I. J. Computer Network and Information Security, 2012, 10, 76-92
Published Online September 2012 in MECS (http://www.mecs-press.org/)
DOI: 10.5815/ijcnis.2012.10.08

Adaptive Steganography: A survey of Recent Statistical Aware Steganography Techniques

Manish Mahajan
Faculty Department of Information Technology Chandigarh Engg College Landran, Mohali , Punjab India
manishmahajan4u@gmail.com
Dr. Navdeep Kaur
Faculty Department of Information Technology Chandigarh Engg College Landran, Mohali , Punjab India
drnavdeep.cec@gmail.com

Abstract — Steganography is the science that deals with hiding of secret data in some carrier media which may be image, audio, formatted text or video. The main idea behind this is to conceal the very existence of data. We will be dealing here with image steganography. Many algorithms have been proposed for this purpose in spatial & frequency domain. But in almost all the algorithms it has been noticed that as we embed the secret data in the image the certain characteristics or statistics of the image get disturbed. Based on these disturbed statistics steganalysts can get the reflection about the existence of secret data which they further decode with the help of available steganalytic tools. Steganalysis is a science of attacking the hidden data to get an authorized access. Although steganalysis is not a part of this work but it may be sometimes discussed as a part of literature. Even in steganography we are not purely concerned with spatial or frequency domain rather our main emphasis is on adaptive steganography or model based steganography. Adaptive steganography is not entirely a new branch of steganography rather it is based upon spatial & frequency domain with an additional layer of mathematical model. So here we will be dealing with adaptive steganography which take care about the important characteristics & statistics of the cover image well in advance to the embedding of secret data so that the disturbance of image statistics as mentioned earlier, which attracts the forgery or unauthorized access, can be minimized. In this survey we will analyze the various steganography algorithms which are based upon certain mathematical model or in other words algorithms which come under the category of model based steganography.

Index terms — Model based steganography, frequency domain, Spatial domain and Adaptive steganography

I. INTRODUCTION

Since the dawn of human communication, there has been a need to protect messages that travel between multiple parties. One of the earliest forms of protection is known as steganography [10].The word "steganography" can be defined as "covered writing" or the technique of hiding messages inside other messages. This idea of data hiding is not a novelty, it has been used for centuries all across the world under different regimes - but to date it is still unknown to most people - is a tool for hiding information so that it does not even appear to exist [1]. This is a process, which can be used for example by civil rights organizations in repressive states to communicate their message to the outside world without their own government being aware of it. Less virtuously it can be used by terrorists to communicate with one another without anyone else's knowledge. In both cases the objective is not to make it difficult to read the message as cryptography does, it is to hide the existence of the message in the first place possibly to protect the courier [2]. With the emergence of the Internet and its explosive growth as a communication medium and in content distribution capabilities, the need to protect ourselves and our property is greater than it has ever been. It is this necessity for protection that has fueled intense development of steganographic applications. A steganographic system thus embeds hidden content in unremarkable cover media so as not to arouse an eavesdropper's suspicion [10]

1.1 Terminology

In the field of steganography, some terminology has developed. The adjectives cover, embedded and stego were defined at the Information Hiding Workshop held in Cambridge, England . The information to be hidden in the [3] cover data is known as the "embedded" data. The "stego" data is the data containing both the cover signal and the "embedded" information. Logically, the process of putting the hidden or embedded data, into the cover data, is sometimes known as embedding. Occasionally and especially when referring to image steganography, the cover image is known as the container. The term "cover" is used to describe the original, innocent message, data, audio, still, video and so on. When referring to audio signal steganography, the cover signal is sometimes called the "host" signal. This process could be represented the following formula:

cover medium + embedded message + stegokey = stego-medium [2].

Detection of steganography, estimation of message length, and its extraction belong to the field of steganalysis. Steganalysis has recently received a great deal of attention both from law enforcement and the media [36].

II. HISTORY OF INFORMATION HIDING

The idea of communicating secretly is as old as communication itself. While information hiding techniques have received a tremendous attention recently, its application goes back to Greek times. According to Greek historian Herodotus, the famous Greek tyrant Histiaeus, while in prison, used unusual method to send message to his son-in-law. He shaved the head of a slave to tattoo a message on his scalp. Histiaeus then waited until the hair grew back on slave's head prior to sending him off to his son-in law. In the second story Demeratus removed the wax from the tablet, wrote the secret message on the underlying wood, recovered the tablet with wax to make it appear as a blank tablet and finally sent the document without being detected. Ancient Romans used to write between lines using invisible inks based on readily available substances such as fruit juices, urine and milk. When heated, the invisible inks would darken, and become legible Ovid in his "Art of Love" suggests using milk to write invisibly. Later chemically affected sympathetic inks were developed. Invisible inks were used as recently as World War II. Nowadays "VOID" is printed on checks and other official documents in an ink that appears under the strong ultraviolet light used for photocopies [4]. The monk Johannes Trithemius, considered one of the founders of modern cryptography, had ingenuity in spades. His three volume work Steganographia, written around 1500, describes an extensive system for concealing secret messages within innocuous texts [4]. On its surface, the book seems to be a magical text, and the initial reaction in the 16th century was so strong that Steganographia was only circulated privately until publication in 1606. But less than five years ago, Jim Reeds of AT&T Labs deciphered mysterious codes in the third volume, showing that Trithemius' work is more a treatise on cryptology than demonology [4]. Reeds' fascinating account of the code breaking process is quite readable. One of Trithemius' schemes was to conceal messages in long invocations of the names of angels, with the secret message appearing as a pattern of letters within the words. For example, as every other letter in every other word [4]:

"padiel aporsy mesarpon omeuas peludyn alpreaxo" which reveals "prymus apex."

Another clever invention in Steganographia was the "Ave Maria" cipher. The book contains a series of tables, each of which has a list of words, one per letter [4]. To code a message, the message letters are replaced by the corresponding words. If the tables are used in order, one table per letter, then the coded message will appear to be an innocent prayer [4]. The earliest actual book on steganography was a four hundred page work written by Gaspari Schott in 1665 and called Steganographica. Although most of the ideas came from Trithemius, it was a start. [4]

2.1 Historical division of steganography

Throughout history there have been two major types of steganography, technical and linguistic. Technical steganography is more based upon scientific methods of hiding information while linguistic employs more creative and non-apparent methods. [4]

2.1.1 Technical Steganography

The most well known technical means is invisible ink. The process is simple, some form of writing utensil is dipped into a special liquid that when dry disappears. The paper will then appear to be blank. Whenever it needs to be read the recipient can use a variety of methods to see the text written, depending on what type of ink was used [4]. The most common methods of decoding the message are the use of ultra-violet light, a special "decoder pen" that you write over the hidden text, and applying heat to the document [10]. Ancient Romans used to write between lines using invisible inks based on readily available substances such as fruit juices, urine and milk. When heated, the invisible inks would darken, and become legible. During World War II, null ciphers (unencrypted message) were used to hide secret messages. The null cipher, which often appeared to be innocent message about ordinary occurrences, would not alert suspicion, and would thus not be intercepted. With the advent of photography, microfilm was created as a way to store a large amount of information in a very small space.

Contemporary color laser jet printers have been using a similar idea by printing a pattern of extremely small yellow dots onto each page. Under normal white light the dots are nearly invisible, but when placed under pure blue light they can be seen. These patterns of dots encode the serial number of the printer and the timestamp of when the document was printed. The intention of this technique was to prevent counterfeiting (EFF) [4].

2.1.2 Linguistic Steganography

Linguistic steganography utilizes more openly visible methods of hiding information that depend on manipulation of language and text and not technology. It can be subdivided into two categories: open codes and semagrams. Open codes hide messages in other reasonable messages in ways that aren't obvious to the average reader [1]. An example of an open code:"News Eight Weather: Tonight increasing snow. Unexpected precipitation smothers eastern towns. Be extremely cautious and use snowtires especially heading east. The highway is not knowingly slippery. Highway evacuation is suspected. Police report emergency situations in downtown ending near Tuesday."

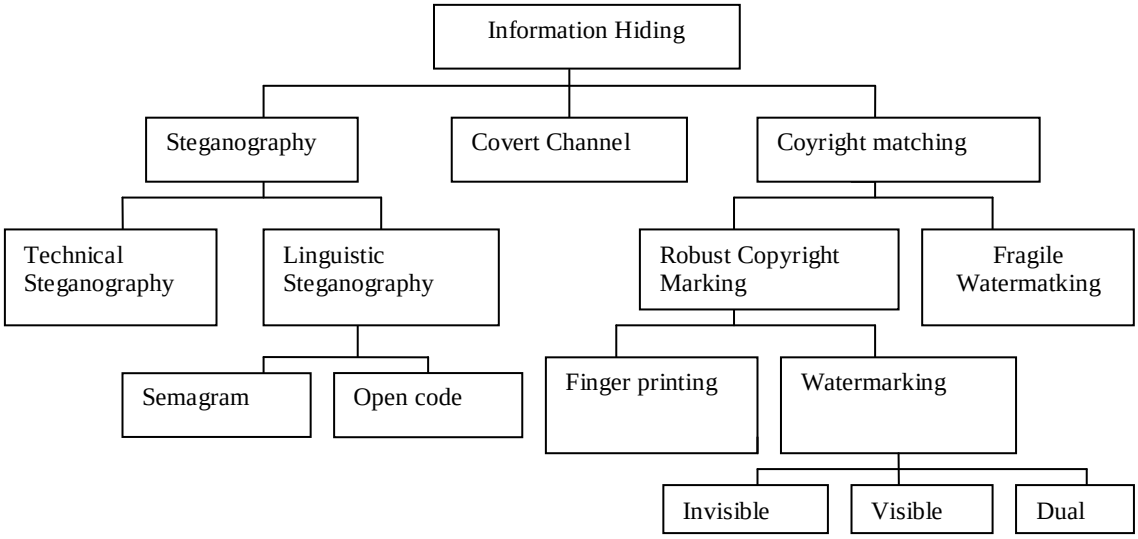


Fig. 1 Information Hiding Techniques

The example above is what is called a null cipher. In a null cipher only some of the information presented is important, in this case the first letter of every word. When we read the first letter of every word we see that the hidden message is "Newt is upset because he thinks he is President" (Kessler).

