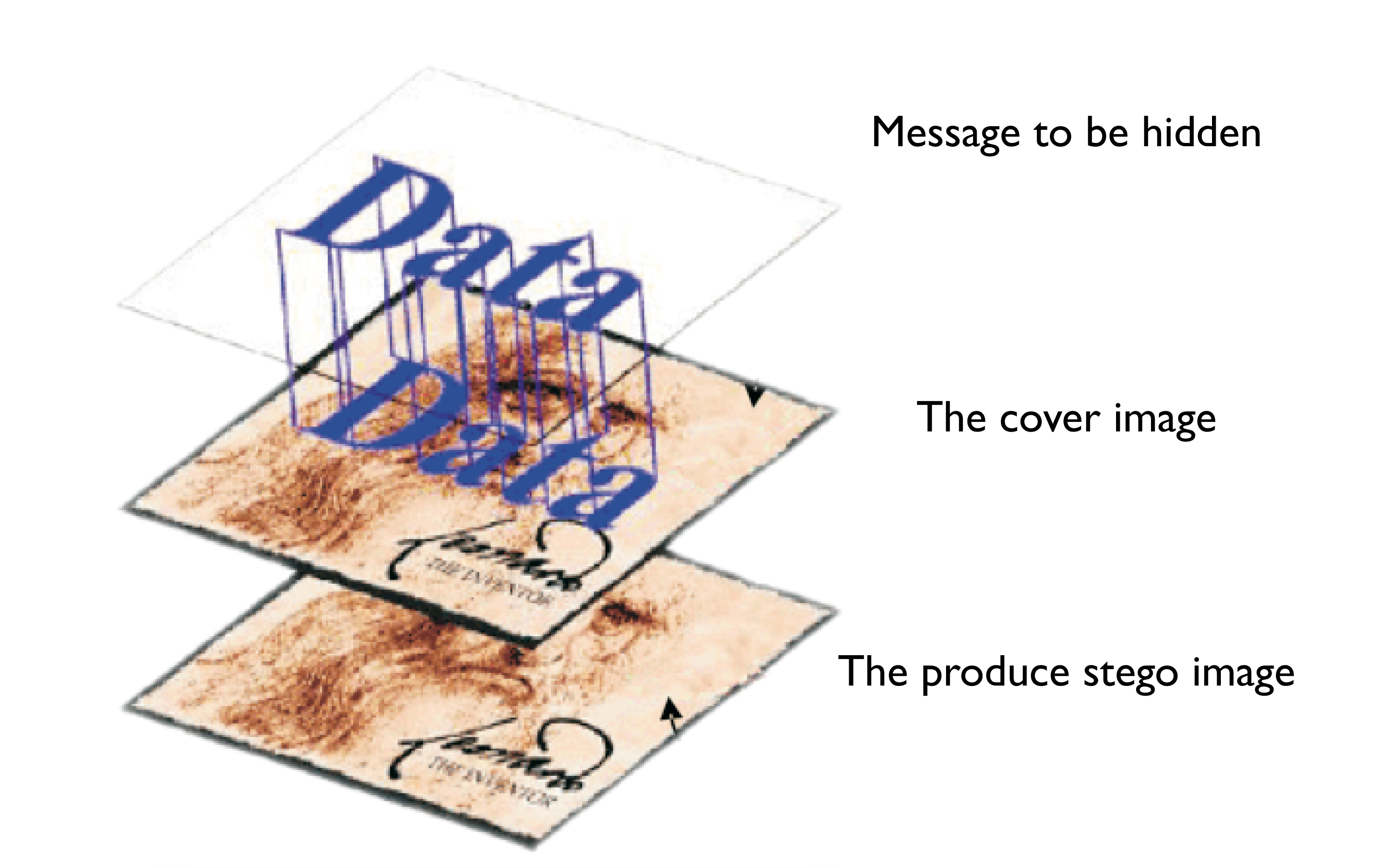
The contemporary digital culture have made available various new prospects for the rapid and economical dissemination of digital contents. Exchanging contents or communicating in a secret way is, in general tantamount to express in code the circulation of the message. For instance, if someone wants tocommunicate a secret to the partner, it is healthier hiding the message in aninoffensive object such as an mp3, mpeg and a jpg. Quite a lot of techniques to hide information arepresented, terminology and possible related attacks, with specific attentionon Steganographic and copyright schemes. The protection of the hidden data from an enemy is the most significant objective of steganography and therefore it is evident that the security of a steganography system will increase if the payload remains obscured, hard to decipher to an enemy even if the enemy holds some knowledge about the embedding method. Data hiding is the process of encoding additional information in an image by making small modifications to its pixels. Steganography has a number of useful applications. Nevertheless, comparable to any other science it can be used for ill intentions. It has been driven to the forefront of contemporary security techniques by the significant growth in computational power, the intensification in security consciousness by, for instance, individuals, groups, agencies, government and through intellectual pursuit. Steganography's definitive objectives, which are undetectability, robustness (that is resistance to various image processing methods and compression) and capacity of the hidden data, are the main factors that separate it from other related techniques such as watermarking and cryptography. To be practical, the hidden data must be perceptually undetectable yet robust to common signal processing operations. In this research work we will discuss how secret image data can be used as a carrier to hide messages. This research work presents anoverview of information hiding in general, steganography and copyrightprotection in particular. Determinations have been given to certify that the proposed mechanism toe the line to high imperceptibility and fidelity which are the critical quality requirements for any image steganography system.

***Keywords:*** Steganography, robustness, undetectability, copyright protection, information hiding, secret data, LSB Matching, C# Coding.

Chapter 1

Introduction

Information hiding or steganography is early from the Greek word “steganos” and means concealed; “graphy” which also means “writings”. It is the secured communication over public network. The central resolution of steganography is to hide data in a cover media so that others will not be able to be aware of it, figure 1 illustrate the processes of how this works. While cryptography is about protecting the content of the messages, steganography is about concealing their very existence [1]. The solicitations of information hiding systems largely displays over a broad area from military, intelligence agencies, online elections, internet banking, medical-imaging and so on. These variability of solicitations make steganography a hot topic for study. The cover medium is usually chosen, keeping in mind the type and the size of the secret message and many different carrier file formats can be used. In the current situation digital images are the most popular carrier or cover files that can be used to transmit secret information.



