International Journal of Science and Research (IJSR)
ISSN: 2319-7064
ResearchGate Impact Factor (2018): 0.28 | SJIF (2019): 7.583

Efficient Image Encryption EIE - Compression System Using Haar Wavelets Using Matlab

Kavita[1], Anil Vadhwa[2]

Computer Science & Engineering Department, Rao Pahlad Singh College of Engineering, Mahendergarh, India

Abstract: ***Recently, multimedia and network technologies field is developing rapidly. For that reason privacy and security becomes the leading challenging issues as the data is transmitted openly across the network and along with this, storage space is also an important issue which can't be unseen. So encryption is used to provide the privacy and security to the multimedia, and similarly compression can be used to reduce the storage space. Size reduction also minimizes the transmission time. For securing images, several encryption techniques have been used. In this Report, an efficient image encryption-compression system is designed. The proposed image encryption scheme operated in the prediction error domain is shown to be able to provide a reasonably high level of security. A new image compression algorithm is also implemented using Haar Wavelet Transform which efficiently compresses the encrypted image. By Using Haar wavelet transform with ETC there is better compression efficiency. The approach applied in this Report is proved more efficient in terms of Compression Ratio (CR), Mean Square Error (MSE), Peak Signal to Noise Ratio (PSNR). For implementing the proposed algorithm, the Image Processing Toolbox under MATLAB software is used. Present day application requires various kinds of images and pictures as sources of information for interpretation and analysis. Whenever an image is converted from one form to another such as digitizing, scanning, transmitting, storing, etc., some of the degradation may occur at the output. Hence the output image has to undergo a process called image enhancement which consists of a collection of techniques that seek to improve the visual appearance of the image. Image enhancement is basically improving the interpretability or perception of information in images for human viewer and providing better input for other automated image processing techniques. The Filters Set Theory is incorporated to handle the uncertainties (arising from the deficiencies of information available from situation like the darkness may result from incomplete, imprecise and not fully reliable, vague). The Filters Logic provides a mathematical framework for representation and processing of expert knowledge. The concept of if-then rule plays a role in approximation of variables like cross over point. Also uncertainties within image are not always due to randomness but often due to vagueness and ambiguity.***

Keywords: Image fusion Pixel significance, Multi-focus Multi-sensor Bilateral filter, Cross bilateral filter, Detail image Detail strength

1. Introduction

Medical images are very important in the field of medicine. Many of medical imaging techniques such as Computed Tomography (CT) are used to develop the medical images, produce a sufficient data which requires a large storage area. An average 12-bit X-ray image is nearly 2048 pixels by 2560 pixels dimensionally, converting to a file of size 10,485,760 bytes. An expressive transmission cannot be achieved if the image compression is not efficient, which helps in reducing the file sizes at the same time preserving the image quality.

At first, the compression of medical images begun with using the image preservation techniques such as Scan pixel difference, which is pursued by intra and inter-frame redundancy reduction considered linear. The main challenge coped by medical compression techniques is that there is constant change in the imaging devices and as they used the different techniques to produce the medical images, so the new compression techniques are required. Comprehensively, there are two compression techniques described as follow: Lossless Compression: In the lossless compression technique, when the decompression of compressed image is conducted, the image retrieved is same as the original image before compression

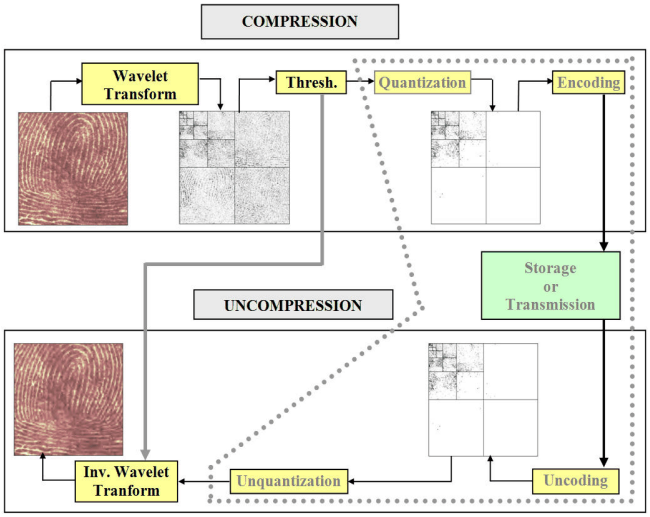

Figure 1: Basic Block Diagram of Image Compression System

Lossy Compression: In the case of lossy compression technique, the image which is compressed if decompressed, the image retrieved is not same as the original image before compression, some of information is lost. The compression ratio of the lossy technique is more than the lossless technique. But the lossy compression techniques are not used extensively in medical imaging. There may be the loss of data which contains useful information, affecting the diagnosis of the patient. An expressive transmission cannot be achieved if the image compression is not efficient,

