Global Journal of Computer Science and Technology
Graphics & Vision
Volume 12 Issue 14 Version 1.0 Year 2012
Type: Double Blind Peer Reviewed International Research Journal
Publisher: Global Journals Inc. (USA)
Online ISSN: 0975-4172 & Print ISSN: 0975-4350

Implementation of Embedding and Extracting Watermarking

By Kareem Mohammed Jubor
Thiqar university-Iraq

Abstract - In this paper, we used an image with a gray scale (256 bits) and bmp type. An image can be converted into binary file by using one of filters (Sober, Prewitt, and Robert) to find edges of the original image. Then we input the watermark to prove the authentic and password that used as a key for ciphering the information. This information will embed by using the Vigenere system that will store the cipher information in the edge of the image. As a result invisible watermark is not noticeable to viewer and without any degrade the quality of the content. The product invisible watermark is robust against distortions processes and resistant to intentional tampering solely intended to remove the watermark. Only the person who know the password and watermark and the cipher system, can read the information, we use a visual basic 6.0 program to implement this work.

Keywords : image processing, filters, edge detection, information hiding, cryptography.

GJCST-F Classification: I.4.0

Implementation of Embedding and Extracting Watermarking

Kareem Mohammed Jubor

Abstract - In this paper, we used an image with a gray scale (256 bits) and bmp type. An image can be converted into binary file by using one of filters (Sober, Prewitt, and Robert) to find edges of the original image. Then we input the watermark to prove the authentic and password that used as a key for ciphering the information. This information will embed by using the Vigenere system that will store the cipher information in the edge of the image. As a result invisible watermark is not noticeable to viewer and without any degrade the quality of the content. The product invisible watermark is robust against distortions processes and resistant to intentional tampering solely intended to remove the watermark. Only the person who know the password and watermark and the cipher system, can read the information, we use a visual basic 6.0 program to implement this work.

Keywords : image processing, filters, edge detection, information hiding, cryptography.

I. Introduction

There has been a rapid growth in digital imagery and digital watermark technology recently. Especially, the recent growth of network multimedia system has caused problems regarding the protection of intellectual property right such as the true image, the audio and video data [1]. Digital watermark technology has been developed quickly during the recent few years and widely applied to protect the copyright. The watermark is a digital code irremovable robustly and imperceptibly embedded in the host data and typically contains information about origin, status, and destination data [2].Given the motivation to protect intellectual property, Digital Watermarking has been suggested as a form of copyright protection and a deterrant to those wishing to obtain images illegally [3].

While the cryptographic techniques provide secrecy for the communication by scrambling a message which cannot be understood a cryptographic message can be intercepted by an eavesdropper because the encrypted message brings suspicion especially in military communications [4]. So, there is need for embedding data in a way that should be invisible to a human observer and doesn't make any suspicion. Then we encrypt the information by using Vigenere system, to prevent any unauthorized persons from getting the information [5].

II. Edge Detection

The edge and line detection operators presented here represent the various types of operators in use today. Many are implemented with convolution masks, and most are based on discrete approximations to differential operators. Differential operations measure the rate of change as a function of (in this case) the image brightness function. A large change in image brightness over a short spatial distance indicates the presence of an edge [6]. Some edge detection operators return orientation information (information about the direction of the edge), whereas others only return information about the existence of an edge at each point. Also included in this section is a special transform, the Hough Transform, which is specifically defined to find lines [7].

Edges detection methods are used as a first step in the line detection process. Edge detection is also used to find complex object boundaries by marking potential edge points corresponding to places in an image where rapid changes in brightness occur. After these edges points have been marked, they can be merged to form lines and object outlines [8].

With many of these operators, noise in the image can create problems. That is why it is best to preprocess the image to eliminate, or at least minimize, noise effects. To deal with noise effects, we must make tradeoffs between the sensitivity and the accuracy of an edge detector [9].