**Secret Data**

Figure1. Data Hiding Scheme

Steganography equation is given as [Stego-medium = Cover medium + Secret message + Stego key]. The over-all model of data hiding can be described as follows. The embedded data is the message that one wishes to send secretly. It is usually hidden in an inoffensive message referred to as a cover text or cover-image or cover-audio as applicable, producing the stego-text or other stego-object. A stego-key is used to control the hiding process so as to confine recognition and or recovery of the embedded data to parties who know it [2].

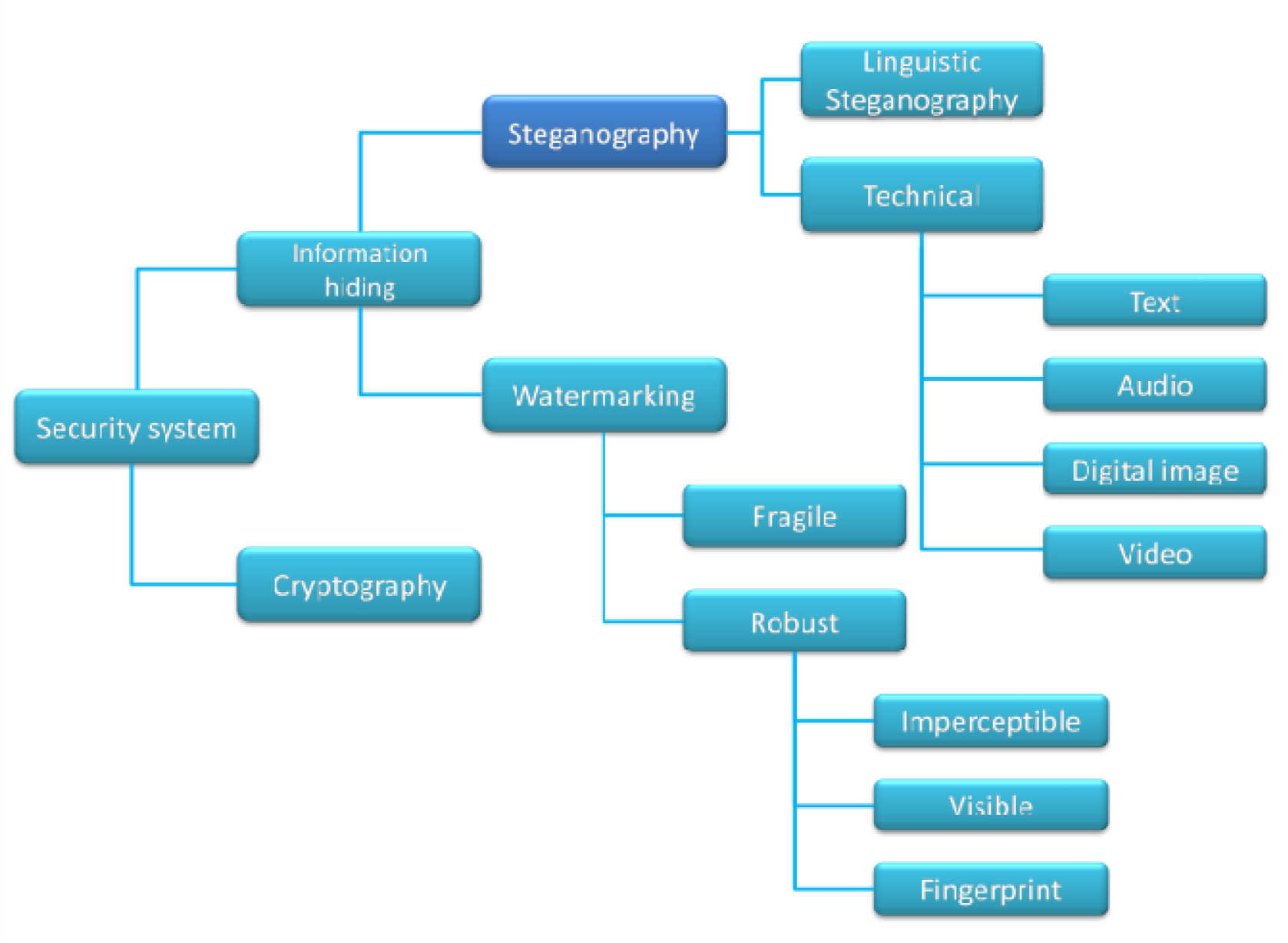


Figure 2: Steganography in security domain

(Source: www.ijarcsse.comVol. 1, issue. 1 Dec 2011)

Image steganography is the science of obscuring information and messages contained by an image using some embedding algorithm. Figure 3 illustrate Information Hiding hierarchy.