which helps in reducing the file sizes at the same time preserving the image quality. Encryption-then-Compression System using Haar Wavelet Transform.

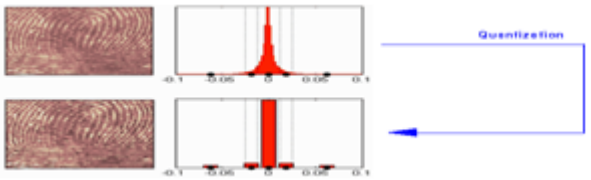

Figure 2: Image Compression using Quantization Process

The development of multimedia and network technologies, the security of multimedia application becomes more and more important, when the multimedia data are transmitted over open networks more and more frequently. Moreover, reliable security is necessary to content protection of digital images and videos. Encryption Techniques for multimedia data needs has to be specifically designed to protect multimedia content and fulfil the security requirements for a particular multimedia application.

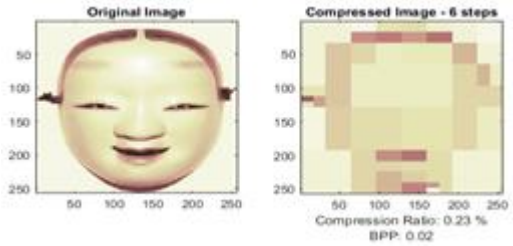

Figure 3: Image Compression using Steganographic Process

In the basic Steganographic process, the secret message is hidden into a cover object. The cover object can be any either a text, an image, an audio file or a video clip.

Human face detection by computer systems has become a major field of interest. Face detection algorithms are used in a wide range of applications, such as security control, video retrieving, biometric signal processing, human computer interface, face recognitions and image database management. However, it is difficult to develop a complete robust face detector due to various light conditions, face sizes, face orientations, background and skin colours. In this report, we propose a face detection method for colour images. Our method detects skin regions over the entire image, and then generates face candidates based on a connected component analysis. Finally, the face candidates are divided into human face and non-face images by an enhanced version of the template-matching method. Experimental results demonstrate successful face detection over the EE368 training images.

Connected Component Analysis The colour segmentation generates a Binary Mask with the same size of the original image.

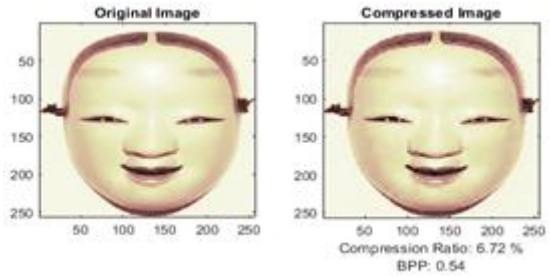

Figure 4: Connected component Analysis

2. Literature Survey

Most of the Pixel significance using cross Wavelet Coefficient work has been limited to monochrome images. Of late, algorithms which utilize human colour perception are attracting the Pixel significance using cross Wavelet Coefficient community with great interest.

Pros and Cons of Cryptography, Steganography and Perturbation "**Clair Bryan, "Steganography: How to Send a Secret Message Cryptology**" was as significant as weapons during the World War II and the Cold War. There were lots of studies to develop robust crypto-systems and to use them in communications. These studies have continued up to now. Today some of those crypto-systems called as "classical crypto-systems" are improved and still being used.

