International Journal of Information & Computation Technology.
ISSN 0974-2239 Volume 2, Number 2 (2012), pp. 111-123

http://www. ripublication.com

Information Security through Image Fusion

[1]S. Magesh Kumar, [1]K. Mohan, [2]S.E. Neelakandan and [1]S. Muruganandam

[1]Department of Computer Science and Engineering,
Thirumalai Engineering College, Kanchipuram, India
[2]Department of Information Technology,
Thirumalai Engineering College, Kanchipuram, India
E-mail: mails:mageshkumars@yahoo.com, jackmoh2000.2009@gmail.com,
murugansoft@hotmail.com, se.neela@gmail.com

Abstract

Multiple images are fused into a single image with a technique 3-D Wavelet Transform in this many images are fused into a single image. A set of data had been embedded with a technique of LSB Matching to hide the data in the image by that information security is been provided. The steganography used to hide the information behind the image, audio and video. Most of the existing system used many techniques. In this paper, data hiding is been done by LSB matching technique, then the generated stegno image file to apply the image fusion. So it is very hard to find the original data from the image fusion. We can get very secured information by using this system.

Keywords: 3-D WT, Stegnography, LSB Matching.

Introduction

The Greek word “steganos” meaning covered writing is basically the concept behind the theory of steganography. Here it is difficult to even detect that a message is being sent. This type of ciphering called steganography, the ancient art of hiding messages sent undetectable. This methodology is gaining popularity with everyday passing because of its unique properties and those days are not far off when it would be adopted by armies of the world for secret message passing. The history of sending hidden message is very old. Greeks used it writing message on some material and later covering it with wax, tattooing messages on bald head, later growing hair to cover it up. In World War II invisible inks were used to write messages in between the lines of normal text message [1]. World War II saw the use of microdots by Germans. In microdots technology, photograph of secret message taken was reduced

to size of a period. This technology was called “the enemy’s master piece of espionage” by FBI director J. Edgar Hoover [1]. Normal and innocent messages carrying secret messages moved from one place to another.

Image Stegnography

There are currently three effective methods in applying Image Steganography LSB Substitution, Blocking, and Palette Modification [2]. LSB (Least Significant Bit) Substitution is the process of modifying the least significant bit of the pixels of the carrier image. Blocking works by breaking up an image into “blocks” and using Discrete Cosine Transforms (DCT). Each block is broken into 64 DCT coefficients that approximate luminance and color—the values of which are modified for hiding messages. Palette Modification replaces the unused colors within an image’s color palette with colors that represent the hidden message. [1]

We have chosen to implement LSB Substitution in my project because of its ubiquity among carrier formats and message types. With LSB Substitution we could easily change from Image Steganography to Audio Steganography and hide a zip archive instead of a text message. LSB Substitution lends itself to become a very powerful Steganographic method with few limitations. LSB Substitution works by iterating through the pixels of an image and extracting the ARGB values. It then separates the color channels and gets the least significant bit. Meanwhile, it also iterates through the characters of the message setting the bit to its corresponding binary value [3].

Techniques

The three basic techniques used for Steganography are

Injection: Hiding data in sections of a file that are ignored by the processing application. Therefore avoid modifying those file bits that are relevant to an end-user leaving the cover file perfectly usable.

Substitution: Replacement of the least significant bits of information that determine the meaningful content of the original file with new data in a way that causes the least amount of distortion.

Generation: Unlike injection and substitution, this does not require an existing cover file but generates a cover file for the sole purpose of hiding the message.

The steps in steganography include the writing the text messages, encryption of the text message is one of the options available. Later, text is hidden in the selected media and transmitted to recipient. At receiver end, reverse process is implemented to recover the original text message. Various techniques used in the art of steganography is the arrangements of various bits of the characters of the text in an image or other media. Keeping in mind the above, two files are needed; the image file and the text file that contains the data.

