ISSN: 0975-8585

Research Journal of Pharmaceutical, Biological and Chemical Sciences

Realization of Multimedia Applications on Re-Configurable Platform

P Rajkumar[1]*, and I Mary Sajin Sanju[2].

[1]Department of ETCE, Sathyabama University, Chennai, Tamil Nadu, India.
[2]Department of ECE, Sathyabama University, Chennai, Tamil Nadu, India.

ABSTRACT

Digital images store large amount of data and in sequence. This information can be manipulated to several extend without being detected by human eyes. An example of such manipulations is supplement of secret information which is often referred to as information hiding. A successful supplement of a message into an image is more difficult using color images than that of gray scale images. A successful information hiding should result in the extraction of the hidden data from the image with high degree of data integrity. In this work we presents an information hiding technique that utilizes lifting schemes to effectively hide information in color images. We propose an information hiding techniques that utilizes lifting schemes to effectively hide information in images. In this proposed system we introduces a method of secret message encoding that makes use of wavelets. It makes use of the integer based wavelet transformation, lifting, and a least Significant Bits (LSB) approach to hide messages in covers images. In this work we have presented a new method of adaptive steganography with higher embedding capacity. The embedding capacity of the approach is controlled through the filter cut-off frequency. The approach was analyzed and shown to have a very high confidentiality due to the sharpness of information recovery with the cut-off frequency.

Keywords: Steganography, Cryptography, Image processing, DCT, Watermarking.

Corresponding author

ISSN: 0975-8585

INTRODUCTION

Computer security is the procedure of preventing and detecting unconstitutional use of your computer. Prevention measures help you to discontinue unconstitutional users (also known as "intruders") from accessing any part of your computer system. Detection helps you to establish whether or not an important person attempted to break keen on your system, if they were flourishing, and what they may have been done. Network security starts from authenticating the user, commonly with a username and a secret word. Since this requires just one thing besides the user name, i.e. the secret word which is something you 'know', this is sometimes termed one factor confirmation. With two factor confirmation something you 'have' is also used (e.g. a security token or 'dongle', an ATM card, or your mobile phone), or with three factor confirmation something you 'are' is also used (e.g. a fingerprint or retinal scan). Network security is generally taken as long as protection at the limitations of an organization by observance out intruders. Information security, however, unambiguously focuses on protecting data resources from malware attack or simple mistakes by populace within an organization by use of data loss prevention (DLP) techniques. One of these techniques is used to compartmentalize huge networks with internal limitations.

Once authenticated, a firewall enforces access policies such a services are allowed to be accessed by the set of connections or users. Though efficient to prevent unauthorized access, to this component may fail to check potentially damaging content such as computer worms or Trojans being transmitted over the set of connections. Anti-virus software or an intrusion prevention system (IPS) helps detect and restrain the action of such malware [12]. An anomaly-based interruption detection system may also monitor the set of connections and traffic for unexpected (i.e. suspicious) content or performance and other anomalies to save from harm resources, e.g. from denial of examination attacks or an employee accessing files at strange times. Personality events occurring on the network may be logged for audit purposes and for later high level analysis.

Communication between two hosts using the set of connections could be encrypted to maintain privacy. Honeypots, essentially decoy network-accessible resources, could be deployed in a network as examination and early-warning tackle. Techniques used by the attackers that attempt to compromise these decoy resources are studied during and after an attack to keep an eye on new exploitation techniques. Such analysis could be used for further tighten security of the actual network being protected by the honeypot. Frequently used security for data exchange is done in encryption and decryption [11]. Encryption is the procedure of transforming information (referred to as plaintext) using an algorithm (called cipher) to make it incomprehensible to anyone except those possessing special knowledge, usually referred to as a key and vice versa for decryption. But the most secure is steganography.

Steganography is the art and science of writing secrete information in such a way that no one can be, apart from the sender and intended recipient, suspect the survival of the communication, a form of security throughout oburiscty. The word steganography is of Greek derivation and means "concealed writing" from the Greek words steganos meaning enclosed or sheltered and graphing meaning to write. In generally, messages will appear to be something else: like images, articles, shopping lists, or some other cover text and, characteristically, the hidden message may be in invisible link between the perceptible lines of a confidential letter.

