International Journal of Enhanced Research in Science Technology & Engineering, ISSN: 2319-7463
Vol. 3 Issue 10, October-2014, pp: (211-216), Impact Factor: 1.252, Available online at: www.erpublications.com

A Comprehensive Study of Digital Image Processing

Manjul Kumar Malik
Teaching Assistant, Bhagat Phool Singh Mahila Vishvavidhalaya, Khanpur Kalan, Sonepat, Haryana

Abstract: Every digital image processing system can be represented by a block diagram containing three main elements. Image processing started with the input of an image in the processing system. The integrated software within the chip handles the task. Again it can be further processed based on the need. But the application of the processing method or algorithm depends on how the image is inputted, and stored. The quality of the processed image also depends on many criterions. In this article digital processed image quality comparison, hardware comparison and human perception and visual limitations are analyzed to find out common quality dependencies of processed image. The objective of this article is to educate newcomer to basic and fundamental technique of different types of image processing and to find out common image quality dependencies. All fundamental algorithms of image processing will be discussed and quality of processed image output comparison will be shown to find out dependencies.

Keywords: Digital Image Processing, Image algebra, Image Quality standard, steganography, steganalysis.

Introduction

Vision processing incorporates human perception and intelligence which makes the field most interesting to the research community as it can mimic human be havi our in the computer system by means of video surveillance system, integrating more intelligence to machines such as robots, as well as in ecology, biometrics and medical applications. Interestingly, recent NASA’s mission “Curiosity” on Mars, sending valuable images and information of Mars environment in a secure communication channel, transmitted images also need to processed exhaustively to find out any vital information about Mars. Hardware designs for image and video processing is used for faster performance rather than software, to meet the requirements of the end users, keeping its market relevancy and at the same time security is another concern, so the necessity to communicate these media data securely among multiple platforms after processing to enhance human perception and satisfaction in which our focus lies. The basic 4 steps in image processing domain are pre-processing, segmentation, feature extraction and recognition [1] and those has been keeping their strong importance in research mostly in the case of software implementation and very few implemented on hardware. Initial pre-processing step is carried out to enhance the quality of the original image by removing noise, unbalanced brightness etc as common interfering elements followed by segmentation where images are separated from the background into various elements with properties. Next in the feature extraction stage, extraction is performed on every detected object to reduce its information to a list of parameters storing in memory. Finally in the recognition stage a set of signals are generated using this list which constitute the upper level of processing assigning a specific meaning to every detected object. In this paper we focused on image Thresholding which is mainly used in the pre-processing and segmentation stages respectively, where our implementation is performing well enough in comparison to existing work (compared below), followed by secured transmission of the image data between multiple FPGA platforms and to the best of our knowledge this design belongs to a class of advanced implementation. Rest of the paper consists of three sections i.e. Hardware architecture and implementation design, results and observation followed by conclusion.

Image Thresholding as a Segmentation Step

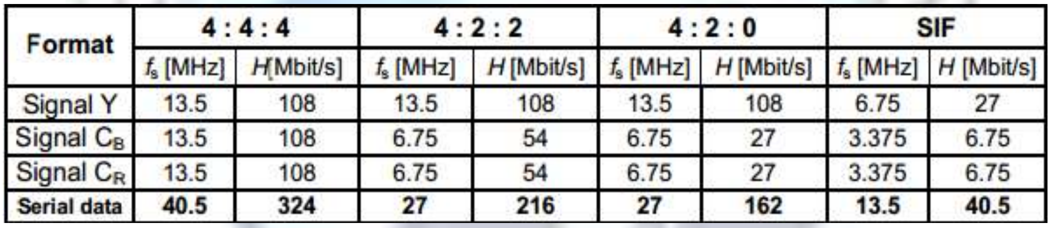
The first stage that we can think of in all stage of image processing and analysis is image binarization (i.e. to make binary image, the image should contain any two pixel values either 0 or 1 in contrast with gray images which can contains 255 pixel values for 8 bit image) which poses as one of the serious problem in applications like machine vision, pattern recognition, target tracking and image segmentation where the gray level information is required to reduce to bi-level information. In order to extract the useful information from an image it needs to be divided into distinct components like foreground (where pixel value is ‘1’) and background (where pixel value is ‘0’) objects for further analysis where most often the gray level pixels of foreground components are quite different from that of background and in this context a very crucial and significant technique available in literature known as thresholding is applied which is the process of partitioning pixels in the images into object and background classes based upon the relationship between the gray level value of a pixel and the significant parameter threshold to separate the object from the background, finding the correct value of which to separate an image into desirable foreground and background remains a very crucial step in image processing domain [2]. Because of its efficient performance and simplicity in theory, thresholding techniques have been studied extensively and a large number of thresholding methods have been published so far.