**Information Hiding**

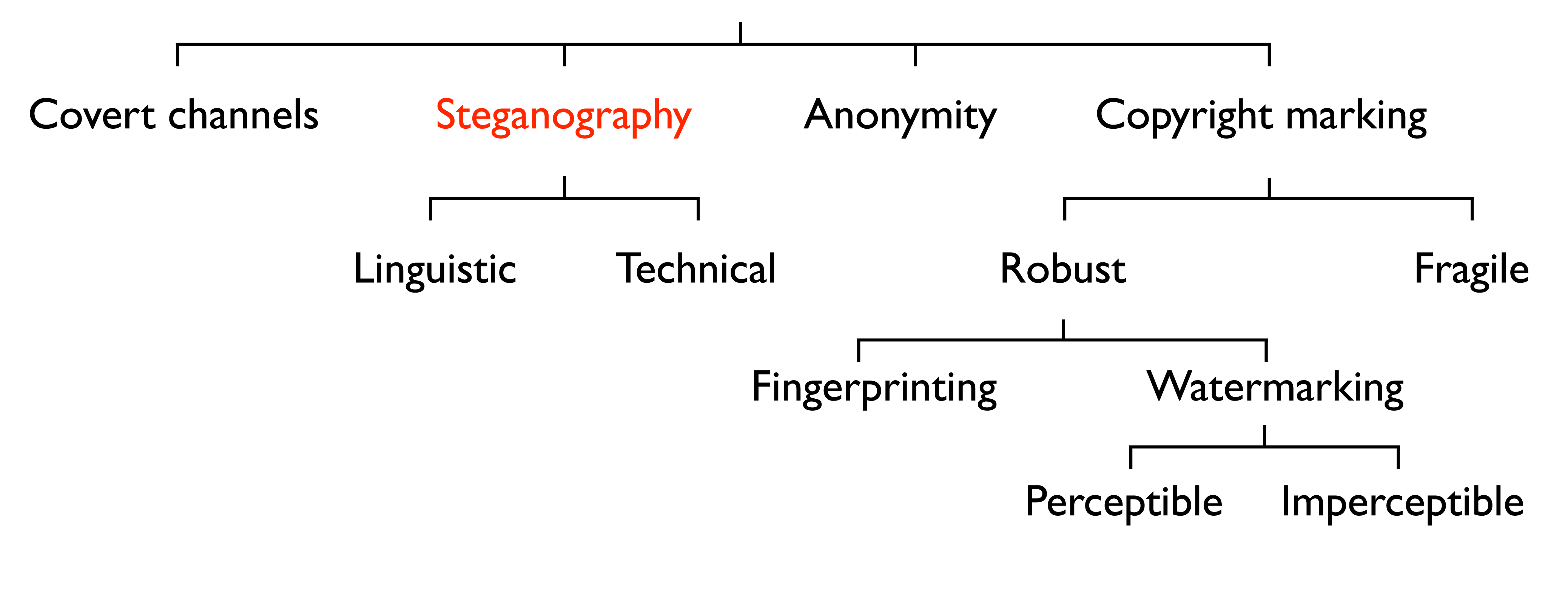


Figure 3: Information Hiding Hierarchy

(Source: http://ic.unicamp.br/~rocha/wvu/talks/infoHidingTypesAndApplications-White.pdf)

In our contemporary times communication security is the essential requirement even though achievement of comprehensive security is an excellent state of affairs. The concept of “What You See Is What You Get (WYSIWYG)” related with printing proficiencies of a printing machine for an image, is now a fallacy [3]. A conventional image is no longer a regular image. It could be a concealment over a secret message. In image Steganography, the concealment used to hide any message is a color or grayscale image. Images can be more than what we see with our Human Visual System (HVS); therefore they can express more than merely 1000 words. For decades now people endeavored to fashion methods for secret communication. Although Steganography is described elsewhere in detail, we make available here a brief history. The word Steganography is initially a Greek word which means “Covered Writing”. It has been used in various forms for thousands of years. In the 5th century BC Histaiacus shaved a slave’s head, tattooed a message on his skull and was send off with the message after his hair grew back [4].

With the enhancement of computer power, the internet and with the development of Digital Signal Processing (DSP), Information Theory and Coding Theory, Steganography went “Digital”. In the realm of this digital world Steganography has created an atmosphere of community awareness that has produced various interesting applications of such science. The contemporary information hiding is due to [5] for his article titled “***The prisoners’ Problem and the Subliminal Channel***”.

The remainder of this section highlights some historical facts and attacks on methods (Steg-analysis). Steganography is define as the art and science of “invisible" communication. Steganography word is classified into two parts: Steganos which means “secret or covered” (where you want to hide the secret messages) and the graphic which means “writing” (text).The stenographic procedure places a hidden message in a transport medium, called the carrier. The carrier may be publicly visible. The vital aim in steganography is to hide the very existence of the message in the cover medium [6].

There are two extensive approaches used in image steganography.

1. The reversible image steganography and
2. The irreversible image steganography.

Message to be embedded within an image is known as the payload. After embedding the payload in image (more specifically cover image) the resulting image called the stego image is sent to the authorized recipient, where the payload is recovered. Reversible image steganography derives its name from the mode of recovery of the payload wherein the recovered cover image is noiseless. On the contrary irreversible image steganography strives to achieve high capacity embedding without giving much emphasis on the carrier recovered during the extraction process. Reversible image steganography facilitates the easy detection of any alteration in the stego image whereas irreversible image steganography achieve high embedding capacity. Motivation for modern day’s image steganography techniques comes from the fact that no existing method is self-sufficient. Increasing the embedded information could cause easy detection by an attacker, whereas enhancing the security could increase the computation and communication overhead due to the fact that one secret message will take several transmissions. A trade-off between embedding capacity and the level of security needs a strong base for a security measure.

While steganography can be achieved using any cover media, we are concerned with hiding data in digital images. The features expected of a stego-medium are imperceptibility and robustness, so that the secret message is known only to the intended receiver and also the stego-medium being able to withstand attacks from intruders. The amount of secret message embedded should be such that it doesn’t reduce the quality of the stego image.

2. Steganography Techniques:

2.1. Classification of Steganographic Categories

Steganography is classified into three main categories. These are as follows

1. Pure steganography where there is no stego key. It is based on the assumption that no other party is aware of the communication.
2. Secret key steganography where the stego key is exchanged prior to communication. This is most susceptible to interception.
3. Public key steganography where a public key and a private key is used for secure communication.

2.2. Classification of Steganographic Methods

Steganography methods can be classified mainly into six categories. Although in some cases exact classification is not possible. [2]. Figure 4 illustrate the six classification of Steganographic methods.