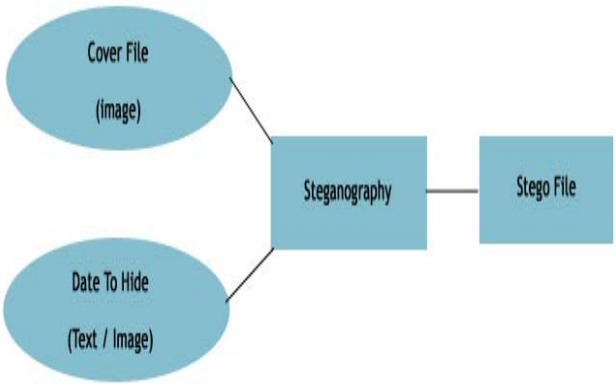


Figure 1: The processing of hiding data

LSB affects the smallest changes of the 8 bits therefore it alters the image to minimum [4]. The most common method used is called LSB (Least Significant Bit) Mechanism that is hiding if the data in the least significant Bit (LSB) of the message.

However, one of its major limitations is small size of data which can be embedded in such type of images using only LSB. LSB is extremely vulnerable to attacks. LSB techniques implemented to 24 bit formats are difficult to detect contrary to 8 bit format. The other techniques include Masking and Filtering. It is normally associated with JPEG. In this technique image data is extended by masking secret data over it. Therefore, experts do not include this [5] as a form of Steganography.

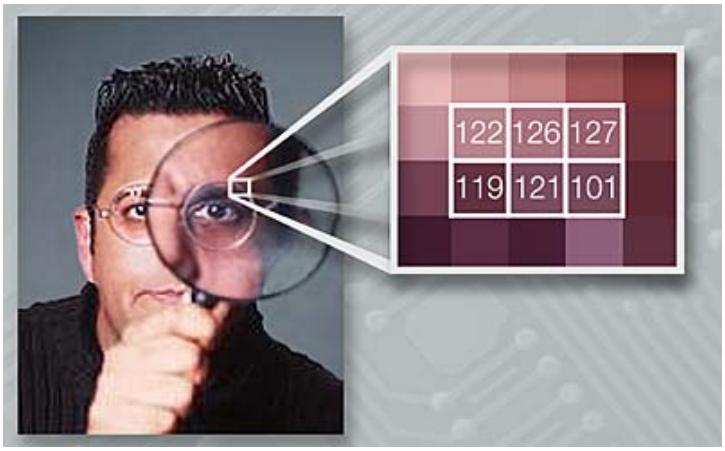


Figure 3: Hiding the data behind the image

All algorithms employed for any type of format have pros and cons and depend upon the environments used. It also depends upon the information to be embedded. Various techniques developed were compared [6].Section VI gives out the details of the proposed technique.

Implementation

Steganography, as defined above is a technique to hide a data in an image in such a manner that it is unperceivable. To achieve such outcome one may think of chopping the raw data that is the data to be hidden in equal number of block and hide it in specific areas within an image. Such a thought interprets that the concept is not vivid. That is, one is not able to extract the true beauty of Steganography. Presently the technology being mostly used is Digital Images [7]. By digital Images we presume to deal with bits that is 0's and 1's.

Digital Images we have selected are 24-bit depth color images using RGB color model. 24-bit refers to 8-bit for each RGB color channel, i.e. 8-bits for red.8-bits for green and 8-bits for blue and 24-bit depth with width and height of 800 x 600 pixels. It must be remembered that image resolution is highly dependent on the monitor screen resolution.

The idea is to hide text in image with the conditions that the image quality is retained along with the size of the image. Here, a thought may arise that why we need to hide text in an image if we can easily encrypt is using several ways. This is the point where cryptography and steganography differs. Applying, cryptography result in an output of an unreadable text (cipher text), which when send over an internet is easily detectable that some important information is being conveyed. On the contrary, hiding message in an image, along with the conditions, may seem just an exchange of picture between two ends.