A dedicated custom hardware on FPGA can process image in real time with fairly lower processing cost and power compare to software. Field Programmable Gate Arrays (FPGAs), can be used to speed up image processing applications. An application implemented on an FPGA can be one to two orders of magnitude faster than the same application implemented in software where parallel computation of hardware should be one of the important merit of hardware platform. In this paper we have designed and implemented an adaptive thresholding as a function of the image pixel intensities. Finding an optimal threshold value leading to an effective binarized image requires skill as the choice of the method must be done judiciously. After an initial pre-processing of the image the thresholding has been applied where the threshold value is dependent on the nature of the image which becomes a very dominant factor at the end.

Transmitted Digital Image

The mentioned DVB non-compressed digital image corresponds to the CCIR ITU-R 601 recommendation and the transmission components are the luminance signal Y and chrominance signals CB and CR. Each signal component is sampled by the standardized sampling frequency and quantized by 8 bits per sample (256 levels) in broadcast quality or 10 bits per sample (1024 levels) in studio quality. The data rate of the digital video signal and its serial/parallel data multiplex depends on the sampling format. The Table I shows the possible sampling frequencies and according data rates for the sampling formats in baseband, serial multiplex and broadcast quality. The data rates are 0.768 times multiplied when only active part of image is in-process [3].

Table I: Sampling frequencies and data rates of signal components (broadcast quality).



Format	4 : 4 : 4		4 : 2 : 2		4 : 2 : 0		SIF	
	f_s [MHz]	H[Mbit/s]	f_s [MHz]	H [Mbit/s]	f_s [MHz]	H [Mbit/s]	f_s [MHz]	H [Mbit/s]
Signal Y	13.5	108	13.5	108	13.5	108	6.75	27
Signal C_B	13.5	108	6.75	54	6.75	27	3.375	6.75
Signal C_R	13.5	108	6.75	54	6.75	27	3.375	6.75
Serial data	**40.5**	**324**	**27**	**216**	**27**	**162**	**13.5**	**40.5**

The 4:4:4 sampling format is used for master record, the 4:2:2 and 4:2:0 sampling formats are used for standard television broadcasting (quality accords to PAL CCIR 625/50) and format SIF (Source Input Format) is used for low-quality transmissions (video conferences).

The digital transmission channel model

The channel is modelled as non-recursive digital filter FIR [4]. The simulation of the channel appears from the similarity with the characteristics and the process of design and realization of the digital filters. The mentioned filter is a single-purpose digital device or equipment that works with the input digital signal in according to saved programme. It has finite impulse response, numerical stable algorithm of design and relatively easy hardware implementation on Digital Signal Processor (DSP) platform. Another advantage of this filter is the linear phase characteristic in mentioned frequency band that is important especially for digital components signal transmission in digital television technique. The simulation of the digital filter characteristics is generally very efficient way to design. The conventional model [5] for digital transmission channel simulation for baseband digital television transmission is the FIR filter with low-pass character and variable parameters and methods of design. The developed model [3] can change the character of the filter (LP, HP, BP, BS, multiband), possibility of design method selection and it has variable parameters (filter order, cut-off frequencies, attenuations and allowed ripples of transmission module in passband and stopband, eventually interactive design by using the tolerant field of the digital transmission channel model).

Image Rectification and Registration

Geometric distortions manifest themselves as errors in the position of a pixel relative to other pixels in the scene and with respect to their absolute position within some defined map projection. If left uncorrected, these geometric distortions render any data extracted from the image useless. This is particularly so if the information is to be compared to other data sets, be it from another image or a GIS data set. Distortions occur for many reasons.