Edge detection operators are based on the idea that edge information in an image is found by looking at the relationship a pixel has with its neighbors. If a pixel's gray-level value is similar to those around it, there is probably not an edge at that point. However, if a pixel has neighbors with widely varying gray levels, it may represent an edge point. In other words, an edge is defined by a discontinuity in gray-level values. Ideally, an edge separates two distinct objects. In practice, apparent edges are caused by changes in color or texture or by the specific lighting conditions present during the image acquisition process [8, 9].

a) Roberts Operator

The Roberts operator marks edge points only; it does not return any information about the edge orientation. It is the simplest of the edge detection operators and will work best with binary images (gray-level images can be made binary by a threshold

Author : Computer Department-Computer and Mathmetic Collage – Thiqar university-Iraq. E-mail : kalbakaa@yahoo.com

operation). There are two forms of the Roberts operator. The first consists of the square root of the sum of the differences of the diagonal neighbors squared, as follows

$$\sqrt{[I(r,c)-I(r-l,c-l)]^2+[(I(r,c-l)-I(r-l,c)]^2} \quad (1)$$

The second form of the Roberts operator is the sum of the magnitude of the differences of the diagonal neighbors, as follows:

$$|I(r,c) - I(r\text{-}l,c\text{-}l)| + |I(r,c\ \text{-}l) - I(r\text{-}l,c)| \quad (2)$$

The second form of the equation is often used in practice due to its computational efficiency- it is typically faster for a computer to find an absolute value than to find square roots.

b) Sobel Operator

The Sobel edge detection masks look for edges in both the horizontal and vertical directions and then combine this information into a single metric.

At each pixel location we now have two numbers: s1, corresponding to the result from the row mask, and s2, from the column mask. We use these numbers to compute two metrics, the edge magnitude and the edge direction, which are defined as follows

$$\text{EDGE MAGNITUDE} = \sqrt{s_1^2 - s_2^2} \quad (3)$$

$$\text{EDGE DIRECTION} = \tan^{1}\left[\frac{s_1}{s_2}\right] \quad (4)$$

The edge direction is perpendicular to the edge itself because the direction specified is the direction of the gradient, along which the gray levels are changing.

c) Prewitt Operator

The Prewitt is similar to the Sobel, but with different mask coefficients.

These masks are each convolved with the image. At each pixel location we find two numbers: p1, corresponding to the result from the row mask, and p2, from the column mask. We use these results to determine two metrics, the edge magnitude and the edge direction, which are defined as follows

$$\text{EDGE MAGNITUDE} = \sqrt{p_1^2 + p_2^2} \quad (5)$$

$$\text{EDGE DIRECTION} = \tan^{-1}\left[\frac{p_1}{p_2}\right] \quad (6)$$

As with the Sobel edge detector, the direction lies 90o from the apparent direction of the edge.

III. Digital Watermarking

Digital watermarking technology is an emerging field in computer science, cryptography, signal processing and communications. Digital Watermarking is intended by its developers as the solution to the need to provide value added protection on top of data encryption and scrambling for content protection [5].

Watermarking technique is to hide secret information into the digital signals so as to discourage unauthorized copying or attest the origin of the media. The watermark is a digital code embedded in the image data and is invisible. A digital watermark is permanently embedded in the data, that is, it remains present within the original data after any distortion process. A watermark could be used to provide proof of authorship of a signal [10].

IV. Vigenere System Cipher

A popular form of periodic substitution cipher based on shifting alphabets is the Vigenere cipher. As noticed this cipher has been falsely attributed to the 16th century Fench cryptologist Blaise de Vigenere. The key K is specified by a sequence of letters K=k1, k2,…….kd, Where ki (i=1,……..d) gives the amount of shift in the ith alphabet ; that is [5]

$$f_i(a)= (a+k_i)\text{mod } n \quad (7)$$

Where a is the location of alphabet, where n is the number of the letters in the alphabet.

V. Result

The implementation of watermark and information embedding process and extracting process. Data storage process is performed in original image in edge points corresponding to the same place in a binary image. These edges are specified based on location of the edge that depend on the threshold (we take it 128, if the value => 128, then there is edge so we store the cipher information in this edge) Fig.(1) shows the block diagram for watermark and information embedding process.

a) Algorithm of Watermark & Information Embedding

1. Input the password text (5byte), as a letters
2. Input the marker (4 byte), as a numbers.
3. Input text of information hiding, as a letters
4. Convert the letters in steps (1&3) to ASCII Code then to decimal number
5. Convert the color image into grayscale (256 bits).
6. Find edges detection of the original image by selecting one of filters (Sobel, Prewitt, Robert), and then obtain binary file depending on a specified threshold.
7. Compare the value of threshold (128) with the values of file that obtain the image, if TH>128 then input the information sequence (Watermark, Password, Information) step 14 (that mean every 14 edges put one value, depend on sum of value of watermark “2+0+3+9=14”)
8. Return the image in gray scale that obtain the information, as shown in Fig (2).