"Popa R.,(1998) "An Analysis of Steganographic System", The "Polyethnic" University of Timisoara, Faculty of Automatics and Computers, Department of Computer Science and Software Engineering "Real Time Images'' in International Journal of Engineering Research and Applications. vol. 3, Issue 2, March -April 2013, pp.1246-1249 Image steganography is an engineering term defining a different and significant discipline for information hiding. This process can be described as „hiding of secret information behind an image". Discrete Wavelet Transform (DWT) is one of the known methods used in steganography. The focus of the proposed work in this report is on decreasing the complexity in image hiding through DWT technique while providing better undetectability and lesser distortion in the stego image

N. Johnson and S. Jajodia, "Steganalysis: The investigation of hidden information", Proc. of the 1998 IEEE Information Technology Conference, 1998. Image steganography has been a vast area of research for many years now. It is a process that hides the secret image behind the cover image in such a way that the presence of the secret image is locked and the cover image appears to be the same.

Cachin C., "An Information-Theoretic, Model for Steganography", in proceeding 2nd Information Hiding Workshop, vol. 1525, pp. 306-318,1998. Discrete wavelet transforms are used to convert the image in spatial domain to frequency domain, where the wavelet coefficients so generated, are modified to conceal the image. In this kind of transformation the wavelet coefficients separates the high and low frequency information on a pixel to pixel basis [3]. The DWT approach applied in the proposed work is the "Haar DWT", simplest of all the wavelet transform approaches. In this transform, time domain is passed through

low-pass and high pass filters and the high and low frequency wavelet coefficients are generated by taking the difference and average of the two pixel values respectively [4].

Nosrati, Masoud, RonakKarimi, HamedNosrati and Maryam Karimi "An introduction to steganography methods," World Applied Programming, Vol 1, No 1, pp. 37-41, Apr. 2011. There are three basic types of secure system by which we can protect or secure our data. Those are Cryptography, Steganography and Perturbation technique. Let us discuss one by one with pros and cons of each one. Cryptography is the science of writing in secret code and is an ancient art[14] .Cryptography is necessary when communicating over any untrusted medium, which includes just about any network, particularly the Internet. Cryptography, then, not only protects data from theft or alteration, but can also be used for user authentication.

Amritha.G ,MeethuVarkey, "Biometric Steganographic Technique Using ADFC and Encryption" in International Journal of Advanced Research in Computer Science and Software Engineering, vol. 3, Issue 3, March 2013. I. STEGANOGRAPHIC METHODS The Internet provides an increasingly broad band of communication as a means to distribute information to the masses. Such information includes text, images, and audio to convey ideas for mass communication.

W. Bender, D. Gruhl, N. Morimoto and A. Lu, "Techniques for Data Hiding," I.B.M. Systems Journal, Vol. 35(3-4): pp. 313-336, 1996. Steganography is the art and science of communicating in such a way that the presence of a message cannot be detected. This report considers steganography with a passive adversary. The model is perhaps best illustrated by Simmons' "Prisoners' Problem" [16]: Alice and Bob are in jail, locked up in separate cells far apart from each other, and wish to devise an escape plan. They are allowed to communicate by means of sending authenticated messages via trusted couriers, provided they do not deal with escape plans.

T. Morkel, J. Eloff, and M. Olivier, "An overview of image steganography," in Proc. of the 5th Annual Information Security South Africa Conference, Sandton, South Africa, Jun/Jul. 2005.

The word steganography comes from the Greek Steganos, which mean covered or secret and –graphy mean writing or drawing. Therefore, steganography means, literally, covered writing. Steganography is the art and science of hiding information such that its presence cannot be detected [7] and a communication is happening [8, 17]. A secret information is encoding in a manner such that the very existence of the information is concealed. Paired with existing communication methods, steganography[12] can be used to carry out hidden exchanges. The main goal of steganography is to communicate securely in a completely undetectable manner [9] and to avoid drawing suspicion to the transmission of a hidden data [10].

H. Wang, and S. Wang, "Cyber warfare: Steganography vs. Steganalysis", Communications of the ACM 47, No.10, pp. 76-82, Oct. 2004. Basically, the purpose of cryptography and steganography is to provide secret communication. However, steganography is not the same as cryptography. Cryptography hides the contents of a secret message from a malicious people, whereas steganography even conceals the existence of the message. Steganography must not be confused with cryptography, where we transform the message so as to make it meaning obscure to a malicious people who intercept it. Therefore, the definition of breaking the system is different [6].