The second form of linguistic steganography is the Semagram [1]. Semagrams hide information by the use of visual signs. These signs can be pictures or changes in the visual style of text. The simplest example of this type would be: "There are *mor e at*ing *meal*s *t*owards the *8*5th street." In previous example, italic letters are used to identify the important pieces of the message, which read "meet me at 8." Semagrams like the one just described aren't the most secure of the bunch, and for anyone really looking for steganography would pick up on this very quickly [1]. However, other types of semagrams, such as arranging items on a desk in a certain fashion or a picture that conveys meaning are very effective. [10]

2.2 Modern Steganography

In order to embed secret data into a cover message, the cover must contain a sufficient amount of redundant data or noise. This is because in the embedding process Steganography actually replaces redundant data with the secret message. This limits the types of data that we can use with Steganography. There are basically three types of steganographic protocols used. They are Pure Steganography, Secret Key Steganography, and Public Key Steganography [4]. Pure Steganography is defined as a steganographic system that does not require the exchange of a cipher such as a stego-key. This method of Steganography is the least secure means by which to communicate secretly because the sender and receiver can rely only upon the presumption that no other parties are aware of this secret message.

Secret Key Steganography is defined as a Steganographic system that requires the exchange of a secret key (stego-key) prior to communication [4]. Secret Key Steganography takes a cover message and embeds the secret message inside of it using a secret key (stego-key). Only the parties who know the secret key can reverse the process and read the secret message. Unlike Pure Steganography where a perceived invisible communication channel is present, Secret Key Steganography exchanges a stego-key, which makes it more susceptible to interception. The benefit to Secret Key Steganography is even if it is intercepted; only parties who know the secret key can extract the secret message Public Key Steganography takes the concepts from Public Key Cryptography as explained below.

Public Key Steganography is defined as a steganographic system that uses a public key and a private key to secure the communication between the parties wanting to communicate secretly [4]. The sender will use the public key during the encoding process and only the private key, which has a direst mathematical relationship with the public key, can decipher the secret message. Public Key Steganography provides a more robust way of implementing a steganographic system because it can utilize a much more robust and researched technology in Public Key Cryptography. [4]

III . STEGANOGRAPHY REQUIREMENTS & DOMAINS

3.1 Kerchoff's Principle

The security of the system has to be based on the assumption that the enemy has full knowledge of the design and implementation details of the steganographic system. The only missing information for the enemy is a short, easily exchangeable random number sequence, the secret key. Without this secret key, the enemy should not have the chance to even suspect that on an observed communication channel, hidden communication is taking place [1]

3.2 Various Domains of Steganography

In this paper we are dealing with steganography methods where the carrier file is image only as it is the most common medium for transferring secret information on the internet. As per literature broadly there are mainly two domains for image processing that is spatial domain & frequency domain. As we are considering only image as carrier so steganography will also be considered in these two domains or a domain based on these two domains.

Spatial domain steganography is a technique in which secret message is encoded in the LSBs of carrier image. More the number of LSBs used for hiding the secret message more will be the capacity of carrier image but also more will be the distortion in the stego image. Stego1bit [2], Stego2bit [2], Stego3bit [2], Stego4bit [2], Stego Colour cycle [2], Stego1bitprng [2], Stegofridrich [2] , color palette based steganography [2], +/- 1 steganography, random channel steganography, blue channel steganograhy are certain spatial based steganography techniques which uses LSBs of carrier image to embed secret message. Although spatial domain methods are simple to implement but these methods cannot easily deceive the Human Visual System (HVS). So their imperceptibility factor is really low. We can try to increase imperceptibility by using only one or two LSB bits of carrier but it will decrease the capacity. So there is trade-off between payload & cover image distortion. Even by reducing the capacity the careful analysis of bit patters can easily break the spatial domain steganography. Robustness factor for the spatial domain steganography is also not very impressive. Some other algorithms related to this field & other image processing tasks like compression have been studied to get am good understanding [61- 64].

Further LSB encoding is extremely sensitive to any kind of filtering or manipulation of the stego mage [65-68].

So we need a steganography method which is good in deceiving Human Visual System. New algorithms emerged by the rapid development of information technology and by the need for an enhanced security system & the next milestone were frequency domain. It comprises algorithms based upon discrete cosine transforms (DCT), Fourier transforms (FT), and discrete wavelet transforms (DWT). In this domain various algorithms are Li and Wang steganography [5], McKeon 2DdiscreteFourier transform (DFT) based steganography [44], Jsteg for jpeg images [6, 7], OutGuess [8], "F5''algorithm [9]. Besides some DWT based techniques like W.Y.Chen, Color image steganography scheme using set partitioning in hierarchical trees coding [11], Abdulaziz and Pang technique based upon vector quantization called Linde-Buzo-Gray (LBG)coupled with block codes known as BCH code and 1-stage discrete Haar wavelet transforms [12] are certain wavelet based steganography techniques. The DWT-based embedding technique is still in its infancy. Paulson [13] reports tha a group of scientists at Iowa State University are focusing on the development of an innovative application which they call' Artificial Neural Network Technology for steganography (ANNTS)''aimed at detecting all present steganography techniques including DCT, DWT and DFT. In frequency domain generally secret message is embedded in DCT or DWT coefficients. Inserting in one coefficient will affect whole block or image which is almost unnoticeable in most of the cases. Undoubtedly frequency domain based steganography techniques are very much successful in deceiving HVS but selecting the coefficients for inserting the secret bits is really important because certain DCT coefficients are more sensitive than others in terms of image distortion. So if coefficients are not selected carefully image distortion can be easily seen with naked eye. Jsteg algorithm [6, 7] leaves a significant amount of signature so they can be easily broken by X^2 test. Wayner [14] stated that the coefficients in JPEG compression normally fall along a bell curve and the hidden information embedded by JSteg distorts this. Manikopoulos et al. [15] discussed an algorithm that utilizes the probability density function (PDF) to generate discriminator features fed into a neural network system which detects hidden data in this domain. Provosetal [8, 16, 17] suggest applying an extended version of the X^2 test which can beat the Outguess [8] algorithm. Similarly Fridrichetal. [18] proposed steganalysis that can break F5. In DWT based algorithms it should be noted that extracted payload may not be totally identical to the embedded version [19]. So even in DWT we cannot even expect 100% accuracy of the hidden message being decoded at receiver end.

IV. SIGNIFICANCE & EVOLUTION OF MODEL BASED STEGANOGRAPHY

No new domain in any field can evolve without its need. Even no field can be developed at one go. It needs certain stages & lot of research work, only then a field can evolve up to some maturity. Same is the case with adaptive steganography which is evolved due to appealing need of secure communication & still getting mature. The various details of its evolution are discussed below.

4.1 Need of Model based steganography

So it can be easily seen that both spatial domain & frequency domain techniques have their own advantages & disadvantages. No doubt we get certain security benefits in frequency domain over spatial domain but the simplicity of the spatial domain cannot be ignored. We have analyzed that most of the security loopholes in the steganographic system are due to the certain statistics of stego image which reflect or indicate the presence of certain hidden data in the image .Another factor that contributes towards the indication of the hidden information is distortion of image or artifacts present in the image that attracts the attention of the observer.To solve these problems to

certain extent there exists a third category of steganography based on two former categories which is known as model based steganography. This category of steganography is basically implemented in spatial or frequency domain but before manipulating or interacting with LSBs or DCT/DWT coefficients, the characteristics or features are studied, statistics of image are analyzed & then based upon these results certain mathematical model is generated that is why this category is known as model based steganography. This type of steganography is also known as adaptive steganography (as hidden data is adapted according to given model) & statistical aware steganography (as statistics of image are analyzed before hiding the data.

4.2 Need of the Survey of Adaptive Steganography techniques

Johnson et al. [20] published a survey of various available techniques of steganography in 2000. They include all the carrier media like audio files, echo hiding, formatted text etc. But we are presenting a paper for digital images as carrier only & besides the concept of adaptive steganography is really new which is not even touched in the work of Johnson et al. [20].In another work of Bailey and Curran [2] only available tools based upon spatial domain are analyzed even they did not touched the concept of adaptive steganography as this concept was very new at that time.Another work by Sabu M. Thampi "Information Hiding Techniques: A Tutorial Review" was published in 2004 but the latest paper cited was of 2001 so even they were not able to consider the concept of model based steganography [4].

Above all the concept of adaptive steganography has been started in 2003 when Sallee proposed an idea for model based steganography [21]. This idea is new but there are remarkable numbers of techniques which have been proposed in this field in last seven years. So this field individually needs a survey so that all the techniques can be analyzed at one place with pros & cons of each.