Techniques used in Steganography

Miscellaneous

Cover Generation

Substitution

Insertion / Injection

Hybrid Approach

Transform Domain

Statistical Methods

Spread Spectrum

Distortion

1. Substitution methods substitute redundant parts of a cover with a secret message (spatial domain).
2. Transform domain techniques embed secret information in a transform space of the signal (frequency domain)
3. Spread spectrum techniques adopt ideas from spread spectrum communication.
4. Statistical methods encode information by changing several statistical properties of a cover and use hypothesis testing in the extraction process.
5. Distortion techniques store information by signal distortion and measure the deviation from the original cover in the decoding step.
6. Cover generation methods encode information in the way a cover for secret communication is created.

2.3. Properties

Collectively, every data hiding technique must of necessity have definite properties that are verbalized by the intended application. The most important properties of data hiding schemes are robustness, undetectability, invisibility, security, complexity, and capacity. The meanings of these concepts are presented below.

1. Robustness

Robustness controls the algorithm performance towards data distortions presented 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 accessibility of the indicator function.

1. Undetectability

Undetectability is typically required for secure covert communication. The embedded information is undetectable if the image with embedded data is dependable 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 have a duty to do so not making statistically significant changes to the noise in the carrier. The concept of undetectability is intrinsically tied to the statistical model of the cover-object source. If an attacker has a more in depth 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.

1. Invisibility

Invisibility is based on properties of human visual system or human audio system. The embedding information ought not to introduce any observable work of art or relics, 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 observable work of art or relics caused by data embedding schemes. If the observable work of art or relics was tested by presenting both covers with or without embedding information, a concept of indiscernibility would result.

1. Security

The embedding algorithm is said to be secure if embedded information cannot be removed beyond dependable detection by targeted attacks based on a complete understanding of the embedding algorithm and detector (except the secret key), and the understanding of at least one carrier with hidden message. This leads us now to the introduction of the secure black-box public and the secure public detectors. Secure black-box public detector is a message detector implemented in a tamper-proof hardware. It is anticipated that the box cannot be a reverse engineered. The secret key used to read the hidden messages is wired-in the black-box and cannot be recovered. The accessibility of the black-box should not enable an attacker to recover the secret key or remove the hidden information from the carrier. Here also, we assume that the attacker has a complete understanding of embedding algorithm and the inner workings of detection function. Of course, any embedding technique that has a secure black-box public detector must also be secure in the sense defined above. At present, it is not clear if a secure black-box public detector can be built at all. In recent times, attacks on a general class of data embedding techniques that are based on linear correlators have been described [7 - 11]. As an alternative, secure public detector is an even stronger concept for which all details of detector are publicly known. If such a detector is ever built, it would find several applications and could be implemented in software rather than tamper-proof hardware. It would also enable structure intelligent Internet browsers proficient in filtering images containing certain marks, automatic display of copyright information with every image, etc. Special care would have to be taken to overcome so called mosaic attack [12]. So far, no secure public detectors exist.

1. Conflicting Requirements

The above requirements are commonly reasonable and cannot be clearly improved 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 of necessity 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 dependably hidden cannot be too long. This observation is schematically depicted in the figure below.

**CAPACITY**

Naive steganography

**UNDETECTABILITY**

**ROBUSTENESS**

*Figure 5: Trade-off among undetectability, capacity and robustness.*

Chapter 2

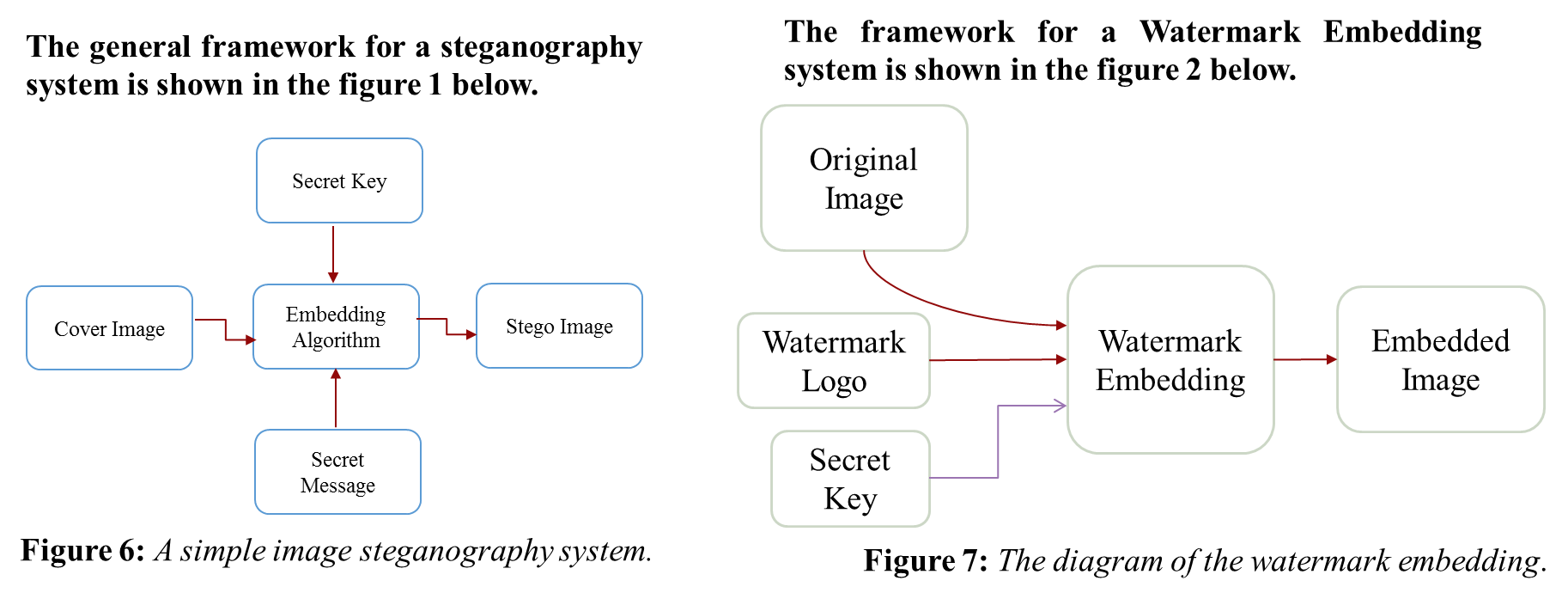
Limited Overview of the Field:

This Chapter make available some necessary literature reviews which includes Steganographic algorithms, Digital Watermarking and Encryption algorithms. There are quite a lot of surveys that have already been done in this area of knowledge. Some of the studies are discussed in this chapter.

