A Simultaneous Implementation of Message Encoding using LSB Stegnography & Image Compression using Lifting Scheme on FPGA

Jondhale S. R.
M.E.(Embedded & VLSI System)
PREC, Pravaranagar

Ansari A. H.
Asst.Professor(E&TC Dept.)
PREC, Pravaranagar

ABSTRACT
The data in digital images can be manipulated to some extend without being detected by human eyes. An example of such manipulations is insertion of secret information which is often referred to as information hiding.In this research we embedded the secret text data in spatial domain of a given 8 bit gray scale image followed by image compression using IWT on hardware Spartan III(XC3S200TQ144-4).A successful information hiding should result in the undistinguishable Stego image to be transmitted via internet as well as the extraction of the hidden data from this Stego image with high degree of data integrity.This research provides a hardware solution for data hiding in 8 bit gray scale image using wellknown LSB Image Stegnography technique,followed by image compression using IWT so as to efficiently utilize network bandwidth for high speed operation.Also it is noticed that at receiver side using Reverse IWT both original image as well as hidden data can be successfully extracted.The design architecture when implemented on FPGA Spartan offers a processing time of just 19.11 Sec for 128*128 gray scale image of bit depth 8 bits which might give an impulse for the researchers to a very fast,programmabale & cost effective hardware solution in the area of Secure Communication.

Keywords
IWT-IntegerWavelet
Transform,JPEG-Joint Photographic Expert Group,FPGA-Field Programmable Gate Arrays.

1. INTRODUCTION
The popularity of the Internet offers a great convenience to the transmission of a large amount of data over networks. Some of them may be secret information which is candidate to unauthorized access.For instance confidential transmission, video surveillance, military and medical applications.In order to keep the unauthorized user away, variety of techniques have been proposed, data encryption and data hiding are two main methods in data security. Data encryption uses a certain algorithm to convert plaintext into cipher text & thus only one who has keys can decrypt the secret data from the cipher texts.However the appearance of cipher texts would give unauthorized user an impulse to recover them.Also the unauthorized users might even simply destroy the ciphertext out of range so that the legal receivers cannot extract the plaintext successfully[1]. That is the reason why data hiding has been currently the hot topic in the area of secure communication. Data hiding techniques embed the important data into multimedia data such as images, videos or sounds. Digital images are considered good cover carriers because of their insensitivity to human visual system. Watermarking and Steganography are two major branches of information hiding technology. Each has its own specific characteristics. When working with larger images of greater bit depth, the images tend to become too large to transmit over a standard Internet connection. In order to display an image in a reasonable amount of time, techniques must be incorporated to reduce the image's file size. These techniques make use of mathematical algorithms to analyse and condense image data, resulting in smaller file sizes. This process is called compression [4]. Image compression is very important for efficient transmission and storage of images.In images there are two types of compression: lossy and lossless [4]. Both methods save storage space, but the procedures that they implement differ.

This research is greatly inspired from the work of authors Rahman Tashakkori & at.al."Message Encoding in Images Using Lifting Schemes"IEEE 2010.But unlike above mentioned work,our research provides a hardware solution for the idea proposed by above mentioned authors. The rest of the paper is organized as follows.The Section II introduces The State Of Art Of Stegnography,section III introduces Image Compression by IWT.The Section IV illustrates Implementation Scheme(hardware & software requirement).The Section V concludes the implementation.

2. THE STATE OF ART OF STEGNOGRAPHY
Steganography is the science that involves communicating secret data in an appropriate multimedia carrier, e.g., image,audio, and video files. It comes under the assumption that if the feature is visible, the point of attack is evident, thus the goal here is always to conceal the very existence of the embedded data.Steganography's ultimate objectives are undetectability, robustness (resistance to various image processing methods and compression) and capacity of the hidden data, are the main factors that separate it from related techniques such as watermarking and cryptography[2],[3]. Images can be used as the transmission of such secure data because the use of digital images has increased rapidly on the Internet. The transmission of images is taking place very frequently on internet and images containing secure data have been also proved to be very useful in many application.

