وزارة التعليم العالي والبحث العلمي
جامعة ديالى – كلية التربية
قسم الحاسبات

برنامج حذف الإضافات

بحث مقدم إلى قسم علوم الحاسبات

اعداد الطلبة

1. احمد رعد رحيم
2. اشرف ارشد
3. زياد خليفة
4. علي حسن نعمان

أشراف الاستاذ

احسان سلمان جاسم

١٤٢٨ هـ - ٢٠٠٧ م

Abstract

As in digital representations, images usually require a very large number of bits. In many applications, it is important to consider techniques for representing an image, or the information contained in the image, with fewer bits. In the terminology of information theory this is referred to as source encoding.
Applications of source encoding in the field of image processing generally fall into one of three categories:

1. Image data compression.
2. Image Hiding.
3. Image transmission.
4. Feature extraction.

In the past, most encoding image techniques (i.e., many types included with image hiding) have been applied only to gray scale images.

Now, many valuable images are color images. Thus, it has become important to be able to apply image-encoding techniques to hide color images. So, our proposed scheme can not only be applied to a color host image hiding a color secret image, but also to a color host image hiding a gray scale secret image. Our scheme utilizes the rightmost 3, 2 and 3 bits of the R, G, B channels of every pixel in the host image to hide related information from the secret image. Meanwhile, we utilize the leftmost 5, 6, 5 bits of the R, G, B channels of every pixel in the host image and set the remaining bits as zero to generate a palette.

We then use the palette to conduct color quantization on the secret image to convert its 24-bit pixels into pixels with 8-bit palette index values. DES encryption is then conducted on the index values before the secret image is embedded into the rightmost 3, 2, 3 bits of the R, G, B channels of every pixel in the host image.

The experimental results show that even under the worst case scenario our scheme guarantees an average host image PSNR value of 39.184 and an average PSNR value of 27.3415 for the retrieved secret image. In addition to the guarantee of the quality of host images and retrieved secret images, our scheme further strengthens the protection of the secret image by conducting color quantization and DES encryption on the secret image in advance. Therefore, our scheme not only expands the application area of image hiding, but is also practical and secure(1).

Contents

Chapter I

An Overview of Image Encoding.

1-1 Introduction:

The methods discussed in this chapter are applicable to any of these four categories. It is important to note, however, that these techniques are very much problem-oriented. In other words, while [he final objective of encoding is data reduction, the. choice of one encoding technique over another is dictated by the problem at hand. For example, data compression applications are motivated by the need to reduce storage requirements. In this particular problem, it is usually important to employ encoding techniques that allow perfect reconstruction (by means of a *decoder)* of the data from their coded form. Encoder-decoder pairs that incur zero error are referred to as *information preserving.*[(2)]

In image-transmission applications, such as the transmission of space-probe pictures for human interpretation, interest lies in techniques that achieve maximum reduction in the quantity of data to be transmitted, subject to the constraint that a reasonable amount of fidelity be preserved. In this case, emphasis is placed on reducing the amount of data that must be transmitted and the encoding technique need not be information-preserving, as long as the resulting images arc acceptable for visual or machine analysis.

Feature extraction applications are used primarily for pattern recognition by computer. In this case. the most important consideration is the choice of encoding techniques that will reduce the data subject to the constraint that enough information be preserved to allow a machine to differentiate between items of interest in an image. Consider, for example, the problem of classifying by machine different types of agricultural crops in a satellite image. Two types of features are important in this case; those that differentiate between vegetation and non vegetation: and those that can be used to differentiate between types of vegetation . Other features, such as those related to the difference between a road and a river, need not be taken into account in selecting an encoding procedure for this particular problem.

1-2 The Encoding Process [(2)]

Encoders can be modeled as a sequence of three operations, where images are expressed in vector form. The mapping operation maps the input data from the pixel domain into another domain when the quantizer and coder can be used more efficiently in the sense that fewer bits are required to code the mapped data than would be required lo code the original input data. The quantizer rounds off each mapped datum to one of a smaller number of possible values so that fewer code words with fewer bits are required. The encoding assigns a code word to each quantizer output.

So, we can find the following process:

1. The Mapping.
2. The Quantizer.
3. The Coder
    a. Huffman code.
    b. B- codes
    c. Shift code

Some typical codes

Input	Natural code	Gray code	B1 code	B2 code	B3 code
w1	000	111	C0	C00	00
w2	001	110	C1	C01	01
w3	010	100	C0C0	C10	10
w4	011	101	C0C1	C11	1100
w5	100	001	C1C0	C00C00	1101
w6	101	000	C1C1	C00C01	1110
w7	110	010	C0C0C0	C00C10	111100
w8	111	011	C0C0C1	C00C11	111101

1-3 Work Objective :-

Our goal to implement Encoding operation to one image in order to keep or transmit it securely. So, we explained the encoding methods in the next chapter with many techniques and concentrate on the HIDING Method and we had been implement a program using Microsoft Visual Basic ver.6 as demon started in chapter3.

Chapter II
Image Encoding Techniques

2-1 when encoded images are to be used ultimately for human and approbation , one must take into the effects account produced by the encoding in a reconstructed on the visual system the of the human system to errors in a reconstructed image depends on such factors as the frequency spectrum of the error, the gray-level content, and the amount of detail in the image. Hence, it is minimize degrade in subjective quality.

Transform encoding is an example account. Transform encoders perform a sequence of two operations, the first of which is based Statistical considerations and the second on psycho visual consideration. The first operation is a linear transformation whose objective is to reduce the statistical dependence of the pixels. The second operation is to quantize individually and code each of the resulting coefficients. The number of this required to code the coefficients depends on the number of quantize level, which is dictated sensivitivity of the visual system to the subjective effect of the quantize. (2)