Our algorithm is simple and flexible using LSB technique. We have selected the formats that commonly use lossless compression that is BMP, PNG, TIFF and GIF. We can make use of any of these formats or convert BMP into any of the above said formats. When data is streamed, it is captured after the header and chopped into 8 bits. It has been analyzed that the conversions do not distort the images to a level where the degradation can be felt with the naked eye.

Figure 2: Simple conversion of a BMP to GIF

Figure 3: Simple conversion of a BMP to TIF

The technique we are using is Least Significant Bit (LSB) i.e. storing in LSB of a byte (pixel). As mentioned above, the RGB model is used, we first stream an Image file and read the file in bits and then seek the position ahead the header bits.

Figure 4: Resultant image after hiding data in GIF

Figure 5: Resultant image after hiding data in BMP/PNG

After reaching the redefined location, read bits in group of 8 (byte) and replace the last bit with the intended data to be hidden in the image. Let us consider the above mentioned images to hide the data. The topmost left area of image will compose of different shades of blue indicating sky and sea. Let us consider the first image pixel of value 194:213:243, 200:244:243, 192:213:243, (shade of a blue) of binary value

11000010:11010101:1110011:11001000:
11110100:11110011:11000000:11010101

and Text T of binary value 1010100.To store these 8 bits of character T, we will require 8 pixels. Since, we are using one bit of each pixel.

T = 1 0 1 0 1 0 0

Pixel Values

11000010:11010101:11110011:11001000:
11110100:11110011:11000000:11010101

LSB Matching

LSB steganography, in which the lowest bit plane of a bitmap image is used to convey the secret data, has long been known to steganographers. Because the eye cannot detect the very small perturbations it introduces into an image and because it is extremely simple to implement, LSB methods are commonly used among the many free steganography tools available on the internet. There are two types of LSB steganography: LSB replacement can be uncovered relatively easily, but fewer and weaker detectors have been proposed for LSB matching. It is the latter we consider here, in the particular case when the covers are grayscale images. The LSB matching embedding algorithm is as follows.

Convert the secret data into a stream of bits. Take each pixel of the cover image (possibly in a pseudo-random order generated by a shared secret key): if the LSB of the next cover pixel matches the next bit of secret data, do nothing; otherwise, choose to add or subtract one from the cover pixel value, at random. When the secret message is fewer bits in length than the number of pixels in the cover image, the pseudo-random permutation ensures that changes are spread uniformly throughout the image. The allowable range of pixel values will force the decision of whether to increment or decrement, when the cover pixel is saturated.

LSB replacement is very similar, except that the LSBs of the cover pixels are simply overwritten by the secret bit stream. In either case, the decoding method for the recipient is simply to read back the LSBs of the stego image, according to the order specified by the secret key, if needed; the original cover image is not needed by the recipient and should be discarded by the sender.

3-D WT Image Fusion

The wavelet transform offers several advantages over similar pyramid based techniques when applied to image fusion: (a) the wavelet transform is a more compact

representation than the image pyramid. This becomes of very great importance when it comes to fusion of 3-D and 4-D images. The size of the WT is the same as the size of the image. On the other hand, the size of a Laplacian pyramid, for instance, is 4/3 of the size of the image; the wavelet transform provides directional information, while the pyramid representation doesn't introduce any spatial orientation in the decomposition process [8]; in pyramid based image fusion, the fused images often contain blocking effects in the regions where the input images are significantly different. No such artifacts are observed in similar wavelet based fusion results [8]; images generated by wavelet image fusion have better signal to noise ratios (SNR) than images generated by pyramid image fusion, when the same fusion rules are used [9]. When subject to human analysis, wavelet fused images are also better perceived according to [8, 9].

