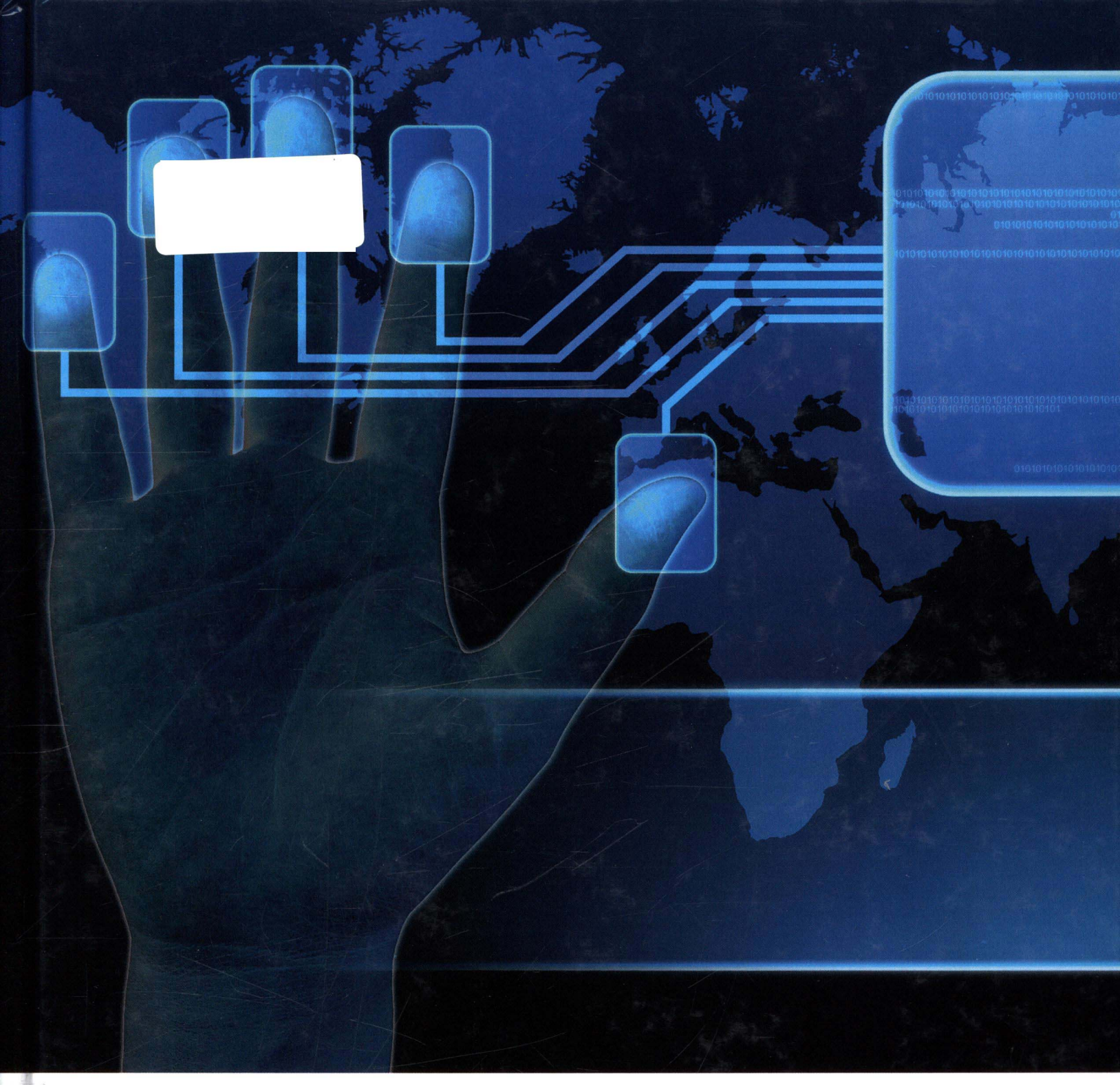

Information Security

Principles and New Concepts

Volume II

Fiona Hobbs

Information Security: Principles and New Concepts

Volume II

About the Book

This is the era of information. We can read up about everything on the internet. The data is freely available, thus the important data needs to be secured. Hence, the need for information security has risen in the past few years. This book includes specialised researches on topics related to information security, along with new concepts and theories in this field.