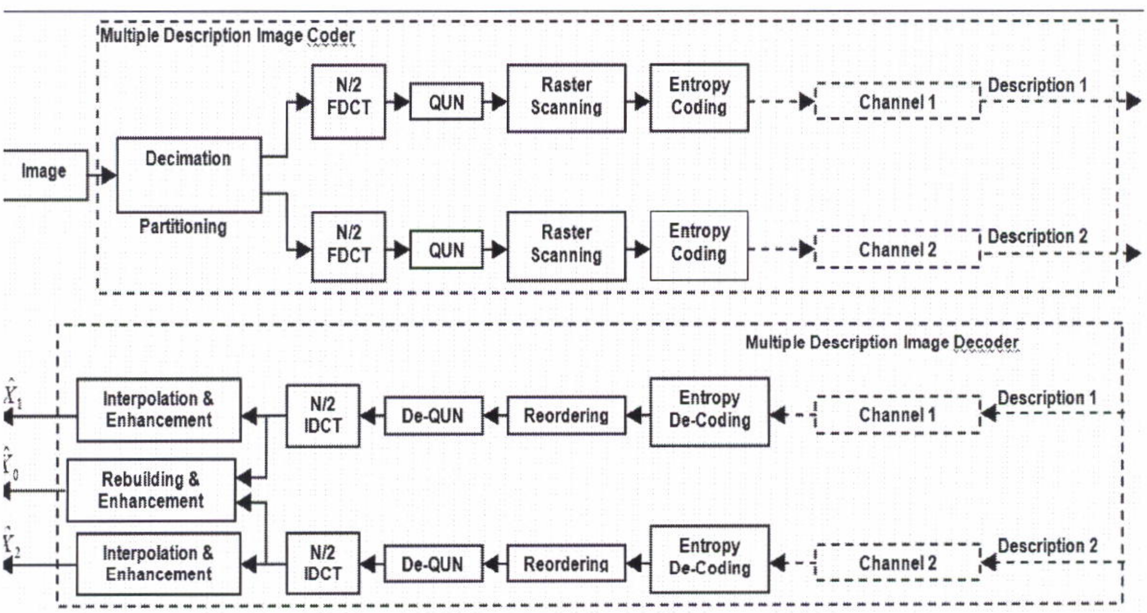


Figure 1: The presented MD image encoding system (3)

Multiple Description Image Encoder/Decoder

Our JPEG based MD image encoder/decoder consists of several stages:

• Decimation can be performed horizontally, vertically and horizontally-vertically. In the horizontal decimation, an image partitions in to two sub images. Sub image one and two consist of odd and even rows, respectively. Figure 2 shows the detail of such a partitioning technique in an 8*8 block.

• *N*/2 Point Discrete Cosine Transform (DCT)

Quantization, Scanning and Entropy Encoding

DCT coefficients are mapped into a relatively small set of possible values using an uniform quantization method. Then the DCT coefficients are mapped to new symbols using a horizontal scanning method. And finally, proper code words are assigned to the symbols using a standard Huffman Encoding algorithm in the JPEG standard and transmitted over two different channels.

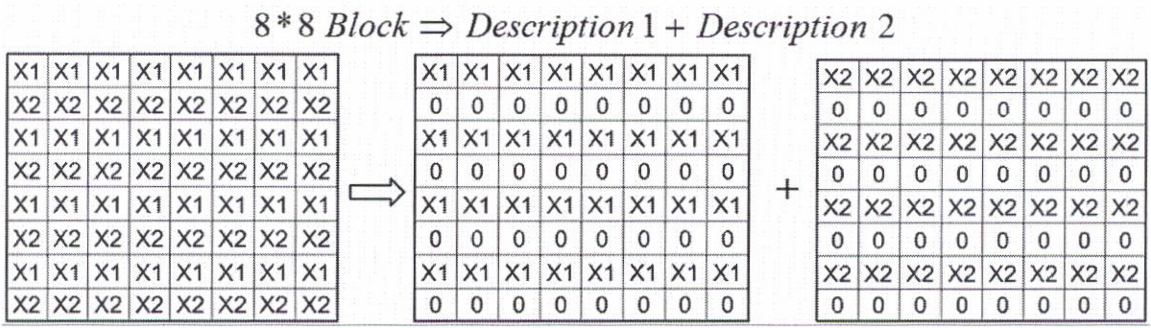


Figure 2: Horizontal decimation in each block.[3]

Simulation Results

To evaluate the performance of the presented method, the standard Lena image (with 512*512 pixels and 8 Bpp bit rate) is used as the test image in the simulation. Figure 3 shows the PSNR of the output image obtained from a single description versus the combined bit-rate (CBR) of both descriptions. This measurement shows the ability of a given approach to find a good trade off between encoding efficiency and the reconstruction quality, when only one description is available. Furthermore, figure 4 shows the reconstructed images from both descriptions and a single description, respectively. In this case a simple linear interpolation is used to interpolate the missing pixels.

In addition, Table 1 has provided a comparison between the presented method and other JPEG based MD image encoding techniques in the literature [8, 9]. In this comparison, after the de encoding of each of the descriptions, missing pixels are interpolated using the same methods; furthermore, no image enhancement algorithms have been used. It is obvious that, this method by decreasing the complexity and the amount of computation at the encoder has an acceptable performance for reconstructing an image with high quality.

2-2 HIDING:

Information hiding is a new technology which integrates with theories and technologies of many academic and technical subjects. For information hiding, digital media are used as the carrier of the information to be hidden. The carrier conceals secret messages by covering the form of their existence. So, many thing here can be introduce like the definition, basic models and basic characters of information hiding. The application and research trends for information hiding system are concerned. The information hiding technology based on digital image processing is closely related to human vision system. When the messages are having been concealed, the human eyes are due to verify the existence of hiding messages. That is, the status of information coverage depends on the human vision system. It is obvious that the characteristics of human vision system are to be taken advantage. The added secrete information in the digital image should have no any effect onto human eyes. In our research work, an implementation of information hiding technology system which is based on digital image encoding is proposed. First by analyzing knowledge of digital image processing and the model of human vision system, we discussed the algorithm of time domain appending method and the algorithm of substitution of lease significant bit. Secondly, we analyzed theory and algorithms of 2-D discrete wavelet transform and frequency domain algorithm based on discrete wavelet transformation. Carefully design software for information hiding based on digital image using Microsoft Visual C++6.0 or Visual basic.6 implemented. The communication with hiding messages may use any format of images such as BMP. It is proved to be an effective application[(9)].

Also we propose a method such that a secret image is shared by *n* shadow images, and any *r* shadow images ($r \leqslant n$) of them can be used to restore the whole secret image. The size of each shadow image is smaller than the secret image in our method. This property gives the benefit in further process of the shadow images, such as storage, transmission, or image([10]).