Steganography is a modus operandi in which the secret message or secret information is hidden into the cover medium. The cover medium may be any type of medium such as text, image, audio or video file. The secret message which can be embedded into the text file has inadequacy of size, because, for example in text file very less data can be hidden. Steganography technique provides more security than that of cryptography technique. Cryptography technique protects the contents of a message. Steganography technique protects both the messages (secret message and cover message) and communicating parties. Steganography contains the hiding information within the computer files. In digital steganography, document file, image file, program or protocol are also used as a medium for hiding data. Media files are large in size. So, these media files are more effectively used for the steganography technique.

The leading expressions used in the Steganography systems are: ***the cover message, secret message, and secret key and embedding algorithm*** [13].

* ***The cover message*** is the carrier of the message such as image, video, audio, text, or some other digital media. ***The secret message*** is the information which is needed to be hidden in the suitable digital media.
* ***The secret key*** is usually used to embed the message depending on the hiding algorithms.
* ***The embedding algorithm*** is the way or the idea that usually use to embed the secret information in the cover message. [14, 15]



The present-day rapid improvement and disposition of new IT technologies for the fast delivery of commercial multimedia services has given rise to a robust demand for reliable and secure copyright protection methods for multimedia data.

Copyright protection of digital images is defined as the process of proving the intellectual property rights to a court of law against the unauthorized reproduction, processing, transformation or broadcasting of a digital image.

In recent years, the Camera Smartphone has become a prevalent consumer electronics product. Many young people and even adults like to use it to record their daily live activities; moreover, they will share these photos and information to their friends and love ones. On the other hand, these information's maybe used without their permission after they are uploaded on Blogs [16]. Since digital images can easily be redistributed without agreement, related researches on digital right protection have attracted much attention in recent years. The fact that it is not difficult copying and distributing digital multimedia data, protection against copyright violations is an important issue for the copyright owner and should form an integral part of the manipulation process for all stakeholders.

Watermarking is defined as a sequence of digital bits placed in a digital cover file that recognizes the file’s copyright information [17]. Digital watermarking is used to embed some information into the digital media which needs to be protected from illegal copying and for the purpose of authentication. It is the digital counter-part of paper water-marking. The kind of information hidden in an object when using watermarking is usually a signature to signify origin or ownership for the purpose of copyright watermarking all of the instances of an object are marked in the same way for protection [18,19]. There are several watermarking methods developed in recent years. These can be divided into two broad categories, those working in the spatial and time domain and those working in the transform (frequency) domain [20].

Watermarking algorithms can also be classified based on the domain used for watermark embedding [21]. Spatial domain watermarking directly embeds the watermark into the object [22] while frequency domain watermarking embeds the watermark by changing frequency component values by an orthogonal transformation [23]. To obtain better imperceptibility as well as robustness, the addition of the watermark is done in a transformed domain [24,25]. Digital watermarking techniques are used to protect the copyright of digital files. A variety of watermarking schemes have been proposed over the years to safeguard the digital media like music, images, official documents, etc. Digital watermarks can be used in the form of logos or images in a corner of a document or they can be invisible like in the case of digital signatures. Digital watermarking is commonly used in E-commerce to provide conditional and user specific access to some resources. Hence, the use of digital watermarking encourages creative professionals to use the internet so that their work can reach a wider audience.

2.1. State of the Art Literature Review on Steganography

Quiet a large number of schemes have been recommended in reversible and irreversible image steganography. The most important work that is going on in image steganography endeavors to structure Steganographic configuration that efficiently hides the secret image (payload). Further security is added by encrypting the secret image (payload) with encryption algorithms, this may however increase the complexity of the Steganographic scheme twofold.

The essential prerequisite for any secure steganography scheme is its capacity to cover the hidden message in the cover image. A system is considered to be secure if an intruder cannot make a distinction between the cover image and the stego image. There are diverse measures for Steganographic security. The most common measure is called detectability of a stego system. Detectability is defined as the relative entropy between the probability distribution of cover image and the stego image. Any steganography system is called  -secure if the relative entropy of the system is at most  [26].  
A steganography scheme is said to be impeccably secure if detectability is zero. A reduction in detectability means reduced embedding capacity. Any image steganography scheme should optimize the embedding capacity to achieve minimum possible detectability taking into account the computational overhead.  
Steganographic capacity is the maximum number of bits that can be embedded in a cover image and recovered from the stego image without violating the undetectability constraints. The maximum Steganographic capacity that an existent reversible Steganographic scheme can achieve is approximately 3 bpp [27]. Perceptual dependability and robustness are the utmost desirable characteristics of any Steganographic system. The capability of the Steganographic system is systematically boosted by irreversible models of image steganography. Peak signal to noise ratio can be used as a measure of Steganographic security where the embedding capacity of a model is outsized. Increasing the secret information embedding capacity would mean straightforward steganalytic and detection of the hidden information. The State of the art steganalytic endeavor to subdue any steganography scheme. The principal test of a steganography scheme is its ability to outwit all steganalytic schemes [26]. The science of detecting a hidden message in a cover image is steganalytic. The conflict between steganography and steganalytic has been on since the advancement of the science of steganography. There are quite a lot of techniques in which steganalytic can be used to crash the structure of steganography. The most common techniques are scrutiny of the inner structure of LSBs, Histogram analysis, feature vector analysis et cetera [26]. Primary goal of any image steganography scheme is to achieve high level of security with high capacity embedding, reduced noise, and minimum computation time.