M. Mozammel Hoque Chowdhury, Md. Ezharul Islam, Nasima Begum and Md. Al-Amin Bhuiyan [3] proposed Digital Image Enhancement with Fuzzy Rule-Based . This proposed technique presents a new approach for image enhancement with fuzzy rule-based filtering. Compared to other non-linear techniques, fuzzy filter gives the better performance and is able to represent knowledge in a comprehensible way. Types of image enhancement include: noise reduction, edge enhancement and contrast improvement .This proposed technique presents an enhancement technique based on fuzzy set theory to reduce image noise and to increase the contrast of structures of interest in image. Compared to other techniques, fuzzy method can manage the vagueness and ambiguity in many image processing applications efficiently. The method is able to represent and process human knowledge and applies fuzzy if-then rules.

Fabrizio Russo and Giovanni Ramponi [5] proposed A Fuzzy Operator for the Enhancement of Blurred and Noisy Images. Rule-based fuzzy operators are a novel class of operators specifically designed in order to apply the principles of approximate reasoning to digital image processing. This proposed technique shows how a fuzzy operator that is able to perform detail sharpening but is insensitive to noise can be designed. The results obtainable by the proposed technique in the enhancement of a real image are presented. Fuzzy rules allow processing directives to be described in terms of human-like reasoning.

Prof. Mrs. Preethi S.J, Prof.Mrs. K. Rajeswari [6] Department of Computer Engineering, Pimpri Chinchwad College of Engineering, Pune-44, India proposed Membership Function modification for Image Enhancement using fuzzy logic. Objective of this technique is to introduce ramp membership function and the modification of membership function using square and cube operator for enhancing the visual appearance of digital image using fuzzy logic based approach. The proposed algorithm can be applied to enhance the medical images to make the diagnosis easy or can be applied to color photographs to enhance the visual appearance of the low contrast photographs taken in dark.

I. Suneetha, Dr. T. Venkateswarlu [7] proposed Enhancement Techniques for Gray scale Images in Spatial Domain. Image enhancement plays a vital role in every field where images have to be understood and analyzed. Many images like medical images, satellite

images, microscopy images, aerial images and even real life photographs suffer from poor contrast and noise

ZhiguoGui, Yi Liu [8] proposed An image sharpening algorithm based on fuzzy logic. The proposed technique presents a solution to the problem of enhancing the spatial local contrast of images with nonlinear module. The proposed method that exploits the undedicated discrete fuzzy logic has much reduced noise sensitivity with respect to the linear non sharp masking technique and it permits to obtain perceptually pleasant results. The proposed method also compares favorably with other algorithms which recently have been studied to improve the behavior of the unsharp masking approach. and results are presented and discussed on different images.

R. Pushpavalli, A. Sivaraman[24] proposedImage Enhancement Using Adaptive Neuro-Fuzzy Inference System The proposed technique presents a hybrid filter for de-noising and enhancing digital image in situation where the image is corrupted by salt and pepper noise. Image de-noising and enhancement are important pre processing and post processing steps in image analysis. Successful results of image analysis extremely depend on image enhancement. There are several filters have been illustrated till date. But they are highly sensitive to noise. The structure of the proposed hybrid filter, to make the process robust against noise, is a combination of nonlinear switching median filter and neuro-fuzzy network.

3. Proposed Work

Some drawbacks and limitations of the original model have been mentioned of the diffusion equation, imposed by using the Wavelet Coefficient diffusion coefficient, and proposed a regularized version wherein the coefficient is a function of a smoothed gradient. Investigated the stability of the wavelet coefficient diffusion equation by spatial discretization and proposed a generalized regularization formula in the continuous domain.

a) Proposed Method

The proposed method is composed of several parts. First, SWT is applied to decompose all the sources images into a set of sub-images which contain the important features of these sources images. Then, the MFs are used for these sub-images to generate the corresponding membership matrix for representing the quality of the coefficients of sub-images. At next step, the LSF of membership matrix is calculated to enhance the regional features of the sub-images, and median filter is utilized to remove the abrupt or undesired noises in the LSF of membership matrix.

b) List of Figure Set

The visually important or unimportant pixels for the nonlinear human visual characteristics are related to neighboring pixels, therefore, regional information is very significant for human visual system and image fusion [23], [24]. Due to the membership matrix only represents the pixel information of single point, so it needs regional information in a certain area in order to enhance the effectiveness of feature extraction for the image. Local spatial frequency (LSF) is an excellent technique for describing the regionally detailed information of source image, and it consists of local row frequency (LRF) which can make the regional features of the