We propose a new method for invisibly watermarking high-quality color and gray-scale images. This method is intended for use in image verification applications, where one is interested in knowing whether the content of an image has been altered since some earlier time, perhaps because of the act of a malicious party. It consists of both a watermark stamping process which embeds a watermark in a source image, and a watermark extraction process which extracts a watermark from a stamped image. The extracted watermark can be used to determine whether the image has been altered. The processing used in the stamping and extraction processes is presented. We also discuss some advantages of this technique over other invisible watermarking techniques for the verification application; these include a high degree of invisibility, color preservation, ease of de encoding, and a high degree of protection against retention of the watermark after unauthorized alterations

There are many types of HIDING:

2-2-1 A JOINT SOURCE-CHANNEL ENCODING SCHEME FOR IMAGE-IN-IMAGE DATA HIDING[9]

By this technique, we consider the problem of hiding images in images. In addition to the usual design constraints such as imperceptible host degradation and robustness in presence of variety of attacks, we impose the condition that the quality of the recovered signature image should be better if the attack is milder. We present a simple hybrid analog digital hiding technique for this purpose. The signature image is compressed efficiently (using JPEG) into a sequence of bits, which is hidden using a previously proposed digital hiding scheme. The residual error between the original and compressed signature image is then hidden using an analog hiding scheme. The results show (perceptual as well as mean-square error) improvement as the attack becomes milder.

Driven by applications such as steganography, digital watermarking, addition of meta-content, and document authentication, there has been a growing body of work in data hiding (see, for example,
[1, 2, 3, 4, 5, 6], and references therein). We consider the problem of image-in-image hiding in this paper, where, the basic design criteria are as follows:

(a) The degradation to the host image is imperceptible,
(b) It should be possible to recover the hidden, or signature, image under a variety of attacks
(c) The quality of the recovered signature image should be better if the attack is milder.

In recent work [1, 2, 3, 5, 7], it has been shown that digital data can be effectively hidden in an image so as to satisfy criteria (a) and (b) by hiding in the choice of quantize for the host data. The main idea is to view the data hiding problem as communication with channel side information ([8, 9, 4]): the channel experienced by the data comprises of the host interference and the attack, and the channel side information

is the knowledge of the host. Therefore, recent advances in source encoding and channel encoding can be leveraged for developing data hiding schemes.

Unfortunately, these schemes do not satisfy the design criterion (c) - they exhibit the threshold effect: if the actual attack is more severe than the attack the scheme was designed for, there is a catastrophic failure in recovering the hidden image, while if the actual attack is less severe, then we are still stuck with the design attack image quality. In practice, the attack level is seldom known priory, and ideally, we would like a scheme that results in graceful improvement and degradation in the image quality with less and more severe attacks respectively. Such schemes require distortion. One of the goals of joint source-channel encoding is to provide improvement for less severe attacks. For the Gaussian channel (that is, the host is absent), a number of joint source channel encoding methods have been proposed. In

[10], codes based on chaotic systems have been proposed, which recently were shown to have optimal scaling properties in the high signal-to-noise regime in [12]. In [11, 14], hybrid digital-analog codes have been proposed.

However, for the data hiding channel, joint source-channel codes have not been studied so far and a number of issues are open.
In this paper, we exhibit a practical hybrid digital-analog scheme for image-in-image hiding, which is similar to the scheme proposed in [14] for the Gaussian channel. The idea is to compress the signature image efficiently into a sequence of bits, which is hidden using a previously proposed digital hiding scheme [3]. The residual error between the original and compressed signature image
is then hidden using an analog hiding scheme (proposed in Section 3). With practical issues in mind, we focus our attention to JPEG compression attacks instead of the Gaussian attack. We chose to develop a hybrid digital-analog scheme for the following purposes.

- It allows us to exploit advantages of the digital scheme in [2, 3], which hides high volume of data using image-adaptive criteria and turbo-like codes, and is also robust against a variety of attacks.
- Due to the limited dynamic range of the analog residue, it is feasible to send them reliably over a limited number of host symbols.

2-2-1-a HIDING ANALOG INFORMATION

In this section, we propose a strategy to hide an analog number into a host sample. The hiding strategy involves quantization of the host followed by replacing the residue with the appropriately scaled source and is given in Section 3.1. The MMSE decoder is derived in Section 3.2.

2-2-1-b Hiding using scalar quantization of the host

In this section, we tried to hide an analog number *m* into a host sample *h*, we first quantize the host *h* using a quantizer of step size ¢, and then replace the residue with the source *m*, which has been companded or scaled to lie in the interval (0; ¢). Let us consider an example where ¢ = 1 and the host symbol is, say, 6.235. We want to send a source symbol whose value is 0.729 (a real number *2* (0; ¢)) through the hiding channel. The encoder first determines that the host symbol lies between 6 and 7 (an interval (*n*¢; (*n*+1)¢)), then it sends the source symbol directly within that interval, i.e., it just sends 6.729.

In practice, we use a hiding strategy that always *measures* the message *m* from an even reconstruction point of the host. This is done to avoid catastrophic error when a hidden coefficient switches to a different integer interval as a result of attack. Thus, the symbol *y* to be sent for hiding a message *m* into a host symbol *h* is given by,

y = ¢(*bh*=¢*c*) + *m;* if *bh*=¢*c* is even,
= ¢(*bh*=¢*c* + 1) ¡ *m;* if *bh*=¢*c* is odd*:* (2)

Here, *b*¢*c* denotes the floor operation (defined as the largest integer smaller than or equal to the given number)
(ii) Even Crossing: As mentioned above there could be two cases for even crossing, each involving either *n* or (*n* + 1) being even.
The analysis is similar in both the cases and hence we just consider the first case (*n* even). Let us define *R*1 = *n* ¡ (*z* ¡ ±=2) and
*R*2 = (*z* + ±=2) ¡ *n* as the distances between the even crossing point *n*, and, the lower and upper points of the ambiguity interval respectively

2-2-2 JOINT SOURCE-CHANNEL HIDING[9]

To provide a background for joint source-channel encoding, we first briefly consider some fundamental limits for the Gaussian data hiding channel ([8, 9]). Consider an i.i.d. Gaussian signature source with zero mean and variance ¾2, which has to be embedded in a Gaussian host. The hider is at most allowed to introduce a mean square error *D*1 per host symbol. Further, we assume a Gaussian attack (that simply adds i.i.d. Gaussian noise), which introduces an additional distortion of at most*D*2 per host symbol. In general, the host and the signature have different sizes, and so we assume that
½ channel uses per source symbol are allowed. At the receiver, we are interested in recovering the signature with distortion *D*3 per signature symbol. From the information capacity results from [8], and rate distortion theory ([13]), we can easily deduce that,

*D*3 ¸
¾2
_1 + *D*1
*D*2 _½ =: *Dmin:* (1)
Given *D*1, *D*2 and ½, the smallest feasible distortion above can
be approached in principle by separate source and channel encoding.
Unfortunately, such schemes have the drawback that even if the
Gaussian attack channel introduces a distortion less that *D*2, we suffer distortion *Dmin*, though in principle we can have smaller

2-2-2-1 IMAGE-IN-IMAGE HIDING[9]

In this section we describe the actual implementation of the entire system for image-in-image hiding. The encoding process can be divided into following parts.

