International Journal of Engineering Research and Applications (IJERA) ISSN: 2248-9622
International Conference on Industrial Automation and Computing (ICIAC-12-13th April 2014)

RESEARCH ARTICLE OPEN ACCESS

Digital Image Steganography Using Integer Wavelet Transform On ARM Processor Platform

Mr. Omkar A. Mane*, Dr. S. M. Deokar**
*(Department of Electronics & Telecommunication, Sinhagad Institute of Technology & Science, University of Pune, Pune-41
Email: mane_omkara@yahoo.com)
** (Head of Department, Department of Electronics & Telecommunication, Sinhagad Institute of Technology & Science,
University of Pune, Pune-41
Email: smd_1876@rediffmail.com)

ABSTRACT
Being in an information age lots of information such as images, audios, and videos is being shared or communicated via mobile phones. Steganography technique is not new to the world and lots of development is being done all around the globe. While sharing highly confidential data on internet or by any other means, we need to take care that it is not used by unwanted person because such data only intended for particular person or organization. It is easy to think of ARM processor as integral part of high end mobile phones. This paper proposes a secure image Steganography technique to hide a secret image using the key. The secret image itself is not hidden, instead a key is generated and the key is hidden in the cover image. Using the key the secret image can be extracted. Integer Wavelet Transform (IWT) is used to hide the key. So it is very secure and robust because no one can realize the hidden information and it cannot be lost due to noise or any signal processing operations. We have used Samsung's S3C6440 processor for our project. Our Embedded system uses ARM 32 bit Microcontroller has feature of image/video processing by using various features. Experimental results show very good Peak Signal to Noise Ratio (PSNR), which is a measure of security. In this technique the secret information is hidden in the middle bit-planes of the integer wavelet coefficients in high frequency sub-bands.
Keywords **-** DWT, IWT, PSNR, S3C6410 controller, Steganography.

I. INTRODUCTION

Information security is very important for confidential information exchange. Steganography and cryptography are two ways of achieving secret information exchange. Steganography is different from cryptography. In cryptography, the information is unintelligible while steganography attempts to hide the existence of the information. Research in steganography has mainly been driven by a lack of strength in cryptographic systems. Many governments have created laws to either limit the strength of a cryptographic system or to prohibit it altogether, forcing people to study other methods of secure information transfer. Steganography finds application in defense, police department, detective investigation department, medical field etc. Businesses have also started to realize the potential of steganography in communicating trade secrets or new product information. Avoiding communication through well known channels greatly reduces the risk of information being leaked in transit. Hiding information in a photograph of the company picnic is less suspicious than communicating an encrypted file. The main purpose of steganography is to convey the information secretly by concealing the very existence of information in some other medium such as image, audio or video. The content used to embed information is called as cover object. The cover along with the hidden information is called as stego-object [1]. In this paper grey scale images are considered for both cover object and secret information. The secret image is hidden by generating a key and Integer Wavelet Transform (IWT) is used to hide the key. In steganography transform domain techniques have the advantage of withstanding signal processing operations.

1.1 Discrete Wavelet Transform in Images

Discrete Wavelet Transform (DWT) transforms discrete signal from the time domain into time frequency domain. The transformation product is set of coefficient organized in the way that enables not only spectrum analysis of the signal but also spectral behavior of the signal in time. The wavelet transform has emerged as a cutting edge technology, within the field of image compression. Wavelet-based coding provides substantial improvements in picture quality at higher compression ratios. [2] Fig. 1 shows the 2D DWT for image at various levels

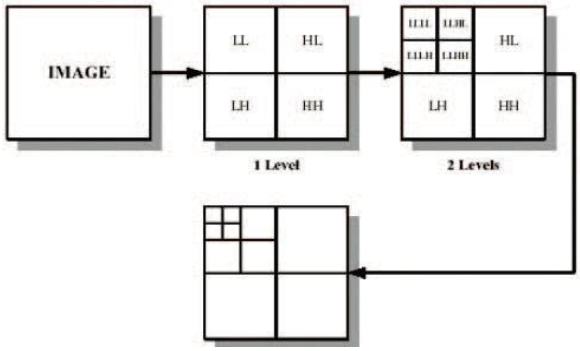

Fig 1: Two dimensional DWT for images

When DWT is applied to an image it is decomposed into 4 sub bands: LL, HL, LH and HH. LL part contains the most significant features. So if the information is hidden in LL part the stego image can withstand compression or other manipulations. But sometimes distortion may be produced in the stego image and then other sub bands can be used.