b) Algorithm of Watermark & Information Extracting

1. Read the image was produced from embedding algorithm
2. Compare the value of threshold with the value of file that obtain the image, if TH>128 then read the information sequence (Watermark, Password, Information)
3. Input the marker (4 byte), as a numbers, and compare it by the first (4-byte) extract from 56 edge (each 14 edges one value) if they equaled, then the water marker is authentic and continue, else massage box "you in un authentication person.
4. Convert the (5 bye) in 70 edges start form edge 56, to ASCII code then to letters and make it as key
5. Convert(22 byte) the in 308 edges start form edge 126, to ASCII code then to letters
6. Decipher the information by using Vigenere system with key from step 4, as shown in Fig (3).

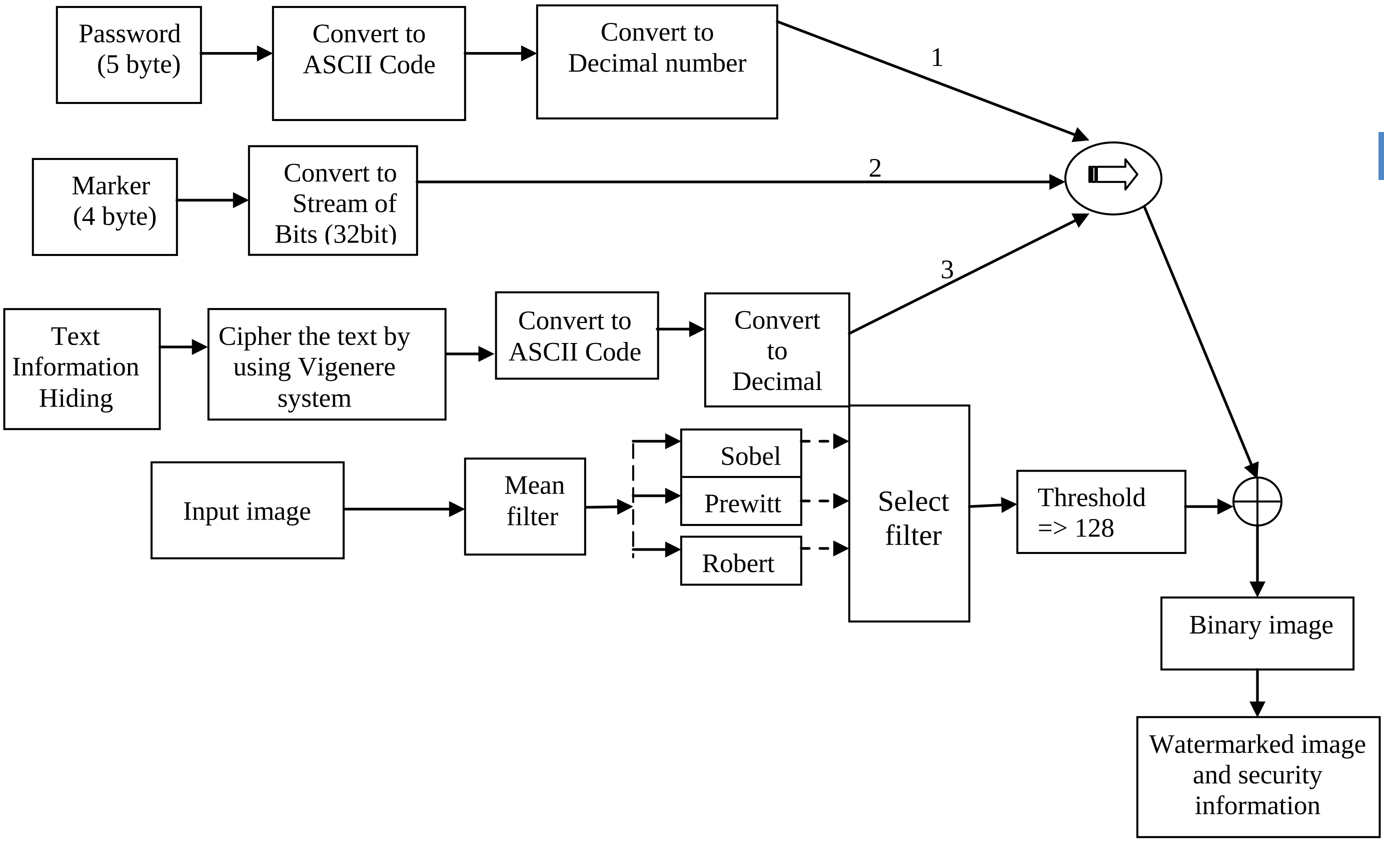
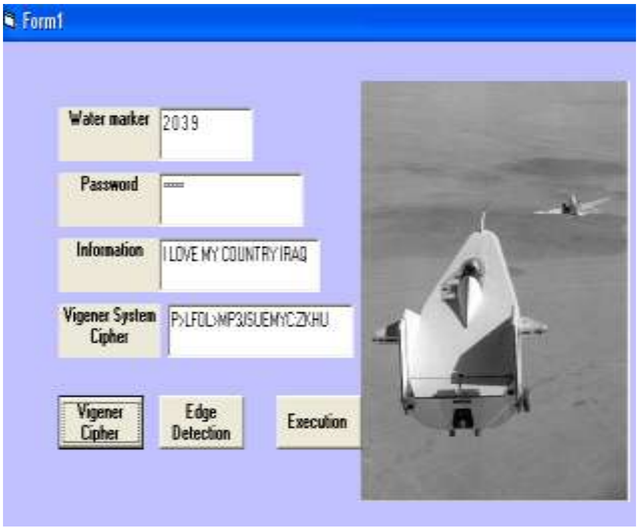