Processing the signature image: This step involves separating the signature image into digital and analog parts. The image is compressed using JPEG to generate a bit stream, which constitutes the digital part. The analog part is obtained by computing the residual errors of pre-selected DCT coefficients after the quantization based on design *signature* quantization matrix. Note that, the design quality factor, and the number of analog residues chosen to send, are predetermined at the design stage.

Allocating the channels: Here, we allocate the host coefficients (i.e., channel) for the digital and analog parts respectively.

A few low frequency coefficients (other than the DC coefficient) of each 8£8 host block are reserved for the analog channel. Remaining low and/or mid frequency coefficients are dedicated to the digital channel. Thus the decoder would know where to look for analog and digital data respectively.

Hiding the digital part: The digital bit stream is hidden into its allocated channel using the RA-coded Selectively Embedding in Coefficients (SEC) scheme of [2, 3]. The bit stream to be hidden is coded using turbo-like RA code at a low rate. This coded bit stream is hidden into the host coefficients such that a code symbol is *erased at the encoder*, if the floor of its magnitude is smaller than or equal to a predetermined integer threshold. The decoder uses the same threshold criteria to estimate the erasure locations.

The RA code rate is designed in such a way that one can also deal with the additional errors and erasures due to attack.

Hiding the analog part: The analog residues of selected low frequency coefficients are sent through its allocated channel using the hiding scheme of Section 3. Since the residue always lies in [0*;¢sig*), where *¢sig* is specified by the design quantizer, we simply scale it to lie in [0*;* 1).

The decoder decodes the analog and digital parts separately and adds them together to give an estimate of the sent signature image. The de encoding of the analog part is done using the knowledge of attack ±, and assuming a slowly varying host distribution

The digital part is iteratively decoded using sumproduct algorithm. Now we present two example implementations to show that there is an improvement in perceptual quality as well as the mean-squared error (MSE) for the received signature

image as the attack becomes milder. Note that though we present two specific examples here, the scheme is applicable for any image-in image hiding scenario.

Example 1: We hide a 128£128 image into a 512£512 image, with the design quality factor of 25. Figure 1 shows the recovered signature images when the host image undergoes JPEG compression at varying levels, starting from the worst case QF of 25. The signature image is JPEG compressed at QF = 10 to form the digital part and the residues of 16 low frequency coefficients make up the analog part. We use one coefficient from each 8£8 host block for transmitting the analog data. 34 coefficients constitute the *digital channel*.

Example 2: A 256£256 image is hidden with a design QF of 50. Table 1 shows the MSE of the received image after varying levels of JPEG compression. The signature image is JPEG compressed at QF=18, and residues of 12 low frequency coefficients constitute the analog part. 3 coefficients per host block are used for sending analog residue and another 32 coefficients form the candidate embedding band for the digital data.

2-2-3 COLOR IMAGE SCALABLE ENCODING WITH MATCHING PURSUIT[9]

This technique is aimed to present a new scalable and highly flexible color image coder based on a Matching Pursuit expansion. The Matching Pursuit algorithm provides an intrinsically progressive stream and the proposed coder allows us to reconstruct color information from the first bit received. In order to efficiently capture edges in natural images, the dictionary of atoms is built by translation, rotation and anisotropic refinement of a wavelet-like mother function. This dictionary is moreover invariant under shifts and isotropic scaling, thus leading to very simple spatial resizing operations. This flexibility and adaptivity of the MP coder makes it appropriate for asymmetric applications with heterogeneous end user terminals.

Most visual encoding schemes generally first compress luminance image components, and then extend encoding to color components. They use color spaces with luminance and chrominance channels, where the latter may easily be down sampled, due to the fact that they carry much less information than the luminance component. Moreover, in the classical encoding paradigm, decorrelation between channels is generally seen as an advantage. However, when a similar strategy is applied to scalable color image encoding, it often causes colors to only appear after a certain time, or with severe distortion.

Matching Pursuit for Color images

Matching Pursuit (MP) image representation with a dictionary based on anisotropic refinement atoms and Gaussians has proved to give good compression results [3], in addition to intrinsic spatial and rate scalability properties [1]. MP is a greedy algorithm that iteratively chooses the atom of a redundant dictionary that provides the best correlation with the input signal (see [4, 5] for details on the algorithm). Let

D = {gγ}γ Γ be a dictionary of P > M1 ×M2 unit norm vectors. This dictionary includes M1 ×M2 linearly independent vectors that define a basis of the space CM1×M2 of signals of size M1 ×M2. Also, let Rnf be the residual of an n term representation of signal f, with R0f = f. The signal decomposition with MP then can be written as follows:

f =N−1

_

n=0_Rnf, gγn_gγn + RNf, (1)

where gγn is the dictionary vector that maximizes the energy taken from Rnf at every iteration:

|_Rnf, gγn_| = arg max D |_Rnf, gγ_| . (2)

Instead of performing independent iterations in each color channel, a vector search algorithm is used in the proposed color image encoder. This is equivalent to using a dictionary of P vector atoms of the form { _ gγ = [gγ, gγ, gγ]}γ Γ.
In practice though, each channel is evaluated with one single component of the vector atom, whose global energy is given by adding together its respective contribution in each channel. MP then naturally chooses the vector atom, or equivalently the vector component gγ, with the highest energy.

Most of the image encoding techniques use color spaces such as YUV, LAB of CrCbCg. These color spaces have less redundancy among channels than RGB. For example, YUV has all the luminance information in the Y channel, and the U and V channels have less information. LAB and CrCbCg color spaces have the drawback that they have some user defined parameters, not standardized for all the displays.

They do not present the same amount of redundancy among channels as RGB does. The techniques which use the YUV color space generally take profit from the fact that the human eye is less sensitive to color than luminance localization in images, and hence down sample the U and V channels in order to reduce the amount of data. Such a down sampling is not helpful anymore in the context of the proposed MP coder, since the same function is used for the three color channels, in order to limit the encoding cost of atom indexes.

Since, in addition, the use of the same function in Y, U and V channels may induce color distortion; RGB becomes clearly the preferred color space for the MP coder.

2-3 FIDELITY CRITERIA[6]

Objective Fidelity Criteria

In some image-transmission systems some errors in the reconstructed image can be tolerated. In this case a fidelity criterion can be used as a measure of system quality.