4.3 Model Based Steganography

Model-based steganography introduces a different methodology, where the message is embedded in the cover according to a model representing cover message statistics. Masking techniques are very much near to model based steganography. Masking is more robust than LSB insertion with respect to compression, cropping, and some image processing [22]. Masking techniques embed information in significant areas so that the hidden message is more integral to the cover image than just hiding it in the "noise" level. This makes it more suitable than LSB with, for instance, lossy JPEG images [22].Image properties such as luminance can also be manipulated. Patchwork [25] and similar techniques use redundant pattern encoding or spread spectrum methods [26] to scatter hidden information throughout the cover images ("patchwork" is a method that marks image areas, or patches). These approaches may help protect against image processing such as cropping and rotating, and they hide information more thoroughly than by simple masking. They also support image manipulation more readily than tools that rely on LSB [22].

A framework has been proposed by N. Provos & P. Honeyman [8] for an embedding algorithm that uses global image statistics to influence how coefficients should be changed. To embed a single bit, one can either increment or decrement a DCT coefficient's value. This allows change a DCT coefficient's least-significant bit in two different ways [8]. Additionally, author created groups of DCT coefficients and use the parity1 of their least-significant bits as message bits to further increase the number of ways to embed a single bit. For every DCT block, it searches the space of all possible changes to find a configuration that minimizes the change to image statistics [8]. Still they are searching for solutions that maintain the blockiness, the block variance, and the coefficient histogram. Author discussed two different classes of detection algorithms: one based on inherent statistical properties and the other on class discrimination. Detection algorithms based on inherent statistical properties have the advantage that they do not need to find a representative training set; moreover, they often let us estimate an embedded message's length [8]. However, each steganographic system requires its own detection algorithm. Class discrimination, on the other hand, is universal even though it doesn't provide an estimate of the hidden message's length, and creating a representative training set is often difficult [8]. A feature vector can help detect several steganographic systems, once we get a good training set. It remains to be seen if new steganographic systems can circumvent detection using class discrimination [8].Various steganography methods as well as many steganalysis methods are compared to get into the depth that how message can be concealed in image with maximum imperceptibility. Security can be maximized by studying the methods of breaching security.

4.4 Principles of Model-based Steganography

Model-based steganography was first introduced in 2003 [21]. The aim of Model-based steganography is in characterizing some statistical properties of the cover message in order to embed the secret message without altering these properties. The outline of Model-based steganography is described in the following [21]: A cover message, represented as a random variable X, is split into two parts, X_a that remain unaltered during the embedding, and X_b, that is modified to carry the embedded message. X_a is selected so as to preserve the relevant characteristics of the cover, whereas Xb can be modified without altering the perceptual and statistical characteristics of the cover message [21]. By modeling the cover message class X according to a probability distribution $\overline{P_X}$ (x) it is possible to calculate the conditioned probability distribution $\overline{P}_{X_b|X_a}(x_b|x_a)$.The embedded message is assumed to be a uniform random stream of bits, which is in fact the same distribution

shown by encrypted messages. The embedding outline is shown in Figure 2 below. The cover message x is split into xa and xb, then the embedded message is processed by an entropy decoder according to the conditioned probability distribution PXb|Xa(xb|xa). The output of the decoder is denoted by x′b and replaces xb to form together with xa the stego message x′ [21]. The extraction outline is shown in Figure 3 below. Its structure is very similar to the embedding scheme: the main difference consists in the replacement of the entropy decoder by an entropy encoder [21]. The stego message x′ is separated in xa and x′b. The conditioned probability distribution P Xb|Xa (x′b |xa) is calculated, then the entropy encoder process x′b according to the model distribution. The encoder the output is the embedded message [21]. Based on this principle a novel technique "Peak-Shaped-Based Steganographic Technique for JPEG Images" is proposed [27].To test the validity of proposed technique, PSB is compared to the original Model-based steganography (MB1 and MB2, described in [21]). PSB embedding capacity, is the smallest among the techniques because of PSB unitary coefficients exclusion PSB achieves slightly higher PSNR with respect to MB1 and MB2 (0.5dB higher); moreover PSNR is adequate to ignore the visual degradation introduced by the three techniques. The degradation introduced by MB2 blockiness compensation is negligible [27]. By comparing the embedding impact to the error probability and PSNR it results that the embedding impact has a minor relevance with respect to the selection of the modifiable coefficients. In fact, PSB outperforms MB1 in error probability and gets similar PSNR with a larger embedding impact [27].These superior performances are achieved by taking into account discrepancy and quantization matrix in order to select the modifiable coefficients set. MB2 modifies additional coefficients to preserve a superior-order statistical measure, but the additional coefficients to be replaced are not selected carefully, getting the worst performances [27]. PSB novelty is in a more accurate coefficient selection, taking into account quantization and coefficient relevancy. A novel block measure, named discrepancy, is introduced to describe how much a block is suitable to embed a message. PSB model derives from heuristic hypothesis about histogram shape, moreover the model depends on the stegokey, and therefore an attacker cannot calculate exactly the model.

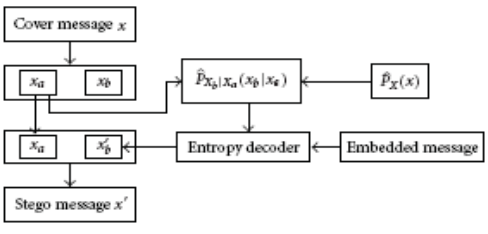


Fig. 2 Model based embedding scheme by Sallee [21]

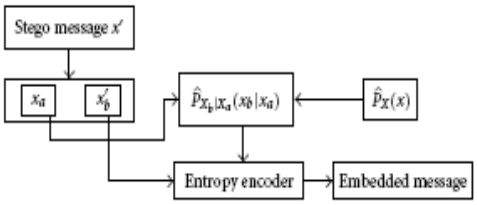


Fig. 3 Model based extraction scheme by Sallee [21]

4.5 Milestones for Adaptive steganography

The model-based technique, proposed by Sallee, tries to model statistical properties of an image and preserves them during embedding process. Sallee breaks down transformed image coefficients into two parts and replaces the perceptually insignificant component with the coded message bits [21]. Initially, the marginal statistics of quantized (nonzero) ac DCT coefficients are modeled with a parametric density function. For this, a low-precision histogram of each frequency channel is obtained, and the model is fit to each histogram by determining the corresponding model parameters [21]. Sallee defines the offset value of a coefficient within a histogram bin as a symbol and computes the corresponding symbol probabilities from the relative frequencies of symbols (offset values of coefficients in all histogram bins) [21].At the heart of the embedding operation is a non adaptive arithmetic decoder that takes as input the message signal and decodes it with respect to measured symbol probabilities. Then the entropy decoded message is embedded by specifying new bin offsets for each coefficient. In other words, the coefficients in each histogram bin are modified with respect to embedding rule, while the global histogram and symbol probabilities are preserved [21]. Extraction, on the other hand, is similar to embedding. That is, model parameters are determined to measure symbol probabilities and to obtain the embedded symbol sequence (decoded message) (Note that the obtained model parameters and the symbol probabilities are the same both at the embedder and detector). The embedded message is extracted by entropy encoding the symbol sequence. The model-based technique does not recompress the image before embedding. Therefore, a comparison of recompressed and stego images does not apply in this case [21].

Other than quality factor, image properties such as image texture could be used to categorize the images. There are many approaches to quantify the texture of an image. A crude measure of image texture would be the mean variance of JPEG blocks [28]. This measure is simple and can be efficiently computed, even with large data set. To examine the effect of image texture on steganalysis, the mean block variance of the images in dataset is calculated. The variance is observed to change from 0 to 11,600. Using the mean of the available range, the cover image set was divided into two categories—of high and low variance. Each cover image set was then used to obtain a stego data set,

using the model based embedding technique, with different message lengths [28].It is observed that the performance of the classifier is affected by the variance of the images being used. More specifically, the classifier performs less accurately when confronted with high-variance images i.e., highly textured or noisy as expected [28, 29]. It is characterized by a random adaptive selection of pixels depending on the cover image and the selection of pixels in a block with large local STD (standard deviation). The latter is meant to avoid areas of uniform color (smooth areas). This behavior makes adaptive steganography seek images with existing or deliberately added noise and images that demonstrate color complexity [19].

The main aim of steganography is to avoid detection to an undesirable user. So it is quite appealing to understand up to some extent about the detection scheme of statistics of various orders. Hany Farid [30] proposed such a model for higher order statistics. According to him, the detection scheme can be separated in two parts. In the first part extracts a set of statistics, called the feature vector, for each investigated image [30]. In the second part a classification algorithm is used to separate original images from stego images by means of their feature vectors. Messages can be embedded into digital images in ways that are imperceptible to the human eye, and yet, these manipulations can significantly alter the underlying statistics of an image. To detect the presence of hidden messages a model based on higher-order statistics taken from a multi-scale decomposition has been employed [30]. This model includes basic coefficient statistics as well as error statistics from an optimal linear predictor of coefficient magnitude. These higher order statistics appear to capture certain properties of "natural" images, and more importantly, these statistics are significantly altered when a message is embedded within an image [30]. This makes it possible to detect, with a reasonable degree of accuracy, the presence of hidden messages in digital images. To avoid detection, of course, one need only embed a small enough message that does not significantly disturb the image statistics. [30].