1.2 Integer Wavelet Transform

Integer Wavelet Transform (IWT) is a more efficient approach to lossless compression. The coefficients in this transform are represented by finite precision numbers which allows for lossless encoding. This wavelet transform map integers to integers. In case of DWT, if the input consists of integers (as in the case of images), the resulting output no longer consists of integers. Thus the perfect reconstruction of the original image becomes difficult [4]. If the original image (I) is X pixels high and Y pixels wide, the level of each of the pixel at (i,j) is denoted by $I_{i,j}$.

The IWT coefficients are given by

$$LL_{i,j} = [\ (I_{2i,\,2j} + I_{2i+1,\,2j})\ /2\ ] \quad (1)$$

$$HL_{i,j} = I_{2i+1,\,2j} - I_{2i,\,2j} \quad (2)$$

$$LH_{i,j} = I_{2i,\,2j+1} - I_{2i,\,2j} \quad (3)$$

$$HH_{i,j} = I_{2i+1,\,2j+1} - I_{2i,\,2j} \quad (4)$$

The inverse transform is given by

$$I_{2i,\,2j} = LL_{i,j} - [\ HL_{i,j}/2\ ] \quad (5)$$

$$I_{2i,\,2j+1} = LL_{i,j} + [\ (HL_{i,j}+1)/2\ ] \quad (6)$$

$$I_{2i+1,\,2j} = I_{2i,\,2j+1} + LH_{i,j} - HL_{i,j} \quad (7)$$

$$I_{2i+1,\,2j+1} = I_{2i+1,2j} + HH_{i,j} - LH_{i,j} \quad (8)$$

where, $1 \le i \le X/2$, $1 \le j \le Y/2$ and [] denotes floor value.

The major objective of steganography is to prevent some unintended observer from stealing or destroying the confidential information. There are some factors to be considered when designing a steganography system: [1]

• Invisibility: Invisibility is the ability to be unnoticed by the human.

• Security: Even if an attacker realizes the existence of the information in the stego object it should be impossible for the attacker to detect the information. The closer the stego image to the cover image, the higher the security. It is measured in terms of PSNR.

$$PSNR = 10\log_{10}\frac{L^2}{MSE} \quad (9)$$

where L = maximum value, MSE = Mean Square Error.

$$MSE = \frac{1}{MXN}\sum_1^M \sum_1^N (f_{ij} - g_{ij})^2 \quad (10)$$

where X = original value, X' = stego value and N = number of samples.

High PSNR value indicates high security because then the difference between the original and stego values is minimum. So no one can suspect the hidden information.

• Capacity: The amount of information that can be hidden relative to the size of the cover object without deteriorating the quality of the cover object

• Robustness: It is the ability of the stego to withstand manipulations such as filtering, cropping, rotation, compression etc.

II. SYSTEM DESIGN MODEL

In this project we going use S3C6410 based microcontroller, which is the current dominant microcontroller in mobile based products. To reduce total system cost and enhance overall functionality, the S3C6410X includes many hardware peripherals such as a Camera Interface, TFT 24-bit true color LCD controller, System Manager (power management & etc.), 4-channel UART, 32-channel DMA, 5-channel 32bit Timers with 2PWM output, General Purpose I/O Ports, I2S-Bus interface, I2C-BUS interface, USB Host, USB OTG Device operating at high speed (480Mbps), 3-channel SD/MMC Host Controller and PLLs for clock generation etc. as shown in figure 2.

S3C6410 is a Samsung company's microcontroller. This microcontroller works for an voltage of +3.3V DC and at an operating frequency of 533 MHz. The maximum frequency up to which this micro controller can work is 667 MHz. We cannot get S3C6410 microcontroller individually. We will get it in the form of FRIENDLY ARM board otherwise we can call it as MINI 6410 board.