Information Hiding
Characters in the ASCII code can be represented using 8 bits. The values pixels of original image can be manipulated slightly without being noticed by visual inspection[3].This research project is based on the premise that the bits of ASCII characters can be included in each one LSB of pixel of original image without resulting in a visible appearance in the so constructed image.If the number was large, 1028 for example, and the LSB was changed from zero to one, the number would be changed from 1028 to 1029, which is a change of only 0.097%. Pixel values in an 8-bit gray-scale image usually range from zero to 255 inclusive for an 8-bit image. If the LSB of 255 were changed to a zero from a one, the result would be 254, a change of 0.39%. That means

greater the bit depth of an image better would be the quality of manipulated image (i.e. Stego image).

3. IMAGE COMPRESSION BY INTEGER WAVELET TRANSFORM

The wavelet transform has proved to be an indispensable tool in data compression due to its ability to decorrelate data effectively and efficiently.There are basically two types of compression: Lossy & Lossless.Unlike lossless compression,Lossy image compression can provide acceptable image quality while also providing dramatic reductions in image size.However in applicatons where qulity of reconstructed image from compressed one is must, one need to go for lossless image compression method.For example :

- Medical images,
- Seismic data,
- Satellite images,
- Secret Millitary Communication,…etc.

A. Image Format

Digital images are represented interms of integer numbers depending upon the intensity of corresponding pixel of the given image.For the purpose of this research, two test images (parth.bmp & Barbara.bmp) are selected & then using Matlab 7.1 they are converted into gray scale images of 128*128 format with total number of pixels 16384.Each pixel in these gray scale image has a bit depth of 8. A bit depth of 8 means that each pixel can contain a value in the range 0 to 255. The usual bit depths are 8 and 16 with 8 being the most common; however, other bit depths are possible. For this research, a bit depth of 8 was used for test images.

B. Image Entropy

The definition of entropy is the measure of disorder or randomness in a closed system [4]. When applied to digital images, entropy is a measure of the amount of detail in the image. The application created from this research, computes an entropy value of the test images. The entropy value can be useful because it can provide an idea of how much detail is in the image before the user adds 'noise' to the image by inserting a message. Adding a message to an image modifies some of the bits of the pixels, thus modifying the randomness of the image as well. The entropy is calculated using equation 3.1 as shown below.

$$Entropy = \sum_{j} \Pr(aj)\, log2\,[\Pr(aj)] \qquad (3.1)$$

where *aj* represents the *jth* unique intensity value observed in a reading of the images pixel values and Pr(*aj*) is the probability of that pixel value occurring within the image.At the end experimentation on several images we came to a conclusion that higher the entropy of given image,least noticeable would be the change in its quality after data hiding.

C. Lifting Scheme

In order to reduce complexities of the design, linear algebra view of DWT(i.e. IWT and Reverse IWT) has been used.Unlike traditional WT,IWT does computation in place making the implementation much simpler.Similar to wavelet transformations, lifting schemes break a signal, the image, into its component parts 'trends' that approximates the original values and 'details' which refers to the noise or high frequency data in the image. A lifting scheme produces integers and this allows the original space to be used to hold the results [6].

To separate the trends from the details as two component signals, a permutation step is done. When applied to a row of data, permutation moves all the trend pixels to the left, and the detail pixels to the right. This produces a meaningful view of the data. Because images are stored as two dimensional arrays, applying lifting schemes and permutations as described above must be done in two dimensions, once for rows and once for columns [6].

This research makes the use of Haar based Lifting Scheme. The Haar lifting calculation of the details and the trends for row *i* are shown in 3.2 and 3.3, respectively[8].