Examples of objective fidelity criteria are the root-mean-square (rms) error between the input image and output image and the rms signal-to-noise ratio of the output image. Suppose that the input image consists of the $N \times N$ array of pixels $f(x, y)$, $x, y = 0, 1, \ldots, N - 1$. Each pixel is an m-bit binary word corresponding to one of the 2^m possible gray-level values. The encoder reduces the data bulk from $N \times N \times m$ bits to a fewer number of bits. The decoder processes these bits to reconstruct the output picture consisting of the $N \times N$ array of picture elements $g(x, y)$. $x, y = 0, 1, \ldots, N - 1$. where each pixel is also an m-bit binary word corresponding to one of 2^m possible gray-level values.

For any value of x and y in the range $0, 1, \ldots, N - 1$, the error between an input pixel and the corresponding output pixel is

$$e(x, y) = g(x, y) - f(x, y)$$

$$e^2 = \frac{1}{N^2} \sum_{x=0}^{N-1} \sum_{y=0}^{N-1} e^2(x, y)$$

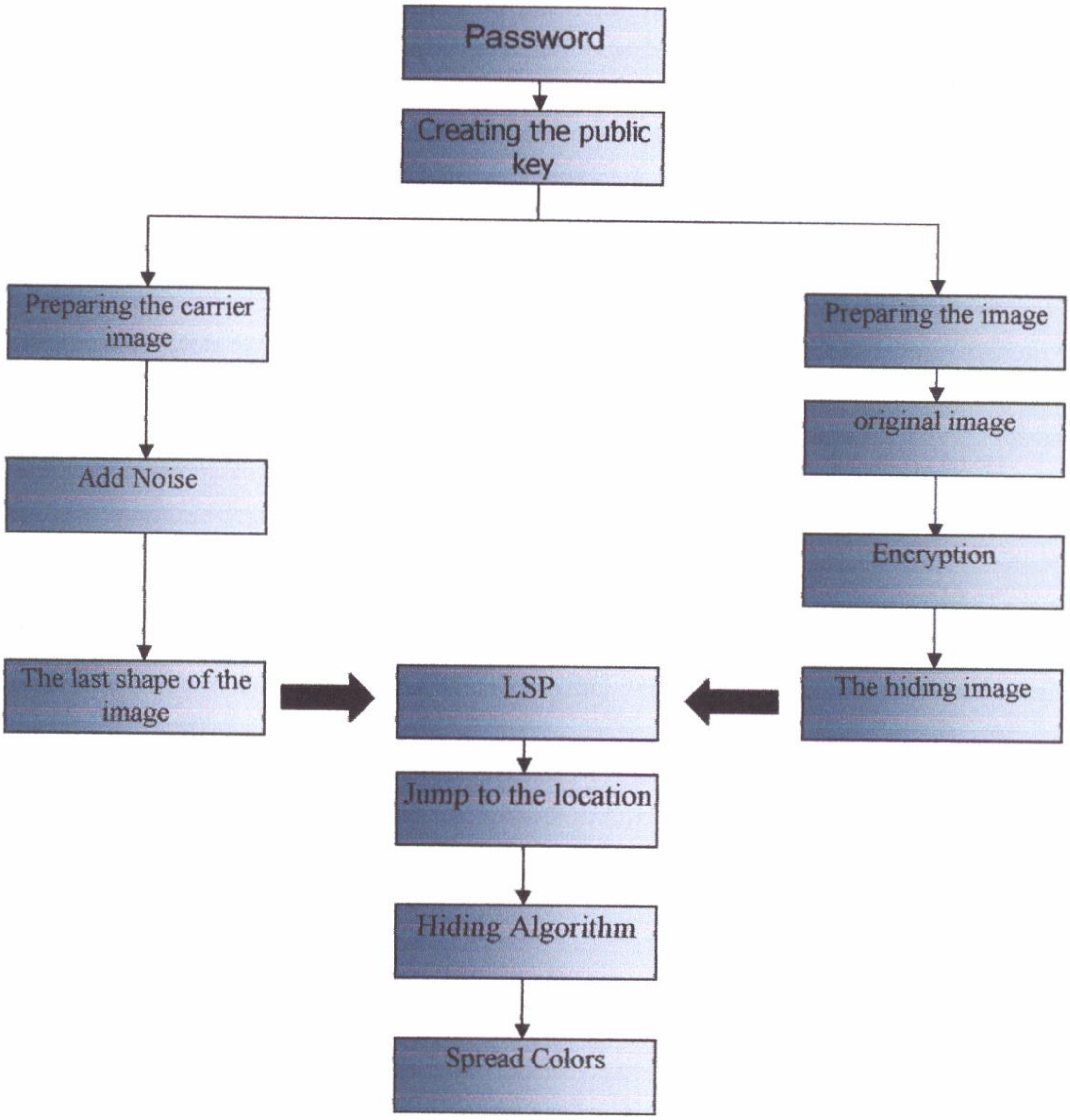
$$= \frac{1}{N^2} \sum_{x=0}^{N-1} \sum_{y=0}^{N-1} [g(x, y) - f(x, y)]^2$$