About the Editor

Fiona Hobbs received her master's in computer science and her PhD in information security from the Royal Holloway, University of London, United Kingdom. She is a senior professor in the Department of Computer Science and Information Technology in an American University. Her academic interests lie in developing data and computer security algorithms. Hobbs has authored and edited numerous well-published articles, journal papers and books on computer science and information security.

CLANRYE INTERNATIONAL
www.clanryeinternational.com

ISBN 978-1-63240-307-0
9 781632 403070

Hobbs

Information Security: Principles and New Concepts

NAL

Information Security: Principles and New Concepts

Volume II

Edited by **Fiona Hobbs**

常州大学图书馆
藏书章

LANRYE
NTERNATIONAL
New Jersey

Published by Clanrye International,
55 Van Reypen Street,
Jersey City, NJ 07306, USA
www.clanryeinternational.com

Information Security: Principles and New Concepts
Volume II
Edited by Fiona Hobbs

© 2015 Clanrye International

International Standard Book Number: 978-1-63240-307-0 (Hardback)

This book contains information obtained from authentic and highly regarded sources. Copyright for all individual chapters remain with the respective authors as indicated. A wide variety of references are listed. Permission and sources are indicated; for detailed attributions, please refer to the permissions page. Reasonable efforts have been made to publish reliable data and information, but the authors, editors and publisher cannot assume any responsibility for the validity of all materials or the consequences of their use.

The publisher's policy is to use permanent paper from mills that operate a sustainable forestry policy. Furthermore, the publisher ensures that the text paper and cover boards used have met acceptable environmental accreditation standards.

Trademark Notice: Registered trademark of products or corporate names are used only for explanation and identification without intent to infringe.

Printed in China.

此为试读，需要完整PDF请访问：www.ertongbook.com

Information Security: Principles and New Concepts

Volume II

Preface

In contemporary times, there is no dearth of information. In fact, since the advent of technology and the World Wide Web, there has been an overload of information. All data needs to be recorded, saved and stored. However, some information is more crucial as compared to others. And this is where the concept of Information Security comes in. The origins of Information Security can be traced to the times of Julius Caesar in 50 B.C, when he invented the Caesar cipher. This mechanism was used to protect the confidentiality of correspondence and provided a means of detecting tampering, in case any. Regardless of the form that the data may take, electronic or physical, Information Security is a must in present times.

Information Security has grown and evolved significantly in recent years. Numerous occurrences of international terrorism, through disruption of data fuelled the need for better methods of Information Security. Today, it is an indispensable part of all the business operations across different domains. Protecting information has also become an ethical and legal requirement in many cases. Essentially, the practice of defending information from unauthorized access, use, disclosure and destruction is referred to as Information Security. The CIA triad of confidentiality, integrity and availability is one of the core principles of information security.

There are two important aspects to Information Security. These are Information Technology Security, which is concerned with technology security and Information Assurance, whose aim is to ensure that data is not lost during critical times.

I would like to thank all the contributors who have shared their knowledge in this book. I would also like to thank my family for their constant trust and support.

Editor

Contents

	Preface	**IX**
Chapter 1	**A Robust Method to Detect Hidden Data from Digital Images** Romany F. Mansour, W. F. Awwad, A. A. Mohammed	**1**
Chapter 2	**A Visual Cryptography Based Digital Image Copyright Protection** Adel Hammad Abusitta	**6**
Chapter 3	**Effect of Network Traffic on IPS Performance** Shahriar Mohammadi, Vahid Allahvakil, Mojtaba Khaghani	**15**
Chapter 4	**Digital Evidence for Database Tamper Detection** Shweta Tripathi, Bandu Baburao Meshram	**22**
Chapter 5	**Experimental Evaluation of Cisco ASA-5510 Intrusion Prevention System against Denial of Service Attacks** Raja Sekhar Reddy Gade, Sanjeev Kumar	**31**
Chapter 6	**New Video Watermark Scheme Resistant to Super Strong Cropping Attacks** Ming Tong, Tao Chen, Wei Zhang, Linna Dong	**47**
Chapter 7	**Detecting Threats of Acoustic Information Leakage through Fiber Optic Communications** Vladimir V. Grishachev	**58**
Chapter 8	**Digital Image Watermarking Based on Mixed Error Correcting Code** Yonghong Chen, Jiancong Chen	**65**
Chapter 9	**A Fair Electronic Cash System with Identity-Based Group Signature Scheme** Khalid. O. Elaalim, Shoubao Yang	**71**
Chapter 10	**A Tree Model for Identification of Threats as the First Stage of Risk Assessment in HIS** Ahmad Bakhtiyari Shahri, Zuraini Ismail	**78**
Chapter 11	**Hardware Performance Evaluation of SHA-3 Candidate Algorithms** Yaser Jararweh, Lo'ai Tawalbeh, Hala Tawalbeh, Abidalrahman Moh'd	**86**