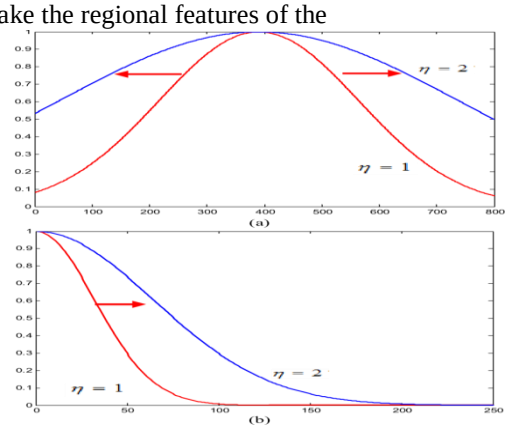

Figure 5: An illustration of MF for low and high frequency sub-images. (a) MF of low frequency sub-image (ηD 1 and ηD 2). (b) MF of high frequency sub-image (ηD 1 and ηD 2). sub-image be easier to extract. Therefore, the fused coefficients would be selected by comparing the value of LSF, as (13)-(15). And an illustration of LSF for membership matrixes of low frequency and high frequency sub-images is shown in Fig. 5, and it shows that the LSF can enhance the features of sub-image.

4. Results and Discussion

In this work we have explored the problem of bottom-up figure-ground segmentation, both as an image segmentation task, and as a perceptual grouping problem. We presented an comprehensive overview of current research in both fields, and discussed reasons why despite a vast research effort, image segmentation and perceptual grouping on unconstrained images continue to be extremely challenging.

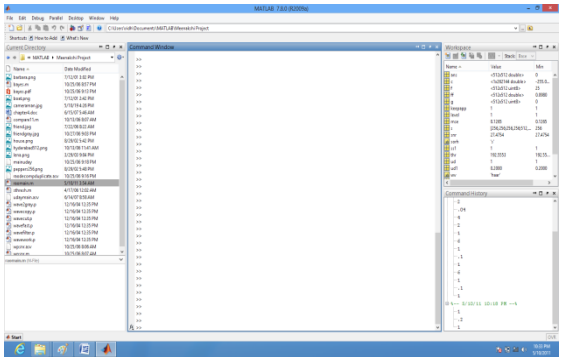

Figure 6: Input image with a PSNR 30.02, (b) The Bayes Shrink method [10]

The development of multimedia and network technologies, the security of multimedia application becomes more and more important, when the multimedia data are transmitted over open networks more and more frequently. Moreover, reliable security is necessary to content protection of digital images and videos. Encryption Techniques for multimedia data needs has to be specifically designed to protect multimedia content and fulfil the security requirements for a particular multimedia application.

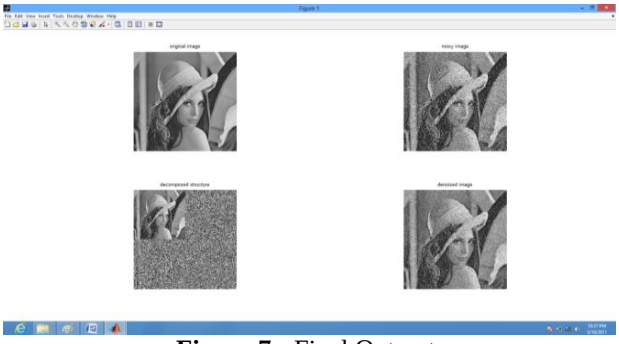

Figure 7: Final Out put

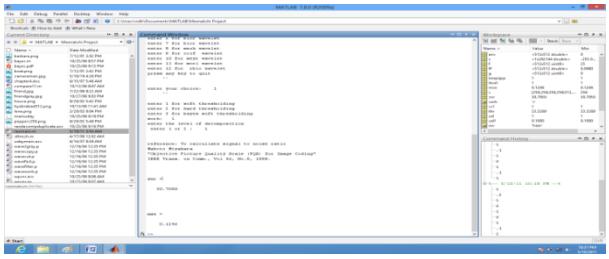

Figure 8: Select Wavelet Coefficient

Most of these information are now collected and stored on electronic computers and transmitted across network to other computer, if this confidential images about enemy positions ,patient ,and geographical areas fall into the wrong hands, After than such a breach of security could lead to lots of war , wrong treatment etc. Protecting confidential images is an ethical and legal requirement.