The method proposed by Roman et al using higher-order statistics gave very interesting insights into both JSTEG (Jsteg is a publicly available steganographic tool written by Derek Upham [33]) & HPDM (A basically new steganographic embedding algorithm based on histogram-preserving data mapping (HPDM) has been presented by Eggers [32] Their approach is based on Cachin's definition of security in steganographic algorithms.[31]) Based on these insights we were able to modify HPDM to obtain a steganographic algorithm being perfectly secure with respect to Farid's detection method [29].

Wayner [34] dedicated a complete chapter in a book to what he called ''life in noise'', pointing to the usefulness of data embedding in noise. It is proven to be robust with respect to compression, cropping and image processing. Amin Milani Fard et al. in [7] proposed a GA based algorithm for secure steganography in jpeg images. This method optimizes localization in which the message is to be embedded on the cover image. Also it is supposed to defeat almost all known steganalysis methods. The model-based method (MB1), described in [21], generates a stego-image based on a given distribution model, using a generalized Cauchy distribution, that results in the minimum distortion. Due to the lack of a perfect model, this steganographic algorithm can be broken using the first-order statistics [35]. Moreover, it can also be detected by the difference of ''blockiness'' between a stego-image and its estimated image reliably [41]. The discovery of ''blockiness'' led the author in [21] to produce an enhanced version called MB2, a model-based with de-blocking. Unfortunately, even MB2 can be attacked. Ullerich and Westfeld [37] successfully attacked MB2 using coefficient types that are derived from the blockiness adjustment of MB2. They adapt Sallee's Cauchy model itself to detect Cauchy model-based embedded messages [37].In [38], Chen and Shi, attacked MB2 and other JPEG-based algorithms using Markov process (MP) that exploits the intra-block and inter-block correlations among JPEG coefficients.

In [39] another novel steganographic method to hide data in spatial domain of images imperceptibly is drawn. It was based on the human visual system sensitivity to image contrast change. It uses the concept that the pixels in edge areas may tolerate larger changes without making perceptible distortion. The number of bits to be embedded for each pixel is variable and determined by the correlation between neighboring pixels [39]. This method does not replace the LSBs of pixel value directly, but changes the pixel value into another similar value. The range of changeable pixel value in smooth areas is small and in edge areas is large, so that the stego-image still maintains good perceptual quality. Also, the embedded secret data can be extracted from the stego-image without referencing the original image [39]. This steganographic method provides a large embedding capacity with little perceptual distortion. Also this method performs better than conventional LSBs substitution method in both visual effect and security. [39]

Edge embedding follows edge segment locations of objects in the host gray scale image in a fixed block fashion each of which has its centre on an edge pixel. According to Whilst simple, this method is robust to many attacks and it follows that this adaptive method is also an excellent means of hiding data while maintaining a good perceptibility [19]. In [40] dithering based steganography is used by modifying the dithering criteria to produce a novel algorithm but it has still certain limitation which needs to be considered in future.

In [35] a technique for breaking cauchy's model based steganography has been proposed. Results show a good detection ratio for a large test set of typical JPEG images. The attack is successful because of

weaknesses in the model and does not put into question the theoretical framework of model-based steganography.

Plus minus 1 (PM1) [43] is an improved method which not only foils typical attacks against LSB-based techniques, but also provides high capacity but the method to apply it on jpeg image was not clear so in [41] genetic algorithm (GA) based PM1 algorithm has been proposed in which the GA is used to optimize the performance, such as minimizing blockiness. Theoretical analysis to the histogram characteristics is done which proves that PM1 used in JPEG images preserves the first-order statistical properties. This method outperforms the other methods in terms of capacity and security [41]

Chin-Chen et al. [42], propose an adaptive technique applied to the LSB substitution method. Their idea is to exploit the correlation between neighboring pixels to estimate the degree of smoothness. They discuss the choices of having 2–4 sided matches. The payload (embedding capacity) was high. A range of distance thresholds has been selected. Larger the threshold more sub clusters will be there with large sizes smaller the threshold most of the sub clusters will be of small size so smaller capacity [42]. But large threshold may distort the image sometimes. So choosing the appropriate threshold values can solve the tradeoff between capacity & quality [42].

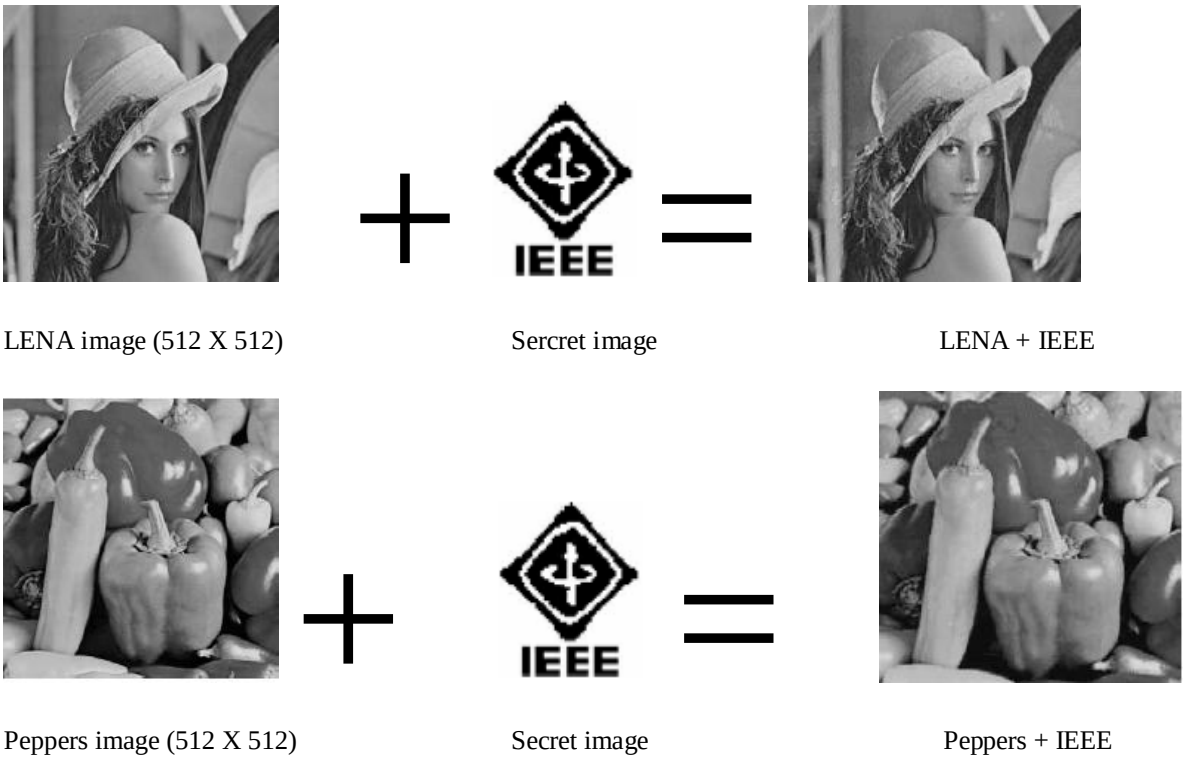


Fig. 4 Result of Chin-Chen et al. [42] method hiding secret IEEE image

Hioki [44], presented an adaptive method termed ‘‘A Block Complexity based Data Embedding’’ (ABCDE). ABCDE works in a very similar method as BPCS, but employs a more sophisticated complexity metric. BPCS merely counts the number of bit-flips in each row and column of a given tile, with the assumption that a large number of bit flips indicate a lack of structure [44]. The two new complexity measures: the run-length irregularity β and the border noisiness γ are used in ABCDE to properly identify complex blocks in noisy regions. Here one can properly reject blocks those have regular periodical pattern or those on the boundary of a noisy region and an informative region by the two complexity measures β and γ [44]. Also threshold values for the two complex measures can be specified independently for each bit-plane. This enables to keep the image quality high and to make the embedding capacity large at the same time. The results shown in the images below in fig 5 & fig 6 are particularly impressive. Despite the watermarked image having more than 60% of its image data overwritten, the differences between it and the original image are nearly imperceptible. [44] The ABCDE method introduced a large embedding capacity; however, certain control parameters had to be configured manually, e.g., finding an appropriate section length for sectioning a stream of resource blocks and finding the threshold value that controls identification of complex blocks. These requirements

render the method unsuitable for automatic processes. [44]

Table 1 MSE & PSNR for various images after applying ABCDE [44]

S.no	Name of image	MSE	PSNR
1	Madrill.jpg	0.1144	24.2714
2	Lena.jpg	0.0781	25.9289
3	Fruits.jpg	0.0701	26.3985

Before ABCDE After ABCDE

Fig 5 Mandrill image before & after applying ABCDE algorithm [44]

Fig. 6 Fruits image after applying ABCDE [44]

Fig. 7 Lena image after applying ABCDE [44]

There are two vague issues which are obscurely discussed at the end of Hioki's work. One arises when the carrier image's dimensions are not proportional to the block division scheme and so fragments from these dimensions are kept away from the embedding process. There was no indication by the author of the possible impact of this decision as it might leave a clear contrast between the modified and the intact parts of the image which distorts its statistical properties. The second point is the introduction of the zero padding when the compressed resource file size is not a multiple of the block size. The author did not show any explanation on how to generate complexity from such a compressed file since there will be a sequence of zeros resulting from the ''0'' padding notion. The author in the experimental section does not show how resilient the algorithm is to different image processing attacks, e.g., rotation, additive noise, cropping, and compression. Indeed, the ABCDE algorithm provides an improvement over a former method known as BPCS (bit plane complexity segmentation) [45].This research proposes a method of embedding secret data into a DWT transformed image using the previously described BPCS. The coefficients of the DWT have many image-like properties, and BPCS is ideal for exploiting them. The main properties leveraged for BPCS are [45]:

1) Correspondence: Spacial areas in each section of the coefficients' sub bands correspond directly to areas in the original image.