Detail:

$$S_{i,2j+1} = S_{i,2j+1} - S_{i,2j} \;, j=0,1,\ldots n/2 \quad (3.2)$$

Trend:

$$S_{i,2j} = S_{i,2j} + (S_{i,2j+1})/2, \; j=0,1,\ldots n/2 \quad (3.3)$$

These calculations are done in the order shown above because the detail value calculated in 2.2 is used in the second term of 2.3. Lifting schemes can be applied on a signal more than once in successive applications of the transformation which are known as levels of transformation. In this research we are applying single level decomposition of given image**.**The Inverse transformation for the Haar lifting scheme is shown in 3.4 and 3.5[8].

Inverse Trend :

$$S_{i,2j} = S_{i,2j} - (S_{i,2j+1})/2, \; j=0,1,\ldots n/2 \quad (3.4)$$

Inverse Detail :

$$S_{i,2j+1} = S_{i,2j+1} + S_{i,2j} \;, j=0,1,\ldots n/2 \quad (3.5)$$

Advantages of lifting scheme

- Allows a faster implementation of the wavelet transform,
- Saves storage by providing an in- place calculation of the wavelet transform,
- Simplifies determining the inverse wavelet transform,
- Provides a natural way to introduce and think about wavelets.

The main difference with classical constructions is that it does not rely on the Fourier transform[6],[7]. Due to this reformulation, second generation wavelets can be constructed. Second generation wavelets, unlike traditional, first generation wavelets, are not necessarily translates and dilates of a function. In this way, wavelets can be applied to non- smooth domains and curves or surfaces.

4. IMPLEMENTATION SCHEME

This design implementation required XPS EDK 10.1 software platform along with Matlab 7.5 & Visual Basic Studio 6 to display images on computer screen. The conversion of true color image into gray scale image as well as resizing of image into (128 * 128) format was carried out using Matlab 7.5 Image Processing Toolbox. While coding of our design which include LSB encoding,Forward IWT,LSB decoding & Reverse IWT, was carried out using Impulse C Language in XPS EDK 10.1.The Top-Down Approach followed with the use IP core Microblaze (32 bit RISC Processor) yields Fig.3
This implementation first hides bits of secret message in the whole original gray scale *.bmp test image of size 128*128 ,followed by IWT at single level decomposition to produce LL,LH,HL & HH bands each of size 64*64. Hiding the bit in

the image was accomplished by overwriting the selected bits of a pixel with the value of the bit. This was done by performing a bitwise AND operation of each one LSB of pixels of original image with 0, which effectively set all LSB bits to 0. Then the bit of secret message to be hidden in this pixel was then combined with the pixel by a bitwise OR operator, effectively setting these pixel bits to the message bits.

The processing steps are described below at macroscopic level , followed by detail of each.The whole process flow is shown in fig.1.

Step I : First Resize the given true colour image into standard 128*128 form.Then convert it into gray scale form (i.e. arrange the given image into Equivalent Matrix Domain or Header File) as shown in fig.3(a) & fig.4(a)
e.g. parth.jpeg is converted to gray scale parth.bmp

Step II : Hide given secret text message at one LSB of each pixel of parth.bmp using LSB Stegnography to produce Stego Image as shown in fig.3(b) & fig.4(b).

Step III : Apply Haar Wavelet based Lifting Scheme of Wavelet Transform (IWT) on Stego image produced in step II to yield single level decomposition of Stego image into four Bands labeled LL[64][64] , LH[64][64] ,HL[64][64] & HH[64][64] as shown in fig.3(c) & fig.4(c)Now send these bands to destination serially over internet.

Step IV : At destination side apply decoding process to extract secret message hidden from compressed image obtained in Step III

Step V : Apply Reverse WT on compressed image obtained in step III so as to reconstruct the original image as shown in fig.3(d) & fig.4(d).