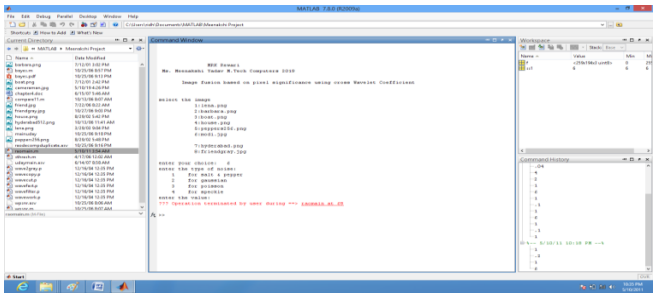

Figure 9: Select Type of Noise

A secret key is also used and the secret message is embedded into the cover object using the secret key.. In this way security is achieved by hiding the existence of the message.

Human face detection by computer systems has become a major field of interest. Face detection algorithms are used in a wide range of applications, such as security control, video retrieving, biometric signal processing, human computer interface, face recognitions and image database management.

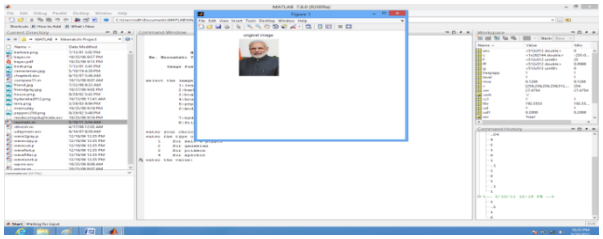

Figure 10: Noise Output

However, it is difficult to develop a complete robust face detector due to various light conditions, face sizes, face orientations, background and skin colors. In this report, we propose a face detection method for color images. Our method detects skin regions over the entire image, and then generates face candidates based on a connected component analysis. Finally, the face candidates are divided into human face and non-face images by an enhanced version of the template-matching method. Experimental results demonstrate successful face detection over the EE368 training images.

		BEW(BIT ERROR RATE)		Entropy	
S.No	Image (.Jpeg)	Existing Method	Proposed Method	Existing Method	Proposed Method
1	Synpic22042	1.5	0.3131	6.3414	12.6996
2	Synpic22043	1.5	0.3855	6.6679	13.1697
3	Synpic22044	1.5	0.3505	5.4066	10.9849
4	Synpic22045	1.5	0.1238	2.924	5.3315
5	Synpic22046	1.5	0.3744	5.4837	10.9892
Average			0.30946		10.63498

Table: Comparisons of BER and the Entropy with the existing system

Figure 11: Result Table

5. Conclusion

In this research work, we have designed an efficient image Encryption-Compression system. Within the proposed framework, the image encryption has to be achieved via random permutation. Highly efficient compression of encrypted image has been realized by a new image compression algorithm of Haar and Daubechies wavelet transform. To proposed ‘designing an Efficient Image Encryption-Then-Compression System with HAAR and DAUBECHIES Wavelet Transform’. Then encrypt image using pseudo random permutation. In this method the pixel values are same after encryption but their position will be changed. The image obtained is nearly similar to the original image due to high correlation between the adjacent pixels. Then compression of encrypted images, majority of pixels are converted to a series of coefficients using an orthogonal transform, and after then the fine information and excessively rough in the coefficients is removed, leading to a reduced data amount. Many Image Compression techniques have been proposed earlier but they were not secure enough and compression ratio is poor. Image Compression could not provide better results as technique used for Compression with DAUBECHIES wavelet alone was not good enough. Therefore Haar wavelet used with Daubechies wavelet for data compression. And propose ‘designing an Efficient Image Encryption-Then-Compression System with HAAR and DAUBECHIES Wavelet Transform. In future the same technique can be extended by applying

different transforms to cover image and thus robustness of algorithm can be verified

References

[1] Popa R.,(1998) "An Analysis of Steganographic System", The "Polyethnic" University of Timisoara, Faculty of Automatics and Computers, Department of Computer Science and Software Engineering "Real Time Images'' in International Journal of Engineering Research and Applications: How to Send a Secret Message Cryptology," 8 Nov. 2001.