Chapter 12 **Reference Encryption for Access Right Segregation and Domain Representation** 94
Lanfranco Lopriore

Chapter 13 **Comparative Evaluation of Semifragile Watermarking Algorithms for Image Authentication** 99
Archana Tiwari, Manisha Sharma

Chapter 14 **Digital Forensics and Cyber Crime Datamining** 106
K. K. Sindhu, B. B. Meshram

Chapter 15 **A New Steganography Method Based on the Complex Pixels** 112
Amin Hashemi Pour, Ali Payandeh

Chapter 16 **The Application of Mixed Method in Developing a Cyber Terrorism Framework** 119
Rabiah Ahmad, Zahri Yunos

Chapter 17 **Data Stream Subspace Clustering for Anomalous Network Packet Detection** 125
Zachary Miller, Wei Hu

Chapter 18 **Enhanced Timestamp Discrepancy to Limit Impact of Replay Attacks in MANETs** 134
Aziz Baayer, Nourddine Enneya, Mohammed Elkoutbi

Chapter 19 **Feedback Reliability Ratio of an Intrusion Detection System** 141
Usha Banerjee, Gaurav Batra, K. V. Arya

Chapter 20 **Perception on Cyber Terrorism: A Focus Group Discussion Approach** 148
Rabiah Ahmad, Zahri Yunos, Shahrin Sahib, Mariana Yusoff

Chapter 21 **The Extended Tanh Method for Compactons and Solitons Solutions for the CH(n,$2n$ - 1,$2n$,-n) Equations** 155
Xinqian Lin, Shengqiang Tang, Wentao Huang

Chapter 22 **C3SM: Information Assurance Based on Cryptographic Checksum with Clustering Security Management Protocol** 159
Moad Mowafi, Lo'ai Tawalbeh, Walid Aljoby, Mohammad Al-Rousan

Chapter 23 **Two Approaches on Implementation of CBR and CRM Technologies to the Spam Filtering Problem** 168
Rasim Alguliyev, Saadat Nazirova

Chapter 24 **Unsupervised Multi-Level Non-Negative Matrix Factorization Model: Binary Data Case** 175
Qingquan Sun, Peng Wu, Yeqing Wu, Mengcheng Guo, Jiang Lu

此为试读，需要完整PDF请访问：www.ertongbook.com

Chapter 25 **State of the Art for String Analysis and Pattern Search Using CPU and GPU Based Programming** 181
Mario Góngora-Blandón, Miguel Vargas-Lombardo

Chapter 26 **Category-Based Intrusion Detection Using PCA** 186
Gholam Reza Zargar, Tania Baghaie

Chapter 27 **SPCS: Secure and Privacy-Preserving Charging-Station Searching Using VANET** 199
Tat Wing Chim, Jeanno Chin Long Cheung, Siu Ming Yiu, Lucas Chi Kwong Hui, Victor On Kwok Li

Permissions

List of Contributors

A Robust Method to Detect Hidden Data from Digital Images

Romany F. Mansour[1], W. F. Awwad[1], A. A. Mohammed[2]
[1]Department of Computer Science, Faculty of Science, Northern Borders Univeristy, Arar, KSA
[2]Department of Computer Science, Faculty of Science, South Valley University, Qena, Egypt

ABSTRACT

Recently, numerous novel algorithms have been proposed in the fields of steganography and visual cryptography with the goals of improving security, reliability, and efficiency. Steganography detection is a technique to tell whether there are secret messages hidden in images. The performance of a steganalysis system is mainly determined by the method of feature extraction and the architecture selection of the classifier. In this paper, we present a new method *Visual Pixel Detection VPD* for extract data from a color or a grayscale images. Because the human eye can recognize the hidden information in the image after using this detection. The experimental results show that the proposed method provides a better performance on testing images in comparison with the existing method in attacking Steghide, Outguess and F5.