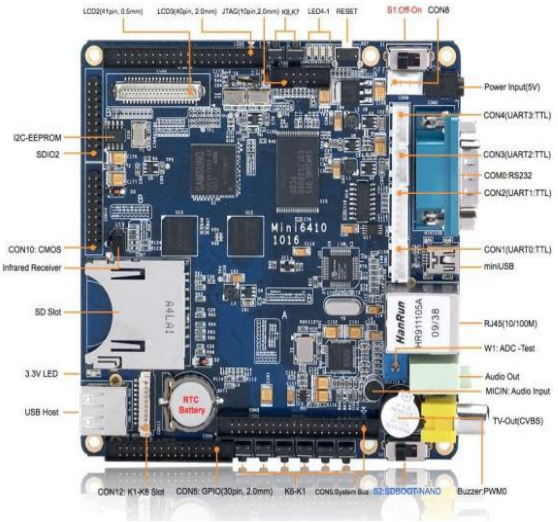

Fig 2: MINI 6410

In this project, OV9605 Color CMOS camera is used as an image-capture device; TFT LCD is used for displaying captured image as well as for inputting text data in order to hide the message into an image and after creating an stego image it is transferred to PC using USB. SD card is used for storing images. As shown in Figure 3, system block diagram of the encoder

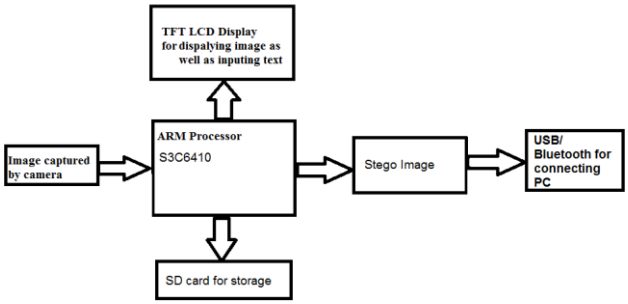

Fig 3: Block diagram for encoder

Similarly, Stego image can be received from computer connected to ARM which will be displayed on TFT LCD and the hidden text message is retrieved and is displayed on the same LCD. The system block diagram for decoder is shown in Figure 4.

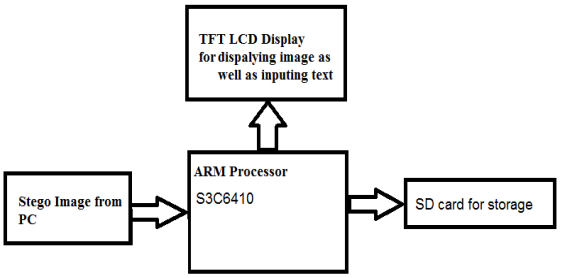

Fig 4: Block diagram for decoder

2.1 Software module implementation

In order to work with ARM 11 micro controllers we require 3 things. They are listed below:

1. Boot Loader
2. Kernel
3. Root File System

2.1.1 Boot loader:

The main functionality of boot loader is to initialize all the devices that are present on the mother board of MINI 6410 and at the same time to find out whether any problem or any other fault is there in the devices that are present on that mother board of MINI 6410. The other feature of the boot loader is to find out what are the different operating systems that are present in the standard storage devices and to show it on to the display device so that user can select between the operating systems into which he wants to enter. One other feature of the boot loader is to load operating system related files byte-by-byte into the temporary memory like RAM. In our current project we are using boot loader like Super vivi which is MINI 6410 specific.

2.1.2 Kernel:
The core part of an operating system we call kernel. Operating system will perform its functionalities like File management, Process management, Memory management, Network management and Interrupt management with the help of the kernel only. Kernel holds the device related drivers that are present on the motherboard. FRIENDLY ARM board supports for operating systems like SYMBION, ANDROID, EMBEDDED LINUX, WIN CE. But in all these operating systems EMBEDDED LINUX will provide high security to drivers and files. So in our current project we are making use of kernel of EMBEDDED LINUX with which device related drivers that are present on the mother board of FRIENDLY ARM board will automatically come when we load EMBEDDED LINUX related kernel.