The benefit of steganography, over cryptography alone, is that messages do not attract concentration to themselves. Plainly perceptible encrypted messages, no matter how unbreakable will arouse mistrust, and may in themselves be incriminating in countries where encryption is against the law. Therefore, whereas cryptography protects the contents of a message, where as steganography can be said to protect both messages and communicating parties.

Steganography includes the camouflage of information within system files. In digital steganography, electronic transportation may include steganographic coding inside of a transport layer, such as a manuscript file, illustration file, and protocol. Media files are perfect for steganographic transmission because of their huge size [10]. As a simple example, a sender might start with an inoffensive image file and adjust the color of every 100th pixel to correspond to a letter in the alphabet, a change so restrained that someone not purposely looking for it is unlikely to notice it. We propose an information hiding techniques that utilizes lifting schemes to effectively hide information in images. In this work we introduces a method of secret message encoding that

makes use of wavelets. It makes use of the integer based wavelet transformation, lifting, and a Least Significant Bits (LSB) move toward to the hide messages in the cover images.

STEGANOGRAPHY

Steganography means to hide secret information into blameless data. Digital images are ideal for trouncing secret information. In an image containing a secret message is called a cover image [9]. There are three different cover images. They are (i) first; the difference of the cover image and the stego image should be visually imperceptible. The embedding itself should draw there is no extra attention is given to the stego image so that no hackers would try to extract the concealed message illegitimately. (ii) Second; the message hiding method should be reliable. It is unfeasible for someone to extract the hidden message if she/he does not have a special extracting technique and a proper secret key. (iii) In the third, the maximum measurement lengthwise of the secret memorandum that can be hidden and it should be as long as possible to hold the hidden message. There are few Steganography techniques which are exist as follows

- Physical Steganography
- Digital Steganography
- Printed Steganography

Goal of the proposed system

- To compile an introduction to the subject of Steganography and steganalysis. There survive a number of case studies on various algorithms.

- To search for algorithms that can be used to put into practice for the discovery of steganographic techniques.

- To appraise their performance with different image quality metrics. And these properties were chosen because they have the maximum collision on the detection of steganography algorithms

Basic Method behind Steganography

Image Files

To a computer, an image is an array of numbers that represent illumination intensities at various points or pixels. These pixels make up the illustration acts raster data. A common image sizes should be 640 * 480 and 256 colors (or 8 bits per pixel). Such type of image could contain about 300 kb of information. But for the digital images are typically stored as either 24-bit or 8-bit files. In a 24-bit image it will provides the more space for hiding a information; however, it can be quite large except for the type of JPEG images. A 24-bit image of 1,024 pixels width and 768 pixels height has more than two million pixels, each pixels should having 24-bits information, which would produce a file exceeding 2 Megabytes in size. Such a file would attract attention during transmission. File compression would thus be favorable, if not necessary, to transmit such a file.

File Compression

There are two different types of file compression methods they are firmly called as lossless and lossy. In both methods are used to save storage space, but they have different results, by interfering with the hidden information, when that information is uncompressed. Lossless firmness lets us reconstruct the unique message exactly; therefore it is preferred when the unique information must remain undamaged (as with steganographic images). Lossless compression is typical for the images saved as GIF and 8-bit BMP format.

Concealment in Digital Images

Information can be hidden in many different ways in images. To hide the information, straight message supplement may encode every small piece of information in the message or selectively embed the

message in strident areas that draw less attention those areas where there is a great covenant of natural color dissimilarity. This message may also be scattered randomly throughout the image. Superfluous pattern encoding wallpapers to the cover image with the message. A number of ways survive to hide information in digital images. Common approaches which are include hiding the information they are:

- Least Significant Bit Insertion
- Masking and filtering
- Algorithms and Transformations
- Spread Spectrum Method

Adaptive Steganography Using Filtering

Adaptive Steganography reduces modifications to the image, and it adapts the message embedding practice to the actual content and features of the image. In general, we keep a high-quality degree of stealthiest, Adaptive methods embed message bits into certain accidental clusters of pixels (avoiding areas of uniform color) by selecting the pixels with large local standard deviation or image blocks containing a number of dissimilar colors [8]. The main advantage of adaptive steganography is that the changes can made in the cover image that will take into an account the sensitivity of the human visual system and also a variety of statistical parameters generally being used by stego-analysis algorithms. The main confront posed to existing adaptive steganography techniques [3,4,5,6] is that the methods so far urbanized doesn't seem to have a way to control the amount of information that is to be concealed, for a given cover image. This problem can be overcome in this method.