For instance distortions occur due to changes in platform attitude (roll, pitch and yaw), altitude, earth rotation, earth curvature, panoramic distortion and detector delay. Most of these distortions can be modelled mathematically and are removed before you buy an image. Changes in attitude however can be difficult to account for mathematically and so a procedure called image rectification is performed. Satellite systems are however geometrically quite stable and geometric rectification is a simple procedure based on a mapping transformation relating real ground coordinates, say in easting and northing, to image line and pixel coordinates. Rectification is a process of geometrically correcting an image so that it can be represented on a planar surface , conform to other images or conform to a map (Fig. 1). That is, it is the process by which geometry of an image is made planimetric. It is necessary when accurate area, distance and direction measurements are required to be made from the imagery. It is achieved by transforming the data from one grid system into another grid system using a geometric transformation.

Rectification is not necessary if there is no distortion in the image. For example, if an image file is produced by scanning or digitizing a paper map that is in the desired projection system, then that image is already planar and does not require rectification unless there is some skew or rotation of the image. Scanning and digitizing produce images that are planar, but do not contain any map coordinate information. These images need only to be geo-referenced, which is a much simpler process than rectification. In many cases, the image header can simply be updated with new map coordinate information. This involves redefining the map coordinate of the upper left corner of the image and the cell size (the area represented by each pixel). Ground Control Points (GCP) are the specific pixels in the input image for which the output map coordinates are known. By using more points than necessary to solve the transformation equations a least squares solution may be found that minimises the sum of the squares of the errors. Care should be exercised when selecting ground control points as their number, quality and distribution affect the result of the rectification. Once the mapping transformation has been determined a procedure called resampling is employed. Resampling matches the coordinates of image pixels to their real world coordinates and writes a new image on a pixel by pixel basis. Since the grid of pixels in the source image rarely matches the grid for the reference image, the pixels are resampled so that new data file values for the output file can be calculated.

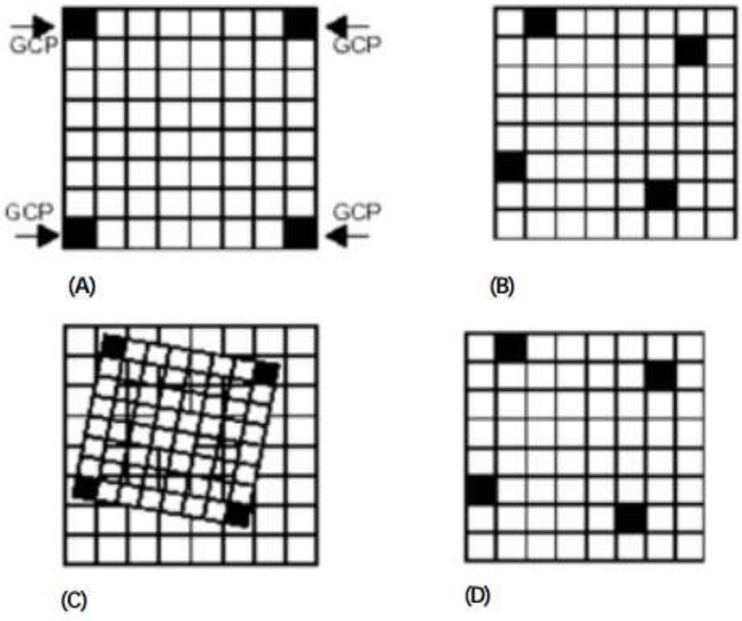


Figure 1 : Image Rectification (a & b) Input and reference image with GCP locations, (c) using polynomial equations the grids are fitted together, (d) using resampling method the output grid pixel values are assigned (source modified from ERDAS Field guide