Several wavelet based techniques for fusion of 2-D images have been described in the literature [10, 11]. All of these publications study only the case of 2-D image fusion. In this paper, we have extended some of the above mentioned 2-D fusion schemes to 3-D images. New 3-D fusion schemes are also presented. The 3-D WT image fusion algorithms described in this study have been used to combine both phantom (texture and non-texture) images (Figure 5) and multimodality (CT and MR) images (Figures 6 and 7).

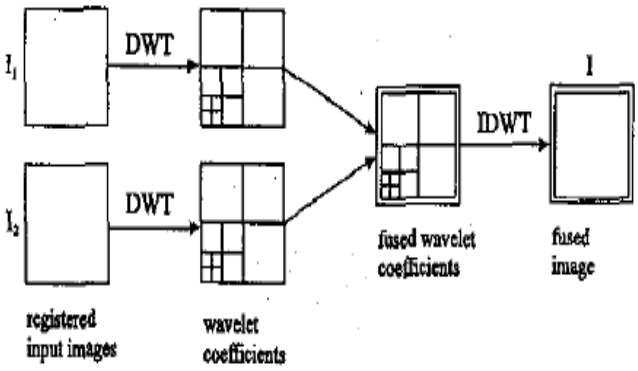


Figure 6: Fusion of the WT of two images

The general idea of all wavelet based image fusion schemes is that the wavelet transforms *w* of the two registered input images I_1(z, Y, zan)d *Iz(x., y, z)* are computed and these transforms are combined utilizing some kind of fusion rule Φ (Figure 6). Then, the inverse wavelet transform *w-l* is computed, and the fused image *I* is reconstructed:

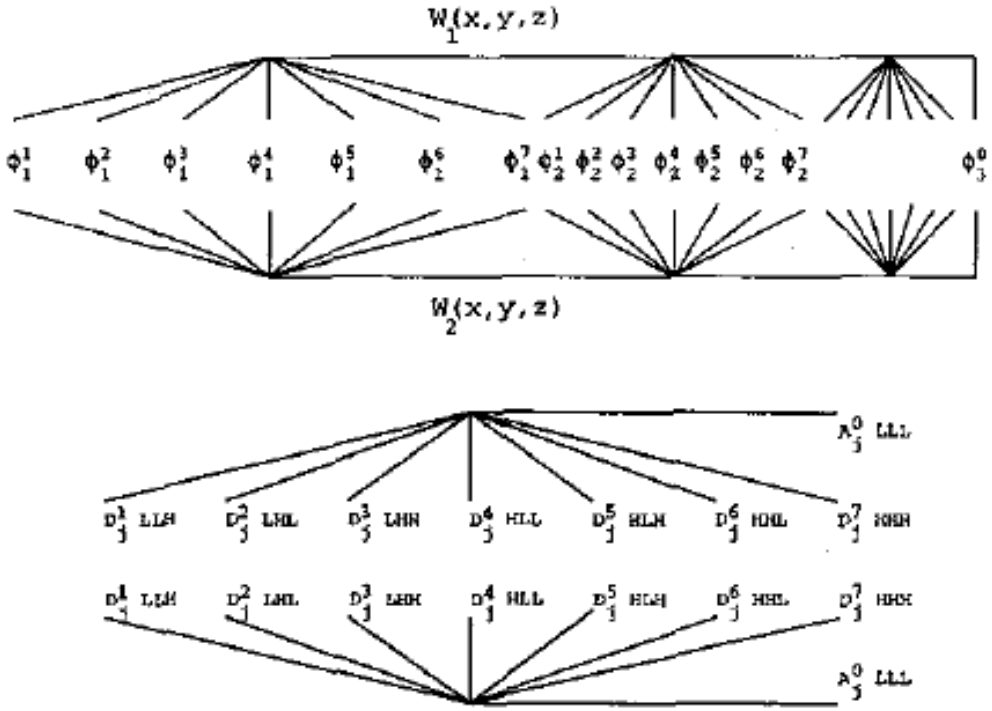
Figure 7: A WT fusion diagram (top) - the upper part of the diagram shows the wavelet decomposition of the first 3-D image, while the lower part - the wavelet decomposition of the second 3-D image; WT fusion diagram notation (bottom).