Keywords: Data Hiding; Steganography; Steganalysis; Attack; Color Image Hiding; Stego-Image

1. Introduction

Steganography is the art, science, or practice in which messages, images, or files are hidden inside other messages, images, or files. The concept of steganography is not a new one; it dates back many millennia when messages used to be hidden on things of everyday use such as watermarks on letters, carvings on bottom sides of tables, and other objects. The more recent use of this concept emerged with the dawn of the digital world. Experiments have shown that data can be hidden in many ways inside different types of digital files. The main benefit of steganography is that the payload is not expected by the investigators who get to examine the computer data. The person sending the hidden data and the person meant to receive the data are the only ones who know about it; but to everyone else, the object containing the hidden data just seems like an everyday normal object. A classification of information hiding techniques is described in [1].

Generally, steganographic methods proposed in the past few years can be categorized into two types. The methods of the first type employ the spatial domain of a host image to hide secret data. In other words, secret data are directly embedded into the pixels of the host image [2-5].

Steganographic methods of the second type employ the transformed domain of a host image to hide secret data [6-10]. Transformation functions like the discrete cosine transform (DCT) or discrete wavelet transform (DWT) are first exploited to transform the pixel values in the spatial domain to coefficients in the frequency domain. Then the secret data are embedded in the coefficients.

Recently, the scheme proposed in [11] hid large amounts of data in the pixels of a true color image, which used 8 bits to represent each color component of a color pixel. The secret image can be both a grayscale and a true color image. However, the quality of the extracted color secret image is not good in terms of the peak signal-to-noise ratio (PSNR) value and visual observation. In this paper, we propose a steganographic method which hides a color or a grayscale image in a true color image.

The detection of hidden data presents a big challenge to investigators and individuals looking for hidden data. For images only, there are hundreds of billions of images on the web and looking through all of them would be a very time consuming and computationally challenging task; let alone the other types of files that data can possibly be hidden in. Even if someone manages to go through all the current images on the web, what if some new algorithm for hiding data in images emerges? Is the application used to scan the images for hidden data suitable for and capable of uncovering the hidden data? And is it feasible to go back and rescan all the images all over again with the same or other software updated to detect the hidden data by the new algorithm? The answer to the above questions is that it's close to impossible to be able to accurately scan or attempt to detect hidden data on

such a wide scope of suspect images. It is somewhat easier for investigators to scan for hidden data on a smaller scale such as an image of a hard drive, but they are still faced with the same software inaccuracy and the possibility of encountering unknown data-hiding algorithms.

In our proposed method, the local color information of an image can be preserved well because the technique of color quantization in the proposed method is image-dependent and adaptive color quantization [12]. The extracted color secret image is perceptibly almost identical to the original image, and its PSNR value is very high Moreover, the hiding capacity of the host image and the quality of the stego-image in the proposed method are also superior to that of the scheme in [11].

The remainder of this paper is organized as follows. In Section 2, a brief description of the scheme related to this paper will be given. In Section 3, we shall present our proposed method. The overall algorithm for the proposed method will be provided in Section 4. Finally, the experiments and conclusions shall be given in Sections 5 and 6.

2. Color Quantization

Color quantization is the process that drastically reduces the number of colors used in a digital color image by approximating the original pixels with their nearest representative colors. The true color image is usually quantized to reduce the size of the image to be stored or transmitted. This means the 224 colors of a true color image have to be greatly reduced to a limited number of representative colors, which is called a color table (palette).

Typically, a color table consists of 256 entries where each entry represents a color containing red, green, and blue components. In general, a palette-based image mainly consists of a color table and some image data, which contain indices corresponding to the color table entries.