Digital Image Processing & Steganography Applications

Steganography is employed in various useful applications, e.g., copyright control of materials, enhancing robustness of image search engines and smart IDs (identity cards) where individuals' details are embedded in their photographs. Other applications are video-audio synchronization, companies' safe circulation of secret data, TV broadcasting, TCP/IP packets (for instance a unique ID can be embedded into an image to analyze the network traffic of particular users) [6], and also checksum embedding [5]. Petitcolas [6] demonstrated some contemporary applications, one of which was in Medical Imaging Systems where a separation is considered necessary for confidentiality between patients' image data or DNA sequences and their captions, e.g., physician, patient's name, address and other particulars. A link however, must be maintained between the two. Thus, embedding the patient's information in the image could be a useful safety measure and helps in solving such problems. Steganography would provide an ultimate guarantee of authentication that no other security tool may ensure. Miaou et al. [7] present an LSB embedding technique for electronic patient records based on bi-polar multiple-base data hiding. A pixel value difference between an original image and its JPEG version is taken to be a number conversion base. Nirinjan and Anand [8] and Li et al. [9] also discuss patient data concealment in digital images.

Inspired by the notion that steganography can be embedded as part of the normal printing process, the Japanese firm Fujitsu is developing technology to encode data into a printed picture that is invisible to the human eye (data), but can be decoded by a mobile phone with a camera as exemplified in Fig. 2a and shown in action in Fig. 2b. The process takes less than one second as the embedded data is merely 12 bytes. Hence, users will be able to use their cellular phones to capture encoded data. They charge a small fee for the use of their decoding software which sits on the firm's own servers. The basic idea is to transform the image colour scheme prior to printing to its Hue, Saturation and Value components (HSV), then embed into the Hue domain to which human eyes are not sensitive. Mobile cameras can see the coded data and retrieve it. This application can be used for "doctor's prescriptions, food wrappers, billboards, business cards and printed media such as magazines and pamphlets" [20], or to replace barcodes.

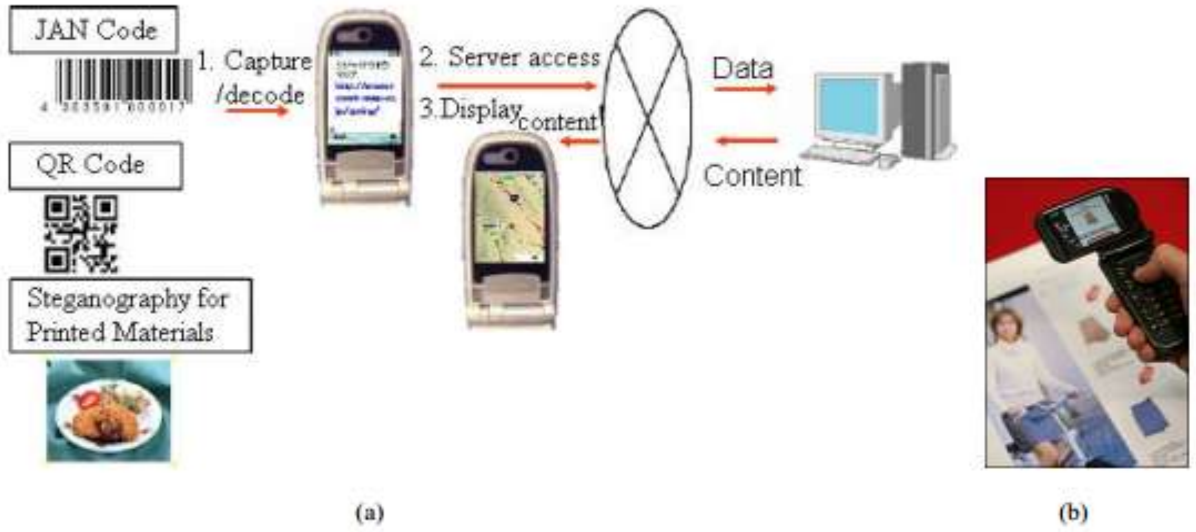


Fig. 2. Fujitsu exploitation of steganography: (a) a sketch representing the concept and (b) the idea deployed into a mobile phone shown at an exhibition recently

.