2) Complexity: The bit planes at corresponding significance levels of the wavelet coefficients and the original image are usually proportionally complex.

3) Resilience: Changes in the values of the wavelet coefficients do not create disproportionately large changes in the reconstructed image.

Since this system embeds into the wavelet coefficients, the subsequent encoder is not important, as long as it is lossless. EZW was chosen for its ease of implementation and relatively good encoding efficiency. This opens the way for application of this system to many of today's best wavelet based image CODECs, as well as future ones. This will create a system that will allow many more people access to the benefits of BPCS steganography without sacrificing the use of a cutting edge image compression system [45].

Fridrich, J [46] explored the strength of data hiding in digital imagery as a new and powerful technology with applications including robust digital watermarking of images for copyright protection, image fingerprinting, authentication and tamper detection etc. He stated that BPCS steganography was introduced to overcome the disadvantages of LSB steganography [46].

Table 2 Results for BPCS using EZW encoded images [45]

S.no	Planes for embedding	Planes used	Complexity threshold	Embedded data (bytes)	Compressed (bytes)	PSNR (db)
1	8	3	6	5104	24219	31.6
2	8	3	4	7216	26599	30.3
3	9	4	6	12442	47791	33.0
4	9	4	4	16750	52073	31.5

As we know that Medical records of patients are extremely sensitive information, needing uncompromising security during both storage and transmission. In addition, these records often have to be traceable to patient medical data such as X-ray or scan (CAT, MRI etc.) images. For this purpose in [47] an improved version of a high capacity data hiding scheme, called Bit-Plane Complexity Segmentation (BPCS) steganography, is explained, and its effectiveness in hiding medical records in color cervical images is demonstrated. The merits of BPCS-Steganography found by the experiments are as follows [48]:

1. The information hiding capacity of a true color image is around 50%.
2. A sharpening operation on the dummy image increases the embedding capacity quite a bit.
3. Canonical Gray coded bit planes are more suitable for BPCS-Steganography than the standard binary bit planes.
4. Randomization of the secret data by a compression operation makes the embedded data more intangible.
5. Customization of a BPCS-Steganography program for each user is easy. It further protects against eavesdropping on the embedded information.

It defines the image complexity α by the following [48]. $\alpha = \frac{k}{\text{The maximum possible B - W changes in the image}}$ (A)

Where, k is the total length of black-and-white border in the image. So, the value ranges over

$$0 \leq \alpha \leq 1 \quad \text{(B)}$$

(A) is defined globally, i.e., α is calculated over the whole image area [48]. It gives us the global complexity of a binary image. However, one can also use α for a local image complexity (e.g., an 8 × 8 pixel-size area). But the computational complexity of the algorithm to find a phase key that passes the threshold is time consuming and there is no guarantee that it will always evolve into an optimal solution [47].

BPCS steganography is not robust to even small changes in the image [48]; this intolerance to any manipulation of the stego-image is perceived by the authors in [48] as a merit. This can be viewed as a good thing in applications where an unknowing user might acquire an embedded image. Any alteration, such as clipping, sharpening or lossy compression, would "destroy the evidence" and make it unusable for later extraction. Extracting the embedded information requires a deliberate attempt by a knowledgeable user on an unaltered image. The lack of robustness also ties in to the fact that a malicious user cannot alter the embedded data without knowledge of the customization parameters but this is not true in case of every application because high robustness is basic parameter for good steganography and this weakness is inherited by the ABCDE algorithm also since its underlying framework is based on BPCS [19].This is definitely not shown in Kawaguchi's argument [48]. Their algorithm would fail to retrieve the embedded data in two cases: first when the stego-image is attacked resulting in the destruction of the embedded data, and second when an image is plain clear (meaning that no embedding process took place). These two contradictory justifications, due primarily to lack of robustness, would not be appealing characteristics to forensics experts or other interested bodies.

In [49], the authors chose to use wavelet transforms that map integers to integers instead of using the conventional wavelet Transforms. It embeds the secret data in low and mid frequency regions of image which have large energies. This can overcome the difficulty of floating point conversion that occurs after embedding [49]. Their scheme embeds the payload in non overlapping 4*4 blocks of the low frequency, where two pixels at a time are chosen one on either side of the principal diagonal. Cover image adjustment was required to prevent the problem of under/over flow of pixel values after embedding. Tests for the similarity between the condition number of the cover image and the stego image are done for further embedding. They also perform cover image adjustment before embedding the payload in order to ensure lossless recovery [49]. Embedding done in the low frequency bands ensures robustness against attacks such as compression and filtering. Experimental results show better trade off between Visual perceptivity and capacity compared to the existing algorithms [49].For a true color image format, they apply the algorithm on each color plane separately. This step ignores the high correlation between color planes in natural images. Not taking this phenomenon into consideration means the embedding scenario will corrupt some of the inherited statistics of the cover image, a trap that severely exposes the stego-image to steganalysis attacks [49]. The authors also state some assumptions; first, embedding is carried out only on non-singular matrices, also +/-15 is imperceptible to human vision; finally ,the cover image and payload are assumed to be JPEG and the cover be a square matrix of size 51x512. The

second assertion is doubtful however. Even though this can be possibly acceptable from a human visual perspective, however, from a statistical point of view, this amount of change is intolerable. Before they conclude, they state that their cover image and stego-image version are similar, even though the best candidate in their experiments has a PSNR that did not exceed 45 [49].

In [50], the authors attempt to create a method to restore the marked image to its pristine state after extracting the embedded data. They achieve this by applying the pick point of a histogram in the difference image to generate an inverse transformation in the spatial domain. Here author observed the characteristic of an image carefully & discovered that in terms of an image, there is a large probability that adjacent pixels in an image have similar pixel values. From this observation, they concluded that the difference between two adjacent pixels in an image can be a value in its difference image The cover image is divided into non-overlapping 4*4 blocks where a difference matrix of size3*4 is generated for each block. The selection of the local histogram's peak point pb will direct the embedding process and matrix manipulation [50]. The example shown in their hiding phase section might not be sufficient to verify the accuracy of the algorithm. As hiding algorithm is based on a multilevel concept, the algorithm can be performed repeatedly to convey a large amount of embedded messages [50]. By combining the peak point of a difference image concept with a multilevel hiding strategy, the proposed hiding scheme not only hides a large amount of embedded messages but also achieves reversibility. Certainly, it is hard to maintain a balance between hiding capacity and image distortion in marked images. But experimental results confirm that proposed multilevel reversible data hiding scheme can provide higher hiding capacity while keeping distortion low [50]. Even when proposed hiding algorithm is performed for nine rounds, the average PSNR is still higher than 30 dB and the average hiding capacity still can reach 1.3 bpp. Performance comparisons with existing reversible schemes further demonstrate the effectiveness of the proposed scheme [50].

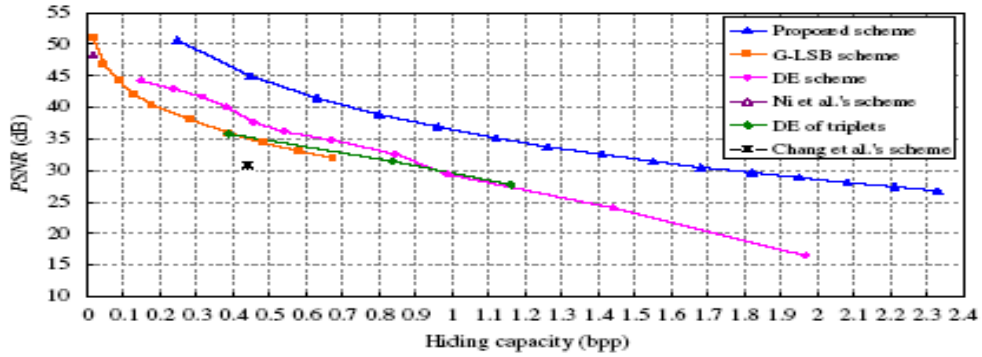


Fig 8 Graph representing the PSNR & hiding capacity with other well known techniques [50]

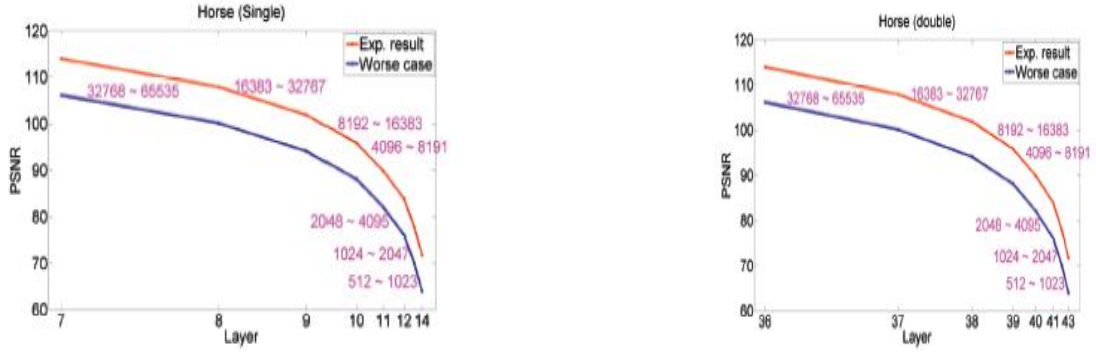
The authors in [19] pointed out that some questions remain unanswered in [50] such as what happens when we have two peak points instead of one? On which criterion will we base our selection? Another issue occurs when transforming the matrix SD_b to RD_b; it is highly likely that after the subtraction process we will have some values that collude with the peak value which confuses the extraction of the embedded data. To prevent over/underflow, caused by the arithmetic operations on values close to boundaries (i.e.0, 255), the authors use the modulus operator (i.e. mod 256). There was no adequate explanation on the effect of homogeneous, dark, bright, and edged blocks on the algorithm efficiency [19].