A number of fusion rules can be used to combine the wavelet coefficients of two 3-D wavelet transforms. Some fusion rules (1, 2, 3) have been suggested by other authors to combine 2-D images. Here we have given their 3-D equivalents. Other,

more advanced fusion schemes (4, 5, 6) are proposed in this study. Some of them have been used by the authors to fuse 3-D phantom and medical images.

$$\begin{aligned} I(x,y,z) &= \omega^{-1}(\phi(\omega(I_1(x,y,z)),\omega(I_2(x,y,z)))) \\ &= \omega^{-1}(\phi(W_1(x,y,z),W_2(x,y,z))) \quad (1) \end{aligned}$$

The fusion rule ϕ is actually a set of fusion rules ϕ_j^c, where $j = 1,..,J$ and $c = 1,\ldots,7$, which define the fusion of each pair of corresponding channels for each band.



1. fusion by averaging [10] (see Figure 5 (middle left and right)) - for each band of decomposition and for each channel the wavelet coefficients of the two images are averaged, i.e. $D_j^c I = (D_j^c I_1 + D_j^c I_2)/2$, $A_J^0 I = (A_J^0 I_1 + A_J^0 I_2)/2$, where $j = 1,..,J$ and $c = 1,\ldots,7$.

2. fusion by maximum [6, 10, 2] (see Figure 5 (bottom left) and Figure 7 (bottom)) - for each band of decomposition and for each channel, the maximum of the respective wavelet coefficients is taken, i.e. $D_j^c I = \max(D_j^c I_1, D_j^c I_2)$, $A_J^0 I = \max(A_J^0 I_1, A_J^0 I_2)$, where $j = 1, .., J$ and $c = 1, \ldots, 7$. An better option is $A_J^0 I = (A_J^0 I_1 + A_J^0 I_2)/2$.

3. high/low fusion [10] (see Figure 5 (bottom right)) - the high frequency information is kept from one image while the low frequency information is kept from the other, e.g. $D_j^c I = D_j^c I_1$ and $A_J^0 I = A_J^0 I_2$, where $j = 1, .., J$ and $c = 1, \ldots, 7$.

4. composite fusion - various combinations of the different channels of $W_1(x, y, z)$ and $W_2(x, y, z)$ are composed, where some channels are taken from the first WT and some from the second.

5. fusion by denoising (hard or soft thresholding) - the wavelet coefficients of the high frequency components $D_j^7 I_k$ are thresholded by either hard or soft thresholding, where $j = 1, .., J$, $c = 1, \ldots, 7$ and $k = \{1, 2\}$. The main goal of thresholding is to remove the noise in the input images. In hard thresholding the absolute values of all wavelet coefficients are compared to a fixed threshold τ. If the magnitude of the coefficient

is less than the threshold, the coefficient is replaced by zero:

$$\tilde{D}_j^c I = \begin{cases} 0 & \text{if } D_j^c I < \tau \\ D_j^c I & \text{otherwise} \end{cases} \qquad (2)$$

Soft thresholding (see Figure 6 (bottom)) shrinks all the wavelet coefficients towards zero:

$$\tilde{D}_j^c I = sign(D_j^c I)(|D_j^c I| - \tau)_+ \qquad (3)$$

6. fusion of the graphs formed from the WT maxima - the WT maxima (the multiscale edges of the 3-D image) can be linked to construct graphs. These graphs can be combined instead of combining all the wavelet coefficients. This fusion technique is based on the results reported in [11, 12].

Several other 2-D WT image fusion algorithms have been proposed in the literature, which are based on some of the principles of visual perception, e.g. fusion using an area based selection rule with a consistency verification [8] or contrast sensitivity fusion [9]. Since some of these methods have been designed specifically to improve the interpretation of fused 2-D images, their three-dimensional analogues are difficult to construct.