In 2015, 2003:G. Prashanti and K. Sandhyarani, Provos, N. and Honeyman, P respectively [28, 29] have done some surveys on recent achievements of LSB based image steganography. In this surveys the authors argued the enhancements that boost the Steganographic results such as high robustness, high embedding capacity and un-detectability of hidden information. In conjunction with this survey two new techniques are also proposed. The first technique is used to embed data or secret messages into the cover image and in the second technique a secret gray scale image is embedded into another gray scale image. These techniques use four state table that produce pseudo random numbers. This is used for embedding the secret information. These two methods have greater security because secret information is hidden on random selected locations of LSBs of the image with the help of pseudo random numbers generated by the table.

Chih-Chiang Lee et al. proposed an adaptive lossless image steganography scheme, this scheme embeds variable length secret information into fixed sized blocks of the cover image. The amount of information embedded in each block depends on the complexity of the cover image [30]. This technique is an enhancement over Alattar’s scheme based on generalized difference expansion [30], where N successive pixels of the cover image are taken to embed N-1 bits of secret information. The enhancement is attained in embedding capacity by the use of a number of non-overlapping blocks of size *m* x *n* in place of N-1 difference values to hide the secret information as proposed by Alattar [30]. If the secret information under consideration is a grayscale image of size *a* x *b* and average number of bits embedded in each block of size *m* x *n* is four (4), then the total number of such blocks required is . Hence the size of the required cover image is. In this scheme, the secret information is embedded into the centralized difference values without encryption. If a small sized grayscale image is to be embedded using state of art encryption techniques to add another layer of security, huge computation time may lessen the proficiency of the technique.

In the Reversible image hiding scheme proposed in [31], the embeds secret information is done by shifting the histogram of residual image computed as the difference of the original cover image and the corresponding predictive pixel, called the basic pixel, obtained using linear prediction technique. This scheme is also is an improvement over reversible data hiding scheme proposed in [32]. The hiding capacity is increased by employing linear prediction technique on the cover image to form the residual image. A similar approach has been proposed by Lin et al. [33].

The secret information embedding scheme proposed in [34] hides encrypted payload into a hiding tree computed from frequency of absolute error values obtained as the difference of the cover image (host image) and predictive image. Predictive image is generated using median edge detector (MED) predictor. Similar reversible image steganography schemes have been proposed in [35-36], where error values are explored to embed the secret information. Although state of art steganography methods hide the secret information systematically, encryption is applied on the secret message to provide an extra layer of security. The approaches of image steganography proposed in [31-36] are themselves complex enough; hence extra computational complexity of standard encryption techniques, such as AES or DES, can reduce the efficiency of the Steganographic system. LSB replacement is the most commonly used irreversible Steganographic method.

In this method, only the LSB plane of the cover image is replaced with any of the bit plane of the grayscale payload. As a result, the change in bit structure of the original cover image is predictable, and as a result the existence of the hidden payload even at a low embedding rate is possible with the use of some existing steganalytic algorithms, such as the Chi-squared attack [37], regular or singular groups (RS) analysis [38] and sample pair analysis [39]. LSB matching (LSBM) is an improvement over LSB replacement. A precise pixel intensity of the cover image is either increased or decreased by 1 if there is a match between the secret bit and the LSB of that pixel. Several steganalytic algorithms [40-43] have been proposed to analyze the stego image encoded using LSBM scheme. Encryption techniques are used to foil these steganalytic algorithms.

The proposed technique spreads the payload across different matrices to attain the same visual distortion as any encryption technique. As the payload is spread into different matrices any intruder has to retrieve all matrices to re-compute the payload precisely. Any image steganography scheme should eradicate the suspicion of the existence of any hidden information within the cover image.

Chapter 3

My Theory/Solution/Algorithm/Program:

3.1 My Theory:

In this paper our data will be the plain text that we need to hide, and the unused data is the least significant bits (LSBs) in the image pixels. The methodology use to hiding the text inside the image is explained by the following steps:

1. Loop through the pixels of the image. In each iteration, get the RGB values separated each in a separate integer.
2. For each of R, G, and B, make the LSB equals to 0. These bits will be used in hiding characters.
3. Get the current character and convert it to integer. Then hide its 8 bits in R1, G1, B1, R2, G2, B2, R3, G3, where the numbers refer to the numbers of the pixels. In each LSB of these elements (from R1 to G3), hide the bits of the character consecutively.
4. When the 8 bits of the character are processed, jump to the next character, and repeat the process until the whole text is processed.
5. The text can be hidden in a small part of the image according to the length of that text. So, there must be something to indicate that here we reached the end of the text. The indicator is simply 8 consecutive zeros. This will be needed when extracting the text from the image.

We use database to store and also recommendations of different user to avid missed up. AForge and OpenCV is used for the image processing. AForge has lots of filters and is probably excellent for different transforms and image manipulation. AFORGE.NET, plus its Image Processing Lab makes much sense for filtering options such as edge detection, thresholds, and so forth and easing viewing functionalities. OpenCV has a rich feature set like SIFT/SURF and other more sophisticated image processing routines.

3.2 Algorithm

In this paper we proposed Discrete Wavelet Transform and Permutation Method. The discrete wavelet transform and permutation method are used to falsify the original image and watermark, respectively to embed watermark into the original image. We use a binary or gray-scale logo as a watermark. The permutated watermark embeds in the wavelet coefficients of the DWT of an image.

Assuming that the watermark of length *Nw* is binary and comprises of elements from the set {0, 1}. To embed the mark in the discrete wavelet domain, comparative modifications are executed on the coefficients so that the host image is not required for extraction. We first permutated the watermark and then embed it into the element components of the original image with the use of a key.

This key *k* comprises of three main components:

1. The particular DWT used to embed the watermark
2. The embedding parameter *Q*
3. The coefficient assortment key *Ks*

The coefficient assortment key *Ks* is indiscriminately generated by the linear congruential generator (LCG) algorithm that is used to select the exact locations in the wavelet domain in which to embed the permutated watermark. For each coefficient within the wavelet domain the key *Ks*, has a value of one (1) or zero (0) to signify that the coefficient is to be mark or not, respectively.