2.1.3 Root File System:
File system will tell how the files are arranged in the internal standard storage devices. In embedded Linux, kernel treats everything as a file even the input and output devices also. In embedded Linux, Root is the parent directory it contains other sub directories like dev, lib, home, bin, sbin, media, mnt, temp, proc, etc, opt and etc. According to our application we will interface some external devices also. All the devices means internal devices that are present on the motherboard of MINI 6410 will get their corresponding drivers when we load Embedded Linux related kernel. But these device drivers require micro controller related header files and some other header files which will be present in the lib directory which is present in the root directory and also the devices related driers will be present in the device directory which is again present in the root directory. So whenever we will load the Root File System then we will get different directories which will be helpful to the kernel. So compulsorily we need to load the Root File System. MINI 6410 specific Root File System is Root Qtopia.

The essential programs that are required in order to work with MINI 6410 like Boot loader, Embedded Linux related Kernel, Root File System will be loaded into the NOR flash which is present on the MINI 6410 board itself. The program that is related with the application will be loaded into NAND flash which is also present on the MINI 6410 board itself. By using boot strap switch that is present on the MINI 6410 will help the user to select either NOR or NAND flash. After that by using DNW tool we can load Boot loader, Embedded Linux related kernel and Root File System into NOR flash by using USB cable and the application related program into NAND flash.

Once loading everything into MINI 6410 board it will work based on the application program that we have loaded into the NAND flash. Now the USB type camera will be interfaced to the MINI 6410 board itself. The camera will capture the image and stores into the internal memory of the micro controller. We select another image from the SD card as a cover image. We hide secrete i.e captured by camera in real time into a cover image. The processor performs IWT over an image.

III. PROPOSED ALGORITHM

In this paper the watermarking technique used in [3] is applied to steganography. The cover image considered is grayscale image of size 256X256 and the secret information is also greyscale image of size 128X128. To transfer the secret image confidentially, the secret image itself is not hidden, instead a key is generated and the IWT is used to hide the key in the cover image.

3.1 Key Generation

The following steps are used to generate a key for the secret image:

• Obtain single level 2D DWT of the cover-image C and secret-image S.

• The resulting transformed matrix consists of four sub-bands CLL, CHL, CLH and CHH and SLL, SHL, SLH and SHH obtained by transforming images C and S respectively.

• The sub-images CLL and SLL are subdivided into non-overlapping blocks BCk1 ($1 \leq k1 < nc$) and BSi ($1 \leq i < ns$) of size 4x4 where nc, ns are the total number of non-overlapping blocks obtained from sub-images CLL and SLL respectively.

• Every block BSi, is compared with block BCk1. The pair of blocks which have the least Root Mean Square Error (RMSE) is determined. A key is used to determine the address of the best matched block BCk1 for the block BSi.

Then IDWT is applied to get cover C

3.2 Key Embedding using IWT

The generated key is hidden in the cover using the watermarking technique proposed in [3] using IWT.

Since in steganography, the cover image is not required at the receiver once the secret information is extracted, some of the bit planes of the transformed coefficients of the cover can be entirely modified to hide the secret information. This increases the hiding capacity. In order to increase the robustness and security the middle bit planes of the higher frequency components of the transformed cover image are used. The steps to hide the key are as follows:

• Find the integer wavelet transform of the cover image

• Construct the binary image using the middle bit planes of the higher frequency components of the transformed image

• Compress the Key

• Replace the middle bit planes of the higher frequency components of the transformed image by the bits of the compressed key.

• Obtain the inverse IWT of the resulting image to get the stego image.