In the proposed approach we utilizes the sensitivity of the human illustration system that can be adaptively modify the intensities of some pixels in a high frequency gears spatial image (HFSI) of the cover image. The modification of pixel intensities it will depends on the magnitude of the pixels in HFSI and also on the local facial appearance of the cover image. If the contrast of the image is bulky (e.g., an edge), the intensities can also be changed very much without introducing any distortion to human eyes. On the other hand, if the contrast of the image is petite (e.g.a smooth), then the intensities can only be tuned faintly.
In this technique, at first the cover image is agreed through a filter to separate the frequency then the high and low frequency components of the image [8]. Then the inverse transform should be implemented on both the images is computed. at this instant the pixels values of the HFSI are modified and it depends on the magnitude of the pixel i.e. if the magnitude more than the Least Significant Bits is also more (LSB's) of that the pixel are changed and also its local features of cover image are considered. at this moment both the LFSI (Low Frequency components spatial image of cover image) and HFSI are added to the stego - image. At the receiver side, the reverse process is to be done to recuperate the message.

An FPGA-Based Architecture for Real Time Image Feature Extraction

Real time image pattern recognition is a challenging task which involves image processing, and the corresponding feature extraction and pattern classification. And it can be implemented to a wide range of applications such as multimedia, military and medical ones. Its high computational necessities force systems is one of the very expensive clusters, in the custom VLSI designs or even both. These approaches can suffer from various disadvantages, such as expensive in cost and long progress times.

Recent advantage in fabrication technology that can allow the manufacturing of high concentration and high performance Field Programmable Gate Arrays (FPGAs) so it can capable of performing many complex computations in parallel and it while hosted by conventional computer hardware. So that a variety of architecture designs is capable of supporting a real time pattern recognition have been proposed in the recent literatures, such as implementations of algorithms for an image and video processing, and classification of the image feature extraction algorithms.

Although the texture plays a significant role in image investigation and pattern identification only a few architectures that can implemented in on-board textural feature extraction. Most prominent approaches that will include the extraction of Gabor wavelet features particular for face/object recognition and the computation of mean and contrast [7]. Gray Level Co occurrence Matrix (GLCM) features. In the second method; the two different features are approximated without computing GLCMs. That will combines both software and

ISSN: 0975-8585

hardware to raster scan for the given input images with sliding windows and it will produce 16-dimensional feature vectors consisting of four GLCM features that can be calculated for four directions.

Discrete Wavelet Transform

By calculating wavelet coefficients at every possible scale is a fair amount of work, and it generates an awful lot of data [6]. If the scales and positions are chosen based on powers of two, the so-called dyadic scales and positions, then calculating wavelet coefficients are efficient and just as accurate. This is obtained from discrete wavelet transform (DWT).

1-D Wavelet Transforms

The standard form for a one-dimensional (1-D) wavelet transform is shown in Fig. 1. Here a signal is conceded through a low pass and high pass filter, 'q' and 'p' respectively, then down sampled by a factor of 2, by constituting one level of transform.

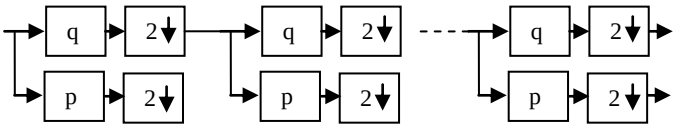

Figure: 1 1D Wavelet Disintegration

Repeating the concept of filtering and decimation process on the low pass limb outputs make several levels or "scales" can only passed by the wavelet transform. This process is typically carried out for a restricted number of levels are denoted by K, and the resulting coefficients are called wavelet coefficients.