3.3. Key Generation Algorithm

1. Start with a seed value of *Z0* and length *L*
2. Calculate the *Zi = (a\*Zi-1+c)* mod *m* where *a* = multiplier, *c* = increment and *m* = modules
3. *Ks(i) = Zi/m*;
4. Increment *c = c*+*1* and *i* = *i*+*1* where *i* = index of *Ks*
5. Continue step 2 until *c* = *L*

3.4 Watermark Embedding

In this segment, as already stated above we at first applied the permutation on the watermark to challenge the watermark, for which the watermark is imperceptible to the human visual system (HVS). We embed the permutated watermark into the detail wavelet coefficients of the original image with the use of a key. On the other hand, in the wavelet base watermarking, the watermark is spread all over the image. The block diagram of our proposed method for watermark embedding is shown in Fig. 8.

***Figure 8 illustrates a block diagram of the proposed Watermark Embedding***.

Step 1:

The original image is transformed into the discrete wavelet domain. Precisely, we perform the Lth level DWT of the original image to produce a sequence of 3L detail images at each of the L resolution levels, and an unsophisticated approximation of the image at the roughest resolution level. We signify the *O*th frequency orientation at the *l*th resolution level of the image f by f*o,l (m, n)* where *O* 󠅬 {1,2,3) represents the frequency orientation equivalent to the horizontal, diagonal and vertical image details, *l* {1,2, . . , L) is the resolution level and *(m, n)* is the precise spatial location index at the resolution 1. The unsophisticated approximation is represented by  *f*4, L*(m, n)* where the subscript "4" is used instead of *O* to signify the unsophisticated image approximation at resolution L.

Step 2:

In this phase we permutated the watermark and the permutated watermark bits are embedded in the original indicator coefficients specified by the key *Ks*. If the *Ks* specifies that the location *(m, n)* at resolution l can be marked, then we perform the following steps:

1. The detail coefficients *f1,l(m, n), f2,l(m, n)* and *f3,l(m, n)* are sorted in ascending order. We signify these ordered coefficients by *fo1,l(m, n), fo2,l(m, n)* and *fo3,l(m, n).*

Where,

*fo1, l (m, n)* *fo2, l (m, n) fo3, l (m, n)*

Such that *o1, o2, o3* {1, 2, 3) and *o1 ≠ o2, o2 ≠ o3*:and *o1 ≠ o3*.

1. A single permutated watermark bit is embedded by modifying the median value of the detail coefficients at resolution *l* (i.e.,  *fo2,l(m, n)*) at spatial location *(m, n)*. To embed the watermark, we quantize *fo2, l (m, n)*. The range of values between *fo1,l(m, n)* and *fo3,l (m, n)* are divided into bins of width

where *Q* is a key -specified quantization variable. To embed a permutated watermark bit of value zero (0) or one (1) *fo2,l (m, n)* is quantized to the nearest value. The new watermarked coefficients are denoted *fwo, l (m, n)*.

It should be clarified that an attacker cannot without difficulty determine the precise key *Ks*, and eradicate the watermark specified, but only the watermarked image if the specific wavelet transform used in the decomposition of stage *I* is kept secret and *Q* is unknown.

For that reason, it is not conceivable to use the relative value of the coefficients to determine the watermark locations and hence destroy the mark by arbitrarily altering the coefficient subscriptions by small amounts. The value of *Q* determines the trade-off between robustness and visibility of the watermark. The smaller its value, the more robust is the mark.

Step 3:

The resultant *Lth* level inverse DWT of the coefficients *fwo, l(m, n)* is computed to form the watermarked image *fw* . The complexity of the first and third stages rest on the particular DWT employed (which is specified in *K*) and its associated implementation.

3.5 The Watermark Extraction

***Figure 9, illustrate a block diagram of Watermark Extraction***

Let *f’w*, be the indicator from which we would like to extract the watermark. We first apply an *Lth* level DWT on *f’w* to produce the coefficients *fwo, l' (m, n).* We use the key *Ks*, to find the locations in which the watermark was embedded for each resolution level *l*. We extract the watermark bits from these coefficients using these steps:

1. The detail coefficients *f1,l(m, n), f2,l(m, n) and f3,l(m, n)* are sorted in ascending order. The ordered coefficients are represented by

*fw’o1, l (m, n) fw’o2, l (m, n) fw’o3, l (m, n)*

Such that *o1, o2, o3 {1, 2, 3)* and *o1 ≠ o2, o2 ≠ o3* and *o1 ≠ o3*.

1. The watermark bit value is predictable from the relative position of *fw’o2, l (m, n)*. By means of the same value of *Q* as for embedding (which is given by *K*), the watermark value is determined by finding the closest quantized value, to *fw’o2,l (m, n)* and converting it to its associated binary number.
2. If the watermark classification has been embedded a number of times, then the most common extracted bit value is taken for the watermark estimate. Our methodology improved the performance from characterizing the misrepresentation on the watermarked indicator for fusion watermarking. We propose a method to improve the performance of a broad class of watermarking schemes through attack characterization.

3.6 Algorithm (Encoding)

Our algorithm provide double protections to maintain privacy, accuracy and confidentiality in data. As previous we show the framework of the process. Our system hide the messages in image and also the receiver can decry pt. that messages. It is impossible for anyone to access the data from image, username and password are required. Only legitimate user can access. The following steps was taking:

step1: Type the messages in text format

step2: covert the messages into binary codes

step3: Now set bit per unit to zero

step4: Encode the messages

step5: add by 2 unit for bits per unit

step6: image with secret message is received.