Steganalysis

This article does not delve into the details of the methods of Steganalysis although this work presents, herein, a brief description and some standards that a steganographer should usually examine. Steganalysis is the science of attacking steganography in a battle that never ends. It mimics the already established science of Cryptanalysis. Note that steganographers can create a steganalysis system merely to test the strength of their algorithm. Steganalysis is achieved through applying different image processing techniques, e.g., image filtering, rotating, cropping, and translating. More deliberately, it can be achieved by coding a program that examines the stegoimage structure and measures its statistical properties, e.g., first order statistics (histograms) or second order statistics (correlations between pixels, distance, direction). JPEG double compression and the distribution of DCT (Discrete Cosine Transform) coefficients can give hints on the use of DCT-based image Steganography. Passive steganalysis attempts to destroy any trace of secret communication, without bother to detect the secrete data, by using the above mentioned image processing techniques: changing the image format, flipping all LSBs or by undertaking a severe lossy compression, e.g., JPEG. Active steganalysis however, is any specialized algorithm that detects the existence of stego-images. Spatial steganography generates unusual patterns such as sorting of colour palettes, relationships between indexed colours and exaggerated "noise", as can seen in Fig. 26, all of which leave traces to be picked up by steganalysis tools. This method is very fragile. "LSB encoding is extremely sensitive to any kind of filtering or manipulation of the stego-image. Scaling, rotation, cropping, addition of noise, or lossy compression to the stego-image is very likely to destroy the message. Furthermore an attacker can easily remove the message by removing (zeroing) the entire LSB plane with very little change in the perceptual quality of the modified stego-image" [9]. Almost any filtering process will alter the values of many of the LSBs.

By inspecting the inner structure of the LSBs, Fridrich and her colleagues [10] claimed to be able to extract hidden messages as short as 0.03bpp (bit per pixel). Xiangwei et al. stated that the LSB methods can result in the "pair effect" in the image histograms. This "pair effect" phenomenon is empirically observed in steganography based on the modulus operator. Note that it is not always the case that modulus steganography produces such noticeable phenomenon. This operator acts as a means to generate random locations (i.e. not sequential) to embed data. It can be a complicated process or a simple one like testing, in a raster scan fashion (if a pixel value is even then embed, otherwise do nothing). Avcibas et al. [11] applied binary similarity measures and multivariate regression to detect what they call "telltale marks" generated by the 7th and 8th bit planes of a stego image.

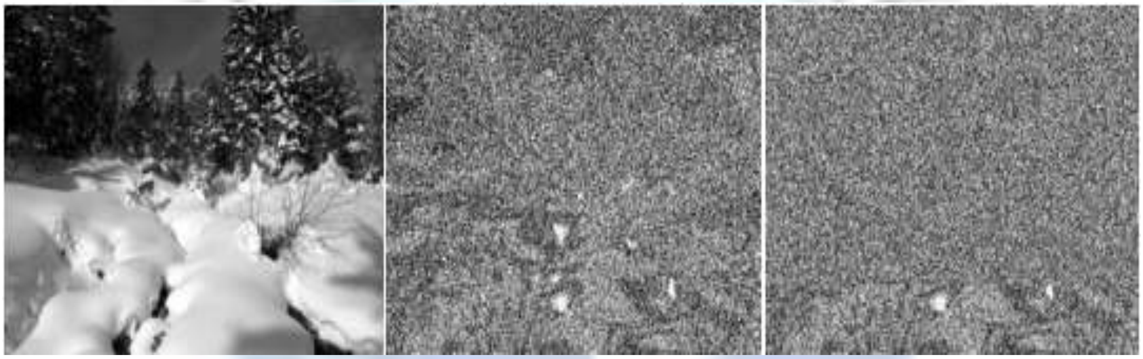


Fig. 3. Steganalysis using visual inspection: (left-to-right) original image, LSBs of the image before embedding and after embedding, respectively.

Conclusions

This paper presents a comprehensive study of digital image processing and its applications. The emerging techniques such as DCT, DWT and Adaptive steganography are not too prone to attacks, especially when the hidden message is small. This is because they alter coefficients in the transform domain, thus image distortion is kept to a minimum. Generally these methods tend to have a lower payload compared to spatial domain algorithms. There are different ways to reduce the bits needed to encode a hidden message. Apparent methods can be compression or correlated steganography, as proposed by Zheng and Cox which is based on the conditional entropy of the message given the cover. In short, there has always been a trade-off between robustness and payload. might occur by accident and not necessarily via an attack.