Bitmap images consist of matrices of numbered points with two dimensions for grayscale and three dimensions for RGB color images. The grayscale images, also called intensity images, contain numbered values at these points, called pixels, between 0 for black and 255 for white, which can be represented as 8-bit binary strings (2^8 = 256). The numbers between represent gradient gray values between black and white. The RGB, abbreviated for Red, Green and Blue, images are actually three two-dimension image layers, a red, a green and a blue layer, that are combined to produce the full color image. Each layer of a color image also contains values from 0 for black to 255 for the lightest shade of the color. The RGB color scheme is referred to as an additive scheme because adding the effective value of the three layers usually produces a lighter color at that pixel.

For instance if all three values that comprise a pixel are 0, *i.e.* (0, 0, 0) for (red, green, blue), they produce the color black. If the three are 255, *i.e.* (255, 255, 255) they add to produce a much lighter shade, white. The product of these three layers can produce over 16 million different colors and is called 24-bit color because $256^3 = (2^8)^3 = 2^{24}$ = 16,777,216, in which three 8-bit binary strings represent pixel colors. They are intensity, color, red layer, green layer and blue layer, from left to right. Notice that the vertical white line that appears in the center of the intensity and color images is lighter than that in the RGB layers and that the blackish colors appear black in all images. This demonstrates the additive nature of RGB color images with respect to intensity.

Messages are hidden in the least significant bits of the 8-bit binary strings representing the color numbers; hence the abbreviated name for this method is "lsb" steganography. Each character in a message has a binary representation under the ASCII (American Standard Code for Information Interchange) character system, which assigns characters with integer values between 0 and 255. This system represents a way to express all necessary single character letters, numbers, punctuations, symbols, etc. for general communication purposes. The pixel is capable of representing 2^{24} or 16,777,216 color values. If we use the lower 2 bits of each color channel to hide data as shown in **Figure 1**.

3. The Proposed Scheme

In this section, we shall present the proposed the VDX method for extracting hiding a color or a grayscale secret image in a true color host image.

The proposed method is described below.

3.1. Requirements of Hiding Information Digitally

There are many different protocols and embedding techniques that enable us to hide data in a given object. However, all of the protocols and techniques must satisfy a number of requirements so that steganography can be applied correctly. The following is a list of main requirements that steganography techniques must satisfy:

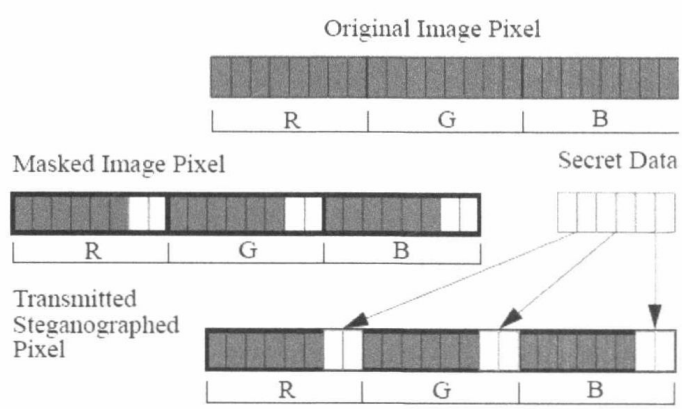

Figure 1. Illustrated representing the pixel values used the lower 2 bits of each color channel to hide data.

- The integrity of the hidden information after it has been embedded inside the stego object must be correct. The secret message must not change in any way, such as additional information being added, loss of information or changes to the secret information after it has been hidden. If secret information is changed during steganography, it would defeat the whole point of the process.
- The stego object must remain unchanged or almost unchanged to the naked eye. If the stego object changes significantly and can be noticed, a third party may see that information is being hidden and therefore could attempt to extract or to destroy it.
- In watermarking, changes in the stego object must have no effect on the watermark. Imagine if you had an illegal copy of an image that you would like to manipulate in various ways. These manipulations can be simple processes such as resizing, trimming or rotating the image. The watermark inside the image must survive these manipulations, otherwise the attackers can very easily remove the watermark and the point of steganography will be broken.
- Finally, we always assume that the attacker knows that there is hidden information inside the stego object.