The one-dimensional ahead wavelet transform is defined by a pair of filters 'a' and 'b' that are convolved with the data and then the data should be at either in even or odd locations [5]. The filters and bused for the ahead transform are called analysis filters and it can be expressed as

$$w_i = \sum_{m=-p_w}^{p_w} a_j x 2i_{+j} \quad \text{and} \quad z_i = \sum_{m=-p_w}^{p_z} b_j x 2i_{+w+j} \text{------ (1)}$$

Although 'w' and 'z' are two separate output streams, together but they have the same total number of coefficients as the unique data. The output stream 'w' which is commonly referred to as the low-pass information may then have the identical process applied again continually. The other output stream, 'z' (or high-pass data), generally remains undamaged. The inverse process expands the two separate low- and high-pass information streams by inserting zeros between every other sample data, it convolves the resulting information streams with two new synthesis filters 'a' and 'b', and adds them together to regenerate the original double size information stream. And it can be expressed as

$$w_i = \sum_{m=-p_z}^{p_z} b'_j w'_{i+j} + \sum_{m=-p_z}^{p_w} a'_j z'_{i+j} \text{ ---------- (2)}$$

Where

$$w_{2i} = y_i, \quad w'_{2i+w} = 0, z'_{2i+w} = z_i, z'2i = 0$$

To convene the description of a wavelet transform, the analysis and synthesis filters a, b, a' and b' must be chosen so that the inverse transform absolutely reconstructs the original information. Since the wavelet transform maintains the same number of coefficients that they having in the original information, the transform itself does not provide any firmness. However, the constitution provided by the transform and the expected principles of the coefficients will be given in the form that is much more amenable to firmness than the original information. Since the filters a, b, a' and b' are chosen to be absolutely invertible, the wavelet transform itself is lossless. Later relevance of the quantization step will cause some information loss and it can

ISSN: 0975-8585

be used to control the degree of firmness. The forward wavelet-based transform uses a 1-D sub-band disintegration practice; here a 1-D set of samples is rehabilitated into the low-pass sub-band (wi) and high-pass sub-band (zi). The low-pass sub-band represents a down sampled low-pledge version of the original image. The high-pass sub-band represents remaining information of the original image, needed for the perfect rebuilding of the original image from the low-pass sub-band.

LL1	**HL1**
LH1	**HH1**

Figure: 2 Sub-band Labeling Scheme for a one level, 2-D Wavelet Transform

The original image of a one-level (K=1), 2-D wavelet transform, with equivalent notation is shown in Fig. 2. The example is repetitive for a three-level (K =3) wavelet development in Fig. 5.13. In all of the argument *K* represents the peak level of the disintegration of the wavelet transform.

<table>
<tr><td>LL_1</td><td>HL_1</td><td rowspan="2">HL_2</td><td rowspan="3">HL_3</td></tr>
<tr><td>LH_1</td><td>HH_1</td></tr>
<tr><td colspan="2">LH_2</td><td>HH_2</td></tr>
<tr><td colspan="3">LH_3</td><td>HH_3</td></tr>
</table>

Figure: 3 Sub-band labeling Scheme for a Three Level,

2-D Wavelet Transforms

The 2-D sub-band disintegration is just an extension of 1-D sub-band disintegration. The whole process is carried out by executing 1-D sub-band disintegration twice, but at first in one direction (horizontal), then in the orthogonal (vertical) direction. For example, the low-pass sub-bands (wi) resulting from the horizontal track is further decomposed in the vertical track, but it is leading to LLi and LHi sub-bands.

Similarly, the high pass sub-band (zi) is further festering into HLi and HHi. Subsequent to one level of transform, then the image can be further festering by applying the 2-D sub-band disintegration to the existing LLi sub-band. This iterative development results in multiple “transform levels”. In Fig.3.1.4it will shows the first level of transform results in LH1, HL1, and HH1, in accumulation to LL1, which is further festering into LH2, HL2, HH2, LL2 at the second stage, and the information of LL2 is used for the third stage transform. The sub-band LLi is a low-pledge sub-band and high-pass sub-bands LHi, HLi, HHi are horizontal, orthogonal, and diagonal sub-band respectively since they represent the horizontal, orthogonal, and diagonal enduring information of the original image [5]. An example of three-level disintegration into sub-bands of the image castle is illustrated in the below figure.