This paper also discusses with some detail of applications of steganography and watermarking. The various non-oblivious watermarking techniques available, which are highly resilient to image processing and geometric attacks, aim to detect the presence of a watermark using a correlation with an original template except in the rare watermarking blind detection scenario such as the work in [12]. This resilience can be seen for instance in the invariance proposed in the work of Deng et al. [14, 15]. However, in steganography, this detection is not required as the aim is to correctly extract the hidden bits without the availability of any side information such as the original image and watermark. However, what is evident is that steganography can have some useful applications, and like other technologies (i.e., encryption) it can be misused. These applications are numerous.

References

[1]. M. Kutter and F. Petitcolas, A fair benchmark for image watermarking systems, in: Proceedings of Electronic Imaging '99, Security and Watermarking of Multimedia Contents, San Jose, California, U.S.A, 25–27 January 1999, vol. 3657, pp. 226-239.

[2]. S.C. Katzenbeisser, Principles of steganography, in: S. Katzenbeisser and F.A.P Petitcolas, (ed.), Information hiding techniques for steganography and digital watermarking, Norwood: Artech House, INC, 2000.

[3]. J. Fridrich and M. Goljan, Practical steganalysis of digital images-state of the art, in: Proceedings of SPIE Photonics West, Electronic Imaging'02, Security and Watermarking of Multimedia Contents, San Jose, California, January 2002, vol. 4675, pp. 1-13.

[4]. A. Martin, G. Sapiro and G. Seroussi, Is image steganography natural?, IEEE Transactions on Image Processing, 14(12)(2005)2040-2050.

[5]. S. Areepongsa, N. Kaewkamnerd, Y.F. Syed and K.R. Rao, Exploring on steganography for low bit rate wavelet based coder in image retrieval system, in: Proceedings of IEEE TENCON, Kuala Lumpur, Malaysia, 2000, vol.3, pp. 250-255.

[6]. P. Kruus, C. Scace, M. Heyman and M. Mundy, A survey of steganographic techniques for image files, Advanced Security Research Journal, V (I) (2003)41-51.

[7]. A. Cheddad, J. Condell, K. Curran and P. Mc Kevitt, Skin tone based steganography in video files exploiting the YCbCr colour space, in: Proceedings of the IEEE International Conference on Multimedia and Expo, Hannover, Germany, June 23-26, 2008, pp.905-909.

[8]. A. Cheddad, J. Condell, K. Curran and P. Mc Kevitt, A skin tone detection algorithm for an adaptive approach to steganography, Signal Processing, 89 (12)(2009) 2465-2478.

[9]. A. Nikolaidis and I. Pitas, Region-based image watermarking, IEEE Transactions on Image Processing, 10(11)(2001)1726-1740.

[10]. A. Nikolaidis and I. Pitas, Robust watermarking of facial images based on salient geometric pattern matching, IEEE Transactions on Multimedia, 2(3)(2000)172-184.

[11]. D.C. Lou and 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.

[12]. A. Cheddad, J. Condell, K. Curran and P. Mc Kevitt, Securing information content using new encryption method and steganography, in: Proceedings of the 3rd IEEE International Conference on Digital Information Management, University of East London, UK, 13-16 Nov. 2008, pp. 563-568.

[13]. D.C. Wu and W.H. Tsai, A steganographic method for images by pixel-value differencing, Pattern Recognition Letters, 24 (9-10)(2003)1613-1626.

[14]. J. Kodovsky and J. Fridrich, Influence of embedding strategies on security of steganographic methods in the JPEG domain, in: Proceedings of SPIE Electronic Imaging, Security, Forensics, Steganography, and Watermarking of Multimedia Contents X, San Jose, CA, January 28-30, 2008, vol. 6819, pp. 1-13.

[15]. Y.S. Chen and R.Z. Wang, steganalysis of reversible contrast mapping watermarking, IEEE Signal Processing Letters, 16(2)(2009)125-128.