$$e_{rms} = [e^2]^{1/2}$$

$$g(x, y) = f(x, y) - e(x, y)$$

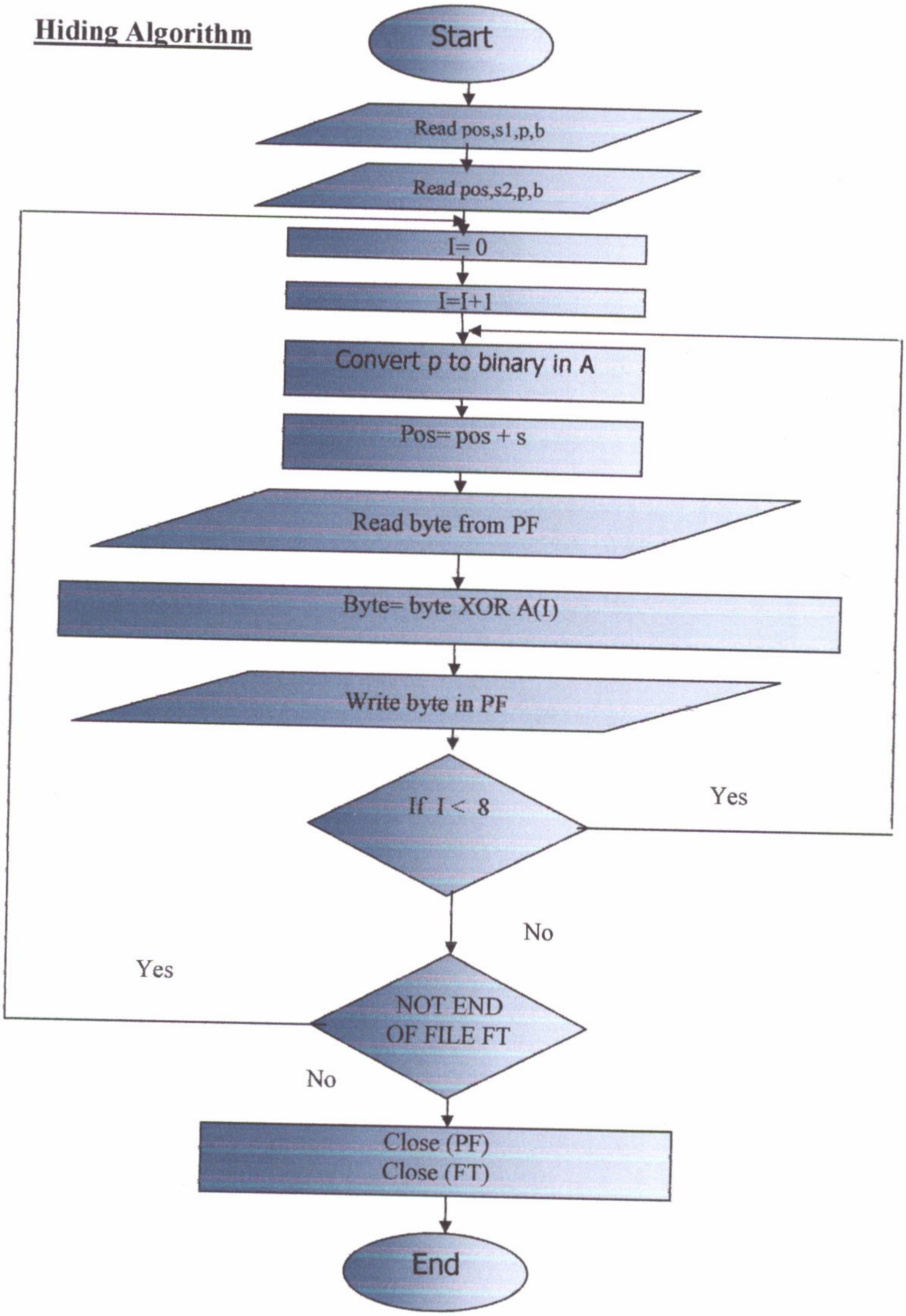
Chapter III

Image Hiding Technique

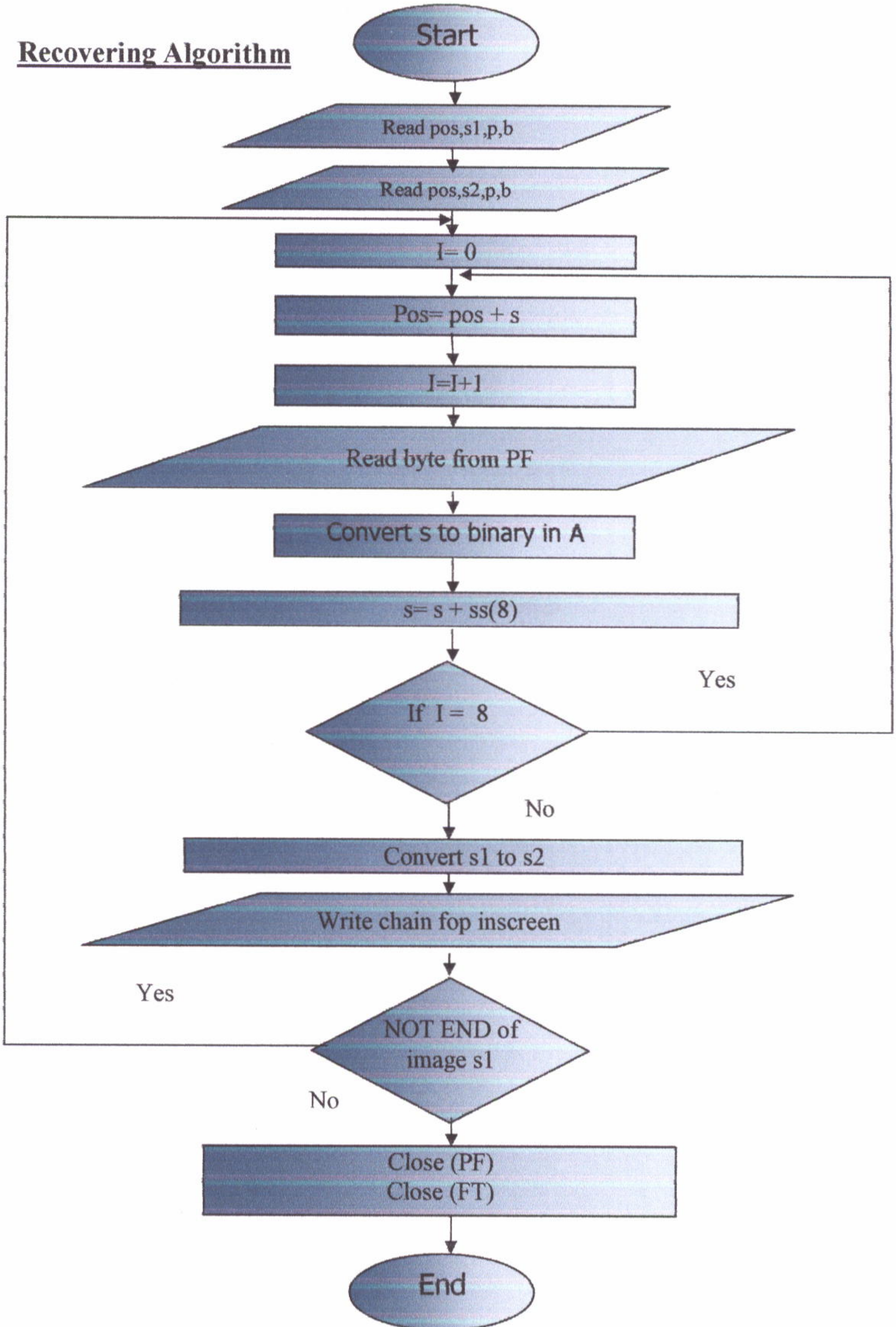


A Flowchart explains Hiding Technique

Hiding Algorithm



Recovering Algorithm



Chapter III
Practical work

3-1 program outputs:-

by using Microsoft Visual Basic ver.6, we implement a program demonstrated three operations:-

a) Encoding operation.
The program starts with the main menu form with selecting an image have (*.bmp) extension. So the Encoding operation gave been applied it.

b) Hiding operation:-
the program starts with an image. So the hiding operation have been applied on it.

c) Appearing operation:-
the hiding will be neglected and the form return to the previous Main Menu form.