Figure: 4 2-Dimension wavelet transform applied through three transform levels

Awic Filter Choice

The main difference between sub-band and wavelet coding is the preference of filters to be used in the transform. The filters which are used in wavelet coding systems were typically designed to convince certain effortlessness constraints. In dissimilarity, sub-band filters were designed to approximately convince the criteria

of non-overlapping regularity responses. There are two types of filters they are, orthogonal and biorthogonal. In the biorthogonal wavelet transform has the benefit that it can use linear phase filters, but the drawback is that it is not vigor preserving. The fact that biorthogonal wavelets are not vigor preserving but it does not turn out to be a big quandary, since there are linear phase biorthogonal filter coefficients, which are "secure" to being orthogonal.

The 9-7 and 5-3 Daubechies biorthogonal filters, were chosen as ideal for image compression. Both the biorthogonal 9-7 and 5-3 filters were used in AWIC (Rushanan1997). The detracting visual artifact at high compression rates using the longer filter is ringing, while the shorter filter produces stair casing. The design trade-off between these two filters is speed performance and quality performance. Visually, the level of ringing artifacts and stair casing artifacts appears to be nearly equivalent, dependent on subjective opinion. The peak-signal-to-noise ratio favors the ringing artifact over the stair casing.

The Daubechies 5-tap/3-tap filter is used in forward wavelet transform and it has good localization and symmetric properties, which allows simple border treatment, high-speed calculation, and high eminence compressed image. The following equation can represents the Daubechies 5-tap/3-tap filter.

$$L[2n] = \frac{[-x[2n-2] + 2x[2n-1] + 6x[2n] + 2x[2n+2] + 2]}{4} \quad \text{------- (3)}$$

$$H[2n+1] = \frac{[-x[2n-1] + 2x[2n+1] - x[2n+2]]}{2} \quad \text{-------- (4)}$$

Wavelet Computation

In order to obtain an efficient wavelet computation, it is important to eradicate as many unnecessary computations as possible. A careful assessment of the forward and reverse transforms shows that about half the operations either lead to information which are cracked or are null operations (as in multiplication by 0). The one-dimensional wavelet transform is computed by autonomously applying two analysis filters at irregular smooth and peculiar locations [4]. But in the inverse procedure first doubles the length of each signal by inserting zeros in every other situation, then applies the appropriate synthesis filter to each signal and adds the filtered signals to get the concluding reverse transform.

Algorithms and Transformations

To Encode the Hidden Data

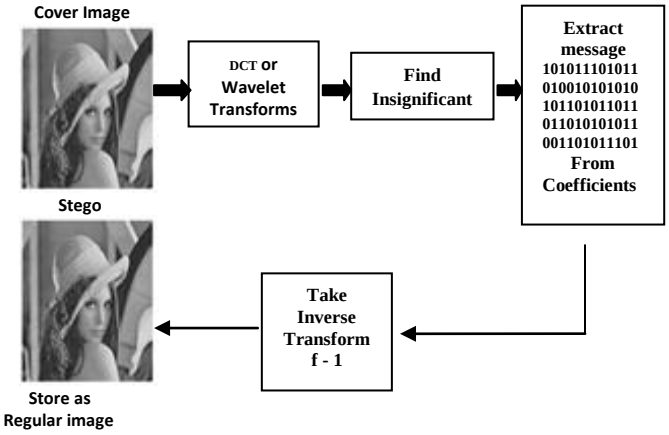

Figure: 5 Encoding block diagram

Another steganography method is to hide information in mathematical functions that are in firmness algorithms. Two functions are there in Discrete Cosine Transformation (DCT) and Wavelet Transformation. The Discrete Cosine Transformation and wavelet functions transform the information from single domain into another. The Discrete Cosine Transformation function transforms that information from a spatial province to a frequency domain. The plan behind it in observe to steganography is to secrete the information bits in the slightest significant coefficients.