Transformation Level & Message Hiding Capacity

The Levels of transformation determine how much processing to be done on the given image before the message hiding.The transformation level & Lifting Tech used for WT together determines the maximum size of message that can be encoded in given image.If secret message encoding is done after IWT,then maximum size of message can be calculated using following equations.

$$max=(w*h)/4^{(n+1)} \quad (4.1)$$

$$max=3(w*h)/4^{(n+1)} \quad (4.2)$$

Where n is transformation level and w and h represents the number of pixels along the width & height of four bands produced after forward IWT.If the trend section of distorted image is used to hide the message,then maximum message size can be calculated using equation 4.1 while if detail section is used,then it can be calculated using equation 4.2.
This research implementation as apply LSB stegnography prior to image compression (Spatial Domain Image Stegnography rather than Transform Domain),we could hide as many secret message bits as number of available pixels in selected test images.Therefore the message hiding capacity of our image "parth.bmp" & "barbara.bmp" of 128*128 format is 16384 bits.But we recommend to hide less message bits in given *.bmp file depending upon its entropy value,as its quality degrades as we try to attempt its full message hiding capacity.Further security can also be enhanced by sending this Stego image among several other such *.bmp images over the internet & conveying the occurance of our Stego image to the authorized recipient in advance so as to increase the security level.

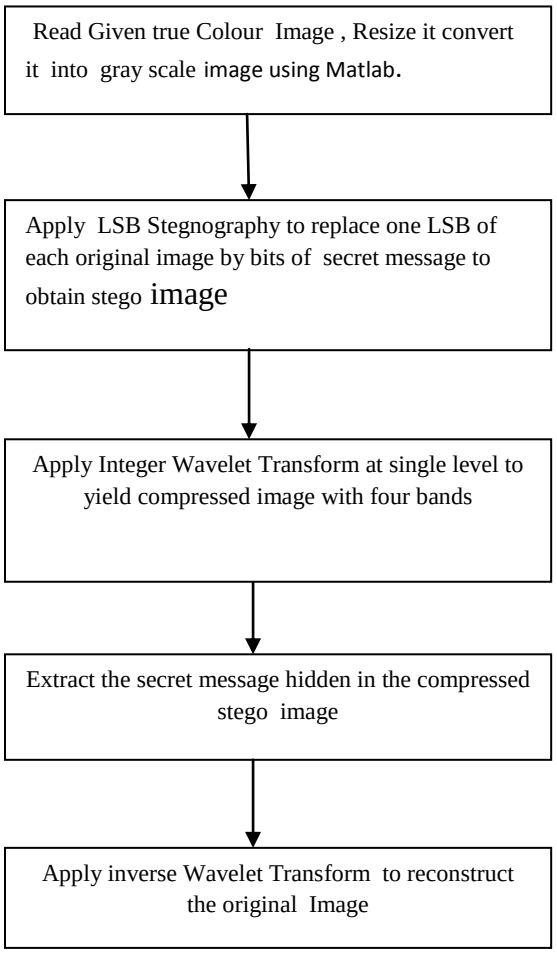

Fig.1 The Process Flow

5. CONCLUSION

From experimental results we observe that Stego barbara image(entropy=7.4614)shows least noticeable change in its quality as compared to Stego parth image(entropy=6.6076). That is why after hiding 27 ASCII characters in these two test images,stego image of parth.bmp shows more noticeable blurring at the contours & edges than that in Barbara.bmp. Thus the entropy of the image plays a major role in determining how suitable an image is for information hiding.Also we successfully recovered the secret data hidden from the Stego images at receiver end.By employing Top-Down approach in Spartan XC3S200TQ144-4 ,the observed total CPU time to XST completion was just 19.11 seconds with the total memory requirement of just 188.152 Mbytes as shown by device utilization summary in Table.1.

6. REFERENCES

[1] B. Weaver, Now You See It, Scientific Computing 24.6 (May 2007): 18-39.

[2] B. Glass, Hide in Plain Sight, PC Magazine 21.18 (15 Oct. 2002): 75.

[3] Tucker, Patrick. "Hiding Secrets in Computer Files." Futurist 40.5 (Sep. 2006): 12-12.

[4] R. Gonzales, and R. Woods, Digital Image Processing, Addison Wesley Publishing Co.1993.