In [51], a GA-based algorithm is presented which generates a stego-image to break the detection of the spatial domain and the frequency-domain steganalysis systems by artificially counterfeiting statistical features. A new concept of developing a robust steganographic system by artificially counterfeiting statistic features instead of the traditional strategy by avoiding the change of statistic features is proposed [51]. They apply genetic algorithm based methodology by adjusting gray values of a cover-image while creating the desired statistic features to generate the stego images that can break the inspection of steganalytic systems Again authors in [19] mentioned that time complexity, which is usually the drawback of genetic based algorithms, was not discussed though. They mentioned that ''the process is repeated until a predefined condition is satisfied or a constant number of iterations are reached. The pre defined condition is the situation when we can correctly extract the desired hidden message.'' Again, it was not stated whether the process of determining such a condition was done automatically or involved a human inference (visual perception).The suggested GA-based rounding-error correction algorithm, whilst interesting, still needs proof of generalization [19].

Wu and Shih [51] closed their introduction section by saying, ''this is the first paper of utilizing the evolutionary algorithms in the field of steganographic systems ''.It should be noted that image hiding using genetic algorithm was known prior to their work such as the work in [52]. It attempts to use GA for finding out values of parameters, namely reference amplitude (A) and modulation index (μ) both with linear and non linear transformation functions, for achieving the

optimal data imperceptibility. Results on security for the embedded data and robustness against linear, non linear filtering, noise addition, and lossy compression are reported here for some benchmark images [52]. Still robustness performance against various types of distortions in stego images along with higher embedding rate can be achieved. In [41], the authors proposed extending the conventional [47] algorithm to JPEG images using genetic algorithm. This is done because there was no reference in literature that how to use PM1 steganography in jpeg images. GA is used to optimize the performance, such as minimizing blockiness. Theoretical analysis to the histogram proves that PM1 used in JPEG images preserves the first-order statistical properties. Experiments show that the proposed method outperforms the other methods in terms of capacity and security [41].

Kong et al [53] proposed a content-based image embedding based on segmenting homogenous grayscale areas using water shed method coupled with Fuzzy C-Means (FCM).Entropy was then calculated for each region. Entropy values dictated the embedding strength where four LSBs of each of the cover's RGB primaries were used if it exceeded a specific threshold otherwise only two LSBs for each were used [53]. This method can overcome the disadvantage of block-based steganographic techniques. Experimental results show that the security and performance of the proposed scheme are high. The drawback of this method was its sensitivity to intensity changes which would affect severely the extraction of the correct secret bits. As a side note, Kong et al [53] also reported the use of a logistic map to encrypt the secret bit stream which seems venerable to a Chosen-plain text attack (CPA). Chao et al. [54] presented a 3D steganography scheme. The embedding scheme hides secret messages in the vertices of3D polygon models as shown in following fig. It has been shown that that PSNR rates exponentially decrease with the number of layers. The PSNR decreases sharply when the number of layers is larger than 10.It is also shown that difference between the stego and the cover models is imperceptible even for the worst embedding case [54] as shown in following graph (fig 9). Also the outline of embedding & extraction process of algorithm is shown in fig 10.



(a) (b)

Fig. 9 Relation between number of layers & PSNR for (a) single precision format (b) double precision format [54].

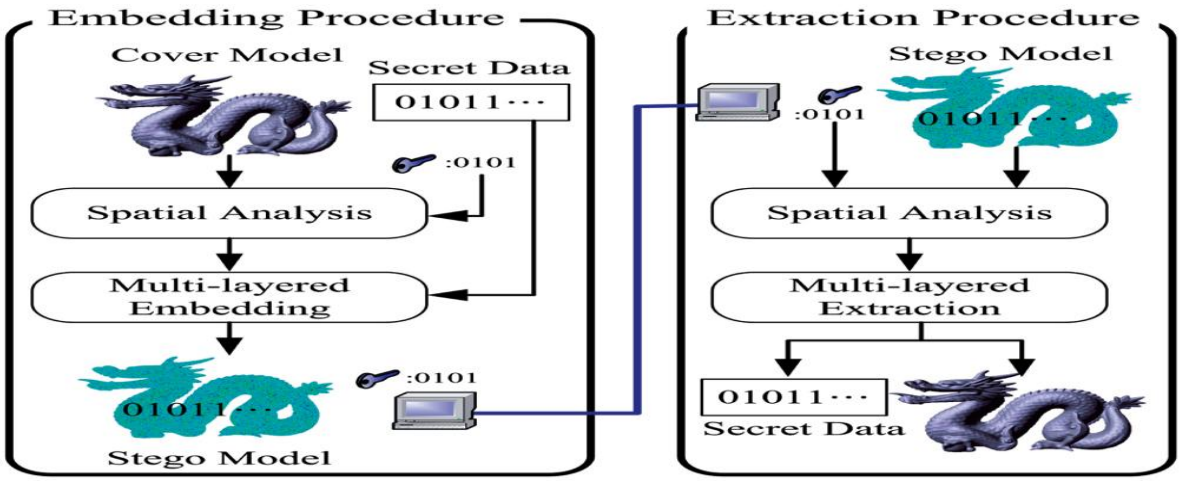


Fig. 10 Insertion & extraction procedure for 3D Steganography scheme [54]

The experimental results showed that the proposed method [54] can provide much higher capacity than previous approaches. The proposed approach has the following limitations. Perfectly smooth (i.e., sphere) or extremely small-size models are not suitable for selection as cover models because the hidden data might be easily observed after even a very small modification by any embedding method [19]. Utilizing

PCA to determine the vertex traverse list may potentially hinder the robustness of the proposed method. Although the end vertices and initial triangle obtained from cover and stego models are identical in all cases in the experiments, we cannot guarantee that both are always exactly identical [19] .One simple solution is to simply project vertices on the x; y; and z-axes. However, this approach cannot withstand similarity transformations. A better approach for determining vertex traverse list is required in the future. Another limitation is that this approach cannot withstand certain malicious attacks such as smoothing, additional noise, non uniform scaling, simplification, and vertices resampling [19]. As a result, the proposed approach is not suitable for the applications of digital content protection and authentication .Similarly, Bogomjakov et al [55], hide a message in the indexed representation of a mesh by permuting the order in which faces and vertices are stored. The permutation is relative to a reference ordering that encoder and decoder derive from the mesh connectivity in a consistent manner. This method is distortion-free because it does not modify the geometry of the mesh [55]. Compared to previous steganographic methods for polygonal meshes the capacity is up to an order of magnitude better. This steganography algorithm is universal and can be used instead of the standard permutation steganography algorithm on arbitrary datasets. The standard permutation algorithms runs in $\Omega(n^2 \log^2 n \log\log n)$ time and achieves optimal O (nlogn) bit capacity on datasets with n elements. In contrast, this algorithm runs in O (n) time, achieves a capacity that is only one bit per element less than optimal, and is extremely simple to implement [55]. Although, such methods claim higher embed- ding capacity, however time complexity to generate the mesh and then rendering can be an issue.Moreover3D graphics are not that portable compared to digital images. Nakamura and Zhao [56], propose a morphing process that takes as input the secret image and the cover file. Earlier also authors also proposed a technique for information hiding based on image morphing. Since the cover message can be changed after embedding the secret message, the cover rate of the technique was much larger than that of existing techniques [56]. However, this technique has two fatal problems. First, the stegodata may not look natural due to inaccurate definition of the feature lines. Second, the secret image might be estimated to some extent from the stegodata. To overcome these disadvantages they propose several methods. First, to make the stegodata more natural, they propose to scale down the secret message before calculating the stegodata [56]. To solve the second problem, they propose to encrypt the secret message first, and then hide it into the warped cover image [56]. To increase the security further, they also propose to separate the stego key and the secret message. On the negative side the method does not discuss the generated features from the cover and secret images used for morphing and how to regenerate them from the stego-image. Zeki and Azizah [57] proposed what they termed as ‘‘the intermediate significant bit algorithm’ They studied different ranges of an 8bit image and found the best compromise for distortion and robustness was in the following range:[0:15] [16:31]…. y …[224:239] [240:255]. The core idea in the embedding process is to find the nearest range that matches the secret bit in the next or previous range [57]. Also the various planes of a digital image used by Zeki et al. are shown in fig 11.