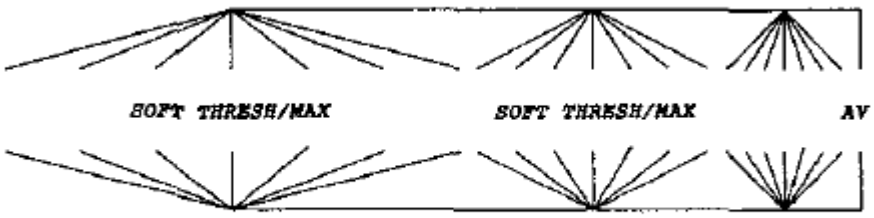
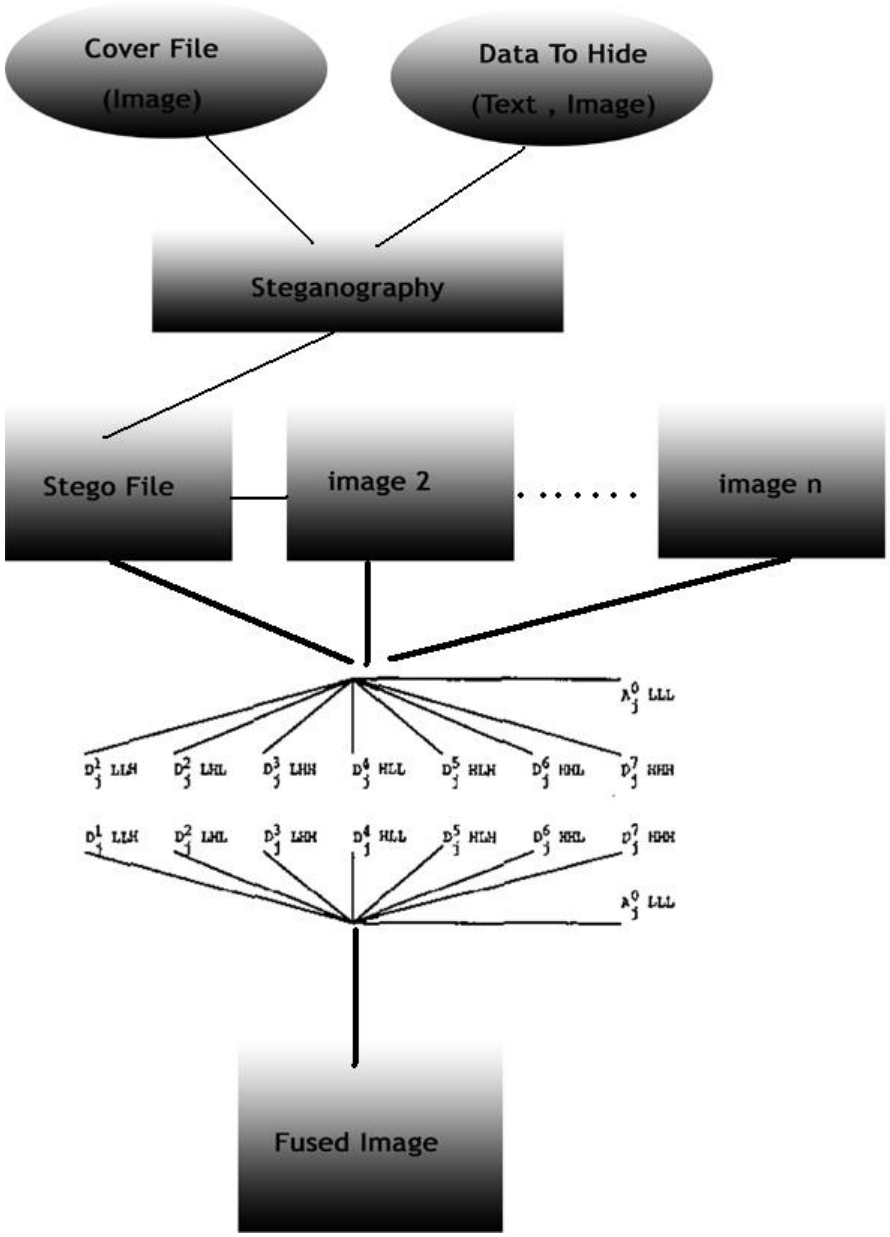