- Obtain the wavelet transform of the cover image
- And find the coefficients below a convinced threshold
- Replace these bits with the data to be concealed (can use LSB insertion)
- Obtain the inverse transform
- accumulate as regular image

To Decode the Hidden Data

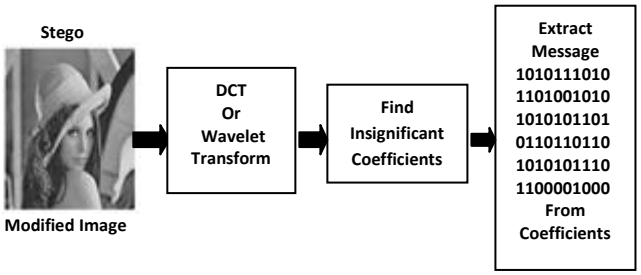

Figure: 6 Decoding block diagram

- Obtain the transform of the modified image
- And find the coefficients below a convinced threshold
- Then extract the bits of data from these coefficients
- Coalesce the bits into an actual message

Context Technique

To be able to correctly identify the regions where the information will be inserted, the gray scale level is analyzed in the spatial distribution, looking for the areas with greater diversity of gray scale levels [2]. The selection process of the pixel where the information will be inserted is described in the following steps:

- Partition the image in non overlapping blocks of3x3 pixels
- The block of 3x3 is alienated in four sub-blocks of2x2 pixels
- Each sub-block of 2x2 is painstaking valid if there are at least 3 values of gray scale levels
- The data is inserted in the 3x3 block middle if the four sub-blocks are applicable
- The strength of the four sub-blocks of 2x2 is verified after having inserted the information. If some 2x2 sub-block is not applicable after hiding the information in the 3x3 block, then the inserted bit is not considered as secreted to avoid losing information during the revival process

Context Hardware Architecture

As it can be respected from the contexts technique, the most demanding operation is the association of the pixel values of the 4 generated sub-blocks.

32	42	56	76	70	74	80	95	94	49
9	10	10	23	44	52	58	73	53	16
14	5	0	4	16	11	8	22	24	3
29	19	7	11	20	11	5	16	11	7
20	26	16	1	15	15	12	17	12	16
17	41	36	9	5	13	12	6	8	17
26	55	50	19	12	23	21	12	10	15
26	40	34	17	18	22	18	14	13	17
36	34	24	21	27	21	13	16	8	14
8	12	16	27	33	19	5	11	11	6

Figure: 7 Image is divided in 3x3 block

ISSN: 0975-8585

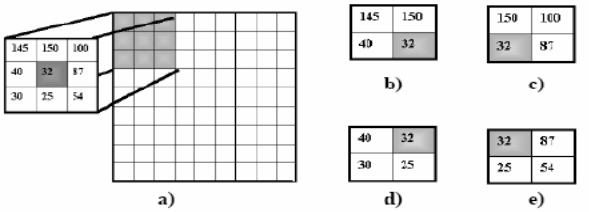

Figure: 8 Sub-blocks division

The hardware execution was based on the generation of blocks that perform simple operations, following the Top - Down methodology.

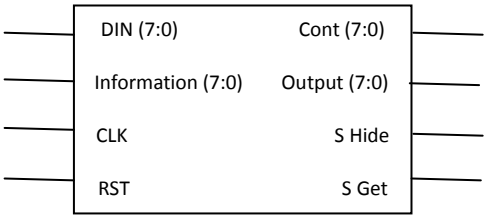

Figure: 9 Context Interface

The general block of the structural design, showing the input and output data for the Contexts technique.