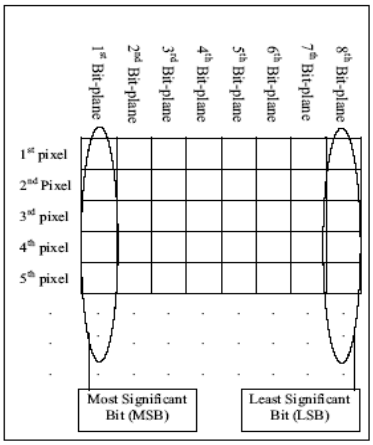


Fig. 11 Various bit planes of digital images [57]

To verify the robustness of the proposed method normalized cross correlation NCC will be used for this purpose. It is found that the best normalized cross correlation was in 4th bit-plane [57]. This study tested the location of the watermark pixel according to the range of each bit-plane, so if the watermarked pixel is in the middle of the range then any effect on the pixel by attacks will be difficult to move the selected bit to another range [57]. While if the pixel value is located in the edges of ranges, any small change by attacks will move the pixel from a range to another, and the watermark cannot be extracted [57]. But the robustness of the proposed method has not been improved against geometry transform attacks which do not change the value of the pixel but they transform the pixel to another location. To solve this problem repeating the watermark embedded in a special form may be done for this purpose.

In this way various authors have proposed different steganography techniques based on certain mathematical model. From the above discussion we can see that model based steganography has given a new direction for secret communication but adaptive steganography is still in its infancy & needs a lot of new methods are awaited to come.

V. CONCLUSION

From the analysis of various adaptive steganography algorithms it can be seen that as these methods are based upon the certain statistics of cover image so these are less prone to attacks as compared to earlier methods which were only based upon spatial or

frequency domain without considering any features or statistics of the image .Besides these methods give good embedding capacity with good embedding efficiency as compared to two principle domains [21] taking care of statistics of image. We cannot isolate these methods from spatial or frequency domain methods because finally the implementation of steganography algorithm will be done either in spatial domain or frequency domain (using DCT or DWT) but only addition is the care of image characteristics or statistics before embedding the secret data. In other words we can say that adaptive steganography has provided an additional layer above & common to both spatial domain & frequency domain techniques as shown in fig 12.

ADAPTIVE STEGANOGRAPHY MODEL	
Spatial Domain Steganography Techniques	Frequency Domain Steganography Techniques

Fig. 12 Conceptual model of Adaptive steganography

Though model based steganography has provided an additional security layer but still we cannot say that it has provided 100% relief from forgery. Still we should remember certain points while hiding the data that secret message should be firstly encrypted before hiding because no steganography algorithm is 100% secure so at least this encryption will provide a security layer [69, 70]. Secondly only a limited number of bits should be inserted so that no or less visual degradation is present in the image which cannot be easily judged. Finally always try to choose the noisy areas for embedding instead of homogeneous areas as guided by Wayner in a book as "life in noise" [34, 71]. In the survey we have seen that every adaptive steganography technique has its own pros & cons so still we are long way away from perfect steganography. But adaptive steganography has opened a new away towards secure steganography that is firstly analyze the characteristics & important features of cover image in terms of its statistics followed by development of a mathematical model & only then embed the secret message according to developed model so that the distortion & artifacts present in the image are minimum. So it is concluded that adaptive steganography is right way towards secure steganography but the trade-off between the various mathematical models is still on. We are still in dilemma that whether steganography model should provide more imperceptibility or more capacity. Robustness parameter is also a requirement of steganographic algorithm as said by .Katzenbeisser [58] or it is a requirement only of watermarking techniques as said by Cox [59, 60]. In fact there is no end for trade off between three basis parameters of steganography that is capacity, imperceptibility & robustness. But still we need a lot of research dedicated to adaptive steganography so that we can get closer to the model which can narrow down the bridges between these three basic parameters & can provide maximum security for communication over untrusted media like internet.

REFERENCES

[1] Kefa Rabah, Department of Physics, Eastern Mediterranean University, Gazimagusa, North Cyprus, Turkey, "Steganography-The Art of Hiding Data", Information Technology Journal 3 (3): 245-269, 2004,ISSN 1682-6027

[2] Kevin Curran, Internet Technologies Research Group, University of Ulster, Karen Bailey, Institute of Technology, Letterkenny, Ireland, "An Evaluation of Image Based Steganography Methods", International Journal of Digital Evidence Fall 2003,Volume2,Issue 2

[3] Petitcolas, F.A.B., 1997,The information hiding homepage-digital watermarking and steganography http://www.cl.cam.ac.uk/ fapp2/steganography,University of Cambridge, Computer Laboratory, Security Group.

[4] Sabu M Thampi,Assistant Professor ,Department of Computer Science & Engineering, LBS College of Engineering, Kasaragod, Kerala-671542, S.India "Information Hiding Techniques: A Tutorial Review", ISTE-STTP on Network Security & Cryptography, LBSCE 2004.

[5] X.Li,J.Wang ,"A steganographic method based upon JPEG and particle swarm optimization algorithm", Information Sciences 177 (15) (2007) 3099–3109.

[6] C.C.Chang, T.S.Chen ,L.Z.Chung ,"A steganographic method based upon JPEG and quantization table modification", InformationSciences 141(1–2)(2002)123–138.

[7] A.M.Fard ,M.Akbarzadeh- T,F.Varasteh-A, "A new genetic algorithm approach for secure JPEG steganography",in: Proceedings of IEEE International Conference on Engineering of Intelligent Systems, 22–23 April2006, pp.1–6.

[8] N.Provos, P.Honeyman, "Hide and seek: an introduction to steganography" ,IEEE Security and Privacy1(3)(2003)32–44.

[9] A.Westfeld, "F5-A steganographic algorithm:high capacity despite better steganalysis" ,in: Proceedings of Fourth International Workshop on Information Hiding, Lecture Notes in Computer Science, vol. 2137,Pittsburgh, USA, April 2001 pp.289–302.

[10] http://en.wikipedia.org/wiki/Steganography

[11] W.Y.Chen, "Color image steganography scheme using set partitioning in hierarchical trees coding, digital Fourier transform and adaptive phase modulation", Applied Mathematics and Computation 185(1)(2007)432–448.

[12] N.K.Abdulaziz, K.K.Pang, "Robust data hiding for images", in Proceedings of IEEE International Conference on Communication Technology, WCC-ICCT'02, vol.1,21–25 August 2000 ,pp.380–383.

[13] L.D. Paulson, "New system fights steganography" News Briefs, IEEE Computer Society 39(8) (2006)25–27.

[14] P.Wayner, "Disappearing Cryptography", seconded, Morgan Kaufmann Publishers, 2002.
[15] C.Manikopoulos, S.Yun-Qing, S.Sui, Z.Zheng, N.Zhicheng, Z.Dekun, "Detection of block DCT-based steganography in gray-scale images", in:Proceedings of the IEEE Workshop on Multimedia Signal Processing, 9–11December2002,pp.355–358.
[16] N.Provos, Defending against statistical steganalysis ", Center for Information Technology Integration, University ofMichigan, Technical report,February2001.
[17] N.Provos, P.Honeyman, "Detecting steganographic content on the Internet", Center for Information Technology Integration, University of Michigan, Technical report, August31, 2001.
[18] J.Fridrich, M.Goljan, D.Hogeg, "Steganalysis of JPEG images: breaking the F5 algorithm", in: Proceedings of Information Hiding: Fifth International Workshop, IH 2002 Noordwijkerhout, The Netherlands, Lecture Notes in Computer Science, Springer, October 7–9, 2002, 2578/2003, pp.310–323.
[19] Abbas Cheddad , Joan Condell, Kevin Curran, Paul McKevitt "Digital image steganography: Survey and analysis of current methods" in the journal of Signal processing, Aug 2009.
[20] N.F.Johnson ,S.C. Katzenbeisser, "A survey of steganographic techniques" in: S. Katzenbeisser, F.A.P.Petitcolas (Eds.),Information Hiding Techniques for Steganography and Digital Watermarking,Artech ouse,Inc.,Norwood,2000.
[21] P.Sallee, "Model-based steganography",in: Proceedings of the Second International Workshop on Digital Watermarking, Seoul, Korea, October 20–22,2003,Lecture Notes in Computer Science,vol.2939,pp. 254–260.
[22] N.F.Johnson, S.Jajodia, "Exploring steganography: seeing the unseen", IEEE Computer31 (2) (1998)26–34.
[23] T.L.Thomas,"Alqaeda and the internet: the danger of' cyber planning'', parametrs, US Army War College Quarterly-Spring 2003. Available from:/www.carlislearmy.mil/ usawc / Parameters/03spring/thomas.pdfS.
[24] C.Hosmer, "Discovering hidden evidence", Journal of Digital Forensic Practice (1)(2006)47–56.
[25] W. Bender et al., "Techniques for Data Hiding," IBM Systems J., Vol. 35, Nos. 3 and 4, 1996, pp. 313-336.
[26] I.J. Cox et al., "Secure Spread Spectrum Watermarking for Multimedia" Tech.Report 95-10, NEC Research Inst., Princeton, N.J., 1995.
[27] Lorenzo Rossi, Fabio Garzia, and Roberto Cusani "Peak-Shaped-Based Steganographic Technique for JPEG Images" EURASIP Journal on Information Security Volume 2009, Article ID 382310, 8 pages doi:10.1155/2009/382310
[28] M. Kharrazi, H.T. Sencar, N. Memon, "Performance study of common image steganography and steganalysis techniques", Journal of Electrical Imaging 15 (4) (2006) 1–16.
[29] R. Tzschoppe, R. Baum, J. Huber, A. Kaup, "Steganographic system based on higher-order statistics" , in: Proceedings of SPIE, Security and Watermarking of Multimedia Contents V. Santa Clara, California,USA2003,vol.5020,p.156-166.
[30] H. Farid "Detecting hidden messages using higher-order statistical models",in ICIP 2002, Rochester, NewYork,SA, September 2002.
[31] C. Cachin, "An information-theoretic model for steganography," in Proceedings of 2nd Workshop on Information Hiding, D. Aucsmith, ed., 1525, Lecture Notes in Computer Science, Springer-Verlag, (Portland, Oregon, USA), May 1998.
[32] J. J. Eggers, R. B Äauml, and B. Girod, "A communications approach to image steganography," in Proc. Of SPIE Vol. 4675, Security and Watermarking of Multimedia Contents IV, (San Jose, Ca, USA), January 2002.
[33] xhttp://munitions.iglu.cjb.net/software/steganography/jpeg-jsteg-v4.diff.gz
[34] P. Wayner, "Disappearing Cryptography", second ed, Morgan Kaufmann Publishers, 2002.
[35] R.Bohme, A.Westfeld, "Breaking Cauchy model-based JPEG steganography with first order statistics" , in: Proceedings of the European Symposium on Research in Computer security, ESORICS 2004, Valbonne, France, 13thSeptember 2004, Lecture Notes in Computer Science,vol.3193,pp.125–140.
[36] J.Fridrich, M.Goljan, "Practical steganalysis of digital images- state of the art",in: Proceedings of SPIEP hotonics West, Electronic Imaging'02,SecurityandWatermarkingofMulti-media Contents, SanJose, California, January2002, vol.4675, pp. 1–13.
[37] C. Ullerich, A. Westfeld, "Weaknesses of MB2", in: Proceedings of the Sixth International Workshop on Digital Watermarking, Guangz- hou, China, December 3–5, 2007, pp. 127–142.
[38] C. Chen, Y.Q. Shi, "JPEG image steganalysis utilizing both intra block and Inter block correlations", in: Proceedings of IEEE International Symposium on Circuits and Systems, ISCAS 2008, Seattle, Wa- shington, USA, 18–21 May 2008, pp. 3029–3032.
[39] C.C. Chang, H.W. Tseng, "A steganographic method for digital images using side match, Pattern Recognition" Letters 25 (12) (2004) 1431–1437.
[40] E. Franz, A. Schne idewind, "Adaptive steganography based on dithering", in: Proceedings of the ACM Workshop on Multimedia and Security, September 20–21, 2004, Magdeburg, Germany, pp. 56–62.
[41] L.Yu, Y.Zhao, R.Ni, Z.Zhu, "PM1 steganography in JPEG images using genetic algorithm",Soft Computing13(4)(2009)393–400.
[42] C.C. Chang, P. Tsai, M.H. Lin, "An adaptive steganography for index- based images using