* + 1. Algorithm (For Decoding)

Step1: Take image

step2: Calculate bit per unit

step3: Decode binary codes

step4: Shift by 2 unit for bit per unit

step5: Convert binary to text

step6: Output secret messages

Chapter 4

Description of Implementation:

There are different languages to implementing any project like C, C++, C#, Java, Matlab etc. In this paper, we have chosen the C-Sharp (C#) language programming. C-Sharp (C#) is a hybrid of [C](https://www.webopedia.com/TERM/C/C.html) and [C++](https://www.webopedia.com/TERM/C/C_plus_plus.html), it is a [Microsoft](https://www.webopedia.com/TERM/M/Microsoft.html) [programming language](https://www.webopedia.com/TERM/P/programming_language.html) developed to compete with [Sun's](https://www.webopedia.com/TERM/S/Sun_Microsystems.html) [Java](https://www.webopedia.com/TERM/J/Java.html) language. It is an [object-oriented](https://www.webopedia.com/TERM/O/object_oriented.html) programming language used with [XML](https://www.webopedia.com/TERM/X/XML.html)-based [Web services](https://www.webopedia.com/TERM/W/Web_Services.html) on the [NET](https://www.webopedia.com/TERM/D/dot_NET.html) platform and designed for improving efficiency in the development of Web applications. C-Sharp (C#) boasts type-safety, garbage collection, simplified type declarations, versioning and scalability support, and other features that make developing solutions faster and easier, especially for COM+ and Web services.

Chapter 5

Comparative Study and Results:

In this segment, we make available some comparisons of existing methods in the direction of our proposed method. In Md. Selim el al [44] method, the system permutated the watermark and embed the permutated watermark into the wavelet coefficients of the original image by using a key. The key is indiscriminately produced and used to select the locations in the wavelet domain in which to embed the permutated watermark. In Chang -Hsing Lee and Yeuan-Kuen Lee’s method [45], the watermark used as a key rather than a randomly generated number. The proposed method uses the linear congruential generator (LCG) algorithm for generating the key based on a seed value. The key is generated by using this formula, Ks(j): = rand Seed (0,1) which is based on an undeviating random number generator between 0 and 1. In Abou Ella Hassanien’s method [46], the key is randomly generated from the image and takes more time for generating the key. The embedding stage of Abou Ella Hassanien’s method, decompose the original image into the 3-level wavelet decomposition. And the watermark values are frequently embedded in diverse coefficients selected by the key. Chang-Hsing Lee and Yeuan-Kuen Lee’s method, the permutated watermark is embed into the spatial location of the host image.

In our proposed method, we crumble the original image into 4-level wavelet transform using The Wavelet Studio project, which is a set of tools built in C# to assist the signal processing with Wavelet Analysis and also permutated the watermark. The permutated watermark values are continually embedded in diverse coefficients selected by the key so that it will be able to spread the watermark to all over the original image and more robust to attacks on the embedded watermark.

With the extraction segment, Chang-Hsing Lee and Yeuan-Kuen Lee’s method [45], need the original image for the watermark extraction. In Abou Ella Hassanien’s method [46], need the watermark and key for extraction. Our proposed method and that of Md. Selim el al [44] method are quiet similar, we can extract the watermark without reference to original image, and the method only needs the key to extract.

Chapter 6

Conclusion

A copyright protection for a secret data hiding scheme based on discrete wavelet transform and permutation is proposed. The proposed algorithms follows a sequence of steps which includes watermark embedding and watermark detection has been described in this paper. With the application of discrete wavelet, the watermark spread abroad over the image and by permutation, the watermark becomes invisible to the human eyes.

Result:

using System;

using System.Collections.Generic;

using System.Linq;

using System.Windows.Forms;

namespace Encryption

{

static class Program

{

/// <summary>

/// The main entry point for the application.

/// </summary>

[STAThread]

static void Main()

{

Application.EnableVisualStyles();

Application.SetCompatibleTextRenderingDefault(false);

Application.Run(new Form1());

}

}

}

For generating Images:

using System;

using System.Collections.Generic;

using System.Linq;

using System.Text;

using System.Drawing;

using System.Drawing.Drawing2D;

using System.Drawing.Text;

using System.Drawing.Imaging;

using System.IO;

namespace Encryption

{

public class GenerateImage

{

public Bitmap CreateBitmap(string txt, string fontname, int fontsize)

{

//creating bitmap image

Bitmap bmp = new Bitmap(1, 1);

//FromImage method creates a new Graphics from the specified Image.

Graphics graphics = Graphics.FromImage(bmp);

// Create the Font object for the image text drawing.

Font font = new Font(fontname, fontsize);

// Instantiating object of Bitmap image again with the correct size for the text and font.

SizeF stringSize = graphics.MeasureString(txt, font);

bmp = new Bitmap(bmp, (int)stringSize.Width, (int)stringSize.Height);

graphics = Graphics.FromImage(bmp);

/\* It can also be a way

bmp = new Bitmap(bmp, new Size((int)graphics.MeasureString(txt, font).Width, (int)graphics.MeasureString(txt, font).Height));\*/

//Draw Specified text with specified format

graphics.DrawString(txt, font, Brushes.Red, 0, 0);

font.Dispose();

graphics.Flush();

graphics.Dispose();

return bmp; //return Bitmap Image

}

}

}

For DECS.CS

using System;

using System.Collections.Generic;

using System.ComponentModel;

using System.Data;

using System.Drawing;

using System.Linq;

using System.Text;

using System.Windows.Forms;

using System.IO;

using System.Data;

using System.Data.SqlClient;

using System.Security;

using System.Security.Cryptography;

namespace Encryption

{

public partial class DECS : Form

{

string imgPath = null;

public DECS()

{

InitializeComponent();

}

public void check()

{

DataTable dt = new DataTable();

DatabaseCOnn objCon = new DatabaseCOnn();

dt = objCon.ExecDataTable("select \* from tblCDATA where IMG = '"+imgPath+"'");

if (dt.Rows.Count == 1)

{

string data = dt.Rows[0]["CDATA"].ToString();

string show = AESDecrypt(data);

lblData.Text = show;

}

else

{

MessageBox.Show("DATA IS NOT AVAILABLE");

}

}

Appendices