Simulation Results

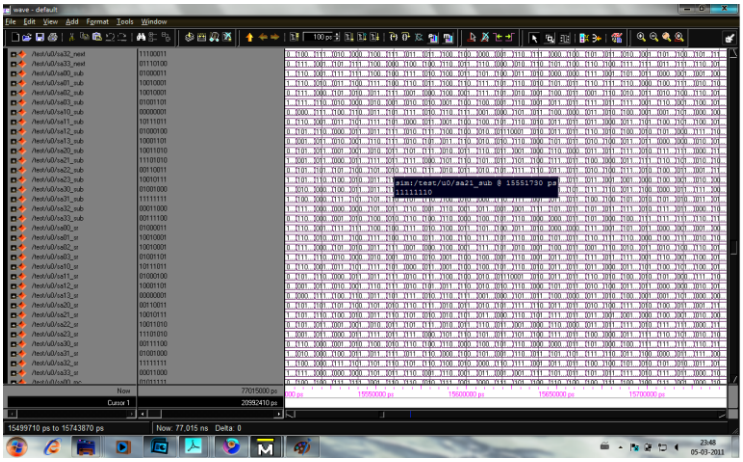

Figure: 10 Input image signal

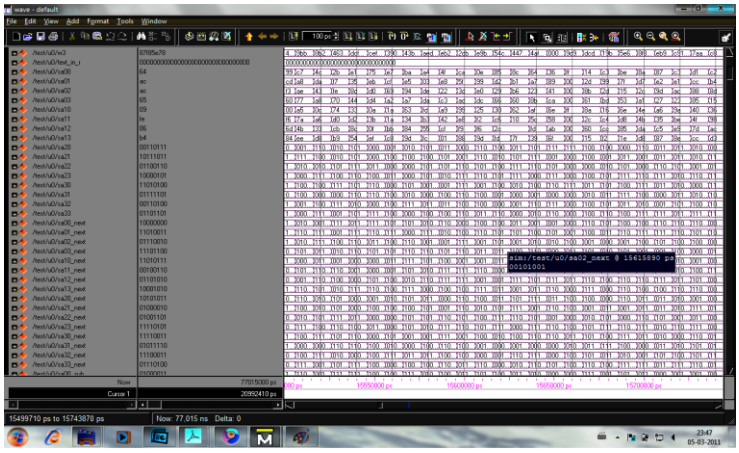

Figure: 11 Pattern key signal

ISSN: 0975-8585

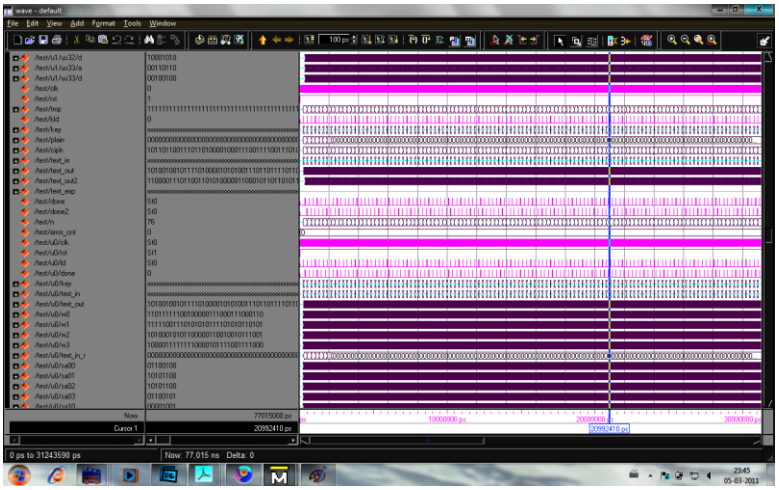

Figure: 12 Test in and out signal

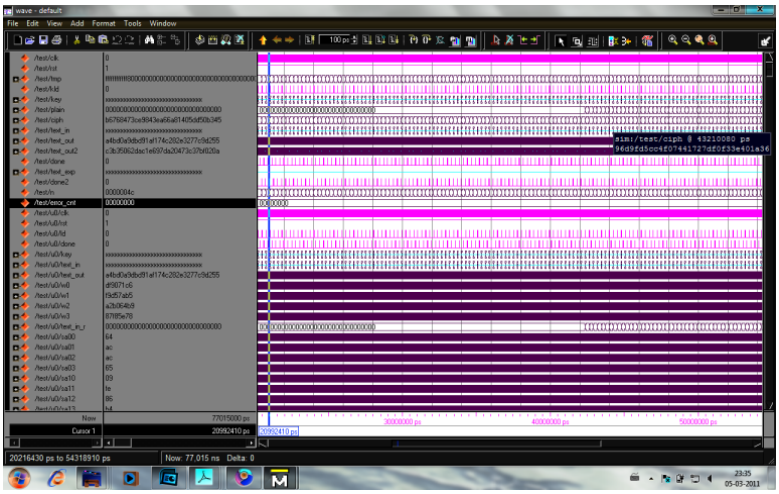

Figure: 13 Output signal

CONCLUSIONS

In this work we tried to give an all-round view of steganography, both techniques are used to exchange messages and watermarking. And we gave an outline of the problem, telling also some of the olden times of this quickly developing field. Then we showed the different techniques invented, from the simplest to the more composite ones, trying to evaluate them under many points of sight. Major emphasis was put on information hiding in images, for the techniques implicated are usually more mature than the corresponding ones for other kinds of information's. In the image encoding algorithms can also be delegate for manipulation of other types of media like voice, text, binary files, communication channels etc. Then we gave an outline of the problems which can involved with watermarking, a field that has come into illumination after the development of broadband worldwide digital networks. Steganography and digital watermarking are undergoing a development process similar to that of encryption. Steganography acts machine in security is to supplement cryptography and not to reinstate it. There is a constant invention of latest techniques for steganography followed by successful breakings and new improvements of them.