Fig. 1 : Block diagram for watermark and information embedding process



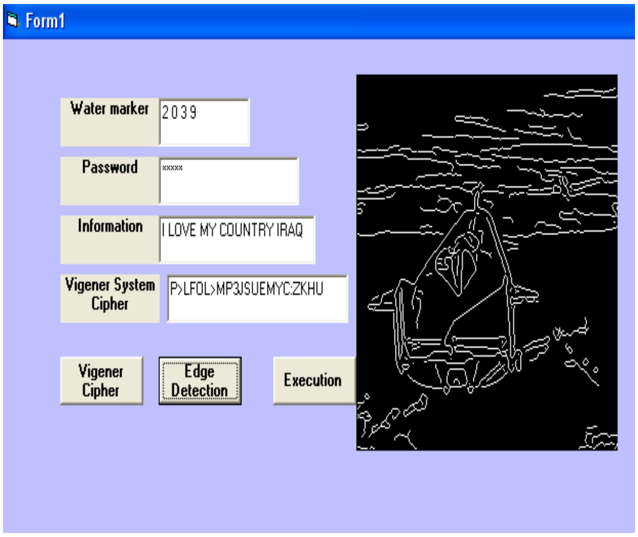
Water marker 2039

Password *****

Information I LOVE MY COUNTRY IRAQ

Vigener System Cipher P>LFOL>MP3JSUEMYCZKHU

Fig. (2-a) : Illustrated the input of PW.,WM. , INF., and ciphering



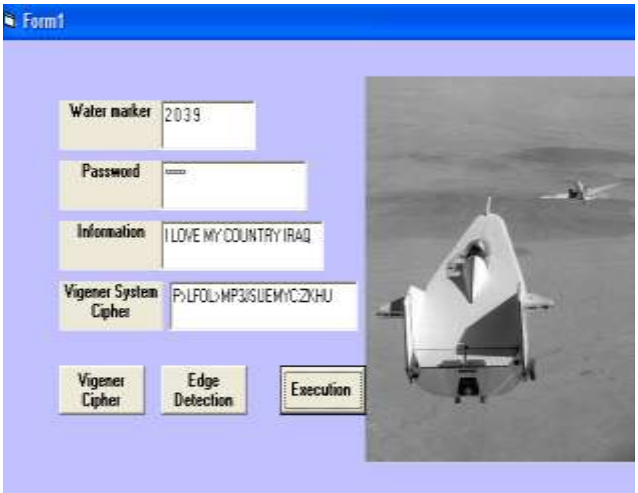
Water marker 2039

Password *****

Information I LOVE MY COUNTRY IRAQ

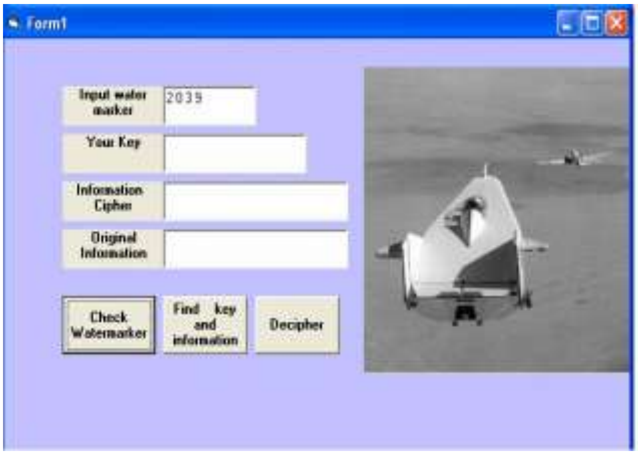
Vigener System Cipher P>LFOL>MP3JSUEMYCZKHU