[5] W. Sweldens, Building Your Own Wavelets at Home, Wavelets in Computer Graphics, ACM SIGRAPH Course Notes, 1996.

[6] A. Calderbank, I. Daubechies, W. Sweldens, and B. Yeo, Wavelet Transforms that Map Integers to Integers, Mathematics Subject Classification, 42C15, 94A29, 1996.

[7] I.Daubechies & W.Sweldens,Factoring Wavelet Transforms into Lifting Steps.Technical Report Bell Laboratories,Lucent Technologies ,1996.

[8] Rahman Tashakkori,Christopher D.Scholar,"Message Encoding in Images Using Lifting Schemes",IEEE 2010.

Device Utilization Summary :

Table 1. Device Utilization Summary for message hiding of 27 ASCII Characters in test images parth.bmp & barbara.bmp using Spartan XC3S200TQ144-4 .

Elements in FPGA	Amount Utilized	Amount Available	% Utilization
Number of Slices	1880	1920	97 %
Number of Slice Flipflops	2118	3840	55 %
Number of 4 Input LUT's	2971	3840	77 %
Number of Bonded IOB's	62	97	63 %
Number of BRAM's	4	12	33 %
Number of MULT18X18s	3	12	25 %
Number of DCMs	1	4	25 %
Number of GCLKs	4	8	50 %

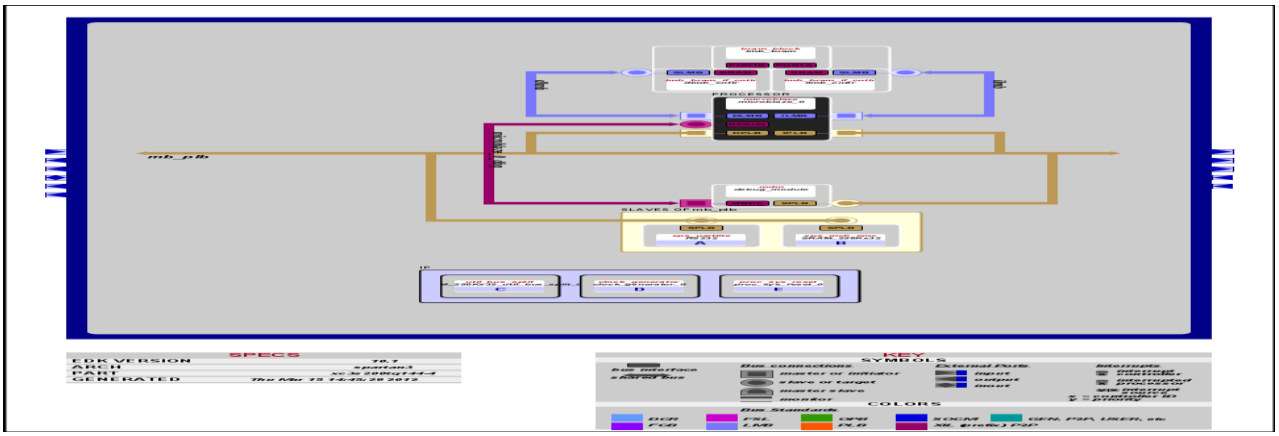

Fig. 2 Implementation Scheme employing Hard Core of Microblaze Processor in XPS Software XPS : Xilinx Platform Studio including XPS EDK 10.1

			
Fig.3(a) Original Image " parth.bmp"	**Fig.3(b) Stego Image after hiding 27 ASCII Characters of Secret Message.**	**Fig.3(c) Stego Image after IWT**	**Fig.3(d)Image extracted from Fig.4(c) by applying reverse IWT**

			
Fig.4(a) Original Image " barbara.bmp"	**Fig.4(b) Stego Image after hiding 27 ASCII Characters of Secret Message.**	**Fig.4(c) Stego Image after IWT at single level decomposition**	**Fig.4(d)Image extracted from Fig.4(c) by applying reverse IWT**