In this work we have presented a new method of adaptive steganography with higher embedding capacity. The embedding capacity of the approach is controlled through the filter cut-off frequency. The approach was analyzed and shown to have a very high secrecy due to the sharpness of information recovery with the cut-off frequency.

Future Enhancements

Considering the incredible amount of research work currently in progress to make Steganography as a secure transmission medium, makes us believe that in future we will be able to apply Steganography to number of scenarios such as confidential image transmission over the network. Currently, the better known techniques of Steganalysis only makes it hard to detect the possibility of hidden data in an anonymous image currently being transmitted over the network and thus we must improvise Steganalysis process such that it will become much easier to detect even small messages within an image Finally, the fact that adding hidden data adds random noise to the target image making it hard to recover the hidden data, so it follows that a properly tuned noise detection algorithm could recognize whether or not a picture had steganographic data or not.

REFERENCES

[1] ShinoharaH, Monji H, Iida M, SueyoshiT.A Novel Technique to Create Energy-Efficient Contexts for Reconfigurable LogicField-Programmable Custom Computing Machines,. 15th Annual IEEE Symposium Publication Year: 2007, Page(s): 285 - 286

[2] Haopeng Liu , Weiguang Sheng, Weifeng He, Zhigang Mao.Delay hidden techniques based onconfiguration contexts reuse and differential reconfiguration in coarse-grained reconfigurable processorASIC (ASICON), 2013 IEEE 10th International Conference Publication Year: 2013 , Page: 1 - 4

[3] Qureshi MA, Ran Tao. Technical Challenges for Digital Watermarking. Computational Engineering in Systems Applications, IMACS Multiconference on Volume: 1 Publication Year: 2006, Pages: 444 - 447

[4] Prabakaran G, Bhavani R. A modified secure digital image steganography based on Discrete Wavelet Transform.Computing, Electronics and Electrical Technologies (ICCEET), 2012 International Conference Publication Year: 2012,Pages:1096-1100.

[5] S Mallat and F Falzon.IEEE Trans Signal Process 1998;46(4):1027–1042.

[6] Dutta J, DasP, Bandyopadhyay R, BandyopadhyaySK, TaihoonKim. DiscreteFourier Transformation based Image Authentication technique.Cognitive Informatics, 2009. 8th IEEE International Conference Publication Year: 2009, Page(s): 196 – 200.

[7] BariamisDG, IakovidisDK, Maroulis DE,KarkanisSA.An FPGAbased architecture for real time image featureextraction. Pattern Recognition, 2004. Proceedings of the 17th International Conference Volume: 1 Publication Year: 2004 , Page(s):801-804Vol.1

[8] R Chandramouli, ND Memon and G Li. Adaptive Steganography,Proc. Security and Watermarking of Multimedia Contents III, Special session on Steganalysis, SPIE Photonics West, Calif. 2002, pp. 69-78.

[9] Neil F Johnson and SushilJajodia.Steganalysis: The Investigation of Hidden Information, Information Technology Conference, IEEE. Pages.113 - 116. sep.1998.

[10] MM Amin, M Salleh, S Ibrahim, et al.InformationHiding using Steganography, 4th national Conference on Telecommunication Technology, NCTT 2003, IEEE. Pp 21 - 25.

[11] G Naveen Samuel, Immanuel Ganadurai**.**Int JEng Res Technol 2012;1(6).

[12] Zhenfei Zhang, Susilo W, Raad R. Mobile ad-hoc network key management with certificateless cryptographySignal Processing and Communication Systems, 2008. ICSPCS 2008. 2nd International Conference on PublicationYear:2008 ,Page(s):1-10