By using Microsoft Visual Basic ver.6

Fig (3) The main Menu

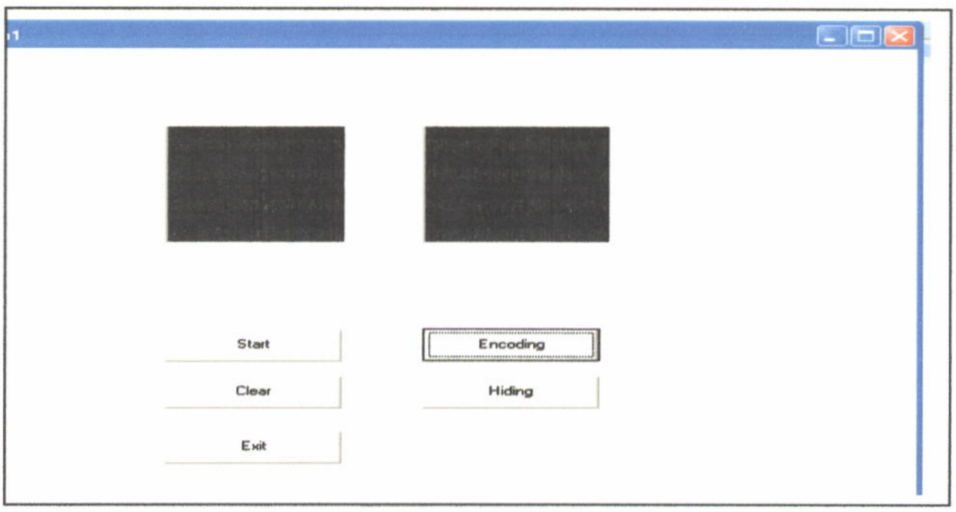
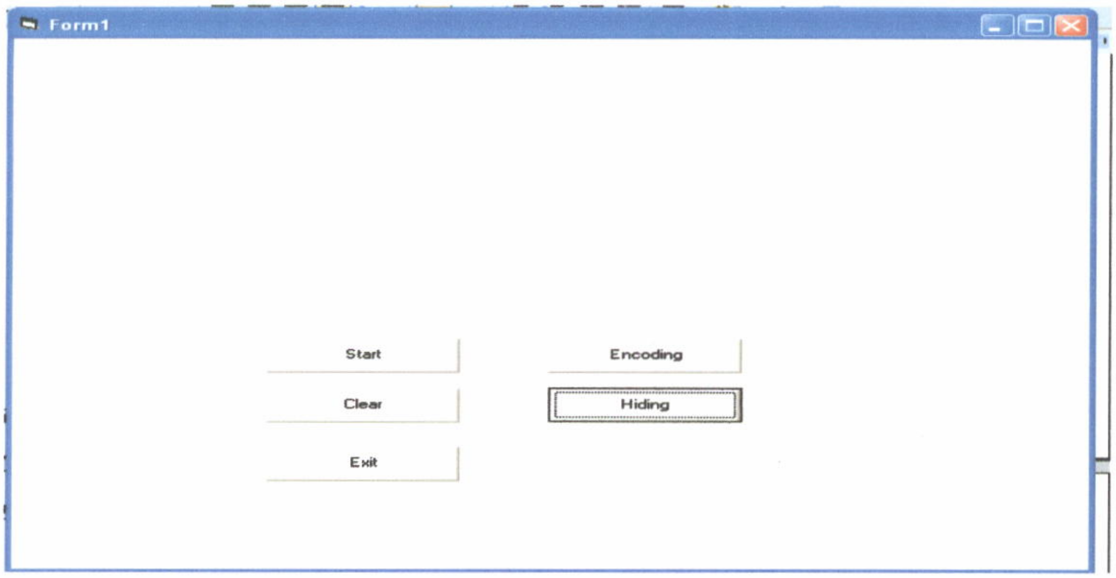