3.2. Embedding and Detecting a Mark

Figure 2 shows a simple representation of the generic embedding and decoding process in steganography. In this example, a secret image is being embedded inside a cover image to produce the stego image. The first step in embedding and hiding information is to pass both the secret message and the cover message into the encoder. Inside the encoder, one or several protocols will be implemented to embed the secret information into the cover message. The type of protocol will depend on what information you are trying to embed and what you are embedding it in. For example, you will use an image protocol to embed information inside images.

4. The Overall Proposed System Is Designed to Extract the Hidden Data

Hiding information in digital media requires alterations of the media properties, which may introduce some form of degradation or unusual characteristics. The degradation, at times, may become perceptible [1]. These characteristics may act as signatures that broadcast the existence of the embedded message and steganography tools used, thus defeating the purpose of stenography, which is hiding the existence of a message.

The passive attacks of steganalysis involve the detection of these characteristics and signatures. Manipulating digital media in an effort to disable or remove the embedded

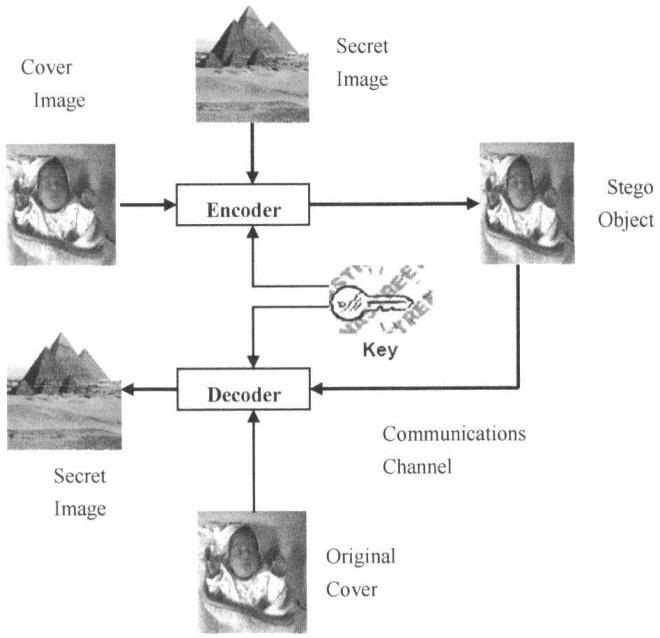

Figure 2. Generic processes of encoding and decoding.

messages is a simpler task than detecting the messages. Any image can be manipulated with the intent of destroying some hidden information whether an embedded message exists or not. Detecting the existence of a hidden message will save time in the activity to disable or remove messages by guiding the analyst to process only the media that contain hidden information [2].

4.1. Visual Pixel Detection

Some steganographic algorithms are embedded data in the media by replacing some bits of media with bits of data. For images, these algorithms will replace the bits of pixels by bits of data needed to hide it or changing the palette of image that depends on the value of data. The changing or replacing in values of pixels will be in most cases not sense or seeing by human eyes and will have effect in relation between pixels by increasing the amount of difference between the neighborhood pixels in the same level.

Any pixels have the same color or equal to the neighborhood pixels in the same portion or object in image. When we measure the difference between the pixels in the same portion, and evaluate the relation between these pixels, we can represent the image by these differences or relations.

The image that has no noise changing in the portions will have a good view for user. A user can see the most edge of object in this image, and the user has the ability to distinguish the details of the image. For some case the image will appear with a good efficient viewing. Some images have a bad image pattern details viewing, but have a number of edges and with details clear. When the image has some noise or hidden data in it, the looking

will not be clear. Most edges will be destroyed and the image details will not be clear and this depends on the amount of noise or hidden data and the algorithms that are used to hide data.

The visual pixel detection takes the relation between the pixels in images. It deals with BMP and GIF image file format only. The visual pixel detection works as a filter. Its filtering the pixels depends on its information and relation between other neighborhood pixels. This filter can remove from image pixels 1, 2, 3, 4 or 5 bits then re-drew the image depends on these bits.