[2] **Pros and Cons of Cryptography, Steganography and Perturbation** "**Clair Bryan, "Steganography: How to Send a Secret Message Cryptology** The "Politehnica" University of Timisoara, Faculty of Automatics and Computers, Department of Computer Science and Software Engineering, May 25, 1998.

[3] Miss. PrajaktaDeshmane and Prof. S.R. Jagtap.''Skin Tone Steganography for Real Time Images'' in International Journal of Engineering Research and Applications . vol. 3, Issue 2, March -April 2013, pp.1246-1249

[4] N. Johnson and S. Jajodia, "Steganalysis: The investigation of hidden information", Proc. of the 1998 IEEE Information Technology Conference, 1998.

[5] Cachin C., "An InformamWorkshop, vol. 1525, pp. 306-318, 1998.

[6] Cachin C., "An Information-Theoretic, Model for Steganography", in proceeding 2nd Information Hiding Workshop, vol. 1525, pp. 306-318,1998.

[7] Nosrati, Masoud, RonakKarimi, HamedNosrati and Maryam Karimi "An introduction to steganography methods," World Applied Programming, Vol 1, No 1, pp. 37-41, Apr. 2011.

[8] Amritha.G , MeethuVarkey, "Biometric Steganographic Technique Using IMAGE FUSION BASED ON PIXEL SIGNIFICANCE USING CROSS WAVELET COEFFICIENTand Encryption" in International Journal of Advanced Research in Computer Science and Software Engineering, vol. 3, Issue 3, March 2013.

[9] W. Bender, D. Gruhl, N. Morimoto and A. Lu, "Techniques for Data Hiding," I.B.M. Systems Journal, Vol. 35(3-4): pp. 313-336, 1996.

[10] T. Morkel, J. Eloff, and M. Olivier, "An overview of image steganography," in Proc. of the 5th Annual Information Security South Africa Conference, Sandton, South Africa, Jun/Jul. 2005.

[11] H. Wang, and S. Wang, "Cyber warfare: Steganography vs. Steganalysis", Communications of the ACM 47, No.10, pp. 76-82, Oct. 2004.

[12] AtulKahate, "Cryptographic Techniques," in Computer and Network security, 2nd edition, Tata McGraw-Hill, Ch.2, sec. 2.5, pp.42,1996.

[13] BeenishMehboob and Rashid Aziz Faruqui, "A Steganography Implementation," Biometrics and Security Technologies, ISBAST 2008, International Symposium, pp-1-5, 2008.

[14] L. Davidson and P. Goutam, "Locating secret message in images", in ACM SIGKDD International conference on Knowledge discovery and data mining, Seattle, Washington, 22-25 Aug. 2004, ACM 1-58113-888-1.

[15] Provos, N. and Honeyman, P. (2003) "Hide and Seek: An Introduction to Steganography" IEEE Security and Privacy, vol. 01 (3), pp. 32-44,2003.

[16] Akram, M. Zeki, Azizah A. Manaf and Shayma S. Mahmod "High Watermarking Capacity Based on Spatial Domain Technique", Information Technology Journal, Vol. 10, pp.1367-1373,2011.

[17] **Nikolaidis, N. and Pitas I. (1998) "**Robust image watermarking in the spatial domain", Signal Processing, vol. 66, pp. 385-403,1998.

[18] Anu, Rekha and Praveen (2001) "Digital image steganography", International journal of computer science & informatics, volume-1, issue-ii, 2011.

[19] Akram, M. Zeki, Azizah A. Manaf and Shayma S. Mahmod "High Watermarking Capacity Based on Spatial Domain Technique", Information Technology Journal, Vol. 10, pp.1367-1373,2011.

[20] Richard B., "A Comprehensive Bibliography of Linguistic Steganography",

[21] Abbas Cheddad, Joan Condell, Kevin Curran and Paul McKevitt, "Securing Information Content, using New Encryption Method and Steganography".

[22] Amritha.G and MeethuVarkey,"Biometric Steganographic Technique Using IMAGE FUSION BASED ON PIXEL SIGNIFICANCE USING CROSS WAVELET COEFFICIENTand Encryption", Volume 3, Issue 3, March 2013