fig (4) Encoding operation



fig(5) hiding operation

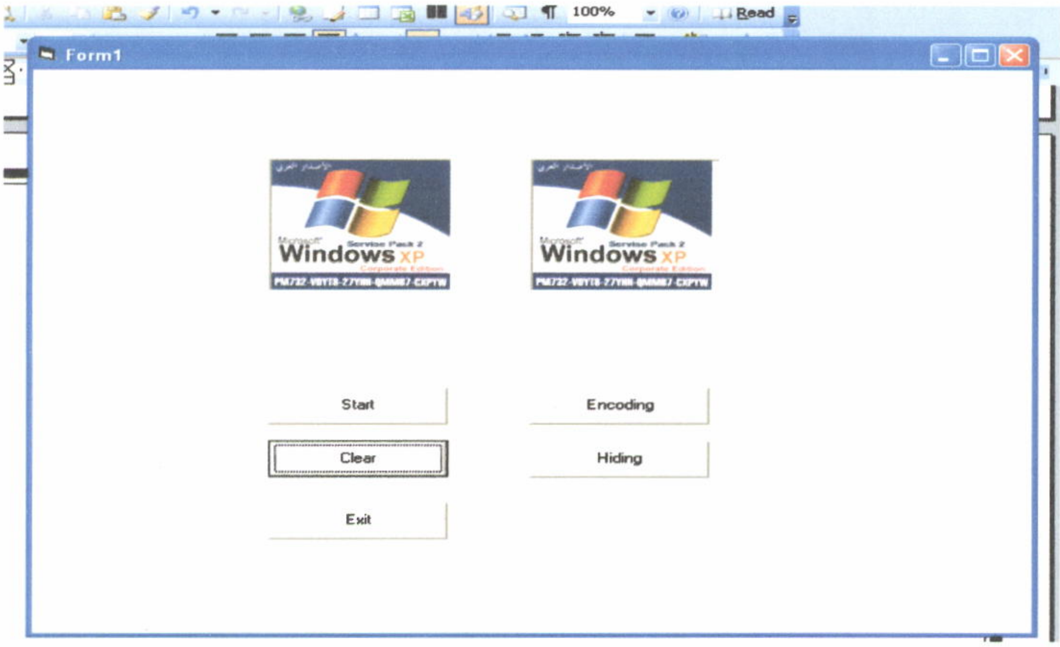


fig (6) Re appearing operation and return to the Main Menu

program code :-

```
On Error Resume Next
Dim c As Long, red As Byte, green As Byte, blue As Byte
Dim i As Integer, j As Integer
For i = 0 To Picture1.Width Step 10
   For j = 0 To Picture1.Height Step 10
c = Picture1.Point(i, j)
red = c Mod 256
red = red - 50
If red < 0 Then red = 0
green = ((c And &HFF00FF00) / 256)
green = green - 50
If green < 0 Then green = 0
blue = ((c And &HFF0000) / 65536)
blue = blue - 50
If blue < 0 Then blue = 0
Picture1.PSet (i, j), RGB(0, 0, 0)
Picture2.PSet (i, j), RGB(0, 0, 0)

Next j
Next i
Private Sub Command4_Click()
On Error Resume Next
Dim c As Long, red As Byte, green As Byte, blue As Byte
Dim i As Integer, j As Integer
Dim a As Long
Picture1.Visible = True
Picture2.Visible = True

End Sub

Private Sub Command5_Click()
On Error Resume Next
Dim c As Long, red As Byte, green As Byte, blue As Byte
Dim i As Integer, j As Integer
Dim a As Long
Picture1.Visible = False
```

Discussion and Concluding

4-1 Concluding Remarks

1) The success of any encoding technique is ultimately dependent on how well it matches the structure (i.e., departure from randomness) in a given image. The, ideal approach in designing an efficient encoder is first to determine the structure of the data and then choose a method that best fits that structure. Since structural properties inherent in pictorial data are not well understood, however, the design and implementation of an image encoder often involves a certain amount of experimentation. The concepts introduced in this chapter are representative of available techniques that have been found of practical value in image-processing applications.

2) In some applications, such as encoding images that exhibit regularity (rivers, man-made objects, etc.), the structural properties of interest often manifest themselves in the form of boundaries. Encoding strategies that take this type of structure into account include the contour-encoding approach are also important. In other applications, such as encoding satellite imagery, the structure is not so obvious, and a typical approach is to let the statistical information in the image dictate the choice of encoding technique. The Hotelling transformation is an example of this approach.

References:

1 -Both color and gray scale secret images hiding in a color image, Author(s) LIN Min-Hui; HU Yu-Chen; CHANG Chin-Chen, Department of Computer Science and Information Management, Providence University, Taichung, 433, TAIWAN, PROVINCE DE CHINE, Department of Computer Science and Information Engineering, National Chung Cheng University, Chiayi, 62107, CHINE, International journal of pattern recognition and artificial intelligence ISSN 0218-0014, 2002, vol. 16, n°6, pp. 697-713 [17 page(s) (article)] (15 ref.),Publisher World Scientific, Singapore, SINGAPOUR (1987) (Revue).

2- Digital image processing, 2nd edition, by Rafael C. Gonzalez- Engineering Dep. University of Tennessee Knoxville, 1987.

3- Electronic Imaging and Multimedia Technology IV. Edited by Li, Chung-Sheng; Yeung, Minerva M. Proceedings of the SPIE, Volume 5637, pp. 477-483 (2005).

4- International journal of pattern recognition and artificial intelligence ISSN 0218-0014, 2002, vol. 16, n°6, pp. 697-713 [17 page(s) (article)] (15 ref.),Publisher World Scientific, Singapore, SINGAPOUR (1987) (Revue),

5- S. J. P. Westen, R. L. Lagendijk and J. Biemond, "Perceptual Image Quality based on a Multiple Channel HVS Model," Proceedings of ICASSP, pp. 2351-2354, 1995

6- D. J. Heeger and P. C. Teo, "A model of perceptual image fidelity," Proc. Of IEEE Int'l Conf. on Image Proc., Oct. 23-26 1995, Washington, D.C., USA, pp. 343-345.

7- S. Lee, M. S. Pattichis, and A. C. Bovik, “Foveated video quality assessment,” *IEEE Trans. Multimedia*, vol. 3, 2001.

8-Marc Antonini, Michel Barlaud, Pierre Mathieu, and Ingrid Daubechies, “Image Encoding Using Wavelet Transform,” IEEE Transaction on Image Processing, vol. 1, no. 2, pp. 205–220, April 1992.

9- A study on information hiding technology in image from SAO NASA ADS Physics Abstract Service, by the Authors: Li, Li; Yao, Zhihai; Wu, Haitao; Dai, Qiang, Affiliation: AA(Changchun Univ. of Science and Technology (China)), AB(Changchun Univ. of Science and Technology (China)), AC(Changchun Univ. of Science and Technology (China)), AD(Changchun Univ. of Science and Technology (China)), Publication: Electronic Imaging and Multimedia Technology IV. Edited by Li, Chung-Sheng; Yeung, Minerva M. Proceedings of the SPIE, Volume 5637, pp. 477-483 (2005). (SPIE Homepage), 02/2005

10 - Secret image sharing, By Chih-Ching Thien and Ja-Chen Lin, Department of Computer and Information Science, National Chiao Tung University, Hsinchu 300, Taiwan, ROC, 4 October 2002

الملخص:

إن معظم تقنيات تشفير الصور التي كانت شائعة في الماضي و منها تلك المستخدمة لإخفاء الصور كانت قد طبقت في الصور القديمة.

إما ألان فان العديد من الصور الرائعة هي صور ملونة.لذا أصبح من الضروري إن يتم تطبيق هذه التقنيات لإخفاء ألوان الصور.

وعليه لن نستخدم خطتنا المقترحة في إخفاء الصور المستضيفة للون فحسب بل للصور القديمة كذلك. و سنستفيد من الجزيئات 3 2 3 في أقصى اليمين للقنوات لكل بكسل للصورة المستضيفة معطيا للجزيئات المتبقية صفرا لغرض توليد الألوان.

بعد ذلك نستخدم هذه الألوان لإجراء تنويع الألوان على الصورة السرية لتحويل وحدات البكسل الخاصة بها من 24 إلى 8 وحدات لونية.

على هذه القيم قبيل ا يتم مزجها بالوحدات 3 2 3 DES(Data Encryption System) ال ثم نقوم بعد ذلك بتشفير لكل بكسل في الصورة المستضيفة. R G B للقنوات النتائج المستوحاة من التجربة تبين انه حتى في أسوأ الحالات فان مخططنا يضمن صورة مستضيفة بمعدل 39.184 من حيث القيمة و صورة ذات قيمة 27,3415 و هي الصورة المسترجعة.