Fig.8. Wavelet transform fusion by soft thresholding and maximum

Fusion diagrams can be used to illustrate more complex WT fusion schemes where one or several filters are applied to each band of the two wavelet transforms prior to fusion (Figure 8). Many multimodality images are made up of both smooth and textured regions. Such images can be segmented in terms of smooth and textured regions by analysing their wavelet transforms [12], and depending on each pair of regions to be combined (i.e.smooth with smooth region, smooth with textured region, textured with textured region), different fusion rules can be used. Several examples of 3-D WT image fusion are presented in this paper.

System Flow Chart



From the flow chart we can get clear idea about our paper. In this paper, we proposed new method of secured data using steganography. The process of steganography is classified into two major parts. They are

- Secret file: Which information going to hide behind the cover file.
- Cover file: Hide the information by using some other file called cover file that is, here we used image file as cover file in this process.

Here image fusion is been done by 3-D Wavelet Transform.

Conclusion

In this paper, information is highly secured by using image fusion in steganography. The proposed technique chops the data in 8 bits after the header and uses LSB to hide data from a pre defined position agreed between two parties. Same position is only used once to enhance security. After get the stegno file to apply to 3-D Wavelet Transform. A very important advantage of using 3-D WT image fusion over alternative image fusion algorithms is that it may be combined with other 3-D image processing algorithms working in the wavelet domain, such as 'smooth versus textured' region segmentation where only a small part of all wavelet coefficients are preserved, and volume rendering [3, 51, where the volume rendering integral is approximated using multiresolution spaces. The integration of 3-D WT image fusion in the broader framework of 3-D WT image processing and visualisation is the ultimate goal of the present study.

References

[1] D. Kahn, the Codebreakers, Macmillan, New York, 1967.
[2] Kesslet, Gary C. An Overview of Steganography for the Computer Forensics Examiner, Burlington, 2004.
[3] Hosmer, Chet. Discovering Hidden Evidence, Cortland, 2006.
[4] Denning, Dorothy E. Information Warfare and Security. Boston, MA: ACM Press, 1999: 310-313
[5] Kafa Rabah. Steganography - The Art of Hiding Data. Information technology Journal 3 (3) - 2004
[6] T. Morkel, J. H. P. Eloff, M. S. Olivier, "An Overview of Image Steganography", Information and Computer Security Architecture (ICSA) Research Group, Department of Computer Science, University of Pretoria, SA.
[7] Bret Dunbar. A detailed look at Steganographic techniques and their use in an open – systems environment: SANS Institute, 2002
[8] Koren I., Laine A., and Taylor F., 1995, "Image fusion using steerable dyadic wavelet transforms". In *Proceedings 1995 IEEE International Conference on Image Processing, Washington D.C.,* IEEE, 232-235.

[9] Chipman L. J. and Orr T. M., 1995, ”Wavelets and image fusion”. In *Proceedings 1995 IEEE International Conference on Image Processing, Washington D.C.,* IEEE, 248-251.

[10] Le Moigne J. and Cromp R. F., 1996, ”The use of wavelets for remote sensing image registration and fusion”. Technical Report TR-96-171, NASA Goddard Space Flight Center.

[11] Mallat S., 1989, “ A theory for multiscale signal decomposition : The wavelet representation”. IEEE Transactions on PAMI, -11(7), 674-693

[12] Porter R. And Canagarajah N., 1996, "A robust Automatic clustering scheme for image segmentation Using wavelets". *IEEE Trunsactions onimage Processing,* -5(4), 662-665.