codeword grouping", Advances in Multimedia Information Processing-PCM, Springer, vol. 3333, 2004, pp. 731–738 images using codeword grouping, Advances in Multimedia Information Processing-PCM, Springer, vol. 3333, 2004, pp.731-738.

[43] Weiming Zhang, Xinpeng Zhang, and Shuozhong Wang "A Double Layered "Plus- Minus One Data Embedding Scheme"IEEE signal processing letters, vol. 14, no. 11, november 2007.

[44] H.Hioki, "A data embedding method using BPCS principle with new complexity measures", in: Proceedings of Pacific Rim Workshop on Digital Steganography, July2002, pp.30–47.

[45] J.Spaulding, H.Noda, M.N.Shirazi, E.Kawaguchi, "BPCS steganography using EZW lossy compressed images", Pattern Recognition Letters 23(13) (2002)1579–1587.

[46] J.Fridrich, "Application of data hiding in digital images", Tutorial for the ISSPA' 99, Brisbane, Australia, August22–25,1999.

[47] Y.Srinivasan, B.Nutter, S.Mitra, B.Phillips, D.Ferris, "Secure transmission of medical records using high capacity steganography", in: Proceedings of the 17th IEEE Symposium on Computer-Based Medical Systems, CBMS'04 , 2004, pp.122–127.

[48] E.Kawaguchi, R.O.Eason, "Principle and applications of BPCS steganography", in: Proceedings of SPIE International Symposium on Voice, Video and Data Communications 2–4 November1998, pp. 464–473.

[49] K.B.Raja, S.Sindhu, T.D.Mahalakshmi, S.Akshatha, B.K.Nithin, M. Sarvajith, K.R.Venugopal, L.M.Patnaik, "Robust image adaptive steganography using integer Wavelets", in: Proceedings of the 3rd International Conference on Communication Systems Software and Middleware and Workshops, COMSWARE' 08,6–10 January 2008, pp. 614–621.

[50] C.C.Lin, W.L.Tai, C.C.Chang,"Multilevel reversible data hiding based on histogram modification of difference images", Pattern Recognition 41(12)(2008)3582–3591.

[51] Y.T.Wu, F.Y.Shih, "Genetic algorithm based methodology for breaking the steganalytic systems", IEEE Transactions on Systems, Man, and Cybernetics part B: cybernetics 36 (1) (2006) 24–31.

[52] S.P.Maity, M.K.Kundu, P.K.Nandi, "Genetic algorithm for optimal imperceptibility in image communication through noisy Channel", in: Proceedings of the International Conference on Neural Information Processing (ICONIP'2004), India,29 October 2004, pp. 700–705.

[53] J. Kong, H. Jia, X. Li, Z. Qi, "A novel content-based information hiding scheme", in: Proceedings of the International Conference on Computer Engineering and Technology, 22–24 January 2009, vol. 1, pp. 436–440.

[54] M.W. Chao, C.H. Lin, C.W. Yu, T.Y. Lee, "A high capacity 3D steganography algorithm", IEEE Transactions on Visualization and Computer Graphics 15 (2) (2009) 274–284.

[55] A. Bogomjakov, C. Gotsman, M. Isenburg, "Distortion-free steganography for polygon meshes", in: Proceedings of Computer Graphics Forum, Eurographics'08, pril 2008, vol. 27 (2), pp. 637–642.

[56] H. Nakamura, Q. Zhao, "Information hiding based on image morphing", in: Proceedings of 22nd International Conference on Advanced Information Networking and Applications Workshops, AINAW, 25–28 March 2008, pp. 1585-1590.

[57] A.M. Zeki, A.A. Manaf, "A novel digital watermarking technique based on ISB (Intermediate Significant Bit)", World Academy of Science, Engineering and Technology 38 (2009) 1080–1087.

[58] S.C. Katzenbeisser, "Principles of steganography", in: S.Katzenbeisser, F.A.P. Petitcolas (Eds.), Information Hiding Techniques for Steganography and Digital Water marking, Artech House Inc, Norwood, 2000.

[59] L. Zheng, I.Cox, "JPEG based conditional entropy coding for correlated Steganography", in: Proceedings of IEEE International Conference on Multimedia and Expo, Beijing, China, 2–5 July 2007, pp. 1251–1254.

[60] I.Cox, "Information hiding, watermarking and steganography", Public Seminar, Intelligent Systems Research Centre(ISRC), University of Ulster at Magee,Northern Ireland, 28th April 2009.

[61] Y.H.Yu, C.C.Chang, I.C.Lin, "A new steganographic method for color and gray scale image hiding", Computer Vision and ImageUnderstanding 107(3)(2007)183–194.

[62] M.Drew, S.Bergner, "Spatio-chromatic decorrelation for color image compression", Technical Report, School of Computing Science, Simon Fraser University, Vancouver, Canada, 2007, available from:/http:// fas.sfu.ca/ pub/cs/TR/2007/CMPT2007-09.pdfS.

[63] M.Saenz, R.Oktem, K.Egiazarian, E.Delp, "Color image wavelet compression using vector morphology", in: Proceedings of the European SignalProcessingConference,September5–82000, Tampere,Finland,2000,pp.5–8.

[64] A.Rodriguez, L.Rowe, Multimedia systems and applications, IEEEComputer 28(5)(1995) 20–22.

[65] L.M.Marvel, C.T.Retter, "A methodology for data hiding using Images", in: Proceedings of IEEE Military Communications Conference, MILCOM'98,Boston, MA, USA,18–21October 1998, pp.1044–1047.

[66] R.J.Anderson, F.A.P.Petitcolas, "On the limits of steganography", IEEE Journal of Selected Areas in Communications 16(4)(1998)474–481.

[67] P.Bas,"Analyse steganographique d' images numeriques: Comparaison de differentes methods", Rapportdestage, Laboratoire des Images et des

Signaux, University of Joseph Fourier, 23rdJune 2003, (in French).
[68] J.Fridrich, M.Goljan, R.Du, Reliable detection of LSB stegano- graphy in grayscale and colorimages",in: Proceedings of ACM, Special Session on Multimedia Security and Watermarking, Ottawa, Canada, 5th October 2001 , pp.27–30.
[69] D.C.Lou, C.H. Sung, "A steganographic scheme for secure communications based on the chaos and Euler theorem", IEEE Transactions on Multimedia 6(3)(2004)501–509.
[70] A.Cheddad, J.Condell, K.Curran, P.McKevitt, "Securing information content using new encryption method and steganography", in: Proceedings of the Third IEEE International Conference on Digital Information management, University of East London, UK,13–16 November 2008, pp.563–568.
[71] D.C. Wu, W.H. Tsai, A steganographic method for images by pixel value differencing", Pattern Recognition Letters24 (9–10)(2003) 1613–1626.

Mr. Manish Mahajan completed his M-Tech 2010 & pursuing his Ph.D. from Punjab Technical University. Currently working in I.T. deptt. of CEC, Landran Mohali.

Dr. Navdeep Kaur completed her Ph. D from IIT Roorkee. Currently she is working as Professor with CSE deptt. of CEC, Landran Mohali.