Fig. (2-b) : Illustrated the edge detection for the image



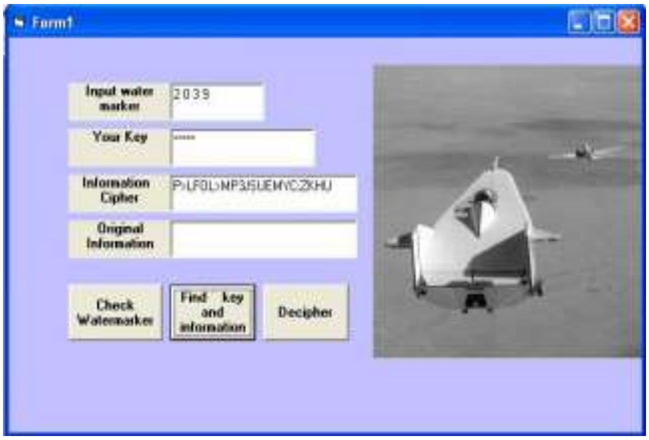
Water marker: 2039
Password: ****
Information: I LOVE MY COUNTRY IRAQ
Vigener System Cipher: P>LFOL>MP3JSUEMYCZKHU

Fig. (2-c) : Illustrated the embedding



Input water marker: 2039
Your Key:
Information Cipher:
Original Information:

Fig. (3-a) : Illustrated the checking for water marker



Input water marker: 2039
Your Key: ****
Information Cipher: P>LFOL>MP3JSUEMYCZKHU
Original Information:

Fig. (3-b) : Illustrated the extracting the original information

VI. Conclusions

1. In this paper the invisible watermark is not noticeable to viewer and without any degrades the quality of the content.
2. Data storage process is based on the existence of the edges in the image. These edges or the storage location in the image is not specified but depends on characteristic of image
3. The product invisible watermark is robust against distortions processes and resistant to intentional tampering solely intended to remove the watermark.
4. Returning information is impossible except when we know the type of used filter and used threshold value in case of converting image into binary image. In addition, we must know the password, watermarked image and the system cipher.
5. Watermarking provides the capability to specify the original image and ownership to this image and prevent counterfeits processes to this watermarking.

References Références Referencias

1. M. Shen and L. Sun, “A method For Digital Image Watermarking Using ICA” Science Research center, Shantou University, Guangdone 515063, China 1999. (mfshen@stu.edu.cn)
2. S. Katzenbeisser. F.A.P. P “Information Hiding Techniques for Steganography and Digital Watermarking” Artech House, INC., 2000.
3. J.Neil, D. Zoran and J. Sushil, “Information Hiding Steganography and Watermarking“ Kluwer Academic Publishers, USA, 2001.
4. Homer, “The Iliad” (trans. R. Fragels), Middlesex, England: Penguin, 1972.
5. D. Elizabeth “ Cryptography and data security” Addison-Wesley publishing company 1983
6. Scott E Umbaugh, PH.D. “Computer Vision and Image Processing”. A Practical Approach Using CVIPtools. To join a Prentice Hall PTR mailing list, point to:http://www.prenhall.com/mail_list/.
7. E.T.Lin, C.I. Podilchuk, and E.J.Delp, ”Detection of Image Iteration using Semi-fragile Watermarks”, http://www.ece.porduce.edu/~ace, 1995.
8. F. Jiri, “Application of Data Hiding in Digital Image“, Tutorial for ISPACS 98 Conference Melborne, Australia November 4-6, 1998.
9. J. Fridrich,” Method for Tamper Detection in Digital Image”, http@binghamton.edu, 2000.
10. Hal Berghel, “Watermarking Cyberspace”, Communications of the ACM, Nov. 1997, Vol.40, No.11, pp.19-24.