The embedding process is explained graphically in Fig. 5

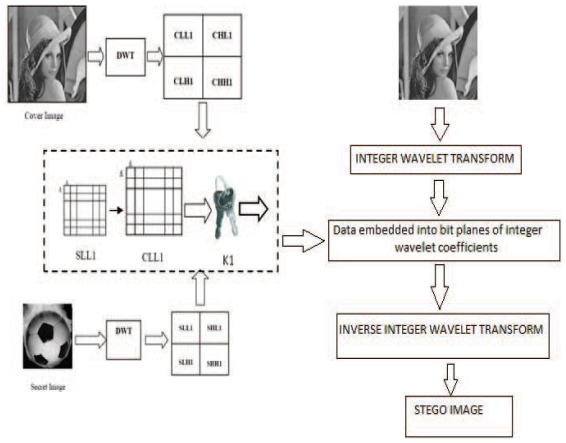

Fig 5. Embedding process.

The extraction process also consists of two steps:

3.3 Key Extraction

The steps are as follows:

• Find the integer wavelet transform of the stego image

• Construct the binary image using the middle bit planes of the higher frequency components of the transformed image

• The middle bit planes of the higher frequency components contain the compressed key.

• Decompress it to obtain the original key

3.4 Secret Image Generation

• Transform the stego-image into single level 2D DWT.

• This transformation results in four sub-bands GLL, GHL, GLH and GHH.

• Divide the sub-band image GLL into 4x4 non-overlapping blocks. The key is used to obtain the blocks that have the nearest approximation to the original blocks in secret image.

• The obtained blocks are then rearranged to obtain the sub-band image SLLnew. Assuming SHLnew, SLHnew, SHHnew are zero matrices of dimension similar to SLLnew , 2D IDWT is obtained.

• The resultant image is the secret image S.

IV. EXPERIMENTAL RESULTS

The cover image considered is Lena with dimensions 512x512 and the secret image is the image capured in real time with dimensions 128x128. All the images under consideration are grey scale. Fig. 6 shows the cover images and secret image while Fig. 7 shows the stego image and extracted image.

Fig 6: (a) Cover image : Lena (b)Secret image

Fig 7: (a) Stego image (b) Extracted Secret image

Table 1: PSNR values (in dB) of the stego-image wrt the cover image and PSNR values (in dB) of the extracted secret-image wrt the original secret image

PSNR values (in dB) of the stego-image wrt the cover image	26.0480
PSNR values (in dB) of the extracted secret-image wrt the original secret image	27.5819

The secret images of size 256X256 can be used with the proposed technique. With 128X128 as the dimension for secret image it takes an execution time of nearly 8 seconds.

V. CONCLUSION

In this paper, a secure image steganography technique is proposed to hide images using ARM processor, which also tells how to hide data bits. The experimental results show that the technique produces good quality stego images with good PSNR values with reasonable execution time

REFERENCES

Journal Papers:

[1] Samir K Bandyopadhyay, Debnath Bhattacharyya, Debashis Ganguly, Swarnendu Mukherjee and Poulami Das, *A Tutorial Review on Steganography* (IC3–2008 UFL & JIITU, p. no. 105-114).

[2] V.Srinivasa rao, Dr P.Rajesh Kumar, G.V.H.Prasad, M.Prema Kumar, S.Ravichand, *"Discrete Cosine Transform Vs Discrete Wavelet Transform: An Objective Comparison of Image Compression Techniques for JPEG Encoder"*, International Journal of Advanced Engineering & Applications, Jan. 2010.

Transaction Paper:

[3] Guorong Xuan, Jiang Zhu, Jidong Chen, Yun Q. Shi, Zhicheng Ni and Wei Su, *"Distortionless data hiding based on integer wavelet transform"*, IEEE Electronic letters, December 2002 Vol. 38 No. 25, pp.1646-1648.

Journal Paper:

[4] M. F. Tolba, M. A. Ghonemy, I. A. Taha,, A. S. Khalifa *"Using Integer Wavelet Transforms in Colored Image-Stegnography"*, International Journal on Intelligent Cooperative Information Systems, Volume 4, July 2004,pp 75-85.

Conference Paper:

[5] Hemalatha S, U. Dinesh Acharya, Renuka A, Priya R Kamath, *"A Secure Image Steganography Technique Using Integer Wavelet Transform"*, 2012 World Congress on Information and Communication Technologies, IEEE 2012