4.2. Visual Pixel Detection Algorithm

Step1: Load Images.

Step2: Get color of pixels (Red, Green, Blue).

Step3: Calculate the relation between pixels in the same portion.

Step4: Compare between the values of pixel with the neighborhood pixels (4-neighborhood, 8-neighborhood).

Step5: Cut one bit from the pixels then re-draw the image which depends on these bits of pixels and the relation between the pixel and pixels in the neighborhood.

Step6: Repeat Step5 by changing the number of bits from 2 to 5 bit cut from the pixels and re-draw the images.

Step7: End.

The output images will help user to see the amount of hidden data noise. When original image pixels change by 1-bit the output images after filter are follows:

1) When the filter cut 1-bit from suspected image pixels, image output will be destroyed by amount of hidden data.

2) When the filter cut 2-bit from pixels, image output will be approximately clear (have some noise).

3) When the filter cut 3, 4, 5 bits from pixels, images output will be clear 3, 4, 5 bit or have a few noises. If the image has hidden information in two bits (1-2 bits), the output images from the filter will be:

- For 1, 2-bit images not clear.
- For 3, 4, 5-bits image approximately clear.

This filter will be very sensitive to any change in the first five bits of pixels in any BMP or GIF file format images. The number of color levels will not affect the filter results. The filter has the ability to deal with color level, it works in 256, 16-bit high color and true color for BMP images type. This filter also gives good results when used on GIF images; this is due to the fact that GIF file format has a maximum of 256 colors.

5. Experimental

To evaluate the effectiveness of the proposed method, we apply the proposed method "VPD" on deferent three types of secret images, hiding a color secret image, hiding a palette-based 256-color secret image, and hiding a grayscale image in a true color image the VPD Method will detect the stego objects from the different image that contain the stego objects as shown in **Figures 3** and **4** in the first both types but it fail in the third type.

The proposed method also is compared with Fridrich's method [13], Y. Q. Shi's method [14] and Z. M. He's method [15]. The averaged results of four independent runs for different steganographic embedding techniques are shown in **Tables 1-3**.

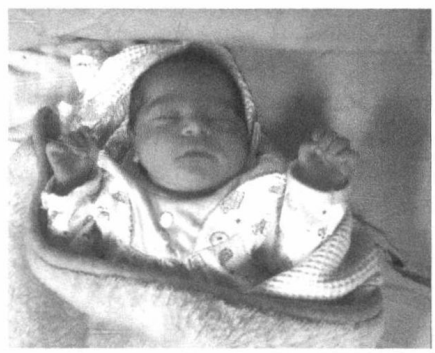

Figure 3. Original image with secret image.

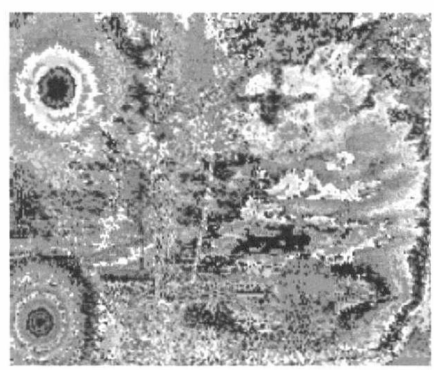

Figure 4. After using visual pixel detection.

Table 1. Detection accuracy for OutGuess.

bpc	Fridrich's	Y.Q.Shi's	Z.M. He's	proposed
0.05	74.65	88.00	89.60	91.65
0.1	92.00	98.00	99.70	99.86
0.2	99.25	99.85	100.00	100.00

Table 2. Detection accuracy for F5.

bpc	Fridrich's	Y.Q.Shi's	Z.M. He's	proposed
0.05	69.15	57.65	69.70	77.30
0.1	88.45	77.00	90.90	92.70
0.2	99.20	97.10	99.25	99.10

Table 3. Detection accuracy for Steghide.

bpc	Fridrich's	Y.Q.Shi's	Z.M. He's	proposed
0.05	71.80	86.70	86.95	87.10
0.1	79.45	96.60	96.05	96.00
0.2	89.20	99.70	99.90	98.90

此为试读，需要完整PDF请访问：www.ertongbook.com